구성 및 관리

OnCommand Insight

NetApp
April 01, 2024

목차

구성 및 관리

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

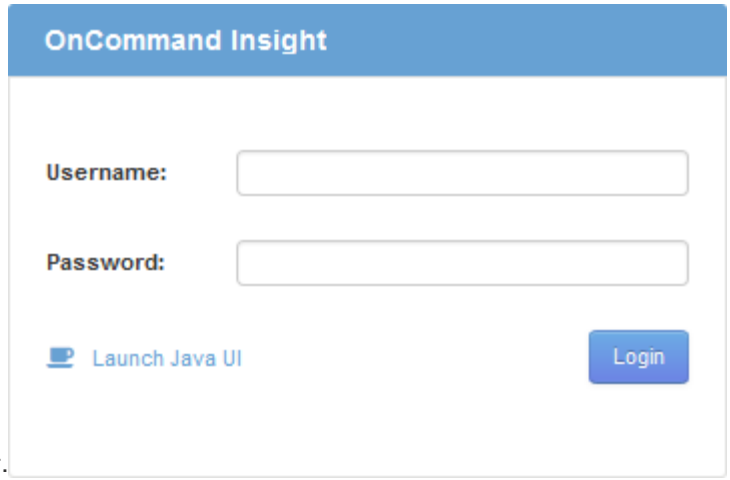
1. 다음 중 하나를 수행합니다.
   - Insight 서버에 대한 Insight를 엽니다.

     ```
     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.

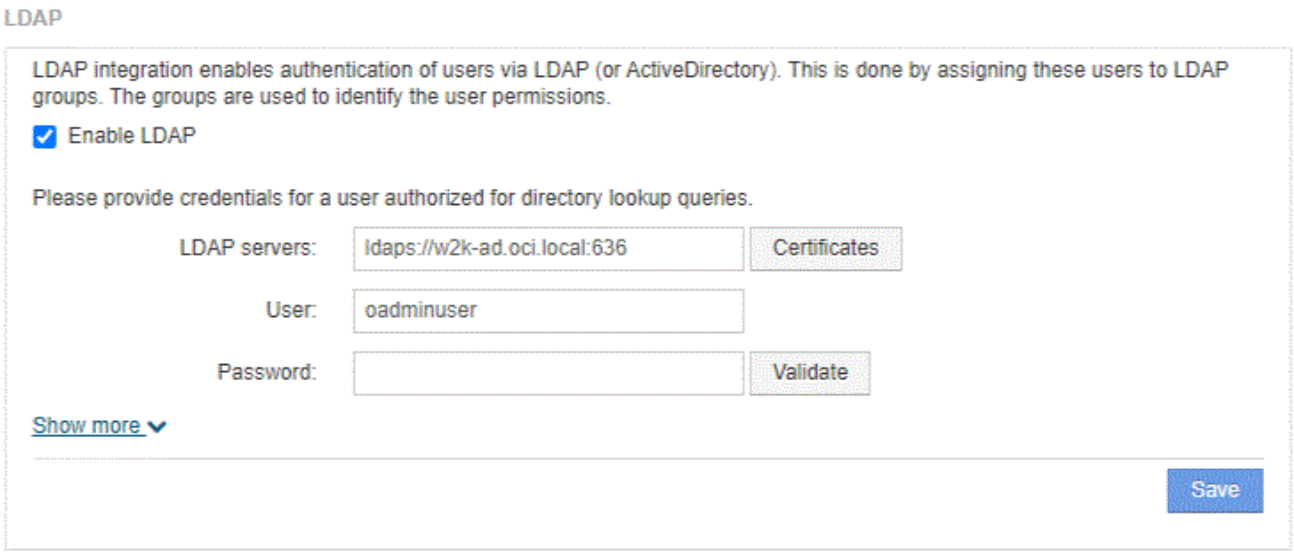
이 작업에 대해

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.

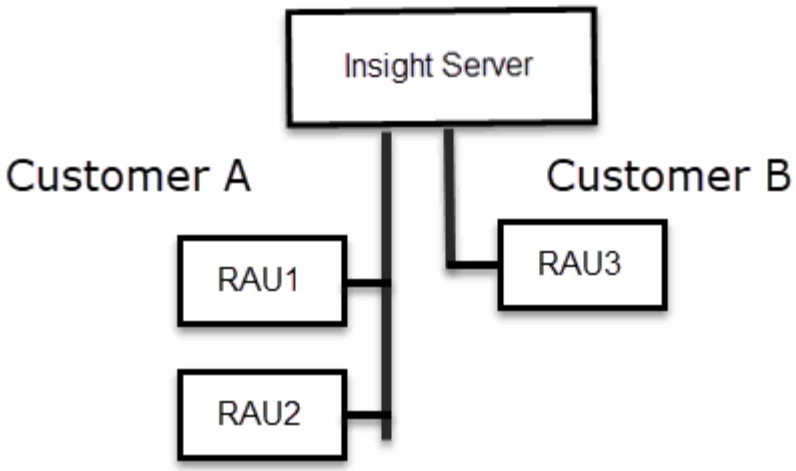
업그레이드 및 설치 고려 사항

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

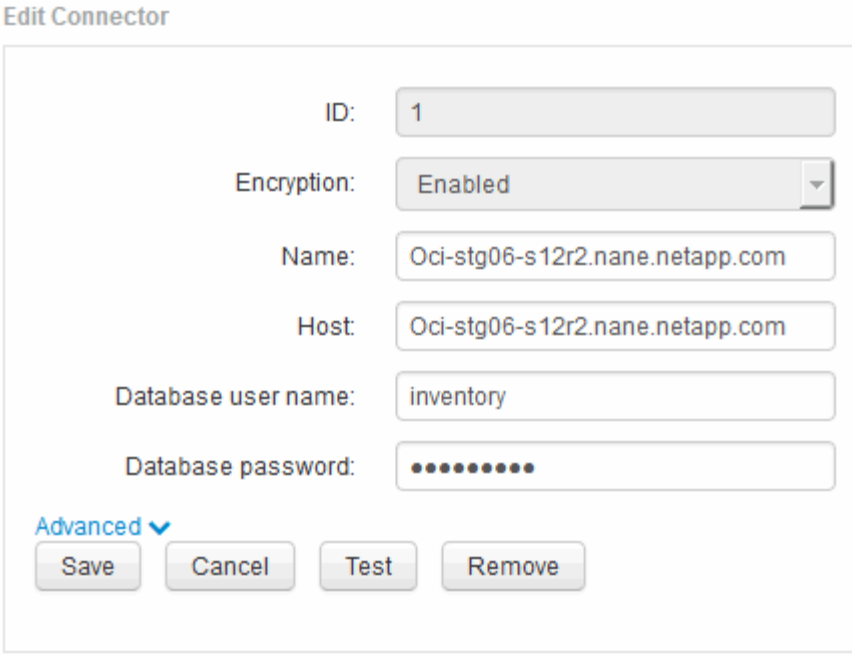
시작하기 전에

이 작업을 수행하려면 관리자로 로그인해야 합니다.

단계

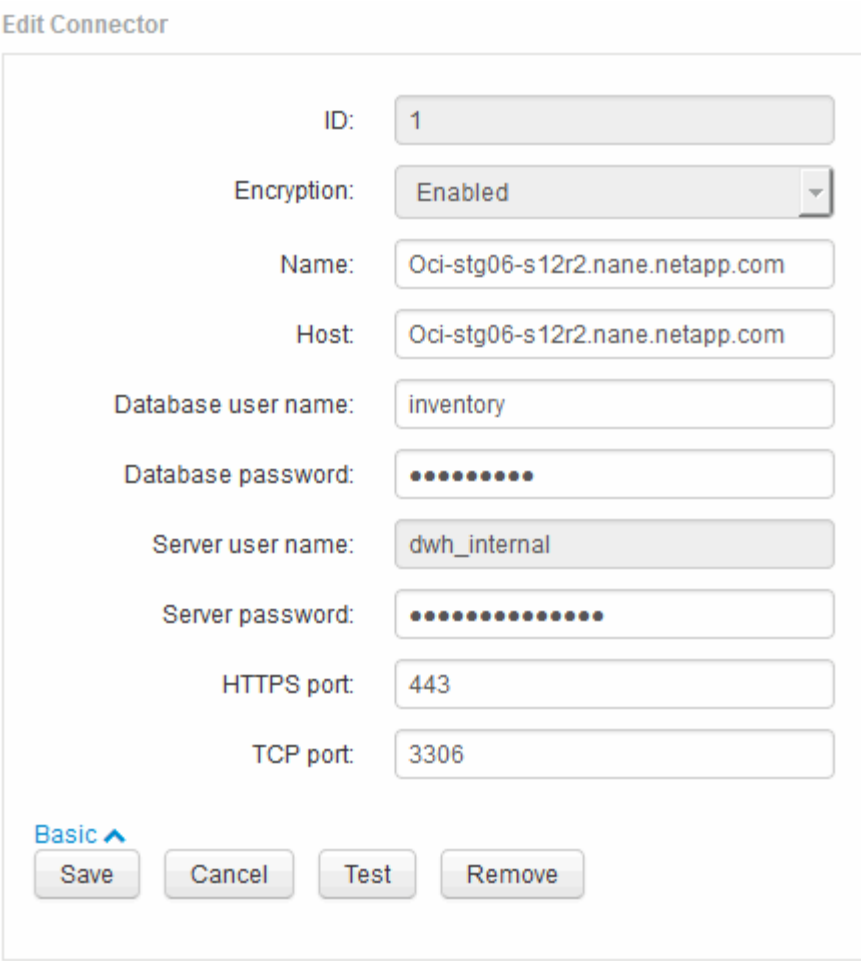
1. 에서 데이터 웨어하우스 포털에 로그인합니다 https://hostname/dwh여기서 hostname 은 OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 커넥터 * 를 클릭합니다.

   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.

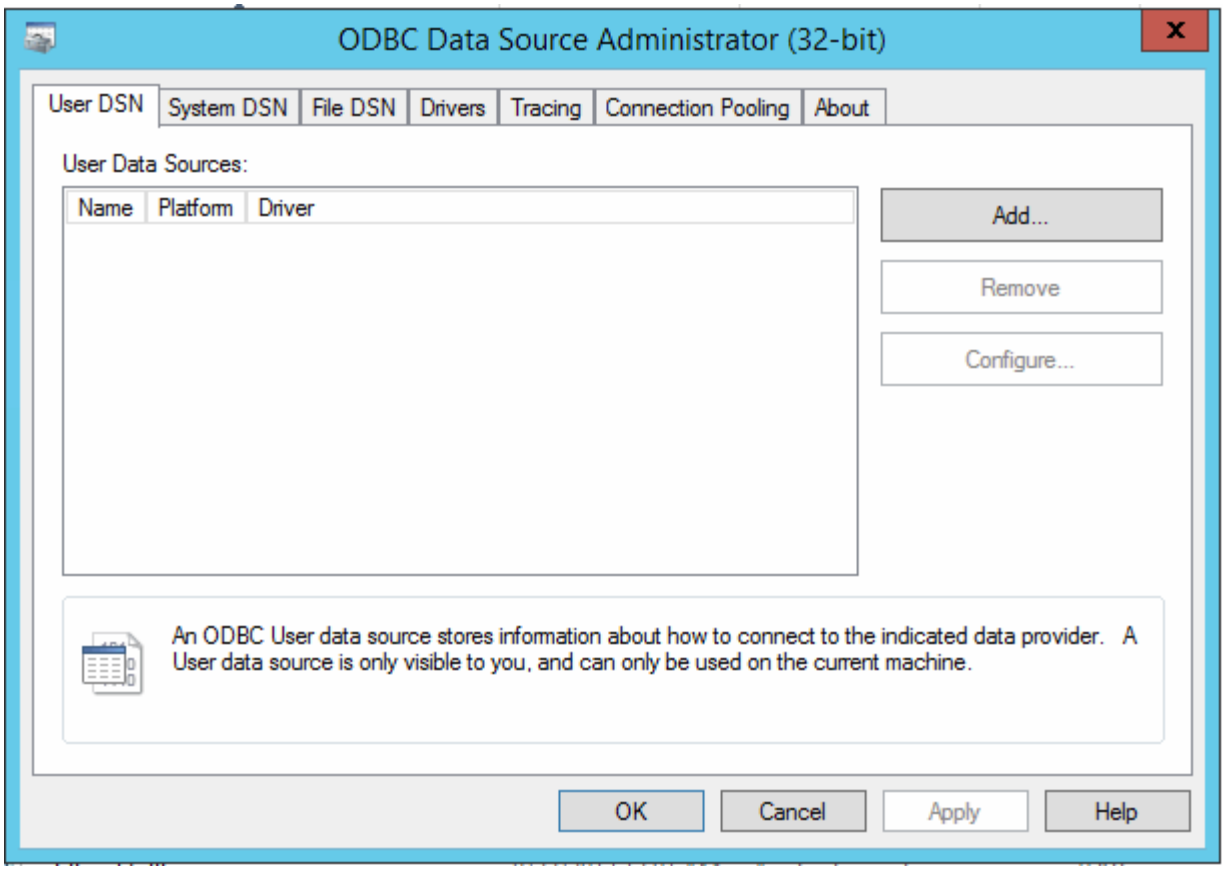
시작하기 전에

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

단계

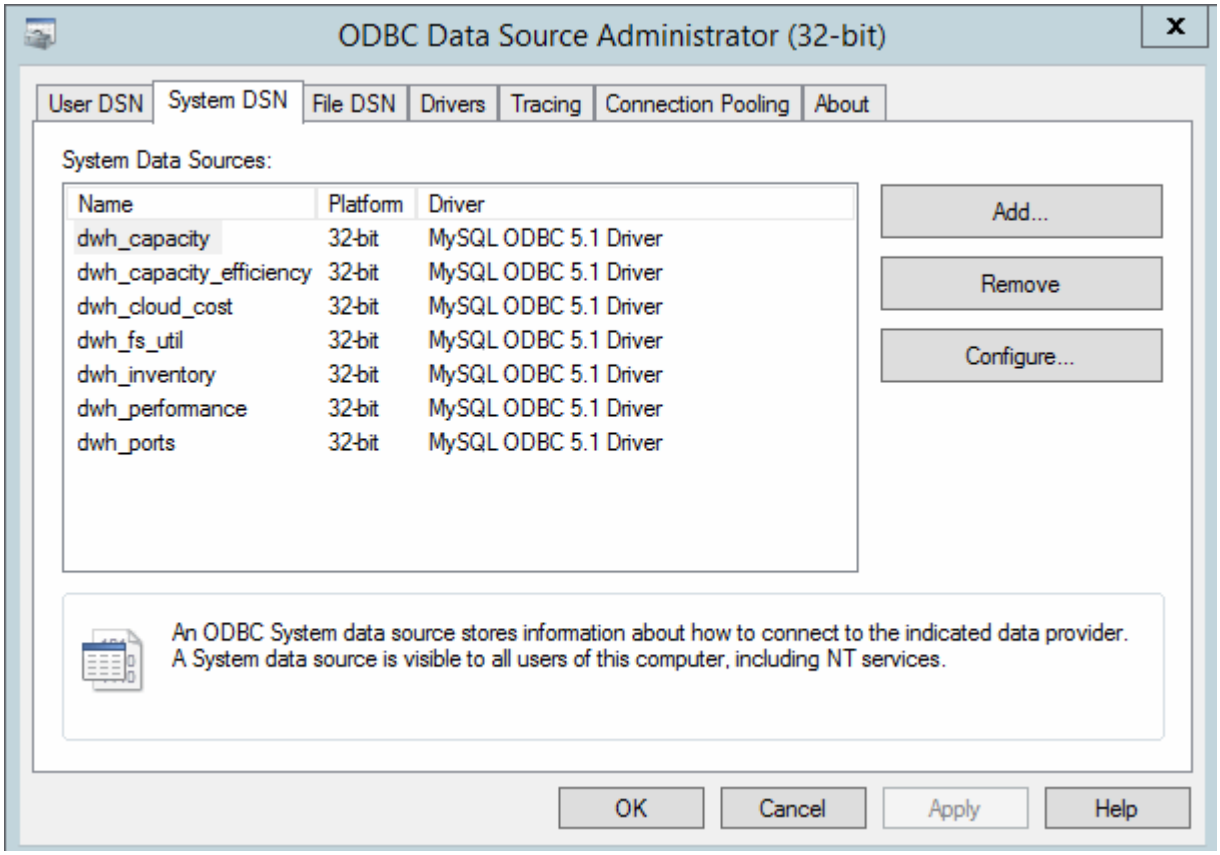
1. 해당 데이터 웨어하우스를 호스팅하는 서버에 원격 로그인을 수행합니다.
2. 에서 ODBC 관리 도구에 액세스합니다 `C:\Windows\SysWOW64\odbcad32.exe`

   ODBC 데이터 원본 관리자 화면이 표시됩니다.



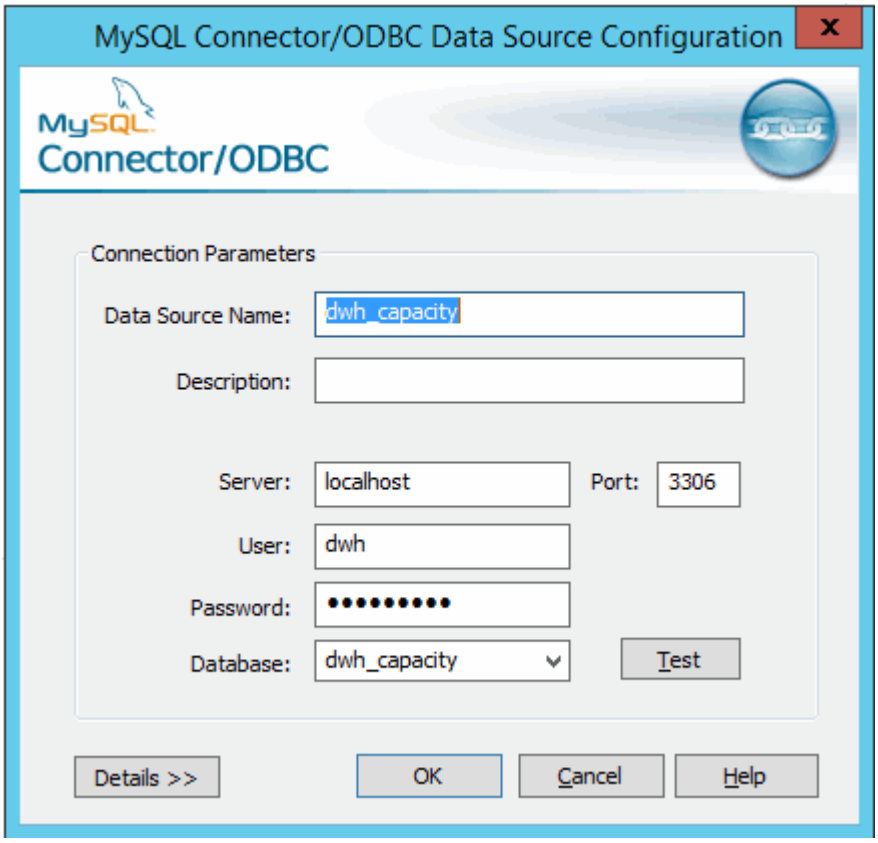
3. 시스템 DSN*을 클릭합니다

   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 **DWH**에 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 엔티티 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.

사용자 정의 주석 작성

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

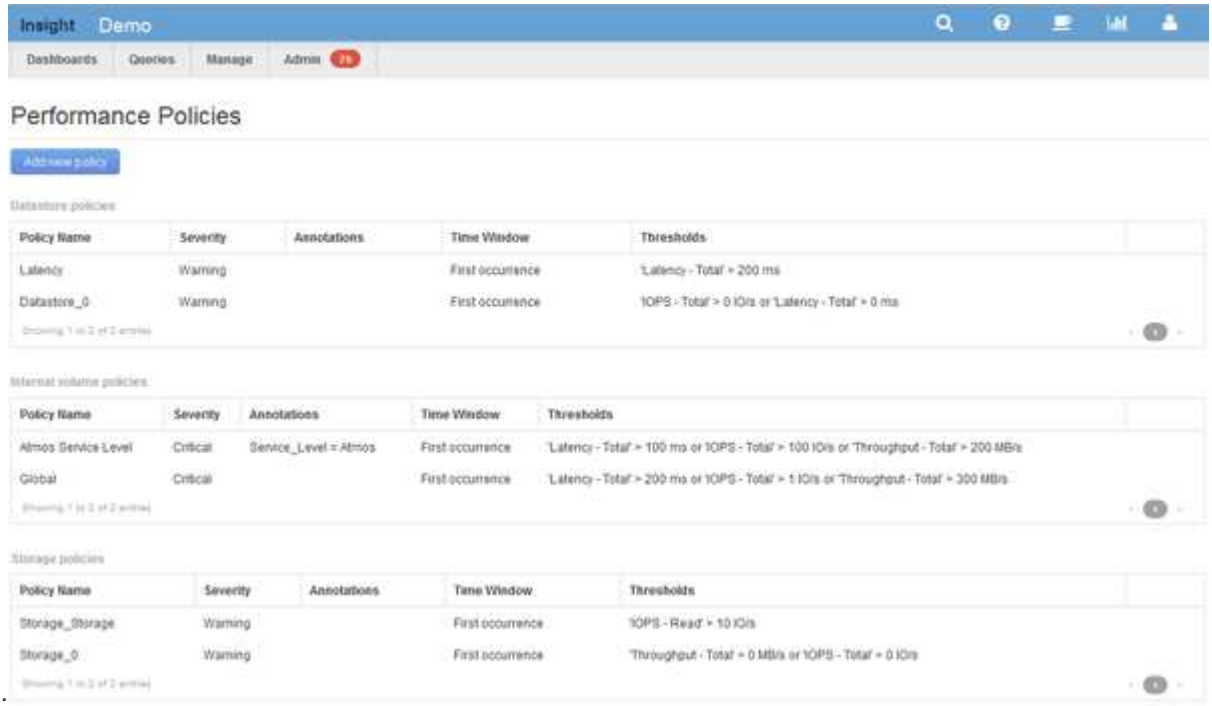
  계층별 지연 시간 및 볼륨 정책 정렬 불량이 있습니다.

성능 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

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.

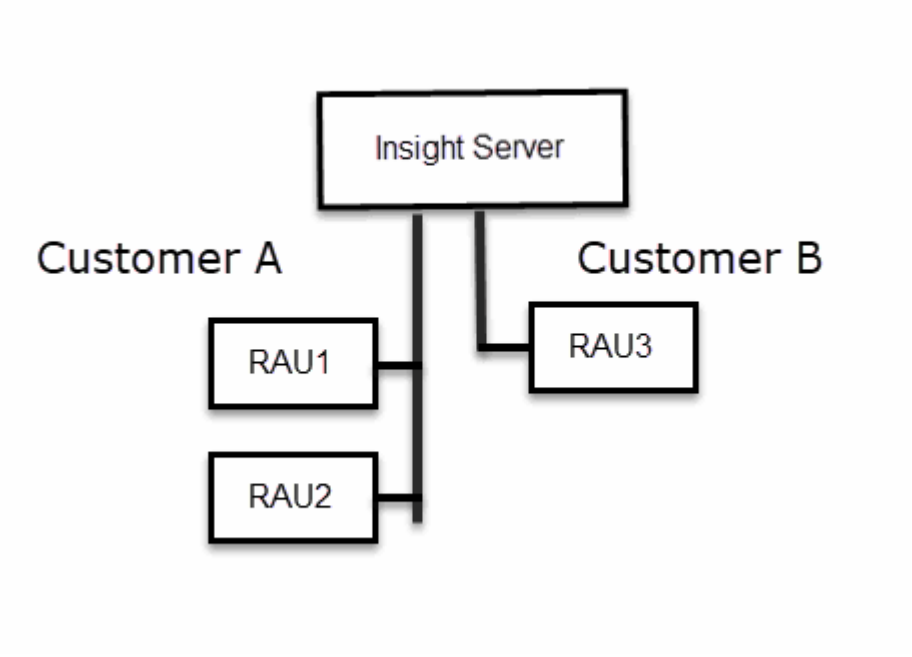
업그레이드 및 설치 고려 사항

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

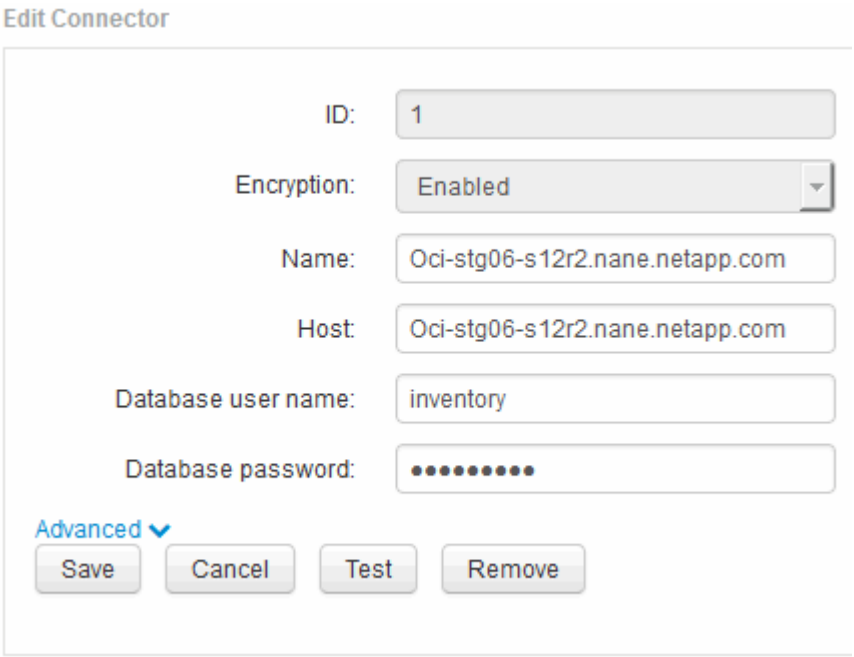
시작하기 전에

이 작업을 수행하려면 관리자로 로그인해야 합니다.

단계

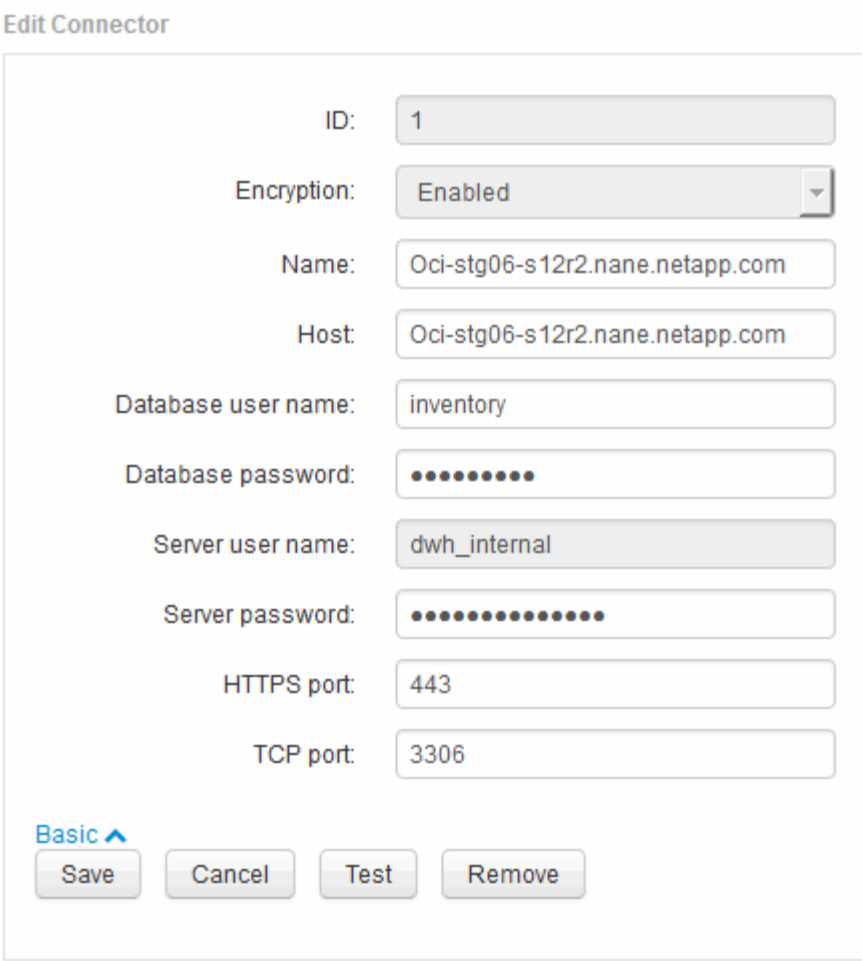
1. 에서 데이터 웨어하우스 포털에 로그인합니다 https://hostname/dwh여기서 hostname 은 OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 커넥터 * 를 클릭합니다.

   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.

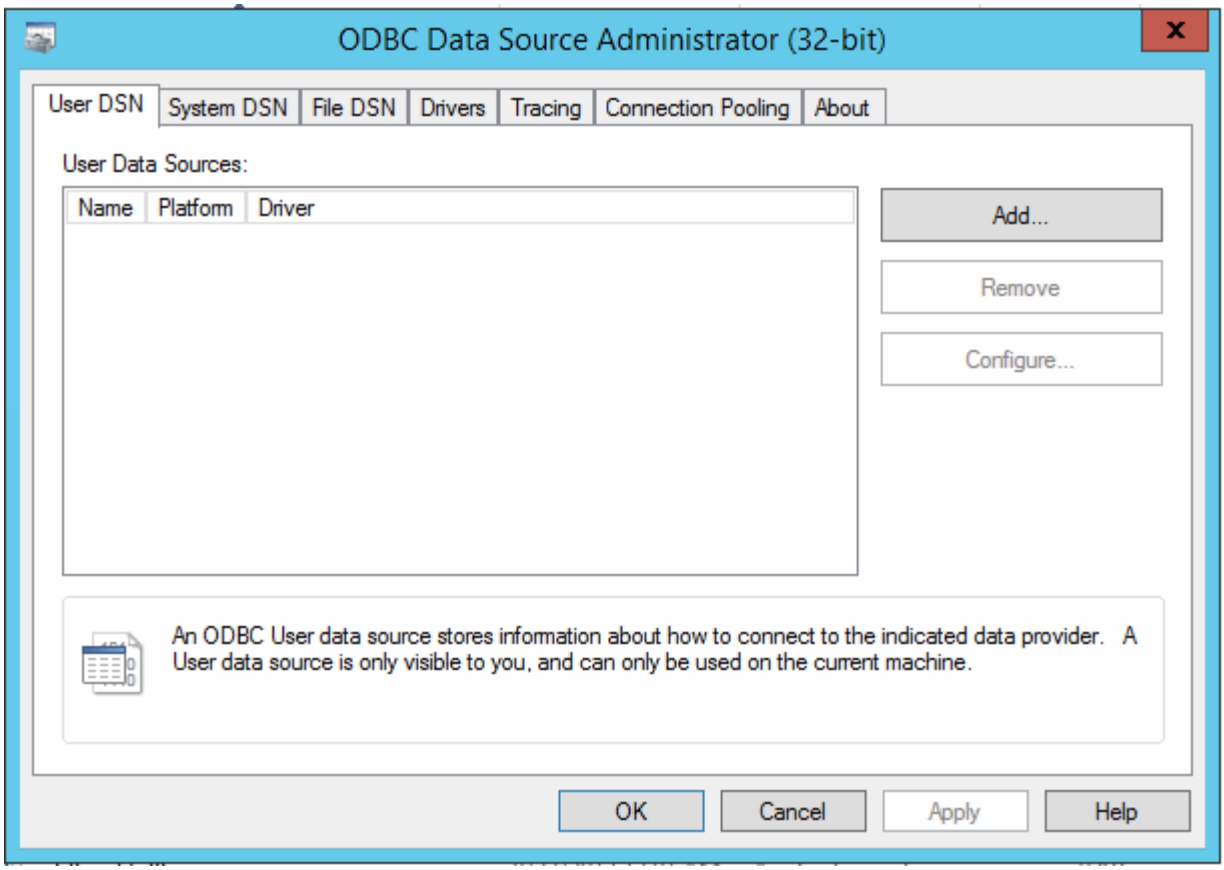
시작하기 전에

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

단계

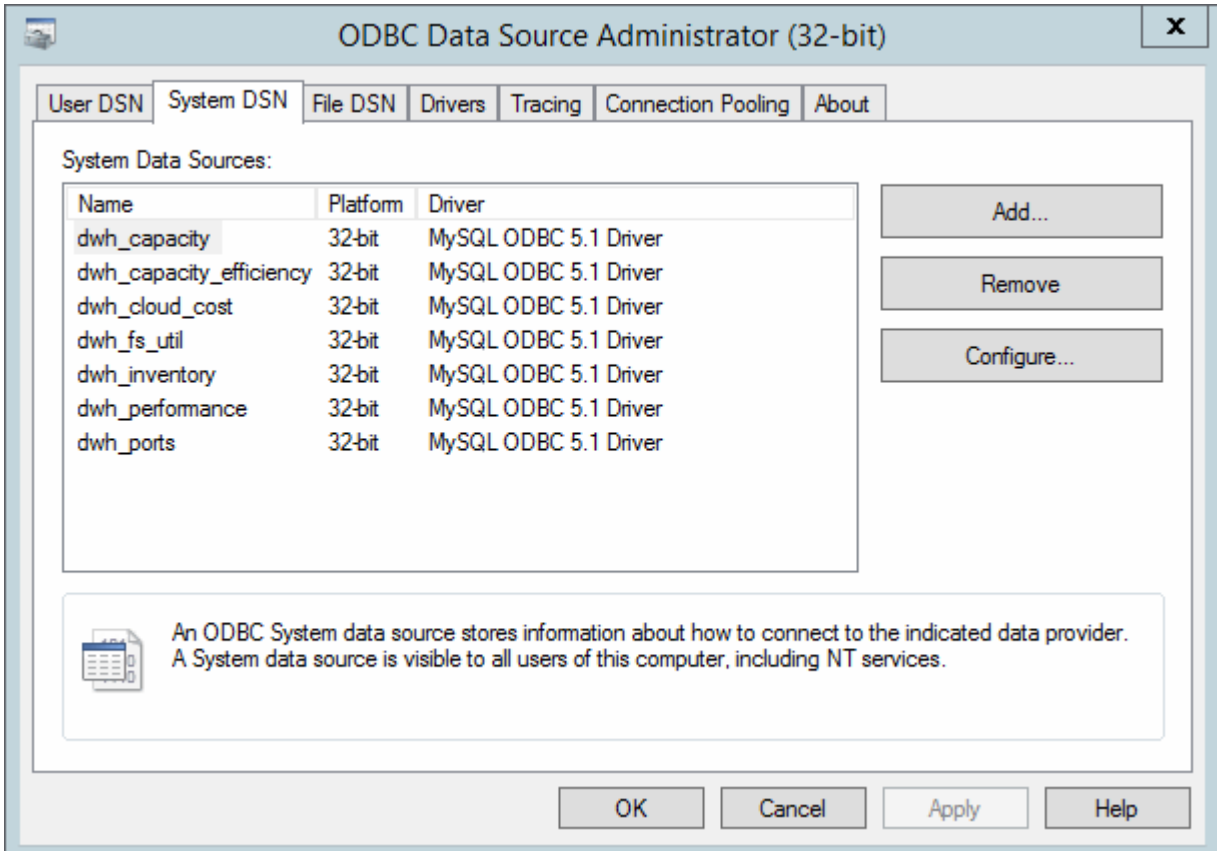
1. 해당 데이터 웨어하우스를 호스팅하는 서버에 원격 로그인을 수행합니다.
2. 에서 ODBC 관리 도구에 액세스합니다 `C:\Windows\SysWOW64\odbcad32.exe`

   ODBC 데이터 원본 관리자 화면이 표시됩니다.



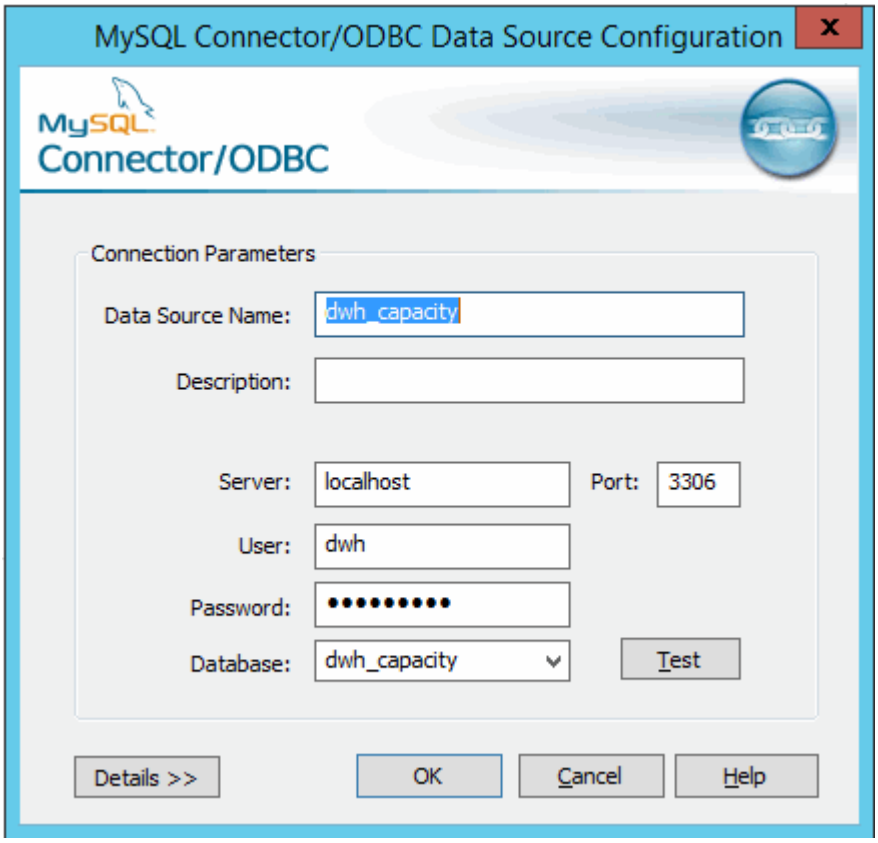
3. 시스템 DSN*을 클릭합니다

   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(인증기관) 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.

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 엔티티 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.

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.

사용자 정의 주석 작성

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.

Insight 데이터 소스 관리

데이터 소스는 OnCommand Insight 환경을 유지 관리하는 데 사용되는 가장 중요한 구성 요소입니다. 이러한 정보가 Insight의 주요 정보원이므로 실행 중인 상태에서 데이터 소스를 유지하는 것이 중요합니다.

데이터 소스를 선택하여 상태와 관련된 이벤트를 확인하고 문제가 발생했을 수 있는 변경 사항을 확인하여 네트워크의 데이터 소스를 모니터링할 수 있습니다.

개별 데이터 소스를 검사하는 것 외에도 다음과 같은 작업을 수행할 수 있습니다.

- 데이터 소스를 복제하여 Insight에서 유사한 여러 데이터 소스를 생성합니다
- 데이터 원본 정보를 편집합니다
- 자격 증명을 변경합니다
- 폴링 제어
- 데이터 원본을 삭제합니다
- 데이터 소스 패치를 설치합니다
- 패치에서 새 데이터 원본을 설치합니다
- NetApp 고객 지원을 위한 오류 보고서 준비

Insight에서 데이터 소스 설정

데이터 소스는 Insight 환경을 유지하려고 할 때 가장 중요한 구성 요소입니다. 데이터 소스는 분석 및 검증에 사용되는 네트워크 정보를 검색합니다. Insight 내에서 데이터 소스를 구성하여 네트워크 내에서 모니터링할 수 있어야 합니다.

각 데이터 소스에 대해 데이터 소스를 정의하는 특정 요구 사항은 해당 디바이스의 공급업체 및 모델에 따라 다릅니다. 데이터 소스를 추가하기 전에 모든 장치에 대한 네트워크 주소, 계정 정보 및 암호가 필요하며, 이러한 추가 세부 정보는 다음과 같습니다.

- 스위치
- 장치 관리 스테이션

- IP 접속이 가능한 스토리지 시스템
- 스토리지 관리 스테이션
- IP 연결이 없는 스토리지 디바이스에 대해 관리 소프트웨어를 실행하는 호스트 서버입니다

데이터 소스 정의에 대한 자세한 내용은 이 섹션의 "공급업체별 데이터 소스 참조" 정보를 참조하십시오.

데이터 소스 지원 정보

구성 계획의 일환으로 Insight에서 사용자 환경의 장치를 모니터링할 수 있는지 확인해야 합니다. 이렇게 하려면 데이터 소스 지원 매트릭스에서 운영 체제, 특정 장치 및 프로토콜에 대한 자세한 내용을 확인할 수 있습니다. 일부 데이터 소스는 일부 운영 체제에서 사용하지 못할 수 있습니다.

데이터 소스 지원 매트릭스의 최신 버전 위치

OnCommand Insight 데이터 소스 지원 매트릭스는 각 서비스 팩 릴리스에 따라 업데이트됩니다. 문서의 최신 버전은 에서 찾을 수 있습니다 "NetApp Support 사이트". .

데이터 소스 추가

데이터 원본 추가 대화 상자를 사용하여 데이터 원본을 빠르게 추가할 수 있습니다.

단계

1. 브라우저에서 OnCommand Insight를 열고 관리자 권한이 있는 사용자로 로그인합니다.
2. Admin * 을 선택하고 * Data Sources * 를 선택합니다.
3. 추가 * 버튼을 클릭합니다.

   데이터 소스 추가 마법사가 열립니다.

4. 설정 * 섹션에서 다음 정보를 입력합니다.

필드에 입력합니다	설명
이름	이 데이터 원본의 고유한 네트워크 이름을 입력합니다. 참고: 데이터 소스 이름에는 문자, 숫자 및 밑줄(_) 문자만 사용할 수 있습니다.
공급업체	드롭다운에서 데이터 소스의 공급업체를 선택합니다.
모델	드롭다운에서 데이터 원본의 모델을 선택합니다.
실행 위치	로컬 을 선택하거나 환경에 RAU가 구성되어 있는 경우 원격 획득 장치를 선택할 수 있습니다.

수집 대상	대부분의 데이터 원본의 경우 이러한 옵션은 인벤토리 및 성능 입니다. 재고는 항상 기본적으로 선택되며 선택 취소할 수 없습니다. 일부 데이터 원본의 경우 옵션이 다를 수 있습니다. 선택한 컬렉션 옵션은 구성 및 고급 구성 섹션에서 사용 가능한 필드를 변경합니다.

