Insight 설정

OnCommand Insight

NetApp
April 01, 2024

목차

Insight 설정

Insight를 설정하려면 Insight 라이센스를 활성화하고, 데이터 소스를 설정하고, 사용자와 알림을 정의하고, 백업을 설정하고, 필요한 고급 구성 단계를 수행해야 합니다.

OnCommand Insight 시스템을 설치한 후 다음 설치 작업을 수행해야 합니다.

- Insight 라이센스를 설치합니다.
- Insight에서 데이터 소스 설정
- 사용자 계정을 설정합니다.
- 이메일을 구성합니다.
- 필요한 경우 SNMP, e-메일 또는 syslog 알림을 정의합니다.
- Insight 데이터베이스의 주별 자동 백업을 설정합니다.
- 주석 및 임계값 정의를 포함하여 필요한 고급 구성 단계를 수행합니다.

웹 UI 액세스

OnCommand Insight를 설치한 후에는 라이센스를 설치한 다음 환경을 모니터링할 Insight를 설정해야 합니다. 웹 브라우저를 사용하여 Insight 웹 UI에 액세스하면 됩니다.

단계

1. 다음 중 하나를 수행합니다.

    - Insight 서버에 대한 Insight를 엽니다.

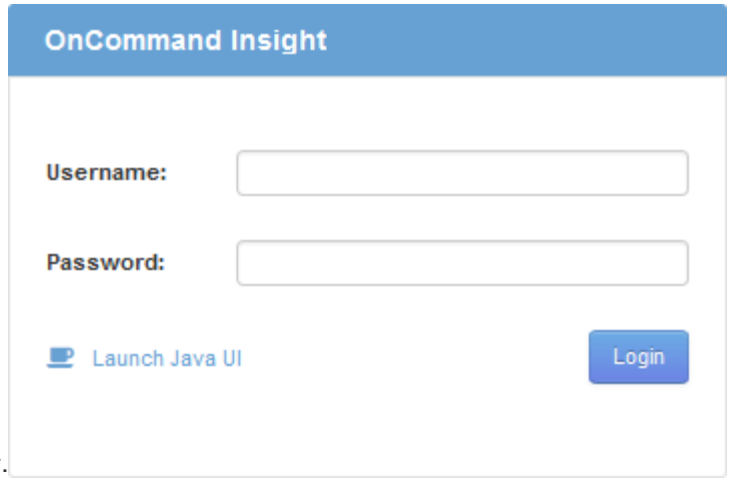
      ```
      https://fqdn
      ```

    - 다른 위치에서 Insight 열기:

      ```
      https://fqdn:port
      ```

      포트 번호는 Insight 서버를 설치할 때 구성된 443 또는 다른 포트입니다. URL에서 포트 번호를 지정하지 않으면 포트 번호는 443으로 기본 설정됩니다.

OnCommand Insight 대화 상자가 표시됩니다.



2. 사용자 이름과 암호를 입력하고 * 로그인 * 을 클릭합니다.

   라이센스가 설치된 경우 데이터 소스 설정 페이지가 표시됩니다.

> 30분 동안 비활성 상태인 Insight 브라우저 세션이 시간 초과되고 시스템에서 자동으로 로그아웃됩니다. 보안 강화를 위해 Insight에서 로그아웃한 후 브라우저를 닫는 것이 좋습니다.

Insight 라이센스 설치

NetApp의 Insight 라이센스 키가 포함된 라이센스 파일을 받으면 설정 기능을 사용하여 모든 라이센스를 동시에 설치할 수 있습니다.

이 작업에 대해

Insight 라이센스 키는 에 저장됩니다 `.txt` 또는 `.lcn` 파일.

단계

1. 텍스트 편집기에서 라이센스 파일을 열고 텍스트를 복사합니다.
2. 브라우저에서 Insight를 엽니다.
3. Insight 도구 모음에서 * Admin * 을 클릭합니다.
4. 설정 * 을 클릭합니다.
5. Licenses * 탭을 클릭합니다.
6. Update License * 를 클릭합니다.
7. 라이센스 키 텍스트를 * 라이센스 * 텍스트 상자에 복사합니다.
8. 업데이트(가장 일반적인) * 작업을 선택합니다.
9. 저장 * 을 클릭합니다.
10. Insight 소비 라이센스 모델을 사용하는 경우 * Send usage information * 섹션에서 * Enable susage information to NetApp * 확인란을 선택해야 합니다. 프록시는 환경에 맞게 적절히 구성 및 설정되어 있어야 합니다.

작업을 마친 후

라이센스를 설치한 후 다음 구성 작업을 수행할 수 있습니다.

- 데이터 소스를 구성합니다.
- OnCommand Insight 사용자 계정을 생성합니다.

OnCommand Insight 라이센스

OnCommand Insight는 Insight 서버에서 특정 기능을 활성화하는 라이센스로 작동합니다.

- * 발견 *

  Discover는 재고를 지원하는 기본 Insight 라이센스입니다. OnCommand Insight를 사용하려면 Discover 라이센스가 있어야 하며 Discover 라이센스가 최소한 하나의 보증, 수행 또는 계획 라이센스와 페어링되어야 합니다.

- * 보증 *

  보증 라이센스는 글로벌 및 SAN 경로 정책, 위반 관리를 비롯한 보증 기능을 지원합니다. 라이선스 보증으로 취약점을 보고 관리할 수도 있습니다.

- * 성능 *

  Perform 라이센스는 자산 페이지, 대시보드 위젯, 쿼리 등의 성능 모니터링을 지원할 뿐 아니라 성능 정책 및 위반 사항을 관리합니다.

- * 계획 *

  플랜 라이센스는 리소스 사용 및 할당을 비롯한 계획 기능을 지원합니다.

- * 호스트 활용률 팩 *

  Host Utilization 라이센스는 호스트 및 가상 머신의 파일 시스템 활용도를 지원합니다.

- * 보고서 작성 *

  보고서 작성 라이센스는 보고를 위한 추가 작성자를 지원합니다. 이 라이센스에는 플랜 라이센스가 필요합니다.

OnCommand Insight 모듈은 연간 기간 또는 영구 라이센스됩니다.

- 검색, 보증, 계획, 모듈 수행을 위해 테라바이트별로 모니터링되는 용량을 기준으로 합니다
- 호스트 활용도 팩의 호스트 수 기준
- 보고서 작성을 위해 필요한 Cognos 전문가 집필자 수 기준

라이센스 키는 각 고객에 대해 생성되는 고유한 문자열 집합입니다. OnCommand Insight 담당자에게 라이센스 키를 받을 수 있습니다.

설치된 라이센스는 소프트웨어에서 사용할 수 있는 다음 옵션을 제어합니다.

- * 발견 *

  재고 확보 및 관리(기초)

  변경 사항을 모니터링하고 인벤토리 정책을 관리합니다

- * 보증 *

  SAN 경로 정책 및 위반 사항을 확인하고 관리합니다

  취약점을 보고 관리합니다

  작업 및 마이그레이션 보기 및 관리

- * 계획 *

  요청을 보고 관리합니다

  보류 중인 작업을 보고 관리합니다

  예약 위반 사항을 보고 관리합니다

  포트 균형 위반을 보고 관리합니다

- * 성능 *

  대시보드 위젯, 자산 페이지 및 쿼리의 데이터를 비롯한 성능 데이터를 모니터링합니다

  성능 정책 및 위반 사항을 확인하고 관리합니다

다음 표에서는 admin 사용자 및 admin이 아닌 사용자에 대한 Perform 라이선스와 함께 사용할 수 있는 기능에 대한 세부 정보를 제공합니다.

기능(관리자)	Perform 라이센스 사용	Perform 라이센스 없음
응용 프로그램	예	성능 데이터 또는 차트가 없습니다
가상 머신	예	성능 데이터 또는 차트가 없습니다
하이퍼바이저	예	성능 데이터 또는 차트가 없습니다
호스트	예	성능 데이터 또는 차트가 없습니다
데이터 저장소	예	성능 데이터 또는 차트가 없습니다
VMDK입니다	예	성능 데이터 또는 차트가 없습니다
내부 볼륨	예	성능 데이터 또는 차트가 없습니다

볼륨	예	성능 데이터 또는 차트가 없습니다
스토리지 풀	예	성능 데이터 또는 차트가 없습니다
디스크	예	성능 데이터 또는 차트가 없습니다
스토리지	예	성능 데이터 또는 차트가 없습니다
스토리지 노드	예	성능 데이터 또는 차트가 없습니다
패브릭	예	성능 데이터 또는 차트가 없습니다
스위치 포트	예	성능 데이터 또는 차트 없음, "포트 오류"는 "해당 없음"으로 표시됨
스토리지 포트입니다	예	예
NPV 포트입니다	예	성능 데이터 또는 차트가 없습니다
스위치	예	성능 데이터 또는 차트가 없습니다
NPV 전환	예	성능 데이터 또는 차트가 없습니다
Qtree	예	성능 데이터 또는 차트가 없습니다
할당량	예	성능 데이터 또는 차트가 없습니다
경로	예	성능 데이터 또는 차트가 없습니다
Zone(영역)	예	성능 데이터 또는 차트가 없습니다
Zone 멤버	예	성능 데이터 또는 차트가 없습니다
일반 장치	예	성능 데이터 또는 차트가 없습니다
테이프	예	성능 데이터 또는 차트가 없습니다
마스킹	예	성능 데이터 또는 차트가 없습니다
iSCSI 세션	예	성능 데이터 또는 차트가 없습니다
ICSI 네트워크 포털	예	성능 데이터 또는 차트가 없습니다

검색	예	예
관리자	예	예
대시보드	예	예
위젯	예	부분적으로 사용 가능(자산, 쿼리 및 관리 위젯만 사용 가능)
위반 대시보드	예	숨김
자산 대시보드	예	부분적으로 사용 가능(스토리지 IOPS 및 VM IOPS 위젯이 숨겨짐)
성능 정책 관리	예	숨김
주석 관리	예	예
주석 규칙을 관리합니다	예	예
애플리케이션 관리	예	예
쿼리	예	예
업무 엔티티를 관리합니다	예	예

피처	사용자 - Perform 라이센스가 있는 경우	게스트 - Perform 라이센스 포함	사용자 - Perform 라이센스가 없습니다	게스트 - Perform 라이센스 없음
자산 대시보드	예	예	부분적으로 사용 가능(스토리지 IOPS 및 VM IOPS 위젯이 숨겨짐)	부분적으로 사용 가능(스토리지 IOPS 및 VM IOPS 위젯이 숨겨짐)
맞춤형 대시보드	보기 전용(만들기, 편집 또는 저장 옵션 없음)	보기 전용(만들기, 편집 또는 저장 옵션 없음)	보기 전용(만들기, 편집 또는 저장 옵션 없음)	보기 전용(만들기, 편집 또는 저장 옵션 없음)
성능 정책 관리	예	숨김	숨김	숨김
주석 관리	예	숨김	예	숨김
애플리케이션 관리	예	숨김	예	숨김

업무 엔티티를 관리합니다	예	숨김	예	숨김
쿼리	예	보기 및 편집만(저장 옵션 없음)	예	보기 및 편집만(저장 옵션 없음)

사용자 계정 설정 및 관리

사용자 계정, 사용자 인증 및 사용자 인증은 Microsoft Active Directory(버전 2 또는 3) LDAP(Lightweight Directory Access Protocol) 서버 또는 내부 OnCommand Insight 사용자 데이터베이스의 두 가지 방법 중 하나로 정의 및 관리할 수 있습니다. 각 사용자에 대해 다른 사용자 계정을 만들면 액세스 권한, 개인 기본 설정 및 책임을 제어할 수 있습니다. 이 작업에 대한 관리자 권한이 있는 계정을 사용합니다.

시작하기 전에

다음 작업을 완료해야 합니다.

- OnCommand Insight 라이센스를 설치합니다.
- 각 사용자에 대해 고유한 사용자 이름을 할당합니다.
- 사용할 암호를 결정합니다.
- 올바른 사용자 역할을 할당합니다.

> 관리자가 비 관리자/표준 사용자의 대화형 로그인을 방지하도록 호스트 운영 체제를 구성하는 것이 보안 모범 사례입니다.

단계

1. 브라우저에서 Insight를 엽니다.
2. Insight 도구 모음에서 * Admin * 을 클릭합니다.
3. 설정 * 을 클릭합니다.
4. 사용자 탭을 선택합니다.
5. 새 사용자를 생성하려면 * Actions * 버튼을 클릭하고 * Add user * 를 선택합니다.

   이름 *, * 암호 *, * 이메일 * 주소를 입력하고 관리자, 사용자 또는 게스트로 * 역할 * 사용자 중 하나를 선택합니다.

6. 사용자 정보를 변경하려면 목록에서 사용자를 선택하고 사용자 설명 오른쪽에 있는 * 사용자 계정 편집 * 기호를 클릭합니다.
7. OnCommand Insight 시스템에서 사용자를 제거하려면 목록에서 사용자를 선택하고 사용자 설명 오른쪽에 있는 * 사용자 계정 삭제 * 를 클릭합니다.

결과

사용자가 OnCommand Insight에 로그인하면 LDAP가 활성화된 경우 서버에서 먼저 LDAP를 통해 인증을 시도합니다. OnCommand Insight가 LDAP 서버에서 사용자를 찾을 수 없는 경우 로컬 Insight 데이터베이스에서 검색합니다.

Insight 사용자 역할

각 사용자 계정에는 세 가지 가능한 권한 수준 중 하나가 할당됩니다.

- 게스트는 Insight에 로그인하고 다양한 페이지를 볼 수 있도록 허용합니다.
- 사용자는 모든 게스트 수준 권한을 허용하며 정책 정의 및 일반 장치 식별과 같은 Insight 작업에 액세스할 수 있습니다. 사용자 계정 유형에서는 데이터 원본 작업을 수행하거나 사용자 계정이 아닌 다른 사용자 계정을 추가 또는 편집할 수 없습니다.
- 관리자는 새 사용자 추가 및 데이터 원본 관리를 포함하여 모든 작업을 수행할 수 있도록 허용합니다.
- 모범 사례: * 사용자 또는 게스트에 대한 대부분의 계정을 만들어 관리자 권한이 있는 사용자의 수를 제한합니다.

LDAP에 대한 **Insight** 구성

OnCommand Insight는 회사 LDAP 도메인에서 구성되므로 LDAP(Lightweight Directory Access Protocol) 설정으로 구성해야 합니다.

LDAP 또는 보안 LDAP(LDAPS)와 함께 사용하도록 Insight를 구성하기 전에 회사 환경의 Active Directory 구성을 기록해 두십시오. Insight 설정은 조직의 LDAP 도메인 구성에 있는 설정과 일치해야 합니다. LDAP와 함께 사용하도록 Insight를 구성하기 전에 아래 개념을 검토하고 LDAP 도메인 관리자에게 해당 환경에서 사용할 수 있는 적절한 속성을 확인하십시오.

모든 보안 Active Directory(예: LDAPS) 사용자의 경우 인증서에 정의된 대로 AD 서버 이름을 정확히 사용해야 합니다. 보안 AD 로그인에 IP 주소를 사용할 수 없습니다.

> OnCommand Insight는 Microsoft Active Directory 서버 또는 Azure AD를 통해 LDAP 및 LDAPS를 지원합니다. 추가 LDAP 구현은 작동할 수 있지만 Insight에서 검증되지 않았습니다. 이 가이드의 절차에서는 Microsoft Active Directory 버전 2 또는 3 LDAP(Lightweight Directory Access Protocol)를 사용하고 있다고 가정합니다.

- 사용자 기본 이름 속성: *

LDAP 사용자 기본 이름 속성(userPrincipalName)은 Insight에서 사용자 이름 속성으로 사용하는 속성입니다. 사용자 주체 이름은 AD(Active Directory) 포리스트에서 전역적으로 고유하도록 보장되지만 많은 대규모 조직에서 사용자의 주 이름이 즉시 분명하지 않거나 알려지지 않을 수 있습니다. 조직에서 기본 사용자 이름에 사용자 기본 이름 속성 대신 을 사용할 수 있습니다.

다음은 User Principal Name 속성 필드에 대한 몇 가지 대체 값입니다.

- * sAMAccountName *

  이 사용자 속성은 기존 Windows 2000 NT 이전 사용자 이름입니다. 대부분의 사용자가 개인 Windows 시스템에 로그인하는 데 익숙합니다. 이는 AD 포리스트 전체에서 전체적으로 고유한 것으로 보장되지는 않습니다.

  > sAMAccountName은 User Principal Name 속성에 대해 대/소문자를 구분합니다.

- 메일 *

  MS Exchange가 있는 AD 환경에서는 이 속성이 최종 사용자의 기본 이메일 주소입니다. 이는 해당 userPrincipalName 특성과 달리 AD 포리스트 전체에서 전역적으로 고유해야 하며 최종 사용자에게 익숙한 것이어야 합니다. 대부분의 비 MS Exchange 환경에는 메일 특성이 없습니다.

- * 조회 *

  LDAP 호출은 요청된 개체의 복사본이 없거나 더 정확하게는 클라이언트 응용 프로그램에 대한 도메인 컨트롤러의 표시 방식입니다. 실제로 존재하는 경우 해당 개체가 될 디렉터리 트리의 섹션을 보유하지 않고 클라이언트에 개체를 보관할 수 있는 위치를 제공합니다. 클라이언트는 도메인 컨트롤러에 대한 DNS 검색 기준으로 조회를 사용합니다. 가장 이상적인 방법은 항상 개체를 포함하는 도메인 컨트롤러를 참조하는 것입니다. 그러나 참조된 도메인 컨트롤러가 다른 조회를 생성할 수는 있지만 일반적으로 개체가 존재하지 않는다는 사실을 발견하고 클라이언트에 알리는 데 시간이 오래 걸리지는 않습니다.

> sAMAccountName은 일반적으로 User Principal Name 보다 선호됩니다. sAMAccountName은 도메인에서 고유하지만(도메인 포리스트에서는 고유하지 않을 수 있음) 일반적으로 로그인에 사용하는 문자열 도메인 사용자입니다(예: *NetApp\username*). 고유 이름은 포리스트의 고유 이름이지만 일반적으로 사용자가 알 수 없습니다.

> 동일한 도메인의 Windows 시스템 부분에서 항상 명령 프롬프트를 열고 set 을 입력하여 적절한 도메인 이름(USERDOMAIN=)을 찾을 수 있습니다. 그러면 OCI 로그인 이름이 가 됩니다 `USERDOMAIN\sAMAccountName`.

도메인 이름 * mydomain.x.y.z.com * 에 를 사용합니다 `DC=x,DC=y,DC=z,DC=com` Insight의 Domain 필드

- 포트 *:

LDAP의 기본 포트는 389이고 LDAPS의 기본 포트는 636입니다

LDAPS의 일반 URL: `ldaps://<ldap_server_host_name>:636`

로그 위치:`\\<install directory>\SANscreen\wildfly\standalone\log\ldap.log`

기본적으로 Insight는 다음 필드에 표시된 값을 예상합니다. Active Directory 환경에서 이러한 변경 사항이 발생할 경우 Insight LDAP 구성에서 변경해야 합니다.

역할 속성
멤버
메일 속성입니다
메일
고유 이름 특성입니다
DistinguishedName입니다

불합격
를 따릅니다

그룹: *

OnCommand Insight 및 DWH 서버에서 서로 다른 액세스 역할을 가진 사용자를 인증하려면 Active Directory에서 그룹을 만들고 OnCommand Insight 및 DWH 서버에 해당 그룹 이름을 입력해야 합니다. 아래 그룹 이름은 예제일 뿐이며 Insight에서 LDAP에 대해 구성하는 이름은 Active Directory 환경에 대해 설정된 이름과 일치해야 합니다.

Insight Group	예
Insight 서버 관리자 그룹	insight.server.admins
Insight administrators 그룹	Insight.admins입니다
Insight 사용자 그룹	insight.users
Insight Guest 그룹	Insight.게스트
보고 관리자 그룹	Insight.report.admins입니다
보고 전문가 저자 그룹	insight.report.proauthors
보고 작성자 그룹	insight.report.business.authors
보고 소비자 그룹	Insight.report.business.consumer 를 참조하십시오
보고 받는 사람 그룹	Insight.report.수신자

LDAP를 사용하여 사용자 정의 구성

LDAP 서버에서 사용자 인증 및 승인을 위해 OnCommand Insight(OCI)를 구성하려면 OnCommand Insight 서버 관리자로 LDAP 서버에 정의되어 있어야 합니다.

시작하기 전에

LDAP 도메인에서 Insight에 대해 구성된 사용자 및 그룹 속성을 알아야 합니다.

모든 보안 Active Directory(예: LDAPS) 사용자의 경우 인증서에 정의된 대로 AD 서버 이름을 정확히 사용해야 합니다. 보안 AD 로그인에 IP 주소를 사용할 수 없습니다.

이 작업에 대해

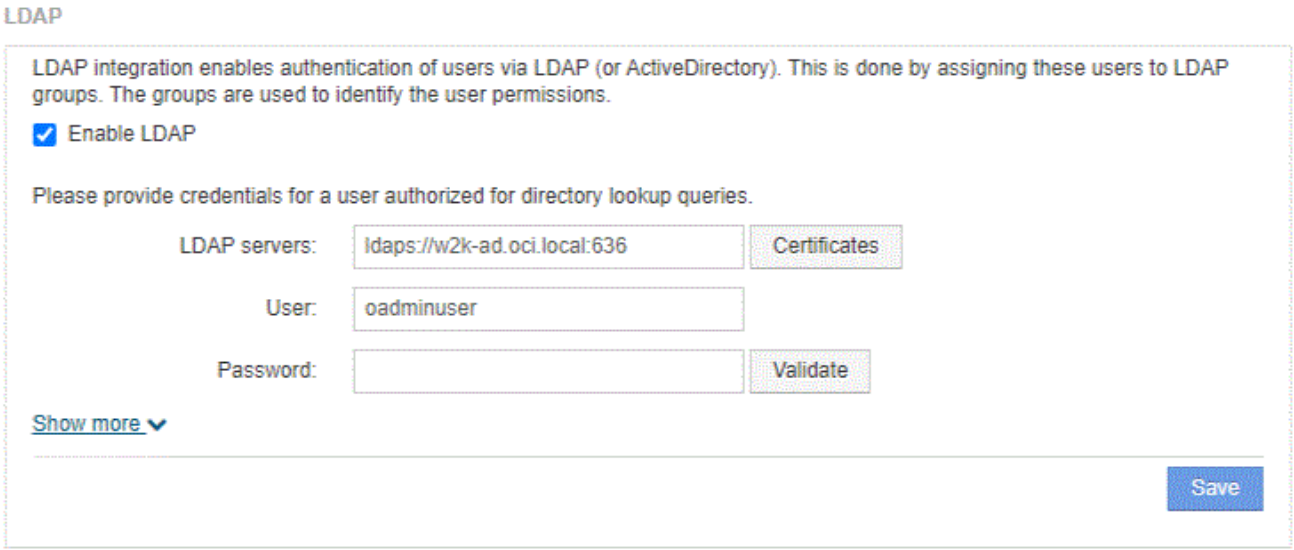
OnCommand Insight는 Microsoft Active Directory 서버를 통해 LDAP 및 LDAPS를 지원합니다. 추가 LDAP 구현은 작동할 수 있지만 Insight에서 검증되지 않았습니다. 이 절차에서는 Microsoft Active Directory 버전 2 또는 3

LDAP(Lightweight Directory Access Protocol)를 사용하고 있다고 가정합니다.

LDAP 사용자는 * Admin * > menu:Setup [Users](설정 [사용자]) 목록에 로컬로 정의된 사용자와 함께 표시됩니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 설정 * 을 클릭합니다.
3. 사용자 * 탭을 클릭합니다.
4. 여기에 표시된 것처럼 LDAP 섹션으로 스크롤합니다.



5. LDAP 사용자 인증 및 권한 부여를 허용하려면 * LDAP 활성화 * 를 클릭합니다.
6. 다음 필드에 내용을 입력합니다.

   - `LDAP servers`:Insight는 쉼표로 구분된 LDAP URL 목록을 허용합니다. Insight는 LDAP 프로토콜의 유효성을 검사하지 않고 제공된 URL에 연결을 시도합니다.

     > LDAP 인증서를 가져오려면 * Certificates * 를 클릭하고 인증서 파일을 자동으로 가져오거나 수동으로 찾습니다.

     LDAP 서버를 식별하는 데 사용되는 IP 주소 또는 DNS 이름은 일반적으로 다음 형식으로 입력됩니다.

     ```
     ldap://<ldap-server-address>:port
     ```

     또는 기본 포트를 사용하는 경우:

     ```
     ldap://<ldap-server-address>
     ```

     + 이 필드에 여러 LDAP 서버를 입력할 때 각 항목에 올바른 포트 번호가 사용되는지 확인하십시오.

- `User name`: LDAP 서버에서 디렉터리 조회 쿼리에 대해 승인된 사용자의 자격 증명을 입력합니다.
- `Password`: 위 사용자의 암호를 입력합니다. LDAP 서버에서 이 암호를 확인하려면 * Validate * 를 클릭합니다.

7. 이 LDAP 사용자를 보다 정확하게 정의하려면 * 더 보기 * 를 클릭하고 나열된 속성의 필드를 채웁니다.

   이러한 설정은 LDAP 도메인에 구성된 속성과 일치해야 합니다. 이러한 필드에 입력할 값이 확실하지 않으면 Active Directory 관리자에게 문의하십시오.

   - * Admins 그룹 *

     Insight Administrator 권한이 있는 사용자를 위한 LDAP 그룹입니다. 기본값은 입니다 `insight.admins`.

   - * 사용자 그룹 *

     Insight 사용자 권한이 있는 사용자를 위한 LDAP 그룹입니다. 기본값은 입니다 `insight.users`.

   - * 손님 그룹 *

     Insight 게스트 권한이 있는 사용자를 위한 LDAP 그룹입니다. 기본값은 입니다 `insight.guests`.

   - * 서버 관리자 그룹 *

     Insight Server 관리자 권한이 있는 사용자를 위한 LDAP 그룹입니다. 기본값은 입니다 `insight.server.admins`.

   - * 시간 초과 *

     시간 초과 전에 LDAP 서버의 응답을 기다리는 시간(밀리초)입니다. 기본값은 2,000이며, 모든 경우에 적절하며 수정할 수 없습니다.

   - * 도메인 *

     OnCommand Insight가 LDAP 사용자를 찾기 시작해야 하는 LDAP 노드입니다. 일반적으로 조직의 최상위 도메인입니다. 예를 들면 다음과 같습니다.