5. Configuration* 링크를 클릭하고 선택한 데이터 수집 유형을 사용하여 데이터 원본에 필요한 기본 설정 정보를 입력합니다.
6. 이러한 유형의 데이터 소스를 네트워크에 설정하기 위해 일반적으로 더 자세한 정보가 필요한 경우 * 고급 구성 * 링크를 클릭하여 추가 정보를 입력합니다.
7. 특정 데이터 소스에 필요하거나 사용할 수 있는 구성 또는 고급 구성 정보에 대한 자세한 내용은 를 참조하십시오 "공급업체별 데이터 소스 참조".
8. 데이터 소스가 올바르게 구성되었는지 확인하려면 * Test *(테스트 *) 링크를 클릭합니다.
9. 저장 * 을 클릭합니다.

스프레드시트에서 데이터 원본을 가져옵니다

스프레드시트에서 여러 데이터 원본을 OnCommand Insight로 가져올 수 있습니다. 이 기능은 검색 장치를 스프레드시트에 이미 유지 관리하는 경우에 유용할 수 있습니다. 이 프로세스는 새 데이터 원본을 추가하지만 기존 데이터 원본을 업데이트하는 데 사용할 수는 없습니다.

이 작업에 대해

OnCommand Insight에는 데이터 원본을 만드는 데 도움이 되는 스프레드시트가 포함되어 있습니다. 이 스프레드시트에는 다음과 같은 속성이 있습니다.

- 스프레드시트는 Microsoft Excel 2003 이상에서 사용할 수 있습니다.
- 각 탭에는 데이터 소스 유형(예: Brocade SSH/CLI)이 하나씩 있습니다.
- 각 행은 만들 새 데이터 소스의 인스턴스를 나타냅니다.

스프레드시트에는 OnCommand Insight에서 새 데이터 원본을 만드는 매크로가 포함되어 있습니다.

단계

1. 에서 스프레드시트를 찾습니다 `<install_directory>/SANscreen/acq/bin/acqcli/SiteSurvey_DataSourceImporter_w_Macro.zip`.
2. 스프레드시트에서 색이 있는 셀에 데이터 원본 정보를 입력합니다.
3. 빈 행을 삭제합니다.
4. 스프레드시트에서 을 실행합니다 `CreateDataSources` 데이터 원본을 만드는 매크로
5. 자격 증명을 묻는 메시지가 나타나면 OnCommand Insight 서버 관리 사용자 이름과 암호를 입력합니다.

   결과는 획득 로그에 기록됩니다.

6. 현재 매크로를 실행 중인 컴퓨터에 OnCommand Insight가 설치되어 있는지 묻는 메시지가 나타납니다.

다음 중 하나를 선택합니다.

- 아니요: OnCommand Insight 시스템에서 실행해야 하는 배치 파일을 만들 경우 "아니요"를 선택합니다. 설치 디렉토리에서 이 배치 파일을 실행합니다.
- 예: OnCommand Insight가 이미 설치되어 있고 데이터 소스 정보를 생성하는 데 추가 단계가 필요하지 않은 경우 "예"를 선택합니다.

7. 데이터 소스가 추가되었는지 확인하려면 브라우저에서 Insight를 엽니다.
8. Insight 도구 모음에서 * Admin * 을 클릭합니다.
9. 가져온 데이터 원본에 대한 데이터 원본 목록을 확인합니다.

패치를 사용하여 새 데이터 원본을 추가합니다

새 데이터 소스는 패치 프로세스를 사용하여 시스템에 로드할 수 있는 패치 파일로 릴리스됩니다. 이 프로세스를 통해 예약된 OnCommand Insight 릴리스 간에 새 데이터 소스를 사용할 수 있습니다.

시작하기 전에

설치할 패치 파일을 업로드해야 합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 패치 * 를 선택합니다.
3. Actions * > * Install service pack or patch * 를 선택합니다.
4. 서비스 팩 또는 패치* 설치 대화 상자에서 * 찾아보기 * 를 클릭하여 업로드한 패치 파일을 찾아 선택합니다.
5. 패치 요약 * 대화 상자에서 * 다음 * 을 클릭합니다.
6. 추가 정보 * 를 검토하고 계속하려면 * 다음 * 을 클릭합니다.
7. 설치 * 대화 상자에서 * 마침 * 을 클릭합니다.

데이터 소스 클론 생성

클론 기능을 사용하면 다른 데이터 소스와 동일한 자격 증명 및 속성을 가진 데이터 소스를 빠르게 추가할 수 있습니다. 클론 생성 기능을 사용하면 동일한 디바이스 유형의 여러 인스턴스를 쉽게 구성할 수 있습니다.

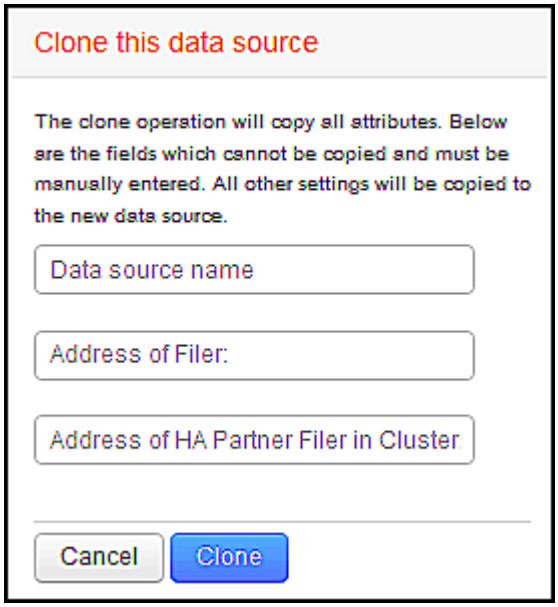
단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.

   데이터 소스 목록이 열립니다.

2. 새 데이터 원본에 사용할 설정 정보가 있는 데이터 원본을 강조 표시합니다.
3. 강조 표시된 데이터 소스의 오른쪽에 있는 * Clone * 아이콘을 클릭합니다.

이 데이터 소스 클론 복제 대화 상자에는 NetApp 데이터 소스에 대해 다음 예와 같이 선택한 데이터 소스에 대해 제공해야 하는 정보가 표시됩니다.



4. 필드에 필수 정보를 입력합니다. 이러한 세부 정보는 기존 데이터 원본에서 복사할 수 없습니다.
5. 클론 * 을 클릭합니다.

결과

클론 작업은 다른 모든 속성 및 설정을 복제하여 새 데이터 소스를 생성합니다.

데이터 소스 구성을 테스트하는 중입니다

데이터 소스를 추가할 때 해당 데이터 소스를 저장하거나 업데이트하기 전에 장치와 통신하도록 구성이 올바른지 확인할 수 있습니다.

데이터 소스 마법사에서 * Test * 버튼을 클릭하면 지정된 장치와의 통신이 선택됩니다. 테스트에서 다음 결과 중 하나가 생성됩니다.

- Passed(통과): 데이터 소스가 올바르게 구성되었습니다.
- 경고: 처리 중 시간 초과나 획득 실행 중이 아닌 경우 테스트가 완료되지 않았습니다.
- 실패: 구성된 데이터 소스가 지정된 장치와 통신할 수 없습니다. 구성 설정을 확인하고 다시 테스트하십시오.

공급업체별 데이터 소스 참조

구성 세부 정보는 추가되는 데이터 소스의 공급업체 및 모델에 따라 달라집니다.

공급업체의 데이터 원본에 특별한 요구 사항 및 특정 명령과 같은 고급 Insight 구성 지침이 필요한 경우 이 정보가 이 섹션에 포함됩니다.

3PAR InServ 데이터 소스

OnCommand Insight는 3PAR InServ(펌웨어 2.2.2+, SSH) 데이터 소스를 사용하여 HP

3PAR StoreServ 스토리지 어레이의 인벤토리를 검색합니다.

용어

OnCommand Insight는 3PAR InServ 데이터 소스에서 다음과 같은 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
물리 디스크	디스크
스토리지 시스템	스토리지
컨트롤러 노드	스토리지 노드
공통 프로비저닝 그룹	스토리지 풀
가상 볼륨	볼륨

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- InServ 클러스터의 IP 주소 또는 FQDN입니다
- 인벤토리의 경우 InServ 서버에 대한 읽기 전용 사용자 이름 및 암호입니다.
- 성능을 위해 InServ 서버에 대한 읽기-쓰기 사용자 이름 및 암호.
- 포트 요구 사항: 22(인벤토리 수집), 5988 또는 5989(성능 수집) [참고: 3PAR 성능은 InServ OS 3.x+에서 지원됩니다.]
- 성능 수집을 위해 SSH를 통해 3PAR 스토리지에 로그인하여 SMI-S가 활성화되었는지 확인합니다.

구성

필드에 입력합니다	설명
클러스터 IP	InServ 클러스터의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	InServ 서버의 사용자 이름입니다
암호	InServ 서버에 사용되는 암호입니다
SMI-S 호스트 IP입니다	SMI-S Provider 호스트의 IP 주소입니다

SMI-S 사용자 이름	SMI-S Provider 호스트의 사용자 이름입니다
SMI-S 암호	SMI-S Provider 호스트에 사용되는 암호입니다

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)
장치 제외	제외할 장치 IP의 쉼표로 구분된 목록입니다
SSH 프로세스 대기 시간 초과(초)	SSH 프로세스 시간 초과(기본값 60초)
SSH 재시도 횟수	SSH 재시도 횟수입니다
SSH 배너 대기 시간 제한(초)	SSH 배너 대기 시간 초과(기본값 20초)
SMI-S 포트	SMI-S Provider 호스트에서 사용하는 포트입니다
프로토콜	SMI-S 공급자에 연결하는 데 사용되는 프로토콜입니다
SMI-S 네임스페이스	SMI-S 네임스페이스
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
SMI-S 연결 재시도 횟수	SMI-S 연결 재시도 횟수입니다

Amazon AWS EC2 데이터 소스

OnCommand Insight은 이 데이터 소스를 사용하여 Amazon AWS EC2의 인벤토리 및 성능을 검색합니다.

전제 조건:

Amazon EC2 장치에서 데이터를 수집하려면 다음 정보가 있어야 합니다.

- IAM 액세스 키 ID가 있어야 합니다
- Amazon EC2 클라우드 계정에 대한 비밀 액세스 키가 있어야 합니다
- "조직 목록" 권한이 있어야 합니다
- 포트 433 HTTPS
- EC2 인스턴스는 가상 머신 또는 (비교적 자연스럽게) 호스트로 보고할 수 있습니다. EBS 볼륨은 VM에서 사용하는 가상 디스크와 가상 디스크의 용량을 제공하는 데이터 저장소로 보고될 수 있습니다.

액세스 키는 액세스 키 ID(예: AKIAIOSFODN7EXAMPLE)와 비밀 액세스 키(예: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY)로 구성됩니다. 액세스 키를 사용하여 Amandzon EC2 SDK, REST 또는 쿼리 API 작업을 사용하는 경우 EC@에 만드는 프로그래밍 방식 요청에 서명할 수 있습니다. 이러한 키는 아마존에서 귀하의 계약과 함께 제공됩니다.

이 데이터 소스를 구성하는 방법

Amazon AWS EC2 데이터 소스를 구성하려면 AWS 계정에 대한 AWS IAM 액세스 키 ID와 비밀 액세스 키가 필요합니다.

아래 표에 따라 데이터 원본 필드를 채웁니다.

구성:

필드에 입력합니다	설명
AWS 지역	AWS 지역을 선택하십시오
IAM 역할	AWS의 AU에서 획득한 경우에만 사용합니다. IAM 역할에 대한 자세한 내용은 아래를 참조하십시오.
AWS IAM 액세스 키 ID	AWS IAM 액세스 키 ID를 입력합니다. IAM Role을 사용하지 않는 경우 필수입니다.
AWS IAM 비밀 액세스 키	AWS IAM 비밀 액세스 키를 입력합니다. IAM Role을 사용하지 않는 경우 필수입니다.
저는 AWS가 API 요청에 대해 청구하는 것을 알고 있습니다	이 확인란을 선택하여 AWS에서 Insight 폴링으로 인한 API 요청 비용을 청구하는지 확인하십시오

고급 구성:

필드에 입력합니다	설명
추가 지역 포함	폴링에 포함할 추가 영역을 지정합니다.
교차 계정 역할	서로 다른 AWS 계정의 리소스에 액세스하는 역할입니다.
재고 폴링 간격(분)	재고 조사 간격(기본값: 60분)
HTTP 연결 및 소켓 시간 제한(초)	HTTP 연결 시간 초과(기본값 300초)
AWS 태그 포함	Insight 주석에서 AWS 태그에 대한 지원을 활성화하려면 이 확인란을 선택합니다
성능 폴링 간격(초)	성능 폴링 간격(기본값: 1800초)

AWS 태그를 Insight 주석에 매핑

AWS EC2 데이터 원본에는 AWS에 구성된 태그로 Insight 주석을 채울 수 있는 옵션이 포함되어 있습니다. 주석 이름은 AWS 태그와 정확히 일치해야 합니다. Insight는 항상 같은 이름의 텍스트 유형 주석을 채우고 다른 유형의 주석(숫자, 부울 등)을 채우기 위한 "최선의 시도"를 만듭니다. 주석이 다른 유형이고 데이터 소스가 주석을 채우지 못할 경우 주석을 제거하고 텍스트 유형으로 다시 생성해야 할 수 있습니다.

AWS는 대/소문자를 구분하며 Insight는 대/소문자를 구분합니다. 따라서 Insight에서 "소유자"라는 주석을 만들고 AWS에서 "소유자", "소유자", "소유자", "소유자"라는 태그를 만들면 "소유자"의 모든 AWS 변형이 Insight의 "소유자" 주석에 매핑됩니다.

관련 정보:

"IAM 사용자를 위한 액세스 키 관리"

추가 지역 포함

AWS Data Collector * 고급 구성 * 섹션에서 추가 영역을 포함하도록 * 추가 영역 포함 * 필드를 쉼표 또는 세미콜론으로 구분하여 설정할 수 있습니다. 기본적으로 이 필드는 모든 미국 AWS 지역에서 수집하는 *_us-. * _ * 로 설정됩니다. on_all_regions를 수집하려면 이 필드를 * _. * _ * 로 설정합니다.

추가 영역 포함 * 필드가 비어 있으면 * 구성 * 섹션에 지정된 * AWS 지역 * 필드에 지정된 자산에 대한 데이터 수집기가 수집됩니다.

* AWS 하위 계정에서 수집 *

Insight는 단일 AWS 데이터 수집기 내에서 AWS의 하위 계정 수집을 지원합니다. 이 컬렉션에 대한 구성은 AWS 환경에서 수행됩니다.

- 운영 계정 ID가 하위 계정에서 EC2 세부 정보에 액세스할 수 있도록 각 하위 계정에 AWS 역할을 구성해야 합니다.
- 각 하위 계정에는 동일한 문자열로 구성된 역할 이름이 있어야 합니다
- 이 역할 이름 문자열을 * 교차 계정 역할 * 필드의 Insight AWS Data Collector * 고급 구성 * 섹션에 입력합니다.

모범 사례: AWS 사전 정의된 AmazonEC2ReadOnlyAccess 정책을 ECS 기본 계정에 할당하는 것이 좋습니다. 또한 데이터 소스에서 구성된 사용자는 AWS를 쿼리하기 위해 미리 정의된 *AWSOrganizationReadOnlyAccess* 정책이 할당되어 있어야 합니다.

Insight를 AWS 하위 계정에서 수집할 수 있도록 환경을 구성하는 방법은 다음을 참조하십시오.

"자습서: IAM 역할을 사용하여 AWS 계정 전체에서 대리인 액세스"

"AWS 설정: 사용자가 소유한 다른 AWS 계정에서 IAM 사용자에 대한 액세스 제공"

"IAM 사용자에 대한 권한을 위임하기 위한 역할 생성"

IAM 역할

IAM Role_security를 사용할 때는 생성하거나 지정하는 역할에 리소스에 액세스하는 데 필요한 적절한 권한이 있는지 확인해야 합니다.

예를 들어, 이름이 _InstanceE2ReadOnly_인 IAM 역할을 생성하는 경우 이 IAM 역할에 대한 모든 EC2 리소스에 EC2 읽기 전용 목록 액세스 권한을 부여하도록 정책을 설정해야 합니다. 또한 이 역할이 계정 간에 역할을 수행할 수

있도록 STS(보안 토큰 서비스) 액세스를 부여해야 합니다.

IAM 역할을 생성한 후 새 EC2 인스턴스 또는 기존 EC2 인스턴스를 생성할 때 연결할 수 있습니다.

IAM role_InstanceE2ReadOnly_를 EC2 인스턴스에 연결하면 IAM 역할 이름으로 인스턴스 메타데이터를 통해 임시 자격 증명을 검색하고 이 EC2 인스턴스에서 실행되는 모든 애플리케이션에서 이 자격 증명을 사용하여 AWS 리소스에 액세스할 수 있습니다.

> IAM 역할은 획득 장치가 AWS 인스턴스에서 실행 중인 경우에만 사용할 수 있습니다.

Brocade Enterprise Fabric Connectivity Manager 데이터 소스

OnCommand Insight는 Brocade EFCM(Enterprise Fabric Connectivity Manager) 데이터 소스를 사용하여 Brocade EFCM 스위치의 인벤토리를 검색합니다. Insight는 EFCM 버전 9.5, 9.6 및 9.7을 지원합니다.

요구 사항

> 이 데이터 수집기는 OnCommand Insight 7.3.11부터 사용할 수 없습니다.

- EFCM 서버의 네트워크 주소 또는 정규화된 도메인 이름입니다
- EFCM 버전은 9.5, 9.6 또는 9.7이어야 합니다
- EFCM 서버의 IP 주소입니다
- EFCM 서버에 대한 읽기 전용 사용자 이름 및 암호입니다
- 포트 51512를 통해 읽기 전용 사용자 이름과 암호를 사용하여 Insight 서버에서 텔넷을 통해 Connectrix 스위치에 대한 액세스를 검증했습니다

구성

* 필드 *	* 설명 *
EFC 서버	EFC 서버의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	스위치의 사용자 이름입니다
암호	스위치에 사용되는 암호입니다

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 15분)
패브릭 이름	EFCM 데이터 소스에서 보고할 Fabric 이름입니다. 패브릭 이름을 WWN으로 보고하려면 공백으로 두십시오.

통신 포트	스위치와 통신하는 데 사용되는 포트입니다
트래핑을 활성화합니다	장치에서 SNMP 트랩을 수신할 때 획득을 활성화하려면 선택합니다. 트래핑 활성화를 선택한 경우 SNMP도 활성화해야 합니다.
트랩 사이의 최소 시간(초)	트랩에 의해 트리거된 획득 시도 사이의 최소 시간(기본값 15초)
비활성 Zoneset	활성 영역 세트에서 획득을 수행할 뿐만 아니라 획득을 수행할 비활성 Zoneset의 쉼표로 구분된 목록입니다
사용할 NIC입니다	SAN 디바이스에서 보고할 때 RAU에서 사용해야 하는 네트워크 인터페이스를 지정합니다
장치 제외	폴링에서 포함하거나 제외할 단위 이름의 쉼표로 구분된 목록입니다
EFCM 스위치 별칭을 Insight 스위치 이름으로 사용합니다	EFCM 스위치 별칭을 Insight 스위치 이름으로 사용하려면 선택합니다
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

Brocade FC 스위치 데이터 소스

OnCommand Insight는 Brocade FC 스위치(SSH) 데이터 소스를 사용하여 계수 운영 체제(FOS) 펌웨어 4.2 이상을 실행하는 Brocade 또는 재브랜딩 스위치 디바이스의 인벤토리를 검색합니다. FC 스위치와 액세스 게이트웨이 모드의 디바이스가 모두 지원됩니다.

용어

OnCommand Insight는 Brocade FC 스위치 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
스위치	스위치
포트	포트
가상 패브릭, 물리적 패브릭	패브릭
Zone(영역)	Zone(영역)

논리 스위치	논리 스위치
LSAN 구역	IVR 영역

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 획득 장치(로컬 또는 원격)는 Brocade 스위치의 TCP 포트 22에 대한 연결을 시작하여 인벤토리 데이터를 수집합니다. 또한 AU는 성능 데이터 수집을 위해 UDP 포트 161에 대한 연결을 시작합니다.
- Fabric의 모든 스위치에 대한 IP 연결이 있어야 합니다. Fabric에서 모든 스위치 검색 확인란을 선택하면 OCI가 Fabric의 모든 스위치를 식별하지만, 추가 스위치를 검색하려면 해당 스위치에 대한 IP 연결이 필요합니다.
- Fabric의 모든 스위치에서 동일한 계정이 전 세계적으로 필요합니다. PuTTY(오픈 소스 터미널 에뮬레이터)를 사용하여 액세스를 확인할 수 있습니다.
- Perform 라이센스가 설치된 경우 SNMP 성능 폴링을 위해 Fabric의 모든 스위치에 대해 포트 161과 162가 열려 있어야 합니다.
- SNMP 읽기 전용 커뮤니티 문자열

구성

필드에 입력합니다	설명
스위치 IP	스위치의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	스위치의 사용자 이름입니다
암호	스위치에 사용되는 암호입니다
SNMP 버전	SNMP 버전입니다
SNMP 커뮤니티 문자열	스위치에 액세스하는 데 사용되는 SNMP 읽기 전용 커뮤니티 문자열입니다
SNMP 사용자 이름입니다	SNMP 버전 프로토콜 사용자 이름(SNMP v3에만 적용)
SNMP 암호	SNMP 버전 프로토콜 암호(SNMP v3에만 적용)

고급 구성

필드에 입력합니다	설명
패브릭 이름	데이터 소스에서 보고할 Fabric 이름입니다. 패브릭 이름을 WWN으로 보고하려면 공백으로 두십시오.

장치 제외	폴링에서 제외할 장치 ID의 쉼표로 구분된 목록입니다
재고 폴링 간격(분)	재고 조사 간격(기본값 15분)
시간 초과(초)	연결 시간 초과(기본값 30초)
배너 대기 제한 시간(초)	SSH 배너 대기 시간 초과(기본값 5초)
관리자 도메인이 활성화되었습니다	관리자 도메인을 사용하는 경우 선택합니다
MPR 데이터 검색	다중 프로토콜 라우터(MPR)에서 라우팅 데이터를 가져오려면 선택합니다.
트래핑을 활성화합니다	장치에서 SNMP 트랩을 수신할 때 획득을 활성화하려면 선택합니다. 트래핑 활성화를 선택한 경우 SNMP도 활성화해야 합니다.
트랩 사이의 최소 시간(초)	트랩에 의해 트리거된 획득 시도 사이의 최소 시간(기본값 10초)
패브릭의 모든 스위치를 살펴보십시오	Fabric의 모든 스위치를 검색하려면 선택합니다
HBA와 을 선택합니다 영역 별칭	HBA 또는 영역 별칭을 사용할지 여부를 선택합니다
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
SNMP 인증 프로토콜	SNMP 인증 프로토콜(SNMP v3만 해당)
SNMP 개인 정보 보호 프로토콜	SNMP 개인 정보 보호 프로토콜(SNMP v3만 해당)
SNMP 개인 정보 보호 암호	SNMP 개인 정보 보호 암호(SNMP v3만 해당)
SNMP 재시도	SNMP 재시도 횟수입니다
SNMP 시간 초과(ms)	SNMP 시간 초과(기본값 5,000ms)

Brocade Sphereon/Intrepid 스위치 데이터 소스

OnCommand Insight는 Brocade Sphereon/Intrepid 스위치(SNMP) 데이터 소스를 사용하여 Brocade Sphereon 또는 Intrepid 스위치의 인벤토리를 검색합니다.

요구 사항

이 데이터 수집기는 OnCommand Insight 7.3.11부터 사용할 수 없습니다.

- Fabric의 모든 스위치에 대한 IP 연결이 있어야 합니다. Fabric에서 모든 스위치 검색 확인란을 선택하면 OCI가 Fabric의 모든 스위치를 식별하지만, 추가 스위치를 검색하려면 해당 스위치에 대한 IP 연결이 필요합니다.
- SNMP V1 또는 SNMP V2를 사용하는 경우 읽기 전용 커뮤니티 문자열입니다.
- 조닝 정보를 얻기 위해 스위치에 대한 HTTP 액세스.
- 를 실행하여 액세스 검증을 수행합니다 `snmpwalk` 스위치에 대한 유틸리티(참조 `<install_path\>\bin\)`.

구성

* 필드 *	* 설명 *
Sphereon 스위치	스위치의 IP 주소 또는 정규화된 도메인 이름입니다
SNMP 버전	SNMP 버전입니다
SNMP 커뮤니티	스위치에 액세스하는 데 사용되는 SNMP 읽기 전용 커뮤니티 문자열입니다
사용자 이름	스위치에 대한 SMI-S 사용자 이름(SNMP v3만 해당)
암호	스위치에 대한 SMI-S 암호(SNMP v3만 해당)

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 15분)
SNMP 인증 프로토콜	SNMP 인증 프로토콜(SNMPv3만 해당)
SNMP 개인 정보 보호 프로토콜	SNMP 개인 정보 보호 프로토콜(SNMPv3만 해당)
SNMP 개인 정보 보호 암호	SNMP 개인 정보 보호 암호입니다
SNMP 재시도 횟수	SNMP 재시도 횟수입니다
SNMP 시간 초과(ms)	SNMP 시간 초과(기본값 5,000ms)
패브릭 이름	데이터 소스에서 보고할 Fabric 이름입니다. 패브릭 이름을 WWN으로 보고하려면 공백으로 두십시오.
트래핑을 활성화합니다	장치에서 SNMP 트랩을 수신할 때 획득을 활성화하려면 선택합니다. 트래핑 활성화를 선택한 경우 SNMP도 활성화해야 합니다.

Ttrap(Ttrap) 사이의 최소 시간(초)	트랩에 의해 트리거된 획득 시도 사이의 최소 시간(기본값 10초)
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

Cisco FC 스위치 펌웨어**(SNMP)** 데이터 소스

OnCommand Insight는 Cisco FC 스위치 펌웨어 2.0+(SNMP) 데이터 소스를 사용하여 Cisco MDS 파이버 채널 스위치에 대한 인벤토리 및 FC 서비스가 사용되는 다양한 Cisco Nexus FCoE 스위치를 검색합니다. 또한 이 데이터 소스를 통해 NPV 모드에서 실행되는 여러 Cisco 장치 모델을 발견할 수 있습니다.

용어

OnCommand Insight는 Cisco FC 스위치 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
스위치	스위치
포트	포트
vSAN을 선택합니다	패브릭
Zone(영역)	Zone(영역)
논리 스위치	논리 스위치
이름 서버 항목	이름 서버 항목
IVR(Inter-VSAN Routing) 존	IVR 영역

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 패브릭 또는 개별 스위치에 있는 스위치 중 하나의 IP 주소입니다
- 섀시 검색, 패브릭 검색 지원
- SNMP V2를 사용하는 경우 읽기 전용 커뮤니티 문자열입니다
- 포트 161은 장치에 액세스하는 데 사용됩니다
- 를 사용하여 유효성 검사에 액세스합니다 `snmpwalk` 스위치에 대한 유틸리티(참조 `<install_path\>\bin\`)

구성

필드에 입력합니다	설명
Cisco 스위치 IP	스위치의 IP 주소 또는 정규화된 도메인 이름입니다
SNMP 버전	성능 획득을 위해서는 SNMP 버전 v2 이상이 필요합니다
SNMP 커뮤니티 문자열	스위치에 액세스하는 데 사용되는 SNMP 읽기 전용 커뮤니티 문자열(SNMP v3에는 적용되지 않음)
사용자 이름	스위치의 사용자 이름(SNMP v3만 해당)
암호	스위치에 사용된 암호(SNMPv3만 해당)

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)
SNMP 인증 프로토콜	SNMP 인증 프로토콜(SNMPv3만 해당)
SNMP 개인 정보 보호 프로토콜	SNMP 개인 정보 보호 프로토콜(SNMPv3만 해당)
SNMP 개인 정보 보호 암호	SNMP 개인 정보 보호 암호입니다
SNMP 재시도	SNMP 재시도 횟수입니다
SNMP 시간 초과(ms)	SNMP 시간 초과(기본값 5,000ms)
트래핑을 활성화합니다	트래핑을 활성화하려면 선택합니다. 트래핑을 사용하는 경우 SNMP 알림도 활성화해야 합니다.
트랩 사이의 최소 시간(초)	트랩에 의해 트리거된 획득 시도 사이의 최소 시간(기본값 10초)
모든 패브릭 스위치를 살펴보십시오	Fabric의 모든 스위치를 검색하려면 선택합니다
장치 제외	폴링에서 제외할 장치 IP의 쉼표로 구분된 목록입니다
장치 포함	폴링에 포함할 장치 IP의 쉼표로 구분된 목록입니다
장치 유형을 확인하십시오	자신을 Cisco 장치로 명시적으로 광고하는 장치만 수락하려면 선택합니다

기본 별칭 유형	별칭 해상도에 대한 첫 번째 기본 설정을 제공합니다. 다음 중에서 선택합니다. • * 장치 별칭 * 이 이름은 필요에 따라 모든 구성 명령에 사용할 수 있는 포트 WWN(pwwn)에 대한 사용자 친화적인 이름입니다. Cisco MDS 9000 제품군의 모든 스위치는 분산 장치 별칭(장치 별칭)을 지원합니다. • * 없음 * 별칭을 보고하지 않습니다 • * 포트 설명 * 포트 목록에서 포트를 식별하는 데 도움이 되는 설명입니다 • * 영역 별칭(모두) * 조닝 구성에만 사용할 수 있는 포트에 대한 알기 쉬운 이름입니다 • * 영역 별칭(활성 전용) * 활성 구성에만 사용할 수 있는 포트에 대한 사용자 친화적인 이름입니다. 이것이 기본값입니다.
보조 별칭 유형	별칭 해상도에 대한 두 번째 기본 설정을 제공합니다
제3 별칭 유형	별칭 해상도에 대한 세 번째 기본 설정을 제공합니다
SANTap 프록시 모드 지원을 설정합니다	Cisco 스위치가 프록시 모드에서 SANTap을 사용하고 있는지 여부를 선택합니다. EMC RecoverPoint를 사용하는 경우 SANTap을 사용할 수 있습니다.
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

EMC Celerra 데이터 소스

Celerra(SSH) 데이터 소스는 Celerra 스토리지에서 인벤토리 정보를 수집합니다. 구성의 경우 이 데이터 원본에는 스토리지 프로세서의 IP 주소와 _read-only_user 이름 및 암호가 필요합니다.

용어

OnCommand Insight는 EMC Celerra 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음

용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
Celerra Network Server입니다	스토리지
Celerra 메타 볼륨/Celerra 스토리지 풀	스토리지 풀
파일 시스템	내부 볼륨
Data Mover입니다	컨트롤러
Data Mover에 마운트된 파일 시스템입니다	파일 공유
CIFS 및 NFS 엑스포트	공유
디스크 볼륨	백엔드 LUN

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 스토리지 프로세서의 IP 주소입니다
- 읽기 전용 사용자 이름 및 암호
- SSH 포트 22

구성

필드에 입력합니다	설명
Celerra의 주소입니다	Celerra 디바이스의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	Celerra 디바이스에 로그인하는 데 사용되는 이름입니다
암호	Celerra 디바이스에 로그인하는 데 사용되는 암호입니다

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
SSH 프로세스 대기 시간 초과(초)	SSH 프로세스 시간 초과(기본값 600초)

재시도 횟수	인벤토리 재시도 횟수입니다
SSH 배너 대기 시간 제한(초)	SSH 배너 대기 시간 초과(기본값 20초)

EMC CLARiX(NaviCLI) 데이터 소스

이 데이터 소스를 구성하기 전에 EMC Navisphere CLI가 타겟 디바이스 및 Insight 서버에 설치되어 있는지 확인합니다. Navisphere CLI 버전은 컨트롤러의 펌웨어 버전과 일치해야 합니다. 성능 데이터 수집을 위해 통계 로깅을 설정해야 합니다.

Navisphere 명령줄 인터페이스 구문입니다

```
naviseccli.exe -h <IP address> -user <user> -password <password> -scope
<scope,use 0 for global scope> -port <use 443 by default> command
```

용어

OnCommand Insight는 EMC CLARiX 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
디스크	디스크
스토리지	스토리지
스토리지 프로세서	스토리지 노드
씬 풀, RAID 그룹	스토리지 풀
LUN을 클릭합니다	볼륨

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 각 CLARiX 스토리지 프로세서의 IP 주소입니다
- CLARiX 스토리지에 대한 읽기 전용 Navisphere 사용자 이름 및 암호입니다
- Navicli는 Insight 서버/RAU에 설치해야 합니다
- 액세스 검증: 위의 사용자 이름과 암호를 사용하여 Insight 서버에서 각 어레이로 NaviCLI를 실행합니다.
- Navicli 버전은 스토리지의 최신 FLARE 코드와 일치해야 합니다

- 성능을 위해서는 통계 로깅을 설정해야 합니다.
- 포트 요구 사항: 80, 443

구성

필드에 입력합니다	설명
CLARiX 스토리지	CLARiX 스토리지의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	CLARiX 스토리지 디바이스에 로그인하는 데 사용되는 이름입니다.
암호	CLARiX 스토리지 디바이스에 로그인하는 데 사용되는 암호입니다.
NaviCLI.exe 경로 또는 naviseccli.exe 경로에 대한 CLI 경로	에 대한 전체 경로입니다 `navicli.exe` 또는 `naviseccli.exe` 실행 파일

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)
보안 클라이언트 사용(naviseccli)	보안 클라이언트(navseccli)를 사용하려면 선택합니다.
범위	보안 클라이언트 범위 기본값은 Global 입니다.
CLARiX CLI 포트입니다	CLARiX CLI에 사용되는 포트입니다
재고 외부 프로세스 시간 초과(초)	외부 프로세스 시간 초과(기본값 1800초)
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
성능 외부 프로세스 시간 초과(초)	외부 프로세스 시간 초과(기본값 1800초)

EMC Data Domain 데이터 소스

이 데이터 소스는 EMC Data Domain 데이터 중복 제거 스토리지 시스템에서 스토리지 및 구성 정보를 수집합니다. 데이터 소스를 추가하려면 특정 구성 지침 및 명령을 사용하고 데이터 소스 요구 사항 및 사용 권장 사항을 알고 있어야 합니다.

용어

OnCommand Insight는 EMC Data Domain 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
디스크	디스크
스토리지	스토리지
포트	포트
파일 시스템	내부 볼륨
MTree입니다	qtree를 입력합니다
할당량	할당량
NFS 및 CIFS 공유	파일 공유

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- Data Domain 디바이스의 IP 주소입니다
- Data Domain 스토리지에 대한 읽기 전용 사용자 이름 및 암호
- SSH 포트 22

구성

필드에 입력합니다	설명
IP 주소입니다	Data Domain 스토리지 시스템의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름입니다	Data Domain 스토리지 시스템의 사용자 이름입니다
암호	Data Domain 스토리지 시스템의 암호입니다

고급 구성

필드에 입력합니다	설명

재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
SSH 프로세스 대기 시간 초과(초)	SSH 프로세스 시간 초과(기본값 180초)
SSH 포트	SSH 서비스 포트입니다

EMC ECC StorageScope 데이터 소스

EMC ECC StorageScope 디바이스에는 5.x, 6.0 및 6.1의 세 가지 데이터 소스가 있습니다.

구성

이 데이터 수집기는 OnCommand Insight 7.3.11부터 더 이상 사용할 수 없습니다.

* 필드 *	* 설명 *
ECC 서버	ECC 서버의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	ECC 서버의 사용자 이름입니다
암호	암호 r ECC 서버

고급 구성

* 필드 *	* 설명 *
ECC 포트	ECC 서버에 사용되는 포트입니다
재고 폴링 간격(분)	재고 조사 간격(기본값 30분)
데이터베이스에 연결할 프로토콜입니다	데이터베이스에 연결하는 데 사용되는 프로토콜입니다
파일 시스템 정보를 쿼리합니다	WWN 별칭 및 파일 시스템에 대한 세부 정보를 검색하려면 선택합니다.

Dell EMC ECS 데이터 소스

이 데이터 수집기는 EMC ECS 스토리지 시스템에서 인벤토리 및 성능 데이터를 가져옵니다. 구성을 위해 데이터 수집기는 ECS 서버의 IP 주소와 관리 수준 도메인 계정이 필요합니다.

용어

OnCommand Insight는 EMC ECS 데이터 소스에서 다음과 같은 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
Cluser(사용자)	스토리지
테넌트	스토리지 풀
버킷	내부 볼륨
디스크	디스크

> 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- ECS Management Console의 IP 주소입니다
- ECS 시스템의 관리 수준 도메인 계정입니다
- 포트 443(HTTPS). ECS 시스템에서 TCP 포트 443에 대한 아웃바운드 연결이 필요합니다.
- 성능을 위해 ssh/scp 액세스를 위한 읽기 전용 사용자 이름과 암호를 사용합니다.
- 성능을 위해서는 포트 22가 필요합니다.

구성

필드에 입력합니다	설명
ECS 호스트	ECS 시스템의 IP 주소 또는 정규화된 도메인 이름입니다
ECS 호스트 포트	ECS 호스트와 통신하는 데 사용되는 포트입니다
ECS 공급업체 ID입니다	ECS의 공급업체 ID입니다
암호	ECS에 사용되는 암호입니다

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 360분입니다.

EMC Isilon 데이터 소스

Isilon SSH 데이터 소스는 EMC Isilon 스케일 아웃 NAS 스토리지에서 인벤토리 및 성능을 수집합니다.

용어

OnCommand Insight는 EMC Isilon 데이터 소스에서 다음과 같은 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
드라이브	디스크
클러스터	스토리지
노드	스토리지 노드
파일 시스템	내부 볼륨

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- Isilon 스토리지에 대한 관리자 권한
- 을 사용하여 액세스를 검증했습니다 `telnet` 포트 22로 이동합니다

구성

필드에 입력합니다	설명
IP 주소입니다	Isilon 클러스터의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름입니다	Isilon 클러스터의 사용자 이름입니다
암호	Isilon 클러스터의 암호입니다

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
SSH 프로세스 대기 시간이 초과되었습니다	SSH 프로세스 시간 초과(기본값 60초)
SSH 포트	SSH 서비스 포트입니다

CLI 명령 실행 중

OnCommand Insight 버전 7.3.11 및 서비스 팩 9부터는 EMC Isilon 데이터 소스에 향상된 기능이 포함되어 Insight에서 더 많은 CLI 명령을 실행할 수 있습니다. 데이터 소스 내에서 루트 이외의 사용자를 사용하는 경우 해당 사용자 계정에 SSH를 통해 특정 CLI 명령을 실행할 수 있는 기능을 부여하기 위해 "sudoers" 파일을 구성했을 수 있습니다.

Insight에서 EMC의 "Access Zones" 기능을 이해하기 위해 이제 Insight에서 다음과 같은 새로운 CLI 명령을 추가로 실행합니다.

- `sudo isi zone zones list --format json –verbose`
- `sudo isi zone zones list`

Insight는 이러한 명령의 출력을 구문 분석하고 더 많은 기존 명령 인스턴스를 실행하여 기본 액세스 존이 아닌 영역에 있는 qtree, 할당량 및 NAS 공유/내보내기와 같은 개체의 논리적 구성을 가져옵니다. Insight Now는 이 기능 향상의 결과로 기본값이 아닌 액세스 존에 대한 개체를 보고합니다. Insight가 기존 명령(다른 옵션 사용)을 실행하여 해당 데이터를 가져올 때 해당 명령이 작동하려면 sudoers 파일을 변경할 필요가 없습니다. 이는 변경 사항이 필요하다는 위의 새 명령이 도입된 경우에만 해당됩니다.

Insight 서비스 계정이 이 Insight 릴리즈로 업그레이드하기 전에 해당 명령을 실행할 수 있도록 sudoers 파일을 업데이트하십시오. 그렇지 않으면 Isilon 데이터 소스가 실패합니다.

"파일 시스템" 통계

OnCommand Insight 7.3.12부터 EMC Isilon 데이터 수집기는 EMC Isilon의 노드 객체에 대한 "파일 시스템" 통계를 도입했습니다. OnCommand Insight에서 보고하는 기존 노드 통계는 "디스크" 기반 i.e, 스토리지 노드의 IOPS 및 처리량에 대해 이 노드의 디스크는 Aggregate에서 어떤 작업을 합니까? 그러나 읽기 작업이 메모리에 캐시되거나 압축이 사용 중인 워크로드의 경우 파일 시스템 워크로드가 실제로 디스크에 적중하는 것보다 훨씬 높을 수 있습니다. 5:1을 압축하는 데이터 세트에서는 "파일 시스템 읽기 처리량" 값이 스토리지 노드의 읽기 처리량보다 5배 높을 수 있습니다. 후자는 디스크에서 읽기를 측정하므로 노드가 데이터를 압축 해제하고 클라이언트의 읽기 요청을 처리할 때 5배 확장됩니다.

Dell EMC PowerStore 데이터 소스

Dell EMC PowerStore 데이터 수집기는 Dell EMC PowerStore 스토리지에서 인벤토리 정보를 수집합니다. 구성을 위해 데이터 수집기는 스토리지 프로세서의 IP 주소와 읽기 전용 사용자 이름 및 암호를 필요로 합니다.

용어

OnCommand Insight는 EMC Data Domain 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
호스트	호스트
host_volume_mapping을 선택합니다	host_volume_mapping을 선택합니다

하드웨어("extra_details" 객체 아래에 드라이브가 있음): 드라이브	디스크
어플라이언스	스토리지 풀
클러스터	스토리지
노드	스토리지노드
fc_port 를 선택합니다	포트
볼륨	볼륨
내부 볼륨	파일 시스템
파일 시스템	내부 볼륨
MTree입니다	qtree를 입력합니다
할당량	할당량
NFS 및 CIFS 공유	파일 공유

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 스토리지 프로세서의 IP 주소 또는 정규화된 도메인 이름입니다
- 읽기 전용 사용자 이름 및 암호

상위 일련 번호가 설명되었습니다

일반적으로 Insight는 스토리지 어레이의 일련 번호 또는 개별 스토리지 노드의 일련 번호를 보고할 수 있습니다. 그러나 일부 스토리지 어레이 아키텍처는 이 문제에 완전히 부합되지 않습니다. PowerStore 클러스터는 1-4개의 어플라이언스로 구성될 수 있으며 각 어플라이언스에는 2개의 노드가 있습니다. 어플라이언스 자체에 일련 번호가 있는 경우 해당 일련 번호는 클러스터나 노드의 일련 번호가 아닙니다.

개별 노드가 대형 클러스터의 일부인 중간 어플라이언스/엔클로저 내에 있는 경우 스토리지 노드 개체의 "상위 일련 번호" 속성은 Dell/EMC PowerStore 어레이에 맞게 적절하게 채워집니다.

구성

필드에 입력합니다	설명

PowerStore 게이트웨이	PowerStore 스토리지의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	PowerStore의 사용자 이름입니다
암호	PowerStore에 사용되는 암호입니다

고급 구성

필드에 입력합니다	설명
HTTPS 포트	기본값은 443입니다
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 60분입니다.

OnCommand Insight의 PowerStore 성능 수집을 통해 PowerStore의 5분 단위 소스 데이터를 사용할 수 있습니다. 따라서 Insight는 5분마다 해당 데이터를 폴링하여 구성할 수 없습니다.