     ```
     DC=<enterprise>,DC=com
     ```

   - * 사용자 기본 이름 속성 *

     LDAP 서버의 각 사용자를 식별하는 속성입니다. 기본값은 입니다 `userPrincipalName`이는 세계적으로 고유한 기능입니다. OnCommand Insight는 이 특성의 내용과 위에서 제공한 사용자 이름을 일치시킵니다.

   - * 역할 속성 *

     지정된 그룹 내에서 사용자의 맞춤을 식별하는 LDAP 속성입니다. 기본값은 입니다 `memberOf`.

   - * 메일 속성 *

     사용자의 이메일 주소를 식별하는 LDAP 속성입니다. 기본값은 입니다 `mail`. 이 기능은 OnCommand Insight에서 제공하는 보고서를 구독하려는 경우에 유용합니다. Insight는 각 사용자가 처음 로그인할 때

사용자의 이메일 주소를 선택하며, 그 후에는 이를 찾아보지 않습니다.

> LDAP 서버에서 사용자의 이메일 주소가 변경되면 Insight에서 업데이트해야 합니다.

◦ * 고유 이름 특성 *

사용자의 고유 이름을 식별하는 LDAP 속성입니다. 기본값은 입니다 `distinguishedName`.

8. 저장 * 을 클릭합니다.

사용자 암호 변경

관리자 권한이 있는 사용자는 로컬 서버에 정의된 OnCommand Insight 사용자 계정의 암호를 변경할 수 있습니다.

시작하기 전에

다음 항목을 완료해야 합니다.

- 수정하려는 사용자 계정에 로그인하는 모든 사용자에게 알림.
- 이 변경 후 사용할 새 암호입니다.

이 작업에 대해

이 방법을 사용할 때는 LDAP를 통해 유효성이 검증된 사용자의 암호를 변경할 수 없습니다.

단계

1. 관리자 권한으로 로그인합니다.
2. Insight 도구 모음에서 * Admin * 을 클릭합니다.
3. 설정 * 을 클릭합니다.
4. 사용자 * 탭을 클릭합니다.
5. 수정할 사용자 계정이 표시된 행을 찾습니다.
6. 사용자 정보 오른쪽에서 * 사용자 계정 편집 * 을 클릭합니다.
7. 새 * 암호 * 를 입력한 다음 확인 필드에 다시 입력합니다.
8. 저장 * 을 클릭합니다.

사용자 정의 편집

관리자 권한이 있는 사용자는 사용자 계정을 편집하여 OnCommand Insight 또는 DWH 및 보고 기능의 이메일 주소 또는 역할을 변경할 수 있습니다.

시작하기 전에

변경해야 하는 사용자 계정 유형(OnCommand Insight, DWH 또는 조합)을 확인합니다.

이 작업에 대해

LDAP 사용자의 경우 이 방법을 사용해서만 이메일 주소를 수정할 수 있습니다.

단계

1. 관리자 권한으로 로그인합니다.
2. Insight 도구 모음에서 * Admin * 을 클릭합니다.
3. 설정 * 을 클릭합니다.
4. 사용자 * 탭을 클릭합니다.
5. 수정할 사용자 계정이 표시된 행을 찾습니다.
6. 사용자 정보 오른쪽에서 * 사용자 계정 편집 * 아이콘을 클릭합니다.
7. 필요한 사항을 변경합니다.
8. 저장 * 을 클릭합니다.

사용자 계정을 삭제하는 중입니다

관리자 권한이 있는 사용자는 사용자 계정을 더 이상 사용하지 않을 때(로컬 사용자 정의용) 삭제하거나 사용자가 다음에 로그인할 때(LDAP 사용자의 경우) OnCommand Insight에서 사용자 정보를 다시 검색하도록 할 수 있습니다.

단계

1. 관리자 권한으로 OnCommand Insight에 로그인합니다.
2. Insight 도구 모음에서 * Admin * 을 클릭합니다.
3. 설정 * 을 클릭합니다.
4. 사용자 * 탭을 클릭합니다.
5. 삭제할 사용자 계정을 표시하는 행을 찾습니다.
6. 사용자 정보 오른쪽에서 * 사용자 계정 삭제 * " * x * " 아이콘을 클릭합니다.
7. 저장 * 을 클릭합니다.

로그인 경고 메시지 설정

OnCommand Insight를 사용하면 관리자가 사용자가 로그인할 때 표시되는 사용자 지정 텍스트 메시지를 설정할 수 있습니다.

단계

1. OnCommand Insight 서버에서 메시지를 설정하려면 다음을 수행하십시오.
   a. 관리 [문제 해결 > 고급 문제 해결 > 고급 설정] 메뉴로 이동합니다.
   b. 텍스트 영역에 로그인 메시지를 입력합니다.

c. 클라이언트 디스플레이 로그인 경고 메시지 * 확인란을 클릭합니다.

d. 저장 * 을 클릭합니다.

모든 사용자에 대해 로그인할 때 메시지가 표시됩니다.

2. DWH(Data Warehouse) 및 Cognos(Reporting)에서 메시지를 설정하려면

a. 시스템 정보 * 로 이동하여 * 로그인 경고 * 탭을 클릭합니다.

b. 텍스트 영역에 로그인 메시지를 입력합니다.

c. 저장 * 을 클릭합니다.

이 메시지는 모든 사용자의 DWH 및 Cognos 보고 로그인에 표시됩니다.

Insight Security 를 참조하십시오

OnCommand Insight 7.3.1에서는 향상된 보안으로 Insight 환경을 운영할 수 있는 보안 기능이 도입되었습니다. 암호화, 암호 해싱의 개선, 암호를 암호화하고 해독하는 내부 사용자 암호 및 키 쌍 변경 기능이 포함되어 있습니다. Insight 환경의 모든 서버에서 이러한 기능을 관리할 수 있습니다.

Insight의 기본 설치에는 사용자 환경의 모든 사이트에서 동일한 키와 동일한 기본 암호를 공유하는 보안 구성이 포함됩니다. 중요 데이터를 보호하려면 설치 또는 업그레이드 후에 기본 키와 취득 사용자 암호를 변경하는 것이 좋습니다.

데이터 소스 암호화된 암호는 Insight Server 데이터베이스에 저장됩니다. 서버에 공개 키가 있으며 사용자가 WebUI 데이터 소스 구성 페이지에 암호를 입력할 때 암호를 암호화합니다. 서버에 Server 데이터베이스에 저장된 데이터 소스 암호를 해독하는 데 필요한 개인 키가 없습니다. 획득 장치(Lau, RAU)만 데이터 소스 암호를 해독하는 데 필요한 데이터 소스 개인 키를 가지고 있습니다.

서버 키를 다시 입력합니다

기본 키를 사용하면 환경에 보안 취약점이 발생합니다. 기본적으로 데이터 소스 암호는 Insight 데이터베이스에 암호화됩니다. 모든 Insight 설치에 공통적으로 사용되는 키를 사용하여 암호화됩니다. 기본 구성에서 NetApp에 전송된 Insight 데이터베이스에는 이론적으로 NetApp에 의해 암호 해독될 수 있는 암호가 포함되어 있습니다.

획득 사용자 암호 변경

기본 '획득' 사용자 암호를 사용하면 환경에 보안 취약점이 발생합니다. 모든 획득 장치는 ""획득" 사용자를 사용하여 서버와 통신합니다. 기본 암호가 있는 RA는 이론적으로 기본 암호를 사용하여 모든 Insight 서버에 연결할 수 있습니다.

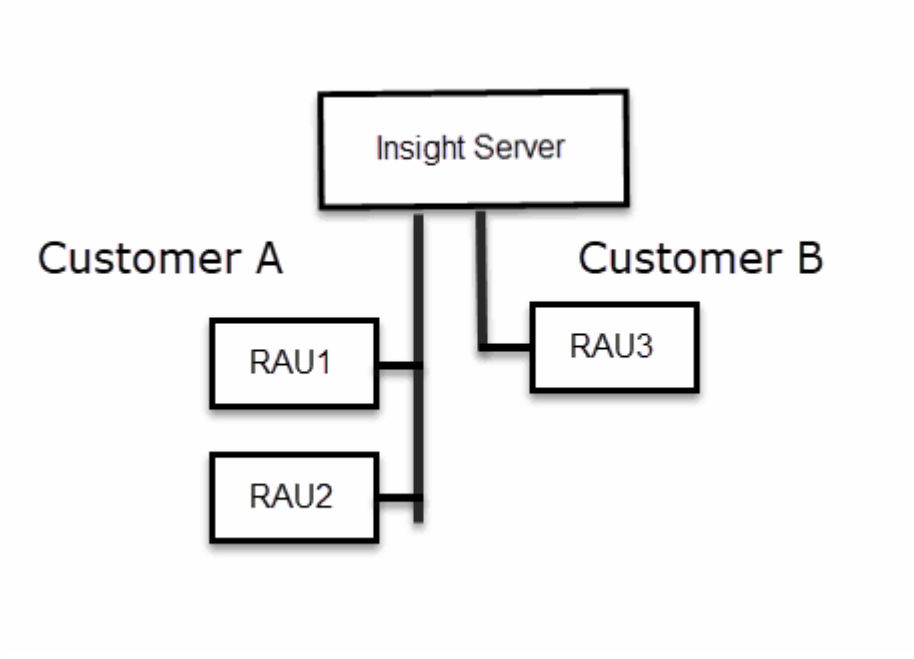
업그레이드 및 설치 고려 사항

Insight 시스템에 기본 보안 구성이 아닌 구성(암호 키를 다시 입력하거나 변경한 경우)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.

복잡한 서비스 공급자 환경에서 키 관리

서비스 공급자는 데이터를 수집하는 여러 OnCommand Insight 고객을 호스팅할 수 있습니다. 이 키는 Insight 서버의 여러 고객이 무단으로 고객 데이터에 액세스하지 못하도록 보호합니다. 각 고객의 데이터는 특정 키 쌍으로 보호됩니다.

이 Insight 구현은 다음 그림과 같이 구성할 수 있습니다.



이 구성에서는 각 고객에 대해 개별 키를 생성해야 합니다. 고객 A는 두 RA 모두에 대해 동일한 키를 필요로 합니다. 고객 B에는 단일 키 세트가 필요합니다.

고객 A의 암호화 키를 변경하는 단계:

1. RAU1을 호스팅하는 서버에 원격 로그인을 수행합니다.
2. 보안 관리 도구를 시작합니다.
3. 기본 키를 대체하려면 암호화 키 변경 을 선택합니다.
4. 백업 을 선택하여 보안 구성의 백업 zip 파일을 생성합니다.
5. RAU2를 호스팅하는 서버에 원격 로그인을 수행합니다.
6. 보안 구성의 백업 zip 파일을 RAU2에 복사합니다.
7. 보안 관리 도구를 시작합니다.
8. 보안 백업을 RAU1에서 현재 서버로 복원합니다.

고객 B의 암호화 키를 변경하는 단계:

1. RAU3을 호스팅하는 서버에 원격 로그인을 수행합니다.
2. 보안 관리 도구를 시작합니다.
3. 기본 키를 대체하려면 암호화 키 변경 을 선택합니다.
4. 백업 을 선택하여 보안 구성의 백업 zip 파일을 생성합니다.

Insight 서버의 보안 관리

를 클릭합니다 `securityadmin` 도구를 사용하면 Insight 서버의 보안 옵션을 관리할 수 있습니다. 보안 관리에는 암호 변경, 새 키 생성, 사용자가 만든 보안 구성 저장 및 복원, 기본 설정으로 구성 복원 등이 포함됩니다.

이 작업에 대해

를 사용합니다 `securityadmin` 보안 관리 도구:

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

단계

1. Insight 서버에 원격 로그인을 수행합니다.
2. 대화형 모드에서 보안 관리 도구를 시작합니다.
   - 윈도우 - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     시스템에서 로그인 자격 증명을 요청합니다.
3. "Admin" 자격 증명이 있는 계정의 사용자 이름과 암호를 입력합니다.
4. 서버 * 를 선택합니다.

   다음 서버 구성 옵션을 사용할 수 있습니다.

   - * 백업 *

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

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

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

     > 복원은 여러 서버의 암호와 키를 동기화하는 데 사용할 수 있습니다. 예를 들어 - 한 서버의 서버 암호화 키 변경 - 볼트 백업 작성 - 두 번째 서버로 볼트 백업을 복원합니다
   - * 암호화 키 변경 *

     프록시 사용자 암호, SMTP 사용자 암호, LDAP 사용자 암호 등을 암호화 또는 해독하는 데 사용되는 서버 암호화 키를 변경합니다.

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

- * 암호 업데이트 *

  Insight에서 사용하는 내부 계정의 암호를 변경합니다. 다음 옵션이 표시됩니다.

  - _내부
  - 획득
  - Cognos_admin
  - DWh _ 내부
  - 호스트
  - 인벤토리
  - 루트

> 암호를 변경할 때 일부 계정을 동기화해야 합니다. 예를 들어, 서버에서 'acquisition' 사용자의 암호를 변경하는 경우 Lau, RAU 및 DWH에서 'acquisition' 사용자의 암호를 변경하여 일치시켜야 합니다. 또한 암호를 변경할 때는 업그레이드 또는 설치 후에 복원할 수 있도록 새 보안 구성을 백업해야 합니다.

- * 기본값으로 재설정 *

  키와 암호를 기본값으로 재설정합니다. 기본값은 설치 중에 제공되는 값입니다.

- * 종료 *

  를 종료합니다 `securityadmin` 도구.

  a. 변경할 옵션을 선택하고 화면의 지시를 따릅니다.

로컬 획득 장치의 보안 관리

를 클릭합니다 `securityadmin` 도구를 사용하면 로컬 획득 사용자(Lau)의 보안 옵션을 관리할 수 있습니다. 보안 관리에는 키 및 암호 관리, 사용자가 만들고 복원한 보안 구성을 기본 설정으로 저장 및 복원하는 작업이 포함됩니다.

시작하기 전에

이(가) 있어야 합니다 `admin` 보안 구성 작업을 수행할 수 있는 권한.

이 작업에 대해

를 사용합니다 `securityadmin` 보안 관리 도구:

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

단계

1. Insight 서버에 원격 로그인을 수행합니다.
2. 대화형 모드에서 보안 관리 도구를 시작합니다.
   - 윈도우 - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     시스템에서 로그인 자격 증명을 요청합니다.
3. "Admin" 자격 증명이 있는 계정의 사용자 이름과 암호를 입력합니다.
4. Local Acquisition Unit(로컬 획득 장치) * 을 선택하여 Local Acquisition Unit(로컬 획득 장치) 보안 구성을 재구성합니다.

   다음 옵션이 표시됩니다.

   - * 백업 *

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

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

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

     > 복원을 사용하여 여러 서버의 패스워드와 키를 동기화할 수 있습니다. 예를 들어: - Lau에서 암호화 키 변경 - 볼트 백업 작성 - 각 RA에 볼트 백업을 복원합니다
   - * 암호화 키 변경 *

     장치 암호를 암호화 또는 해독하는 데 사용되는 AU 암호화 키를 변경합니다.

     > 암호화 키를 변경할 때는 업그레이드 또는 설치 후 복원할 수 있도록 새 보안 구성을 백업해야 합니다.
   - * 암호 업데이트 *

     '촬영' 사용자 계정의 암호를 변경합니다.

     > 암호를 변경할 때 일부 계정을 동기화해야 합니다. 예를 들어, 서버에서 'acquisition' 사용자의 암호를 변경하는 경우 Lau, RAU 및 DWH에서 'acquisition' 사용자의 암호를 변경하여 일치시켜야 합니다. 또한 암호를 변경할 때는 업그레이드 또는 설치 후에 복원할 수 있도록 새 보안 구성을 백업해야 합니다.
   - * 기본값으로 재설정 *

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

값입니다.

- * 종료 *

  를 종료합니다 `securityadmin` 도구.

5. 구성할 옵션을 선택하고 화면의 지시를 따릅니다.

RAU에 대한 보안 관리

를 클릭합니다 `securityadmin` 도구를 사용하면 RA의 보안 옵션을 관리할 수 있습니다. 볼트 구성을 백업 또는 복원하거나 암호화 키를 변경하거나 획득 장치의 암호를 업데이트해야 할 수 있습니다.

이 작업에 대해

를 사용합니다 `securityadmin` 보안 관리 도구:

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

Lau, RAU에 대한 보안 구성을 업데이트하는 한 가지 시나리오는 해당 사용자의 암호가 서버에서 변경된 경우 'acquisition' 사용자 암호를 업데이트하는 것입니다. 모든 RA와 Lau는 서버 '획득' 사용자의 암호와 동일한 암호를 사용하여 서버와 통신합니다.

'acquisition' 사용자는 Insight 서버에만 있습니다. RAU 또는 Lau는 서버에 연결할 때 해당 사용자로 로그인합니다.

RAU에서 보안 옵션을 관리하려면 다음 단계를 따르십시오.

단계

1. RAU를 실행 중인 서버에 원격 로그인을 수행한다
2. 대화형 모드에서 보안 관리 도구를 시작합니다.
   - 윈도우 - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     시스템에서 로그인 자격 증명을 요청합니다.

3. "Admin" 자격 증명이 있는 계정의 사용자 이름과 암호를 입력합니다.

   RAU에 대한 메뉴가 표시됩니다.

   - * 백업 *

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

     - 윈도우 - `C:\Program Files\SANscreen\backup\vault`

    - Linux - `/var/log/netapp/oci/backup/vault`

  - * 복원 *

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

    > 복원은 여러 서버의 암호와 키를 동기화하는 데 사용할 수 있습니다. 예를 들어 - 한 서버의 암호화 키 변경 - 볼트 백업 작성 - 두 번째 서버로 볼트 백업을 복원합니다

  - * 암호화 키 변경 *

    단말기 암호를 암호화 또는 해독하는 데 사용되는 RAU 암호화 키를 변경합니다.

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

  - * 암호 업데이트 *

    '촬영' 사용자 계정의 암호를 변경합니다.

    > 암호를 변경할 때 일부 계정을 동기화해야 합니다. 예를 들어, 서버에서 'acquisition' 사용자의 암호를 변경하는 경우 Lau, RAU 및 DWH에서 'acquisition' 사용자의 암호를 변경하여 일치시켜야 합니다. 또한 암호를 변경할 때는 업그레이드 또는 설치 후에 복원할 수 있도록 새 보안 구성을 백업해야 합니다.

  - * 기본값으로 재설정 *

    암호화 키 및 암호를 기본값으로 재설정합니다. 기본값은 설치 중에 제공되는 값입니다.

  - * 종료 *

    를 종료합니다 `securityadmin` 도구.

데이터 웨어하우스의 보안 관리

를 클릭합니다 `securityadmin` 도구를 사용하면 데이터 웨어하우스 서버의 보안 옵션을 관리할 수 있습니다. 보안 관리에는 DWH 서버의 내부 사용자에 대한 내부 암호 업데이트, 보안 구성 백업 생성 또는 기본 설정으로 구성 복원이 포함됩니다.

이 작업에 대해

를 사용합니다 `securityadmin` 보안 관리 도구:

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

단계

1. 데이터 웨어하우스 서버에 원격 로그인을 수행합니다.

2. 대화형 모드에서 보안 관리 도구를 시작합니다.
   - 윈도우 - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     시스템에서 로그인 자격 증명을 요청합니다.

3. "Admin" 자격 증명이 있는 계정의 사용자 이름과 암호를 입력합니다.

   데이터 웨어하우스에 대한 보안 관리 메뉴가 표시됩니다.

   - * 백업 *

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

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

   - * 복원 *

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

     > 복원은 여러 서버의 암호와 키를 동기화하는 데 사용할 수 있습니다. 예를 들어 - 한 서버의 암호화 키 변경 - 볼트 백업 작성 - 두 번째 서버로 볼트 백업을 복원합니다
     >
     > 를 누릅니다

   - * 암호화 키 변경 *

     커넥터 암호 및 SMPT 암호와 같은 암호를 암호화 또는 해독하는 데 사용되는 DWH 암호화 키를 변경합니다.

   - * 암호 업데이트 *

     특정 사용자 계정의 암호를 변경합니다.

     - _내부
     - 획득
     - Cognos_admin
     - 드Wh
     - DWh _ 내부
     - Dwhuser(사용자)
     - 호스트
     - 인벤토리
     - 루트

> dwhuser, hosts, inventory 또는 root 암호를 변경하면 SHA-256 암호 해싱을 사용할 수 있습니다. 이 옵션을 사용하려면 계정에 액세스하는 모든 클라이언트가 SSL 연결을 사용해야 합니다.

+

- * 기본값으로 재설정 *

  암호화 키 및 암호를 기본값으로 재설정합니다. 기본값은 설치 중에 제공되는 값입니다.

- * 종료 *

  를 종료합니다 `securityadmin` 도구.

OnCommand Insight 내부 사용자 암호 변경

보안 정책에 따라 OnCommand Insight 환경의 암호를 변경해야 할 수 있습니다. 한 서버의 암호 중 일부는 환경의 다른 서버에 있으므로 두 서버의 암호를 변경해야 합니다. 예를 들어, Insight Server에서 ""인벤토리"" 사용자 암호를 변경할 경우 해당 Insight Server에 대해 구성된 데이터 웨어하우스 서버 Connector의 ""인벤토리"" 사용자 암호와 일치해야 합니다.

시작하기 전에

> 암호를 변경하기 전에 사용자 계정의 종속성을 이해해야 합니다. 필요한 모든 서버에서 암호를 업데이트하지 못하면 Insight 구성 요소 간의 통신 장애가 발생합니다.

이 작업에 대해

다음 표에는 Insight Server의 내부 사용자 암호가 나열되어 있으며 새 암호와 일치해야 하는 종속 암호가 있는 Insight 구성 요소가 나열되어 있습니다.

Insight Server 암호	필수 변경 사항
_내부	
획득	Lau, RAU
DWh _ 내부	데이터 웨어하우스
호스트	
인벤토리	데이터 웨어하우스
루트	

다음 표에는 데이터 웨어하우스에 대한 내부 사용자 암호가 나열되어 있으며 새 암호와 일치해야 하는 종속 암호가 있는 Insight 구성 요소가 나열되어 있습니다.

데이터 웨어하우스 암호	필수 변경 사항
Cognos_admin	
드Wh	
dWh_INTERNAL(서버 커넥터 구성 UI를 사용하여 변경)	Insight 서버
Dwhuser(사용자)	
호스트	
인벤토리(서버 커넥터 구성 UI를 사용하여 변경됨)	Insight 서버
루트	

- DWH 서버 연결 구성 UI * 에서 암호 변경

다음 표에는 Lau의 사용자 암호와 새 암호와 일치해야 하는 종속 암호가 있는 Insight 구성 요소가 나열되어 있습니다.

Lau 암호	필수 변경 사항
획득	Insight 서버, RAU

서버 연결 구성 **UI**를 사용하여 **"inventory"** 및 **"dWh_internal"** 암호 변경

데이터 웨어하우스 UI를 사용하는 Insight 서버의 암호와 일치하도록 ""인벤토리" 또는 ""DIH_INTERNAL"" 암호를 변경해야 하는 경우

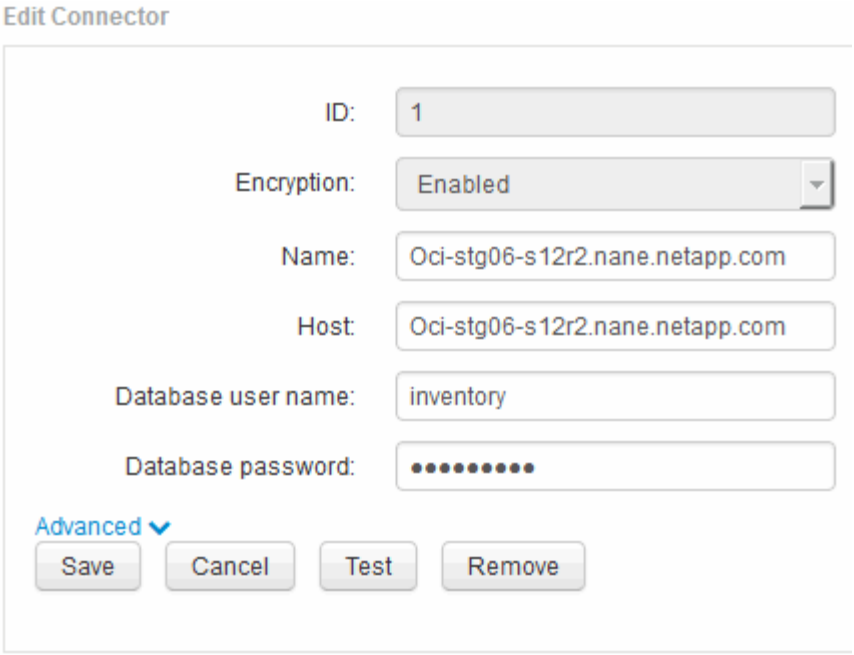
시작하기 전에

이 작업을 수행하려면 관리자로 로그인해야 합니다.

단계

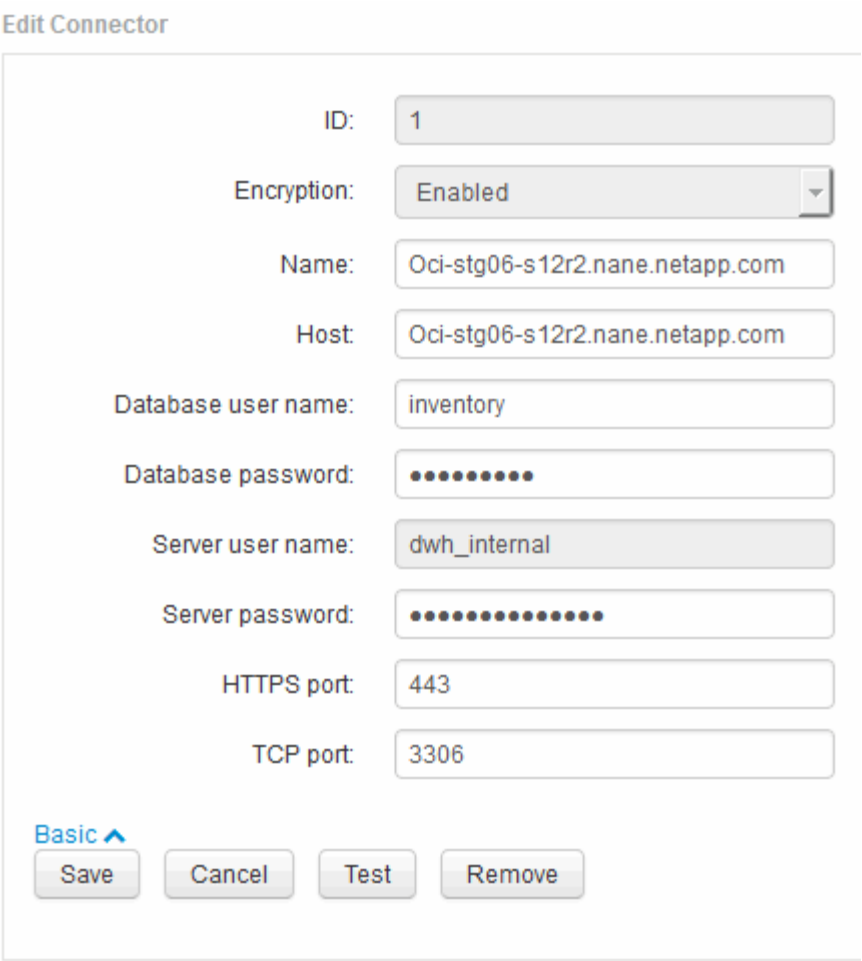
1. 에서 데이터 웨어하우스 포털에 로그인합니다 https://hostname/dwh여기서 hostname 은 OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 커넥터 * 를 클릭합니다.

   커넥터 편집 * 화면이 표시됩니다.



3. Database password * 필드에 새 ""Inventory"" 암호를 입력합니다.
4. 저장 * 을 클릭합니다
5. "dWh_INTERNAL" 암호를 변경하려면 * 고급 * 을 클릭합니다

   커넥터 고급 편집 화면이 표시됩니다.



6. 서버 암호 * 필드에 새 암호를 입력합니다.
7. 저장 을 클릭합니다.

ODBC 관리 도구를 사용하여 **dWh** 암호를 변경합니다

Insight 서버에서 dWh 사용자의 암호를 변경하면 데이터 웨어하우스 서버에서도 암호를 변경해야 합니다. ODBC 데이터 원본 관리자 도구를 사용하여 데이터 웨어하우스의 암호를 변경할 수 있습니다.

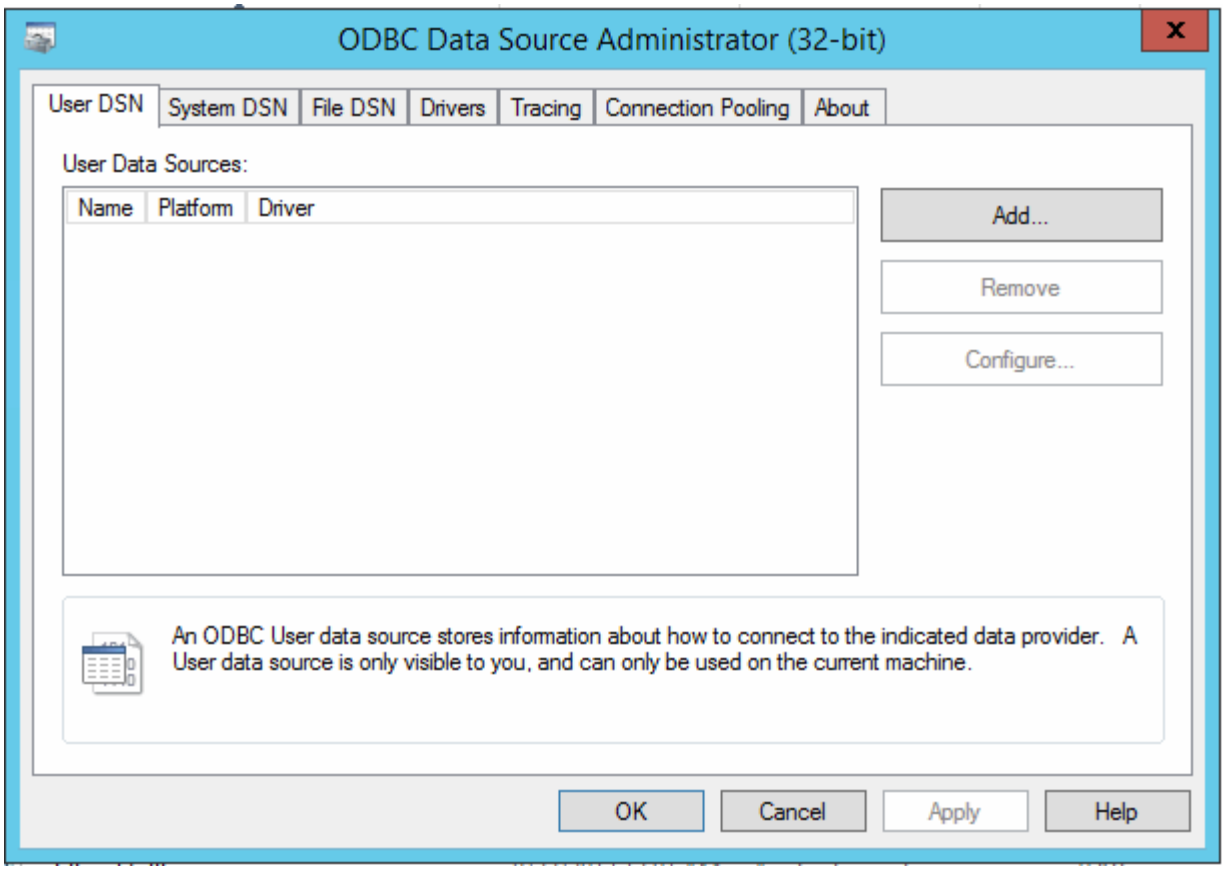
시작하기 전에

관리자 권한이 있는 계정을 사용하여 데이터 웨어하우스 서버에 원격으로 로그인해야 합니다.

단계

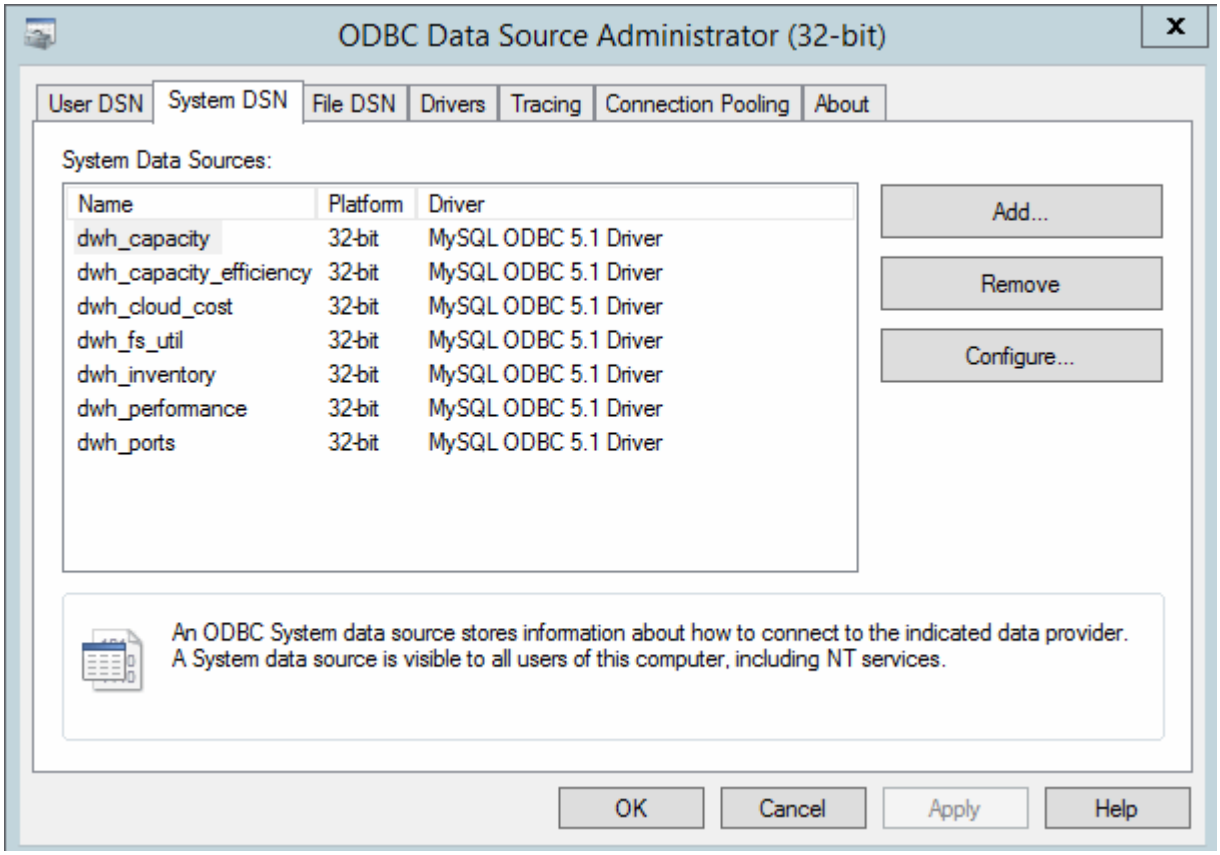
1. 해당 데이터 웨어하우스를 호스팅하는 서버에 원격 로그인을 수행합니다.
2. 에서 ODBC 관리 도구에 액세스합니다 `C:\Windows\SysWOW64\odbcad32.exe`

   ODBC 데이터 원본 관리자 화면이 표시됩니다.



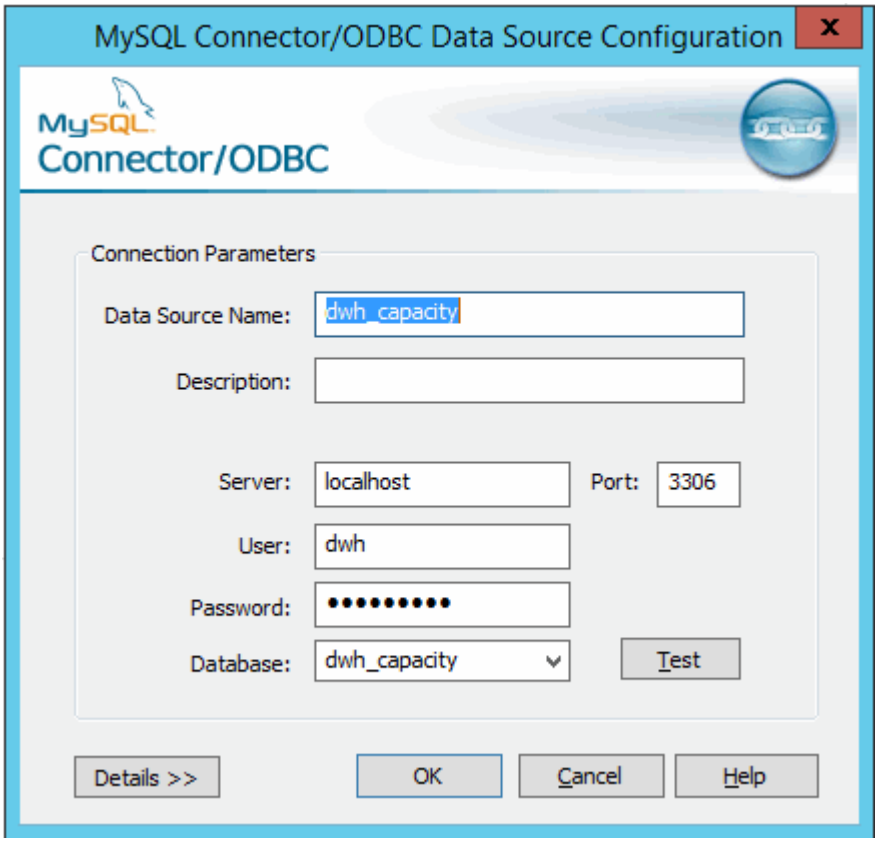
3. 시스템 DSN*을 클릭합니다

   시스템 데이터 소스가 표시됩니다.



4. 목록에서 OnCommand Insight 데이터 원본을 선택합니다.
5. 구성 * 을 클릭합니다

   데이터 소스 구성 화면이 표시됩니다.



6. 암호 * 필드에 새 암호를 입력합니다.

스마트 카드 및 인증서 로그인 지원

OnCommand Insight는 CAC(스마트 카드) 및 인증서를 사용하여 Insight 서버에 로그인하는 사용자를 인증할 수 있습니다. 이러한 기능을 사용하려면 시스템을 구성해야 합니다.

CAC 및 인증서를 지원하도록 시스템을 구성한 후 OnCommand Insight의 새 세션을 탐색하면 브라우저에 기본 대화 상자가 표시되어 사용자가 선택할 수 있는 개인 인증서 목록을 제공합니다. 이러한 인증서는 OnCommand Insight 서버에서 신뢰할 수 있는 CA에서 발급한 개인 인증서 집합을 기반으로 필터링됩니다. 대부분의 경우 단일 선택 옵션이 있습니다. 기본적으로 Internet Explorer는 하나만 선택할 경우 이 대화 상자를 건너뜁니다.

> CAC 사용자의 경우 스마트 카드에는 신뢰할 수 있는 CA와 일치할 수 있는 인증서가 여러 개 있습니다. 에 대한 CAC 인증서입니다 `identification` 사용해야 합니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).

- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

스마트 카드 및 인증서 로그인을 위한 호스트 구성

스마트 카드(CAC) 및 인증서 로그인을 지원하려면 OnCommand Insight 호스트 구성을 수정해야 합니다.

시작하기 전에

- 시스템에서 LDAP를 활성화해야 합니다.
- LDAP입니다 `User principal account name` 속성은 사용자 ID가 포함된 LDAP 필드와 일치해야 합니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).

- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. 를 사용합니다 `regedit` 에서 레지스트리 값을 수정하는 유틸리티입니다 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`:
   a. jvm_option을 변경합니다 `DclientAuth=false` 를 선택합니다 `DclientAuth=true`.
2. 키 저장소 파일을 백업합니다. `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. 를 지정하는 명령 프롬프트를 엽니다 `Run as administrator`

4. 자체 생성된 인증서 삭제: `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. 새 인증서 생성: `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "alias_name" -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 365 -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -dname "CN=commonName,OU=orgUnit,O=orgName,L=localityNameI,S=stateName,C=countryName"`
6. 인증서 서명 요청(CSR) 생성: `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -sigalg SHA1withRSA -alias "alias_name" -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file C:\temp\server.csr"`
7. 6단계에서 CSR이 반환된 후 인증서를 가져온 다음 Base-64 형식으로 인증서를 내보내고 에 넣습니다 `"C:\temp" named servername.cer`.
8. 키 저장소에서 인증서를 추출합니다.`C:\Program Files\SANscreen\java64\bin\keytool.exe -v -importkeystore -srckeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srcalias "alias_name" -destkeystore "C:\temp\file.p12" -deststoretype PKCS12`
9. P12 파일에서 개인 키를 추출합니다. `openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`
10. 7단계에서 내보낸 Base-64 인증서를 개인 키와 병합합니다. `openssl pkcs12 -export -in "<folder>\<certificate>.cer" -inkey "C:\temp\servername.private.pem" -out "C:\temp\servername.new.p12" -name "servername.abc.123.yyy.zzz"`
11. 병합된 인증서를 키 저장소로 가져옵니다. `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -destkeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srckeystore "C:\temp\servername.new.p12" -srcstoretype PKCS12 -alias "alias_name"`
12. 루트 인증서 가져오기: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file "C:\<root_certificate>.cer" -trustcacerts -alias "alias_name"`
13. 루트 인증서를 서버로 가져옵니다. trustore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<email_certificate>.cer" -trustcacerts -alias "alias_name"`
14. 중간 인증서 가져오기: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<intermediate_certificate>.cer" -trustcacerts -alias "alias_name"`

    모든 중간 인증서에 대해 이 단계를 반복합니다.
15. 이 예제와 일치하도록 LDAP에 도메인을 지정합니다.
16. 서버를 다시 시작합니다.

스마트 카드 및 인증서 로그인을 지원하도록 클라이언트 구성

클라이언트 시스템은 스마트 카드 사용 및 인증서 로그인을 지원하기 위해 미들웨어와 브라우저 수정이 필요합니다. 이미 스마트 카드를 사용하고 있는 고객은 클라이언트 시스템을 추가로 수정할 필요가 없습니다.

시작하기 전에

> 최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).
>
> - "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
> - "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
> - "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
> - "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
> - "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

이 작업에 대해

다음은 일반적인 클라이언트 구성 요구 사항입니다.

- ActivClient와 같은 스마트 카드 미들웨어 설치(참조
- IE 브라우저 수정(참조
- Firefox 브라우저 수정(참조

Linux 서버에 대한 **CAC** 활성화

Linux OnCommand Insight 서버에서 CAC를 활성화하려면 몇 가지 수정이 필요합니다.

단계

1. 로 이동합니다 `/opt/netapp/oci/conf/`
2. 편집 `wildfly.properties` 의 값을 변경합니다 `CLIENT_AUTH_ENABLED` "참"으로
3. 아래에 있는 "루트 인증서"를 가져옵니다 `/opt/netapp/oci/wildfly/standalone/configuration/server.keystore`
4. 서버를 다시 시작합니다

스마트 카드 및 인증서 로그인을 위한 데이터 웨어하우스 구성

스마트 카드(CAC) 및 인증서 로그인을 지원하도록 OnCommand Insight 데이터 웨어하우스 구성을 수정해야 합니다.

시작하기 전에

- 시스템에서 LDAP를 활성화해야 합니다.
- LDAP입니다 `User principal account name` 속성은 사용자의 정부 ID 번호가 포함된 LDAP 필드와 일치해야 합니다.

  정부에서 발급한 CAC에 저장된 일반 이름(CN)은 일반적으로 다음과 같은 형식입니다. `first.last.ID`. 와 같은 일부 LDAP 필드의 경우 `sAMAccountName`, 이 형식은 너무 깁니다. 이러한 필드의 경우 OnCommand Insight는 cns에서 ID 번호만 추출합니다.

> 최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).
>
> - "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
> - "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
> - "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
> - "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
> - "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. regedit를 사용하여 의 레지스트리 값을 수정합니다 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. jvm_option을 변경합니다 `-DclientAuth=false` 를 선택합니다 `-DclientAuth=true`.

   Linux의 경우 를 수정합니다 `clientAuth` 매개 변수 in `/opt/netapp/oci/scripts/wildfly.server`

2. CA(인증 기관)를 데이터 웨어하우스 trustore에 추가합니다.

   a. 명령 창에서 로 이동합니다 `..\SANscreen\wildfly\standalone\configuration`.

   b. 를 사용합니다 `keytool` 신뢰할 수 있는 CA를 나열하는 유틸리티: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

      각 줄의 첫 번째 단어는 CA 별칭을 나타냅니다.

   c. 필요한 경우 CA 인증서 파일(일반적으로 A)을 제공합니다 `.pem` 파일. 데이터 웨어하우스 신뢰할 수 있는 CA와 함께 고객의 CA를 포함하려면 을 참조하십시오 `..\SANscreen\wildfly\standalone\configuration` 를 사용합니다 `keytool` 가져오기 명령: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      my_alias는 일반적으로 에서 CA를 쉽게 식별하는 별칭입니다`keytool -list` 작동.

3. OnCommand Insight 서버에서 를 클릭합니다 `wildfly/standalone/configuration/standalone-full.xml` 에서 verify-client를 "requested"로 업데이트하여 파일을 수정해야 합니다 `/subsystem=undertow/server=default-server/https-listener=default-https`CAC 활성화 Insight 서버에 로그인하고 적절한 명령을 실행합니다.

OS	스크립트
Windows	<install dir>\SANscreen\Wildlfly\bin\enableCACforRemoteEJB.bat 을 참조하십시오
리눅스	/opt/netapp/OCI/Wildlfly/bin/enableCACforRemoteEJB.sh 을 참조하십시오

스크립트를 실행한 후 다음 단계로 진행하기 전에 Wildlfly 서버의 재로드가 완료될 때까지 기다립니다.

4. OnCommand Insight 서버를 다시 시작합니다.

스마트 카드 및 인증서 로그인을 위한 **Cognos** 구성**(OnCommand Insight 7.3.5 ~ 7.3.9)**

Cognos 서버에 대한 스마트 카드(CAC) 및 인증서 로그인을 지원하도록 OnCommand Insight 데이터 웨어하우스 구성을 수정해야 합니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.5 ~ 7.3.9를 실행하는 시스템에 적용됩니다.

> 최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).
>
> - "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
> - "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
> - "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
> - "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
> - "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. Cognos Trustore에 CA(인증 기관)를 추가합니다.
   a. 명령 창에서 로 이동합니다 `..\SANscreen\cognos\analytics\configuration\certs\`
   b. 를 사용합니다 `keytool` 신뢰할 수 있는 CA를 나열하는 유틸리티: `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      각 줄의 첫 번째 단어는 CA 별칭을 나타냅니다.

c. 적합한 파일이 없는 경우 CA 인증서 파일(일반적으로 A)을 제공합니다 `.pem` 파일.

d. OnCommand Insight의 신뢰할 수 있는 CA와 함께 고객의 CA를 포함하려면 으로 이동합니다 `..\SANscreen\cognos\analytics\configuration\certs\`.

e. 를 사용합니다 `keytool` 을(를) 가져오는 유틸리티입니다 `.pem` 파일: `..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

   `my_alias` 는 일반적으로 에서 CA를 쉽게 식별하는 별칭입니다`keytool -list` 작동.

f. 암호를 묻는 메시지가 나타나면 를 입력합니다 `NoPassWordSet`.

g. 답변 `yes` 인증서를 신뢰할 수 있는 것인지 묻는 메시지가 표시됩니다.

2. CAC 모드를 활성화하려면 를 실행합니다 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

3. CAC 모드를 해제하려면 를 실행한다 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

스마트 카드 및 인증서 로그인에 대한 **Cognos** 구성**(OnCommand Insight 7.3.10** 이상**)**

Cognos 서버에 대한 스마트 카드(CAC) 및 인증서 로그인을 지원하도록 OnCommand Insight 데이터 웨어하우스 구성을 수정해야 합니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.10 이상을 실행하는 시스템에 적용됩니다.

> 최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).
>
> - "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
> - "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
> - "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
> - "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
> - "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. Cognos Trustore에 CA(인증 기관)를 추가합니다.

   a. 명령 창에서 로 이동합니다 `..\SANscreen\cognos\analytics\configuration\certs\`

   b. 를 사용합니다 `keytool` 신뢰할 수 있는 CA를 나열하는 유틸리티: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      각 줄의 첫 번째 단어는 CA 별칭을 나타냅니다.

c. 적합한 파일이 없는 경우 CA 인증서 파일(일반적으로 A)을 제공합니다 `.pem` 파일.

d. OnCommand Insight의 신뢰할 수 있는 CA와 함께 고객의 CA를 포함하려면 으로 이동합니다 `..\SANscreen\cognos\analytics\configuration\certs\`.

e. 를 사용합니다 `keytool` 을(를) 가져오는 유틸리티입니다 `.pem` 파일: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

   `my_alias` 는 일반적으로 에서 CA를 쉽게 식별하는 별칭입니다`keytool -list` 작동.

f. 암호를 묻는 메시지가 나타나면 를 입력합니다 `NoPassWordSet`.

g. 답변 `yes` 인증서를 신뢰할 수 있는 것인지 묻는 메시지가 표시됩니다.

2. CAC 모드를 활성화하려면 다음을 수행합니다.

   a. 다음 단계에 따라 CAC 로그아웃 페이지를 구성합니다.

      - Cognos 포털 로그온(사용자는 시스템 관리자 그룹(예: cognos_admin)에 속해야 함)
      - (7.3.10 및 7.3.11에만 해당) 관리->구성->시스템->보안을 클릭합니다
      - (7.3.10 및 7.3.11에만 해당) 로그아웃 리디렉션 URL에 대해 cacLogout.html 을 입력합니다.\ → 적용
      - 브라우저를 닫습니다.

   b. 실행 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

   c. IBM Cognos 서비스를 시작합니다. Cognos 서비스가 시작될 때까지 기다립니다.

3. CAC 모드를 해제하려면 다음을 수행합니다.

   a. 실행 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

   b. IBM Cognos 서비스를 시작합니다. Cognos 서비스가 시작될 때까지 기다립니다.

   c. (7.3.10 및 7.3.11에만 해당) 다음 단계에 따라 CAC 로그아웃 페이지를 구성 해제합니다.

      - Cognos 포털 로그온(사용자는 시스템 관리자 그룹(예: cognos_admin)에 속해야 함)
      - 관리\ → 구성\ → 시스템\ → 보안을 클릭합니다
      - 로그아웃 리디렉션 URL \ → 적용에 대해 cacLogout.html 를 입력합니다
      - 브라우저를 닫습니다.

Cognos 및 DWH에 대해 CA 서명 SSL 인증서 가져오기(Insight 7.3.5 ~ 7.3.9)

SSL 인증서를 추가하여 데이터 웨어하우스 및 Cognos 환경에 대한 향상된 인증 및 암호화를 활성화할 수 있습니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.5 ~ 7.3.9를 실행하는 시스템에 적용됩니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).

- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

이 작업에 대해

이 절차를 수행하려면 관리자 권한이 있어야 합니다.

단계

1. 의 백업을 생성합니다 `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`.
2. 아래의 ""certs"" 및 ""csk"" 폴더의 백업을 만듭니다 `..\SANScreen\cognos\analytics\configuration`.
3. Cognos에서 인증서 암호화 요청을 생성합니다. 관리자 CMD 창에서 다음을 실행합니다.
   a. CD `"\Program Files\sanscreen\cognos\analytics\bin"`
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -d "CN=FQDN,O=orgname,C=US" -r c:\temp\encryptRequest.csr`
4. 를 엽니다 `c:\temp\encryptRequest.csr` 생성된 콘텐츠를 파일로 만들어 복사합니다.
5. SSL 인증서를 얻으려면 encryptRequest.csr을 CA(인증 기관)에 보냅니다.

   "san:dns=FQDN(예: hostname.netapp.com)`" SubjectAltName을 추가하려면 추가 속성)을 추가해야 합니다. Google Chrome 버전 58 이상에서 SubjectAltName이 인증서에서 누락되면 불만을 표시합니다.