EMC RecoverPoint 데이터 소스

EMC RecoverPoint 데이터 소스는 EMC RecoverPoint 스토리지에서 인벤토리 정보를 수집합니다. 구성의 경우 데이터 소스에 스토리지 프로세서의 IP 주소와 _read-only_user 이름 및 암호가 필요합니다.

EMC RecoverPoint 데이터 소스는 RecoverPoint가 다른 스토리지 시스템 간에 조정하는 볼륨 간 복제 관계를 수집합니다. OnCommand Insight는 각 RecoverPoint 클러스터의 스토리지 시스템을 보여 주며 해당 클러스터의 노드 및 스토리지 포트에 대한 인벤토리 데이터를 수집합니다. 스토리지 풀 또는 볼륨 데이터가 수집되지 않습니다.

요구 사항

- 스토리지 프로세서의 IP 주소 또는 정규화된 도메인 이름입니다
- 읽기 전용 사용자 이름 및 암호
- 포트 443을 통한 REST API 액세스
- PuTTY를 통한 SSH 액세스

구성

필드에 입력합니다	설명
RecoverPoint의 주소입니다	RecoverPoint 클러스터의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	RecoverPoint 클러스터의 사용자 이름입니다
암호	RecoverPoint 클러스터의 암호입니다

고급 구성

필드에 입력합니다	설명
TCP 포트	RecoverPoint 클러스터에 접속하는 데 사용되는 TCP 포트입니다
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
제외된 클러스터	폴링 시 제외할 클러스터 ID 또는 이름의 쉼표로 구분된 목록입니다

SMI-S 성능 데이터 소스를 지원하는 **EMC Solutions Enabler**

OnCommand Insight는 Solutions Enabler를 사용하여 Symmetrix 스토리지 시스템을 검색합니다 `symcli` 사용자 환경에서 기존 Solutions Enabler 서버와 함께 사용되는 명령입니다. 기존 Solutions Enabler 서버는 게이트키퍼 볼륨에 대한 액세스를 통해 Symmetrix 스토리지에 접속할 수 있습니다. 이 장치에 액세스하려면 관리자 권한이 필요합니다.

용어

OnCommand Insight는 EMC Solutions Enabler 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
디스크	디스크
디스크 그룹	디스크 그룹
스토리지	스토리지
책임자	스토리지 노드
디바이스 풀, SRP(Storage Resource Pool)	스토리지 풀
디바이스, TDEV	볼륨

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

이 데이터 소스를 구성하기 전에 OnCommand Insight 서버가 기존 Solutions Enabler 서버의 포트 2707에 대한 TCP 연결을 가지고 있는지 확인해야 합니다. OnCommand Insight는 해당 서버의 "sycfg list" 출력에 표시된 것처럼 이 서버에 대한 "Local" Symmetrix 스토리지를 모두 검색합니다.

- SMI-S Provider 애플리케이션이 포함된 EMC Solutions Enabler(CLI)가 설치되어 있어야 하며 버전이 Solutions Enabler Server에서 실행 중인 버전과 동일하거나 그 이전이어야 합니다.
- 올바르게 구성되었습니다 `{installdir}\EMC\SYMAPI\config\netcnfg` 파일이 필요합니다. 이 파일은 Solutions Enabler 서버의 서비스 이름 및 액세스 방법(Secure/NOSECURE/Any)을 정의합니다.
- 스토리지 노드 레벨에서 읽기/쓰기 지연 시간이 필요한 경우 SMI-S Provider는 Unisphere for VMAX 애플리케이션의 실행 중인 인스턴스와 통신해야 합니다.
- SE(Solutions Enabler) 서버에 대한 관리자 권한
- SE 소프트웨어의 읽기 전용 사용자 이름 및 암호
- Solutions Enabler Server 6.5X 요구 사항:
  - SMIS-S v1.2용 SMI-S Provider 3.3.1 설치
  - 설치 후 를 실행합니다 `\Program Files\EMC\SYMCLI\bin>stordaemon start storsrvd`
- Unisphere for VMAX 애플리케이션은 SMI-S Provider 설치를 통해 관리되는 Symmetrix VMAX 스토리지 시스템에 대한 통계를 실행 및 수집해야 합니다
- 액세스 검증: SMI-S Provider가 실행 중인지 확인합니다. `telnet <se_server\> 5988`

구성

SMI-S 사용자 인증을 사용하지 않으면 OnCommand Insight 데이터 소스의 기본값이 무시됩니다.

Symmetrix 스토리지에 symauth를 설정하면 OnCommand Insight에서 해당 스토리지를 검색하는 기능이 억제될 수 있습니다. OnCommand Insight 취득은 Solutions Enabler 서버와 통신하는 OnCommand Insight/원격 획득 장치 서버에서 시스템 사용자로 실행됩니다. hostname\system에 symauth 권한이 없으면 OnCommand Insight에서 스토리지를 검색하지 못합니다.

EMC Solutions Enabler Symmetrix CLI 데이터 소스에는 씬 프로비저닝 및 SRDF(Symmetrix Remote Data Facility)에 대한 디바이스 구성이 지원됩니다.

Fibre Channel 및 스위치 성능 패키지에 대한 정의가 제공됩니다.

필드에 입력합니다	설명
서비스 이름	netcnfg 파일에 지정된 서비스 이름입니다
CLI의 전체 경로입니다	Symmetrix CLI의 전체 경로입니다

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)
목록을 지정하려면 '제외' 또는 '포함'을 선택하십시오	데이터를 수집할 때 아래 어레이 목록을 포함할지 제외할지 여부를 지정합니다

재고 제외 장치	포함하거나 제외할 장치 ID의 쉼표로 구분된 목록입니다
연결 캐싱	연결 캐싱 방법 선택: • 로컬은 검색하려는 Symmetrix 스토리지에 Fibre Channel 접속이 가능하고 게이트키퍼 볼륨에 액세스할 수 있는 Solutions Enabler 서버에서 OnCommand Insight 획득 서비스가 실행되고 있음을 의미합니다. 이 문제는 일부 RAU(Remote Acquisition Unit) 구성에서 확인할 수 있습니다. • remote_cached가 기본값입니다. 대부분의 경우 이 기능을 사용해야 합니다. 이 경우 NETCNFG 파일 설정을 사용하여 IP를 사용하여 Solutions Enabler 서버에 접속합니다. 이 서버는 검색할 Symmetrix 스토리지에 Fibre Channel 접속이 있어야 하며 게이트키퍼 볼륨에 액세스할 수 있어야 합니다. • remote_cached 옵션으로 인해 CLI 명령이 실패하는 경우 원격 옵션을 사용합니다. 구입 프로세스가 느려집니다(극단적인 경우 몇 시간 또는 며칠이 걸릴 수 있음). NETCNFG 파일 설정은 검색 중인 Symmetrix 스토리지에 Fibre Channel 접속이 설정된 Solutions Enabler 서버에 대한 IP 접속에 계속 사용됩니다. ⓘ 이 설정은 "symcfg list" 출력에 의해 원격 스토리지로 나열된 스토리지에 대한 OnCommand Insight 동작을 변경하지 않습니다. OnCommand Insight는 이 명령으로 로컬로 표시된 장치에서만 데이터를 수집합니다.
CLI 시간 제한(초)	CLI 프로세스 시간 초과(기본값: 7200초)
SMI-S 호스트 IP입니다	SMI-S Provider 호스트의 IP 주소입니다
SMI-S 포트	SMI-S Provider 호스트에서 사용하는 포트입니다
프로토콜	SMI-S 공급자에 연결하는 데 사용되는 프로토콜입니다
SMI-S 네임스페이스	SMI-S 공급자가 사용하도록 구성된 상호 운용성 네임스페이스입니다
SMI-S 사용자 이름	SMI-S Provider 호스트의 사용자 이름입니다
SMI-S 암호	SMI-S Provider 호스트의 사용자 이름입니다

성능 폴링 간격(초)	성능 폴링 간격(기본값 1000초)
성능 필터 유형	성능 데이터를 수집할 때 아래 스토리지 목록을 포함할지 제외할지 여부를 지정합니다
성능 필터 장치 목록	포함하거나 제외할 장치 ID의 쉼표로 구분된 목록입니다
RPO 폴링 간격(초)	RPO 폴링 간격(기본값 300초)

EMC VNX 데이터 소스

구성의 경우 EMC VNX(SSH) 데이터 소스에는 Control Station의 IP 주소와 _read-only_username 및 암호가 필요합니다.

구성

필드에 입력합니다	설명
VNX IP	VNX Control Station의 IP 주소 또는 정규화된 도메인 이름입니다
VNX 사용자 이름입니다	VNX Control Station의 사용자 이름입니다
VNX 암호	VNX Control Station의 암호입니다

요구 사항

- Control Station의 IP 주소입니다
- 읽기 전용 사용자 이름 및 암호.
- 액세스 검증: PuTTY를 통해 SSH 액세스를 검증합니다.

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)
VNX SSH 프로세스 대기 시간 초과(초)	VNX SSH 프로세스 시간 초과(기본값 600초)
Celerra 명령 재시도 횟수입니다	Celerra 명령 재시도 횟수입니다
인벤토리에 대한 CLARiX 외부 프로세스 시간 초과(초)	인벤토리에 대한 CLARiX 외부 프로세스 시간 초과(기본값 1800초)

성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
CLARiX 외부 프로세스 성능 제한 시간(초)	성능을 위한 CLARiX 외부 프로세스 시간 초과(기본값 1800초)

EMC VNXe 데이터 소스

EMC VNXe 데이터 소스는 EMC VNXe 및 Unity 유니파이드 스토리지 시스템에 대한 인벤토리 지원을 제공합니다.

이 데이터 소스는 CLI 기반이며 VNXe 데이터 소스가 상주하는 수집 유닛에 Unisphere for VNXe CLI(uemcli.exe)를 설치해야 합니다. uemcli.exe 전송 프로토콜로 HTTPS를 사용하므로 획득 장치에서 VNXe/Unity 어레이에 대한 HTTPS 연결을 시작할 수 있어야 합니다. 데이터 소스에서 사용할 수 있는 읽기 전용 사용자가 적어도 있어야 합니다.

용어

OnCommand Insight는 EMC VNXe 데이터 소스에서 다음과 같은 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
디스크	디스크
스토리지	스토리지
프로세서	스토리지 노드
스토리지 풀	스토리지 풀
일반 iSCSI 블록 정보, VMware VMFS	볼륨
공유 폴더	내부 볼륨
CIFS 공유, NFS 공유, VMware NFS 데이터 저장소에서 공유	공유
복제 원격 시스템	동기화
iSCSI 노드	iSCSI 타겟 노드
iSCSI 초기자	iSCSI 대상 초기자

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

다음은 이 데이터 소스를 구성하고 사용하기 위한 요구 사항입니다.

- VNXe 데이터 수집기는 CLI를 기반으로 합니다. VNXe 데이터 수집기가 있는 획득 유닛에 Unisphere for VNXe CLI(uemcli.exe)를 설치해야 합니다.
- uemcli.exe 전송 프로토콜로 HTTPS를 사용하므로 획득 장치에서 VNXe에 대한 HTTPS 연결을 시작할 수 있어야 합니다.
- 데이터 소스에서 사용할 수 있는 읽기 전용 사용자가 적어도 있어야 합니다.
- 관리 솔루션 Enabler 서버의 IP 주소입니다.
- 포트 443의 HTTPS가 필요합니다
- EMC VNXe 데이터 수집기는 인벤토리에 대한 NAS 및 iSCSI 지원을 제공합니다. Fibre Channel 볼륨은 검색되지만 Insight는 FC 매핑, 마스킹 또는 스토리지 포트에 대해서는 보고하지 않습니다.

구성

필드에 입력합니다	설명
VNXe 스토리지	VNXe 디바이스의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	VNXe 디바이스의 사용자 이름입니다
암호	VNXe 디바이스의 암호입니다
uemcli 실행 파일의 전체 경로입니다	에 대한 전체 경로입니다 `uemcli.exe` 실행 파일

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)
VNXe CLI 포트	VNXe CLI에 사용되는 포트입니다
재고 외부 프로세스 시간 초과(초)	외부 프로세스 시간 초과(기본값 1800초)

EMC VPLEX 데이터 소스

구성의 경우 이 데이터 소스에 VPLEX 서버의 IP 주소와 관리 레벨 도메인 계정이 필요합니다.

용어

OnCommand Insight는 EMC VPLEX 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
클러스터	스토리지
엔진	스토리지 노드
장치, 시스템 확장	백엔드 스토리지 풀입니다
가상 볼륨	볼륨
프런트엔드 포트, 백엔드 포트	포트
분산 장치	저장소 동기화
스토리지 보기	볼륨 맵, 볼륨 마스크
스토리지 볼륨	백엔드 LUN
ITL	백엔드 경로

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- VPLEX 서버의 IP 주소입니다
- VPLEX 서버의 관리 레벨 도메인 계정입니다
- 포트 443(HTTPS). VPLEX 관리 스테이션의 TCP 포트 443에 대한 아웃바운드 연결이 필요합니다.
- 성능을 위해 ssh/scp 액세스를 위한 읽기 전용 사용자 이름과 암호를 사용합니다.
- 성능을 위해서는 포트 22가 필요합니다.
- 액세스 확인: 을 사용하여 확인합니다 `telnet` 포트 443으로 이동합니다. 기본 포트 이외의 포트에 대해 브라우저를 사용할 수 있습니다

구성

필드에 입력합니다	설명
VPLEX Management Console의 IP 주소입니다	VPLEX Management Console의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	VPLEX CLI의 사용자 이름입니다
암호	VPLEX CLI에 사용되는 암호입니다

VPLEX Management Console의 성능 원격 IP 주소입니다	VPLEX Management Console의 성능 원격 IP 주소입니다
성능 원격 사용자 이름입니다	VPLEX Management Console의 Performance Remote 사용자 이름입니다
성능 원격 암호	VPLEX Management Console의 성능 원격 암호

고급 구성

필드에 입력합니다	설명
통신 포트	VPLEX CLI에 사용되는 포트입니다
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
연결 시간 초과(초)	연결 시간 초과(기본값 60초)
재시도 횟수	인벤토리 재시도 횟수입니다
성능 폴링 간격(초)	성능 폴링 간격(기본값 600초)
성능 SSH 프로세스 대기 시간 초과(초)	SSH 프로세스 시간 초과(기본값 600초)
SSH 배너 대기 시간 제한(초)	SSH 배너 대기 시간 초과(기본값 20초)
재시도 횟수	성능 재시도 횟수입니다

EMC XtremIO 데이터 소스

EMC XtremIO(HTTP) 데이터 소스를 구성하려면 XtremIO 관리 서버(XMS) 호스트 주소와 관리자 권한이 있는 계정이 있어야 합니다.

용어

OnCommand Insight는 EMC XtremIO 데이터 소스에서 다음 인벤토리 정보를 수집합니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
디스크(SSD)	디스크
클러스터	스토리지

컨트롤러	스토리지 노드
볼륨	볼륨
LUN 매핑	볼륨 맵
초기자, 대상	볼륨 마스크

> 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 각 XtremIO 관리 서버의 IP 주소
- 관리자 권한이 있는 계정입니다
- 포트 443(HTTPS)에 대한 액세스

구성

필드에 입력합니다	설명
XMS 호스트	XtremIO 관리 서버의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름입니다	XtremIO 관리 서버의 사용자 이름입니다
암호	XtremIO 관리 서버의 암호입니다

고급 구성

필드에 입력합니다	설명
TCP 포트	XTremIO 관리 서버에 연결하는 데 사용되는 TCP 포트(기본값 443)
재고 폴링 간격(분)	재고 조사 간격(기본값: 60분)
연결 시간 초과(초)	연결 시간 초과(기본값 60초)
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

Fujitsu ETERNUS 데이터 소스

Fujitsu ETERNUS 데이터 원본에는 스토리지의 IP 주소가 필요합니다. 쉼표로 구분할 수

없습니다.

용어

OnCommand Insight는 Fujitsu ETERNUS 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
디스크	디스크
스토리지	스토리지
씬 풀, 유연한 계층 풀, RAID 그룹	스토리지 풀
표준 볼륨, 스냅 데이터 볼륨(SDV), 스냅 데이터 풀 볼륨(SDPV), 씬 프로비저닝 볼륨(TPV)	볼륨

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- ETERNUS 저장소의 IP 주소로, 쉼표로 구분될 수 없습니다
- SSH 관리 수준 사용자 이름 및 암호
- 포트 22
- 페이지 스크롤이 비활성화되어 있는지 확인합니다. (clienv -show -more -scroll disable)

구성

필드에 입력합니다	설명
ETERNUS 스토리지의 IP 주소입니다	ETERNUS 스토리지의 IP 주소입니다
사용자 이름	ETERNUS 스토리지에 대한 사용자 이름입니다
암호	흉기에 사용되는 암호입니다

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
SSH 프로세스 대기 시간 초과(초)	SSH 프로세스 시간 초과(기본값 600초)

Hitachi Content Platform(HCP) 데이터 소스

이 데이터 수집기는 HCP 관리 API를 사용하는 HCP(Hitachi Content Platform)를 지원합니다.

용어

OnCommand Insight는 HCP 데이터 소스에서 다음 재고 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
HCP 클러스터	스토리지
테넌트	스토리지 풀
네임스페이스	내부 볼륨
노드	노드

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

재고 요건

- HCP 서버의 IP 주소입니다
- HCP 소프트웨어 및 피어 권한에 대한 읽기 전용 사용자 이름 및 암호입니다

구성

* 필드 *	* 설명 *
HCP 호스트	HCP 호스트의 IP 주소 또는 정규화된 도메인 이름입니다
HCP 포트	기본값은 9090입니다
HCP 사용자 ID입니다	HCP 호스트의 사용자 이름입니다

HCP 암호	HCP 호스트에 사용되는 암호입니다
HCP 인증 유형	HCP_LOCAL 또는 ACTIVE_DIRECTORY 를 선택합니다

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값: 60분)
성능 폴링 간격(초)	성능 폴링 간격(기본값 900초)

HDS HiCommand Device Manager 데이터 소스

HDS HiCommand 및 HiCommand Lite 데이터 소스는 HiCommand Device Manager 서버를 지원합니다. OnCommand Insight는 표준 HiCommand API를 사용하여 HiCommand Device Manager 서버와 통신합니다.

용어

OnCommand Insight는 HDS HiCommand 및 HiCommand Lite 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
개발	디스크
저널 풀	디스크 그룹
스토리지	스토리지
포트 컨트롤러	스토리지 노드
스토리지 그룹, DP 풀	스토리지 풀
논리 유닛, LDEV	볼륨

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

재고 요건

- HiCommand Device Manager 서버의 IP 주소입니다

- HiCommand Device Manager 소프트웨어 및 피어 권한에 대한 읽기 전용 사용자 이름 및 암호입니다
- 포트 요구 사항: 2001(http) 또는 2443(https)
- 액세스 확인:
  - 피어 사용자 이름 및 암호를 사용하여 HiCommand Device Manager 소프트웨어에 로그인합니다.
  - HiCommand Device Manager API에 대한 액세스 확인: `telnet <HiCommand Device_Manager_server_ip\> 2001`

성능 요구사항

- HDS USP, USP V 및 VSP 성능
  - 성능 모니터에 라이센스가 있어야 합니다.
  - 모니터링 스위치를 활성화해야 합니다.
  - 내보내기 도구 (`Export.exe`)을 OnCommand Insight 서버에 복사해야 합니다.
  - 내보내기 도구 버전은 대상 스토리지의 마이크로코드 버전과 일치해야 합니다.
- HDS AMS 성능
  - 성능 모니터의 라이센스를 받아야 합니다.
  - SNM2(Storage Navigator Modular 2) CLI 유틸리티를 OnCommand Insight 서버에 설치해야 합니다.
  - 다음 명령을 사용하여 OnCommand Insight에서 성능을 획득해야 하는 모든 AMS, WMS, SMS 저장소 어레이를 등록해야 합니다.
  - 등록한 모든 스토리지가 다음 명령의 출력에 나열되어 있는지 확인해야 합니다. `auunitref.exe`.

구성

* 필드 *	* 설명 *
HiCommand 서버	HiCommand Device Manager 서버의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	HiCommand Device Manager 서버의 사용자 이름입니다.
암호	HiCommand Device Manager 서버에 사용되는 암호입니다.

디바이스 - VSP G1000(R800), VSP(R700), HUS VM(HM700) 및 USP 스토리지	VSP G1000(R800), VSP(R700), HUS VM(HM700) 및 USP 스토리지를 위한 장치 목록입니다. 각 스토리지에는 다음이 필요합니다. • 스토리지의 IP: 스토리지의 IP 주소입니다 • User Name: 스토리지의 사용자 이름입니다 • 암호: 스토리지의 암호입니다 • Export Utility Jar Files(유틸리티 JAR 파일 내보내기): Export Utility(내보내기 유틸리티)가 포함된 폴더입니다 `.jar` 파일
SNM2Devices - WMS/SMS/AMS 저장소	WMS/SMS/AMS 저장소에 대한 장치 목록입니다. 각 스토리지에는 다음이 필요합니다. • 스토리지의 IP: 스토리지의 IP 주소입니다 • Storage Navigator CLI 경로: SNM2 CLI 경로 • 계정 인증 유효: 유효한 계정 인증을 선택하려면 선택합니다 • User Name: 스토리지의 사용자 이름입니다 • 암호: 스토리지의 암호입니다
성능 조정 관리자 를 선택합니다	성능 튜닝 관리자를 선택하고 다른 성능 옵션을 재정의합니다
튜닝 관리자 호스트	튜닝 관리자의 IP 주소 또는 정규화된 도메인 이름입니다
Tuning Manager 포트	Tuning Manager에 사용되는 포트입니다
튜닝 관리자 사용자 이름	Tuning Manager의 사용자 이름입니다
조정 관리자 암호	Tuning Manager 암호

HDS USP, USP V 및 VSP에서 모든 디스크는 둘 이상의 스토리지 그룹에 속할 수 있습니다.

고급 구성

필드에 입력합니다	설명
HiCommand 서버 포트	HiCommand 장치 관리자에 사용되는 포트입니다
HTTPS가 활성화되었습니다	HTTPS를 활성화하려면 선택합니다
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)

목록을 지정하려면 '제외' 또는 '포함'을 선택하십시오	데이터를 수집할 때 아래 어레이 목록을 포함할지 제외할지 여부를 지정합니다
장치 제외 또는 포함	포함하거나 제외할 장치 ID 또는 배열 이름의 쉼표로 구분된 목록입니다
호스트 관리자를 쿼리합니다	호스트 관리자를 쿼리하려면 선택합니다
HTTP 시간 제한(초)	HTTP 연결 시간 초과(기본값 60초)
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
내보내기 제한 시간(초	내보내기 유틸리티 시간 초과(기본값 300초)

Hitachi Ops Center 데이터 수집기

이 데이터 수집기는 Hitachi Ops Center의 통합 애플리케이션 제품군을 사용하여 여러 스토리지 디바이스의 인벤토리 및 성능 데이터에 액세스합니다. 인벤토리 및 용량 검색을 위해 Ops Center 설치에는 "공통 서비스" 및 "관리자" 구성 요소가 모두 포함되어야 합니다. 성능 수집을 위해 "Analyzer"를 추가로 구축해야 합니다.

용어

OnCommand Insight는 이 데이터 수집기에서 다음 인벤토리 정보를 가져옵니다. 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	**OnCommand Insight** 용어입니다
스토리지 시스템	스토리지
볼륨	볼륨
패리티 그룹	스토리지 풀(RAID), 디스크 그룹
디스크	디스크
스토리지 풀	스토리지 풀(씬, 스냅)
외부 패리티 그룹	스토리지 풀(백엔드), 디스크 그룹
포트	스토리지 노드 → 컨트롤러 노드 → 포트
호스트 그룹	볼륨 매핑 및 마스킹
볼륨 쌍	저장소 동기화

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

재고 요건

재고 데이터를 수집하려면 다음이 있어야 합니다.

- "공통 서비스" 구성 요소를 호스팅하는 Ops Center 서버의 IP 주소 또는 호스트 이름입니다
- Ops Center 구성 요소를 호스팅하는 모든 서버에 있는 루트/sysadmin 사용자 계정 및 암호입니다. HDS는 Ops Center 10.8 이상이 될 때까지 LDAP/SSO 사용자의 REST API 지원을 구현하지 않았습니다

성능 요구사항

성능 데이터를 수집하려면 다음 요구사항을 충족해야 합니다.

- HDS Ops Center "Analyzer" 모듈을 설치해야 합니다
- 스토리지 어레이가 운영 센터 "Analyzer" 모듈에 제공되어야 합니다

구성

필드에 입력합니다	설명
Hitachi Ops Center IP 주소입니다	"공통 서비스" 구성 요소를 호스팅하는 Ops Center 서버의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	Ops Center 서버의 사용자 이름입니다.
암호	Ops Center 서버에 사용되는 암호입니다.

고급 구성

필드에 입력합니다	설명
연결 유형	기본값은 HTTPS(포트 443)입니다
TCP 포트를 재정의합니다	기본값이 아닌 경우 사용할 포트를 지정합니다
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 40입니다.
목록을 지정하려면 '제외' 또는 '포함'을 선택하십시오	데이터를 수집할 때 아래 어레이 목록을 포함할지 제외할지 여부를 지정합니다.
장치 목록을 필터링합니다	포함하거나 제외할 장치 일련 번호의 쉼표로 구분된 목록입니다
성능 폴링 간격(초)	성능 폴링 간격입니다. 기본값은 300입니다.

HDS 스토리지

HDS 스토리지 자산 랜딩 페이지에서 찾을 수 있는 오브젝트나 참조에 적용되는 용어입니다.

HDS 스토리지 용어

다음 용어는 HDS 스토리지 자산 랜딩 페이지에서 찾을 수 있는 오브젝트 또는 참조에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

- 이름 — GetStorageArray XML API 호출을 통해 HDS HiCommand Device Manager의 ""이름" 속성에서 직접 가져옵니다
- 모델 - GetStorageArray XML API 호출을 통해 HDS HiCommand Device Manager의 ""arrayType"" 특성에서 직접 제공됩니다

- 공급업체 — HDS
- Family - GetStorageArray XML API 호출을 통해 HDS HiCommand Device Manager의 ""arrayFamily" 속성에서 직접 제공됩니다
- IP — 어레이의 모든 IP 주소 목록이 아니라 어레이의 관리 IP 주소입니다
- Raw Capacity — 디스크 역할에 관계없이 이 시스템에 있는 모든 디스크의 총 용량 합계를 나타내는 Base2 값입니다.

HDS 스토리지 풀

HDS 스토리지 풀 자산 랜딩 페이지에서 찾을 수 있는 오브젝트나 참조에 적용되는 용어입니다.

HDS 스토리지 풀 용어

다음 용어는 HDS 스토리지 풀 자산 랜딩 페이지에서 찾을 수 있는 오브젝트 또는 참조에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

- 유형: 여기에 있는 값은 다음 중 하나입니다.
  - 예약됨 — 이 풀이 데이터 볼륨(예: 저널링, 스냅샷)이 아닌 다른 용도로 사용되는 경우
  - 씬 프로비저닝 — HDP 풀인 경우
  - RAID 그룹 — 다음과 같은 몇 가지 이유로 이러한 항목이 표시되지 않을 수 있습니다.

    OCI는 용량을 모든 비용에 두 배로 늘리는 것을 피하기 위해 강력한 입지를 가지고 있습니다. HDS에서는 일반적으로 디스크에서 RAID 그룹을 구축하고, 해당 RAID 그룹에 풀 볼륨을 생성하고, 해당 풀 볼륨에서 풀(대개 HDP이지만 특수한 용도로 사용될 수 있음)을 구성해야 합니다. OCI가 기본 RAID 그룹과 풀을 모두 보고한 경우 원시 용량의 합이 디스크 합보다 엄청나게 큽니다.

  대신, OCI의 HDS HiCommand 데이터 수집기는 풀 볼륨의 용량에 따라 RAID 그룹의 크기를 임의로 축소합니다. 결과적으로 OCI가 RAID 그룹을 보고하지 않을 수 있습니다. 또한 결과 RAID 그룹은 OCI WebUI에서 표시되지 않지만 DWH(OCI 데이터 웨어하우스)로 흐르게 되는 방식으로 플래그가 지정됩니다. 이러한 의사 결정의 목적은 대부분의 사용자가 신경 쓰지 않는 것들에 대한 UI 혼란을 피하는 것입니다. HDS 어레이에 50MB의 여유 공간이 있는 RAID 그룹이 있는 경우, 의미 있는 결과를 얻기 위해 이 여유 공간을 사용할 수 없을 것입니다.

- HDS 풀은 특정 노드에 연결되지 않으므로 노드 N/A입니다
- 이중화 - 풀의 RAID 레벨입니다. 여러 RAID 유형으로 구성된 HDP 풀의 값이 여러 개일 수 있습니다
- 용량 % - 풀의 사용된 GB 및 총 논리적 GB 크기와 함께 데이터 사용에 사용된 풀의 비율
- 과도하게 커밋된 용량 - 이 풀의 논리적 용량이 풀의 논리적 용량을 이 비율로 초과하는 논리적 볼륨의 합계로 이 비율에 의해 초과 할당되고 있습니다.
- 스냅샷 - 이 풀의 스냅샷 사용을 위해 예약된 용량을 표시합니다

HDS 스토리지 노드

HDS 스토리지 노드 자산 랜딩 페이지에서 찾을 수 있는 오브젝트나 참조에 적용되는 용어입니다.

HDS 스토리지 노드 용어

다음 용어는 HDS 스토리지 노드 자산 랜딩 페이지에서 찾을 수 있는 오브젝트 또는 참조에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

- 이름 - 모놀리식 어레이에 있는 프런트엔드 디렉터(FED) 또는 채널 어댑터의 이름 또는 모듈식 어레이에서 컨트롤러의 이름입니다. 주어진 HDS 어레이에는 2개 이상의 스토리지 노드가 있습니다
- 볼륨 — 볼륨 테이블에는 이 스토리지 노드가 소유한 포트에 매핑된 모든 볼륨이 표시됩니다

Hitachi Ops Center 데이터 수집기

이 데이터 수집기는 Hitachi Ops Center의 통합 애플리케이션 제품군을 사용하여 여러 스토리지 디바이스의 인벤토리 및 성능 데이터에 액세스합니다. 인벤토리 및 용량 검색을 위해 Ops Center 설치에는 "공통 서비스" 및 "관리자" 구성 요소가 모두 포함되어야 합니다. 성능 수집을 위해 "Analyzer"를 추가로 구축해야 합니다.

용어

OnCommand Insight는 이 데이터 수집기에서 다음 인벤토리 정보를 가져옵니다. 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	**OnCommand Insight** 용어입니다
스토리지 시스템	스토리지
볼륨	볼륨
패리티 그룹	스토리지 풀(RAID), 디스크 그룹
디스크	디스크
스토리지 풀	스토리지 풀(씬, 스냅)
외부 패리티 그룹	스토리지 풀(백엔드), 디스크 그룹
포트	스토리지 노드 → 컨트롤러 노드 → 포트
호스트 그룹	볼륨 매핑 및 마스킹
볼륨 쌍	저장소 동기화

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

재고 요건

재고 데이터를 수집하려면 다음이 있어야 합니다.

- "공통 서비스" 구성 요소를 호스팅하는 Ops Center 서버의 IP 주소 또는 호스트 이름입니다
- Ops Center 구성 요소를 호스팅하는 모든 서버에 있는 루트/sysadmin 사용자 계정 및 암호입니다. HDS는 Ops Center 10.8 이상이 될 때까지 LDAP/SSO 사용자의 REST API 지원을 구현하지 않았습니다

성능 요구사항

성능 데이터를 수집하려면 다음 요구사항을 충족해야 합니다.

- HDS Ops Center "Analyzer" 모듈을 설치해야 합니다
- 스토리지 어레이가 운영 센터 "Analyzer" 모듈에 제공되어야 합니다

구성

필드에 입력합니다	설명
Hitachi Ops Center IP 주소입니다	"공통 서비스" 구성 요소를 호스팅하는 Ops Center 서버의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	Ops Center 서버의 사용자 이름입니다.
암호	Ops Center 서버에 사용되는 암호입니다.

고급 구성

필드에 입력합니다	설명
연결 유형	기본값은 HTTPS(포트 443)입니다
TCP 포트를 재정의합니다	기본값이 아닌 경우 사용할 포트를 지정합니다
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 40입니다.
목록을 지정하려면 '제외' 또는 '포함'을 선택하십시오	데이터를 수집할 때 아래 어레이 목록을 포함할지 제외할지 여부를 지정합니다.
장치 목록을 필터링합니다	포함하거나 제외할 장치 일련 번호의 쉼표로 구분된 목록입니다
성능 폴링 간격(초)	성능 폴링 간격입니다. 기본값은 300입니다.

HDS NAS(HNAS) 데이터 소스

HDS NAS(HNAS) 데이터 소스는 HDS NAS 클러스터의 검색을 지원하는 인벤토리 및 구성 데이터 소스입니다. Insight는 NFS 및 CIFS 공유, 파일 시스템(Insight 내부 볼륨) 및 확장(Insight 스토리지 풀)을 검색할 수 있도록 지원합니다.

이 데이터 소스는 SSH 기반이므로 HNAS 자체의 TCP 22 또는 클러스터가 연결된 시스템 관리 장치(SMU)에 대해 SSH 세션을 시작할 수 있어야 합니다.

용어

OnCommand Insight는 HNAS 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
계층	디스크 그룹
클러스터	스토리지

노드	스토리지 노드
스팬	스토리지 풀
파일 시스템	내부 볼륨

> 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

다음은 이 데이터 소스를 구성하고 사용하기 위한 요구 사항입니다.

- 장치 IP 주소입니다
- 포트 22, SSH 프로토콜
- 사용자 이름 및 암호 권한 수준: 감독자
- 참고: 이 데이터 수집기는 SSH 기반이므로 HNAS 자체의 TCP 22 또는 클러스터가 연결된 시스템 관리 장치(SMU)에 대해 SSH 세션을 시작할 수 있어야 합니다.

> 이 데이터 수집기는 SSH 기반이므로 HNAS 자체의 TCP 22 또는 클러스터가 연결된 시스템 관리 장치(SMU)에 대해 SSH 세션을 시작할 수 있어야 합니다.

구성

필드에 입력합니다	설명
HNAS 호스트	HNAS 관리 호스트의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	HNAS CLI의 사용자 이름입니다
암호	HNAS CLI에 사용되는 암호입니다

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 30분)
SSH 배너 대기 시간 제한(초)	SSH 배너 대기 시간 초과(기본값 15초)
SSH 명령 시간 초과(초)	SSH 명령 시간 초과(기본값 30초)

HP CommandView AE 데이터 소스

HP CommandView Advanced Edition(AE) 및 CommandView AE CLI/SMI(AE Lite) 데이터 소스는 CommandView(HiCommand) 장치 관리자 서버라고도 함)의 인벤토리 및 성능을 지원합니다.

용어

OnCommand Insight는 HP CommandView AE 및 AE Lite 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
개발	디스크
저널 풀	디스크 그룹
스토리지	스토리지
포트 컨트롤러	스토리지 노드
스토리지 그룹, DP 풀	스토리지 풀
논리 유닛, LDEV	볼륨

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

재고 요건

- HiCommand Device Manager 서버의 IP 주소입니다
- CommandView AE 소프트웨어 및 피어 권한에 대한 읽기 전용 사용자 이름 및 암호
- 장치 관리자의 CommandView AE Lite 버전에는 CLI 라이센스만 있습니다
- 포트 요구 사항: 2001

성능 요구사항

- HDS USP, USP V 및 VSP 성능
  - 성능 모니터에 라이센스가 있어야 합니다.
  - 모니터링 스위치를 활성화해야 합니다.
  - 내보내기 도구 (`Export.exe`)을 OnCommand Insight 서버에 복사해야 합니다.
  - 내보내기 도구 버전은 대상 스토리지의 마이크로코드 버전과 일치해야 합니다.
- HDS AMS 성능

- 성능 모니터의 라이센스를 받아야 합니다.
- SNM2(Storage Navigator Modular 2) CLI 유틸리티를 OnCommand Insight 서버에 설치해야 합니다.
- 다음 명령을 사용하여 OnCommand Insight에서 성능을 획득해야 하는 모든 AMS, WMS, SMS 저장소 어레이를 등록해야 합니다.
- 등록한 모든 스토리지가 다음 명령의 출력에 나열되어 있는지 확인해야 합니다. `auunitref.exe`.

구성

* 필드 *	* 설명 *
HiCommand 서버	HiCommand Device Manager 서버의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	HiCommand Device Manager 서버의 사용자 이름입니다.
암호	HiCommand Device Manager 서버에 사용되는 암호입니다.
장치 - USP, USP V, VSP/R600 보관	VSP G1000(R800), VSP(R700), HUS VM(HM700) 및 USP 스토리지를 위한 장치 목록입니다. 각 스토리지에는 다음이 필요합니다. • 스토리지의 IP: 스토리지의 IP 주소입니다 • User Name: 스토리지의 사용자 이름입니다 • 암호: 스토리지의 암호입니다 • Export Utility Jar Files(유틸리티 JAR 파일 내보내기): Export Utility(내보내기 유틸리티)가 포함된 폴더입니다 `.jar` 파일
SNM2Devices - WMS/SMS/AMS 저장소	WMS/SMS/AMS 저장소에 대한 장치 목록입니다. 각 스토리지에는 다음이 필요합니다. • 스토리지의 IP: 스토리지의 IP 주소입니다 • Storage Navigator CLI 경로: SNM2 CLI 경로 • 계정 인증 유효: 유효한 계정 인증을 선택하려면 선택합니다 • User Name: 스토리지의 사용자 이름입니다 • 암호: 스토리지의 암호입니다
성능 조정 관리자 를 선택합니다	성능 튜닝 관리자를 선택하고 다른 성능 옵션을 재정의합니다
튜닝 관리자 호스트	튜닝 관리자의 IP 주소 또는 정규화된 도메인 이름입니다

Tuning Manager 포트	Tuning Manager에 사용되는 포트입니다
튜닝 관리자 사용자 이름	Tuning Manager의 사용자 이름입니다
조정 관리자 암호	Tuning Manager 암호

HDS USP, USP V 및 VSP에서 모든 디스크는 둘 이상의 스토리지 그룹에 속할 수 있습니다.

고급 구성

필드에 입력합니다	설명
HiCommand 서버 포트	HiCommand 장치 관리자에 사용되는 포트입니다
HTTPS가 활성화되었습니다	HTTPS를 활성화하려면 선택합니다
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)
목록을 지정하려면 '제외' 또는 '포함'을 선택하십시오	데이터를 수집할 때 아래 어레이 목록을 포함할지 제외할지 여부를 지정합니다
장치 제외 또는 포함	포함하거나 제외할 장치 ID 또는 배열 이름의 쉼표로 구분된 목록입니다
호스트 관리자를 쿼리합니다	호스트 관리자를 쿼리하려면 선택합니다
HTTP 시간 제한(초)	HTTP 연결 시간 초과(기본값 60초)
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
내보내기 제한 시간(초	내보내기 유틸리티 시간 초과(기본값 300초)

HP EVA 스토리지 데이터 소스

구성을 위해 EVA 스토리지(SSSU) 데이터 원본에는 명령 보기(CV) 서버의 IP 주소와 CV 소프트웨어에 대한 _read-only_username 및 암호가 필요합니다. 사용자는 CV 소프트웨어에서 정의해야 합니다.

용어

OnCommand Insight는 HP EVA 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
디스크	디스크
디스크 그룹	디스크 그룹(모델링되지 않음)
스토리지 셀	스토리지
가상 디스크	스토리지 풀
가상 디스크	볼륨

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

재고 요건

- CV 서버의 IP 주소입니다
- CV 소프트웨어에 대한 읽기 전용 사용자 이름 및 암호 사용자는 CV 소프트웨어에서 정의해야 합니다.
- OnCommand Insight 서버/RAU에 설치된 타사 소프트웨어: `sssu.exe`. 를 클릭합니다 `sssu.exe` 버전은 CV 버전과 일치해야 합니다.
- 액세스 검증: 실행 `sssu.exe` 사용자 이름 및 암호를 사용하는 명령입니다.

성능 요구사항

HP StorageWorks 명령 보기 EVA 소프트웨어 제품군을 OnCommand Insight 서버에 설치해야 합니다. 또는 EVA 서버에 RAU(원격 획득 장치)를 설치할 수 있습니다.

1. OnCommand Insight 서버에 HP StorageWorks 명령 보기 EVA 소프트웨어 제품군을 설치하거나 명령 보기 EVA 서버에 원격 획득 장치를 설치합니다.
2. 를 찾습니다 `evaperf.exe` 명령. 예를 들면, 다음과 같습니다. `c:\Program Files\Hewlett-Packard\EVA Performance Monitor\`
3. Command View 서버의 IP를 사용하여 다음 단계를 수행하십시오.
   a. 860이 기본 포트인 경우 이 명령을 실행합니다 `Evaperf.exe server <Command View Server IP\> 860 <username\>`
   b. 암호 프롬프트에 Command View 서버 암호를 입력합니다.

      이렇게 하면 명령줄 프롬프트가 반환되고 다른 것은 반환되지 않습니다.
4. 를 실행하여 설정을 확인합니다 `evaperf.exe ls`.

   Command View 서버에서 관리하는 어레이 또는 컨트롤러 목록이 표시됩니다. 각 라인은 EVA 어레이에서 컨트롤러를 표시합니다.

구성

* 필드 *	* 설명 *
CommandView 서버	EVA Storage Manager의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	Command View Manager의 사용자 이름입니다. 이름은 Command View에서 정의해야 합니다.
암호	Command View Manager에 사용되는 암호입니다.
성능 사용자 이름입니다	성능을 위해 Command View Manager의 사용자 이름입니다. 이름은 Command View에서 정의해야 합니다.
성능 암호	성능을 위해 Command View Manager에 사용되는 암호입니다.

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)
CLI 홈	CLI 홈 디렉토리의 전체 경로 이름 `sssu.exe` 있습니다
재고 제외 장치	쉼표로 구분된 포함할 장치 이름 목록입니다
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
Performance CLI Home을 참조하십시오	어레이 성능의 경우 sssu.exe 있는 CLI 홈 디렉토리의 전체 경로 이름입니다. 액세스를 확인하려면 를 실행합니다 `sssu.exe`
명령 시간 초과(초)	`evaperf` 명령 대기 시간 초과(기본값 600초)
성능 제외 장치	성능 데이터 수집에서 제외할 장치 이름의 쉼표로 구분된 목록입니다

HPE Nimble 데이터 소스

HPE Nimble 데이터 수집기는 HPE Nimble 스토리지 어레이에 대한 인벤토리 및 성능 데이터를 지원합니다.