6. PKCS7 형식을 사용하여 루트 인증서를 포함시켜 체인 인증서를 다운로드합니다

   FQDN.p7b 파일이 다운로드됩니다

7. CA에서 .p7b 형식의 인증서를 가져옵니다. Cognos Webserver의 인증서로 표시하는 이름을 사용합니다.
8. ThirdPartyCertificateTool.bat 에서 전체 체인을 가져오지 못하므로 모든 인증서를 내보내려면 여러 단계가 필요합니다. 다음과 같이 체인을 개별적으로 내보내서 분할합니다.
   a. ""Crypto Shell Extensions""에서 .p7b 인증서를 엽니다.
   b. 왼쪽 창에서 ""인증서""를 찾습니다.
   c. 루트 CA > 모든 작업 > 내보내기를 마우스 오른쪽 버튼으로 클릭합니다.
   d. Base64 출력을 선택합니다.
   e. 루트 인증서로 식별하는 파일 이름을 입력합니다.

   f. 모든 인증서를 .cer 파일로 별도로 내보내려면 8a-8C단계를 반복합니다.
   g. 파일 이름을 mediateX.cer 및 cognos.cer 로 지정합니다.
9. CA 인증서가 하나만 있는 경우 이 단계를 무시하거나, 그렇지 않으면 root.cer와 mediateX.cer를 모두 하나의 파일로 병합합니다.
   a. 메모장에서 intermediate.cer를 열고 내용을 복사합니다.
   b. 메모장에서 root.cer를 열고 9a의 콘텐츠를 저장합니다.
   c. 파일을 CA.CER로 저장합니다.
10. 관리자 CMD 프롬프트를 사용하여 Cognos 키 저장소로 인증서를 가져옵니다.
   a. cd ""Program Files\SANscreen\cognos\analytics\bin"
   b. ThirdPartyCertificateTool.bat - java:local -i -T -r c:\temp\CA.cer

      그러면 CA.cer가 루트 인증 기관으로 설정됩니다.

   c. ThirdPartyCertificateTool.bat - java:local -i -e -r c:\temp\cognos.cer -t c:\temp\CA.cer

      이렇게 하면 Cognos.cer 가 CA.cer 에 의해 서명된 암호화 인증서로 설정됩니다.

11. IBM Cognos 구성을 엽니다.
   a. 로컬 구성 -→ 보안 -→ 암호화 -→ Cognos 를 선택합니다
   b. "Use third party CA?"를 변경합니다. 를 True로 설정합니다.
   c. 구성을 저장합니다.
   d. Cognos를 다시 시작합니다
12. 관리 CMD 프롬프트를 사용하여 최신 Cognos 인증서를 cognos.crt로 내보냅니다.
   a. "D:\Program Files\SANscreen\Java\bin\keytool.exe" -exportcert -file "" c:\temp\cognos.crt" -keystore "D:\Program Files\SANscreen\cognos\analytics\configuration\certs\CAMKeystore" -storetype PKCS12-storepass NoPassSet-alias 암호화
13. 관리 CMD 프롬프트 창을 사용하여 "'c:\temp\cognos.crt""를 dWh trustore로 가져와서 Cognos와 DWH 간에 SSL 통신을 설정합니다.
   a. "D:\Program Files\SANscreen\Java\bin\keytool.exe" - importcert -file ""c:\temp\cognos.crt" - keystore "D:\Program Files\SANscreen\standalone\configuration\server.trustore" - storepass changeit -alias cognosert
14. SANscreen 서비스를 다시 시작합니다.
15. DWH 백업을 수행하여 DWH가 Cognos와 통신하는지 확인합니다.

Cognos 및 **DWH**에 대해 **CA** 서명 **SSL** 인증서 가져오기**(Insight 7.3.10** 이상**)**

SSL 인증서를 추가하여 데이터 웨어하우스 및 Cognos 환경에 대한 향상된 인증 및 암호화를 활성화할 수 있습니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.10 이상을 실행하는 시스템에 적용됩니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).

- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

이 작업에 대해

이 절차를 수행하려면 관리자 권한이 있어야 합니다.

단계

1. IBM Cognos 구성 도구를 사용하여 Cognos를 중지합니다. Cognos를 닫습니다.
2. 의 백업을 생성합니다 `..\SANScreen\cognos\analytics\configuration` 및 `..\SANScreen\cognos\analytics\temp\cam\freshness` 폴더.
3. Cognos에서 인증서 암호화 요청을 생성합니다. 관리자 CMD 창에서 다음을 실행합니다.
   a. CD `"\Program Files\sanscreen\cognos\analytics\bin"`
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress"`. 참고: 여기서 -H와 -I는 DNS 및 ipaddress와 같은 subjectAltNames를 추가합니다.
4. 를 엽니다 `c:\temp\encryptRequest.csr` 생성된 콘텐츠를 파일로 만들어 복사합니다.
5. encryptRequest.csr 콘텐츠를 입력하고 CA 서명 포털을 사용하여 인증서를 생성합니다.
6. PKCS7 형식을 사용하여 루트 인증서를 포함시켜 체인 인증서를 다운로드합니다

   FQDN.p7b 파일이 다운로드됩니다

7. CA에서 .p7b 형식의 인증서를 가져옵니다. Cognos Webserver의 인증서로 표시하는 이름을 사용합니다.
8. ThirdPartyCertificateTool.bat 에서 전체 체인을 가져오지 못하므로 모든 인증서를 내보내려면 여러 단계가 필요합니다. 다음과 같이 체인을 개별적으로 내보내서 분할합니다.
   a. ""Crypto Shell Extensions""에서 .p7b 인증서를 엽니다.
   b. 왼쪽 창에서 ""인증서""를 찾습니다.
   c. 루트 CA > 모든 작업 > 내보내기를 마우스 오른쪽 버튼으로 클릭합니다.
   d. Base64 출력을 선택합니다.
   e. 루트 인증서로 식별하는 파일 이름을 입력합니다.
   f. 모든 인증서를 .cer 파일로 별도로 내보내려면 8a ~ 8e 단계를 반복합니다.

g. 파일 이름을 mediateX.cer 및 cognos.cer 로 지정합니다.

9. CA 인증서가 하나만 있는 경우 이 단계를 무시하거나, 그렇지 않으면 root.cer와 mediateX.cer를 모두 하나의 파일로 병합합니다.
   a. 메모장에서 root.cer를 열고 내용을 복사합니다.
   b. 메모장을 사용하여 intermediate.cer를 열고 9a(중간 우선 및 루트 다음)의 콘텐츠를 추가합니다.
   c. 파일을 chain.cer로 저장합니다.
10. 관리자 CMD 프롬프트를 사용하여 Cognos 키 저장소로 인증서를 가져옵니다.
   a. cd ""Program Files\SANscreen\cognos\analytics\bin"
   b. ThirdPartyCertificateTool.bat - java:local -i -T -r c:\temp\root.cer
   c. ThirdPartyCertificateTool.bat - java:local -i -T -r c:\temp\intermediate.cer
   d. ThirdPartyCertificateTool.bat - java:local -i -e -r c:\temp\cognos.cer -t c:\temp\chain.cer
11. IBM Cognos 구성을 엽니다.
   a. 로컬 구성 -→ 보안 -→ 암호화 -→ Cognos 를 선택합니다
   b. "Use third party CA?"를 변경합니다. 를 True로 설정합니다.
   c. 구성을 저장합니다.
   d. Cognos를 다시 시작합니다
12. 관리 CMD 프롬프트를 사용하여 최신 Cognos 인증서를 cognos.crt로 내보냅니다.
   a. CD "'C:\Program Files\SANscreen"
   b. java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\analytics\configuration\certs\CAMKeystore-storetype pkcs12-storepass NoPassWordSet-alias encryption
13. 에서 DWH 서버 트뤼스토어를 백업합니다`..\SANscreen\wildfly\standalone\configuration\server.trustore`
14. 관리 CMD 프롬프트 창을 사용하여 "'c:\temp\cognos.crt""를 DWH trustore로 가져와서 Cognos와 DWH 간에 SSL 통신을 설정합니다.
   a. CD "'C:\Program Files\SANscreen"
   b. java\bin\keytool.exe - importcert -file c:\temp\cognos.crt -keystore wandiderfly\standalone\configuration\server.trutstore -storephass changeit -alias coclnos3rdca
15. SANscreen 서비스를 다시 시작합니다.
16. DWH 백업을 수행하여 DWH가 Cognos와 통신하는지 확인합니다.
17. 'sl 인증서'만 변경되고 기본 Cognos 인증서는 변경되지 않은 경우에도 다음 단계를 수행해야 합니다. 그렇지 않으면 Cognos가 새 SANscreen 인증서에 대해 불만을 제기하거나 DWH 백업을 생성할 수 없습니다.
   a. `cd "%SANSCREEN_HOME%cognos\analytics\bin\"`
   b. `"%SANSCREEN_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sanscreen.cer" -keystore "%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass changeit -alias "ssl certificate"`
   c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sanscreen.cer"`

일반적으로 이러한 단계는 에 설명된 Cognos 인증서 가져오기 프로세스의 일부로 수행됩니다 "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

스마트 카드 및 인증서 로그인을 위한 데이터 웨어하우스 구성

스마트 카드(CAC) 및 인증서 로그인을 지원하도록 OnCommand Insight 데이터 웨어하우스 구성을 수정해야 합니다.

시작하기 전에

- 시스템에서 LDAP를 활성화해야 합니다.
- LDAP입니다 `User principal account name` 속성은 사용자의 정부 ID 번호가 포함된 LDAP 필드와 일치해야 합니다.

  정부에서 발급한 CAC에 저장된 일반 이름(CN)은 일반적으로 다음과 같은 형식입니다. `first.last.ID`. 와 같은 일부 LDAP 필드의 경우 `sAMAccountName`, 이 형식은 너무 깁니다. 이러한 필드의 경우 OnCommand Insight는 cns에서 ID 번호만 추출합니다.

> 최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).
>
> - "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
> - "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
> - "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
> - "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
> - "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. regedit를 사용하여 의 레지스트리 값을 수정합니다 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. jvm_option을 변경합니다 `-DclientAuth=false` 를 선택합니다 `-DclientAuth=true`.

   Linux의 경우 를 수정합니다 `clientAuth` 매개 변수 in `/opt/netapp/oci/scripts/wildfly.server`

2. CA(인증 기관)를 데이터 웨어하우스 trustore에 추가합니다.

   a. 명령 창에서 로 이동합니다 `..\SANscreen\wildfly\standalone\configuration`.

   b. 를 사용합니다 `keytool` 신뢰할 수 있는 CA를 나열하는 유틸리티: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

각 줄의 첫 번째 단어는 CA 별칭을 나타냅니다.

c. 필요한 경우 CA 인증서 파일(일반적으로 A)을 제공합니다 `.pem` 파일. 데이터 웨어하우스 신뢰할 수 있는 CA와 함께 고객의 CA를 포함하려면 을 참조하십시오 `..\SANscreen\wildfly\standalone\configuration` 를 사용합니다 `keytool` 가져오기 명령:
```
C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore
server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts
```

my_alias는 일반적으로 에서 CA를 쉽게 식별하는 별칭입니다`keytool -list` 작동.

3. OnCommand Insight 서버에서 를 클릭합니다 `wildfly/standalone/configuration/standalone-full.xml` 에서 verify-client를 "requested"로 업데이트하여 파일을 수정해야 합니다 `/subsystem=undertow/server=default-server/https-listener=default-https`CAC 활성화 Insight 서버에 로그인하고 적절한 명령을 실행합니다.

OS	스크립트
Windows	<install dir>\SANscreen\Wildlfly\bin\enableCACforRemoteEJB.bat 을 참조하십시오
리눅스	/opt/netapp/OCI/Wildlfly/bin/enableCACforRemoteEJB.sh 을 참조하십시오

스크립트를 실행한 후 다음 단계로 진행하기 전에 Wildlfly 서버의 재로드가 완료될 때까지 기다립니다.

4. OnCommand Insight 서버를 다시 시작합니다.

스마트 카드 및 인증서 로그인을 위한 **Cognos** 구성(**OnCommand Insight 7.3.5 ~ 7.3.9**)

Cognos 서버에 대한 스마트 카드(CAC) 및 인증서 로그인을 지원하도록 OnCommand Insight 데이터 웨어하우스 구성을 수정해야 합니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.5 ~ 7.3.9를 실행하는 시스템에 적용됩니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).

- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. Cognos Trustore에 CA(인증 기관)를 추가합니다.
   a. 명령 창에서 로 이동합니다 `..\SANscreen\cognos\analytics\configuration\certs\`
   b. 를 사용합니다 `keytool` 신뢰할 수 있는 CA를 나열하는 유틸리티: `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      각 줄의 첫 번째 단어는 CA 별칭을 나타냅니다.
   c. 적합한 파일이 없는 경우 CA 인증서 파일(일반적으로 A)을 제공합니다 `.pem` 파일.
   d. OnCommand Insight의 신뢰할 수 있는 CA와 함께 고객의 CA를 포함하려면 으로 이동합니다 `..\SANscreen\cognos\analytics\configuration\certs\`.
   e. 를 사용합니다 `keytool` 을(를) 가져오는 유틸리티입니다 `.pem` 파일: `..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` 는 일반적으로 에서 CA를 쉽게 식별하는 별칭입니다`keytool -list` 작동.
   f. 암호를 묻는 메시지가 나타나면 를 입력합니다 `NoPassWordSet`.
   g. 답변 `yes` 인증서를 신뢰할 수 있는 것인지 묻는 메시지가 표시됩니다.
2. CAC 모드를 활성화하려면 를 실행합니다 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
3. CAC 모드를 해제하려면 를 실행한다 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

스마트 카드 및 인증서 로그인에 대한 **Cognos** 구성(**OnCommand Insight 7.3.10** 이상)

Cognos 서버에 대한 스마트 카드(CAC) 및 인증서 로그인을 지원하도록 OnCommand Insight 데이터 웨어하우스 구성을 수정해야 합니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.10 이상을 실행하는 시스템에 적용됩니다.

> 최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).
>
> - "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
> - "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
> - "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
> - "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
> - "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. Cognos Trustore에 CA(인증 기관)를 추가합니다.
   a. 명령 창에서 로 이동합니다 `..\SANscreen\cognos\analytics\configuration\certs\`
   b. 를 사용합니다 `keytool` 신뢰할 수 있는 CA를 나열하는 유틸리티: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      각 줄의 첫 번째 단어는 CA 별칭을 나타냅니다.
   c. 적합한 파일이 없는 경우 CA 인증서 파일(일반적으로 A)을 제공합니다 `.pem` 파일.
   d. OnCommand Insight의 신뢰할 수 있는 CA와 함께 고객의 CA를 포함하려면 으로 이동합니다 `..\SANscreen\cognos\analytics\configuration\certs\`.
   e. 를 사용합니다 `keytool` 을(를) 가져오는 유틸리티입니다 `.pem` 파일: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` 는 일반적으로 에서 CA를 쉽게 식별하는 별칭입니다`keytool -list` 작동.
   f. 암호를 묻는 메시지가 나타나면 를 입력합니다 `NoPassWordSet`.
   g. 답변 `yes` 인증서를 신뢰할 수 있는 것인지 묻는 메시지가 표시됩니다.
2. CAC 모드를 활성화하려면 다음을 수행합니다.
   a. 다음 단계에 따라 CAC 로그아웃 페이지를 구성합니다.
      - Cognos 포털 로그온(사용자는 시스템 관리자 그룹(예: cognos_admin)에 속해야 함)
      - (7.3.10 및 7.3.11에만 해당) 관리->구성->시스템->보안을 클릭합니다
      - (7.3.10 및 7.3.11에만 해당) 로그아웃 리디렉션 URL에 대해 cacLogout.html 을 입력합니다.\ → 적용
      - 브라우저를 닫습니다.

b. 실행 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

c. IBM Cognos 서비스를 시작합니다. Cognos 서비스가 시작될 때까지 기다립니다.

3. CAC 모드를 해제하려면 다음을 수행합니다.

a. 실행 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

b. IBM Cognos 서비스를 시작합니다. Cognos 서비스가 시작될 때까지 기다립니다.

c. (7.3.10 및 7.3.11에만 해당) 다음 단계에 따라 CAC 로그아웃 페이지를 구성 해제합니다.

- Cognos 포털 로그온(사용자는 시스템 관리자 그룹(예: cognos_admin)에 속해야 함)
- 관리\ → 구성\ → 시스템\ → 보안을 클릭합니다
- 로그아웃 리디렉션 URL \ → 적용에 대해 cacLogout.html 를 입력합니다
- 브라우저를 닫습니다.

Cognos 및 DWH에 대해 CA 서명 SSL 인증서 가져오기(Insight 7.3.5 ~ 7.3.9)

SSL 인증서를 추가하여 데이터 웨어하우스 및 Cognos 환경에 대한 향상된 인증 및 암호화를 활성화할 수 있습니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.5 ~ 7.3.9를 실행하는 시스템에 적용됩니다.

> 최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).
>
> - "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
> - "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
> - "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
> - "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
> - "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

이 작업에 대해

이 절차를 수행하려면 관리자 권한이 있어야 합니다.

단계

1. 의 백업을 생성합니다 `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`.
2. 아래의 ""certs"" 및 ""csk"" 폴더의 백업을 만듭니다 `..\SANScreen\cognos\analytics\configuration`.

3. Cognos에서 인증서 암호화 요청을 생성합니다. 관리자 CMD 창에서 다음을 실행합니다.
   a. CD “`\Program Files\sanscreen\cognos\analytics\bin`”
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -d “CN=FQDN,O=orgname,C=US” -r c:\temp\encryptRequest.csr`
4. 를 엽니다 `c:\temp\encryptRequest.csr` 생성된 콘텐츠를 파일로 만들어 복사합니다.
5. SSL 인증서를 얻으려면 encryptRequest.csr을 CA(인증 기관)에 보냅니다.

   "san:dns=FQDN(예: hostname.netapp.com)`" SubjectAltName을 추가하려면 추가 속성)을 추가해야 합니다. Google Chrome 버전 58 이상에서 SubjectAltName이 인증서에서 누락되면 불만을 표시합니다.

6. PKCS7 형식을 사용하여 루트 인증서를 포함시켜 체인 인증서를 다운로드합니다

   FQDN.p7b 파일이 다운로드됩니다

7. CA에서 .p7b 형식의 인증서를 가져옵니다. Cognos Webserver의 인증서로 표시하는 이름을 사용합니다.
8. ThirdPartyCertificateTool.bat 에서 전체 체인을 가져오지 못하므로 모든 인증서를 내보내려면 여러 단계가 필요합니다. 다음과 같이 체인을 개별적으로 내보내서 분할합니다.
   a. ""Crypto Shell Extensions""에서 .p7b 인증서를 엽니다.
   b. 왼쪽 창에서 ""인증서""를 찾습니다.
   c. 루트 CA > 모든 작업 > 내보내기를 마우스 오른쪽 버튼으로 클릭합니다.
   d. Base64 출력을 선택합니다.
   e. 루트 인증서로 식별하는 파일 이름을 입력합니다.
   f. 모든 인증서를 .cer 파일로 별도로 내보내려면 8a-8C단계를 반복합니다.
   g. 파일 이름을 mediateX.cer 및 cognos.cer 로 지정합니다.
9. CA 인증서가 하나만 있는 경우 이 단계를 무시하거나, 그렇지 않으면 root.cer와 mediateX.cer를 모두 하나의 파일로 병합합니다.
   a. 메모장에서 intermediate.cer를 열고 내용을 복사합니다.
   b. 메모장에서 root.cer를 열고 9a의 콘텐츠를 저장합니다.
   c. 파일을 CA.CER로 저장합니다.
10. 관리자 CMD 프롬프트를 사용하여 Cognos 키 저장소로 인증서를 가져옵니다.
    a. cd ""Program Files\SANscreen\cognos\analytics\bin"
    b. ThirdPartyCertificateTool.bat - java:local -i -T -r c:\temp\CA.cer

       그러면 CA.cer가 루트 인증 기관으로 설정됩니다.

    c. ThirdPartyCertificateTool.bat - java:local -i -e -r c:\temp\cognos.cer -t c:\temp\CA.cer

       이렇게 하면 Cognos.cer 가 CA.cer 에 의해 서명된 암호화 인증서로 설정됩니다.

11. IBM Cognos 구성을 엽니다.
    a. 로컬 구성 -→ 보안 -→ 암호화 -→ Cognos 를 선택합니다
    b. "Use third party CA?"를 변경합니다. 를 True로 설정합니다.

c. 구성을 저장합니다.

d. Cognos를 다시 시작합니다

12. 관리 CMD 프롬프트를 사용하여 최신 Cognos 인증서를 cognos.crt로 내보냅니다.

    a. "D:\Program Files\SANscreen\Java\bin\keytool.exe" -exportcert -file "" c:\temp\cognos.crt" -keystore "D:\Program Files\SANscreen\cognos\analytics\configuration\certs\CAMKeystore" -storetype PKCS12-storepass NoPassSet-alias 암호화

13. 관리 CMD 프롬프트 창을 사용하여 "'c:\temp\cognos.crt""를 dWh trustore로 가져와서 Cognos와 DWH 간에 SSL 통신을 설정합니다.

    a. "D:\Program Files\SANscreen\Java\bin\keytool.exe" - importcert -file ""c:\temp\cognos.crt" - keystore "D:\Program Files\SANscreen\standalone\configuration\server.trustore" - storepass changeit -alias cognosert

14. SANscreen 서비스를 다시 시작합니다.

15. DWH 백업을 수행하여 DWH가 Cognos와 통신하는지 확인합니다.

Cognos 및 DWH에 대해 CA 서명 SSL 인증서 가져오기(Insight 7.3.10 이상)

SSL 인증서를 추가하여 데이터 웨어하우스 및 Cognos 환경에 대한 향상된 인증 및 암호화를 활성화할 수 있습니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.10 이상을 실행하는 시스템에 적용됩니다.

> 최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).
>
> - "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
> - "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
> - "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
> - "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
> - "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

이 작업에 대해

이 절차를 수행하려면 관리자 권한이 있어야 합니다.

단계

1. IBM Cognos 구성 도구를 사용하여 Cognos를 중지합니다. Cognos를 닫습니다.

2. 의 백업을 생성합니다 `..\SANScreen\cognos\analytics\configuration` 및 `..\SANScreen\cognos\analytics\temp\cam\freshness` 폴더.
3. Cognos에서 인증서 암호화 요청을 생성합니다. 관리자 CMD 창에서 다음을 실행합니다.
   a. CD `"\Program Files\sanscreen\cognos\analytics\bin"`
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress"`. 참고: 여기서 -H와 -I는 DNS 및 ipaddress와 같은 subjectAltNames를 추가합니다.
4. 를 엽니다 `c:\temp\encryptRequest.csr` 생성된 콘텐츠를 파일로 만들어 복사합니다.
5. encryptRequest.csr 콘텐츠를 입력하고 CA 서명 포털을 사용하여 인증서를 생성합니다.
6. PKCS7 형식을 사용하여 루트 인증서를 포함시켜 체인 인증서를 다운로드합니다

   FQDN.p7b 파일이 다운로드됩니다
7. CA에서 .p7b 형식의 인증서를 가져옵니다. Cognos Webserver의 인증서로 표시하는 이름을 사용합니다.
8. ThirdPartyCertificateTool.bat 에서 전체 체인을 가져오지 못하므로 모든 인증서를 내보내려면 여러 단계가 필요합니다. 다음과 같이 체인을 개별적으로 내보내서 분할합니다.
   a. ""Crypto Shell Extensions""에서 .p7b 인증서를 엽니다.
   b. 왼쪽 창에서 ""인증서""를 찾습니다.
   c. 루트 CA > 모든 작업 > 내보내기를 마우스 오른쪽 버튼으로 클릭합니다.
   d. Base64 출력을 선택합니다.
   e. 루트 인증서로 식별하는 파일 이름을 입력합니다.
   f. 모든 인증서를 .cer 파일로 별도로 내보내려면 8a ~ 8e 단계를 반복합니다.
   g. 파일 이름을 mediateX.cer 및 cognos.cer 로 지정합니다.
9. CA 인증서가 하나만 있는 경우 이 단계를 무시하거나, 그렇지 않으면 root.cer와 mediateX.cer를 모두 하나의 파일로 병합합니다.
   a. 메모장에서 root.cer를 열고 내용을 복사합니다.
   b. 메모장을 사용하여 intermediate.cer를 열고 9a(중간 우선 및 루트 다음)의 콘텐츠를 추가합니다.
   c. 파일을 chain.cer로 저장합니다.
10. 관리자 CMD 프롬프트를 사용하여 Cognos 키 저장소로 인증서를 가져옵니다.
    a. cd ""Program Files\SANscreen\cognos\analytics\bin"
    b. ThirdPartyCertificateTool.bat - java:local -i -T -r c:\temp\root.cer
    c. ThirdPartyCertificateTool.bat - java:local -i -T -r c:\temp\intermediate.cer
    d. ThirdPartyCertificateTool.bat - java:local -i -e -r c:\temp\cognos.cer -t c:\temp\chain.cer
11. IBM Cognos 구성을 엽니다.
    a. 로컬 구성 -→ 보안 -→ 암호화 -→ Cognos 를 선택합니다
    b. "Use third party CA?"를 변경합니다. 를 True로 설정합니다.
    c. 구성을 저장합니다.

d. Cognos를 다시 시작합니다

12. 관리 CMD 프롬프트를 사용하여 최신 Cognos 인증서를 cognos.crt로 내보냅니다.
    a. CD "'C:\Program Files\SANscreen"
    b. java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\analytics\configuration\certs\CAMKeystore-storetype pkcs12-storepass NoPassWordSet-alias encryption
13. 에서 DWH 서버 트뤼스토어를 백업합니다`..\SANscreen\wildfly\standalone\configuration\server.trustore`
14. 관리 CMD 프롬프트 창을 사용하여 "'c:\temp\cognos.crt""를 DWH trustore로 가져와서 Cognos와 DWH 간에 SSL 통신을 설정합니다.
    a. CD "'C:\Program Files\SANscreen"
    b. java\bin\keytool.exe - importcert -file c:\temp\cognos.crt -keystore wandiderfly\standalone\configuration\server.trutstore -storephass changeit -alias coclnos3rdca
15. SANscreen 서비스를 다시 시작합니다.
16. DWH 백업을 수행하여 DWH가 Cognos와 통신하는지 확인합니다.
17. 'sl 인증서'만 변경되고 기본 Cognos 인증서는 변경되지 않은 경우에도 다음 단계를 수행해야 합니다. 그렇지 않으면 Cognos가 새 SANscreen 인증서에 대해 불만을 제기하거나 DWH 백업을 생성할 수 없습니다.
    a. `cd "%SANSCREEN_HOME%cognos\analytics\bin\"`
    b. `"%SANSCREEN_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sanscreen.cer" -keystore "%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass changeit -alias "ssl certificate"`
    c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sanscreen.cer"`

    일반적으로 이러한 단계는 에 설명된 Cognos 인증서 가져오기 프로세스의 일부로 수행됩니다 "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

SSL 인증서를 가져오는 중입니다

SSL 인증서를 추가하여 OnCommand Insight 환경의 보안을 강화하기 위한 향상된 인증 및 암호화를 활성화할 수 있습니다.