용어

OnCommand Insight는 HPE Nimble 데이터 소스에서 다음 인벤토리 정보를 수집합니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
스토리지	스토리지
디스크	디스크
수영장	스토리지 풀
볼륨	볼륨
이니시에이터	스토리지 호스트 별칭입니다
컨트롤러	스토리지 노드
Fibre Channel 인터페이스	컨트롤러

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 스토리지를 설치하고 구성해야 하며 FQDN(정규화된 도메인 이름) 또는 스토리지 관리 IP 주소를 통해 클라이언트에서 연결할 수 있어야 합니다.
- 스토리지에서 NimbleOS 2.3.x 이상을 실행해야 합니다.
- 어레이에 대한 유효한 사용자 이름과 암호가 있어야 합니다.
- 포트 5392가 어레이에서 열려 있어야 합니다.

구성

* 필드 *	* 설명 *
스토리지 관리 IP 주소입니다	FQDN(정규화된 도메인 이름) 또는 스토리지 관리 IP 주소입니다.
사용자 이름	Nimble 스토리지의 사용자 이름입니다
암호	Nimble 스토리지의 암호입니다

고급 구성

* 필드 *	* 설명 *
포트	Nimble REST API에서 사용하는 포트입니다. 기본값은 5392입니다.
재고 폴링 간격(분)	재고 조사 간격(기본값: 60분)

참고: 기본 성능 폴링 간격은 300초이며 변경할 수 없습니다. Nimble에서 지원하는 유일한 간격입니다.

Huawei OceanStor 데이터 소스

OnCommand Insight는 Huawei OceanStor(REST/HTTPS) 데이터 소스를 사용하여 Huawei OceanStor 스토리지의 인벤토리를 검색합니다.

용어

OnCommand Insight는 Huawei OceanStor로부터 다음과 같은 인벤토리 및 성능 정보를 수집합니다. OnCommand Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	OnCommand Insight 용어입니다
스토리지 풀	스토리지 풀
파일 시스템	내부 볼륨
컨트롤러	스토리지 노드
FC 포트(매핑)	볼륨 맵
호스트 FC 이니시에이터(매핑)	볼륨 마스크
NFS/CIFS 공유입니다	공유
공유	iSCSI 타겟 노드
iSCSI 링크 초기자	iSCSI 이니시에이터 노드입니다
디스크	디스크
LUN을 클릭합니다	볼륨

요구 사항

다음은 이 데이터 수집기를 구성하고 사용하기 위한 요구 사항입니다.

- 장치 IP
- OceanStor 장치 관리자에 액세스하기 위한 자격 증명
- 포트 8088을 사용할 수 있어야 합니다

구성

필드에 입력합니다	설명
OceanStor 호스트 IP 주소입니다	OceanStor Device Manager의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	OceanStor Device Manager에 로그인하는 데 사용되는 이름입니다
암호	OceanStor Device Manager에 로그인하는 데 사용되는 암호입니다

고급 구성

필드에 입력합니다	설명
TCP 포트	OceanStor Device Manager에 연결하는 데 사용되는 TCP 포트(기본값 8088)
재고 폴링 간격(분)	재고 조사 간격(기본값: 60분)
연결 시간 초과(초)	연결 시간 초과(기본값 60초)

IBM Cleversafe 데이터 소스

이 데이터 소스는 IBM Cleversafe에 대한 인벤토리 및 성능 데이터를 수집합니다.

요구 사항

다음은 이 데이터 소스를 구성하기 위한 요구 사항입니다.

- 관리자 IP 주소 또는 호스트 이름
- 동일한 사용자 이름과 암호
- 포트 9440

구성

필드에 입력합니다	설명

Cleversafe 관리자 호스트 이름 또는 IP 주소	클레버세이프 장치의 호스트 IP 주소입니다
사용자 이름	Cleversafe에 로그인하는 데 사용되는 이름입니다
암호	Cleversafe에 로그인하는 데 사용되는 암호입니다

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	기본값은 60분입니다
HTTP 연결 시간 초과)	기본값은 60초입니다

IBM DS 데이터 소스

IBM DS(CLI) 데이터 소스는 DS6xxx 및 DS8xxx 디바이스만 지원합니다. DS3xxx, DS4xxx 및 DS5xxx 장치는 NetApp E-Series 데이터 소스에서 지원됩니다. 지원되는 모델 및 펌웨어 버전은 Insight 데이터 소스 지원 매트릭스를 참조하십시오.

용어

OnCommand Insight는 IBM DS 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
디스크 드라이브 모듈	디스크
스토리지 이미지	스토리지
익스텐트 풀	스토리지 풀
고정 블록 볼륨	볼륨

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 각 DS 배열의 IP 주소입니다
- 스토리지 표시 이름은 선택 사항이며 외관만 가능합니다
- 각 DS 어레이에 대한 읽기 전용 사용자 이름 및 암호

- Insight 서버에 설치된 타사 소프트웨어: IBM dscli
- 액세스 검증: 실행 `dscli` 사용자 이름 및 암호를 사용하는 명령입니다
- 포트 요구 사항: 80, 443 및 1750

구성

필드에 입력합니다	설명
DS 스토리지	DS Storage Host의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	DS CLI에 사용되는 이름입니다
암호	DS CLI에 사용되는 암호입니다
실행 파일 dscli.exe 경로	에 대한 전체 경로입니다 `dscli.exe`유틸리티.

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)
스토리지 표시 이름	IBM DS 스토리지 어레이의 이름입니다
재고 제외 장치	인벤토리 수집에서 제외할 장치 일련 번호의 쉼표로 구분된 목록입니다
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
성능 필터 유형	Include(포함): 목록의 장치에서만 수집된 데이터입니다. 제외: 이러한 장치에서 데이터가 수집되지 않습니다
성능 필터 장치 목록	성능 컬렉션에서 포함하거나 제외할 장치 ID의 쉼표로 구분된 목록입니다

IBM PowerVM 데이터 소스

IBM PowerVM(SSH) 데이터 소스는 HMC(하드웨어 관리 콘솔)에서 관리하는 IBM POWER 하드웨어 인스턴스에서 실행되는 가상 파티션에 대한 정보를 수집합니다. 구성의 경우 이 데이터 원본에서는 SSH를 통해 HMC에 로그인하기 위한 사용자 이름과 HMC 구성에 대한 보기 수준 권한이 필요합니다.

용어

OnCommand Insight는 IBM PowerVM 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
hdisk	가상 디스크
관리 대상 시스템	호스트
LPAR, VIO 서버	가상 머신
볼륨 그룹	데이터 저장소
물리적 볼륨	LUN을 클릭합니다

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- HMC(Hardware Management Console)의 IP 주소
- SSH를 통해 HMC에 대한 액세스를 제공하는 사용자 이름 및 암호
- 포트 요구 사항 SSH-22
- 모든 관리 시스템 및 논리 파티션 보안 도메인에 대한 권한을 봅니다

  또한 HMC 구성에 대한 보기 권한과 HMC 콘솔 보안 그룹화를 위한 VPD 정보를 수집할 수 있는 기능도 있어야 합니다. 또한 사용자는 논리 파티션 보안 그룹화를 통해 가상 IO 서버 명령 액세스를 허용해야 합니다. 작업자의 역할에서 시작하여 모든 역할을 제거하는 것이 가장 좋습니다. HMC의 읽기 전용 사용자는 AIX 호스트에서 프록시 명령을 실행할 권한이 없습니다.

- IBM 모범 사례는 두 개 이상의 HMCS를 통해 디바이스를 모니터링하는 것입니다. 이렇게 하면 OnCommand Insight에서 중복된 디바이스를 보고할 수 있으므로 이 데이터 수집기의 고급 구성에 있는 "장치 제외" 목록에 중복 디바이스를 추가하는 것이 좋습니다.

구성

* 필드 *	* 설명 *
HMC(Hardware Management Console) 주소입니다	PowerVM 하드웨어 관리 콘솔의 IP 주소 또는 정규화된 도메인 이름입니다
HMC 사용자	하드웨어 관리 콘솔의 사용자 이름입니다
암호	하드웨어 관리 콘솔에 사용되는 암호입니다

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
SSH 포트	SSH에서 PowerVM에 사용되는 포트입니다
SSH 프로세스 대기 시간 초과(초)	SSH 프로세스 시간 초과(기본값 600초)
재시도 횟수	인벤토리 재시도 횟수입니다
장치 제외	제외할 장치 ID 또는 표시 이름의 쉼표로 구분된 목록입니다

IBM SVC 데이터 소스

IBM SVC 데이터 소스는 SSH를 사용하여 인벤토리 및 성능 데이터를 수집하여 SVC 운영 체제를 실행하는 다양한 디바이스를 지원합니다. 지원되는 디바이스 목록에는 SVC, V7000, V5000 및 V3700과 같은 모델이 포함됩니다. 지원되는 모델 및 펌웨어 버전은 Insight 데이터 소스 지원 매트릭스를 참조하십시오.

용어

OnCommand Insight는 IBM SVC 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
드라이브	디스크
클러스터	스토리지
노드	스토리지 노드
Mdisk 그룹	스토리지 풀
vDisk를 선택합니다	볼륨
Mdisk	백엔드 LUN

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

재고 요건

- 각 SVC 클러스터의 IP 주소입니다
- 포트 22를 사용할 수 있습니다
- Insight에서 생성하거나 이미 SVC에서 사용 중인 키 쌍을 재사용하는 공개 키 및 개인 키 쌍

  기존 키 쌍을 재사용하는 경우 Putty 형식에서 OpenSSH 형식으로 변환해야 합니다.

- SVC 클러스터에 설치된 공개 키
- 개인 키는 데이터 소스에서 식별되어야 합니다
- 액세스 검증: 열기 `ssh` 개인 키를 사용하여 SVC 클러스터에 대한 세션입니다

> 타사 소프트웨어를 설치할 필요가 없습니다.

성능 요구사항

- SVC 콘솔은 모든 SVC 클러스터에 필수이며 SVC 검색 기반 패키지에 필요합니다.
- 관리 액세스 수준은 클러스터 노드에서 구성 노드로 성능 데이터 파일을 복사하는 경우에만 필요합니다.

> SVC Foundation Discovery Package에 이 액세스 수준이 필요하지 않으므로 SVC Foundation 사용자가 정상적으로 작동하지 않을 수 있습니다.

- 포트 22가 필요합니다
- 이 사용자에 대해 개인 및 공용 SSH 키를 생성하고 개인 키를 저장하여 획득 장치에서 액세스할 수 있도록 해야 합니다. SVC Foundation 사용자에게 적절한 권한이 있는 경우 동일한 사용자 및 키가 작동합니다. 인벤토리 및 성능 데이터에 동일한 SSH 키를 사용할 수 있습니다.
- SSH를 통해 SVC 클러스터에 접속하고 다음을 실행하여 데이터 수집을 활성화합니다. `svctask startstats -interval 1`

> 또는 SVC 관리 사용자 인터페이스를 사용하여 데이터 수집을 사용하도록 설정합니다.

상위 일련 번호가 설명되었습니다

일반적으로 Insight는 스토리지 어레이의 일련 번호 또는 개별 스토리지 노드의 일련 번호를 보고할 수 있습니다. 그러나 일부 스토리지 어레이 아키텍처는 이 문제에 완전히 부합되지 않습니다. SVC 클러스터는 1-4개의 어플라이언스로 구성될 수 있으며, 각 어플라이언스에는 2개의 노드가 있습니다. 어플라이언스 자체에 일련 번호가 있는 경우 해당 일련 번호는 클러스터나 노드의 일련 번호가 아닙니다.

개별 노드가 대규모 클러스터의 일부인 중간 어플라이언스/엔클로저 내에 있는 경우 스토리지 노드 객체의 "상위 일련 번호" 속성이 IBM SVC 스토리지에 맞게 채워집니다.

구성

* 필드 *	* 설명 *

클러스터 IP입니다	SVC 스토리지에 대한 정규화된 도메인 이름의 IP 주소입니다
자격 증명 유형을 지정하려면 '암호' 또는 'OpenSSH 키 파일'을 선택하십시오	SSH를 통해 장치에 연결하는 데 사용되는 자격 증명 유형입니다
재고 사용자 이름입니다	SVC CLI의 사용자 이름입니다
재고 암호	SVC CLI의 암호입니다
재고 개인 키에 대한 전체 경로	인벤토리 개인 키 파일의 전체 경로입니다
성능 사용자 이름입니다	성능 수집을 위한 SVC CLI의 사용자 이름입니다
성능 암호	성능 수집을 위한 SVC CLI의 암호입니다
성능 개인 키로 가는 전체 경로	성능 개인 키 파일의 전체 경로입니다

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)
장치 제외	인벤토리 수집에서 제외할 장치 ID의 쉼표로 구분된 목록입니다
SSH 프로세스 대기 시간 초과(초)	SSH 프로세스 시간 초과(기본값 200초)
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
성능 제외 장치	성능 컬렉션에서 제외할 장치 ID의 쉼표로 구분된 목록입니다
성능 SSH 프로세스 대기 시간 초과(초)	SSH 프로세스 시간 초과(기본값 200초)
덤프된 통계 파일 정리	덤프된 통계 파일을 정리하려면 선택합니다

IBM Tivoli Monitoring 데이터 소스

이 데이터 소스는 파일 시스템 사용에만 사용됩니다. Tivoli Monitoring Data Warehouse라고도 하는 Tivoli Monitoring Database와 직접 통신합니다. Oracle 및 DB2 데이터베이스가 지원됩니다.

Oracle 오류 메시지입니다

이 데이터 수집기는 OnCommand Insight 7.3.11부터 더 이상 사용할 수 없습니다.

지정된 SID로 인해 연결 시도 시 "ORA-12154"가 포함된 오류 메시지가 나타나는 경우 Oracle DB 네트워크 서비스 구성을 다시 확인하십시오. 액세스 구성에서 정규화된 호스트 이름(예: "names.default_domain")을 지정하는 경우 SID 필드에 정규화된 서비스 이름을 삽입하십시오. 간단한 예로 SID에 대한 연결을 들 수 있습니다 `testdb` 가 실패하고 Oracle 구성이 의 도메인을 지정합니다`company.com`. 연결을 시도하기 위해 기본 SID 대신 다음 문자열을 사용할 수 있습니다. `testdb.company.com`.

구성

필드에 입력합니다	설명
Tivoli 모니터링 데이터베이스 IP	Tivoli Monitoring 서버의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	Tivoli Monitoring 서버의 사용자 이름입니다
암호	Tivoli 모니터링 서버의 암호입니다

고급 구성

필드에 입력합니다	설명
Tivoli 모니터링 데이터베이스 포트	Tivoli 모니터링 데이터베이스에 사용되는 포트입니다
Oracle SID 또는 DB2 데이터베이스 이름입니다	Oracle 리스너 서비스 ID 또는 DB2 데이터베이스 이름입니다
재고 폴링 간격(분)	재고 조사 간격(기본값: 60분)
사용할 데이터베이스 드라이버	사용할 데이터베이스 드라이버를 선택합니다
데이터베이스에 연결하는 데 사용되는 프로토콜입니다	데이터베이스에 연결하는 데 사용되는 프로토콜입니다
데이터베이스 스키마	데이터베이스 스키마를 입력합니다

IBM TotalStorage DS4000 데이터 소스

이 데이터 소스는 인벤토리 및 성능 정보를 수집합니다. 두 가지 구성(펌웨어 6.x 및 7.x+)이 있으며 두 구성 모두 동일한 값을 갖습니다. API는 볼륨 데이터 통계를 수집합니다.

구성

* 필드 *	* 설명 *

쉼표로 구분된 Array SANtricity 컨트롤러 IP 목록입니다	쉼표로 구분된 컨트롤러의 IP 주소 또는 정규화된 도메인 이름입니다

요구 사항

- 각 DS5 또는 FAStT 스토리지의 IP 주소입니다
- 액세스 검증: 각 어레이에서 두 컨트롤러의 IP 주소를 Ping(핑)합니다.

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 30분)
성능 폴링 간격(최대 3600초)	성능 폴링 간격(기본값 300초)

IBM XIV 데이터 소스

IBM XIV(CLI) 데이터 소스 인벤토리는 XIV 명령줄 인터페이스를 사용하여 수행됩니다. XIV 성능은 포트 5989에서 SMI-S 공급자를 실행하는 XIV 스토리지에 대한 SMI-S 호출을 통해 구현됩니다.

용어

OnCommand Insight는 IBM XIV 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
디스크	디스크
스토리지 시스템	스토리지
스토리지 풀	스토리지 풀
볼륨	볼륨

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 포트 요구 사항: TCP 포트 7778
- XIV 관리 인터페이스의 IP 주소입니다

- 읽기 전용 사용자 이름 및 암호
- XIV CLI는 Insight 서버 또는 RAU에 설치해야 합니다
- 액세스 검증: 사용자 이름과 암호를 사용하여 Insight 서버에서 XIV 사용자 인터페이스에 로그인합니다.

구성

* 필드 *	* 설명 *
IP 주소	XIV 스토리지의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	XIV 스토리지의 사용자 이름입니다
암호	XIV 스토리지의 암호입니다
XIV CLI 디렉토리의 전체 경로입니다	XIV CLI 디렉토리의 전체 경로입니다

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)
CLI 프로세스 대기 시간 초과(ms)	CLI 프로세스 시간 초과(기본 7200000ms)
SMI-S 호스트 IP입니다	SMI-S Provider 호스트의 IP 주소입니다
SMI-S 포트	SMI-S Provider 호스트에서 사용하는 포트입니다
SMI-S 프로토콜	SMI-S 공급자에 연결하는 데 사용되는 프로토콜입니다
SMI-S 네임스페이스	SMI-S 네임스페이스
사용자 이름	SMI-S Provider 호스트의 사용자 이름입니다
암호	SMI-S Provider 호스트의 암호입니다
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
SMI-S 연결 재시도 횟수	SMI-S 연결 재시도 횟수입니다

Infinidat .NET 데이터 소스

Infinidat .NET(HTTP) 데이터 소스는 Infinidat Microsoft .NET Framework 스토리지로부터 정보를 수집하는 데 사용됩니다. 따라서, 귀하는 반드시 서비스 플랫폼 관리 노드에 대한 액세스

권한이 있어야 합니다.

용어

OnCommand Insight는 다음과 같은 인벤토리 정보를 데이터 소스에서 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
드라이브	디스크
상자	스토리지
노드	스토리지 노드
수영장	스토리지 풀
볼륨	볼륨
FC 포트	포트
파일 시스템	내부 볼륨
파일 시스템	파일 공유
파일 시스템 내보내기	공유

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

구성

필드에 입력합니다	설명
서비스 박스 호스트	IP 주소 또는 Management Node의 정규화된 도메인 이름입니다
사용자 이름	작업 영역 관리 노드에 대한 사용자 이름입니다
암호	작업 영역 관리 노드에 대한 암호입니다

고급 구성

필드에 입력합니다	설명

TCP 포트	TCP 포트 - Microsoft Windows Server에 연결하는 데 사용됩니다(기본 443).
재고 폴링 간격(분)	재고 조사 간격(기본값: 60분)
연결 시간 초과	연결 시간 초과(기본값 60초)

Microsoft Azure 컴퓨팅 데이터 소스

OnCommand Insights는 Azure 컴퓨팅 데이터 수집기를 사용하여 Azure 컴퓨팅 인스턴스에서 인벤토리 및 성능 데이터를 가져옵니다.

요구 사항

이 데이터 수집기를 구성하려면 다음 정보가 필요합니다.

- 포트 요구 사항: 443 HTTPS
- Azure 관리 REST IP(management.azure.com)
- Azure 서비스 주 응용 프로그램(클라이언트) ID(사용자 계정)
- Azure Service Principal Authentication 키(사용자 암호)

Insight 검색을 위해 Azure 계정을 설정해야 합니다. 계정이 올바르게 구성되고 Azure에 애플리케이션을 등록하면 Insight에서 Azure 인스턴스를 검색하는 데 필요한 자격 증명이 제공됩니다. 다음 링크에서는 검색을 위해 계정을 설정하는 방법에 대해 설명합니다. https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

구성

아래 표에 따라 데이터 원본 필드에 데이터를 입력합니다.

필드에 입력합니다	설명
Azure 서비스 주 응용 프로그램(클라이언트) ID(리더 역할 필요)	Azure에 로그인 ID를 입력합니다. 리더 역할 액세스가 필요합니다.
Azure 테넌트 ID입니다	Microsoft 테넌트 ID입니다
Azure 서비스 주 인증 키	로그인 인증 키
API 요청에 대한 Microsoft의 청구서를 알고 있습니다	Insight 폴링을 통해 API 요청이 접수된다는 사실을 알고 있는지 확인하려면 이 확인란을 선택하십시오.

고급 구성

아래 표에 따라 데이터 원본 필드에 데이터를 입력합니다.

필드에 입력합니다	설명
재고 폴링 간격(분)	기본값은 60입니다
태그별로 VM 필터링에 적용하려면 '제외' 또는 '포함'을 선택합니다	데이터를 수집할 때 태그별로 VM을 포함할지 제외할지 여부를 지정합니다. "포함"을 선택하면 태그 키 필드를 비워둘 수 없습니다.
태그 키 및 VM을 필터링할 값	VM의 키 및 태그 값과 일치하는 키 및 값을 필터링하여 포함/제외할 VM(및 관련 디스크)을 선택하려면 * + 필터 태그 * 를 클릭합니다. 태그 키는 필수이며 태그 값은 선택 사항입니다. 태그 값이 비어 있으면 태그 키와 일치하는 한 VM이 필터링됩니다.
성능 폴링 간격(초)	

Azure NetApp Files 데이터 소스

이 데이터 소스는 ANF(Azure NetApp Files)에 대한 인벤토리 및 성능 데이터를 가져옵니다.

요구 사항

다음은 이 데이터 소스를 구성하기 위한 요구 사항입니다.

- 포트 요구 사항: 443 HTTPS
- Azure 관리 REST IP(management.azure.com)
- Azure 서비스 주 응용 프로그램(클라이언트) ID(사용자 계정)
- Azure Service Principal 인증 키(사용자 암호)
- Cloud Insights 검색을 위해 Azure 계정을 설정해야 합니다.

  계정이 올바르게 구성되고 Azure에 애플리케이션을 등록하면 Cloud Insights로 Azure 인스턴스를 검색하는 데 필요한 자격 증명이 제공됩니다. 다음 링크에서는 검색을 위해 계정을 설정하는 방법에 대해 설명합니다.

  https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

구성

필드에 입력합니다	설명
Azure 서비스 주 응용 프로그램(클라이언트) ID입니다	Azure에 로그인 ID를 입력합니다
Azure 테넌트 ID입니다	Azure 테넌트 ID입니다
Azure 서비스 주 인증 키	로그인 인증 키

API 요청에 대한 Microsoft의 청구서를 알고 있습니다	Insight 폴링을 통해 API 요청이 접수된다는 사실을 알고 있는지 확인하려면 이 확인란을 선택하십시오.

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	기본값은 60분입니다

Microsoft Hyper-V 데이터 소스

구성의 경우 Microsoft Hyper-V 데이터 원본에는 물리적 호스트(하이퍼바이저)의 IP 주소 또는 확인 가능한 DNS 이름이 필요합니다. 이 데이터 소스는 Powershell(이전에 사용한 WMI)을 사용합니다.

용어

OnCommand Insight는 Hyper-V 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
가상 하드 디스크	가상 디스크
호스트	호스트
가상 머신	가상 머신
CSV(Cluster Shared Volumes), 파티션 볼륨	데이터 저장소
인터넷 SCSI 장치, 다중 경로 SCSI LUN	LUN을 클릭합니다
Fibre Channel 포트	포트

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- Hyper-V를 사용하려면 데이터 수집 및 원격 액세스/관리를 위해 포트 5985를 열어야 합니다.
- 클러스터링 그룹 노드의 IP 주소입니다
- 하이퍼바이저의 로컬 관리자 사용자 및 암호
- 관리 수준 사용자 계정

- 포트 요구 사항: Windows 2003 및 이전 버전의 경우 포트 135 및 동적 TCP 포트 1024-65535와 Windows 2008의 경우 49152-65535가 할당됩니다.
- 데이터 수집기가 IP 주소만 가리키는 경우에도 DNS 확인이 성공해야 합니다.
- 각 Hyper-V 하이퍼바이저에는 모든 호스트의 모든 VM에 대해 "리소스 계측"이 켜져 있어야 합니다. 따라서 각 하이퍼바이저마다 각 게스트에서 Cloud Insights에 사용할 수 있는 데이터가 더 많아집니다. 이 옵션을 설정하지 않으면 각 게스트에 대해 더 적은 성능 메트릭이 획득됩니다. 리소스 측정에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

  "Hyper-V 리소스 측정 개요"

  "활성화 - VMResourceMetering"

구성

* 필드 *	* 설명 *
물리적 호스트 IP 주소입니다	물리적 호스트(하이퍼바이저)의 IP 주소 또는 정규화된 도메인 이름
사용자 이름	관리자 사용자 이름은 하이퍼바이저를 수행합니다
암호	하이퍼바이저의 암호입니다
NT 도메인	클러스터의 노드에서 사용하는 DNS 이름입니다

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
연결 시간 초과(ms)	연결 시간 초과(기본값 60000ms)

NetApp clustered Data ONTAP 데이터 소스

이 데이터 소스는 clustered Data ONTAP을 사용하는 스토리지 시스템에 사용해야 하며 읽기 전용 API 호출에 사용되는 관리자 계정이 필요합니다.

용어

OnCommand Insight는 clustered Data ONTAP 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다

디스크	디스크
RAID 그룹	디스크 그룹
클러스터	스토리지
노드	스토리지 노드
집계	스토리지 풀
LUN을 클릭합니다	볼륨
볼륨	내부 볼륨

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 읽기 전용 API 호출에 사용되는 관리자 계정입니다
- 타겟 IP는 클러스터 관리 LIF입니다
- NetApp 클러스터에 로그인할 수 있는 사용자 이름(읽기 전용 역할 이름을 ontapi 애플리케이션에 기본 SVM으로 지정) 및 암호
- 포트 요구 사항: 80 또는 443
- 라이센스 요구사항: 검색에 필요한 FCP 라이센스 및 매핑/마스킹된 볼륨

구성

* 필드 *	* 설명 *
NetApp 관리 IP	NetApp 클러스터의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	NetApp 클러스터의 사용자 이름입니다
암호	NetApp 클러스터의 암호입니다

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)

성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

Clustered Data ONTAP 스토리지

NetApp clustered Data ONTAP 스토리지 자산 랜딩 페이지에서 오브젝트 또는 레퍼런스에 적용되는 용어입니다.

Clustered Data ONTAP 스토리지 용어

다음 용어는 NetApp clustered Data ONTAP 스토리지 자산 랜딩 페이지에서 찾을 수 있는 오브젝트 또는 참조에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

- 모델 — 이 클러스터 내에서 고유한 개별 노드 모델 이름을 쉼표로 구분한 목록입니다. 클러스터의 모든 노드가 동일한 모델 유형인 경우 하나의 모델 이름만 표시됩니다.
- 공급업체 — 새 데이터 원본을 구성하는 경우 동일한 공급업체 이름입니다.
- 일련 번호 — 스토리지 일련 번호입니다. NetApp clustered Data ONTAP과 같은 클러스터 아키텍처 스토리지 시스템에서는 이 일련 번호가 개별 "스토리지 노드" 일련 번호보다 덜 유용할 수 있습니다.
- IP — 일반적으로 데이터 소스에 구성된 IP 또는 호스트 이름이 됩니다.
- 마이크로코드 버전 — 펌웨어.
- Raw Capacity - - 역할에 관계없이 시스템의 모든 물리적 디스크에 대한 기본 2개의 합계입니다.
- 지연 시간 — 읽기 및 쓰기 모두에서 호스트에서 발생하는 워크로드를 나타냅니다. 이상적으로는 OCI가 이 가치를 직접 소싱하지만 이 아닌 경우가 많습니다. 이러한 업적을 제공하는 스토리지 대신, OCI는 일반적으로 개별 내부 볼륨 "" 통계에서 파생된 IOP 가중 계산을 수행합니다.
- Throughput - 내부 볼륨에서 집계된 것입니다.
- 관리 — 장치의 관리 인터페이스에 대한 하이퍼링크가 포함될 수 있습니다. 인벤토리 보고의 일부로 Insight 데이터 소스에 의해 프로그래밍 방식으로 만들어집니다.

Clustered Data ONTAP 스토리지 풀

NetApp clustered Data ONTAP 스토리지 풀 자산 랜딩 페이지에서 오브젝트 또는 레퍼런스에 적용되는 용어입니다.

Clustered Data ONTAP 스토리지 풀 용어

다음 용어는 NetApp clustered Data ONTAP 스토리지 풀 자산 랜딩 페이지에서 볼 수 있는 오브젝트 또는 참조에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

- 스토리지 — 이 풀이 상주하는 스토리지 배열입니다. 필수입니다.
- 형식 — 가능성 목록 목록의 설명 값입니다. 가장 흔히 "집계" 또는 "RAID 그룹""이 됩니다.
- 노드 — 이 스토리지 시스템의 아키텍처가 특정 스토리지 노드에 속해 있는 경우 이 스토리지 시스템의 이름은 해당 랜딩 페이지의 하이퍼링크로 표시됩니다.
- Flash Pool 사용 — 예/아니요 가치 — 이 SATA/SAS 기반 풀에 캐싱 가속화에 SSD가 사용됩니까?
- 중복 — RAID 레벨 또는 보호 체계입니다. RAID_DP는 이중 패리티이고, RAID_TP는 삼중 패리티입니다.

- 용량 — 이 값은 사용된 논리적 용량, 가용 용량 및 총 논리적 용량 및 이 용량 전체에서 사용된 비율입니다.
- 과도하게 커밋된 용량 — 효율성 기술을 사용하여 스토리지 풀의 논리적 용량보다 큰 볼륨 또는 내부 볼륨 용량의 합계를 할당한 경우 여기에 있는 백분율 값은 0%보다 큽니다.
- 스냅샷 — 사용 중인 스냅샷 용량 및 총 용량. 스토리지 풀 아키텍처가 용량의 일부를 스냅샷용 영역으로 세그먼트하는 경우 MetroCluster 구성의 ONTAP는 이 문제를 나타낼 가능성이 높지만, 다른 ONTAP 구성은 더 적습니다.
- Utilization — 이 스토리지 풀에 용량을 제공하는 모든 디스크의 사용 중 가장 높은 비율을 나타내는 백분율입니다. 디스크 사용률이 반드시 스토리지 성능과 강력한 상관 관계가 있는 것은 아닙니다. 호스트 기반 워크로드가 없을 경우 디스크 재구축, 중복 제거 작업 등으로 인해 사용률이 높을 수 있습니다. 또한 많은 스토리지 "" 복제 구현으로 인해 내부 볼륨 또는 볼륨 작업 부하로 표시되지 않는 동안 디스크 사용률이 발생할 수 있습니다.
- IOPS — 이 스토리지 풀에 용량을 제공하는 모든 디스크의 IOPS 합계입니다.
- Throughput - - 이 스토리지 풀에 용량을 제공하는 모든 디스크의 총 처리량입니다.

Clustered Data ONTAP 스토리지 노드

NetApp clustered Data ONTAP 스토리지 노드 자산 랜딩 페이지에서 찾을 수 있는 오브젝트 또는 참조에 적용되는 용어입니다.

Clustered Data ONTAP 스토리지 노드 용어

다음 용어는 NetApp clustered Data ONTAP 스토리지 풀 자산 랜딩 페이지에서 찾을 수 있는 오브젝트 또는 참조에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

- 스토리지 — 이 노드가 속하는 스토리지 시스템입니다. 필수입니다.
- HA 파트너 — 노드가 1개 노드로 페일오버되고 다른 1개 노드만 장애 조치되는 플랫폼에서는 일반적으로 이 노드에 표시됩니다.
- State — 노드의 상태입니다. 배열이 데이터 소스에 의해 인벤토리를 작성할 수 있을 만큼 양호한 경우에만 사용할 수 있습니다.
- 모델 — 노드의 모델 이름입니다.
- Version — 디바이스의 버전 이름입니다.
- 일련 번호 — 노드 일련 번호입니다.
- 메모리 — 베이스 2 메모리(있는 경우)
- 활용률 — ONTAP에서 이것은 독점 알고리즘의 컨트롤러 스트레스 인덱스입니다. 성능 폴링이 발생할 때마다 WAFL 디스크 경합 또는 평균 CPU 사용률의 증가인 0에서 100% 사이의 숫자가 보고됩니다. 값이 50%를 초과하는 경우 이는 낮은 크기 조정을 나타내는 것입니다. 컨트롤러/노드가 충분히 크지 않거나 회전 디스크가 부족하여 쓰기 워크로드를 흡수할 수 없습니다.
- IOPS — 노드 개체에 대해 ONTAP ZAPI 호출에서 직접 파생됩니다.
- 지연 시간 — 노드 개체에 대해 ONTAP ZAPI 호출에서 직접 파생됩니다.
- 처리량 — 노드 개체에서 ONTAP ZAPI 호출에서 직접 파생됩니다.
- 프로세서 — CPU 수입니다.

Unified Manager 데이터 소스를 위한 **NetApp clustered Data ONTAP**

이 데이터 소스는 UM(Unified Manager) 6.0+ 데이터베이스에서 ONTAP 8.1.x 데이터를 수집합니다. Insight는 이 데이터 소스를 사용하여 UM에서 구성 및 채워진 모든 클러스터를 검색합니다. 효율성을 위해 Insight는 클러스터 자체의 ZAPI를 호출하지 않습니다. 이 데이터 원본에서는 성능이 지원되지 않습니다.

구성

이 데이터 수집기는 OnCommand Insight 7.3.11부터 더 이상 사용할 수 없습니다.

* 필드 *	* 설명 *
Unified Manager IP를 참조하십시오	Unified Manager의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	Unified Manager의 사용자 이름입니다
암호	Unified Manager의 암호입니다
포트	Unified Manager와의 통신에 사용되는 포트(기본값 3306)

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 15분)
클러스터 제외	제외할 클러스터 IP의 쉼표로 구분된 목록입니다

7-Mode 데이터 소스에서 작동하는 **NetApp Data ONTAP**

7-Mode에서 작동하는 Data ONTAP 소프트웨어를 사용하는 스토리지 시스템의 경우, 용량 번호를 얻기 위해 CLI를 사용하는 ONTAPI 데이터 소스를 사용해야 합니다.

용어

OnCommand Insight는 NetApp Data ONTAP 7-Mode 데이터 소스에서 다음 인벤토리 정보를 수집합니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
디스크	디스크

RAID 그룹	디스크 그룹
파일러	스토리지
파일러	스토리지 노드
집계	스토리지 풀
LUN을 클릭합니다	볼륨
볼륨	내부 볼륨

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- FAS 스토리지 컨트롤러 및 파트너의 IP 주소입니다
- 포트 443
- 컨트롤러 및 파트너의 사용자 이름 및 암호
- 7-Mode에서 다음 역할 기능을 지원하는 컨트롤러 및 파트너 컨트롤러에 대한 사용자 지정 관리자 레벨 사용자 이름 및 암호:
  - "API- *": OnCommand Insight에서 모든 NetApp 스토리지 API 명령을 실행할 수 있도록 허용합니다.
  - "login-http-admin": OnCommand Insight이 HTTP를 통해 NetApp 스토리지에 연결할 수 있도록 허용하려면 이 옵션을 사용하십시오.
  - "security-api-vFiler": OnCommand Insight가 NetApp 스토리지 API 명령을 실행하여 vFiler 유닛 정보를 검색할 수 있도록 합니다.
  - "CLI-options": 스토리지 시스템 옵션을 읽으려면 이 옵션을 사용합니다.
  - "CLI-LUN": LUN 관리를 위한 다음 명령에 액세스합니다. 지정된 LUN 또는 LUN 클래스의 상태(LUN 경로, 크기, 온라인/오프라인 상태 및 공유 상태)를 표시합니다.
  - "CLI-df": 사용 가능한 디스크 공간을 표시하려면 이 옵션을 사용합니다.
  - "CLI-ifconfig": 인터페이스 및 IP 주소를 표시하려면 이 옵션을 사용합니다.

구성

* 필드 *	* 설명 *
파일러 주소	NetApp Filer의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	NetApp Filer의 사용자 이름입니다
암호	NetApp Filer 암호

클러스터에 있는 HA 파트너 파일러의 주소입니다	HA 파트너 파일러의 IP 주소 또는 정규화된 도메인 이름입니다
클러스터에 있는 HA 파트너 파일러의 사용자 이름입니다	NetApp HA 파트너 파일러의 사용자 이름입니다
클러스터에 있는 HA 파트너 파일러의 암호	NetApp HA 파트너 파일러의 암호입니다

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
연결 유형	연결 유형을 선택합니다
연결 포트	NetApp API에 사용되는 포트입니다
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

스토리지 시스템 접속입니다

이 데이터 원본에 대한 기본 관리 사용자를 사용하는 대신 NetApp 스토리지 시스템에서 직접 관리 권한을 가진 사용자를 구성하여 데이터 원본이 NetApp 스토리지 시스템에서 데이터를 가져올 수 있도록 할 수 있습니다.

NetApp 스토리지 시스템에 연결하려면 스토리지 시스템이 있는 기본 pfiler를 획득할 때 지정된 사용자가 다음 조건을 충족해야 합니다.

- 사용자는 vfiler0(루트 파일러/pfiler)에 있어야 합니다.

  스토리지 시스템은 기본 pfiler를 획득할 때 획득됩니다.

- 다음 명령은 사용자 역할 기능을 정의합니다.
  - "API- *": OnCommand Insight에서 모든 NetApp 스토리지 API 명령을 실행할 수 있도록 허용합니다. ZAPI를 사용하려면 이 명령이 필요합니다.
  - "login-http-admin": OnCommand Insight이 HTTP를 통해 NetApp 스토리지에 연결할 수 있도록 허용하려면 이 옵션을 사용하십시오. ZAPI를 사용하려면 이 명령이 필요합니다.
  - "security-api-vFiler": OnCommand Insight가 NetApp 스토리지 API 명령을 실행하여 vFiler 유닛 정보를 검색할 수 있도록 합니다.
  - "CLI-options": "options" 명령에 대해 사용되며 파트너 IP 및 활성화된 라이센스에 사용됩니다.
  - "CLI-LUN": LUN 관리를 위해 다음 명령을 사용합니다. 지정된 LUN 또는 LUN 클래스의 상태(LUN 경로, 크기, 온라인/오프라인 상태 및 공유 상태)를 표시합니다.
  - "CLI-df": "df-s", "df-r", "df-a-r" 명령의 경우 및 사용 가능한 공간을 표시하는 데 사용됩니다.
  - "CLI-ifconfig": "ifconfig -a" 명령용이며 파일러 IP 주소를 가져오는 데 사용됩니다.
  - "CLI-rdfile": "rdfile /etc/netgroup" 명령에 대해, 넷그룹을 가져오는 데 사용됩니다.

- "CLI-date": "date" 명령을 기준으로, 스냅샷 복사본을 얻기 위한 전체 날짜를 얻는 데 사용됩니다.
- "CLI-snap": "snap list" 명령에 사용되며 스냅샷 복사본을 가져오는 데 사용됩니다.

CLI-date 또는 CLI-snap 권한이 제공되지 않는 경우, 획득이 완료될 수 있지만 스냅샷 복사본은 보고되지 않습니다.

7-Mode 데이터 소스를 성공적으로 획득하고 스토리지 시스템에 경고가 표시되지 않도록 하려면 다음 명령 문자열 중 하나를 사용하여 사용자 역할을 정의해야 합니다. 여기에 나열된 두 번째 문자열은 첫 번째 문자열의 간소화된 버전입니다.

```
login-http-admin,api-*,security-api-vfile,cli-rdfile,cli-options,cli-
df,cli-lun,cli-ifconfig,cli-date,cli-snap,
or
login-http-admin,api-*,security-api-vfile,cli-*
```

NetApp E-Series 데이터 소스

NetApp E-Series 데이터 소스에서 인벤토리 및 성능 정보를 수집합니다. 두 가지 구성(펌웨어 6.x 및 펌웨어 7.x+)이 있으며 두 구성 모두 동일한 값을 갖습니다.

용어

OnCommand Insight는 NetApp E-Series 데이터 소스에서 다음 인벤토리 정보를 수집합니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
드라이브	디스크
볼륨 그룹	디스크 그룹
스토리지	스토리지
컨트롤러	스토리지 노드
볼륨 그룹	스토리지 풀
볼륨	볼륨

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 어레이에 있는 각 컨트롤러의 IP 주소입니다

- 포트 요구 사항 2463

구성

* 필드 *	* 설명 *
쉼표로 구분된 Array SANtricity 컨트롤러 IP 목록입니다	스토리지 컨트롤러의 IP 주소 및/또는 정규화된 도메인 이름입니다

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 30분)
성능 폴링 간격(최대 3600초)	성능 폴링 간격(기본값 300초)

E-Series 스토리지

NetApp E-Series 스토리지 자산 랜딩 페이지에서 찾을 수 있는 오브젝트 또는 참조에 적용되는 용어입니다.

E-Series 스토리지 용어

다음 용어는 NetApp E-Series 스토리지 자산 랜딩 페이지에서 볼 수 있는 오브젝트 또는 참조 자료에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

- 모델 — 장치의 모델 이름입니다.
- 공급업체 — 새 데이터 원본을 구성하는 경우 동일한 공급업체 이름입니다.
- 일련 번호 — 스토리지 일련 번호입니다. NetApp clustered Data ONTAP과 같은 클러스터 아키텍처 스토리지 시스템에서는 이 일련 번호가 개별 "스토리지 노드" 일련 번호보다 덜 유용할 수 있습니다.
- IP — 일반적으로 데이터 소스에 구성된 IP 또는 호스트 이름이 됩니다.
- 마이크로코드 버전 — 펌웨어.
- Raw Capacity - - 역할에 관계없이 시스템의 모든 물리적 디스크에 대한 기본 2개의 합계입니다.
- 지연 시간 — 읽기 및 쓰기 모두에서 호스트에서 발생하는 워크로드를 나타냅니다. Insight는 스토리지의 볼륨에서 파생된 IOPS 가중 평균을 계산합니다.
- Throughput — 스토리지의 총 호스트 처리량입니다. Insight는 이 값을 도출하기 위해 볼륨 "의 처리량을 합산합니다.
- 관리 — 장치의 관리 인터페이스에 대한 하이퍼링크가 포함될 수 있습니다. 인벤토리 보고의 일부로 Insight 데이터 소스에 의해 프로그래밍 방식으로 만들어집니다.

E-Series 스토리지 풀

NetApp E-Series 스토리지 풀 자산 랜딩 페이지에서 확인할 수 있는 오브젝트 또는 참조에 적용되는 용어입니다.