시작하기 전에

시스템이 최소 필수 비트 수준(1024비트)을 충족하는지 확인해야 합니다.

이 작업에 대해

> 이 절차를 수행하기 전에 기존 를 백업해야 합니다 `server.keystore` 파일 및 백업 이름을 지정합니다 `server.keystore.old`. 의 손상 또는 손상 `server.keystore` Insight 서버를 다시 시작한 후 Insight 서버가 작동하지 않을 수 있습니다. 백업을 생성하는 경우 문제가 발생할 경우 이전 파일로 되돌릴 수 있습니다.

단계

1. 원본 키 저장소 파일의 복사본을 만듭니다. `cp c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore.old`
2. 키 저장소의 내용을 나열합니다. `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -v -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

   a. 암호를 묻는 메시지가 나타나면 를 입력합니다 `changeit`.

   키 저장소의 내용이 표시됩니다. 키 저장소에 인증서가 하나 이상 있어야 합니다. `"ssl certificate"`.

3. 를 삭제합니다 `"ssl certificate"`: `keytool -delete -alias "ssl certificate" -keystore c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
4. 새 키 생성: `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "ssl certificate" -keyalg RSA -keysize 2048 -validity 365 -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

   a. 성과 이름을 묻는 메시지가 나타나면 사용하려는 FQDN(정규화된 도메인 이름)을 입력합니다.

   b. 조직 및 조직 구조에 대한 다음 정보를 제공합니다.

      - 국가: 해당 국가의 두 글자 ISO 약어(예: US)
      - 시/도: 조직의 본사 소재지가 위치한 시/도의 이름(예: 매사추세츠주)
      - 지역: 조직의 본사 소재지(예: Waltham)의 이름입니다.
      - 조직 이름: 도메인 이름을 소유한 조직의 이름(예: NetApp)
      - 조직 단위 이름: 인증서를 사용할 부서 또는 그룹의 이름(예: 지원)
      - 도메인 이름/일반 이름: 서버의 DNS 조회에 사용되는 FQDN(예: www.example.com) 시스템이 다음과 유사한 정보로 응답합니다. `Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?`

   c. 를 입력합니다 `Yes` CN(Common Name)이 FQDN과 같은 경우

   d. 키 암호를 묻는 메시지가 나타나면 암호를 입력하거나 Enter 키를 눌러 기존 키 저장소 암호를 사용합니다.

5. 인증서 요청 파일 생성: `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -alias "ssl certificate" -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file c:\localhost.csr`

   를 클릭합니다 `c:\localhost.csr` file 은 새로 생성된 인증서 요청 파일입니다.

6. 를 제출합니다 `c:\localhost.csr` 승인을 위해 CA(인증 기관)에 파일을 저장합니다.

   인증서 요청 파일이 승인되면 에서 인증서를 반환하도록 합니다 `.der` 형식. 파일이 로 반환될 수도 있고 반환되지 않을 수도 있습니다 `.der` 파일. 기본 파일 형식은 입니다 `.cer` Microsoft CA 서비스의 경우.

   대부분의 조직의 CA는 루트 CA를 포함하여 신뢰할 수 있는 모델 체인을 사용합니다. 이 모델은 대개 오프라인 상태입니다. 이 인증서는 중간 CA라고 하는 몇 개의 하위 CA에 대해서만 인증서에 서명했습니다.

전체 신뢰 체인에 대한 공개 키(인증서)를 얻어야 합니다. 즉, OnCommand Insight 서버의 인증서에 서명한 CA의 인증서와 조직 루트 CA에 등록하는 CA 간의 모든 인증서를 얻어야 합니다.

일부 조직에서는 서명 요청을 제출할 때 다음 중 하나를 받을 수 있습니다.

- 서명된 인증서와 신뢰 체인에서 모든 공개 인증서가 들어 있는 PKCS12 파일입니다
- A `.zip` 개별 파일(서명된 인증서 포함)과 신뢰 체인에서 모든 공용 인증서를 포함하는 파일입니다
- 서명된 인증서만

  공용 인증서를 얻어야 합니다.

7. server.keystore에 대해 승인된 인증서를 가져옵니다. `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

   a. 메시지가 표시되면 키 저장소 암호를 입력합니다.

      다음 메시지가 표시됩니다. `Certificate reply was installed in keystore`

8. 서버에 대해 승인된 인증서를 가져옵니다. trustore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore"`

   a. 메시지가 표시되면 Trustore 암호를 입력합니다.

      다음 메시지가 표시됩니다. `Certificate reply was installed in trustore`

9. 를 편집합니다 `SANscreen\wildfly\standalone\configuration\standalone-full.xml` 파일:

   다음 별칭 문자열을 대체합니다. `alias="cbc-oci-02.muccbc.hq.netapp.com"`. 예를 들면 다음과 같습니다.

   ```
   <keystore path="server.keystore" relative-to="jboss.server.config.dir" keystore-password="${VAULT::HttpsRealm::keystore_password::1}" alias="cbc-oci-02.muccbc.hq.netapp.com" key-password="${VAULT::HttpsRealm::key_password::1}"/>
   ```

10. SANscreen 서버 서비스를 다시 시작합니다.

    Insight가 실행되면 자물쇠 아이콘을 클릭하여 시스템에 설치된 인증서를 볼 수 있습니다.

    "발급자" 정보와 일치하는 "발급 대상" 정보가 포함된 인증서가 표시되는 경우 자체 서명된 인증서가 설치되어 있는 것입니다. Insight 설치 관리자가 생성한 자체 서명 인증서의 만료 기간은 100년입니다.

    NetApp은 이 절차로 디지털 인증서 경고가 제거된다고 보장할 수 없습니다. NetApp은 최종 사용자 워크스테이션의 구성 방법을 제어할 수 없습니다. 다음과 같은 시나리오를 고려해 보십시오.

    - Microsoft Internet Explorer와 Google Chrome 모두 Windows에서 Microsoft의 기본 인증서 기능을 사용합니다.

즉, Active Directory 관리자가 조직의 CA 인증서를 최종 사용자의 인증서 트뤼스토어로 푸시하면 OnCommand Insight 자체 서명된 인증서가 내부 CA 인프라에서 서명한 인증서로 교체되면 이러한 브라우저의 사용자에게 인증서 경고가 사라집니다.

- Java 및 Mozilla Firefox에는 자체 인증서 저장소가 있습니다.

  시스템 관리자가 CA 인증서를 이러한 응용 프로그램의 신뢰할 수 있는 인증서 저장소에 자동으로 수집하지 않는 경우 자체 서명된 인증서가 교체되더라도 신뢰할 수 없는 인증서로 인해 Firefox 브라우저를 사용하면 인증서 경고가 계속 생성될 수 있습니다. 조직의 인증서 체인을 Trustore에 설치하는 것도 추가 요구 사항입니다.

Insight 데이터베이스의 주별 백업 설정

Insight 데이터베이스의 데이터를 보호하기 위해 매주 자동으로 백업을 설정할 수도 있습니다. 이러한 자동 백업은 지정된 백업 디렉토리의 파일을 덮어씁니다.

이 작업에 대해

- 모범 사례 *: OCI 데이터베이스의 주간 백업을 설정할 때는 서버에 오류가 발생할 경우 Insight에서 사용하는 것과 다른 서버에 백업을 저장해야 합니다. 매주 백업마다 디렉토리의 파일을 덮어쓰므로 수동 백업을 주별 백업 디렉토리에 저장하지 마십시오.

백업 파일에는 다음이 포함됩니다.

- 재고 데이터
- 최대 7일간의 성능 데이터

단계

1. Insight 도구 모음에서 * Admin * > * Setup * 을 클릭합니다.
2. 백업 및 아카이브 * 탭을 클릭합니다.
3. Weekly Backup 섹션에서 * Enable weekly backup * 을 선택합니다.
4. 백업 위치 * 의 경로를 입력합니다. 로컬 Insight 서버의 또는 Insight 서버에서 액세스할 수 있는 원격 서버에 있을 수 있습니다.

   > 백업 위치 설정은 백업 자체에 포함되어 있으므로 다른 시스템에서 백업을 복원할 경우 새 시스템에서 백업 폴더 위치가 잘못되었을 수 있습니다. 백업을 복원한 후 백업 위치 설정을 다시 확인합니다.

5. 마지막 2개 또는 마지막 5개 백업을 유지하려면 * Cleanup * 옵션을 선택합니다.
6. 저장 * 을 클릭합니다.

결과

Admin * > * Troubleshooting * 으로 이동하여 필요 시 백업을 생성할 수도 있습니다.

백업에 포함된 항목

매주 및 필요 시 백업을 문제 해결 또는 마이그레이션에 사용할 수 있습니다.

주별 또는 주문형 백업에는 다음이 포함됩니다.

- 재고 데이터
- 성능 데이터(백업에 포함하도록 선택한 경우)
- 데이터 원본 및 데이터 원본 설정
- 통합 팩
- 원격 획득 장치
- ASUP/프록시 설정
- 위치 설정 백업
- 보관 위치 설정
- 알림 설정
- 사용자
- 성능 정책
- 업무 엔티티 및 애플리케이션
- 장치 해상도 규칙 및 설정
- 대시보드 및 위젯
- 맞춤형 자산 페이지 대시보드 및 위젯
- 쿼리
- 주석 및 주석 규칙

주별 백업에는 다음이 포함되지 않습니다.

- 보안 도구 설정/볼트 정보(별도의 CLI 프로세스를 통해 백업)
- 로그(요청 시 .zip 파일에 저장 가능)
- 성능 데이터(백업에 포함하도록 선택하지 않은 경우)
- 추가 수익 실적을

> 백업에 성능 데이터를 포함하도록 선택하면 최근 7일 동안의 데이터가 백업됩니다. 해당 기능이 활성화된 경우 나머지 데이터는 아카이브에 포함됩니다.

성능 데이터 아카이빙

OnCommand Insight 7.3에는 성능 데이터를 매일 아카이빙하는 기능이 도입되었습니다. 이 기능은 구성 및 제한된 성능 데이터 백업을 보완합니다.

OnCommand Insight은 최대 90일 동안의 성능 및 위반 데이터를 보존합니다. 그러나 해당 데이터의 백업을 생성할

때는 가장 최근의 정보만 백업에 포함됩니다. 아카이빙을 통해 나머지 성능 데이터를 저장하고 필요에 따라 로드할 수 있습니다.

아카이브 위치가 구성되고 아카이빙이 활성화되면 Insight에서 모든 객체에 대한 전날 성능 데이터를 아카이브 위치에 아카이브합니다. 각 날짜의 아카이브는 별도의 파일에 있는 보관 폴더에 보관됩니다. 보관은 백그라운드에서 수행되며 Insight가 실행되는 동안에는 계속됩니다.

최근 90일 동안의 아카이브가 보존되며, 90일이 지난 아카이브 파일은 새 아카이브가 생성됨에 따라 삭제됩니다.

성능 아카이브 지원

성능 데이터 아카이빙을 활성화하려면 다음 단계를 수행하십시오.

단계

1. 도구 모음에서 * Admin * > * Setup * 을 클릭합니다.
2. Backup & Archive * 탭을 선택합니다.
3. 성능 아카이브 섹션에서 성능 아카이브 활성화 가 선택되어 있는지 확인합니다.
4. 올바른 아카이브 위치를 지정하십시오.

   Insight 설치 폴더 아래에 폴더를 지정할 수 없습니다.

   모범 사례: Insight 백업 위치와 동일한 보관 폴더를 지정하지 마십시오.

5. 저장 * 을 클릭합니다.

   아카이브 프로세스는 백그라운드에서 처리되며 다른 Insight 활동을 방해하지 않습니다.

성능 아카이브 로드 중

성능 데이터 아카이브를 로드하려면 다음 단계를 수행하십시오.

시작하기 전에

성능 데이터 아카이브를 로드하기 전에 유효한 주별 또는 수동 백업을 복원해야 합니다.

단계

1. 도구 모음에서 * Admin * > * Troubleshooting * 을 클릭합니다.
2. 복원 섹션의 * 성능 아카이브 로드 * 에서 * 로드 * 를 클릭합니다.

> 아카이브 로딩은 백그라운드에서 처리됩니다. 매일 아카이빙된 성능 데이터가 Insight에 채워지면 전체 아카이브를 로드하는 데 시간이 오래 걸릴 수 있습니다. 아카이브 로드 상태가 이 페이지의 아카이브 섹션에 표시됩니다.

전자 메일 구성

OnCommand Insight Server에서 이메일을 통해 보고서 및 구독자 정보를 제공하고, 문제 해결을 위한 지원 정보를 NetApp 기술 지원 팀에 전송할 수 있도록 이메일 시스템에 액세스하도록 OnCommand Insight를 구성해야 합니다.

e-메일 구성 사전 요구 사항

이메일 시스템에 액세스하도록 OnCommand Insight를 구성하려면 먼저 호스트 이름 또는 IP 주소를 검색하여 (SMTP 또는 Exchange) 메일 서버를 식별하고 OnCommand Insight 보고서에 대한 이메일 계정을 할당해야 합니다.

이메일 관리자에게 문의하여 OnCommand Insight에 대한 이메일 계정을 만드십시오. 다음 정보가 필요합니다.

- 조직에서 사용하는 (SMTP 또는 Exchange) 메일 서버를 식별하기 위한 호스트 이름 또는 IP 주소입니다. 이 정보는 전자 메일을 읽는 데 사용하는 응용 프로그램을 통해 찾을 수 있습니다. 예를 들어 Microsoft Outlook에서 계정 구성을 확인하여 서버의 이름을 찾을 수 있습니다. 도구 - 전자 메일 계정 - 기존 전자 메일 계정을 보거나 변경할 수 있습니다.
- OnCommand Insight에서 정기 보고서를 보내는 데 사용할 전자 메일 계정의 이름입니다. 계정은 조직에서 유효한 이메일 주소여야 합니다. (대부분의 메일 시스템은 유효한 사용자로부터 메시지를 보내지 않는 한 메시지를 보내지 않습니다.) 전자 메일 서버에서 메일을 보내기 위해 사용자 이름과 암호가 필요한 경우 시스템 관리자에게 문의하십시오.

Insight에 대한 이메일 구성

사용자가 자신의 이메일 계정으로 Insight 보고서를 받으려면 이 기능을 사용하도록 이메일 서버를 구성해야 합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭하고 * Notifications * 를 선택합니다.
2. 페이지의 * 이메일 * 섹션으로 스크롤합니다.
3. 서버 * 상자에 조직의 SMTP 서버 이름을 입력합니다. 이 이름은 호스트 이름 또는 IP 주소 (_nnn.nnn.nnn_format)를 사용하여 식별됩니다.

   호스트 이름을 지정하는 경우 DNS를 통해 이름을 확인할 수 있는지 확인합니다.

4. 사용자 이름 * 상자에 사용자 이름을 입력합니다.
5. 암호 * 상자에 전자 메일 서버에 액세스하기 위한 암호를 입력합니다. 이 암호는 SMTP 서버가 암호로 보호되는 경우에만 필요합니다. 이 암호는 전자 메일을 읽을 수 있는 응용 프로그램에 로그인하는 데 사용하는 암호와 동일합니다. 암호가 필요한 경우 확인을 위해 두 번째 암호를 입력해야 합니다.
6. 보낸 사람 e-메일 * 상자에 모든 OnCommand Insight 보고서의 보낸 사람으로 식별되는 보낸 사람 e-메일 계정을 입력합니다.

   이 계정은 조직 내의 유효한 전자 메일 계정이어야 합니다.

7. 전자 메일 서명 * 상자에 보낼 모든 전자 메일에 삽입할 텍스트를 입력합니다.

8. 받는 사람 상자에서 을 클릭합니다 ✚이메일 주소를 입력하고 * 확인 * 을 클릭합니다.

   이메일 주소를 편집하려면 주소를 선택하고 을 클릭합니다 ✎. 이메일 주소를 삭제하려면 주소를 선택하고 을 클릭합니다 ✖.

9. 지정된 수신자에게 테스트 이메일을 보내려면 을 클릭합니다 ✔.
10. 저장 * 을 클릭합니다.

SNMP 알림을 구성합니다

OnCommand Insight는 구성 및 글로벌 경로 정책 변경 및 위반에 대한 SNMP 알림을 지원합니다. 예를 들어, 데이터 소스 임계값이 초과되면 SNMP 알림이 전송됩니다.

시작하기 전에

다음을 완료해야 합니다.

- 각 이벤트 유형에 대한 트랩을 통합하는 서버의 IP 주소를 식별합니다.

  이 정보를 얻으려면 시스템 관리자에게 문의해야 할 수도 있습니다.

- 지정된 시스템에서 각 이벤트 유형에 대해 SNMP 트랩을 가져오는 데 사용되는 포트 번호를 식별합니다.

  SNMP 트랩의 기본 포트는 162입니다.

- 사이트에서 MIB 컴파일.

  독점 MIB는 OnCommand Insight 트랩을 지원하는 설치 소프트웨어와 함께 제공됩니다. NetApp MIB는 모든 표준 SNMP 관리 소프트웨어와 호환되며 의 Insight 서버에서 찾을 수 있습니다 `<install dir>\SANscreen\MIBS\sanscreen.mib`.

단계

1. 관리자 * 를 클릭하고 * 알림 * 을 선택합니다.
2. 페이지의 * SNMP * 섹션으로 스크롤합니다.
3. Actions * 를 클릭하고 * Add trap source * 를 선택합니다.
4. SNMP 트랩 수신자 추가 * 대화 상자에 다음 값을 입력합니다.
   - * IP *

     OnCommand Insight가 SNMP 트랩 메시지를 보내는 IP 주소입니다.

   - * 포트 *

     OnCommand Insight가 SNMP 트랩 메시지를 보내는 포트 번호입니다.

   - * 커뮤니티 문자열 *

     SNMP 트랩 메시지에 ""public""을 사용합니다.

5. 저장 * 을 클릭합니다.

syslog 기능을 활성화합니다

OnCommand Insight 위반 및 성능 경고 로그와 감사 메시지를 위한 위치를 식별하고 로깅 프로세스를 활성화할 수 있습니다.

시작하기 전에

- 시스템 로그를 저장할 서버의 IP 주소가 있어야 합니다.
- local1 또는 user와 같이 메시지를 로깅하는 프로그램 유형에 해당하는 기능 수준을 알아야 합니다.

이 작업에 대해

syslog에는 다음과 같은 유형의 정보가 포함되어 있습니다.

- 위반 메시지
- 성능 경고
- 필요에 따라 감사 로그 메시지를 선택합니다

syslog에 사용되는 단위는 다음과 같습니다.

- 사용률 메트릭: 백분율
- 트래픽 메트릭: MB
- 트래픽 속도: MB/s

단계

1. Insight 도구 모음에서 * Admin * 을 클릭하고 * Notifications * 를 선택합니다.
2. 페이지의 * Syslog * 섹션으로 스크롤합니다.
3. syslog * 활성화 확인란을 선택합니다.
4. 원하는 경우 * Send audit * (감사 보내기 *) 확인란을 선택합니다. 새 감사 로그 메시지는 감사 페이지에 표시될 뿐만 아니라 syslog에 전송됩니다. 이미 존재하는 감사 로그 메시지는 syslog에 전송되지 않으며 새로 생성된 로그 메시지만 전송됩니다.
5. 서버 * 필드에 로그 서버의 IP 주소를 입력합니다.

   서버 IP(예: server:port)의 끝에서 콜론 다음에 사용자 지정 포트를 추가하여 사용자 지정 포트를 지정할 수 있습니다. 포트가 지정되지 않은 경우 기본 syslog 포트 514가 사용됩니다.

6. Facility * 필드에서 메시지를 로깅하는 프로그램 유형에 해당하는 시설 수준을 선택합니다.
7. 저장 * 을 클릭합니다.

Insight syslog 콘텐츠

서버에서 syslog를 활성화하여 활용률 및 트래픽 데이터를 포함한 Insight 위반 및 성능 경고 메시지를 수집할 수 있습니다.

메시지 유형

Insight syslog에는 세 가지 유형의 메시지가 나열됩니다.

- SAN 경로 위반
- 일반 위반
- 성능 경고

데이터가 제공됩니다

위반 설명에는 관련 요소, 이벤트 시간, 위반의 상대적 심각도 또는 우선 순위가 포함됩니다.

성능 알림에는 다음 데이터가 포함됩니다.

- 활용률
- 트래픽 유형
- 트래픽 속도(MB

성능을 구성하고 위반 알림을 확인합니다

OnCommand Insight는 성능 관련 알림을 지원하고 위반을 보장합니다. 기본적으로 Insight는 이러한 위반에 대한 알림을 보내지 않습니다. Insight에서 이메일을 보내거나, syslog 메시지를 syslog 서버로 보내거나, 위반이 발생할 경우 SNMP 알림을 보내도록 구성해야 합니다.

시작하기 전에

위반에 대한 e-메일, syslog 및 SNMP 전송 방법을 구성해야 합니다.

단계

1. 관리자 * > * 알림 * 을 클릭합니다.
2. 이벤트 * 를 클릭합니다.
3. 성능 위반 이벤트 * 또는 * 위반 이벤트 보증 * 섹션에서 원하는 알림 방법(* 이메일 **, * Syslog *** 또는 *** SNMP *)** 목록을 클릭하고 위반의 심각도 수준**(** 경고 이상 * 또는 * 긴급 *)을 선택합니다.
4. 저장 * 을 클릭합니다.

시스템 수준 이벤트 알림 구성

OnCommand Insight는 획득 장치 장애 또는 데이터 소스 오류와 같은 시스템 수준 이벤트에 대한 알림을 지원합니다. 알림을 수신하려면 이러한 이벤트 중 하나 이상이 발생할 때

Insight에서 이메일을 보내도록 구성해야 합니다.

시작하기 전에

관리 * > * 알림 * > * 전송 방법 * 에서 알림을 수신할 이메일 수신자를 구성해야 합니다.

단계

1. 관리자 * > * 알림 * 을 클릭합니다.
2. 이벤트 * 를 클릭합니다.
3. 시스템 경고 이벤트 * 이메일 섹션에서 알림에 대한 심각도 수준(* 경고 이상 * 또는 * 긴급 *)을 선택하거나 시스템 수준 이벤트 알림을 수신하지 않으려면 * 보내지 않음 * 을 선택합니다.
4. 저장 * 을 클릭합니다.
5. Admin * > * System Alerts * 를 클릭하여 알림을 직접 구성합니다.
6. 새 경고를 추가하려면 * + 추가 * 를 클릭하고 알림에 고유한 * 이름 * 을 지정합니다. 오른쪽 아이콘을 클릭하여 기존 경고를 * 편집 * 할 수도 있습니다.
7. 경고할 * 이벤트 유형 * 을 선택합니다(예: _ 획득 장치 실패 _).
8. 선택한 시간 간격 동안 선택한 유형의 중복 이벤트에 대한 알림을 표시하지 않으려면 * Snooze * 간격을 선택합니다. never_를 선택하면 이벤트가 더 이상 발생하지 않을 때까지 1분에 한 번씩 반복 알림이 수신됩니다.
9. 이벤트 알림에 대해 * 심각도 * (경고 또는 위험)를 선택합니다.
10. 이메일 알림은 기본적으로 글로벌 이메일 수신자 목록으로 전송됩니다. 또는 제공된 링크를 클릭하여 글로벌 목록을 재정의하고 특정 수신자에게 알림을 보낼 수 있습니다.
11. 저장을 클릭하여 경고를 추가합니다.

ASUP 처리 구성

모든 NetApp 제품은 자동화된 기능을 갖추고 있어 고객에게 최상의 지원을 제공합니다. 자동화된 지원(ASUP)은 사전 정의된 특정 정보를 고객 지원 팀에 주기적으로 전송합니다. NetApp에 전달할 정보와 전송 빈도를 제어할 수 있습니다.

시작하기 전에

데이터를 전송하기 전에 데이터를 전달하도록 OnCommand Insight를 구성해야 합니다.

이 작업에 대해

ASUP 데이터는 HTTPS 프로토콜을 사용하여 전달됩니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 설정 * 을 클릭합니다.
3. ASUP & Proxy * 탭을 클릭합니다.

4. ASUP * 섹션에서 * ASUP * 활성화 를 선택하여 ASUP 시설을 활성화하십시오.
5. 회사 정보를 변경하려면 다음 필드를 업데이트합니다.
    - * 회사 이름 *
    - * 사이트 이름 *
    - * 전송할 항목 *: 로그, 구성 데이터, 성능 데이터
6. 지정한 연결이 작동하는지 확인하려면 * 연결 테스트 * 를 클릭합니다.
7. 저장 * 을 클릭합니다.
8. Proxy* 섹션에서 * 프록시 * 활성화 여부를 선택하고 프록시 * 호스트 *, * 포트 * 및 * 사용자 * 정보를 지정합니다.
9. 지정한 프록시가 작동하는지 확인하려면 * 연결 테스트 * 를 클릭합니다.
10. 저장 * 을 클릭합니다.

AutoSupport(ASUP) 패키지에 포함된 내용

AutoSupport 패키지에는 데이터베이스 백업과 확장 정보가 들어 있습니다.

AutoSupport 패키지에는 다음이 포함됩니다.

- 재고 데이터
- 성능 데이터(ASUP에 포함할 경우)
- 데이터 원본 및 데이터 원본 설정
- 통합 팩
- 원격 획득 장치
- ASUP/프록시 설정
- 위치 설정 백업
- 보관 위치 설정
- 알림 설정
- 사용자
- 성능 정책
- 업무 엔티티 및 애플리케이션
- 장치 해상도 규칙 및 설정
- 대시보드 및 위젯
- 맞춤형 자산 페이지 대시보드 및 위젯
- 쿼리
- 주석 및 주석 규칙
- 로그
- 추가 수익 실적을
- 획득/데이터 소스 상태

- MySQL 상태
- 시스템 정보

AutoSupport 패키지에는 다음이 포함되지 않습니다.

- 보안 도구 설정/볼트 정보(별도의 CLI 프로세스를 통해 백업)
- 성능 데이터(ASUP에 포함할 것을 선택하지 않은 경우)

> ASUP에 성능 데이터를 포함하려는 경우 가장 최근의 7일 데이터가 포함됩니다. 해당 기능이 활성화된 경우 나머지 데이터는 아카이브에 포함됩니다. 아카이브 데이터는 ASUP에 포함되지 않습니다.

응용 프로그램 정의

사용자 환경에서 실행 중인 특정 애플리케이션과 관련된 데이터를 추적하려면 해당 애플리케이션을 정의해야 합니다.

시작하기 전에

애플리케이션을 업무 엔티티에 연결하려면 이미 업무 엔티티를 생성해야 합니다.

이 작업에 대해

호스트, 가상 머신, 볼륨, 내부 볼륨, qtree, 공유 및 하이퍼바이저.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 관리 * 를 클릭하고 * 응용 프로그램 * 을 선택합니다.

   응용 프로그램을 정의한 후 응용 프로그램 페이지에는 응용 프로그램의 이름, 우선 순위 및 응용 프로그램과 연결된 업무 엔티티가 표시됩니다(해당하는 경우).

3. 추가 * 를 클릭합니다.

   응용 프로그램 추가 대화 상자가 표시됩니다.

4. 이름 * 상자에 응용 프로그램의 고유한 이름을 입력합니다.
5. Priority * 를 클릭하고 해당 환경의 애플리케이션에 대한 우선 순위(중요, 높음, 중간 또는 낮음)를 선택합니다.
6. 이 응용 프로그램을 업무 엔티티와 함께 사용하려면 * 업무 엔티티 * 를 클릭하고 목록에서 엔티티를 선택합니다.
7. * 선택 사항 *: 볼륨 공유를 사용하지 않는 경우 * 볼륨 공유 확인 * 상자를 클릭하여 지웁니다.

   이 작업을 수행하려면 보증 라이센스가 필요합니다. 각 호스트가 클러스터의 동일한 볼륨에 액세스할 수 있도록 하려면 이 옵션을 설정합니다. 예를 들어, high-availability 클러스터의 호스트는 장애 조치를 위해 동일한 볼륨에 마스킹되어야 하는 경우가 많지만, 관련 없는 애플리케이션의 호스트는 일반적으로 동일한 물리적 볼륨에 액세스할 필요가 없습니다. 또한 규정 정책에 따라 보안상의 이유로 관련 없는 응용 프로그램이 동일한 물리적 볼륨에 액세스하는 것을 명시적으로 허용하지 않을 수 있습니다.

8. 저장 * 을 클릭합니다.

   응용 프로그램이 응용 프로그램 페이지에 나타납니다. 애플리케이션 이름을 클릭하면 Insight에서 애플리케이션의 자산 페이지를 표시합니다.

작업을 마친 후

애플리케이션을 정의한 후 호스트, 가상 머신, 볼륨, 내부 볼륨 또는 하이퍼바이저의 자산 페이지로 이동하여 애플리케이션을 자산에 할당할 수 있습니다.

자산에 애플리케이션 할당

비즈니스 엔터티를 사용하거나 사용하지 않고 애플리케이션을 정의한 후 해당 애플리케이션을 자산과 연결할 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 다음 중 하나를 수행하여 애플리케이션을 적용할 자산(호스트, 가상 머신, 볼륨 또는 내부 볼륨)을 찾습니다.
   - Dashboard * 를 클릭하고 * Assets Dashboard * 를 선택한 다음 자산을 클릭합니다.
   - 을 클릭합니다 도구 모음에서 * 자산 검색 * 상자를 표시하려면 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
3. 자산 페이지의 * 사용자 데이터 * 섹션에서 현재 자산에 할당된 애플리케이션 이름(할당된 애플리케이션이 없을 경우 * 없음 * 이 대신 표시됨)에 커서를 놓고 클릭합니다 (응용 프로그램 편집).

   선택한 자산에 대해 사용 가능한 애플리케이션 목록입니다. 현재 자산과 연결된 응용 프로그램 앞에는 확인 표시가 나타납니다.

4. 검색 상자에 입력하여 응용 프로그램 이름을 필터링하거나 목록을 아래로 스크롤할 수 있습니다.
5. 자산과 연결할 애플리케이션을 선택합니다.

   여러 애플리케이션을 호스트, 가상 시스템 및 내부 볼륨에 할당할 수 있지만 하나의 애플리케이션만 볼륨에 할당할 수 있습니다.

6. 을 클릭합니다 선택한 애플리케이션 또는 애플리케이션을 자산에 할당합니다.

   응용 프로그램 이름은 사용자 데이터 섹션에 나타납니다. 응용 프로그램이 업무 엔티티와 연결되어 있으면 이 섹션에도 업무 엔티티의 이름이 표시됩니다.

응용 프로그램 편집

애플리케이션의 우선 순위, 애플리케이션과 연계된 업무 엔티티 또는 볼륨 공유 상태를 변경할 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 관리 * 를 클릭하고 * 응용 프로그램 * 을 선택합니다.
3. 편집하려는 응용 프로그램 위에 커서를 놓고 클릭합니다 .

   응용 프로그램 편집 대화 상자가 표시됩니다.

4. 다음 중 하나를 수행합니다.
   - Priority * 를 클릭하고 다른 우선 순위를 선택합니다.

     응용 프로그램의 이름은 변경할 수 없습니다.

   - [업무 엔티티]를 클릭하고 응용 프로그램을 연결할 다른 업무 엔티티를 선택하거나 [없음]을 선택하여 응용 프로그램과 업무 엔티티의 연결을 제거합니다.
   - 클릭하여 지우거나 * 볼륨 공유 확인 * 을 선택합니다.

     이 옵션은 보증 라이센스가 있는 경우에만 사용할 수 있습니다.

5. 저장 * 을 클릭합니다.

응용 프로그램을 삭제하는 중입니다

사용자 환경에서 더 이상 필요하지 않은 응용 프로그램을 삭제할 수 있습니다.

단계

1. Insight 웹 UI에 로그인합니다.
2. 관리 * 를 클릭하고 * 응용 프로그램 * 을 선택합니다.
3. 삭제할 응용 프로그램 위에 커서를 놓고 클릭합니다 .

   응용 프로그램을 삭제할 것인지 묻는 확인 대화 상자가 표시됩니다.

4. 확인 * 을 클릭합니다.

업무 엔티티 계층 구조

환경 데이터를 더 세밀한 수준에서 추적 및 보고할 비즈니스 엔터티를 정의할 수 있습니다.

OnCommand Insight에서 비즈니스 엔터티 계층에는 다음 수준이 포함되어 있습니다.

- * 테넌트 * 는 서비스 공급자가 주로 리소스를 NetApp과 같은 고객과 연결하는 데 사용됩니다.
- * LOB(Line of Business) * 는 회사 내 사업 부문 또는 제품 라인입니다(예: 데이터 스토리지).
- * 사업부 * 는 법률 또는 마케팅과 같은 전통적인 사업부를 나타냅니다.
- * Project * 는 종종 용량 비용 청구를 원하는 사업부 내의 특정 프로젝트를 식별하는 데 사용됩니다. 예를 들어 "

특허"는 법률 부서의 프로젝트 이름일 수 있으며 "판매 이벤트"는 마케팅 부서의 프로젝트 이름일 수 있습니다. 수준 이름에는 공백이 포함될 수 있습니다.

회사 계층 구조의 디자인에 있는 모든 수준을 사용할 필요는 없습니다.

비즈니스 엔터티 계층 구조 디자인

OnCommand Insight 데이터베이스의 고정 구조가 되기 때문에 회사 구조의 요소와 비즈니스 엔터티에 표시해야 할 요소를 이해해야 합니다. 다음 정보를 사용하여 업무 엔티티를 설정할 수 있습니다. 이러한 범주의 데이터를 수집하기 위해 모든 계층 레벨을 사용할 필요는 없습니다.

단계

1. 각 업무 엔티티 계층 수준을 검토하여 해당 수준이 회사의 업무 엔티티 계층 구조에 포함되어야 하는지 확인합니다.
   - 회사가 ISP인 경우 * Tenant * 레벨이 필요하며, 고객의 자원 사용량을 추적하고자 하는 경우.
   - * 여러 제품 라인의 데이터를 추적해야 하는 경우 계층 구조에 LOB(Line of Business) * 가 필요합니다.
   - 서로 다른 부서의 데이터를 추적해야 하는 경우 * 사업부 * 가 필요합니다. 이러한 계층 수준은 한 부서가 다른 부서에서 사용하지 않는 리소스를 분리하는 데 유용합니다.
   - * Project * 레벨은 부서 내 특수 작업에 사용할 수 있습니다. 이 데이터는 회사 또는 부서의 다른 프로젝트와 비교하여 개별 프로젝트의 기술 요구 사항을 정확히 파악하고 정의하며 모니터링하는 데 유용할 수 있습니다.
2. 각 업무 엔티티를 보여 주는 차트를 만들고 엔티티 내의 모든 수준 이름을 표시합니다.
3. 계층 구조의 이름을 확인하여 OnCommand Insight 보기 및 보고서에 대한 설명이 있는지 확인합니다.
4. 각 업무 엔티티와 관련된 모든 애플리케이션을 식별합니다.

비즈니스 엔터티 생성

회사의 비즈니스 엔터티 계층 구조를 디자인한 후 응용 프로그램을 설정한 다음 비즈니스 엔터티를 응용 프로그램과 연결할 수 있습니다. 이 프로세스는 OnCommand Insight 데이터베이스에 업무 엔티티 구조를 만듭니다.

이 작업에 대해

응용 프로그램을 비즈니스 엔티티와 연결하는 것은 선택 사항이지만 이는 최선의 방법입니다.

단계

1. Insight 웹 UI에 로그인합니다.
2. 관리 * 를 클릭하고 * 업무 엔티티 * 를 선택합니다.

   사업체 페이지가 표시됩니다.

3. 을 클릭합니다 + Add 새 요소 작성을 시작합니다.

   [업무 엔티티 추가] * 대화 상자가 표시됩니다.

4. 각 엔터티 수준(테넌트, 사업부, 사업부 및 프로젝트)에 대해 다음 중 하나를 수행할 수 있습니다.

- 요소 수준 목록을 클릭하고 값을 선택합니다.
- 새 값을 입력하고 Enter 키를 누릅니다.
- 업무 엔티티에 엔티티 수준을 사용하지 않으려면 엔티티 수준 값을 N/A로 둡니다.

5. 저장 * 을 클릭합니다.

자산에 업무 엔티티 할당

자산에 업무 엔티티를 할당할 수 있습니다(호스트, 포트, 스토리지, 스위치, 가상 시스템, 비즈니스 엔티티를 애플리케이션에 연결하지 않고 qtree, 공유, 볼륨 또는 내부 볼륨). 그러나 해당 자산이 비즈니스 엔티티와 관련된 애플리케이션에 연결되어 있는 경우 비즈니스 엔티티가 자산에 자동으로 할당됩니다.

시작하기 전에

이미 업무 엔티티를 생성해야 합니다.

이 작업에 대해

자산에 직접 비즈니스 엔티티를 할당할 수 있지만 자산에 애플리케이션을 할당한 다음 자산에 비즈니스 엔티티를 할당하는 것이 좋습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 다음 중 하나를 수행하여 업무 엔티티를 적용할 자산을 찾습니다.
   - 자산 대시보드에서 자산을 클릭합니다.
   - 을 클릭합니다 도구 모음에서 * 자산 검색 * 상자를 표시하려면 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
3. 자산 페이지의 * 사용자 데이터 * 섹션에서 * 비즈니스 엔터티 * 옆에 * 없음 * 으로 커서를 이동한 다음 를 클릭합니다 .

   사용 가능한 업무 엔티티 목록이 표시됩니다.

4. 검색 * 상자에 특정 엔터티의 목록을 필터링하거나 목록을 아래로 스크롤하거나 목록에서 비즈니스 엔터티를 선택합니다.

   선택한 업무 엔티티가 애플리케이션에 연결되어 있으면 애플리케이션 이름이 표시됩니다. 이 경우 사업주명 옆에 "파생된"이라는 단어가 나타납니다. 연결된 응용 프로그램이 아닌 자산에 대해서만 엔티티를 유지하려면 응용 프로그램의 할당을 수동으로 재정의할 수 있습니다.

5. 업무 엔티티로부터 파생된 응용 프로그램을 재정의하려면 응용 프로그램 이름 위에 커서를 놓고 를 클릭합니다 다른 업무 엔티티를 선택하고 목록에서 다른 애플리케이션을 선택합니다.

여러 자산에 비즈니스 엔티티를 할당하거나 제거합니다

수동으로 할당하거나 제거할 필요 없이 쿼리를 사용하여 여러 자산에 비즈니스 엔티티를 할당하거나 제거할 수 있습니다.

시작하기 전에

원하는 자산에 추가할 비즈니스 엔티티를 이미 만들어야 합니다.

단계

1. 새 쿼리를 만들거나 기존 쿼리를 엽니다.
2. 필요한 경우 비즈니스 엔티티를 추가할 자산을 필터링합니다.
3. 목록에서 원하는 자산을 선택하거나 를 클릭합니다 ☐ ▾ 모두 * 를 선택합니다.

   작업 * 버튼이 표시됩니다.

4. 선택한 자산에 업무 엔티티를 추가하려면 을 클릭합니다 Actions ▾. 선택한 자산 유형에 업무 엔티티가 할당되어 있을 수 있는 경우, [업무 엔티티 추가]에 대한 메뉴 선택이 표시됩니다. 이 옵션을 선택합니다.
5. 목록에서 원하는 업무 엔티티를 선택하고 * 저장 * 을 클릭합니다.

   지정한 새 업무 엔티티는 이미 자산에 할당된 모든 업무 엔티티보다 우선합니다. 자산에 애플리케이션을 할당하면 동일한 방식으로 할당된 비즈니스 엔티티도 무시됩니다. 비즈니스 엔티티를 자산으로 할당하면 해당 자산에 할당된 모든 애플리케이션도 재정의될 수 있습니다.

6. 자산에 할당된 업무 엔티티를 제거하려면 를 클릭합니다 Actions ▾ 을 클릭하고 * 업무 엔티티 제거 * 를 선택합니다.
7. 목록에서 원하는 업무 엔티티를 선택하고 * 삭제 * 를 클릭합니다.

주석 정의

회사 요구사항에 맞게 데이터를 추적하도록 OnCommand Insight을 사용자 지정할 때 자산의 수명 종료, 데이터 센터, 건물 위치, 스토리지 계층 또는 볼륨 등 데이터를 완벽하게 파악하는 데 필요한 특수 주석을 정의할 수 있습니다. 내부 볼륨 서비스 레벨을 지원합니다.

단계

1. 환경 데이터를 연결해야 하는 업계 용어를 나열하십시오.
2. 비즈니스 엔티티를 사용하여 아직 추적되지 않은 환경 데이터를 연결해야 하는 기업 용어를 나열하십시오.
3. 사용할 수 있는 기본 주석 유형을 식별합니다.
4. 만들어야 하는 사용자 지정 주석을 식별합니다.

주석을 사용하여 환경을 모니터링합니다

회사 요구 사항에 맞는 데이터를 추적하도록 OnCommand Insight를 사용자 지정할 때 _annotations_라는 특수 메모를 정의하여 자산에 할당할 수 있습니다. 예를 들어, 자산의 수명 종료, 데이터 센터, 건물 위치, 스토리지 계층 또는 볼륨 서비스 수준과 같은 정보에 주석을 달 수 있습니다.

주석을 사용하여 환경을 모니터링하는 데 유용한 작업은 다음과 같습니다.

- 모든 주석 유형에 대한 정의를 만들거나 편집합니다.
- 자산 페이지를 표시하고 각 자산을 하나 이상의 주석과 연결합니다.

  예를 들어, 자산이 임대되고 2개월 이내에 임대가 만료되는 경우 자산에 수명 종료 주석을 적용할 수 있습니다. 이렇게 하면 다른 사용자가 해당 자산을 장기간 사용하지 못하게 할 수 있습니다.

- 같은 유형의 여러 자산에 주석을 자동으로 적용하는 규칙을 작성합니다.
- 주석 가져오기 유틸리티를 사용하여 주석을 가져옵니다.
- 주석을 기준으로 자산을 필터링합니다.
- 주석을 기반으로 보고서의 데이터를 그룹화하고 해당 보고서를 생성합니다.

  보고서에 대한 자세한 내용은 _OnCommand Insight 보고 가이드_를 참조하십시오.

주석 유형 관리

OnCommand Insight는 자산 수명 주기(생일 또는 수명 종료), 건물 또는 데이터 센터 위치, 계층 등 보고서에 표시되도록 사용자 지정할 수 있는 몇 가지 기본 주석 유형을 제공합니다. 기본 주석 유형의 값을 정의하거나 사용자 정의 주석 유형을 직접 만들 수 있습니다. 나중에 이러한 값을 편집할 수 있습니다.

기본 주석 유형

OnCommandInsight는 몇 가지 기본 주석 유형을 제공합니다. 이러한 주석은 데이터를 필터링하거나 그룹화하고 데이터 보고를 필터링하는 데 사용할 수 있습니다.

다음과 같은 기본 주석 유형과 자산을 연결할 수 있습니다.

- 생일, 일몰 또는 수명 종료 등의 자산 수명 주기
- 데이터 센터, 건물 또는 바닥과 같은 장치에 대한 위치 정보
- 품질(계층), 연결된 장치(스위치 수준) 또는 서비스 수준별 자산 분류
- 핫(높은 활용도) 등의 상태

다음 표에는 기본 주석 유형이 나열되어 있습니다. 이러한 주석 이름을 필요에 맞게 편집할 수 있습니다.

주석 유형	설명	유형
별칭	리소스에 대한 사용자 친화적인 이름입니다.	텍스트
생일	장치가 온라인 상태가 되거나 온라인으로 전환되는 날짜입니다.	날짜
건물	호스트, 스토리지, 스위치 및 테이프 리소스의 물리적 위치	목록

도시	호스트, 스토리지, 스위치 및 테이프 리소스의 지방자치당국 위치	목록
컴퓨팅 리소스 그룹	Host 및 VM Filesystems 데이터 소스에서 사용하는 그룹 할당입니다.	목록
대륙	호스트, 스토리지, 스위치 및 테이프 리소스의 지리적 위치	목록
국가	호스트, 스토리지, 스위치 및 테이프 리소스의 국가별 위치	목록
데이터 센터	리소스의 물리적 위치이며 호스트, 스토리지 시스템, 스위치 및 테이프에서 사용할 수 있습니다.	목록
직접 연결	스토리지 리소스가 호스트에 직접 접속되어 있으면 (예 또는 아니요)를 나타냅니다.	부울
수명 종료	예를 들어 임대가 만료되었거나 하드웨어가 폐기되는 경우 장치가 오프라인 상태가 되는 날짜입니다.	날짜
패브릭 별칭	Fabric의 사용자 친화적인 이름입니다.	텍스트
바닥	건물 바닥에 있는 장치의 위치. 호스트, 스토리지 시스템, 스위치 및 테이프에 대해 설정할 수 있습니다.	목록
핫	이미 사용량이 많은 디바이스를 정기적으로 또는 용량 임계값으로 사용 중입니다.	부울
참고	자원에 연결할 메모입니다.	텍스트
랙	리소스가 상주하는 랙입니다.	텍스트
있습니다	호스트, 스토리지, 스위치 및 테이프 리소스의 건물 또는 기타 위치 내의 공간입니다.	목록

산	네트워크의 논리 파티션입니다. 호스트, 스토리지 시스템, 테이프, 스위치 및 애플리케이션에서 사용할 수 있습니다.	목록
서비스 수준	리소스에 할당할 수 있는 지원되는 서비스 수준 집합입니다. 내부 볼륨, qtree, 볼륨에 대한 정렬 옵션 목록을 제공합니다. 서비스 수준을 편집하여 다양한 수준에 대한 성능 정책을 설정합니다.	목록
시/도	리소스가 있는 시/군/구 또는 시/군/구	목록
일몰	해당 디바이스에 새 할당을 수행할 수 없는 임계값을 설정합니다. 계획된 마이그레이션 및 기타 보류 중인 네트워크 변경에 유용합니다.	날짜
스위치 레벨	에는 스위치에 대한 범주를 설정하기 위한 미리 정의된 옵션이 포함되어 있습니다. 일반적으로 이러한 지정은 필요한 경우 편집할 수 있지만 장치의 수명 기간 동안 유지됩니다. 스위치에만 사용할 수 있습니다.	목록
계층	는 사용자 환경 내에서 서로 다른 서비스 수준을 정의하는 데 사용할 수 있습니다. 계층은 필요한 속도(예: 금 또는 은)와 같은 수준의 유형을 정의할 수 있습니다. 이 기능은 내부 볼륨, Qtree, 스토리지 어레이, 스토리지 풀 및 볼륨에서만 사용할 수 있습니다.	목록
위반 심각도입니다	중요도가 가장 높은 계층부터 가장 낮은 계층까지 위반 등급(예: 중요)의 순위를 지정합니다(예: 호스트 포트 누락 또는 이중화 누락).	목록

별칭, 데이터 센터, 핫, 서비스 레벨, 일몰, 스위치 수준, 서비스 수준, 계층 및 위반 심각성 은 시스템 수준 주석으로, 삭제하거나 이름을 바꿀 수 없습니다. 할당된 값만 변경할 수 있습니다.

주석 지정 방법

주석 규칙을 사용하여 수동으로 또는 자동으로 주석을 지정할 수 있습니다. 또한 OnCommand Insight는 자산 취득 및 상속에 대한 일부 주석을 자동으로 할당합니다. 자산에 할당한 주석은 자산 페이지의 사용자 데이터 섹션에 표시됩니다.

주석은 다음과 같은 방법으로 지정됩니다.

- 주석을 자산에 수동으로 지정할 수 있습니다.

  주석을 자산에 직접 지정하면 주석이 자산 페이지에 일반 텍스트로 표시됩니다. 수동으로 할당된 주석은 항상 주석 규칙에 의해 상속되거나 할당된 주석보다 우선합니다.

- 동일한 유형의 자산에 주석을 자동으로 할당하는 주석 규칙을 생성할 수 있습니다.

  주석이 규칙별로 할당된 경우 Insight는 자산 페이지의 주석 이름 옆에 규칙 이름을 표시합니다.

- Insight는 계층 레벨을 스토리지 계층 모델과 자동으로 연결하여 자산 구입 시 리소스에 스토리지 주석을 신속하게 할당할 수 있습니다.

  특정 스토리지 리소스는 사전 정의된 계층(계층 1 및 계층 2)과 자동으로 연결됩니다. 예를 들어 Symmetrix 스토리지 계층은 Symmetrix 및 VMAX 제품군을 기반으로 하며 계층 1과 연결됩니다. 계층 요구 사항에 맞게 기본값을 변경할 수 있습니다. 주석을 Insight(예: 계층)에 할당하면 자산 페이지의 주석 이름 위에 커서를 놓으면 "시스템 정의"가 표시됩니다.

- 일부 리소스(자산의 하위 항목)는 자산(상위)에서 사전 정의된 계층 주석을 파생시킬 수 있습니다.

  예를 들어, 주석을 스토리지에 할당할 경우 계층 주석은 모든 스토리지 풀, 내부 볼륨, 볼륨, Qtree 및 스토리지에 속한 공유에 의해 파생됩니다. 스토리지의 내부 볼륨에 다른 주석이 적용되는 경우 주석은 이후에 모든 볼륨, qtree 및 공유에 의해 파생됩니다. 자산 페이지의 주석 이름 옆에 "Deribed"가 나타납니다.

주석과 비용 연관

비용 관련 보고서를 실행하기 전에 비용을 서비스 수준, 스위치 수준 및 계층 시스템 수준 주석과 연계해야 합니다. 그러면 운영 및 복제 용량의 실제 사용량을 기준으로 스토리지 사용자에게 비용 청구를 수행할 수 있습니다. 예를 들어, 계층 레벨의 경우 골드 및 실버 등급 값을 가지고 실버 계층보다 더 높은 비용을 골드 계층에 할당할 수 있습니다.

단계

1. Insight트위브 UI에 로그인합니다.
2. 관리를 클릭하고 * 주석 * 을 선택합니다.

   주석 페이지가 표시됩니다.

3. 서비스 수준, 스위치 수준 또는 계층 주석 위에 커서를 놓고 를 클릭합니다 .

   Edit Annotation(주석 편집) 대화 상자가 표시됩니다.

4. 비용 * 필드에 기존 수준의 값을 입력합니다.

   계층 및 서비스 수준 주석에는 각각 자동 계층 및 오브젝트 스토리지 값이 있으며, 이 값은 제거할 수 없습니다.

5. 을 클릭합니다 + Add 를 눌러 수준을 추가합니다.
6. 작업을 마치면 * 저장 * 을 클릭합니다.

주석을 사용하여 비즈니스 요구에 맞는 맞춤형 비즈니스 관련 데이터를 자산에 추가할 수 있습니다. OnCommand Insight에서 기본 주석 집합을 제공하는 경우 다른 방법으로 데이터를 볼 수 있습니다. 사용자 지정 주석의 데이터는 스위치 제조업체, 포트 수 및 성능 통계와 같이 이미 수집된 장치 데이터를 보완합니다. 주석을 사용하여 추가하는 데이터는 Insight에서 검색되지 않습니다.

단계

1. Insight 웹 UI에 로그인합니다.
2. 관리 * 를 클릭하고 * 주석 * 을 선택합니다.

   주석 페이지에는 주석 목록이 표시됩니다.

3. 을 클릭합니다 + Add .

   주석 추가 * 대화 상자가 표시됩니다.

4. 이름 * 및 * 설명 * 필드에 이름과 설명을 입력합니다.

   이 필드에는 최대 255자까지 입력할 수 있습니다.

   > 점 ""으로 시작하거나 끝나는 주석 이름. 지원되지 않습니다.

5. Type * 을 클릭한 다음 이 주석에 허용되는 데이터 유형을 나타내는 다음 옵션 중 하나를 선택합니다.
   - 부울

     그러면 예 및 아니요 선택 항목이 있는 드롭다운 목록이 만들어집니다 예를 들어 "Direct Attached" 주석은 Boolean입니다.

   - 날짜

     이렇게 하면 날짜가 들어 있는 필드가 만들어집니다. 예를 들어, 주석이 날짜가 될 경우 이를 선택합니다.

   - 목록

     이렇게 하면 다음 중 하나가 생성될 수 있습니다.

     - 드롭다운 고정 목록

       다른 사용자가 장치에 이 주석 유형을 할당하는 경우 목록에 값을 더 추가할 수 없습니다.

     - 드롭다운 유연한 목록

       이 목록을 만들 때 * Add new values on the fly * 옵션을 선택하면 다른 사용자가 장치에 이 주석 유형을 할당할 때 목록에 더 많은 값을 추가할 수 있습니다.

   - 번호

이렇게 하면 주석을 지정하는 사용자가 숫자를 입력할 수 있는 필드가 생성됩니다. 예를 들어, 주석 유형이 ""바닥""인 경우 사용자는 ""숫자""의 값 유형을 선택하고 바닥 번호를 입력할 수 있습니다.