E-Series 스토리지 풀 용어

다음 용어는 NetApp E-Series 스토리지 풀 자산 랜딩 페이지에서 볼 수 있는 오브젝트 또는 참조 자료에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

- 스토리지 — 이 풀이 상주하는 스토리지 배열입니다. 필수입니다.
- 형식 — 가능성 목록 목록의 설명 값입니다. 가장 일반적인 것은 "씬 프로비저닝" 또는 "RAID 그룹"입니다.
- 노드 — 이 스토리지 시스템의 아키텍처가 특정 스토리지 노드에 속해 있는 경우 이 스토리지 시스템의 이름은 해당 랜딩 페이지의 하이퍼링크로 표시됩니다.
- Flash Pool 사용 — 예/아니요 값
- 중복 — RAID 레벨 또는 보호 체계입니다. DDP 풀에 대한 E-Series의 보고서 "'RAID 7".
- 용량 — 이 값은 사용된 논리적 용량, 가용 용량 및 총 논리적 용량 및 이 용량 전체에서 사용된 비율입니다. 이러한 값에는 E-Series의 "보존" 용량이 모두 포함되어 있어 E-Series의 사용자 인터페이스에서 표시할 수 있는 용량보다 숫자 및 백분율이 높습니다.
- 과도하게 커밋된 용량 — 효율성 기술을 사용하여 스토리지 풀의 논리적 용량보다 큰 총 볼륨 용량을 할당한 경우 여기에 있는 백분율 값은 0%보다 큽니다.
- 스냅샷 — 사용 중인 스냅샷 용량 및 총 용량. 스토리지 풀 아키텍처가 용량의 일부를 스냅샷용 영역으로 세그먼트하는 경우
- Utilization — 이 스토리지 풀에 용량을 제공하는 디스크 사용량이 가장 높은 비율을 나타내는 백분율입니다. 디스크 사용률이 반드시 스토리지 성능과 강력한 상관관계가 있는 것은 아닙니다. 호스트 기반 워크로드가 없을 경우 디스크 리빌드, 중복 제거 작업 등으로 인해 사용률이 높을 수 있습니다. 또한 많은 스토리지 "" 복제 구현으로 인해 볼륨 작업 부하로 표시되지 않는 동안 디스크 사용률이 발생할 수 있습니다.
- IOPS — 이 스토리지 풀에 용량을 제공하는 모든 디스크의 IOPS 합계입니다.
- Throughput - - 이 스토리지 풀에 용량을 제공하는 모든 디스크의 총 처리량입니다.

E-Series 스토리지 노드

NetApp E-Series 스토리지 노드 자산 랜딩 페이지에서 찾을 수 있는 오브젝트 또는 참조에 적용되는 용어입니다.

E-Series 스토리지 노드 용어

다음 용어는 NetApp E-Series 스토리지 풀 자산 랜딩 페이지에서 볼 수 있는 오브젝트 또는 참조 자료에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

- 스토리지 — 이 노드가 속하는 스토리지 시스템입니다. 필수입니다.
- HA 파트너 — 노드가 1개 노드로 페일오버되고 다른 1개 노드만 장애 조치되는 플랫폼에서는 일반적으로 이 노드에 표시됩니다.
- State — 노드의 상태입니다. 배열이 데이터 소스에 의해 인벤토리를 작성할 수 있을 만큼 양호한 경우에만 사용할 수 있습니다.
- 모델 — 노드의 모델 이름입니다.
- Version — 디바이스의 버전 이름입니다.
- 일련 번호 — 노드 일련 번호입니다.
- 메모리 — 베이스 2 메모리(있는 경우)

- Utilization — 현재 NetApp E-Series에서 사용할 수 없습니다.
- IOPS — 이 노드에만 속하는 볼륨의 모든 IOP를 합산하여 계산됩니다.
- 지연 시간 — 이 컨트롤러의 일반적인 호스트 지연 시간 또는 응답 시간을 나타내는 숫자입니다. Insights는 이 노드에만 속하는 볼륨에서 IOPS 가중 평균을 계산합니다.
- 처리량 — 이 컨트롤러의 호스트 기반 처리량을 나타내는 숫자입니다. 이 노드에만 속하는 볼륨에 대한 모든 처리량을 합산하여 계산됩니다.
- 프로세서 — CPU 수입니다.

NetApp 호스트 및 **VM** 파일 시스템 데이터 소스

NetApp 호스트 및 VM 파일 시스템 데이터 소스를 사용하여 모든 Microsoft Windows 호스트 및 VM(가상 머신) 파일 시스템과 지원되는 모든 Linux VM(가상 매핑된 것에만 해당)에 대한 파일 시스템 세부 정보 및 스토리지 리소스 매핑을 검색할 수 있습니다. 구성된 CRG(Compute Resource Group)로 주석이 추가된 Insight 서버의 기존

일반 요구 사항

- 이 기능은 별도로 구입해야 합니다.

  도움이 필요하면 Insight 담당자에게 문의하십시오.

- Insight Support Matrix를 확인하여 호스트 또는 가상 머신 운영 체제가 지원되는지 확인해야 합니다.

  파일 시스템에서 스토리지 리소스로의 링크가 생성되었는지 확인하려면 관련 스토리지 또는 가상화 공급업체 유형 및 버전이 필요한 볼륨 또는 가상 디스크 식별 데이터를 보고하는지 확인하십시오.

Microsoft Windows 요구 사항

- 이 데이터 소스는 WMI(Window Management Instrumentation) 데이터 구조를 사용하여 데이터를 검색합니다.

  이 서비스는 원격으로 작동하고 사용 가능해야 합니다. 특히, 포트 135에 액세스할 수 있어야 하며 방화벽 뒤에 있는 경우 열어야 합니다.

- Windows 도메인 사용자는 WMI 구조에 액세스할 수 있는 적절한 권한이 있어야 합니다.
- 관리자 권한이 필요합니다.
- Windows 2003 및 이전 버전에서 1024-65535로 할당된 동적 TCP 포트
- Windows 2008의 경우 포트 49152 - -65535

> 일반적으로 Insight, AU 및 이 데이터 소스 간에 방화벽을 사용하려고 할 때 Microsoft 팀에 문의하여 필요한 포트를 확인해야 합니다.

Linux 요구 사항

- 이 데이터 소스는 SSH(Secure Shell) 연결을 사용하여 Linux VM에서 명령을 실행합니다.

  SSH 서비스가 운영되어야 하며 원격으로 이용할 수 있어야 합니다. 특히, 포트 22에 액세스할 수 있어야 하며 방화벽 뒤에 있는 경우 열어야 합니다.

- SSH 사용자는 sudo 권한이 있어야 Linux VM에서 읽기 전용 명령을 실행할 수 있습니다.

  동일한 암호를 사용하여 SSH에 로그인하고 sudo 암호 챌린지에 응답해야 합니다.

사용 권장 사항

- 동일한 Compute Resource Group 주석을 사용하여 공통 운영 체제 자격 증명이 있는 호스트 및 가상 시스템 그룹에 주석을 추가해야 합니다.

  각 그룹에는 이러한 호스트 및 가상 시스템에서 파일 시스템 세부 정보를 검색하는 이 데이터 소스의 인스턴스가 있습니다.

- 성공률이 낮은 이 데이터 소스의 인스턴스가 있는 경우(예: OnCommand Insight가 그룹에 있는 1000개의 호스트 및 가상 머신 중 50개에 대한 파일 시스템 세부 정보를 검색하는 경우), 검색이 성공한 호스트와 가상 머신을 별도의 컴퓨팅 리소스 그룹으로 이동해야 합니다.

구성

필드에 입력합니다	설명
사용자 이름	운영 체제 사용자 Windows 운영 체제 사용자의 파일 시스템 데이터를 검색할 수 있는 적절한 권한이 있어야 합니다. 여기에는 도메인 접두사가 포함되어야 합니다.
암호	운영 체제 사용자의 암호입니다
컴퓨팅 리소스 그룹	데이터 소스에 대한 호스트 및 가상 머신에 플래그를 지정하는 데 사용되는 주석 값은 파일 시스템을 검색합니다. 빈 값은 데이터 소스가 현재 Compute Resource Group(계산 리소스 그룹)으로 주석이 추가되지 않은 모든 호스트 및 가상 시스템에 대한 파일 시스템을 검색함을 나타냅니다.

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 360분)

NetApp SolidFire 데이터 소스

NetApp SolidFire 데이터 소스는 인벤토리 및 성능 수집을 위해 iSCSI와 파이버 채널 SolidFire 구성을 모두 지원합니다.

SolidFire 데이터 소스는 SolidFire REST API를 사용합니다. 데이터 소스가 상주하는 획득 장치에서는 SolidFire 클러스터 관리 IP 주소의 TCP 포트 443에 대한 HTTPS 연결을 시작할 수 있어야 합니다. 데이터 원본에는 SolidFire 클러스터에서 REST API 쿼리를 수행할 수 있는 자격 증명이 필요합니다.

용어

OnCommand Insight는 NetApp SolidFire 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
드라이브	디스크
클러스터	스토리지
노드	스토리지 노드
볼륨	볼륨
Fibre Channel 포트	포트
볼륨 액세스 그룹, LUN 할당	볼륨 맵
iSCSI 세션	볼륨 마스크

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

다음은 이 데이터 소스를 구성하기 위한 요구 사항입니다.

- 관리 가상 IP 주소
- 포트 443

구성

필드에 입력합니다	설명
관리 가상 IP 주소(MVIP)	SolidFire 클러스터의 관리 가상 IP 주소입니다
사용자 이름	SolidFire 클러스터에 로그인하는 데 사용되는 이름입니다
암호	SolidFire 클러스터에 로그인하는 데 사용되는 암호입니다

고급 구성

필드에 입력합니다	설명

재고 폴링 간격(분)	재고 조사 간격(기본값: 60분)
TCP 포트	SolidFire 서버에 연결하는 데 사용되는 TCP 포트(기본값 443)
연결 시간 초과(초)	연결 시간 초과(기본값 60초)
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

문제 해결

SolidFire에서 오류를 보고하면 다음과 같이 OnCommand Insight에 표시됩니다.

```
An error message was received from a SolidFire device while trying to retrieve
data. The call was <method> (<parameterString> ). The error message from the
device was (check the device manual): <message>
```

여기서,

- 메소드>는 GET 또는 PUT와 같은 HTTP 메소드 입니다.
- parameterString>은 REST 호출에 포함된 쉼표로 구분된 매개 변수 목록입니다.
- message>는 오류 메시지로 반환된 장치와 상관없이 표시됩니다.

NetApp StorageGRID 데이터 소스

이 데이터 소스는 StorageGRID에 대한 인벤토리 및 성능 데이터를 수집합니다.

요구 사항

다음은 이 데이터 소스를 구성하기 위한 요구 사항입니다.

- StorageGRID 호스트 IP 주소입니다
- 메트릭 쿼리 및 테넌트 액세스 역할이 할당된 사용자의 사용자 이름 및 암호입니다
- 포트 443

구성

필드에 입력합니다	설명
StorageGRID 호스트 IP 주소(MVIP)	StorageGRID의 호스트 IP 주소입니다
사용자 이름	StorageGRID에 로그인하는 데 사용되는 이름입니다
암호	StorageGRID에 로그인하는 데 사용되는 암호입니다

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값: 60분)
성능 폴링 간격(초)	성능 폴링 간격(기본값 900초)

OpenStack 데이터 소스

OpenStack(REST API/KVM) 데이터 소스에서 OpenStack 하드웨어 인스턴스에 대한 정보를 수집합니다. 이 데이터 소스는 모든 OpenStack 인스턴스에 대한 인벤토리 데이터를 수집하고 선택적으로 VM 성능 데이터를 수집합니다.

요구 사항

다음은 OpenStack 데이터 소스를 구성하기 위한 요구사항입니다.

- OpenStack 컨트롤러의 IP 주소입니다
- OpenStack 관리자 역할 자격 증명 및 Linux KVM 하이퍼바이저에 대한 sudo 액세스를 권장합니다.

> admin 계정 또는 admin에 상응하는 권한을 사용하지 않는 경우에도 데이터 소스에서 데이터를 획득할 수 있습니다. admin 역할이 아닌 사용자가 API를 호출할 수 있도록 정책 구성 파일(예: etc/nova/policy.json)을 수정해야 합니다.

  - "OS_컴퓨팅_API:OS-가용성-영역:세부 정보":"
  - "OS_컴퓨팅_API:OS-하이퍼바이저":"
  - OS_컴퓨팅_API:서버:세부 정보:get_all_tenant":""
- 성능 수집을 위해 OpenStack Ceilometer 모듈을 설치하고 구성해야 합니다. Ceilometer 구성은 를 편집하여 수행할 수 있습니다 `nova.conf` 각 하이퍼바이저에 대해 파일을 생성한 다음 각 하이퍼바이저에서 Nova 컴퓨팅 서비스를 다시 시작합니다. 옵션 이름이 OpenStack의 다양한 릴리즈에서 변경되었습니다.
  - 아이스하우스
  - 준오
  - 킬로
  - 리버티
  - 미타카
  - 뉴턴
  - 옥타
- CPU 통계의 경우 컴퓨팅 노드의 /etc/nova/nova.conf에서 "compute_monitor=ComputeDriverCPUMonitor"를 켜야 합니다.
- 포트 요구 사항:
  - http의 경우 5000, Keystone 서비스의 경우 13000

- 22 KVM SSH의 경우
- Nova 컴퓨팅 서비스: 8774
- 8776을 참조하십시오
- Ceilometer 성능 서비스용 8777
- Glance 이미지 서비스를 위한 9292

> 포트는 특정 서비스에 바인딩되며, 대규모 환경의 컨트롤러 또는 다른 호스트에서 서비스가 실행될 수 있습니다.

구성

* 필드 *	* 설명 *
OpenStack 컨트롤러 IP 주소입니다	OpenStack 컨트롤러의 IP 주소 또는 정규화된 도메인 이름입니다
OpenStack 관리자	OpenStack 관리자의 사용자 이름입니다
OpenStack 암호	OpenStack Admin에 사용되는 암호입니다
OpenStack 관리자 테넌트	OpenStack 관리자 테넌트
KVM Sudo 사용자	KVM Sudo 사용자 이름입니다
자격 증명 유형을 지정하려면 '암호' 또는 'OpenSSH 키 파일'을 선택하십시오	SSH를 통해 장치에 연결하는 데 사용되는 자격 증명 유형입니다
재고 개인 키에 대한 전체 경로	재고 개인 키에 대한 전체 경로
KVM Sudo 암호	KVM Sudo 암호

고급 구성

* 필드 *	* 설명 *
SSH를 통해 하이퍼바이저 인벤토리 검색을 설정합니다	SSH를 통해 하이퍼바이저 인벤토리 검색을 설정하려면 이 확인란을 선택합니다
OpenStack 관리 URL 포트입니다	OpenStack 관리 URL 포트입니다
HTTPS를 사용합니다	보안 HTTP를 사용하려면 선택합니다
HTTP 연결 시간 초과(초)	HTTP 연결 시간 초과(기본값 300초)

SSH 포트	SSH에 사용되는 포트입니다
SSH 프로세스 대기 시간 초과(초)	SSH 프로세스 시간 초과(기본값 30초)
SSH 프로세스 재시도	인벤토리 재시도 횟수입니다
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)

Oracle ZFS 데이터 소스

Oracle ZFS 데이터 소스는 인벤토리 및 성능 수집을 지원합니다.

용어

OnCommand Insight는 이 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
디스크(SDD)	디스크
클러스터	스토리지
컨트롤러	스토리지 노드
LUN을 클릭합니다	볼륨
LUN 매핑	볼륨 맵
초기자, 대상	볼륨 마스크
공유	내부 볼륨

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

다음은 이 데이터 소스를 구성하기 위한 요구 사항입니다.

- ZFS Controller-1 및 ZFS Controller-2의 호스트 이름
- 관리자 사용자 이름 및 자격 증명
- 포트 요구 사항: 215 HTTP/HTTPS

구성

ZFS Controller-1 호스트 이름	스토리지 컨트롤러 1의 호스트 이름입니다
ZFS Controller-2 호스트 이름	스토리지 컨트롤러의 호스트 이름 2
사용자 이름입니다	스토리지 시스템 관리자 사용자 계정의 사용자 이름입니다
암호	관리자 사용자 계정의 암호입니다

고급 구성

필드에 입력합니다	설명
TCP 포트	ZFS에 연결하는 데 사용되는 TCP 포트(기본값 215)
연결 유형	HTTP 또는 HTTPS
인벤토리 폴링 간격입니다	인벤토리 폴링 간격(기본값: 60분)
연결 시간 초과	기본값은 60초입니다
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

문제:	다음을 시도해 보십시오.
"잘못된 로그인 자격 증명"	ZFS 사용자 계정 및 암호를 확인합니다
"구성 오류" 및 "reST 서비스가 비활성화되었습니다" 오류 메시지	이 장치에서 REST 서비스가 활성화되어 있는지 확인합니다.

"구성 오류" 및 "명령에 대한 권한이 없는 사용자" 오류 메시지	특정 역할(예: 'advanced_analytics')이 구성된 사용자 <userName>에 포함되지 않을 수 있습니다. 가능한 해결 방법: • 읽기 전용 역할을 사용하여 ${user} 사용자의 분석(통계) 범위를 수정하십시오. - 구성 → 사용자 화면에서 마우스를 역할 위에 놓고 두 번 클릭하여 편집할 수 있습니다 • 범위 드롭다운 메뉴에서 "분석"을 선택합니다. 가능한 속성 목록이 나타납니다. • 맨 위 확인란을 클릭하면 세 가지 속성이 모두 선택됩니다. - 오른쪽에 있는 추가 단추를 클릭합니다. • 팝업 창의 오른쪽 위에 있는 적용 단추를 클릭합니다. 팝업 창이 닫힙니다.

Pure Storage FlashArray 데이터 소스

Pure Storage FlashArray(HTTP) 데이터 소스는 Pure Storage Flash Array로부터 정보를 수집하는 데 사용됩니다. Insight는 인벤토리 및 성능 수집을 모두 지원합니다.

용어

OnCommand Insight는 Pure Storage FlashArray 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
드라이브(SSD)	디스크
스토리지	스토리지
컨트롤러	스토리지 노드
볼륨	볼륨
포트	포트
LUN 맵(호스트, 호스트 그룹, 타겟 포트)	볼륨 맵, 볼륨 마스크

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 스토리지 시스템 IP 주소입니다

- Pure 스토리지 시스템의 관리자 계정에 대한 사용자 이름 및 암호입니다.
- 포트 요구 사항: HTTP/HTTPS 80/443

구성

* 필드 *	* 설명 *
FlashArray 호스트	FlashArray Management Server의 IIP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	FlashArray 관리 서버의 사용자 이름입니다
암호	FlashArray Management Server의 암호입니다

고급 구성

* 필드 *	* 설명 *
연결 유형	관리 서버
TCP 포트	FlashArray 서버에 연결하는 데 사용되는 TCP 포트 (기본값 443)
연결 시간 초과(초)	연결 시간 초과(기본값 60초)
재고 폴링 간격(분)	재고 조사 간격(기본값: 60분)
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

QLogic FC 스위치 데이터 소스

구성의 경우, QLogic FC 스위치(SNMP) 데이터 소스에는 IP 주소로 지정된 FC 스위치 장치의 네트워크 주소와 장치에 액세스하는 데 사용되는 SNMP_READ-OVERY_COLANCE 문자열이 필요합니다.

구성

* 필드 *	* 설명 *
SANsurfer 스위치	SANsurfer 스위치의 IP 주소 또는 정규화된 도메인 이름입니다
SNMP 버전입니다	SNMP 버전입니다
SNMP 커뮤니티	SNMP 커뮤니티 문자열

사용자 이름	SANsurfer 스위치의 사용자 이름입니다
암호	SANsurfer 스위치의 암호입니다

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 15분)
SNMP 인증 프로토콜	SNMP 인증 프로토콜(SNMPv3만 해당)
SNMP 재시도	SNMP 재시도 횟수입니다
SNMP 시간 초과(ms)	SNMP 시간 초과(기본값 5,000ms)
트래핑을 활성화합니다	트래핑을 활성화하려면 선택합니다
트랩 사이의 최소 시간(초)	트랩에 의해 트리거된 획득 시도 사이의 최소 시간(기본값 10초)
패브릭 이름	데이터 소스에서 보고할 Fabric 이름입니다. 패브릭 이름을 WWN으로 보고하려면 공백으로 두십시오.
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

Red Hat(RHEV) 데이터 소스

Red Hat Enterprise Virtualization(REST) 데이터 소스는 HTTPS를 통해 RHEV 인스턴스에 대한 정보를 수집합니다.

요구 사항

- REST API를 통해 포트 443을 통해 RHEV 서버의 IP 주소입니다
- 읽기 전용 사용자 이름 및 암호
- RHEV 버전 3.0+

구성

필드에 입력합니다	설명
RHEV 서버 IP 주소입니다	RHEV 서버의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	RHEV 서버의 사용자 이름입니다

암호	RHEV 서버에 사용되는 암호입니다

고급 구성

필드에 입력합니다	설명
HTTPS 통신 포트	RHEV에 대한 HTTPS 통신에 사용되는 포트입니다
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
연결 시간 초과(초)	연결 시간 초과(기본값 60초)

Violin Flash Memory Array 데이터 소스

Violin 6000 시리즈 Flash Memory Array(HTTP) 데이터 소스는 Violin 6000 시리즈 플래시 메모리 어레이에서 분석 및 검증을 위해 네트워크 정보를 수집합니다.

용어

이 데이터 수집기는 OnCommand Insight 7.3.11부터 더 이상 사용할 수 없습니다.

OnCommand Insight는 Violin 6000 시리즈 플래시 메모리 어레이 데이터 소스에서 다음 인벤토리 정보를 수집합니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
Violin 지능형 메모리 모듈(VIMM)	디스크
컨테이너	스토리지
메모리 게이트웨이	스토리지 노드
LUN을 클릭합니다	볼륨
이니시에이터, 이니시에이터 그룹, 타겟	볼륨 맵, 볼륨 마스크

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 스토리지에 대한 읽기 전용 사용자 이름과 암호가 필요합니다.
- 스토리지 IP 주소를 사용하여 웹 브라우저에서 액세스를 검증합니다.

구성

필드에 입력합니다	설명
Violin Memory Array 주 게이트웨이의 IP 주소 또는 FQDN	Violin Memory Array Main Gateway의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	Violin Memory Array 주 게이트웨이의 사용자 이름입니다
암호	Violin Memory Array 주 게이트웨이의 암호입니다

고급 구성

필드에 입력합니다	설명
통신 포트	Violin Array와의 통신에 사용되는 포트입니다
HTTPS가 활성화되었습니다	HTTPS를 사용하려면 선택합니다
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
연결 시간 초과(초)	연결 시간 초과(기본값 60초)
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

VMware vSphere 데이터 소스

VMware vSphere(Web Services) 데이터 소스는 ESX 호스트 정보를 수집하고 Virtual Center 내의 모든 객체에 대해 _read-only_권한을 필요로 합니다.

용어

OnCommand Insight는 VMware vSphere 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
가상 디스크	디스크
호스트	호스트
가상 머신	가상 머신
데이터 저장소	데이터 저장소

LUN을 클릭합니다	LUN을 클릭합니다
Fibre Channel 포트	포트

> 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- Virtual Center 서버의 IP 주소입니다
- Virtual Center의 읽기 전용 사용자 이름 및 암호
- Virtual Center 내의 모든 객체에 대한 읽기 전용 권한
- Virtual Center 서버에서 SDK 액세스
- 포트 요구 사항: http-80 https-443
- 사용자 이름 및 암호를 사용하여 Virtual Center Client에 로그인하고 를 입력하여 SDK가 활성화되었는지 확인하여 액세스를 검증합니다 `telnet <vc_ip\> 443`.

구성

* 필드 *
* 설명 *
가상 센터 주소
IP_(nnn.nnn.nnn.nnn_format) 주소 또는 DNS를 통해 확인할 수 있는 호스트 이름으로 지정된 Virtual Center 또는 vSphere 서버의 네트워크 주소입니다.
사용자 이름
VMware 서버의 사용자 이름입니다.
암호
VMware 서버의 암호입니다.

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
연결 시간 초과(ms)	연결 시간 초과(기본값 60000ms)

VM 필터링 기준	VM 필터링 방법을 선택합니다
목록을 지정하려면 '제외' 또는 '포함'을 선택하십시오	데이터를 수집할 때 아래 VM 목록을 포함할지 제외할지 여부를 지정합니다
필터링할 VM 목록(값에 쉼표를 사용하는 경우 쉼표로 구분 또는 세미콜론으로 구분)	폴링을 포함하거나 폴링에서 제외할 VM 목록을 쉼표로 구분하거나 세미콜론으로 구분합니다
vCenter에 대한 요청 재시도 횟수입니다	vCenter 요청 재시도 횟수입니다
통신 포트	VMware 서버에 사용되는 포트입니다
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

데이터 소스 자격 증명을 변경하는 중입니다

같은 유형의 여러 데이터 소스가 사용자 이름과 암호를 공유하는 경우 그룹의 모든 장치에 대한 암호를 동시에 변경할 수 있습니다.

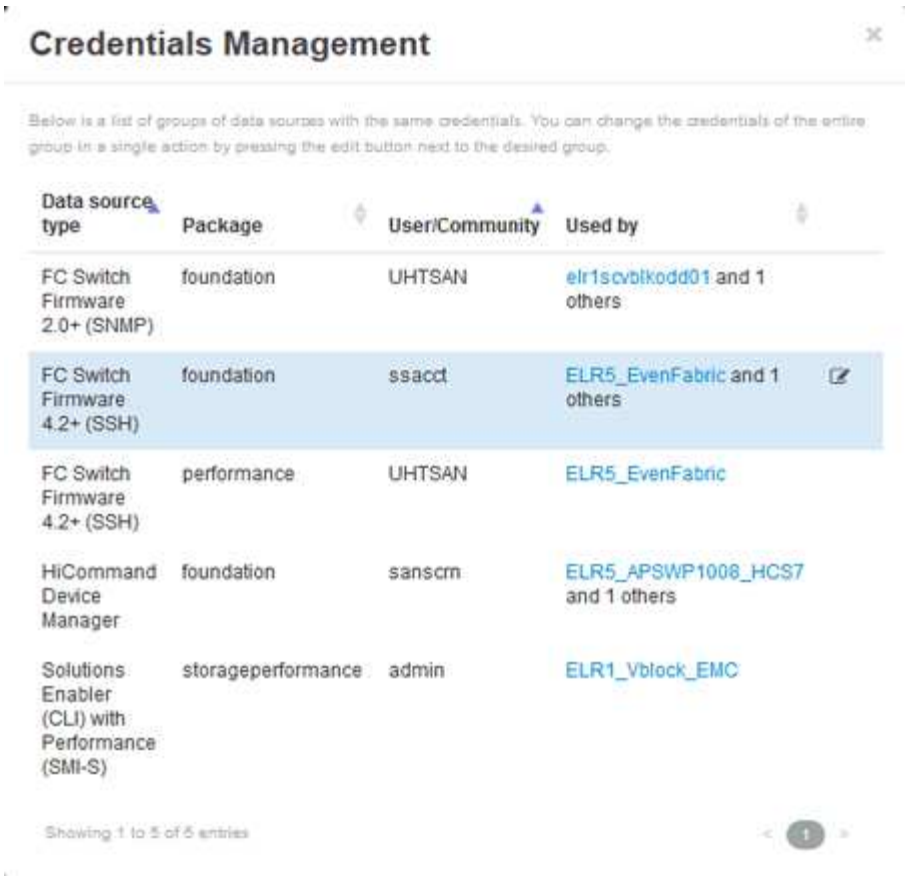
단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.

   데이터 소스 * 목록이 열립니다.

2. Actions * 버튼을 클릭하고 * Change credentials * 옵션을 선택합니다.
3. 자격 증명 관리 대화 상자의 목록에서 데이터 소스 그룹 중 하나를 선택합니다.

   용지 한 장에 있는 펜인 편집 아이콘이 오른쪽으로 활성화됩니다.



4. 편집 * 을 클릭합니다.
5. 새 암호를 입력하고 확인합니다.

데이터 수집 문제를 일으키는 변경 사항

OnCommand Insight에서 데이터 수집 문제가 발생하는 경우 환경 변화가 원인일 수 있습니다. 일반적인 유지 관리 규칙으로서 Insight에서도 환경의 모든 변경 사항을 고려해야 합니다.

이 검사 목록을 사용하여 문제를 일으킬 수 있는 네트워크 변경 사항을 확인할 수 있습니다.

- 암호를 변경했습니까? Insight에서 암호가 변경되었습니까?
- 네트워크에서 장치를 제거했습니까? 또한 장치가 다시 검색되고 다시 도입되지 않도록 OnCommand Insight에서 장치를 제거해야 합니다.
- 인프라 소프트웨어(예: HP CommandView EVA 또는 EMC Solutions Enabler)를 업그레이드했습니까?

  획득 장치에 적절한 버전의 클라이언트 도구가 설치되어 있는지 확인합니다. 데이터 소스 장애가 지속될 경우 기술 지원 부서에 문의하여 지원을 요청하고 데이터 소스 패치를 적용해야 합니다.

- 모든 OnCommand Insight 획득 장치에서 동일한 OnCommand Insight 버전을 사용하고 있습니까? 원격 획득 장치 및 로컬 획득 장치가 서로 다른 OnCommand Insight 버전을 실행 중인 경우 모든 장치에 동일한 버전을 설치하여 데이터 수집 문제를 해결하십시오.

  모든 획득 장치에 새 버전의 OnCommand Insight를 설치해야 하는 경우 지원 사이트로 이동하여 올바른 버전을 다운로드하십시오.

- 도메인 이름을 변경하거나 새 도메인을 추가했습니까? 장치 해상도(이전의 자동 해상도) 방법을 업데이트해야 합니다.

하나의 데이터 소스를 자세히 조사 중입니다

데이터 원본에 오류가 있거나 속도가 느려지면 해당 데이터 원본에 대한 자세한 정보 요약을 검토하여 문제의 원인을 확인할 수 있습니다. 주의를 기울여야 하는 조건이 있는 데이터 소스는 빨간색 원으로 표시됩니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.

   데이터 소스 * 목록이 열립니다. 잠재적인 문제가 있는 나열된 모든 데이터 원본은 빨간색 원으로 표시됩니다. 가장 심각한 문제는 목록의 맨 위에 있습니다.

2. 문제를 일으키는 데이터 소스를 선택합니다.
3. 데이터 원본 이름 링크를 클릭합니다.
4. 데이터 원본 요약 페이지에서 다음 섹션의 정보를 확인합니다.
   - * 이벤트 일정 *

     데이터 소스 목록에 표시된 현재 상태와 연결된 이벤트를 나열합니다. 이 요약의 이벤트는 장치별로 표시됩니다. 오류는 빨간색으로 표시됩니다. 타임라인 항목 위에 마우스 포인터를 놓으면 추가 정보를 표시할 수 있습니다.

   - * 이 데이터 소스에서 보고한 장치 *

     디바이스 유형, 해당 IP 주소 및 각 디바이스에 대한 자세한 정보에 대한 링크를 표시합니다.

   - * 이 데이터 소스에서 보고된 변경 사항(지난 3주) *

     추가 또는 제거되었거나 구성이 변경된 모든 장치를 나열합니다.

5. 데이터 원본 정보를 검토한 후 페이지 맨 위에 있는 단추를 사용하여 다음 작업 중 하나를 수행할 수 있습니다.
   - * 편집 * 문제를 해결하기 위한 데이터 원본에 대한 설명입니다.
   - * 다시 폴링 * 문제가 지속적이었거나 간헐적으로 발생하는지 여부를 폴링하도록 강제합니다.
   - * 3, 7 또는 30일 동안 데이터 소스 폴링을 연기하여 문제를 조사하고 경고 메시지를 중지할 시간을 제공합니다.
   - * 데이터 원본에 패치 * 를 설치하여 문제를 해결합니다.
   - 기술 지원을 위해 * 오류 보고서 * 를 준비합니다.
   - * Insight 모니터링 환경에서 데이터 소스를 * 삭제 * 합니다.

실패한 데이터 소스 조사

데이터 소스에 " * Inventory failed! * " 또는 " * Performance failed! * " 메시지가 있고 High 또는 Medium Impact가 있는 경우 연결된 정보가 있는 데이터 소스 요약 페이지를 사용하여 이 문제를 조사해야 합니다.

단계

1. 데이터 원본의 연결된 * 이름 * 을 클릭하여 요약 페이지를 엽니다.
2. 요약 페이지에서 * Comments * 영역을 확인하여 이 고장을 조사할 수 있는 다른 엔지니어가 남긴 메모를 읽습니다.
3. 성능 메시지를 기록합니다.
4. 이 데이터 원본에 적용되는 패치가 있는 경우 링크를 클릭하여 * 패치 페이지 * 를 확인하여 문제가 발생했는지 확인합니다.
5. 마우스 포인터를 * 이벤트 타임라인 * 그래프 세그먼트 위로 이동하여 추가 정보를 표시합니다.
6. 장치에 대한 오류 메시지를 선택하고 이벤트 타임라인 아래에 표시된 * 오류 세부 정보 * 아이콘을 클릭하면 메시지 오른쪽에 표시됩니다.

   오류 세부 정보에는 오류 메시지 텍스트, 가능한 원인, 사용 중인 정보 및 문제 해결을 위해 시도할 수 있는 권장 사항이 포함됩니다.

7. 이 데이터 소스 영역에서 보고한 장치 영역에서 목록을 필터링하여 관심 있는 장치만 표시할 수 있으며, 장치의 연결된 * 이름 * 을 클릭하여 해당 장치의 _asset 페이지_를 표시할 수 있습니다.
8. 이전에 표시된 페이지로 돌아가려면 다음 방법 중 하나를 사용합니다.
   - 브라우저의 뒤로 화살표를 클릭합니다.
   - 뒤로 화살표를 마우스 오른쪽 단추로 클릭하여 페이지 목록을 표시하고 원하는 페이지를 선택합니다.
9. 다른 자원에 대한 자세한 정보를 표시하려면 연결된 다른 이름을 클릭합니다.
10. 데이터 원본 요약 페이지로 돌아가면 페이지 하단의 * 변경 * 영역을 확인하여 최근 변경으로 인해 문제가 발생했는지 확인합니다.

데이터 소스 폴링을 제어합니다

데이터 원본을 변경한 후 변경 내용을 확인하기 위해 즉시 폴링하거나 문제 해결 중에 데이터 원본의 데이터 수집을 1, 3 또는 5일 동안 연기할 수 있습니다.

단계

1. Admin * 을 클릭하고 데이터 소스 목록 보기로 이동합니다
2. 폴링을 제어할 데이터 소스를 선택합니다.
3. 데이터 원본 이름 링크를 클릭합니다.
4. 데이터 원본 요약 페이지에서 정보를 확인하고 다음 두 폴링 옵션 중 하나를 클릭합니다.
   - * 다시 폴링 * 데이터 소스가 데이터를 즉시 수집하도록 강제합니다.
   - * 연기 * 를 선택하고 폴링 지연 기간을 3일, 7일 또는 30일로 선택합니다.

작업을 마친 후

데이터 소스에서 데이터 수집을 연기하고 컬렉션을 다시 시작하려면 요약 페이지에서 * Resume * 을 클릭합니다.

데이터 원본 정보 편집

데이터 소스 설정 정보를 빠르게 편집할 수 있습니다.

단계

1. Admin * 을 클릭하고 데이터 소스 목록 보기로 이동합니다
2. 편집할 데이터 원본을 찾습니다.
3. 다음 방법 중 하나를 사용하여 변경을 시작합니다.
   - 선택한 데이터 원본의 오른쪽에 있는 * 데이터 원본 편집 * 을 클릭합니다.
   - 선택한 데이터 원본의 연결된 이름을 클릭하고 * 편집 * 을 클릭합니다. 두 방법 중 하나를 선택하면 데이터 원본 편집 대화 상자가 열립니다.
4. 원하는 대로 변경하고 * Save * (저장 *)를 클릭합니다.

여러 데이터 원본에 대한 정보 편집

동일한 공급업체 및 모델의 여러 데이터 원본에 대한 대부분의 정보를 한 번에 편집할 수 있습니다. 예를 들어 이러한 데이터 원본이 사용자 이름과 암호를 공유하는 경우 한 곳에서 암호를 변경하여 선택한 모든 데이터 원본의 암호를 업데이트할 수 있습니다.

이 작업에 대해

선택한 데이터 원본에 대해 편집할 수 없는 옵션은 흐리게 표시되거나 데이터 원본 편집 대화 상자에 표시되지 않습니다. 또한 옵션이 * Mixed * 값을 표시할 때 옵션의 값이 선택한 데이터 소스 간에 다르다는 것을 나타냅니다. 예를 들어 선택한 두 데이터 원본에 대한 * Timeout(sec) * 옵션이 * Mixed * 인 경우 한 데이터 원본의 시간 초과 값은 60이고 다른 데이터 원본의 값은 90일 수 있습니다. 따라서 이 값을 120으로 변경하고 데이터 원본에 대한 변경 내용을 저장하면 두 데이터 원본에 대한 시간 초과 설정이 120이 됩니다.

단계

1. Admin * 을 클릭하고 데이터 소스 목록 보기로 이동합니다
2. 수정할 데이터 원본을 선택합니다. 선택한 데이터 소스는 동일한 공급업체, 모델 및 획득 단위에 속해야 합니다.
3. Actions * 버튼을 클릭하고 * Edit * 옵션을 선택합니다.
4. 편집 대화 상자에서 필요에 따라 * 설정 * 을 변경합니다.
5. 데이터 원본에 대한 기본 옵션을 변경하려면 * 구성 * 링크를 클릭합니다.
6. 데이터 원본에 대한 고급 옵션을 변경하려면 * 고급 구성 * 링크를 클릭합니다.
7. 저장 * 을 클릭합니다.

주석에 데이터 원본 태그 매핑

데이터 소스가 태그 데이터를 폴링하도록 구성된 경우 Insight는 태그와 같은 이름의 기존 Insight 주석에 대한 주석 값을 자동으로 설정합니다.

데이터 소스에서 태그를 사용하기 전에 Insight 주석이 있으면 데이터 소스 태그 데이터가 Insight 주석에 자동으로

추가됩니다.

태그가 활성화된 후 주석을 만들 때 데이터 소스의 초기 폴링은 주석을 자동으로 업데이트하지 않습니다. Insight 주석을 교체하거나 채우는 데 걸리는 시간이 지연됩니다. 지연을 방지하려면 데이터 소스를 연기했다가 다시 시작하면 태그가 주석으로 업데이트되도록 할 수 있습니다.

데이터 원본을 삭제하는 중입니다

환경에서 데이터 소스를 제거한 경우에는 OnCommand Insight 모니터링 환경에서도 삭제해야 합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.

   데이터 소스 목록이 열립니다.

2. 삭제할 데이터 원본을 선택합니다.
3. 연결된 데이터 원본 이름을 클릭합니다.
4. 요약 페이지에서 선택한 데이터 원본에 대한 정보를 확인하여 삭제할 데이터 원본인지 확인합니다.
5. 삭제 * 를 클릭합니다.
6. 확인 * 을 클릭하여 작업을 확인합니다.

어떤 데이터 소스 패치가 있는지 확인합니다

데이터 소스 패치는 기존 패치의 문제를 해결하고 새 데이터 소스 유형(공급업체 및 모델)을 쉽게 추가할 수 있습니다. 네트워크의 각 데이터 소스 유형에 대해 데이터 소스 패치를 업로드할 수 있습니다. 패치 프로세스를 설치, 테스트 및 관리할 수도 있습니다. 그러나 한 번에 하나의 패치만 데이터 소스 유형에 대해 활성화될 수 있습니다.

각 패치에 대해 다음 작업을 수행할 수 있습니다.

- 패치를 수신하는 각 데이터 소스의 비교 전과 후를 확인합니다.
- 의견을 작성하여 결정을 설명하거나 연구를 요약합니다.
- 패치에 잘 응답하지 않는 데이터 소스를 변경합니다.
- Insight 서버에 커밋할 패치를 승인합니다.
- 의도한 대로 작동하지 않는 패치를 롤백합니다.
- 결함이 있는 패치를 다른 패치로 교체합니다.

데이터 소스 패치를 적용하는 중입니다

데이터 소스 패치를 주기적으로 사용할 수 있으며 기존 데이터 소스의 문제를 해결하거나 새 공급업체의 데이터 소스를 추가하거나 공급업체의 새 모델을 추가할 수 있습니다.

시작하기 전에

을(를) 받아야 합니다 `.zip` 최신 데이터 소스가 포함된 파일입니다 `.patch` 기술 지원 부서의 파일.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 패치 * 를 클릭합니다.
3. 작업 버튼에서 * 패치 적용 * 을 선택합니다.
4. 데이터 원본 패치 적용 * 대화 상자에서 * 찾아보기 * 를 클릭하여 을 찾습니다 `.patch` 파일.
5. 패치 이름 *, * 설명 * 및 * 영향받는 데이터 소스 유형 * 을 검사합니다.
6. 선택한 패치가 올바르면 * 패치 적용 * 을 클릭합니다.

   데이터 원본 관련 문제를 해결하는 패치를 적용하는 경우 동일한 유형의 모든 데이터 원본이 패치로 업데이트되므로 패치를 승인해야 합니다. 구성된 데이터 원본에 영향을 주지 않는 패치는 자동으로 승인됩니다.

작업을 마친 후

새 공급업체나 새 모델에 대한 데이터 원본을 추가하는 패치를 적용하는 경우 패치를 적용한 후 데이터 원본을 추가해야 합니다.

하나의 데이터 소스에 패치 설치

데이터 원본 패치를 업로드한 후에는 같은 형식의 모든 데이터 원본에 설치할 수 있습니다.

시작하기 전에

한 유형의 데이터 원본에 설치할 패치 파일을 업로드해야 합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 패치 * 를 클릭합니다.
3. 작업 버튼에서 * 패치 적용 * 을 선택합니다.
4. 데이터 원본 패치 적용 * 대화 상자에서 * 찾아보기 * 를 클릭하여 업로드된 패치 파일을 찾습니다.
5. 패치 이름 *, * 설명 * 및 * 영향받는 데이터 소스 유형 * 을 확인하십시오.
6. 선택한 패치가 올바르면 * 패치 적용 * 을 클릭합니다.

   동일한 유형의 모든 데이터 소스가 이 패치로 업데이트됩니다.

패치 관리

네트워크에 적용되는 모든 데이터 소스 패치의 현재 상태를 검토할 수 있습니다. 패치에 대한 작업을 수행하려면 현재 검토 중인 패치에서 연결된 이름을 클릭하면 됩니다.

시작하기 전에

이미 업로드된 패치를 하나 이상 설치해야 합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 패치 * 를 클릭합니다.

   설치된 패치가 없는 경우 현재 검토 중인 패치 테이블이 비어 있습니다.

3. 현재 검토 중인 * 패치 * 에서 현재 적용 중인 데이터 소스 패치의 상태를 확인합니다.
4. 특정 패치와 관련된 세부 정보를 검사하려면 패치의 연결된 이름을 클릭합니다.
5. 선택한 패치에 대해 다음 옵션을 클릭하여 패치에 대한 다음 작업을 수행할 수 있습니다.
   - * Approve patch * 는 데이터 소스에 패치를 적용합니다.
   - * 롤백 * 은 패치를 제거합니다.
   - * 패치 바꾸기 * 를 사용하면 해당 데이터 원본에 대해 다른 패치를 선택할 수 있습니다.