- 텍스트

  그러면 자유 형식 텍스트를 허용하는 필드가 만들어집니다. 예를 들어, 주석 유형으로 ""Language""를 입력하고 값 유형으로 ""Text""를 선택한 다음 언어를 값으로 입력할 수 있습니다.

> ⓘ 유형을 설정하고 변경 사항을 저장한 후에는 주석 유형을 변경할 수 없습니다. 유형을 변경해야 하는 경우 주석을 삭제하고 새 주석을 만들어야 합니다.

6. 주석 유형으로 목록 을 선택한 경우 다음을 수행합니다.
   a. 자산 페이지에서 주석에 더 많은 값을 추가할 수 있는 기능을 원하는 경우 * 즉시 새 값 추가 * 를 선택하여 유연한 목록을 만듭니다.

      예를 들어 자산 페이지에 있고 자산에는 Detroit, Tampa 및 Boston 값이 있는 City 주석이 있다고 가정해 보겠습니다. 빠른 실행 시 새 값 추가 * 옵션을 선택한 경우 주석 페이지로 이동하여 추가할 필요 없이 자산 페이지에서 샌프란시스코 및 시카고와 같은 도시에 직접 추가 값을 추가할 수 있습니다. 이 옵션을 선택하지 않으면 주석을 적용할 때 새 주석 값을 추가할 수 없습니다. 그러면 고정 목록이 생성됩니다.

   b. 값 * 및 * 설명 * 필드에 값과 이름을 입력합니다.
   c. 을 클릭합니다 ✚ Add 를 눌러 추가 값을 추가합니다.
   d. 을 클릭합니다 🗑 를 눌러 값을 제거합니다.
7. 저장 * 을 클릭합니다.

   주석이 주석 페이지의 목록에 나타납니다.

- 관련 정보 *

"사용자 데이터 가져오기 및 내보내기"

자산에 주석 수동 할당

자산에 주석을 지정하면 비즈니스와 관련된 방식으로 자산을 정렬, 그룹화 및 보고할 수 있습니다. 주석 규칙을 사용하여 특정 유형의 자산에 주석을 자동으로 할당할 수 있지만 자산 페이지를 사용하여 개별 자산에 주석을 할당할 수 있습니다.

시작하기 전에

지정할 주석을 만들어야 합니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 다음 중 하나를 수행하여 주석을 적용할 자산을 찾습니다.
   - 자산 대시보드에서 자산을 클릭합니다.
   - 을 클릭합니다 🔍 도구 모음에서 * 자산 검색 * 상자를 표시하려면 자산의 유형 또는 이름을 입력한 다음

표시되는 목록에서 자산을 선택합니다.

자산 페이지가 표시됩니다.

3. 자산 페이지의 * 사용자 데이터 * 섹션에서 를 클릭합니다 + Add .

   주석 추가 대화 상자가 표시됩니다.

4. Annotation(주석) * 을 클릭하고 목록에서 주석을 선택합니다.
5. 값 * 을 클릭하고 선택한 주석 유형에 따라 다음 중 하나를 수행합니다.
   - 주석 유형이 목록, 날짜 또는 부울인 경우 목록에서 값을 선택합니다.
   - 주석 유형이 텍스트인 경우 값을 입력합니다.
6. 저장 * 을 클릭합니다.
7. 주석을 지정한 후 주석 값을 변경하려면 을 클릭합니다 다른 값을 선택합니다.

   주석이 * 주석 지정 시 동적으로 값 추가 * 옵션을 선택한 목록 유형인 경우 기존 값을 선택하는 것 외에도 새 값을 추가하도록 입력할 수 있습니다.

주석 수정

주석의 이름, 설명 또는 값을 변경하거나 더 이상 사용하지 않을 주석을 삭제할 수 있습니다.

단계

1. OnCommand Insightfob UI에 로그인합니다.
2. 관리 * 를 클릭하고 * 주석 * 을 선택합니다.

   주석 페이지가 표시됩니다.

3. 편집할 주석 위에 커서를 놓고 클릭합니다 .

   Edit Annotation(주석 편집) * 대화 상자가 표시됩니다.

4. 주석을 다음과 같이 수정할 수 있습니다.

   a. 이름, 설명 또는 둘 모두를 변경합니다.

      그러나 이름과 설명 모두에 최대 255자를 입력할 수 있으며 주석 유형은 변경할 수 없습니다. 또한 시스템 수준 주석의 경우 이름이나 설명을 변경할 수 없지만, 주석이 목록 유형인 경우 값을 추가하거나 제거할 수 있습니다.

      > 사용자 지정 주석이 데이터 웨어하우스에 게시되고 이름을 바꾸면 내역 데이터가 손실됩니다.

   a. 목록 유형의 주석에 다른 값을 추가하려면 을 클릭합니다 + Add .
   b. 목록 유형의 주석에서 값을 제거하려면 를 클릭합니다 .

      주석 값이 주석 규칙, 쿼리 또는 성능 정책에 포함된 주석과 관련된 경우 주석 값을 삭제할 수 없습니다.

5. 작업을 마치면 * 저장 * 을 클릭합니다.

작업을 마친 후

데이터 웨어하우스에서 주석을 사용하려는 경우 데이터 웨어하우스에서 주석을 강제로 업데이트해야 합니다. OnCommand Insight 데이터 웨어하우스 관리 가이드 _ 를 참조하십시오.

주석 삭제

더 이상 사용하지 않을 주석을 삭제할 수 있습니다. 시스템 수준 주석 또는 주석 규칙, 쿼리 또는 성능 정책에 사용되는 주석은 삭제할 수 없습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 관리 * 를 클릭하고 * 주석 * 을 선택합니다.

   주석 페이지가 표시됩니다.

3. 삭제할 주석 위에 커서를 놓고 를 클릭합니다 🗑 .

   확인 대화 상자가 표시됩니다.

4. 확인 * 을 클릭합니다.

주석 규칙을 사용하여 자산에 주석 지정

사용자가 정의한 기준에 따라 자산에 주석을 자동으로 할당하려면 주석 규칙을 구성합니다. OnCommand Insight는 이러한 규칙에 따라 자산에 주석을 할당합니다. 또한 Insight에서는 두 가지 기본 주석 규칙을 제공합니다. 이 규칙은 필요에 맞게 수정하거나 사용하지 않으려는 경우 제거할 수 있습니다.

기본 스토리지 주석 규칙

스토리지 주석을 리소스에 빠르게 할당할 수 있도록 OnCommand Insight에는 21개의 기본 주석 규칙이 포함되어 있으며, 이 규칙은 계층 레벨을 스토리지 계층 모델과 연결합니다. 모든 스토리지 리소스는 귀사 환경에서 자산을 획득할 때 계층에 자동으로 연결됩니다.

기본 주석 규칙은 다음과 같은 방법으로 계층 주석을 적용합니다.

- 계층 1, 스토리지 품질 계층

  Tier 1 주석은 EMC(Symmetrix), HDS(HDS9500V, HDS9900, HDS9900V, R600, R700, USP r, USP V), IBM(DS8000), NetApp(FAS6000 또는 FAS6200), Violin(Memory).

- 계층 2, 스토리지 품질 계층

  Tier 2 주석은 HP(3PAR StoreServ 또는 EVA), EMC(CLARiiON), HDS(AMS 또는 D800), IBM(XIV), NetApp(FAS3000, FAS3100 및 FAS3200) 등의 공급업체 및 지정된 제품군에 적용됩니다.

이러한 규칙의 기본 설정을 계층 요구 사항에 맞게 편집하거나 필요하지 않은 경우 제거할 수 있습니다.

주석 규칙 작성

개별 자산에 주석을 수동으로 적용하는 대신 주석 규칙을 사용하여 여러 자산에 주석을 자동으로 적용할 수 있습니다. Insight에서 주석 규칙을 평가할 때 개별 자산 페이지에 수동으로 설정된 주석이 규칙 기반 주석보다 우선합니다.

시작하기 전에

주석 규칙에 대한 쿼리를 만들어야 합니다.

이 작업에 대해

규칙을 만드는 동안 주석 유형을 편집할 수 있지만, 미리 유형을 정의해야 합니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. Manage * 를 클릭하고 * Annotation rules * 를 선택합니다.

   주석 규칙 페이지에는 기존 주석 규칙 목록이 표시됩니다.

3. 을 클릭합니다 + Add .

   규칙 추가 대화 상자가 표시됩니다.

4. 다음을 수행합니다.
   a. 이름 * 상자에 규칙을 설명하는 고유한 이름을 입력합니다.

      이 이름은 주석 규칙 페이지에 표시됩니다.

   b. Query * 를 클릭하고 OnCommand Insight가 에셋에 주석을 적용하는 데 사용해야 하는 쿼리를 선택합니다.
   c. Annotation(주석) * 을 클릭하고 적용할 주석을 선택합니다.
   d. 값 * 을 클릭하고 주석 값을 선택합니다.

      예를 들어 주석으로 생일 을 선택한 경우 값의 날짜를 지정합니다.

5. 저장 * 을 클릭합니다.
6. 모든 규칙을 즉시 실행하려면 * 모든 규칙 실행 * 을 클릭합니다. 그렇지 않으면 규칙들이 정기적으로 예약된 간격으로 실행됩니다.

주석 규칙 우선 순위 설정

기본적으로 OnCommand Insight에서는 주석 규칙을 순차적으로 평가합니다. 그러나 Insight에서 특정 순서로 규칙을 평가하려면 OnCommand Insight에서 주석 규칙을 평가하는 순서를 구성할 수 있습니다.

단계

1. Insight트위브 UI에 로그인합니다.
2. Manage * 를 클릭하고 * Annotation rules * 를 선택합니다.

   주석 규칙 페이지에는 기존 주석 규칙 목록이 표시됩니다.

3. 주석 규칙 위에 커서를 놓습니다.

   우선 순위 화살표가 규칙의 오른쪽에 나타납니다.

4. 목록에서 규칙을 위 또는 아래로 이동하려면 위쪽 화살표 또는 아래쪽 화살표를 클릭합니다.

   기본적으로 새 규칙은 규칙 목록에 순차적으로 추가됩니다. Insight에서 주석 규칙을 평가할 때 개별 자산 페이지에 수동으로 설정된 주석이 규칙 기반 주석보다 우선합니다.

주석 규칙 수정

주석 규칙을 수정하여 규칙 이름, 주석, 주석 값 또는 규칙과 연결된 쿼리를 변경할 수 있습니다.

단계

1. OnCommand Insightfob UI에 로그인합니다.
2. Manage * 를 클릭하고 * Annotation rules * 를 선택합니다.

   주석 규칙 페이지에는 기존 주석 규칙 목록이 표시됩니다.

3. 수정할 규칙을 찾습니다.
   - 주석 규칙 페이지에서 필터 상자에 값을 입력하여 주석 규칙을 필터링할 수 있습니다.
   - 페이지에 맞는 규칙보다 더 많은 규칙이 있는 경우 페이지 번호를 클릭하여 페이지별로 주석 규칙을 찾아봅니다.
4. 다음 중 하나를 수행하여 * 규칙 편집 * 대화 상자를 표시합니다.
   - 주석 규칙 페이지에 있는 경우 주석 규칙 위에 커서를 놓고 을 클릭합니다 .
   - 자산 페이지에 있는 경우 규칙과 연결된 주석 위에 커서를 놓고 규칙 이름이 표시되면 커서를 규칙 이름 위에 놓은 다음 규칙 이름을 클릭합니다.
5. 필요한 내용을 변경하고 * Save * 를 클릭합니다.

주석 규칙 삭제

규칙이 더 이상 네트워크의 개체를 모니터링할 필요가 없는 경우 주석 규칙을 삭제할 수 있습니다.

단계

1. OnCommand Insightfob UI에 로그인합니다.
2. 관리 * 를 클릭하고 * 주석 규칙 * 을 선택합니다.

   주석 규칙 페이지에는 기존 주석 규칙 목록이 표시됩니다.

3. 삭제할 규칙을 찾습니다.
   - 주석 규칙 페이지에서 필터 상자에 값을 입력하여 주석 규칙을 필터링할 수 있습니다.
   - 한 페이지에 맞는 규칙보다 더 많은 규칙이 있는 경우 페이지 번호를 클릭하여 페이지별로 주석 규칙을 찾아봅니다.
4. 삭제할 규칙 위에 커서를 놓은 다음 을 클릭합니다 🗑 .

   규칙을 삭제할 것인지 묻는 확인 메시지가 표시됩니다.

5. 확인 * 을 클릭합니다.

주석 값 불러오기

CSV 파일에서 SAN 객체(예: 스토리지, 호스트, 가상 머신)에 대한 주석을 유지하는 경우 해당 정보를 OnCommand Insight로 가져올 수 있습니다. 응용 프로그램, 사업체 또는 계층 및 건물 등의 주석을 가져올 수 있습니다.

이 작업에 대해

다음 규칙이 적용됩니다.

- 주석 값이 비어 있으면 해당 주석이 개체에서 제거됩니다.
- 볼륨 또는 내부 볼륨에 주석을 달 때 개체 이름은 대시 및 화살표(->) 구분 기호를 사용하여 스토리지 이름과 볼륨 이름의 조합입니다.

```
<storage_name>-><volume_name>
```

- 스토리지, 스위치 또는 포트에 주석이 추가된 경우 응용 프로그램 열은 무시됩니다.
- Tenant, Line_of_Business, Business_Unit 및 Project 열은 업무 엔티티를 만듭니다.

  모든 값은 비워 둘 수 있습니다. 응용 프로그램이 이미 입력 값과 다른 업무 엔티티와 연결되어 있는 경우 응용 프로그램은 새 업무 엔티티에 할당됩니다.

가져오기 유틸리티에서 지원되는 개체 유형 및 키는 다음과 같습니다.

유형	키
호스트	id-><id> 또는 <Name> 또는 <IP>
VM	id-><id> 또는 <Name>
스토리지 풀	id-><id> 또는 `<Storage_name>`를 클릭합니다<Storage_Pool_name>
내부 볼륨	id-><id> 또는 `<Storage_name>`를 클릭합니다<Internal_volume_name>

볼륨	id-><id> 또는 `<Storage_name>`를 클릭합니다<Volume_name>
스토리지	id-><id> 또는 <Name> 또는 <IP>
스위치	id-><id> 또는 <Name> 또는 <IP>
포트	id-><id> 또는 <WWN>
공유	id-><id> 또는 <Storage Name>-><Internal Volume Name>-><Share Name>-><Protocol> <Qtree> 기본 qtree가 있는 경우 선택 사항입니다.
qtree입니다	id-><id> 또는 <Storage Name>-><Internal Volume Name>-><Qtree Name>

CSV 파일은 다음 형식을 사용해야 합니다.

```
, , <Annotation Type> [, <Annotation Type> ...]
[, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]

<Object Type Value 1>, <Object Key 1>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]

...

<Object Type Value N>, <Object Key N>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]
```

단계

1. Insight 웹 UI에 로그인합니다.
2. Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.

   문제 해결 페이지가 표시됩니다.

3. 페이지의 * 기타 작업 섹션 * 에서 * OnCommand Insight 포털 * 링크를 클릭합니다.
4. Insight Connect API * 를 클릭합니다.
5. 포털에 로그인합니다.
6. 주석 가져오기 유틸리티 * 를 클릭합니다.

7. 를 저장합니다 `.zip` 파일을 압축 해제하고 를 읽습니다 `readme.txt` 추가 정보 및 샘플을 위한 파일.
8. CSV 파일을 와 동일한 폴더에 저장합니다 `.zip` 파일.
9. 명령줄 창에서 다음을 입력합니다.

```
java -jar rest-import-utility.jar [-uusername] [-ppassword]
[-aserver name or IP address] [-bbatch size] [-ccase
sensitive:true/false]
[-lextra logging:true/false] csv filename
```

추가 로깅을 사용하는 -l 옵션과 대/소문자 구분을 사용하는 -c 옵션은 기본적으로 false로 설정됩니다. 따라서 피처를 사용하려는 경우에만 지정해야 합니다.

> 옵션과 해당 값 사이에는 공백이 없습니다.

> 다음 키워드는 예약되며 사용자가 주석 이름으로 지정할 수 없습니다. - Application - Application_Priority - Tenant - Line_of_Business - Business_Unit - 예약된 키워드 중 하나를 사용하여 주석 유형을 가져오려고 하면 프로젝트 오류가 생성됩니다. 이러한 키워드를 사용하여 주석 이름을 만든 경우, 불러오기 유틸리티 도구가 올바르게 작동할 수 있도록 주석을 수정해야 합니다.

> 주석 가져오기 유틸리티를 사용하려면 Java 8 또는 Java 11이 필요합니다. 가져오기 유틸리티를 실행하기 전에 이 중 하나가 설치되어 있는지 확인하십시오. 최신 OpenJDK 11을 사용하는 것이 좋습니다.

쿼리를 사용하여 여러 자산에 주석 할당

자산 그룹에 주석을 할당하면 쿼리 또는 대시보드에서 관련 자산을 보다 쉽게 식별하거나 사용할 수 있습니다.

시작하기 전에

자산에 지정하려는 주석이 이미 생성되어 있어야 합니다.

이 작업에 대해

쿼리를 사용하여 여러 자산에 주석을 할당하는 작업을 단순화할 수 있습니다. 예를 들어 특정 데이터 센터 위치의 모든 어레이에 사용자 지정 주소 주석을 할당하려는 경우

단계

1. 새 쿼리를 만들어 주석을 할당할 자산을 식별합니다. 쿼리 * > * + 새 쿼리 * 를 클릭합니다.
2. Search for… * 드롭다운에서 * Storage * 를 선택합니다. 표시된 저장소 목록을 더 좁히도록 필터를 설정할 수 있습니다.
3. 표시된 저장소 목록에서 저장소 이름 옆의 확인란을 클릭하여 하나 이상의 저장소 를 선택합니다. 목록 상단의 기본 확인란을 클릭하여 표시된 모든 저장소를 선택할 수도 있습니다.

4. 원하는 저장소를 모두 선택한 경우 * Actions * > * Edit Annotation * 을 클릭합니다.

   주석 추가 대화 상자가 표시됩니다.

5. 저장소에 할당할 * 주석 * 및 * 값 * 을 선택하고 * 저장 * 을 클릭합니다.

   해당 주석의 열을 표시하는 경우 선택한 모든 저장소에 표시됩니다.

6. 이제 주석을 사용하여 위젯 또는 쿼리의 저장소를 필터링할 수 있습니다. 위젯에서 다음을 수행할 수 있습니다.

   a. 대시보드를 만들거나 기존 대시보드를 엽니다. 변수 * 를 추가하고 위의 저장소에 설정한 주석을 선택합니다. 변수가 대시보드에 추가됩니다.

   b. 방금 추가한 변수 필드에서 * any * 를 클릭하고 필터링할 적절한 값을 입력합니다. 체크 표시를 클릭하여 변수 값을 저장합니다.

   c. 위젯을 추가합니다. 위젯의 쿼리에서 필터 기준 **+** 단추를 클릭하고 목록에서 적절한 주석을 선택합니다.

   d. 아무 * 나 * 를 클릭하고 위에서 추가한 주석 변수를 선택합니다. 작성한 변수는 ""$"로 시작하고 드롭다운에 표시됩니다.

   e. 원하는 다른 필터 또는 필드를 설정한 다음 위젯이 원하는 대로 사용자 지정되면 * 저장 * 을 클릭합니다.

   대시보드의 위젯에는 주석을 할당한 저장소에 대한 데이터만 표시됩니다.

자산 쿼리 중

쿼리를 사용하면 사용자 선택 기준(주석 및 성능 메트릭)에 따라 사용자 환경의 자산을 세분화된 수준으로 검색하여 네트워크를 모니터링하고 문제를 해결할 수 있습니다. 또한 자산에 주석을 자동으로 할당하는 주석 규칙에는 쿼리가 필요합니다.

쿼리 및 대시보드에 사용되는 자산

Insight 쿼리 및 대시보드 위젯은 다양한 자산 유형과 함께 사용할 수 있습니다

쿼리, 대시보드 위젯 및 사용자 지정 자산 페이지에서 다음 자산 유형을 사용할 수 있습니다. 필터, 식 및 표시에 사용할 수 있는 필드와 카운터는 자산 유형에 따라 달라집니다. 일부 자산은 일부 위젯 유형에 사용할 수 없습니다.

- 응용 프로그램
- 데이터 저장소
- 디스크
- 패브릭
- 일반 장치
- 호스트
- 내부 볼륨
- iSCSI 세션
- iSCSI 네트워크 포털
- 경로

- 포트
- qtree입니다
- 할당량
- 공유
- 스토리지
- 스토리지 노드
- 스토리지 풀
- 스위치
- 테이프
- VMDK입니다
- 가상 머신
- 볼륨
- Zone(영역)
- 존 구성원

쿼리 만들기

환경 내의 자산을 세분화된 수준으로 검색할 수 있도록 쿼리를 만들 수 있습니다. 쿼리를 사용하면 필터를 추가한 다음 결과를 정렬하여 하나의 뷰에서 인벤토리 및 성능 데이터를 볼 수 있으므로 데이터를 분류할 수 있습니다.

이 작업에 대해

예를 들어, 볼륨에 대한 쿼리를 생성하고, 선택한 볼륨과 연결된 특정 저장소를 찾기 위한 필터를 추가하고, 필터를 추가하여 선택한 저장소의 계층 1과 같은 특정 주석을 찾을 수 있습니다. 마지막으로 IOPS-Read(IO/s)가 25보다 큰 모든 스토리지를 찾기 위해 다른 필터를 추가합니다. 결과가 표시되면 쿼리와 관련된 정보 열을 오름차순 또는 내림차순으로 정렬할 수 있습니다.

자산을 취득하거나 주석 또는 응용 프로그램 할당을 만드는 새 데이터 원본이 추가되면 쿼리를 인덱싱한 후 정기적으로 예약된 간격으로 이러한 자산, 주석 또는 응용 프로그램을 쿼리할 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 쿼리 * 를 클릭하고 * + 새 쿼리 * 를 선택합니다.
3. 자원 유형 선택 * 을 클릭하고 자산 유형을 선택합니다.

   쿼리에 대해 자원을 선택하면 여러 기본 열이 자동으로 표시됩니다. 이러한 열을 제거하거나 언제든지 새 열을 추가할 수 있습니다.

4. 이름 * 텍스트 상자에 자산 이름을 입력하거나 자산 이름을 기준으로 필터링할 텍스트 부분을 입력합니다.

   다음 중 하나만 사용하거나 조합하여 새 쿼리 페이지의 텍스트 상자에서 검색을 구체화할 수 있습니다.

- 별표를 사용하면 모든 항목을 검색할 수 있습니다. 예를 들면, 다음과 같습니다. `vol*rhel` ""vol""로 시작하고 ""rhel""으로 끝나는 모든 리소스를 표시합니다.
- 물음표를 사용하면 특정 수의 문자를 검색할 수 있습니다. 예를 들면, 다음과 같습니다. `BOS-PRD??-S12` BOS-PRD12-S12, BOS-PRD13-S12 등을 표시합니다.
- 또는 연산자를 사용하여 여러 요소를 지정할 수 있습니다. 예를 들면, 다음과 같습니다. `FAS2240 OR CX600 OR FAS3270` 여러 스토리지 모델을 찾습니다.
- NOT 연산자를 사용하면 검색 결과에서 텍스트를 제외할 수 있습니다. 예를 들면, 다음과 같습니다. `NOT EMC*` "EMC"로 시작하지 않는 모든 항목을 찾습니다. 을 사용할 수 있습니다 `NOT *` 값이 없는 필드를 표시합니다.

5. 을 클릭합니다 ✓ 를 눌러 자산을 표시합니다.
6. 조건을 추가하려면 을 클릭합니다 More 다음 중 하나를 수행합니다.
   - 특정 기준을 검색하여 입력한 다음 선택합니다.
   - 목록을 아래로 스크롤하여 기준을 선택합니다.
   - IOPS-읽기(IO/s)와 같은 성능 메트릭을 선택한 경우 값 범위를 입력합니다. Insight에서 제공하는 기본 주석은 로 표시됩니다 즉, 이름이 중복된 주석이 있을 수 있습니다.

   조건 및 목록의 쿼리 결과에 대한 열이 쿼리 결과 목록에 추가됩니다.
7. 필요에 따라 를 클릭할 수도 있습니다 쿼리 결과에서 주석 또는 성능 메트릭을 제거합니다.

   예를 들어 쿼리에 데이터 저장소의 최대 지연 시간 및 최대 처리량이 표시되고 쿼리 결과 목록에 최대 지연 시간만을 표시하려면 이 단추를 클릭하고 * Throughput - Max * 확인란의 선택을 취소합니다. Throughput-Max(MB/s) 열이 쿼리 결과 목록에서 제거됩니다.

   > 쿼리 결과 테이블에 표시되는 열 수에 따라 추가된 열을 추가로 볼 수 없을 수도 있습니다. 원하는 열이 표시될 때까지 하나 이상의 열을 제거할 수 있습니다.

8. 저장 * 을 클릭하고 쿼리 이름을 입력한 다음 * 저장 * 을 다시 클릭합니다.

   관리자 역할이 있는 계정이 있는 경우 사용자 지정 대시보드를 만들 수 있습니다. 사용자 지정 대시보드는 위젯 라이브러리의 모든 위젯으로 구성될 수 있으며, 이 중 일부는 사용자 지정 대시보드에서 쿼리 결과를 나타낼 수 있습니다. 사용자 지정 대시보드에 대한 자세한 내용은 _OnCommand Insight 시작 가이드_를 참조하십시오.

   - 관련 정보 *

"사용자 데이터 가져오기 및 내보내기"

쿼리 보기

쿼리를 보고 자산을 모니터링하고 쿼리에 자산과 관련된 데이터가 표시되는 방식을 변경할 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 쿼리 * 를 클릭하고 * 모든 쿼리 표시 * 를 선택합니다.

3. 다음 중 하나를 실행하여 쿼리가 표시되는 방식을 변경할 수 있습니다.
    - 필터 * 상자에 텍스트를 입력하여 특정 쿼리를 표시할 수 있습니다.
    - 열 머리글의 화살표를 클릭하여 쿼리 테이블의 열 정렬 순서를 오름차순(위쪽 화살표) 또는 내림차순(아래쪽 화살표)으로 변경할 수 있습니다.
    - 열 크기를 조정하려면 파란색 막대가 나타날 때까지 열 머리글 위로 마우스를 가져갑니다. 마우스를 막대 위에 놓고 오른쪽이나 왼쪽으로 끕니다.
    - 열을 이동하려면 열 머리글을 클릭하고 오른쪽 또는 왼쪽으로 끕니다.
    - 쿼리 결과를 스크롤할 때 Insight에서 자동으로 데이터 원본을 폴링하므로 결과가 변경될 수 있습니다. 이로 인해 일부 항목이 누락되거나 정렬 방식에 따라 일부 항목이 순서대로 표시되지 않을 수 있습니다.