데이터 소스 패치 커밋

패치 요약의 정보를 사용하여 패치가 예상대로 작동하는지 확인한 다음 패치를 네트워크에 커밋합니다.

시작하기 전에

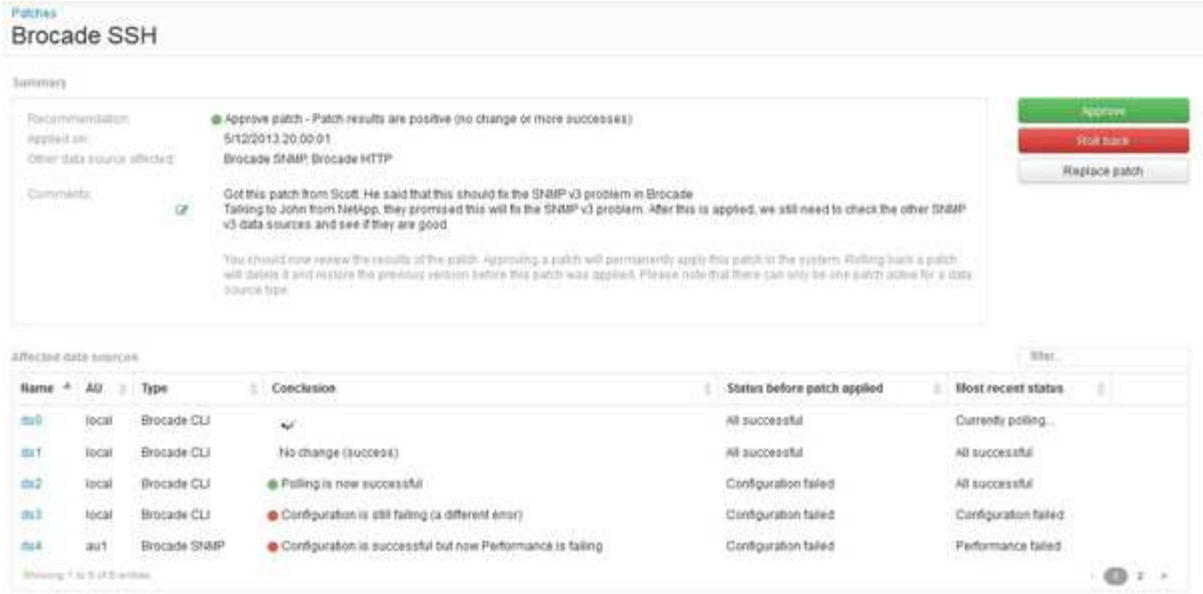
패치를 설치했으며 패치가 성공적인지 확인해야 합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 패치 * 를 클릭합니다.

   설치된 패치가 없으면 현재 검토 중인 패치가 비어 있습니다.

3. 현재 검토 중인 * 패치 * 에서 현재 적용 중인 데이터 소스 패치의 상태를 확인합니다.
4. 특정 패치와 관련된 세부 정보를 검사하려면 패치의 연결된 이름을 클릭합니다.
5. 이 예제에 표시된 패치 요약 정보에서 * 권장 * 및 * 설명 * 을 확인하여 패치의 진행 상황을 평가합니다.



6. 영향을 받는 * 데이터 소스 * 표를 확인하여 패치 전후에 영향을 받는 각 데이터 소스의 상태를 확인하십시오.

   패치하는 데이터 원본 중 하나에 문제가 있는 경우 영향을 받는 데이터 원본 테이블에서 연결된 이름을 클릭합니다.

7. 해당 유형의 데이터 원본에 패치를 적용해야 한다고 판단하면 * Approve * (승인 *)를 클릭합니다.

   데이터 소스가 변경되고 현재 검토 중인 패치에서 패치가 제거됩니다.

데이터 소스 패치를 롤백하는 중입니다

데이터 소스 패치가 예상한 방식으로 작동하지 않으면 롤백할 수 있습니다. 패치를 롤백하면 패치가 삭제되고 이 패치가 적용되기 전의 이전 버전이 복원됩니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 패치 * 를 클릭합니다.
3. 현재 검토 중인 패치 * 에서 실패한 것으로 보이는 패치의 연결된 이름을 클릭합니다.
4. 데이터 원본의 패치 페이지에서 다음 정보를 확인합니다.
   - * 요약 * 은 패치가 적용된 시기, 영향을 받는 데이터 원본, 사용자 또는 팀의 다른 구성원으로부터 받은 패치에 대한 설명을 나타냅니다.
   - 영향을 받는 데이터 소스 * 는 패치되는 모든 데이터 소스를 나열하며 패치 이전 및 이후 상태의 비교를 포함합니다.
5. 패치를 성공적으로 처리하지 않는 데이터 원본에 대한 세부 정보를 표시하려면 연결된 * 이름 * 을 클릭합니다.
   a. 요약 정보를 확인합니다.
   b. 이벤트 타임라인 * 을 확인하여 이 데이터 소스에 영향을 줄 수 있는 구성 또는 성능 데이터를 확인하십시오.
6. 패치가 제대로 실행되지 않을 것이라고 판단될 경우 브라우저의 뒤로 화살표를 클릭하여 패치 요약 페이지로 돌아갑니다.

7. 롤백 * 을 클릭하여 해당 패치를 제거합니다.

   다른 패치가 성공적임을 알고 있는 경우 * 패치 바꾸기 * 를 클릭하고 새 패치를 업로드하십시오.

장치 해상도

OnCommand Insight를 사용하여 모니터링하려는 모든 장치를 검색해야 합니다. 환경의 성능과 인벤토리를 정확하게 추적하려면 검색이 필요합니다. 일반적으로 사용자 환경의 대부분의 장치는 자동 장치 해상도를 통해 검색됩니다.

> 업그레이드를 수행하는 중에 업그레이드 중인 시스템에 비활성 자동 해결 규칙이 있는 경우 업그레이드 중에 이러한 규칙이 삭제됩니다. 비활성 자동 해결 규칙을 유지하려면 업그레이드를 수행하기 전에 규칙을 활성화(확인란 선택)합니다.

데이터 소스를 설치 및 구성한 후에는 스위치, 스토리지 어레이 및 하이퍼바이저와 VM의 가상 인프라를 비롯한 환경의 장치가 식별됩니다. 그러나 이 경우 일반적으로 사용자 환경의 디바이스 중 100%는 식별되지 않습니다.

데이터 소스 유형 디바이스를 구성한 후에는 디바이스 해결 규칙을 활용하여 사용자 환경에서 나머지 알 수 없는 디바이스를 식별하는 것이 가장 좋습니다. 장치 해상도를 통해 알 수 없는 장치를 다음 장치 유형으로 해결할 수 있습니다.

- 물리적 호스트
- 지원합니다
- 테이프
- 스위치

디바이스 확인 후 ""알 수 없음""으로 남아 있는 디바이스는 쿼리와 대시보드에도 표시할 수 있는 일반 디바이스로 간주됩니다.

차례로 생성된 규칙은 사용자 환경에 추가되는 것과 유사한 특성을 가진 새 디바이스를 자동으로 식별합니다. 경우에 따라 장치 해상도를 통해 Insight 내에서 검색되지 않은 장치에 대한 장치 해결 규칙을 우회하여 수동으로 식별할 수도 있습니다.

기기 식별이 완료되지 않으면 다음과 같은 문제가 발생할 수 있습니다.

- 불완전한 경로
- 알 수 없는 다중 경로 연결
- 애플리케이션을 그룹화할 수 없습니다
- 토폴로지 뷰가 부정확합니다
- 데이터 웨어하우스 및 보고의 부정확한 데이터

장치 해상도 기능(* 관리*>* 장치 해상도*)에는 다음 탭이 포함되어 있으며 각 탭은 장치 해상도 계획 및 결과 보기에 역할을 합니다.

- "FC Identify"(FC 식별)에는 자동 디바이스 확인을 통해 해결되지 않은 Fibre Channel 디바이스의 WWN 및 포트 정보가 포함됩니다. 이 탭은 식별된 디바이스의 비율도 식별합니다.

- "IP Identify"(IP 식별)에는 자동 디바이스 확인을 통해 식별되지 않은 CIFS 공유 및 NFS 공유에 액세스하는 디바이스 목록이 포함되어 있습니다. 이 탭은 식별된 디바이스의 비율도 식별합니다.
- "자동 해상도 규칙"에는 Fibre Channel 디바이스 해상도를 수행할 때 실행되는 규칙 목록이 포함되어 있습니다. 식별되지 않은 Fibre Channel 디바이스를 확인하기 위해 생성하는 규칙입니다.
- ""기본 설정""은 환경에 맞게 장치 해상도를 사용자 정의하는 데 사용하는 구성 옵션을 제공합니다.

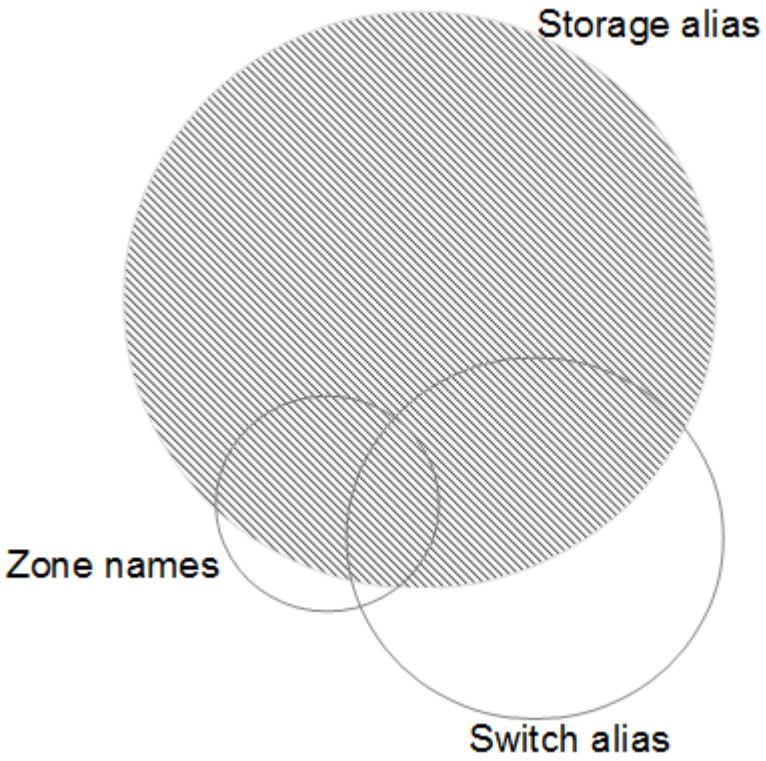
시작하기 전에

디바이스 식별 규칙을 정의하기 전에 환경 구성 방법을 알아야 합니다. 환경에 대해 더 많이 알수록 장치를 더 쉽게 식별할 수 있습니다.

정확한 규칙을 만들려면 다음과 유사한 질문에 대답해야 합니다.

- 귀사의 환경에 존 또는 호스트에 대한 명명 표준이 있습니까? 이 중 몇 퍼센트가 정확합니까?
- 귀사의 환경에서 스위치 별칭 또는 스토리지 별칭이 사용되고 있으며 이 별칭이 호스트 이름과 일치합니까?
- 사용 중인 환경에서 SRM 툴을 사용하고 있으며 이를 사용하여 호스트 이름을 식별할 수 있습니까? SRM은 어떤 서비스를 제공합니까?
- 사용자 환경에서 명명 체계가 얼마나 자주 변경됩니까?
- 서로 다른 이름 지정 체계를 도입한 인수 또는 합병이 있었습니까?

환경을 분석한 후에는 신뢰할 수 있는 명명 기준이 무엇인지 파악할 수 있어야 합니다. 수집한 정보는 다음과 유사한 그림으로 표시될 수 있습니다.

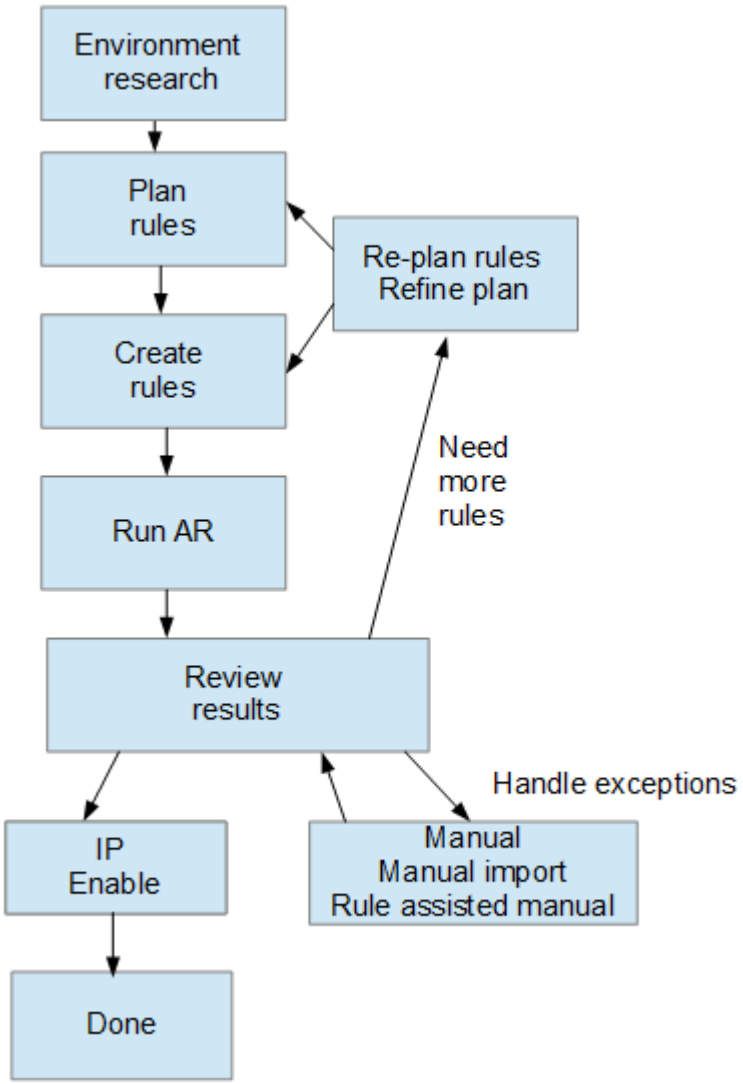


이 예에서는 가장 많은 수의 디바이스가 스토리지 별칭으로 안정적으로 표시됩니다. 스토리지 별칭을 사용하여 호스트를 식별하는 규칙을 먼저 작성하고, 스위치 별칭을 사용하는 규칙을 다음에 작성해야 하며, 마지막으로 생성된 규칙은 존 별칭을 사용해야 합니다. 영역 별칭과 스위치 별칭의 사용이 겹치기 때문에 일부 스토리지 별칭 규칙은 추가 디바이스를

식별할 수 있으므로 영역 별칭과 스위치 별칭에 필요한 규칙이 줄어듭니다.

사용자 환경에서 장치를 정의하는 단계입니다

일반적으로 다음과 유사한 워크플로를 사용하여 사용자 환경에서 장치를 식별합니다. 식별은 반복적인 프로세스이며 규칙을 계획하고 구체화하는 여러 단계가 필요할 수 있습니다.



사용자 환경에 알 수 없는 장치(""알 수 없음" 또는 일반 장치)가 있고 이후에 폴링 시 이러한 장치를 식별하는 데이터 소스를 구성하면 더 이상 일반 장치로 표시되거나 계산되지 않습니다.

환경에 대한 장치 해결 규칙 계획

규칙을 사용하여 사용자 환경에서 장치를 식별하는 것은 일반적으로 환경을 철저히 분석하고 가능한 많은 장치를 식별하기 위해 여러 규칙을 만들어야 하는 반복적인 프로세스입니다. 가장 좋은 시나리오는 환경에 있는 장치의 100%를 식별하기 위한 목표를 설정하는 것입니다.

규칙의 가장 효율적인 순서는 가장 제한적인 규칙을 먼저 배치하여 대부분의 항목이 패턴 일치되지 않도록 하고, 프로세스는 덜 제한적인 규칙으로 진행되도록 하는 것입니다. 이를 통해 Insight는 각 항목에 더 많은 패턴을 적용하여 패턴 일치 및 양성 호스트 식별 가능성을 높일 수 있습니다.

규칙을 만들 때 목표는 가능한 최대 수의 식별되지 않은 장치를 처리하는 규칙을 만드는 것입니다. 예를 들어, 다음과 같은 적용 범위 패턴을 따르는 규칙을 만들면 적용 범위 비율이 낮은 30개의 규칙을 만드는 것이 훨씬 효율적입니다.

규칙	적용 범위의 백분율입니다
규칙 1	60%
규칙 2	25%
규칙 3	8%
규칙 4	4%
규칙 5	1%

장치 해상도 규칙을 만드는 중입니다

디바이스 확인 규칙을 생성하여 현재 OnCommand Insight에서 자동으로 식별되지 않는 호스트, 스토리지 및 테이프를 식별합니다. 생성하는 규칙은 현재 환경에 있는 디바이스를 식별하고 유사한 디바이스를 환경에 추가할 때 식별합니다.

이 작업에 대해

규칙을 만들 때는 먼저 규칙이 실행되는 정보의 소스, 정보를 추출하는 데 사용되는 메서드 및 DNS 조회가 규칙의 결과에 적용되는지 여부를 확인합니다.

장치를 식별하는 데 사용되는 소스입니다
• 호스트에 대한 SRM 별칭입니다 • 포함된 호스트 또는 테이프 이름을 포함하는 스토리지 별칭입니다 • 포함된 호스트 또는 테이프 이름이 포함된 스위치 별칭입니다 • 포함된 호스트 이름이 포함된 영역 이름입니다
소스에서 디바이스 이름을 추출하는 데 사용되는 방법입니다
• 있는 그대로(SRM에서 이름 추출) • 구분 기호 • 정규식입니다
DNS 조회
DNS를 사용하여 호스트 이름을 확인할지 여부를 지정합니다.

자동 해결 규칙 탭에서 규칙을 만듭니다. 다음 단계에서는 규칙 생성 프로세스를 설명합니다.

단계

1. Manage * > * Device resolution * 을 클릭합니다
2. 자동 해상도 규칙 * 탭에서 * + 추가 * 를 클릭합니다

   새 규칙 화면이 표시됩니다.

   > 새 규칙 화면에는 정규식을 만들기 위한 도움말과 예제를 제공하는 *? * 아이콘이 포함되어 있습니다.

3. Type * 목록에서 식별하려는 장치를 선택합니다.

   호스트 또는 테이프 를 선택할 수 있습니다.

4. 소스 * 목록에서 호스트를 식별하는 데 사용할 소스를 선택합니다.

   선택한 소스에 따라 Insight에 다음 응답이 표시됩니다.

   - 영역은 Insight에서 식별해야 하는 영역 및 WWN을 나열합니다.
   - SRM에는 Insight로 식별해야 하는 식별되지 않은 별칭이 나열됩니다
   - 스토리지 별칭에는 Insight에서 식별해야 하는 스토리지 별칭과 WWN이 나열됩니다
   - 스위치 별칭에는 Insight에서 식별해야 하는 스위치 별칭이 나열됩니다

5. Method* 목록에서 호스트를 식별하기 위해 사용할 방법을 선택합니다.

출처	방법
SRM	"있는 그대로", "기한도자", "정규식"
스토리지 별칭입니다	"기한도자" 또는 "정규식"
별칭 전환	"기한도자" 또는 "정규식"
존	"기한도자" 또는 "정규식"

   - "기한자"를 사용하는 규칙에는 구분 기호 및 호스트 이름의 최소 길이가 필요합니다.

     호스트 이름의 최소 길이는 Insight에서 호스트를 식별하는 데 사용해야 하는 문자 수입니다. Insight는 길이가 길거나 긴 호스트 이름에 대해서만 DNS 조회를 수행합니다.

     Delimiters를 사용하는 규칙의 경우 입력 문자열은 구분 기호로 토큰화되며 인접한 토큰을 여러 개 조합하여 호스트 이름 후보 목록이 만들어집니다. 그런 다음 목록이 가장 큰 것부터 가장 작은 순서로 정렬됩니다. 예를 들어 vipsnq03_hba3_emcp3_12ep0의 경우 다음과 같은 결과가 나타납니다.

     - vipsnq03_hba3_emcp3_12ep0을 입력합니다
     - vipsnq03_hba3_emcp3

        - hba3 emc3_12ep0
        - vipsnq03_hba3
        - emc3_12ep0을 참조하십시오
        - hba3_emc3
        - vipsnq03
        - 12ep0
        - emc3
        - hba3
    - 정규식을 사용하는 규칙에는 정규식과 형식, 케이스 민감도를 선택해야 합니다.
6. 을 클릭합니다 ▶ Run AR ▾ 모든 규칙을 실행하거나, 버튼을 눌러 만든 규칙(및 AR의 마지막 전체 실행 이후 생성된 기타 규칙)을 실행합니다.

결과

규칙 실행 결과는 FC 식별 탭에 표시됩니다.

자동 장치 해상도 업데이트를 시작합니다

장치 해상도 업데이트는 마지막 전체 자동 장치 해상도 실행 이후 추가된 수동 변경 사항을 커밋합니다. 업데이트를 실행하면 장치 해상도 구성에 대한 새 수동 항목만 커밋하고 실행할 수 있습니다. 전체 장치 해상도 실행이 수행되지 않습니다.

단계

1. Insight 웹 UI에 로그인합니다.
2. Manage * > * Device Resolution * 을 클릭합니다
3. 장치 해상도 * 화면에서 * AR 실행 * 버튼의 아래쪽 화살표를 클릭합니다.
4. 업데이트를 시작하려면 * 업데이트 * 를 클릭합니다.

규칙 지원 수동 식별

이 기능은 알 수 없는 호스트, 스토리지 및 테이프 디바이스 또는 그룹 문제를 해결하기 위해 특정 규칙 또는 규칙 목록(일회성 순서 재조정 포함 또는 제외)을 실행하려는 특수한 경우에 사용됩니다.

시작하기 전에

식별되지 않은 다수의 장치가 있고 다른 장치를 성공적으로 식별하는 여러 규칙이 있습니다.

이 작업에 대해

> ⓘ 소스에 호스트 또는 장치 이름의 일부만 포함되어 있는 경우 정규식 규칙을 사용하여 서식을 지정하여 누락된 텍스트를 추가합니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. Manage * > * Device resolution * 을 클릭합니다
3. FC 식별 * 탭을 클릭합니다.

   시스템에서 식별된 장치 및 식별되지 않은 장치를 표시합니다.

4. 식별되지 않은 여러 장치를 선택합니다.
5. Identify * > * Set host resolution * 또는 * > Set tape resolution * 을 클릭합니다

   성공적으로 식별된 장치의 모든 규칙 목록이 포함된 식별 화면이 표시됩니다.

6. 규칙 순서를 필요에 맞는 순서로 변경합니다.

   규칙 순서는 식별 화면에서 변경되지만 전역적으로 변경되지는 않습니다.

7. 필요에 맞는 방법을 선택하십시오.

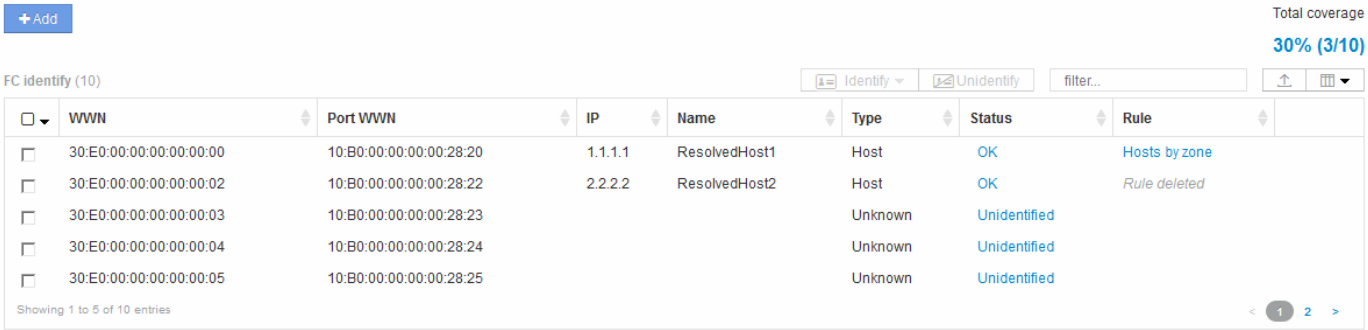
   OnCommand Insight는 메서드가 나타나는 순서대로 호스트 확인 프로세스를 실행하며, 맨 위에 있는 방법부터 시작합니다.

   적용되는 규칙이 있으면 규칙 이름이 규칙 열에 표시되고 수동으로 식별됩니다.

파이버 채널 장치 해상도

FC 식별 화면에는 호스트가 자동 디바이스 확인 방법으로 식별되지 않은 Fibre Channel 디바이스의 WWN 및 WWPN이 표시됩니다. 또한 화면에는 수동 장치 해상도에 의해 해결된 모든 장치가 표시됩니다.

수동 해상도에 의해 해결된 장치에는 ""OK"" 상태가 포함되어 있으며 장치를 식별하는 데 사용되는 규칙을 식별합니다. 누락된 장치는 ""알 수 없음"" 상태입니다. 장치 식별의 총 범위는 이 페이지에 나와 있습니다.



FC 식별 화면의 왼쪽에서 여러 디바이스를 선택하여 대량 작업을 수행합니다. 장치 위로 마우스를 가져간 다음 목록의 맨 오른쪽에 있는 식별 또는 식별 안 함 단추를 선택하여 단일 장치에서 작업을 수행할 수 있습니다.

Total coverage(전체 범위) 링크는 사용자의 구성에 대해 "식별된 장치 수/사용 가능한 장치 수" 목록을 표시합니다.

- SRM 별칭

- 스토리지 별칭입니다
- 별칭 전환
- 존
- 사용자 정의

Fibre Channel 디바이스를 수동으로 추가합니다

디바이스 해상도 FC 식별 탭에서 사용할 수 있는 수동 추가 기능을 사용하여 Fibre Channel 디바이스를 OnCommand Insight에 수동으로 추가할 수 있습니다. 이 프로세스는 향후 발견될 것으로 예상되는 장치를 사전 식별하는 데 사용될 수 있습니다.

시작하기 전에

시스템에 디바이스 ID를 추가하려면 WWN 또는 IP 주소와 디바이스 이름을 알아야 합니다.

이 작업에 대해

호스트, 스토리지, 테이프 또는 알 수 없는 Fibre Channel 디바이스를 수동으로 추가할 수 있습니다.

단계

1. Insight 웹 UI에 로그인합니다
2. Manage * > * Device resolution * 을 클릭합니다
3. FC 식별 * 탭을 클릭합니다.
4. 추가 버튼을 클릭합니다.

   장치 추가 대화 상자가 표시됩니다

5. WWN 또는 IP 주소, 디바이스 이름을 입력하고 디바이스 유형을 선택합니다.

결과

입력한 디바이스가 FC 식별 탭의 디바이스 목록에 추가됩니다. '규칙'은 '수동'으로 식별됩니다.

CSV 파일에서 **Fibre Channel** 디바이스 **ID** 가져오기

CSV 파일의 디바이스 목록을 사용하여 Fibre Channel 디바이스 ID를 OnCommand Insight 디바이스 해상도 기능으로 수동으로 가져올 수 있습니다.

시작하기 전에

장치 식별 정보를 장치 해상도 기능으로 직접 가져오려면 올바른 형식의 CSV 파일이 있어야 합니다. Fibre Channel 디바이스용 CSV 파일에는 다음 정보가 필요합니다.

WWN입니다

IP
이름
유형

> 모범 사례로서 먼저 FC 식별 정보를 CSV 파일로 내보내고 해당 파일에서 원하는 대로 변경한 다음 파일을 다시 FC Identify로 가져오는 것이 좋습니다. 이렇게 하면 예상 열이 올바른 순서로 표시됩니다.

FC 식별 정보를 가져오려면

단계

1. Insight 웹 UI에 로그인합니다.
2. Manage * > * Device Resolution * 을 클릭합니다
3. FC 식별 * 탭을 선택합니다.
4. 식별 * > * 파일에서 식별 * 을 클릭합니다 .
   a. 가져올 CSV 파일이 포함된 폴더로 이동하고 원하는 파일을 선택합니다.

   입력한 디바이스는 FC Identify 탭의 디바이스 목록에 추가됩니다. 규칙(Rule)은 'Manual'(수동)으로 식별됩니다.

Fibre Channel 디바이스 식별 정보를 **CSV** 파일로 내보내는 중입니다

OnCommand Insight 디바이스 확인 기능을 사용하여 기존 Fibre Channel 디바이스 식별 정보를 CSV 파일로 내보낼 수 있습니다. 장치 ID를 수정하여 Insight로 다시 가져온 다음 내보낸 ID와 원래 일치하는 장치를 식별하는 데 이 ID를 사용할 수 있도록 장치 ID를 내보낼 수 있습니다.

이 작업에 대해

이 시나리오는 CSV 파일에서 쉽게 편집한 후 시스템으로 다시 가져올 수 있는 유사한 속성이 장치에 있을 때 사용할 수 있습니다.

Fibre Channel 디바이스 ID를 CSV 파일로 내보낼 때 파일은 다음 정보를 표시된 순서대로 포함합니다.

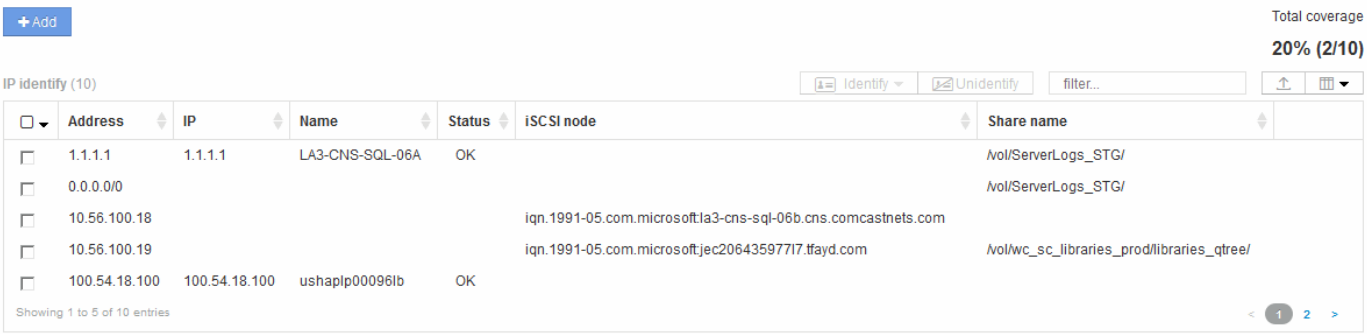
WWN입니다
IP
이름
유형

단계

1. Insight 웹 UI에 로그인합니다.
2. Manage * > * Device Resolution * 을 클릭합니다
3. FC 식별 * 탭을 선택합니다.
4. ID를 내보낼 Fibre Channel 디바이스를 선택합니다.
5. 내보내기를 클릭합니다 ⬆ 아이콘을 클릭합니다.
6. CSV 파일을 열거나 파일을 저장할 것인지 선택합니다.

IP 장치 해상도

IP 식별 화면에는 자동 디바이스 확인 또는 수동 디바이스 확인으로 식별된 iSCSI 및 CIFS 또는 NFS 공유가 표시됩니다. 식별되지 않은 장치도 표시됩니다. 화면에는 장치의 IP 주소, 이름, 상태, iSCSI 노드 및 공유 이름이 포함됩니다. 성공적으로 식별된 디바이스의 비율도 표시됩니다.



수동으로 **IP** 장치 추가

IP 식별 화면에서 사용할 수 있는 수동 추가 기능을 사용하여 IP 장치를 OnCommand Insight에 수동으로 추가할 수 있습니다.

단계

1. Insight 웹 UI에 로그인합니다.
2. Manage * > * Device resolution * 을 클릭합니다
3. IP 식별 * 탭을 클릭합니다.
4. 추가 버튼을 클릭합니다.

   장치 추가 대화 상자가 표시됩니다

5. 주소, IP 주소 및 고유한 장치 이름을 입력합니다.

결과

입력한 장치가 IP 식별 탭의 장치 목록에 추가됩니다.

CSV 파일에서 **IP** 장치 **ID** 가져오기

CSV 파일에서 장치 식별 목록을 사용하여 IP 장치 식별 정보를 장치 해상도 기능으로 수동으로 가져올 수 있습니다.

시작하기 전에

장치 식별 정보를 가져오려면 올바른 형식의 CSV 파일이 있어야 합니다. IP 장치용 CSV 파일에는 다음 정보가 필요합니다.

주소
IP
이름

> 모범 사례로서 먼저 IP 식별 정보를 CSV 파일로 내보내고 해당 파일에서 원하는 대로 변경한 다음 파일을 다시 IP Identify로 가져오는 것이 좋습니다. 이렇게 하면 예상 열이 올바른 순서로 표시됩니다.

IP 식별 정보를 가져오려면

단계

1. Insight 웹 UI에 로그인합니다.
2. Manage * > * Device Resolution * 을 클릭합니다
3. IP 식별 * 탭을 선택합니다.
4. 식별 * > * 파일에서 식별 * 을 클릭합니다 .
   a. 가져올 CSV 파일이 포함된 폴더로 이동하고 원하는 파일을 선택합니다.

   입력한 장치는 IP 식별 탭의 장치 목록에 추가됩니다.

CSV 파일로 **IP** 장치 **ID**를 내보내는 중입니다

장치 해상도 기능을 사용하여 Insight에서 기존 IP 장치 ID를 내보낼 수 있습니다. 장치 ID를 수정한 다음 다시 Insight로 가져와 내보낸 ID와 유사한 장치를 식별하는 데 사용할 수 있도록 장치 ID를 내보낼 수 있습니다.

이 작업에 대해

IP 장치 ID를 CSV 파일로 내보낼 때 파일은 다음 정보를 표시된 순서대로 포함합니다.

주소
IP

이름

단계

1. Insight 웹 UI에 로그인합니다.
2. Manage * > * Device Resolution * 을 클릭합니다
3. IP 식별 * 탭을 선택합니다.
4. ID를 내보내려는 IP 장치 또는 장치를 선택합니다.
5. 내보내기를 클릭합니다 ⬆ 아이콘을 클릭합니다.
6. CSV 파일을 열거나 파일을 저장할 것인지 선택합니다.

기본 설정 탭에서 옵션 설정

장치 해상도 기본 설정 탭에서는 자동 해결 일정을 생성하고, 식별에서 포함하거나 제외할 스토리지 및 테이프 벤더 를 지정하고, DNS 조회 옵션을 설정할 수 있습니다.

자동 해결 일정

자동 해상도 스케줄은 자동 장치 해상도 실행 시기를 지정할 수 있습니다.

옵션을 선택합니다	설명
모든	일, 시간 또는 분 간격으로 자동 장치 해상도를 실행하려면 이 옵션을 사용합니다.
매일	이 옵션을 사용하여 매일 특정 시간에 자동 장치 해상도를 실행할 수 있습니다.
수동	이 옵션은 자동 장치 해상도만 수동으로 실행할 때 사용합니다.
모든 환경은 변동합니다	이 옵션을 사용하면 환경에 변화가 있을 때마다 자동 장치 해상도를 실행할 수 있습니다.

수동으로 지정하면 야간 자동 장치 해결이 비활성화됩니다.

DNS 처리 옵션

DNS 처리 옵션을 사용하여 다음 기능을 선택할 수 있습니다.

- DNS 조회 결과 처리가 활성화되면 DNS 이름 목록을 추가하여 확인된 장치에 추가할 수 있습니다.
- DNS 조회를 사용하여 NFS 공유에 액세스하는 iSCSI 초기자 및 호스트에 대해 자동 호스트 확인을 설정하려면 ""IP 자동 해상도:""를 선택할 수 있습니다. 이 옵션을 지정하지 않으면 FC 기반 해상도만 수행됩니다.
- 호스트 이름에 밑줄을 허용하고 결과에 표준 포트 별칭 대신 "연결됨" 별칭을 사용하도록 선택할 수 있습니다.

특정 스토리지 및 테이프 공급업체 포함 또는 제외

자동 해결을 위해 특정 스토리지 및 테이프 공급업체를 포함하거나 제외할 수 있습니다. 예를 들어 특정 호스트가 기존 호스트가 되어 새 환경에서 제외되어야 한다는 것을 알고 있는 경우 특정 공급업체를 제외할 수 있습니다. 이전에 제외했지만 더 이상 제외하지 않으려는 공급업체를 다시 추가할 수도 있습니다.

> 테이프에 대한 디바이스 확인 규칙은 해당 WWN의 공급업체가 공급업체 기본 설정에서 * 테이프 전용 * 으로 설정된 WWN에만 적용됩니다.

정규식 예

정규식을 소스 명명 전략으로 선택한 경우 정규식 예제를 OnCommand Insight 자동 확인 메서드에서 사용하는 자체 식에 대한 가이드로 사용할 수 있습니다.

정규식 서식 지정

OnCommand Insight 자동 확인을 위한 정규식을 만들 때 이라는 필드에 값을 입력하여 출력 형식을 구성할 수 있습니다 `FORMAT`.

기본 설정은 입니다 `\1`즉, 정규식과 일치하는 영역 이름이 정규식에 의해 만들어진 첫 번째 변수의 내용으로 대체됩니다. 정규식에서 변수 값은 괄호를 사용하여 만들어집니다. 괄호를 여러 개 사용하면 변수가 왼쪽에서 오른쪽으로 숫자로 참조됩니다. 변수는 출력 형식으로 어떤 순서로든 사용할 수 있습니다. 상수 텍스트는 에 추가하여 출력에도 삽입할 수 있습니다 `FORMAT` 필드에 입력합니다.

예를 들어 이 영역 명명 규칙에 다음과 같은 영역 이름이 있을 수 있습니다.

```
[Zone number]_[data center]_[hostname]_[device type]_[interface number]
```

- S123_Miami_hostname1_filer_FC1
- S14_Tampa_hostname2_switch_FC4
- S3991_Boston_hostname3_windows2K_FC0
- S44_Raleigh_hostname4_Solaris_FC1

출력을 다음 형식으로 지정할 수 있습니다.

```
        [hostname]-[data center]-[device type]
```

이렇게 하려면 변수에 호스트 이름, 데이터 센터 및 장치 유형 필드를 캡처하여 출력에 사용해야 합니다. 다음과 같은 정규식을 사용하면 됩니다.

```
.*?_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_.*
```

괄호는 세 개이므로 변수가 됩니다 `\1`, `\2` 및 `\3` 자동으로 채워집니다.

그런 다음 다음 다음 다음 형식을 사용하여 원하는 형식으로 출력을 받을 수 있습니다.

```
\2-\1-\3
```

출력은 다음과 같습니다.

```
hostname1-Miami-filer
hostname2-Tampa-switch
hostname3-Boston-windows2K
hostname4-Raleigh-solaris
```

변수 사이의 하이픈은 서식이 지정된 출력에 삽입된 상수 텍스트의 예를 제공합니다.

영역 이름을 보여 주는 예제 **1**

이 예제에서는 정규식을 사용하여 영역 이름에서 호스트 이름을 추출합니다. 다음 영역 이름과 유사한 항목이 있는 경우 정규식을 만들 수 있습니다.

- S0032_myComputer1Name - HBA0
- S0434_myComputer1Name - HBA1
- S0432_myComputer1Name - HBA3

호스트 이름을 캡처하는 데 사용할 수 있는 정규식은 다음과 같습니다.

```
S[0-9]+_([a-zA-Z0-9]*)[_-]HBA[0-9]
```

결과는 S로 시작하는 모든 영역과 일치하며 그 뒤에 숫자 조합, 밑줄, 영숫자 호스트 이름(myComputer1Name), 밑줄 또는 하이픈, 대문자 HBA 및 단일 숫자(0-9)가 옵니다. 호스트 이름만 *\1 * 변수에 저장됩니다.

정규식은 다음과 같이 해당 구성 요소로 나눌 수 있습니다.

- "S"는 영역 이름을 나타내고 식을 시작합니다. 이것은 영역 이름의 시작 부분에 있는 "S"만 일치합니다.
- 괄호 안의 문자 [0-9]는 "S" 뒤에 오는 문자가 0에서 9 사이의 숫자여야 함을 나타냅니다.
- 기호(+)는 이전 대괄호 안의 정보가 한 번 이상 존재해야 함을 나타냅니다.
- 밑줄(_)은 S 다음에 오는 숫자는 영역 이름에 밑줄만 사용해야 함을 의미합니다. 이 예제에서 영역 명명 규칙은 밑줄을 사용하여 호스트 이름과 영역 이름을 구분합니다.
- 필요한 밑줄 뒤에 괄호는 안에 포함된 패턴이 \1 변수에 저장됨을 나타냅니다.
- 괄호 문자 [A-zA-Z0-9]는 일치하는 문자가 대/소문자를 불문하고 모든 문자와 숫자임을 나타냅니다.
- 괄호 뒤에 있는 * (별표)는 괄호 안의 문자가 0번 이상 발생했음을 나타냅니다.
- 괄호 문자 [_-](밑줄 및 대시)는 영숫자 패턴 뒤에 밑줄이나 대시를 사용해야 함을 나타냅니다.
- 정규식의 문자 HBA는 영역 이름에 이 정확한 문자 시퀀스가 발생해야 함을 나타냅니다.
- 괄호 안의 마지막 문자 세트 [0-9]는 0에서 9 사이의 한 자리 숫자와 일치합니다.

예 **2**

이 예에서는 첫 번째 밑줄 "_"까지 건너뛰고, 그 다음 *E*와 모든 것을 두 번째 "_"까지 일치시킨 다음 그 이후의 모든 내용을 건너뜁니다.

- 영역: * `Z_E2FHDBS01_E1NETAPP`
- 호스트 이름: * `E2FHDBS01`
- 등록: * `.?(E.?).*?`

예 **3**

정규식(아래)의 마지막 섹션 주위의 괄호 "( )"는 호스트 이름인 부분을 식별합니다. VSAN3을 호스트 이름으로 사용하려는 경우 _([A-zA-Z0-9]). * 입니다

- 영역: * `A_VSAN3_SR48KENT_A_CX2578_SPA0`
- 호스트 이름: * `SR48KENT`
- 등록: * `_[a-zA-Z0-9]+_([a-zA-Z0-9]).*`

예제 **4**에서는 보다 복잡한 명명 패턴을 보여 줍니다

다음 영역 이름과 유사한 항목이 있는 경우 정규식을 만들 수 있습니다.

- myComputerName123-HBA1_Symm1_FA3
- myComputerName123-HBA2_Symm1_FA5
- myComputerName123-HBA3_Symm1_FA7

이러한 항목을 캡처하는 데 사용할 수 있는 정규식은 다음과 같습니다.

```
([a-zA-Z0-9]*)_.*
```

를 클릭합니다 `\1` 변수에는 만 포함됩니다 `myComputerName123` 이 식을 사용하여 계산한 후

정규식은 다음과 같이 해당 구성 요소로 나눌 수 있습니다.

- 괄호는 안에 포함된 패턴이 \1 변수에 저장됨을 나타냅니다.
- 괄호 문자 [A-zA-Z0-9]는 모든 문자(대/소문자 구분 없음) 또는 숫자가 일치함을 의미합니다.
- 괄호 뒤에 있는 * (별표)는 괄호 안의 문자가 0번 이상 발생했음을 나타냅니다.
- 정규식의 _ (밑줄) 문자는 영역 이름에 앞의 대괄호와 일치하는 영숫자 문자열 바로 뒤에 밑줄이 있어야 함을 의미합니다.
- 를 클릭합니다. (마침표)는 임의의 문자(와일드카드)와 일치합니다.
- 별표(*)는 이전 기간 와일드카드가 0번 이상 발생할 수 있음을 나타냅니다.

  즉, 조합을 나타냅니다. * 모든 문자를 임의의 횟수만큼 나타냅니다.

예제 **5** 패턴 없이 영역 이름을 표시합니다

다음 영역 이름과 유사한 항목이 있는 경우 정규식을 만들 수 있습니다.

- myComputerName_HBA1_Symm1_FA1
- myComputerName123_HBA1_Symm1_FA1

이러한 항목을 캡처하는 데 사용할 수 있는 정규식은 다음과 같습니다.

```
(.*?)_.*
```

1 변수는 첫 번째 영역 이름 예제에서 *myComputerName* 또는 *myComputerName123*(두 번째 영역 이름 예제의 경우)를 포함합니다. 따라서 이 정규식은 첫 번째 밑줄 이전의 모든 것과 일치합니다.

정규식은 다음과 같이 해당 구성 요소로 나눌 수 있습니다.

- 괄호는 안에 포함된 패턴이 \1 변수에 저장됨을 나타냅니다.
- 마침표 별표(. *)는 임의의 문자(횟수)와 일치합니다.
- 괄호 뒤에 있는 * (별표)는 괄호 안의 문자가 0번 이상 발생했음을 나타냅니다.
- ? Character는 greedy가 아닌 문자와 일치하는 항목을 만듭니다. 이렇게 하면 마지막 밑줄이 아니라 첫 번째 밑줄에서의 일치가 중지됩니다.
- 문자 _. * 는 발견된 첫 번째 밑줄과 그 뒤에 나오는 모든 문자와 일치합니다.

예제 **6** 컴퓨터 이름을 패턴으로 표시합니다

다음 영역 이름과 유사한 항목이 있는 경우 정규식을 만들 수 있습니다.

- storage1_Switch1_myComputerName123A_A1_FC1
- storage2_Switch2_myComputerName123B_A2_FC2 를 참조하십시오
- storage3_Switch3_myComputerName123T_A3_FC3

이러한 항목을 캡처하는 데 사용할 수 있는 정규식은 다음과 같습니다.

```
.*?_.*?_([a-zA-Z0-9]*[ABT])_.*
```

영역 명명 규칙에 더 많은 패턴이 있으므로 위의 식을 사용하여 A, A B 또는 A T로 끝나는 호스트 이름(예: myComputerName)의 모든 인스턴스(예: \1 변수에 해당 호스트 이름을 지정)와 일치시킬 수 있습니다.

정규식은 다음과 같이 해당 구성 요소로 나눌 수 있습니다.

- 마침표 별표(. *)는 임의의 문자(횟수)와 일치합니다.
- ? Character는 greedy가 아닌 문자와 일치하는 항목을 만듭니다. 이렇게 하면 마지막 밑줄이 아니라 첫 번째 밑줄에서의 일치가 중지됩니다.
- 밑줄 문자는 영역 이름의 첫 번째 밑줄과 일치합니다.

- 따라서 첫 번째. *?_ 조합은 첫 번째 영역 이름 예제에서 *storage1_* 문자와 일치합니다.
- 두 번째. *?_ 조합은 첫 번째 과 같이 동작하지만 첫 번째 영역 이름 예제에서 _Switch1__과 일치합니다.
- 괄호는 안에 포함된 패턴이 \1 변수에 저장됨을 나타냅니다.
- 괄호 문자 [A-zA-Z0-9]는 모든 문자(대/소문자 구분 없음) 또는 숫자가 일치함을 의미합니다.
- 괄호 뒤에 있는 * (별표)는 괄호 안의 문자가 0번 이상 발생했음을 나타냅니다.
- 정규식 [ABT]의 괄호 문자는 영역 이름의 단일 문자와 일치해야 하며 A, B 또는 T여야 합니다
- 괄호 뒤에 있는 _ (밑줄)은 [ABT] 문자 일치 뒤에 밑줄을 추가해야 함을 나타냅니다.
- 마침표 별표(. *)는 임의의 문자(횟수)와 일치합니다.

따라서 이 결과로 \1 변수에 다음과 같은 영숫자 문자열이 포함됩니다.

- 앞에 몇 개의 영숫자 문자와 두 개의 밑줄이 있습니다
- 뒤에 밑줄과 영숫자 문자를 차례로 사용했습니다.
- 세 번째 밑줄 앞에 A, B 또는 T의 마지막 문자가 있습니다.

예 **7**

- 영역: * `myComputerName123_HBA1_Symm1_FA1`
- 호스트 이름: * `myComputerName123`
- 등록: * `([a-zA-Z0-9]+)_.*`

예 **8**

이 예제에서는 First _ 앞에 있는 모든 항목을 찾습니다.

- 영역: * `MyComputerName_HBA1_Symm1_FA1`

`MyComputerName123_HBA1_Symm1_FA1`

- 호스트 이름: * `MyComputerName`
- 등록: * `(.?)_.`

예 **9**

이 예제에서는 1_ 이후의 모든 것과 두 번째 _ 까지의 모든 것을 찾습니다.

- 영역: * `Z_MyComputerName_StorageName`
- 호스트 이름: * `MyComputerName`
- 등록: * `.?(.?).*?`

예 **10**

이 예제에서는 영역 예제에서 "MyComputerName123"을 추출합니다.

- 영역: * `Storage1_Switch1_MyComputerName123A_A1_FC1`

`Storage2_Switch2_MyComputerName123B_A2_FC2`

`Storage3_Switch3_MyComputerName123T_A3_FC3`

- 호스트 이름: * `MyComputerName123`
- 등록: * **`.?.?`**`([a-zA-Z0-9]+)`**`[ABT]_.`**

예 **11**

- 영역: * `Storage1_Switch1_MyComputerName123A_A1_FC1`
- 호스트 이름: * `MyComputerName123A`
- 등록: * **`.?.?`**`([a-zA-z0-9]+)`**`.`**`*?`

예 **12**

^(circumflex 또는 caret) * 대괄호 안에 * * 는 식을 부정합니다. 예를 들어 [{캐럿} FF]는 대문자 또는 소문자 F를 제외한 모든 것을 의미하고 [{캐럿} a-z]는 소문자 a ~ z를 제외한 모든 것을 의미합니다. 위의 경우 _ 를 제외한 모든 것을 의미합니다. format 문은 출력 호스트 이름에 "-"를 추가합니다.

- 영역: * `mhs_apps44_d_A_10a0_0429`
- 호스트 이름: * `mhs-apps44-d`
- 등록: * `([^_])_([AB])`**`.`**`*`+OnCommand Insight 형식:

`([^_])_()`**`.`**`*`OnCommand Insight 형식:

예 **13**

이 예제에서 저장소 별칭은 "\"로 구분되며 표현식은 "\\"를 사용하여 문자열에 실제로 "\"가 사용되고 있으며 해당 별칭이 표현식 자체의 일부가 아닌 것을 정의해야 합니다.

- 스토리지 별칭: * `\Hosts\E2DOC01C1\E2DOC01N1`
- 호스트 이름: * `E2DOC01N1`
- 등록: * `\\`**`.?\\.`**`?\\(`**`.`**`*?)`

예 **14**

이 예에서는 영역 예에서 "PD-RV-W-AD-2"를 추출합니다.

- 영역: * `PD_D-PD-RV-W-AD-2_01`
- 호스트 이름: * `PD-RV-W-AD-2`
- 등록: * `[^-]-(`**`.-\d+)`**`.+`

예 **15**

이 경우 형식 설정은 호스트 이름에 "US-BV-"를 추가합니다.

- 영역: * `SRV_USBVM11_F1`
- 호스트 이름: * `US-BV-M11`
- 등록: * `SRV_USBV([A-Za-z0-9]+)_F[12]`
- 형식: * `US-BV-\1`

Insight 유지 관리

Insight를 처음 사용하는 경우 새로운 시스템을 설치했거나 시스템이 일정 시간 운영 중인지에 관계없이 Insight와 네트워크의 원활한 운영을 유지하기 위한 조치를 취해야 합니다. 주요 유지 관리 개념은 일반적으로 네트워크 변경 사항을 Insight에 수용해야 한다는 것입니다.

가장 일반적인 유지보수 작업은 다음과 같습니다.

- Insight 백업 유지 관리
- 만료된 Insight 라이센스를 업데이트하는 중입니다
- 데이터 소스 패치 조정
- 모든 획득 장치에서 Insight 버전을 업데이트합니다
- Insight에서 제거된 데이터 원본 삭제

Insight 관리

OnCommand Insight은 환경을 모니터링하여 위기 상황이 보고되기 전에 잠재적 문제를 조사할 수 있도록 합니다. 자산 대시보드는 요약 원형 차트, IOPS용 열 맵, 사용률이 가장 높은 10개의 스토리지 풀에 대한 대화형 차트를 제공합니다.

단계

1. Insight **Assets Dashboard** 를 열고 커서를 원형 차트 위로 이동하여 다음 세 가지 차트의 자산 분포를 검토합니다.
   - 공급업체별 용량 에는 각 공급업체의 총 스토리지 물리적 용량이 표시됩니다.
   - 계층별 용량은 각 스토리지 계층에 대해 사용 가능한 총 용량을 보여 줍니다.
   - 스위치 포트 원형 차트는 포트 제조업체를 표시하고 사용된 포트 비율을 표시합니다.
2. 환경 관련 정보 * 를 보고 사용 중인 환경의 용량, 용량 효율성, 사용된 FC 리소스 및 가상 인프라 통계에 대한 정보를 확인하십시오.
3. 스토리지 풀의 사용된 용량과 사용되지 않는 용량을 보려면 * 상위 10개 사용 풀 * 차트의 스토리지 풀 바 위에 커서를 놓습니다.
4. 스토리지 IOP * 히트맵에서 큰 텍스트(자산에 문제가 있음을 나타냄)로 표시되는 자산 이름을 클릭하여 해당 자산의 현재 상태를 요약하는 페이지를 표시합니다.

5. 자산 대시보드 * 의 오른쪽 아래 모서리에 있는 * 가상 머신 IOPS * 히트맵에서 큰 텍스트(자산에 문제가 있음을 나타냄)로 표시되는 자산 이름을 클릭하여 자산의 현재 상태를 요약하는 페이지를 표시합니다.
6. Insight 도구 모음에서 * Admin * 을 클릭합니다.
7. 빨간색 원으로 표시된 영역을 확인합니다.

   OnCommand Insightfob UI에서는 잠재적인 문제가 빨간색 원으로 표시됩니다.

8. 데이터 소스 * 를 클릭하여 모니터링된 모든 데이터 소스 목록을 검사합니다.

   빨간색 원으로 고정된 메시지가 포함된 * Status * 열이 있는 데이터 소스를 검사하고, * Impact * 가 High 또는 Medium 으로 나열됩니다. 이러한 항목은 테이블 상단에 있습니다. 이러한 데이터 소스의 문제는 해결해야 하는 네트워크의 중요한 부분에 영향을 미칩니다.

9. Insight를 실행하는 각 IP 주소의 상태를 확인하고 필요한 경우 획득 장치를 다시 시작하려면 * Acquisition Units * (획득 단위)를 클릭합니다
10. Insight 서버의 상위 인스턴스 모니터링을 보려면 * 상태 * 를 클릭하십시오.

OnCommand Insight 시스템 상태 모니터링

Insight 시스템 구성 요소의 현재 상태를 주기적으로 확인하여 각 구성 요소의 상태를 표시하고 문제가 있을 경우 알려줍니다.

단계

1. Insight트위브 UI에 로그인합니다.
2. Admin * 을 클릭하고 * Health * 를 선택합니다.

   상태 페이지가 표시됩니다.

3. 빨간색 원 앞에 있는 * Details * 열의 주의 상태에 특히 주의를 기울인 구성 요소의 현재 상태에 대한 요약을 봅니다. 이 열은 즉각적인 주의가 필요한 문제를 나타냅니다.

   상태 페이지에는 시스템 구성에 따라 다음과 같은 Insight 구성 요소 중 일부 또는 전체에 대한 정보가 표시됩니다.

구성 요소	테스트	세부 정보	표시됩니다
획득	재고 데이터 처리	로컬 획득 장치의 상태입니다	동시 폴링 데이터 소스의 수가 실행 풀 최대값의 75% 미만일 경우 ""OK"(기본값: 30). 사용이 75%를 초과하는 경우 "Acquisition is busy(획득 사용 중)", 폴링 간격을 늘리거나 원격 획득 장치를 더 추가하는 것이 좋습니다.

DWH	백업	데이터 웨어하우스 예약 백업의 상태입니다	DWH 예약 백업이 활성화된 경우 "OK(확인)" 및 마지막으로 성공한 DWH 백업 시간 그렇지 않으면 발견된 오류에 대한 정보가 표시됩니다.
DWH	ETL	데이터 웨어하우스 ETL의 상태입니다	"OK"와 마지막 성공한 DWH 빌드 시간(오류 없음). 그렇지 않으면 발견된 오류에 대한 정보가 표시됩니다.
서버	ASUP	ASUP 상태	""ASUP 활성화"" 및 가능한 경우 마지막으로 성공한 전화집 시간. "ASUP Failed"(ASUP 실패) - phonehome이 활성화되어 있지만 문제가 발생한 경우 백업 디렉토리가 유효하지 않은 경우 + "잘못된 백업 위치" + 마지막으로 성공한 전화 시간과 마지막으로 실패한 시도(있는 경우)를 표시합니다. 폰홈이 비활성화된 경우 + "'ASUP 비활성화'.
서버	자동 해상도	자동 장치 해상도 상태입니다	오류가 없으면 OK를 누릅니다. 확인 오류로 인해 해결 과정이 진행되지 않으면 자동 해결이 차단됩니다. 일반 디바이스의 75% 미만이 식별될 수 있는 경우 + ""낮은 성공률""

서버	Elasticsearch(Elasticsearch)	탄력적인 검색 데이터 저장소의 상태입니다	오류가 없으면 OK를 누릅니다. "서비스를 사용할 수 없습니다."라는 메시지가 표시됩니다. 둘 이상의 노드가 감지되면 + "클러스터 모드 감지됨" 사용된 힙 공간이 85%를 초과하는 경우 + "높은 메모리 사용률" "상태: 빨간색"은 탄성 검색에서 보고된 오류를 나타냅니다. 오류에 대한 정보를 표시하고 고객 지원 센터에 문의할 것을 권장합니다.
서버	CPU	Insight CPU 사용량	CPU 부하가 65% 미만이면 "OK" 시스템 CPU 부하가 높습니다. CPU 부하를 줄입니다." CPU 로드가 65%보다 큰 경우
서버	디스크 공간	디스크 공간의 상태입니다	디스크 여유 공간, Insight에서 사용 중인 디스크 공간 및 Insight용으로 예약된 권장 디스크 공간 디스크 사용률이 80%를 초과할 경우 ""디스크 공간 부족"".
서버	이벤트 버스	EventBus의 상태입니다	EventBus는 비어 있습니다. EventBus 대기열이 비어 있으면 EventBus 대기열 상태를 표시합니다.
서버	재고 데이터 처리	Insight 서버의 인벤토리 데이터 처리 기능 상태입니다	Insight 서버가 사용 중이 아니면 "OK"입니다. 서버가 마지막 시간의 75% 이상 사용 중이면 서버가 사용 중입니다. 에서는 데이터 소스를 더 추가하지 않을 것을 권장하며 환경을 여러 서버로 분할할 것을 권장합니다.

서버	MySQL	MySQL 데이터베이스의 상태입니다	문제가 발견되지 않으면 OK. "데이터베이스에 성능 문제가 있습니다. 일부 쿼리는 느린 쿼리 수가 5%를 초과할 경우 "(을) 실행하는 데 너무 오래 걸립니다. 데이터베이스 로그 파일은 지난 한 시간 동안 <size>보다 더 많이 성장했습니다. 오류 로그가 20KB를 초과할 경우 MySQL 로그 파일 ""을 확인하십시오.
서버	성능 아카이브	성능 아카이브의 상태입니다	"Performance archive is enabled" 또는 "Performance archive is not enabled".
서버	물리적 메모리	물리적 메모리의 상태입니다	메모리 사용량이 85% 미만일 경우 "OK". "메모리 사용량이 높습니다. 시스템 안정성을 위해 전체 메모리 공간을 줄일 수 있습니다."
서버	서비스 팩	서비스 팩 가용성	Insight에서 서비스 팩을 사용할 수 있는지 여부를 표시합니다. 서비스 팩을 사용할 수 있는 경우 에 지침이 표시됩니다.
서버	사용 정보	사용 정보 전송 상태	NetApp에 사용 정보 전송이 설정되었는지 여부를 표시합니다. 는 사용하지 않는 경우 활성화할 것을 권장합니다. 마지막으로 시도했거나 마지막으로 성공한 전송 시간을 표시합니다. + 발생한 문제에 대한 정보를 표시합니다.

서버	위반	미결 위반 상태	개방형 위반 건수가 위반 건수의 75% 미만이면 OK. "허용되는 최대 공개 위반 수는 <number>"입니다. 위반 허용 횟수가 위반 제한의 75%를 초과하는 경우. 에서는 성능 정책 구성을 검토할 것을 권장합니다. 위반 건수가 위반 한도인 경우 위반 관리자가 차단됩니다. +위반 관리자는 새로운 위반 사항을 작성할 수 없으며 성능 정책 구성을 검토할 것을 권장합니다.
서버	주간 백업	주별 백업의 상태입니다	주 단위 백업이 활성화된 경우 "OK(확인)", 그렇지 않으면 "Weekly backup is not enabled(주간 백업이 활성화되지 않음)"가 표시됩니다.

비활성 장치를 삭제하는 중입니다

비활성 상태인 장치를 삭제하면 데이터를 보다 깨끗하게 유지하고 탐색하기 쉽습니다.

이 작업에 대해

Insight에서 비활성 장치를 삭제하려면 다음을 수행합니다.

단계

1. 새 쿼리를 만들거나 기존 쿼리를 엽니다.
2. *generic device*, *host*, *storage*, *switch* 또는 _tape_asset 유형을 선택합니다.
3. 필터 추가 * 가 활성 * 이고 필터를 * 아니요 * 로 설정합니다.

   결과 테이블에는 활성 상태가 아닌 자산만 표시됩니다.

4. 삭제할 장치를 선택합니다.
5. Actions * 버튼을 클릭하고 * Delete Inactive Devices * 를 선택합니다.

   비활성 장치는 삭제되고 더 이상 Insight에 표시되지 않습니다.

시스템 및 사용자 작업 감사

예기치 않은 변경 내용을 찾으려면 OnCommand Insight 시스템 및 해당 사용자 작업의 감사 추적을 볼 수 있습니다. 감사 로그 메시지는 감사 페이지에 표시될 뿐만 아니라 syslog에 선택적으로 보낼 수 있습니다.

이 작업에 대해

Insight는 다음을 비롯하여 스토리지 네트워크 또는 스토리지 관리에 영향을 미치는 모든 사용자 활동에 대한 감사 항목을 생성합니다.

- 로그인 중입니다
- 경로를 승인 또는 승인 해제하는 중입니다
- 승인된 경로 업데이트 중
- 글로벌 정책 또는 임계값 설정
- 데이터 소스 추가 또는 제거
- 데이터 소스 시작 또는 중지
- 데이터 소스 속성을 업데이트하는 중입니다
- 작업 추가, 편집 또는 삭제
- 응용 프로그램 그룹을 제거하는 중입니다
- 장치 ID 식별 또는 변경
- 사용자를 생성합니다
- 사용자를 삭제합니다
- 사용자 역할 변경
- 사용자 수정(Guest à Admin)
- 사용자 로그아웃(강제 로그아웃 또는 수동 로그아웃)
- 획득 장치 삭제
- 라이센스 업데이트
- 백업 설정 중
- 백업을 사용하지 않도록 설정합니다
- ASUP 활성화(동일한 페이지에서 프록시 활성화 가 감사 로그에 보고됨)
- ASUP 비활성화(동일한 페이지에서 프록시 비활성화가 감사 로그에 보고됨)
- 보안 - 키를 다시 누르고 시스템 암호를 변경합니다.
- 자산의 주석 제거/추가
- CAC 사용자 로그온/로그오프
- CAC 사용자 세션 시간 초과

단계

1. 브라우저에서 Insight를 엽니다.
2. Admin * 을 클릭하고 * Audit * 을 선택합니다.

   감사 페이지에는 표에 감사 항목이 표시됩니다.

3. 테이블에서 다음 세부 정보를 볼 수 있습니다.

   - 시간 *

     변경 날짜 및 시간입니다

   - * 사용자 *

     감사 항목과 연결된 사용자의 이름입니다

   - * 역할 *

     게스트, 사용자 또는 관리자인 사용자 계정의 역할

   - * IP *

     감사 항목과 연결된 IP 주소입니다

   - * 작업 *

     감사 항목의 작업 유형입니다

   - * 세부 정보 *

     감사 항목의 세부 정보입니다

     데이터 소스 또는 애플리케이션과 같이 리소스에 영향을 미치는 사용자 활동이 있는 경우 세부 정보에는 리소스의 랜딩 페이지에 대한 링크가 포함됩니다.

     > 데이터 소스가 삭제되면 데이터 소스와 관련된 사용자 활동 세부 정보에 더 이상 데이터 소스의 랜딩 페이지에 대한 링크가 포함되지 않습니다.

4. 특정 기간(1시간, 3시간, 24시간, 3일, 7일)을 선택하여 감사 항목을 표시할 수 있습니다. Insight에서 선택한 기간 동안 최대 1000건의 위반 사례를 보여줍니다.

   한 페이지에 맞는 것보다 많은 데이터가 있는 경우 표 아래의 페이지 번호를 클릭하여 페이지별로 데이터를 탐색할 수 있습니다.

5. 테이블의 열 정렬 순서를 열 머리글의 화살표를 클릭하여 오름차순(위쪽 화살표) 또는 내림차순(아래쪽 화살표)으로 변경하고 기본 정렬 순서로 돌아가려면 다른 열 머리글을 클릭합니다.

   기본적으로 테이블에는 항목이 내림차순으로 표시됩니다.

6. 필터 * 상자를 사용하여 표에 원하는 항목만 표시할 수 있습니다.

사용자가 감사 항목만 표시합니다 `izzyk`를 **입력합니다** `izzyk 필터 * 상자에 입력합니다.

네트워크 위반 모니터링

Insight에서 성능 정책에 설정된 임계값으로 인해 위반을 생성하는 경우 위반 대시보드 를 사용하여 해당 위반 사항을 볼 수 있습니다. 대시보드에는 네트워크에서 발생하는 모든 위반 사항이 나열되며 이를 통해 문제를 찾아 해결할 수 있습니다.

단계

1. 브라우저에서 OnCommand Insight를 엽니다.
2. Insight 도구 모음에서 * 대시보드 * 를 클릭하고 * 위반 대시보드 * 를 선택합니다.

   위반 대시보드가 표시됩니다.

3. Policies * 파이 차트에서는 다음과 같은 방법으로 * 위반 항목을 사용할 수 있습니다.
   - 특정 정책 또는 메트릭에 대해 발생한 총 위반의 비율을 표시하기 위해 차트의 임의 슬라이스 위에 커서를 배치할 수 있습니다.
   - 차트의 한 조각을 "확대"하려면 차트 조각을 클릭하면 나머지 차트에서 멀리 이동하여 해당 슬라이스를 더 강조하고 연구할 수 있습니다.
   - 를 클릭할 수 있습니다 ⤢ 아이콘을 클릭하여 원형 차트를 전체 화면 모드로 표시하고 을 클릭합니다 ⤡ 다시 한 번 클릭하여 원형 차트를 최소화합니다. 파이 차트는 최대 5개의 조각을 포함할 수 있으므로 위반을 생성하는 6개의 정책이 있는 경우 Insight는 5번째 슬라이스와 6번째 슬라이스를 ""기타" 슬라이스로 결합합니다. Insight는 가장 많은 위반 사항을 첫 번째 슬라이스에 할당하고 두 번째 슬라이스에 가장 많은 위반 사항을 할당합니다.
4. 다음과 같은 방법으로 * 위반 이력 * 차트를 사용할 수 있습니다.
   - 차트 위에 커서를 놓으면 특정 시간에 발생한 총 위반 수와 지정된 각 메트릭에 대해 발생한 총 위반 횟수를 표시할 수 있습니다.
   - 범례 레이블을 클릭하여 범례와 관련된 데이터를 차트에서 제거할 수 있습니다.

     범례를 클릭하여 데이터를 다시 표시합니다.

   - 를 클릭할 수 있습니다 ⤢ 아이콘을 클릭하여 차트를 전체 화면 모드로 표시하고 을 클릭합니다 ⤡ 다시 한 번 클릭하여 원형 차트를 최소화합니다.
5. 다음과 같은 방법으로 * 위반 표 * 를 사용할 수 있습니다.
   - 를 클릭할 수 있습니다 ⤢ 아이콘을 클릭하여 전체 화면 모드로 테이블을 표시하고 을 클릭합니다 ⤡ 다시 한 번 클릭하여 원형 차트를 최소화합니다.

     창 크기가 너무 작은 경우 위반 테이블에는 세 개의 열만 표시되지만 을 클릭하면 표시됩니다 ⤢, 추가 열(최대 7개)이 표시됩니다.

   - 특정 기간(* 1h *, * 3h *, * 24h *, * 3D *, * 7d *, 및 * 30d *), Insight에서 선택한 기간 동안 최대 1000건의 위반 사례를 보여줍니다.
   - 필터 * 상자를 사용하여 원하는 위반만 표시할 수 있습니다.
   - 열 머리글의 화살표를 클릭하여 테이블의 열 정렬 순서를 오름차순(위쪽 화살표) 또는 내림차순(아래쪽 화살표)으로 변경할 수 있습니다. 기본 정렬 순서로 돌아가려면 다른 열 머리글을 클릭합니다.

기본적으로 테이블에는 위반사항이 내림차순으로 표시됩니다.

- ID 열에서 위반을 클릭하여 위반 기간 동안 자산 페이지를 표시할 수 있습니다.
- 설명 열에서 리소스 링크(예: 스토리지 풀 및 스토리지 볼륨)를 클릭하여 해당 리소스와 연결된 자산 페이지를 표시할 수 있습니다.
- 정책 열에서 성능 정책 링크를 클릭하여 정책 편집 대화 상자를 표시할 수 있습니다.

  너무 많거나 너무 많은 위반이 발생하는 경우 정책의 임계값을 조정할 수 있습니다.

- 한 페이지에 맞는 것보다 많은 데이터가 있는 경우 페이지 번호를 클릭하여 페이지별로 데이터를 탐색할 수 있습니다.
- 를 클릭할 수 있습니다 ✖ 을 클릭하여 위반 사항을 취소합니다.

획득 장치 상태

Acquisition Unit(획득 장치) 화면에서는 상태 및 현재 오류를 포함하여 모든 획득 장치를 볼 수 있습니다.

서버에 연결된 Insight 획득 장치의 상태가 * Admin * > * Acquisition Units * (획득 단위) 표에 표시됩니다. 이 표에는 각 획득 장치에 대한 다음 정보가 표시됩니다.

- * 이름 *
- * IP *
- * Status * 는 획득 장치의 작동 상태입니다.
- **Last** 보고에 보고됨 획득 장치에 연결된 데이터 소스가 마지막으로 보고된 시간을 표시합니다.
- * 참고 * AU와 관련된 사용자 입력 메모를 표시합니다.

목록의 획득 장치에 문제가 있는 경우 Status(상태) 필드에 문제에 대한 간략한 정보가 포함된 빨간색 원이 표시됩니다. 획득 장치 문제는 데이터 수집에 영향을 줄 수 있으므로 조사해야 합니다.

획득 장치를 다시 시작하려면 장치 위로 마우스를 가져가 나타나는 *Restart Acquisition Unit*(획득 장치 재시작) 버튼을 클릭합니다.

텍스트 메모를 추가하려면 획득 장치 위로 마우스를 가져가 나타나는 *Add Note* 단추를 클릭합니다. 가장 최근에 입력한 메모만 표시됩니다.

Insight 데이터베이스를 복원하는 중입니다

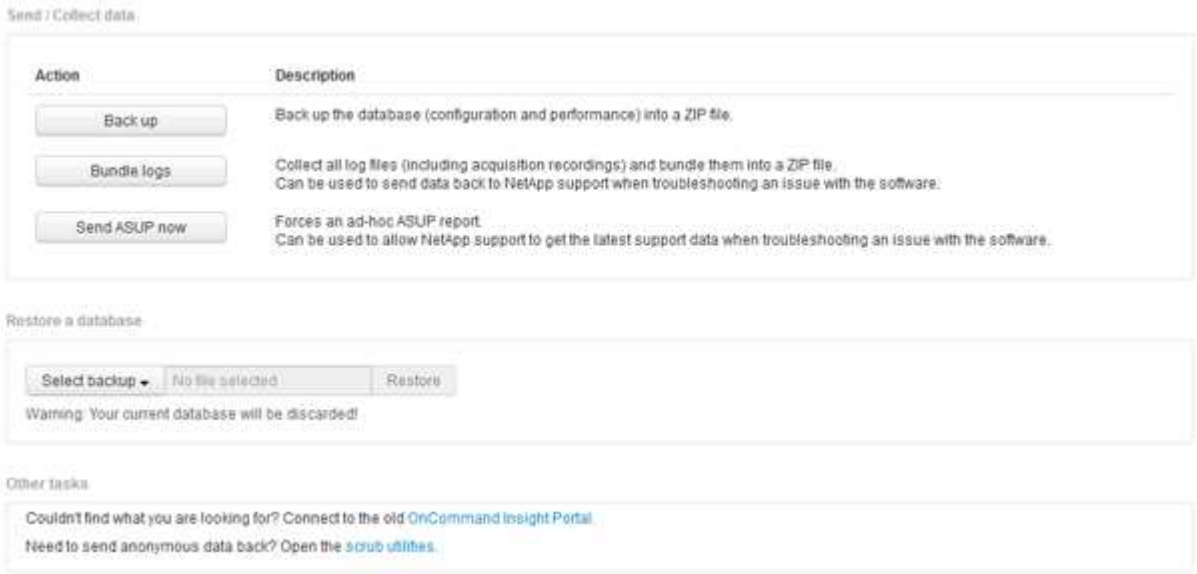
검증된 백업 파일에서 Insight 데이터베이스를 복원하려면 문제 해결 옵션을 사용합니다. 이 작업은 현재 OnCommand Insight 데이터를 완전히 대체합니다.

시작하기 전에

- 모범 사례:** OnCommand Insight 데이터베이스를 복원하기 전에 수동 백업 프로세스를 사용하여 현재 데이터베이스의 복사본을 만듭니다. 복원하려는 백업 파일 확인 복원하려는 파일이 포함된 백업이 성공했는지 확인합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 문제 해결 * 을 클릭합니다.



3. 데이터베이스 복원 섹션의 * 백업 선택 * 메뉴에서 복원할 백업 파일을 선택합니다.
4. 복원 * 을 클릭합니다.
5. 모든 데이터가 교체된다는 경고가 나타나면 * OK * 를 클릭합니다

   복원 작업의 상태가 복원 페이지에 표시됩니다.

만료된 라이센스를 업데이트하는 중입니다

하나 이상의 Insight 라이센스가 만료된 경우 원래 라이센스를 설치할 때와 동일한 절차를 사용하여 라이센스를 빠르게 업데이트할 수 있습니다.

단계

1. 메모장 같은 텍스트 편집기에서 NetApp Support에서 받은 새 라이센스 파일을 열고 라이센스 키 텍스트를 Windows 클립보드로 복사합니다.
2. 브라우저에서 OnCommand Insight를 엽니다.
3. 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.

   이 작업을 수행하면 현재 활성화된 모든 Insight 라이센스에 새 라이센스가 추가됩니다.

9. 저장 * 을 클릭합니다.
10. Insight 소비 라이센싱 모델을 사용하는 경우 사용 섹션에서 * 사용 정보를 NetApp * 으로 전송 가능 확인란을 선택해야 합니다. 프록시는 환경에 맞게 적절히 구성 및 설정되어 있어야 합니다.

라이센스가 더 이상 규정을 준수하지 않습니다

Insight Licenses 페이지에서 "Not Compliant" 메시지가 표시되면 Insight에서 회사의 라이센스된 것보다 테라바이트를 더 많이 관리하고 있는 것입니다.

"규정을 준수하지 않음" 메시지는 회사가 현재 Insight에서 관리하는 것보다 TB를 적게 지불했다는 의미입니다. 관리 테라바이트 및 라이센스 용량(TB)의 차이가 규정 미준수 메시지 옆에 표시됩니다.

Insight 시스템의 작동은 영향을 받지 않지만, NetApp 담당자에게 문의하여 라이센스 범위를 늘리고 적절한 라이센스를 업데이트해야 합니다.

이전 **Insight** 버전의 라이센스 대체

이전 버전과 호환되지 않는 새 Insight 버전을 구입한 경우 이전 라이센스를 새 라이센스로 교체해야 합니다.

새 라이센스를 설치할 때 라이센스 키 텍스트를 저장하기 전에 * 바꾸기 * 작업을 선택해야 합니다.

서비스 팩을 적용하는 중입니다

서비스 팩을 주기적으로 사용할 수 있으며, OnCommand Insight의 수정 및 개선 사항을 활용할 수 있도록 서비스 팩을 적용할 수 있습니다.

시작하기 전에

- 서비스 팩 파일을 다운로드해야 합니다(예: `7.2service_pack_1.patch`)를 참조하십시오.
- 모든 패치를 승인해야 합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 패치 * 를 클릭합니다.
3. 작업 버튼에서 * 패치 적용 * 을 선택합니다.
4. 데이터 소스 패치 적용 * 대화 상자에서 * 찾아보기 * 를 클릭하여 서비스 팩 파일을 찾습니다.
5. 패치 이름 *, * 설명 *, * 영향 받는 데이터 소스 유형 * 을 검사하여 데이터 소스가 영향을 받는지 여부를 확인하고, 서비스 팩에 포함된 개선 사항을 설명하는 * 세부 정보 * 를 확인합니다.
6. 선택한 서비스 팩이 올바르면 * 패치 적용 * 을 클릭합니다.

   서비스 팩은 자동으로 승인되므로 추가 조치가 필요하지 않습니다.

특수 문제 해결 보고서 준비

Insight는 소프트웨어 설치 후 설정한 ASUP 시스템을 통해 NetApp 고객 지원 팀에 정보를 자동으로 전송합니다. 그러나 문제 해결 보고서를 만들고 지원 팀에 특정 문제에 대한 케이스를 개설할 수 있습니다.

Insight의 툴을 사용하여 수동 Insight 백업을 수행하고 로그를 번들로 묶어 NetApp 고객 지원 센터로 보낼 수 있습니다.

OnCommand Insight 데이터베이스를 수동으로 백업합니다

OnCommand Insight 데이터베이스에 대해 주별 백업을 사용하도록 설정한 경우 필요한 경우 데이터베이스를 복구하는 데 사용할 수 있는 복사본을 자동으로 생성합니다. 복원 작업 전에 백업을 생성하거나 NetApp 기술 지원 부서에 지원을 요청해야 하는 경우 백업을 생성할 수 있습니다 `.zip` 파일을 수동으로 선택합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 문제 해결 * 을 클릭합니다.
3. 데이터 보내기/수집 섹션에서 * 백업 * 을 클릭합니다.
4. 파일 저장 * 을 클릭합니다.
5. 확인 * 을 클릭합니다.

지원을 위한 로그 번들링

Insight 소프트웨어의 문제를 해결할 때 "gz" 형식을 사용하여 NetApp 고객 지원 본부에 전송되는 로그 및 수집 기록의 zip 파일을 신속하게 생성할 수 있습니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 문제 해결 * 을 클릭합니다.
3. 데이터 보내기/수집 섹션에서 * 번들 로그 * 를 클릭합니다.
4. 파일 저장 * 을 클릭합니다.
5. 확인 * 을 클릭합니다.

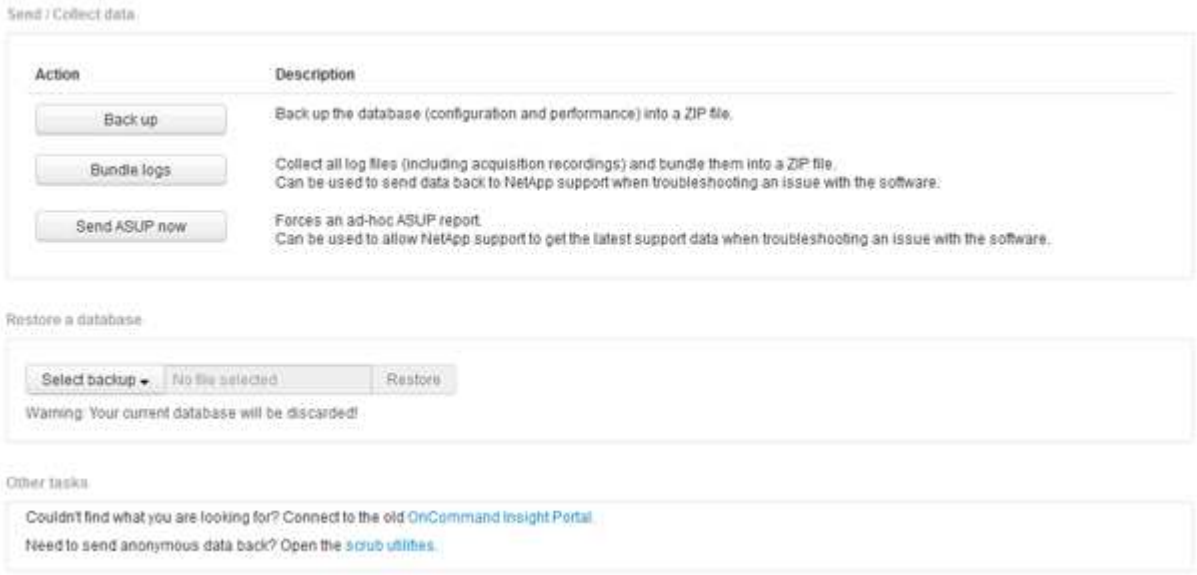
NetApp Support에 정보 전송

NetApp ASUP(자동화된 지원) 기능은 문제 해결 정보를 NetApp 고객 지원 팀에 직접 전송합니다. 특수 보고서를 강제로 전송할 수 있습니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 설정 * 을 클릭합니다.

3. Backup/ASUP * 탭을 클릭합니다.
4. 데이터 보내기/수집 영역에서 * ASUP 지금 전송 * 을 클릭하여 로그, 기록 및 백업을 NetApp 지원에 제출합니다.



전송을 지원하기 위해 데이터를 스크러빙합니다

보안 환경을 갖춘 고객은 NetApp 고객 서비스와 통신하여 데이터베이스 정보를 그대로 유지하면서 발생하는 문제를 해결해야 합니다. OnCommand Insight 스크럽 유틸리티를 사용하면 키워드 및 패턴의 포괄적인 사전을 설정하여 중요한 데이터를 "정리"하고 스크러빙된 파일을 고객 지원 센터로 보낼 수 있습니다.

단계

1. 웹 UI에서 * Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
2. 다른 작업 영역의 페이지 하단에서 * 스크럽 유틸리티 * 링크를 클릭합니다.

   사전, 스크럽 데이터 및 빌드 사전의 조회, 사용자 지정 키워드, 정규식 등 여러 가지 스크럽 섹션이 있습니다.

.

+ .. 사전의 조회 섹션에서 대체 값을 표시할 코드를 입력하거나 값을 입력하여 해당 값을 대체하는 코드를 표시합니다. 참고: 조회를 수행하기 전에 지원 데이터에서 스크럽할 값을 식별하기 위해 사전을 * 구축 * 해야 합니다.

1. 지원 데이터에서 스크럽할 키워드를 직접 추가하려면 * 사용자 정의 키워드 * 섹션에서 메뉴 [사용자 정의 키워드 추가]를 클릭합니다. 키워드를 입력하고 * 저장 * 을 클릭합니다. 키워드가 사전에 추가됩니다.
2. 패턴(regexp) * 을 확장합니다. 새 패턴을 입력하기 위한 대화 상자를 표시하려면 * 추가 * 를 클릭합니다.
3. 정규식을 사용하여 스크럽할 단어나 구를 식별하려면 * 정규식 * 섹션에 패턴이나 패턴을 입력합니다. 메뉴 클릭: 작업 [정규식 추가], 패턴의 이름 및 필드에 정규식을 입력하고 * 저장 * 을 클릭합니다. 사전에 정보가 추가되었습니다.

   패턴은 정규식 캡처 그룹을 식별하기 위해 둥근 괄호로 묶어야 합니다.

4. 빌드 사전** 섹션에서 * 빌드 * 를 클릭하여 OnCommand Insight 데이터베이스에서 중요한 것으로 식별되는 모든 단어의 사전 컴파일을 시작합니다.

   완료되면 개정된 사전을 사용할 수 있음을 알리는 메시지가 표시됩니다. 데이터베이스 설명에는 사전에 있는 키워드 수를 나타내는 줄이 포함됩니다. 사전에 있는 키워드의 정확성을 확인하십시오. 문제를 찾고 사전을 다시 빌드하려면 데이터베이스 블록에서 * 재설정 * 을 클릭하여 OnCommand Insight 데이터베이스에서 수집한 모든 키워드를 사전에서 제거합니다. 메시지가 표시되면 다른 키워드는 삭제되지 않습니다. 스크럽 유틸리티로 돌아가서 사용자 지정 키워드를 다시 입력합니다.

5. 스크럽 사전을 만든 후 이를 사용하여 로그, XML 또는 기타 텍스트 파일을 스크럽하여 데이터를 익명으로 만들 수 있습니다.
6. 로그, XML 또는 기타 텍스트 파일을 스크럽하려면 * 스크럽 데이터 * 섹션에서 찾아보기를 클릭하여 파일을 찾은 다음 * 스크럽 파일 * 을 클릭합니다.

고급 문제 해결

OnCommand Insight 구성을 완료하려면 고급 문제 해결 도구를 사용해야 합니다. 이러한 도구는 브라우저에서 실행되며 * Admin * > * Troubleshooting * 페이지에서 열립니다.