쿼리 결과를 **.csv** 파일로 내보내는 중입니다

쿼리 결과를 .csv 파일로 내보내 데이터를 다른 응용 프로그램으로 가져올 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 쿼리 * 를 클릭하고 * 모든 쿼리 표시 * 를 선택합니다.

   쿼리 페이지가 표시됩니다.

3. 쿼리를 클릭합니다.
4. 을 클릭합니다 ↑ 쿼리 결과를 로 내보냅니다`.csv` 파일.
5. 다음 중 하나를 수행합니다.
    - Open with * 를 클릭한 다음 * OK * 를 클릭하여 Microsoft Excel로 파일을 열고 파일을 특정 위치에 저장합니다.
    - 파일 저장 * 을 클릭한 다음 * 확인 * 을 클릭하여 파일을 다운로드 폴더에 저장합니다. 표시된 열의 속성만 내보내집니다. 표시되는 일부 열, 특히 복잡한 중첩 관계의 일부인 열은 내보내지지 않습니다.

      ⓘ 자산 이름에 쉼표가 나타나면 자산 이름과 올바른 .csv 형식을 유지하면서 내보내기가 따옴표로 이름을 묶습니다.

      + 쿼리 결과를 내보낼 때 결과 테이블의 * 모든 * 행이 화면에서 선택 또는 표시된 행이 아닌 최대 10,000개 행까지 내보내진다는 점에 유의하십시오.

      를 누릅니다

Excel에서 내보낸 .csv 파일을 열 때 NN:NN(두 자리 뒤에 콜론이 두 자리 더 오는 경우) 형식의 개체 이름이나 기타 필드가 있으면 Excel에서 해당 이름을 텍스트 형식 대신 시간 형식으로 해석하는 경우가 있습니다. 이로 인해 Excel에서 해당 열에 잘못된 값이 표시될 수 있습니다. 예를 들어 "81:45"라는 이름의 개체는 Excel에서 "81:45:00"으로 표시됩니다. 이 문제를 해결하려면 다음 단계를 사용하여 .csv를 Excel로 가져옵니다.

를 누릅니다

```
-   Open a new sheet in Excel.
-   On the "Data" tab, choose "From Text".
-   Locate the desired .CSV file and click "Import".
-   In the Import wizard, choose "Delimited" and click Next.
-   Choose "Comma" for the delimiter and click Next.
-   Select the desired columns and choose "Text" for the
column data format.
-   Click Finish.
Your objects should show in Excel in the proper format.
```

를 누릅니다

쿼리 수정

쿼리 중인 자산에 대한 검색 기준을 변경하려는 경우 쿼리와 연결된 조건을 변경할 수 있습니다.

단계

1. Insight트위브 UI에 로그인합니다.
2. 쿼리 * 를 클릭하고 * 모든 쿼리 표시 * 를 선택합니다.

   쿼리 페이지가 표시됩니다.

3. 쿼리 이름을 클릭합니다.
4. 쿼리에서 조건을 제거하려면 을 클릭합니다 🗑 .
5. 쿼리에 조건을 추가하려면 을 클릭합니다 More ▾ 을 클릭하고 목록에서 조건을 선택합니다.
6. 다음 중 하나를 수행합니다.
   - 저장 * 을 클릭하여 처음에 사용된 이름으로 쿼리를 저장합니다.
   - 다른 이름으로 저장을 클릭하여 쿼리를 다른 이름으로 저장합니다.
   - 처음에 사용한 쿼리 이름을 변경하려면 * 이름 바꾸기 * 를 클릭합니다.
   - 쿼리 이름을 처음 사용한 이름으로 다시 변경하려면 * 되돌리기 * 를 클릭합니다.

쿼리를 삭제하는 중입니다

더 이상 자산에 대한 유용한 정보를 수집하지 않을 경우 쿼리를 삭제할 수 있습니다. 쿼리가 주석 규칙에 사용되는 경우 삭제할 수 없습니다.

단계

1. Insight트위브 UI에 로그인합니다.
2. 쿼리 * 를 클릭하고 * 모든 쿼리 표시 * 를 선택합니다.

   쿼리 페이지가 표시됩니다.

3. 삭제할 쿼리 위에 커서를 놓고 클릭합니다 🗑 .

   쿼리를 삭제할 것인지 묻는 확인 메시지가 표시됩니다.

4. 확인 * 을 클릭합니다.

자산에 여러 애플리케이션을 할당하거나 자산에서 여러 애플리케이션을 제거합니다

수동으로 할당하거나 제거할 필요 없이 쿼리를 사용하여 여러 응용 프로그램을 자산에 할당하거나 자산에서 제거할 수 있습니다.

시작하기 전에

편집할 모든 자산을 찾는 쿼리를 이미 만들어야 합니다.

단계

1. 쿼리 * 를 클릭하고 * 모든 쿼리 표시 * 를 선택합니다.

   쿼리 페이지가 표시됩니다.

2. 자산을 찾는 쿼리의 이름을 클릭합니다.

   쿼리와 연결된 자산 목록이 표시됩니다.

3. 목록에서 원하는 자산을 선택하거나 를 클릭합니다 ☐ ▾ 모두 * 를 선택합니다.

   작업 * 버튼이 표시됩니다.

4. 선택한 자산에 애플리케이션을 추가하려면 을 클릭합니다 Actions ▾ 을 클릭하고 * 응용 프로그램 편집 * 을 선택합니다.
   a. 응용 프로그램 * 을 클릭하고 하나 이상의 응용 프로그램을 선택합니다.

      호스트, 내부 볼륨 및 가상 머신에 대해 여러 애플리케이션을 선택할 수 있지만, 볼륨에 대해 하나의 애플리케이션만 선택할 수 있습니다.

   b. 저장 * 을 클릭합니다.

5. 자산에 할당된 애플리케이션을 제거하려면 를 클릭합니다 Actions 을 클릭하고 * 응용 프로그램 제거 * 를 선택합니다.

   a. 제거할 응용 프로그램을 선택합니다.

   b. 삭제 * 를 클릭합니다.

   할당한 모든 새 응용 프로그램은 다른 자산에서 파생된 자산의 모든 응용 프로그램을 재정의합니다. 예를 들어, 볼륨은 호스트에서 애플리케이션을 상속하고 새 애플리케이션이 볼륨에 할당되면 새 애플리케이션이 파생된 애플리케이션보다 우선합니다.

자산에서 여러 주석 편집 또는 제거

수동으로 편집하거나 제거할 필요 없이 쿼리를 사용하여 자산에 대한 여러 주석을 편집하거나 자산에서 여러 주석을 제거할 수 있습니다.

시작하기 전에

편집하려는 모든 자산을 찾는 쿼리를 이미 만들어야 합니다.

단계

1. 쿼리 * 를 클릭하고 * 모든 쿼리 표시 * 를 선택합니다.

   쿼리 페이지가 표시됩니다.

2. 자산을 찾는 쿼리의 이름을 클릭합니다.

   쿼리와 연결된 자산 목록이 표시됩니다.

3. 목록에서 원하는 자산을 선택하거나 를 클릭합니다 ☐ ▾ 모두 * 를 선택합니다.

   작업 * 버튼이 표시됩니다.

4. 자산에 주석을 추가하거나 자산에 할당된 주석 값을 편집하려면 을 클릭합니다 Actions 을 클릭하고 * 주석 편집 * 을 선택합니다.

   a. Annotation(주석) * 을 클릭하고 값을 변경할 주석을 선택하거나 새 주석을 선택하여 모든 자산에 할당합니다.

   b. 값 * 을 클릭하고 주석 값을 선택합니다.

   c. 저장 * 을 클릭합니다.

5. 자산에 할당된 주석을 제거하려면 를 클릭합니다 Actions 을 클릭하고 * 주석 제거 * 를 선택합니다.

   a. Annotation(주석) * 을 클릭하고 자산에서 제거할 주석을 선택합니다.

   b. 삭제 * 를 클릭합니다.

테이블 값 복사 중

테이블의 값을 복사하여 검색 상자 또는 다른 응용 프로그램에서 사용할 수 있습니다.

이 작업에 대해

테이블 또는 쿼리 결과에서 값을 복사하는 데 사용할 수 있는 두 가지 방법이 있습니다.

단계

1. 방법 1: 마우스로 원하는 텍스트를 강조 표시하고 복사한 다음 검색 필드 또는 다른 응용 프로그램에 붙여 넣습니다.
2. 방법 2: 길이가 테이블 열 너비를 초과하는 단일 값 필드의 경우 줄임표(…)로 표시되며 필드 위로 마우스를 가져가서 클립보드 아이콘을 클릭합니다. 검색 필드 또는 기타 응용 프로그램에서 사용할 수 있도록 값이 클립보드에 복사됩니다.

   자산에 대한 링크인 값만 복사할 수 있습니다. 단일 값(예: 비목록)이 포함된 필드에만 복사 아이콘이 있습니다.

성능 정책 관리

OnCommand Insight를 사용하면 성능 정책을 생성하여 네트워크를 모니터링하여 다양한 임계값을 설정할 수 있으며, 임계값을 초과할 경우 경고를 발생시킬 수 있습니다. 성능 정책을 사용하면 임계치 위반을 즉시 탐지하고, 그 영향을 식별하고, 문제의 영향과 근본 원인을 빠르고 효과적으로 수정할 수 있는 방식으로 분석할 수 있습니다.

성능 정책을 사용하면 모든 오브젝트(데이터 저장소, 디스크, 하이퍼바이저, 내부 볼륨, 포트, 스토리지, 스토리지 노드, 스토리지 풀, VMDK, 가상 머신, 성능 카운터(예: 총 IOPS)를 포함하는 볼륨 임계값 위반이 발생하는 경우 Insight는 빨간색 실선 원, 이메일 경고(구성된 경우), 위반 대시보드 또는 위반을 보고하는 사용자 지정 대시보드를 표시하여 관련 자산 페이지에서 이를 감지하여 보고합니다.

Insight에서는 일부 기본 성능 정책을 제공합니다. 이러한 성능 정책은 사용자 환경에 적용할 수 없는 경우 수정하거나 삭제할 수 있으며 다음과 같은 개체에 대해 사용할 수 있습니다.

- 하이퍼바이저

  ESX 스와핑 및 ESX 사용률 정책이 있습니다.

- 내부 볼륨 및 볼륨

  각 리소스에 대해 두 가지 지연 정책이 있으며, 하나는 계층 1에 대해 주석이 추가되고 다른 하나는 계층 2에 대해 주석이 달립니다.

- 포트

  BB 크레딧 0에 대한 정책이 있습니다.

- 스토리지 노드

  노드 활용률에 대한 정책이 있습니다.

- 가상 머신

  VM 스와핑과 ESX CPU 및 메모리 정책이 있습니다.

- 볼륨

계층별 지연 시간 및 볼륨 정책 정렬 불량이 있습니다.

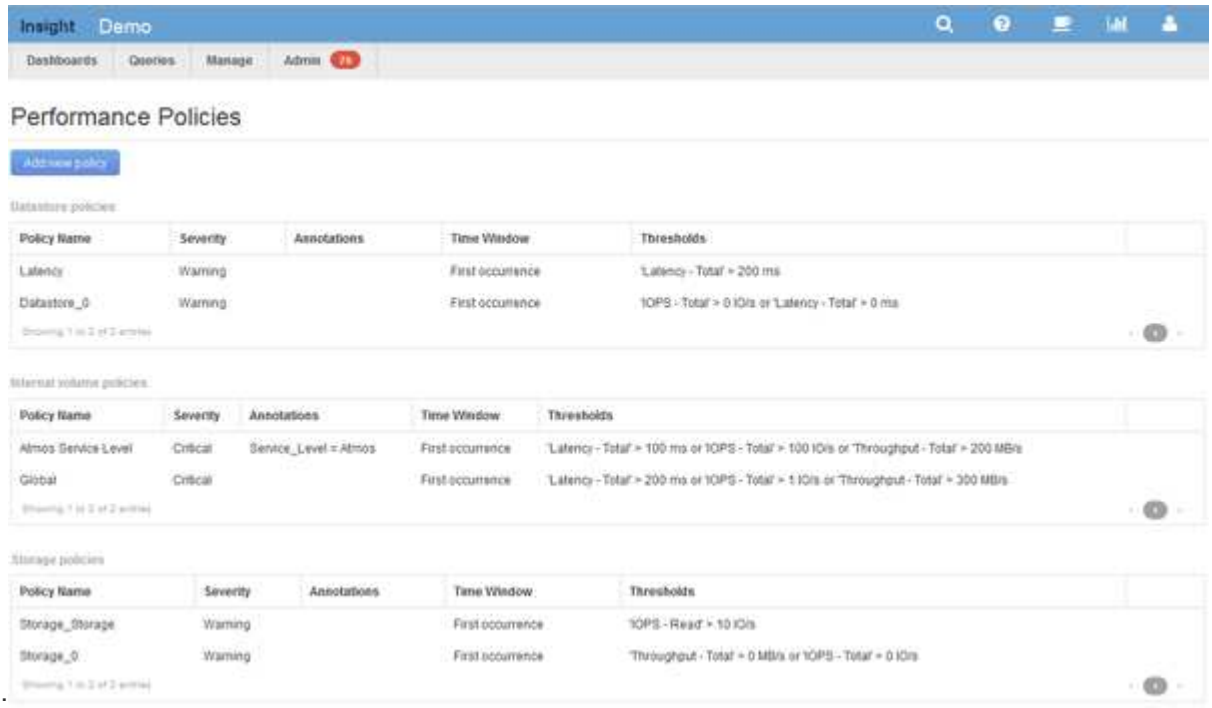
성능 정책 생성 중

성능 정책을 생성하여 네트워크 리소스와 관련된 문제를 알리기 위해 알림을 트리거하는 임계값을 설정합니다. 예를 들어, 스토리지 풀의 총 활용률이 60%를 초과할 경우 알림을 보낼 성능 정책을 생성할 수 있습니다.

단계

1. 브라우저에서 OnCommand Insight를 엽니다.
2. Manage * > * Performance Policies * 를 선택합니다.

   성능 정책 페이지가 표시됩니다



   정책은 객체별로 구성되며 해당 객체의 목록에 나타나는 순서대로 평가됩니다.

3. 새 정책 추가 * 를 클릭합니다.

   정책 추가 대화 상자가 표시됩니다.

4. Policy name * 필드에 정책 이름을 입력합니다.

   개체의 다른 모든 정책 이름과 다른 이름을 사용해야 합니다. 예를 들어, 내부 볼륨에 대해 "지연 시간"이라는 두 가지 정책을 사용할 수는 없지만, 내부 볼륨에 대해 "지연 시간" 정책과 다른 볼륨에 대해 "지연 시간" 정책을 사용할 수 있습니다. 가장 좋은 방법은 개체 유형에 관계없이 모든 정책에 대해 항상 고유한 이름을 사용하는 것입니다.

5. Type * 의 개체에 적용 목록에서 정책이 적용되는 개체 유형을 선택합니다.
6. With annotation * (주석 포함 *) 목록에서 주석 유형을 선택하고, 해당되는 경우 * Value * (값 *) 상자에 주석 값을 입력하여 이 특정 주석 세트가 있는 개체에만 정책을 적용합니다.

7. 객체 유형으로 * Port * 를 선택한 경우 * Connected to * 목록에서 포트가 연결된 대상을 선택합니다.
8. [다음 창 뒤에 적용]목록에서 임계값 위반을 나타내기 위해 경고를 표시할 시기를 선택합니다.

   첫 번째 발생 옵션은 첫 번째 데이터 샘플에서 임계값이 초과되면 알림을 트리거합니다. 다른 모든 옵션은 임계값을 한 번 넘어섰을 때 경고를 발생시키고 지정된 시간 이상 연속적으로 교차하는 경우에 발생합니다.

9. with severity * 목록에서 위반 심각도를 선택합니다.
10. 기본적으로 정책 위반에 대한 전자 메일 알림이 글로벌 전자 메일 목록의 받는 사람에게 전송됩니다. 특정 정책에 대한 알림이 특정 수신자에게 전송되도록 이러한 설정을 재정의할 수 있습니다.
    - 링크를 클릭하여 받는 사람 목록을 연 다음 * + * 버튼을 클릭하여 받는 사람을 추가합니다. 해당 정책에 대한 위반 알림은 목록의 모든 수신자에게 전송됩니다.
11. 다음 중 하나라도 참인 경우 * 알림 생성 섹션에서 * 임의 * 링크를 클릭하여 알림 트리거 방법을 제어합니다.
    - * 모두 *

      이 설정은 정책과 관련된 임계값 중 하나라도 넘을 경우 알림을 생성하는 기본 설정입니다.

    - * 모두 *

      이 설정은 정책에 대한 모든 임계값을 초과할 때 알림을 생성합니다. All * 을 선택하면 성능 정책에 대해 생성한 첫 번째 임계값을 기본 규칙이라고 합니다. 기본 규칙 임계값이 성능 정책에 대해 가장 우려되는 위반인지 확인해야 합니다.

12. Create alert if * 섹션에서 성능 카운터와 연산자를 선택한 다음 값을 입력하여 임계값을 생성합니다.
13. 임계값을 더 추가하려면 * Add threshold * (임계값 추가)를 클릭합니다.
14. 임계값을 제거하려면 휴지통 아이콘을 클릭합니다.
15. 경고 발생 시 정책 처리를 중지하려면 * 알림이 생성되면 추가 정책 처리 중지 * 확인란을 선택합니다.

    예를 들어, 데이터 저장소에 대한 정책이 4개 있고 경고가 발생할 때 처리를 중지하도록 두 번째 정책이 구성된 경우 두 번째 정책 위반이 활성화되어 있는 동안에는 세 번째 정책과 네 번째 정책이 처리되지 않습니다.

16. 저장 * 을 클릭합니다.

    성능 정책 페이지가 표시되고 성능 정책이 개체 유형에 대한 정책 목록에 표시됩니다.

성능 정책 평가 우선 순위

성능 정책 페이지는 정책을 개체 유형별로 그룹화하고 Insight는 개체의 성능 정책 목록에 나타나는 순서대로 정책을 평가합니다. Insight에서 정책을 평가하는 순서를 변경하여 네트워크에서 가장 중요한 정보를 표시할 수 있습니다.

Insight는 성능 데이터 샘플을 해당 개체에 대해 시스템으로 가져올 때 개체에 적용할 수 있는 모든 정책을 순차적으로 평가합니다. 하지만 주석에 따라 일부 정책은 하나의 개체 그룹에 적용되지 않습니다. 예를 들어 내부 볼륨에 다음 정책이 있다고 가정합니다.

- 정책 1(Insight 제공 기본 정책)
- 정책 2('서비스 수준=실버' 주석 및 경고가 생성되면 추가 정책 처리 중지 * 옵션 포함

- 정책 3("서비스 수준 = 골드" 주석 사용)
- 정책 4

Gold 주석이 있는 내부 볼륨 계층의 경우 Insight는 정책 1을 평가하고 정책 2를 무시한 다음 정책 3과 정책 4를 평가합니다. 주석이 없는 계층의 경우 Insight는 정책 순서에 따라 평가하므로 Insight는 정책 1과 정책 4만 평가합니다. Silver 주석이 있는 내부 볼륨 계층의 경우 Insight는 정책 1과 정책 2를 평가합니다. 그러나 정책의 임계값이 한 번 초과되어 정책에 지정된 시간 동안 연속적으로 교차하는 경우에 경고가 트리거되면 Insight는 개체의 현재 카운터를 평가하는 동안 목록의 다른 정책을 더 이상 평가하지 않습니다. Insight에서 객체에 대한 다음 성능 샘플 세트를 캡처하면 해당 객체에 대한 성능 정책을 필터 및 순서별로 다시 평가하기 시작합니다.

성능 정책의 우선 순위 변경

기본적으로 Insight는 오브젝트의 정책을 순차적으로 평가합니다. Insight에서 성능 정책을 평가하는 순서를 구성할 수 있습니다. 예를 들어, 골드 계층 스토리지에 대한 위반이 발생할 경우 해당 정책을 먼저 목록에 배치하고 동일한 스토리지 자산에 대한 일반적인 위반을 더 이상 보지 않도록 할 수 있습니다.

단계

1. 브라우저에서 Insight를 엽니다.
2. Manage * (관리 *) 메뉴에서 * Performance Policies * (성능 정책 *)를 선택합니다.

   성능 정책 페이지가 표시됩니다.

3. 개체 유형의 성능 정책 목록에서 정책 이름 위에 커서를 놓습니다.

   정책 오른쪽에 우선순위 화살표가 나타납니다.

4. 목록에서 정책을 위로 이동하려면 위쪽 화살표를 클릭하고 목록에서 정책을 아래로 이동하려면 아래쪽 화살표를 클릭합니다.

   기본적으로 새 정책은 개체의 정책 목록에 순차적으로 추가됩니다.

성능 정책 편집

기존 및 기본 성능 정책을 편집하여 Insight에서 사용자 네트워크의 관심 조건을 모니터링하는 방법을 변경할 수 있습니다. 예를 들어 정책의 임계값을 변경할 수 있습니다.

단계

1. 브라우저에서 Insight를 엽니다.
2. Manage * (관리 *) 메뉴에서 * Performance Policies * (성능 정책 *)를 선택합니다.

   성능 정책 페이지가 표시됩니다.

3. 개체의 성능 정책 목록에서 정책 이름 위에 커서를 놓습니다.
4. 을 클릭합니다 .

정책 편집 대화 상자가 표시됩니다.

5. 필요한 사항을 변경합니다.

   정책 이름 이외의 다른 옵션을 변경하면 Insight에서 해당 정책에 대한 모든 기존 위반 사항을 삭제합니다.

6. 저장 * 을 클릭합니다

성능 정책을 삭제하는 중입니다

네트워크의 객체를 모니터링하는 데 더 이상 적용되지 않을 경우 성능 정책을 삭제할 수 있습니다.

단계

1. 브라우저에서 Insight를 엽니다.
2. Manage * (관리 *) 메뉴에서 * Performance Policies * (성능 정책 *)를 선택합니다.

   성능 정책 페이지가 표시됩니다.

3. 개체의 성능 정책 목록에 있는 정책 이름 위에 커서를 놓습니다.
4. 을 클릭합니다 ✖.

   정책을 삭제할 것인지 묻는 메시지가 나타납니다.

5. 확인 * 을 클릭합니다.

사용자 데이터 가져오기 및 내보내기

가져오기 및 내보내기 기능을 사용하여 주석, 주석 규칙, 쿼리, 성능 정책 및 사용자 지정 대시보드를 하나의 파일로 내보낼 수 있습니다. 그런 다음 이 파일을 다른 OnCommand Insight 서버로 가져올 수 있습니다.

내보내기 및 가져오기 기능은 동일한 버전의 OnCommand Insight를 실행하는 서버 간에만 지원됩니다.

사용자 데이터를 내보내거나 가져오려면 * Admin * 을 클릭하고 * Setup * 을 선택한 다음 * Import/Export user data * 탭을 선택합니다.

가져오는 개체와 개체 형식에 따라 가져오기 작업 중에 데이터가 추가, 병합 또는 교체됩니다.

- 주석 유형
  - 대상 시스템에 동일한 이름의 주석이 없는 경우 주석을 추가합니다.
  - 주석 유형이 목록이고 이름이 같은 주석이 대상 시스템에 있는 경우 주석을 병합합니다.
  - 주석 유형이 목록 이외의 주석 유형이고 대상 시스템에 동일한 이름의 주석이 있는 경우 주석을 대체합니다.

> 이름이 같지만 유형이 다른 주석이 대상 시스템에 있는 경우 가져오기에 실패합니다. 개체가 실패한 주석에 따라 달라지는 경우 이러한 개체는 부정확하거나 원치 않는 정보를 표시할 수 있습니다. 가져오기 작업이 완료된 후에는 모든 주석 종속성을 확인해야 합니다.

- 주석 규칙
  - 대상 시스템에 같은 이름의 주석 규칙이 없으면 주석 규칙을 추가합니다.
  - 주석 규칙이 대상 시스템에 동일한 이름의 규칙이 있는 경우 주석 규칙을 바꿉니다.

> 주석 규칙은 쿼리와 주석 모두에 따라 달라집니다. 가져오기 작업이 완료된 후 모든 주석 규칙이 정확한지 확인해야 합니다.

- 정책
  - 대상 시스템에 동일한 이름의 정책이 없는 경우 정책을 추가합니다.
  - 대상 시스템에 동일한 이름의 정책이 있는 경우 정책을 교체합니다.

> 가져오기 작업이 완료된 후 정책이 순서를 벗어났을 수 있습니다. 가져온 후에는 정책 순서를 확인해야 합니다. 주석이 잘못된 경우 주석에 종속된 정책이 실패할 수 있습니다. 가져온 후에는 모든 주석 종속성을 확인해야 합니다.
>
> 를 누릅니다

- 쿼리
  - 대상 시스템에 동일한 이름의 쿼리가 없는 경우 쿼리를 추가합니다.
  - 쿼리의 리소스 유형이 다른 경우에도 대상 시스템에 동일한 이름의 쿼리가 있는 경우 쿼리를 바꿉니다.

> 쿼리의 리소스 유형이 다른 경우 가져오기 후 해당 쿼리를 사용하는 대시보드 위젯에 원치 않는 결과 또는 잘못된 결과가 표시될 수 있습니다. 가져오기 후 모든 쿼리 기반 위젯의 정확성을 확인해야 합니다. 주석이 잘못된 경우 주석에 종속된 쿼리가 실패할 수 있습니다. 가져온 후에는 모든 주석 종속성을 확인해야 합니다.
>
> 를 누릅니다

- 대시보드
  - 타겟 시스템에 동일한 이름의 대시보드가 없는 경우 대시보드를 추가합니다.
  - 쿼리의 리소스 유형이 다른 경우에도 대상 시스템에 동일한 이름의 대시보드가 있는 경우 대시보드를 대체합니다.

> 가져오기 후 대시보드의 모든 쿼리 기반 위젯이 정확한지 확인해야 합니다. 소스 서버에 동일한 이름의 대시보드가 여러 개 있는 경우 모두 내보내집니다. 그러나 첫 번째 서버만 대상 서버로 가져옵니다. 가져오는 동안 오류를 방지하려면 대시보드를 내보내기 전에 고유한 이름을 지정해야 합니다.
>
> 를 누릅니다