브라우저에서 고급 문제 해결 도구를 열려면 페이지 하단의 * 고급 문제 해결 * 링크를 클릭하십시오.

고급 문제 해결 도구를 사용하면 다양한 보고서, 시스템 정보, 설치된 패키지 및 로그를 볼 수 있을 뿐만 아니라 서버 또는 획득 장치 재시작, DWH 주석 업데이트, 주석 가져오기 등의 다양한 작업을 수행할 수 있습니다.

사용 가능한 모든 옵션은 고급 문제 해결 페이지를 참조하십시오.

동적 데이터를 무시할 시간 구성

OnCommand Insight에서 사용된 용량과 같은 동적 데이터 업데이트를 무시하는 시간을 구성할 수 있습니다. 기본 6시간이 사용되고 구성이 변경되지 않으면 기본 시간 이후까지 보고서가 동적 데이터로 업데이트되지 않습니다. 이 옵션은 동적 데이터만 변경될 때 업데이트를 지연하므로 성능이 향상됩니다.

이 작업에 대해

이 옵션에 값이 설정되어 있으면 OnCommand Insight는 다음 규칙에 따라 동적 데이터를 업데이트합니다.

- 구성을 변경하지 않고 용량 데이터가 변경되면 데이터가 업데이트되지 않습니다.
- 구성 변경 이외의 동적 데이터는 이 옵션에 지정된 시간 제한 이후에만 업데이트됩니다.
- 구성이 변경되면 구성 및 동적 데이터가 업데이트됩니다.

이 옵션의 영향을 받는 동적 데이터에는 다음이 포함됩니다.

- 용량 위반 데이터
- 파일 시스템에 할당된 용량 및 사용된 용량
- 하이퍼바이저
  - 가상 디스크 사용된 용량

    - 가상 머신 사용 용량
- 내부 볼륨
    - 데이터 할당 용량
    - 사용된 데이터 용량
    - 중복제거 절약
    - 마지막으로 알려진 액세스 시간입니다
    - 마지막 스냅샷 시간입니다
    - 기타 사용된 용량
    - 스냅샷 수
    - 사용된 스냅샷 용량
    - 사용된 총 용량입니다
- iSCSI 세션 초기자 IP, 대상 세션 ID 및 초기자 세션 ID
- 사용된 용량 qtree 할당량
- 사용된 할당량 파일 및 사용된 용량
- 스토리지 효율성 기술, 이득/손실 및 잠재적 이득/손실
- 스토리지 풀
    - 사용된 데이터 용량
    - 중복제거 절약
    - 기타 사용된 용량
    - 사용된 스냅샷 용량
    - 사용된 총 용량입니다
- 볼륨
    - 중복제거 절약
    - 마지막으로 알려진 액세스 시간입니다
    - 사용된 용량

단계

1. Insight 도구 모음에서 * Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
2. 다른 작업 영역의 페이지 하단에서 * 고급 문제 해결 * 링크를 클릭합니다.
3. 고급 설정 * 탭을 클릭하고 획득 동적 속성 섹션에서 OnCommand Insight가 획득 동적 속성의 동적 데이터를 무시해야 하는 시간을 입력합니다.
4. 저장 * 을 클릭합니다.
5. (선택 사항) 획득 장치를 다시 시작하려면 * Restart Acquisition Unit(획득 장치 재시작) * 링크를 클릭합니다.

   로컬 획득 장치를 다시 명시하면 모든 OnCommand Insight 데이터 소스 뷰가 다시 로드됩니다. 이 변경 사항은 다음 폴링 중에 적용되므로 획득 장치를 다시 시작할 필요가 없습니다.

고객 지원을 위한 로그를 생성하는 중입니다

고객 지원 본부에서 요청하는 경우 문제 해결을 위해 서버, 획득 또는 원격 로그를 생성합니다.

이 작업에 대해

NetApp 고객 지원을 요청하는 경우 이 옵션을 사용하여 로그를 생성합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
2. 다른 작업 영역의 페이지 하단에서 * 고급 문제 해결 * 을 클릭합니다.
3. 고급 메뉴의 다음 페이지에서 * 문제 해결 * 링크를 클릭합니다.
4. 로그 * 탭을 클릭하고 다운로드할 로그 파일을 선택합니다.

   로그를 열거나 로그를 로컬로 저장할 수 있는 대화 상자가 열립니다.

시스템 정보를 표시합니다

OnCommand Insight 서버가 배포된 시스템에 대한 Microsoft Windows IP 구성 정보를 표시할 수 있습니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
2. 다른 작업 영역의 페이지 하단에서 * 고급 문제 해결 * 링크를 클릭합니다.
3. 고급 문제 해결 페이지에서 * 보고서 * 탭을 클릭합니다.
4. 시스템 정보 * 를 클릭합니다.

   Windows IP 구성에는 호스트 이름, DNS, IP 주소, 서브넷 마스크, OS 정보 등의 정보가 포함됩니다. 메모리, 부팅 장치 및 연결 이름입니다.

설치된 **OnCommand Insight** 구성 요소 나열

설치된 OnCommand Insight 구성 요소의 목록을 표시할 수 있습니다. 그 중에는 인벤토리, 용량, 치수, 및 데이터 웨어하우스 뷰 고객 지원 팀에서 이 정보를 요청하거나 설치된 소프트웨어 버전과 설치 시기를 확인할 수 있습니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
2. 다른 작업 영역의 페이지 하단에서 * 고급 문제 해결 * 링크를 클릭합니다.
3. 고급 문제 해결 페이지에서 * 보고서 * 탭을 클릭합니다.
4. 설치된 소프트웨어 패키지 * 를 클릭합니다.

데이터베이스 객체 수 계산

OnCommand Insight 데이터베이스의 개체 수를 확인하려면 배율 계산 기능을 사용합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
2. 다른 작업 영역의 페이지 하단에서 * 고급 문제 해결 * 링크를 클릭합니다.
3. 고급 문제 해결 페이지에서 * 보고서 * 탭을 클릭합니다.
4. 계산된 배율 * 을 클릭합니다.

OnCommand Insight 서버를 다시 시작합니다

OnCommand Insight 서버를 다시 시작하면 페이지를 새로 고치고 OnCommand Insight 포털에 다시 로그인합니다.

이 작업에 대해

> 이 두 옵션은 모두 NetApp 고객 지원 본부의 요청에 따라 사용해야 합니다. 다시 시작하기 전에 확인 메시지가 없습니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
2. 다른 작업 영역의 페이지 하단에서 * 고급 문제 해결 * 링크를 클릭합니다.
3. 고급 메뉴의 다음 페이지에서 * 작업 * 탭을 클릭합니다.
4. 서버 재시작 * 을 클릭합니다.

마이그레이션 옵션을 사용하여 **MySQL** 데이터를 이동하는 중입니다

MySQL DATA 디렉터리를 다른 디렉터리로 마이그레이션 을 사용할 수 있습니다. 현재 데이터 디렉토리를 유지할 수 있습니다. 문제 해결 메뉴에서 마이그레이션 옵션을 사용하거나 명령줄을 사용할 수 있습니다. 이 절차에서는 * Troubleshooting * > * Migrate MySQL data * 옵션을 사용하는 방법에 대해 설명합니다.

이 작업에 대해

현재 데이터 디렉토리를 유지하는 경우 해당 디렉토리가 백업으로 유지되고 이름이 변경됩니다.

단계

1. 웹 UI에서 * Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
2. 고급 문제 해결 * 을 클릭합니다.
3. Actions * 탭을 선택합니다
4. Migrate MySQL Data * 를 선택합니다.

5. 데이터를 마이그레이션할 경로를 입력합니다.
6. 기존 데이터 디렉터리를 유지하려면 * 기존 데이터 디렉터리 유지 * 를 선택합니다
7. 마이그레이션 * 을 클릭합니다.

명령줄을 사용하여 **MySQL** 데이터를 이동하는 중입니다

MySQL DATA 디렉터리를 다른 디렉터리로 마이그레이션 을 사용할 수 있습니다. 현재 데이터 디렉토리를 유지할 수 있습니다. 문제 해결 메뉴에서 마이그레이션 옵션을 사용하거나 명령줄을 사용할 수 있습니다. 이 절차에서는 명령줄을 사용하는 방법에 대해 설명합니다.

이 작업에 대해

현재 데이터 디렉토리를 유지하는 경우 해당 디렉토리가 백업으로 유지되고 이름이 변경됩니다.

Migrate MySQL Data 유틸리티를 사용하거나 을 사용할 수 있습니다 `java -jar mysqldatamigrator.jar` 의 OnCommand Insight 경로에 있는 옵션 `\bin\mysqldatamigrator` 다음 매개변수를 사용해야 하는 경우:

- 필수 매개변수
  - * -경로 *

    데이터 폴더가 복사될 새 데이터 경로입니다.
- 선택적 매개 변수입니다
  - * - myCnf <my .cnf file> *

    CNF 파일의 경로입니다. 기본값은 입니다 `<install path>\mysql\my.cnf`. 기본 MySQL이 아닌 MySQL이 사용되는 경우에만 이 플래그를 사용하십시오.
  - * -doBackup *

    이 플래그를 설정하면 현재 데이터 폴더의 이름이 바뀌지만 삭제되지는 않습니다.

단계

1. 명령줄 툴은 여기에서 액세스할 수 있습니다. `<installation path>` bin\mysqldatamigrator\mysqldatamigrator.jar'

사용 예

```
java -jar mysqldatamigrator.jar -path "C:\<new path>" -doBackup
```

주석 업데이트 적용

주석을 변경한 후 즉시 보고서에 사용하려면 힘 주석 옵션 중 하나를 사용합니다.

단계

1. 웹 UI에서 * Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
2. 페이지 하단에서 * 고급 문제 해결 * 링크를 클릭합니다.
3. 작업 * 탭을 클릭합니다.
4. 다음 옵션 중 하나를 선택합니다.
   - * DWH 주석 * 을 업데이트하여 보고서에 데이터 웨어하우스의 주석 업데이트를 사용하도록 합니다.
   - * DWH 주석 업데이트(삭제됨) * 데이터 웨어하우스의 주석 업데이트(삭제된 개체 포함)를 보고서에 사용하도록 강제합니다.

서버 리소스의 상태 확인

이 옵션은 서버 메모리, 디스크 공간, OS, CPU 및 OnCommand Insight 데이터베이스 정보(InnoDB 데이터 크기 포함)와 데이터베이스가 상주하는 디스크 여유 공간 등의 OnCommand Insight 서버 정보를 표시합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
2. 다른 작업 영역의 페이지 하단에서 * OnCommand Insight 포털 * 링크를 클릭합니다.
3. 고급 메뉴의 다음 페이지에서 * 문제 해결 * 링크를 클릭합니다.
4. 서버 리소스 상태 * 를 클릭합니다.
   - 고급 OnCommand Insight 사용자의 경우: * 관리자는 일부 SQL 테스트를 실행하여 정보 요약 끝에 있는 버튼을 통해 데이터베이스와 서버의 응답 시간을 확인할 수 있습니다. 이 옵션은 서버 리소스가 부족할 경우 경고를 표시합니다.

고스트 데이터 소스 찾기

장치를 제거했지만 장치 데이터가 남아 있는 경우 고스트 데이터 원본을 찾아서 제거할 수 있습니다.

단계

1. 웹 UI에서 * Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
2. 다른 작업 영역의 페이지 하단에서 * 고급 문제 해결 * 링크를 클릭합니다.
3. 보고서 * 탭에서 * 고스트 데이터 소스 * 링크를 클릭합니다.

   OnCommand Insight는 장치 정보가 포함된 독창자 목록을 생성합니다.

누락된 디스크 모델을 추가하는 중입니다

알 수 없는 디스크 모델로 인해 획득에 실패한 경우 누락된 디스크 모델을 에 추가할 수 있습니다 `new_disk_models.txt` 촬영 후 다시 실행합니다.

이 작업에 대해

OnCommand Insight 획득을 통해 스토리지 디바이스를 폴링하는 과정에서 스토리지 디바이스의 디스크 모델이 읽힙니다. 공급업체가 Insight에서 알지 못하는 새로운 디스크 모델을 어레이에 추가하거나, Insight가 찾는 모델 번호와 스토리지 장치에서 반환된 모델 번호가 일치하지 않으면 해당 데이터 소스를 획득하지 못하고 오류가 발생합니다. 이러한 오류를 방지하려면 Insight에 알려진 디스크 모델 정보를 업데이트해야 합니다. 업데이트, 패치 및 유지 관리 릴리즈를 통해 새로운 디스크 모델이 Insight에 추가됩니다. 그러나 패치나 업데이트를 기다리는 대신 이 정보를 수동으로 업데이트할 수 있습니다.

OnCommand Insight는 5분마다 디스크 모델 파일을 읽기 때문에 입력한 새 데이터 모델 정보가 자동으로 업데이트됩니다. 변경 사항을 적용하기 위해 서버를 다시 시작할 필요는 없지만 서버 및 원격 획득 장치(RA)를 다시 시작하여 다음 업데이트 전에 변경 사항을 적용할 수 있습니다.

디스크 모델 업데이트가 에 추가됩니다 `new_disk_models.txt` 에 있는 파일`<SANScreenInstallDir>\wildfly\standalone\deployments\datasources.war` 디렉토리. 를 업데이트하기 전에 새 디스크 모델을 설명하는 데 필요한 정보를 파악합니다 `new_disk_models.txt` 파일. 파일의 정보가 부정확하면 잘못된 시스템 데이터가 생성되고 획득 실패를 초래할 수 있습니다.

Insight 디스크 모델을 수동으로 업데이트하려면 다음 지침을 따르십시오.

단계

1. 디스크 모델에 대한 적절한 정보를 찾습니다.
2. 텍스트 편집기를 사용하여 를 엽니다 `new_disk_models.txt` 파일.
3. 새 데이터 원본에 필요한 정보를 추가합니다.
4. 에 파일을 저장합니다 `<SANScreenInstallDir>\wildfly\standalone\deployments\datasources.war` 서버의 디렉터리입니다.
5. 를 백업합니다 `new_disk_models.txt` 파일을 안전한 위치에 보관합니다. 이후의 OnCommand Insight 업그레이드 중에 이 파일을 덮어씁니다. 디스크 모델 정보가 업그레이드된 파일에 없는 경우 다시 입력해야 합니다.

새 디스크 모델에 필요한 정보 찾기

디스크 모델 정보를 찾으려면 공급업체 및 모델 번호를 확인하고 인터넷 검색을 실행합니다.

이 작업에 대해

디스크 모델 정보는 인터넷 검색을 실행하는 것처럼 간단하게 찾을 수 있습니다. 검색하기 전에 공급업체 이름과 디스크 모델 번호를 기록해 두십시오.

단계

1. 공급업체의 데이터 시트 및/또는 드라이브 설치 설명서를 찾으려면 공급업체, 모델 및 문서 유형 ""PDF"에 대한 고급 인터넷 검색을 사용하는 것이 좋습니다. 이러한 데이터 시트는 일반적으로 공급업체 디스크 정보의 가장 좋은 소스입니다.
2. 공급업체 사양이 전체 모델 번호를 기반으로 필요한 모든 정보를 제공하는 것은 아닙니다. 공급업체 사이트에서 모델 번호 문자열의 여러 부분을 검색하여 모든 정보를 찾는 것이 유용합니다.
3. 디스크 공급업체 이름, 전체 모델 번호, 디스크 크기 및 속도 및 인터페이스 유형을 찾습니다. OnCommand Insight에서 새 디스크 모델을 정의하려면 다음 표를 참조하십시오.

이 필드의 경우:	다음 중 무엇입니까?	입력 내용:
모델 번호(aka Key)	필수 요소입니다	
공급업체	필수 요소입니다	
디스크 속도(RPM)	필수 요소입니다	
크기(GB)	필수 요소입니다	
인터페이스 유형(하나 선택)	필수 요소입니다	ATA, SATA, SATA2, SATA3, FC, SAS, FATA, SSD, 기타
탐색 시간(ms)	선택 사항	
최대 전송 속도(MB/sec)입니다	선택 사항	
인터페이스 전송 속도 (MB/sec)입니다	선택 사항	
공급업체/모델 정보 링크	선택 사항이지만 권장됩니다	

4. 에 해당 정보를 입력합니다 `new_disk_models.txt` 파일. 을 참조하십시오 "new_disk_models.txt 파일의 내용입니다" 형식, 순서 및 예제를 보려면

new_disk_models.txt 파일의 내용입니다

를 클릭합니다 `new_disk_models.txt` 파일에 필수 및 옵션 필드가 있습니다. 필드는 쉼표로 구분되므로 필드에 쉼표 _ 를 사용하지 마십시오.

검색 시간, 전송 속도 및 Additional_info를 제외한 모든 필드는 필수입니다. 가능한 경우, SUPPLICATION_info 필드에 공급업체/모델 웹 사이트 링크를 포함합니다.

텍스트 편집기를 사용하여 추가하려는 각 새 디스크 모델에 대해 다음 정보를 쉼표로 구분하여 이 순서로 입력하십시오.

1. * 키 *: 모델 번호 사용(필수)
2. * 벤더 *: 이름(필수)
3. * 모델 번호 *: 전체 번호(일반적으로 "키"와 동일한 값)(필수)
4. 디스크의 * rpm *: 예: 10000 또는 15000(필수)
5. * 크기 *: 용량(GB)(필수)
6. * 인터페이스 유형 *: ATA, SATA, FC, SAS, FATA, SSD, 기타(필수)
7. * 탐색 시간 *: ms(선택 사항)
8. * 잠재적 전송 속도 *: 잠재적인 전송 속도(MB/sec) 디스크 자체의 최대 전송 속도입니다. (선택 사항)

9. * 인터페이스 전송 속도 *: 호스트 간 전송 속도(MB/sec)(선택 사항)
10. * 추가 정보 *: 캡처하려는 추가 정보입니다. 가장 좋은 방법은 사양을 찾은 공급업체 페이지 링크를 참조(선택 사항)하는 것입니다.

비어 있는 옵션 필드의 경우 쉼표를 포함해야 합니다.

예제(각 줄은 공백 없이 한 줄에 하나씩):

```
ST373405,Seagate,ST373405,10000,73,FC,5.3,64,160,http://www.seagate.com/staticfil
es/support/disc/manuals/enterprise/cheetah/73(LP)/100109943e.pdf

SLR5B-M400SS,HITACHI,SLR5B-M400SS,1000000,400,SSD,,,,

X477_THARX04TA07,TOSHIBA,X477_THARX04TA07,7200,4000,SATA,9.5,,,https://storage.to
shiba.eu/export/sites/toshiba-sdd/media/products/datasheets/MG03ACAxxxY.pdf
```

환경을 모니터링합니다

Insight를 사용하면 환경의 문제를 예방하고 잠재적인 문제를 신속하게 해결할 수 있습니다.

자산 페이지 데이터

자산 페이지에서는 성능 문제 해결 데이터를 제공하고 기본 자산(예: 가상 머신 또는 볼륨)과 기본 자산(예: 스토리지 풀, 스토리지 노드, 연결된 스위치 포트)에 대한 요약 정보를 제공하며 추가 정보에 대한 링크를 제공합니다.

OnCommand Insight 7.3.1부터 모든 자산 페이지에는 * 주 * 페이지와 * 추가 데이터 * 페이지가 있습니다. 기본 페이지에는 자산에 대한 요약과 차트, 토폴로지 및 기타 정보에 대한 여러 섹션이 있습니다. Additional data * 페이지에서 현재 자산 유형에 대해 사용자 지정 가능한 대시보드 페이지를 구성할 수 있습니다.

자산 페이지 기본 탭의 선이나 메시지 옆에 있는 빨간색 원은 모니터링되는 환경에서 발생할 수 있는 문제를 나타냅니다.

자산 페이지 유형

자산 페이지는 자산의 현재 상태를 요약하고 자산 및 관련 자산에 대한 추가 정보에 대한 링크를 포함합니다.

OnCommand Insight는 다음 자산에 대한 자산 페이지를 제공합니다.

- 가상 머신
- 볼륨
- 내부 볼륨
- 물리적 호스트
- 스토리지 풀
- 스토리지
- 데이터 저장소

- 하이퍼바이저
- 응용 프로그램
- 스토리지 노드
- qtree입니다
- 디스크
- VMDK입니다
- 포트
- 스위치
- 패브릭
- 오브젝트 스토리지(예: Atmos, Centera, Amazon S3)
- Zone(영역)

매핑 및 마스킹 정보는 영역, 볼륨, VM 및 호스트/하이퍼바이저 자산 페이지의 표에서 볼 수 있습니다.

> 요약 정보는 오브젝트 스토리지 자산에서 사용할 수 있지만 데이터 소스 세부 정보 페이지에서만 이 정보에 액세스할 수 있습니다.

특정 자산을 위한 환경 검색

검색 기능을 사용하여 특정 자산에 대한 정보를 찾을 수 있습니다. 예를 들어, 시스템 사용자가 특정 서버에 대한 불만을 가지고 스토리지 관리자에게 연락할 경우 관리자는 서버 이름을 검색하고 상태를 요약하고 추가 연결 정보를 제공하는 자산 페이지를 표시할 수 있습니다.

단계

1. OnCommand Insightfob UI를 엽니다.
2. 도구 모음에서 를 클릭합니다 .

   자산 검색 * 상자가 표시됩니다.

3. 자산 이름 또는 이름의 일부를 입력합니다.
4. 검색 결과에서 원하는 리소스를 선택합니다.

   해당 자원의 자산 페이지가 표시됩니다.

고급 검색 기술

모니터링되는 환경에서 데이터 또는 개체를 검색하는 데 여러 검색 기술을 사용할 수 있습니다.

와일드카드 검색

문자를 사용하여 여러 문자 와일드카드 검색을 수행할 수 있습니다. 예를 들어, _applic*n_은(는) 응용 프로그램을 반환합니다.

검색에 사용되는 구

구문은 큰따옴표로 둘러싸인 단어 그룹입니다(예: "Paw VNX LUN 5"). 큰따옴표를 사용하여 이름이나 속성에 공백이 포함된 문서를 검색할 수 있습니다.

부울 연산자

부울 연산자를 사용하면 여러 용어를 결합하여 보다 복잡한 쿼리를 만들 수 있습니다.

- * 또는 *
  - 또는 연산자는 기본 결합 연산자입니다.

    두 용어 사이에 부울 연산자가 없으면 OR 연산자가 사용됩니다.

  - OR 연산자는 두 용어를 연결하고 문서에 일치하는 용어가 있는 경우 일치하는 문서를 찾습니다.

    예를 들어, "스토리지 또는 NetApp"은 "스토리지" 또는 "NetApp"이 포함된 문서를 검색합니다.

  - 대부분의 조건과 일치하는 문서에 높은 점수가 부여됩니다.
- 및 *

  AND 연산자를 사용하여 두 검색어가 모두 하나의 문서에 있는 문서를 찾을 수 있습니다. 예를 들어, ""오로라"와 "NetApp""이 모두 포함된 문서를 검색합니다.

  단어 및 대신 && 기호를 사용할 수 있습니다.

- * NOT *

  NOT 연산자를 사용하면 NOT가 포함된 모든 문서가 검색 결과에서 제외됩니다. 예를 들어, "NetApp이 아닌 스토리지"는 "NetApp"이 아닌 "스토리지"만 포함된 문서를 검색합니다.

  기호를 사용할 수 있습니다! 대신 'NOT'이라는 단어를 사용하십시오.

접두사 및 접미사 검색

- 검색 문자열을 입력하기 시작하면 검색 엔진은 가장 일치하는 항목을 찾기 위해 접두사 및 접미사 검색을 수행합니다.
- 정확히 일치하는 항목이 접두사 또는 접미사 일치보다 높은 점수를 받습니다. 점수는 실제 검색 결과와 검색 용어의 거리를 기준으로 계산됩니다. 예를 들어, ""오로라", ""오로라 1", ""오로라 11""의 세 가지 창고를 사용할 수 있습니다. 아우르(Aur)를 검색하면 3곳의 모든 업소를 찾을 수 있습니다. 그러나 검색결과 검색어와 검색문자열 사이의 거리가 가장 가깝기 때문에 검색 결과가 가장 높은 점수를 받게 됩니다.
- 또한 검색 엔진은 검색어를 역순으로 검색하여 접미사 검색을 수행할 수 있습니다. 예를 들어 검색 상자에 ""345""를 입력하면 검색 엔진이 ""345""를 검색합니다.
- 검색은 대/소문자를 구분하지 않습니다.

인덱싱된 용어를 사용하여 검색합니다

인덱싱된 용어 중 더 많은 조건과 일치하는 검색을 수행하면 더 높은 점수를 얻을 수 있습니다.

검색 문자열은 스페이스를 기준으로 별도의 검색어로 분할됩니다. 예를 들어 검색 문자열 "Storage aurora NetApp"은

"Storage", "aurora", "NetApp" 등의 세 가지 키워드로 구분됩니다. 검색은 세 가지 용어를 모두 사용하여 수행됩니다. 이 용어 중 대부분과 일치하는 문서의 점수가 가장 높습니다. 더 많은 정보를 제공할수록 검색 결과가 더 좋습니다. 예를 들어 이름 및 모드로 스토리지를 검색할 수 있습니다.

UI는 범주 별로 검색 결과를 표시하며 범주 당 상위 3개 결과를 표시합니다. 원하는 문서를 찾지 못한 경우 검색 문자열에 더 많은 용어를 포함해서 검색 결과를 개선할 수 있습니다.

다음 표에서는 검색 문자열에 추가할 수 있는 인덱싱된 용어 목록을 제공합니다.

범주	인덱싱된 용어
스토리지	• "스토리지" • 이름 • 공급업체 • 모델
스토리지 풀	• "초라풀" • 이름 • 스토리지의 이름입니다 • 스토리지의 IP 주소입니다 • 스토리지의 일련 번호입니다 • 스토리지 공급업체 • 스토리지 모델 • 연결된 모든 내부 볼륨의 이름입니다 • 연결된 모든 디스크의 이름입니다
내부 볼륨	• "'인턴 볼륨'" • 이름 • 스토리지의 이름입니다 • 스토리지의 IP 주소입니다 • 스토리지의 일련 번호입니다 • 스토리지 공급업체 • 스토리지 모델 • 스토리지 풀의 이름입니다 • 연결된 모든 공유의 이름입니다 • 모든 관련 애플리케이션 및 업무 엔티티의 이름

볼륨	• '"볼륨'" • 이름 • 라벨 • 모든 내부 볼륨의 이름입니다 • 스토리지 풀의 이름입니다 • 스토리지의 이름입니다 • 스토리지의 IP 주소입니다 • 스토리지의 일련 번호입니다 • 스토리지 공급업체 • 스토리지 모델
스토리지 노드	• "거어코드" • 이름 • 스토리지의 이름입니다 • 스토리지의 IP 주소입니다 • 스토리지의 일련 번호입니다 • 스토리지 공급업체 • 스토리지 모델
호스트	• '"호스트'" • 이름 • IP 주소 • 모든 관련 애플리케이션 및 업무 엔티티의 이름
데이터 저장소	• "다타스토어" • 이름 • 가상 센터 IP • 모든 볼륨의 이름입니다 • 모든 내부 볼륨의 이름입니다

가상 머신	• '"가상시스템"' • 이름 • DNS 이름입니다 • IP 주소 • 호스트의 이름입니다 • 호스트의 IP 주소입니다 • 모든 데이터 저장소의 이름입니다 • 모든 관련 애플리케이션 및 업무 엔티티의 이름
스위치(일반 및 NPV)	• 마녀 • IP 주소입니다 • WWN입니다 • 이름 • 일련 번호입니다 • 모델 • 도메인 ID입니다 • 패브릭의 이름입니다 • 패브릭의 WWN입니다
응용 프로그램	• '"응용 프로그램"' • 이름 • 테넌트 • LOB가 포함됩니다 • 부서 • 프로젝트
테이프	• '"테이프"' • IP 주소입니다 • 이름 • 일련 번호입니다 • 공급업체
포트	• '"포트"' • WWN입니다 • 이름

패브릭	• '"fabric'" • WWN입니다 • 이름

표시된 데이터의 시간 범위를 변경합니다

기본적으로 자산 페이지에는 지난 24시간 동안의 데이터가 표시되지만 표시되는 데이터 세그먼트는 다른 고정 시간 또는 사용자 지정 시간 범위를 선택하여 변경하거나 더 적은 데이터 또는 더 많은 데이터를 볼 수 있습니다.

이 작업에 대해

자산 유형에 관계없이 모든 자산 페이지에 있는 옵션을 사용하여 표시된 데이터의 시간 세그먼트를 변경할 수 있습니다.

단계

1. OnCommand Insightfob UI에 로그인합니다.
2. 다음 중 하나를 수행하여 자산 페이지를 찾습니다.
   - Insight 도구 모음에서 를 클릭합니다 을 클릭하고 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
   - 대시보드 * 를 클릭하고 * 자산 대시보드 * 를 선택한 다음 자산 이름을 찾아 클릭합니다. 자산 페이지가 표시됩니다.
3. 페이지의 왼쪽 상단 모서리에서 다음 시간 아이콘 중 하나를 클릭하여 표시되는 데이터의 세그먼트를 변경합니다.
   - 3시간 *

     최근 3시간의 데이터를 표시합니다.

   - * 24시간 *

     최근 24시간 동안의 데이터를 표시합니다.

   - * 3D *

     마지막 3일간의 데이터를 표시합니다.

   - * 7d *

     최근 7일 동안의 데이터를 표시합니다.

   - * 30d *

     최근 30일 동안의 데이터를 표시합니다.

   - * 사용자 정의 *

     사용자 지정 시간 범위를 선택할 수 있는 대화 상자를 표시합니다. 한 번에 최대 31일의 데이터를 표시할 수 있습니다.

4. 사용자 정의 * 를 선택한 경우 다음을 수행합니다.
   a. 날짜 필드를 클릭하고 시작 날짜의 월, 일 및 연도를 선택합니다.
   b. 시간 목록을 클릭하고 시작 시간을 선택합니다.
   c. 끝 데이터와 시간에 대해 a와 b 단계를 모두 반복합니다.
   d. 을 클릭합니다 ✔.

데이터 소스 획득 상태를 확인하는 중입니다

데이터 소스가 Insight의 주요 정보원이기 때문에 데이터 소스가 실행 상태를 유지하도록 하는 것이 중요합니다.

직접 획득한 모든 자산에 대해 모든 자산 페이지에서 데이터 소스 획득 상태를 볼 수 있습니다. 다음 획득 시나리오 중 하나가 발생할 수 있으며, 이 경우 자산 페이지의 오른쪽 상단 모서리에 상태가 표시됩니다.

- 데이터 소스에서 성공적으로 획득되었습니다

  상태 ""를 표시합니다 `xxxx``", where `xxxx` 자산 데이터 소스의 가장 최근 획득 시간을 나타냅니다.

- 획득 오류가 있습니다.

  상태 ""를 표시합니다 `xxxx``", where `xxxx` 에서 자산에 있는 하나 이상의 데이터 소스의 가장 최근 획득 시간을 나타냅니다 ⚠. 를 클릭합니다 ⚠ 창에서 자산에 대한 각 데이터 소스, 데이터 소스의 상태 및 마지막으로 데이터를 획득한 시간을 표시합니다. 데이터 원본을 클릭하면 데이터 원본의 세부 정보 페이지가 표시됩니다.

자산을 직접 획득하지 않으면 상태가 표시되지 않습니다.

자산 페이지 섹션

자산 페이지에는 자산과 관련된 정보가 포함된 여러 섹션이 표시됩니다. 표시되는 섹션은 자산의 유형에 따라 다릅니다.

요약

자산 페이지의 요약 섹션에는 특정 자산에 대한 정보가 요약되어 표시되며, 자산과 관련된 문제가 빨간색 원으로 표시되며 관련 자산 및 자산에 할당된 성능 정책에 대한 추가 정보로 연결되는 하이퍼링크가 표시됩니다.

다음 예에서는 가상 머신에 대한 자산 페이지의 요약 섹션에서 사용할 수 있는 일부 정보 유형을 보여 줍니다. 빨간색 원이 있는 항목은 모니터링되는 환경에서 발생할 수 있는 문제를 나타냅니다.

Summary

Power state:	On
Guest state:	Running
Datastore:	DS_SP1_1
CPU:	41.05%
Memory:	51% (1,047 / 2,048 MB)
Capacity:	10% (19.5 / 195.3 GB)
Latency:	1.93 ms (6.00 ms max)
IOPS:	1,317.33 IO/s (4,964.00 IO/s max)
Throughput:	38.79 MB/s (142.00 MB/s max)
DNS name:	VM_Cs_travBookcomp.com
IP:	10.97.133.23
OS:	Microsoft Windows Server 2008 R2(64-bit)
Processors:	4
FC Fabrics Connected:	1
Performance Policies:	VM Latency-Critical VM Latency-Warning Comp Corp.Customer Support SLA latency Exchange SL0

요약 섹션을 사용합니다

요약 섹션을 보고 자산에 대한 일반 정보를 볼 수 있습니다. 특히 메트릭 또는 성능 정책 옆에 빨간색 원을 표시하여 OnCommand Insight가 나타내는 메트릭(예: 메모리, 용량, 지연 시간)이나 성능 정책이 문제가 되는지 확인하는 것이 좋습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 다음 중 하나를 수행하여 자산 페이지를 찾습니다.
   - Insight 도구 모음에서 를 클릭합니다 을 클릭하고 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
   - 대시보드 * 를 클릭하고 * 자산 대시보드 * 를 선택한 다음 자산 이름을 찾아 클릭합니다. 자산 페이지가 표시됩니다.

     요약 섹션에 표시되는 정보는 보고 있는 자산 페이지 유형에 따라 다릅니다.
3. 자산 링크를 클릭하여 자산 페이지를 볼 수 있습니다.

   예를 들어, 스토리지 노드를 보고 있는 경우 링크를 클릭하여 연결된 스토리지의 자산 페이지를 보거나 HA 파트너의 자산 페이지를 볼 수 있습니다.
4. 자산과 연결된 메트릭을 볼 수 있습니다.

   메트릭 옆에 있는 빨간색 원은 잠재적인 문제를 진단하고 해결해야 할 수 있음을 나타냅니다.

> 일부 스토리지 자산에서는 볼륨 용량이 100% 이상 표시될 수 있습니다. 이는 자산에서 보고하는 사용된 용량 데이터의 일부인 볼륨의 용량과 관련된 메타데이터 때문입니다.

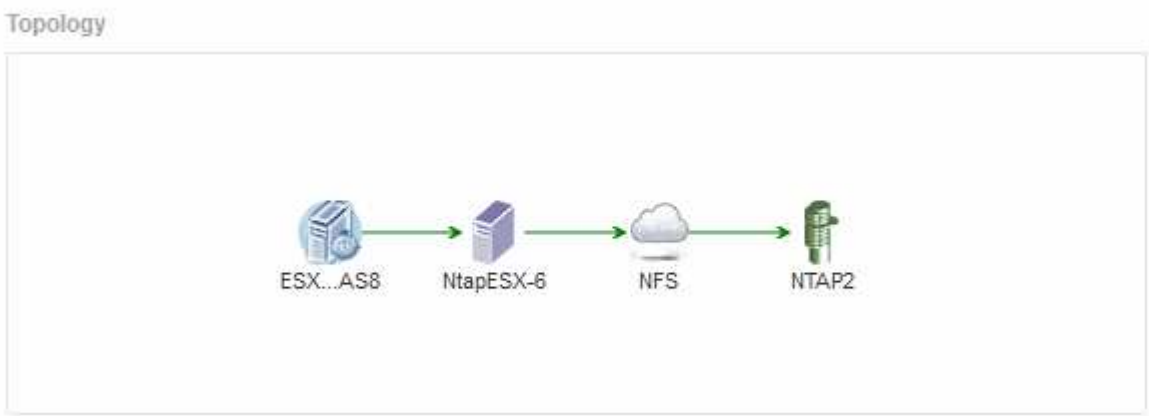
5. 해당되는 경우 성능 정책 링크를 클릭하여 자산과 관련된 성능 정책 또는 정책을 볼 수 있습니다.

   성능 정책 옆에 빨간색 원이 나타나면 자산이 성능 정책의 정의된 임계값을 초과했음을 나타냅니다. 문제를 더 자세히 진단하려면 성능 정책을 검토해야 합니다.

토폴로지

자산에 해당되는 경우 토폴로지 섹션을 통해 기본 자산이 관련 자산에 어떻게 연결되어 있는지 확인할 수 있습니다.

다음은 가상 머신 자산 페이지의 토폴로지 섹션에 표시될 수 있는 항목의 예입니다.



자산의 토폴로지가 섹션에 들어갈 수 있는 것보다 크면 * 토폴로지 * 하이퍼링크를 보기 위한 * 클릭 링크가 대신 표시됩니다.

Topology 섹션 사용

Topology(토폴로지) 섹션에서는 네트워크의 자산이 서로 어떻게 연결되어 있는지 확인하고 관련 자산에 대한 정보를 표시할 수 있습니다.

단계

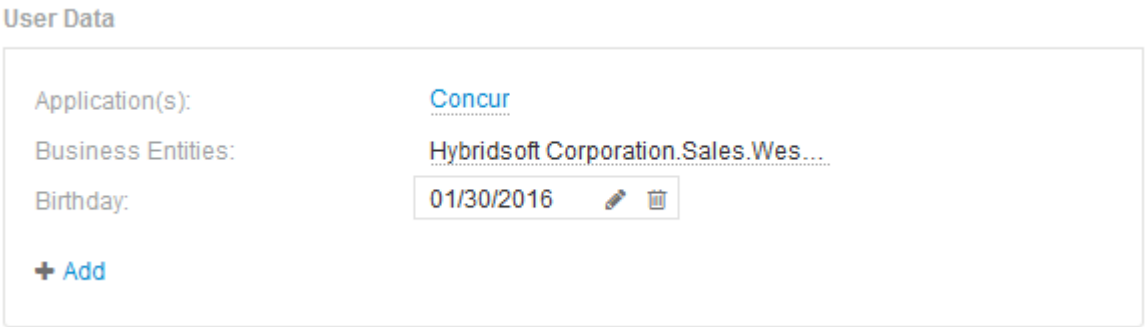
1. OnCommand Insight 웹 UI에 로그인합니다.
2. 다음 중 하나를 수행하여 자산 페이지를 찾습니다.
   - Insight 도구 모음에서 를 클릭합니다 을 클릭하고 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
   - 대시보드 * 를 클릭하고 * 자산 대시보드 * 를 선택한 다음 자산 이름을 찾아 클릭합니다. 자산 페이지가 표시됩니다. 자산 페이지의 오른쪽 상단 모서리에 있는 토폴로지 섹션을 찾을 수 있습니다.

   자산의 토폴로지가 섹션에 들어갈 수 있는 것보다 큰 경우 * 클릭 링크를 클릭하여 토폴로지 * 하이퍼링크를 확인하십시오.

3. 기본 자산의 관련 자산에 대한 자세한 정보를 보려면 토폴로지의 관련 자산 위에 커서를 놓고 해당 이름을 클릭하면 자산 페이지가 표시됩니다.

자산 페이지의 사용자 데이터 섹션이 표시되고 응용 프로그램, 사업체 및 주석과 같은 사용자 정의 데이터를 변경할 수 있습니다.

다음은 애플리케이션, 사업체 및 주석이 자산에 할당될 때 가상 시스템 자산 페이지의 사용자 데이터 섹션에 표시될 수 있는 항목의 예입니다.



사용자 데이터 섹션을 사용하여 응용 프로그램을 할당하거나 수정합니다

사용자 환경에서 실행 중인 애플리케이션을 특정 자산(호스트, 가상 머신, 볼륨, 내부 볼륨 및 하이퍼바이저)에 할당할 수 있습니다. 사용자 데이터 섹션을 사용하면 자산에 할당된 애플리케이션을 변경하거나 애플리케이션 또는 추가 애플리케이션을 자산에 할당할 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 다음 중 하나를 수행하여 자산 페이지를 찾습니다.
   - Insight 도구 모음에서 를 클릭합니다 을 클릭하고 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
   - 대시보드 * 를 클릭하고 * 자산 대시보드 * 를 선택한 다음 자산 이름을 찾아 클릭합니다. 자산 페이지가 표시됩니다.
3. 다음을 수행할 수 있습니다.
   - 응용 프로그램의 자산 페이지를 보려면 응용 프로그램 이름을 클릭합니다.
   - 할당된 응용 프로그램을 변경하거나 응용 프로그램 또는 추가 응용 프로그램을 할당하려면 응용 프로그램 이름 위에 커서를 놓고 응용 프로그램이 할당된 경우 * 없음 * 위에 커서를 놓습니다. 할당된 응용 프로그램이 없는 경우 를 클릭합니다 을 입력하여 응용 프로그램을 검색하거나 목록에서 하나를 선택한 다음 을 클릭합니다 .

     업무 엔티티와 연결된 애플리케이션을 선택하면 업무 엔티티가 자동으로 자산에 할당됩니다. 이 경우 사업체 이름 위에 커서를 놓으면 _Derived_라는 단어가 표시됩니다. 연결된 응용 프로그램이 아닌 자산에 대해서만 엔티티를 유지하려면 응용 프로그램의 할당을 수동으로 재정의할 수 있습니다.

   - 응용 프로그램을 제거하려면 를 클릭합니다 .

사용자 데이터 섹션을 사용하여 업무 엔티티를 할당하거나 수정합니다

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

페이지의 사용자 데이터 섹션을 사용하면 자산에 할당된 업무 엔티티를 변경하거나 자산에서 업무 엔티티를 제거할 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 다음 중 하나를 수행하여 자산 페이지를 찾습니다.
   - Insight 도구 모음에서 를 클릭합니다 을 클릭하고 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
   - 대시보드 * 를 클릭하고 * 자산 대시보드 * 를 선택한 다음 자산 이름을 찾아 클릭합니다. 자산 페이지가 표시됩니다.
3. 다음을 수행할 수 있습니다.
   - 지정된 엔티티를 변경하거나 엔티티를 할당하려면 을 클릭합니다 목록에서 요소를 선택합니다.
   - 업무 엔티티를 제거하려면 을 클릭합니다 .

   자산에 할당된 애플리케이션에서 파생된 엔티티는 제거할 수 없습니다.

User Data(사용자 데이터) 섹션을 사용하여 주석을 할당하거나 수정합니다

회사 요구 사항에 맞는 데이터를 추적하도록 OnCommand Insight를 사용자 지정할 때 _annotations_라는 특수 메모를 정의하여 자산에 할당할 수 있습니다. 자산 페이지의 사용자 데이터 섹션에는 자산에 할당된 주석이 표시되며 해당 자산에 할당된 주석을 변경할 수도 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 다음 중 하나를 수행하여 자산 페이지를 찾습니다.
   - Insight 도구 모음에서 를 클릭합니다 을 클릭하고 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
   - 대시보드 * 를 클릭하고 * 자산 대시보드 * 를 선택한 다음 자산 이름을 찾아 클릭합니다. 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.

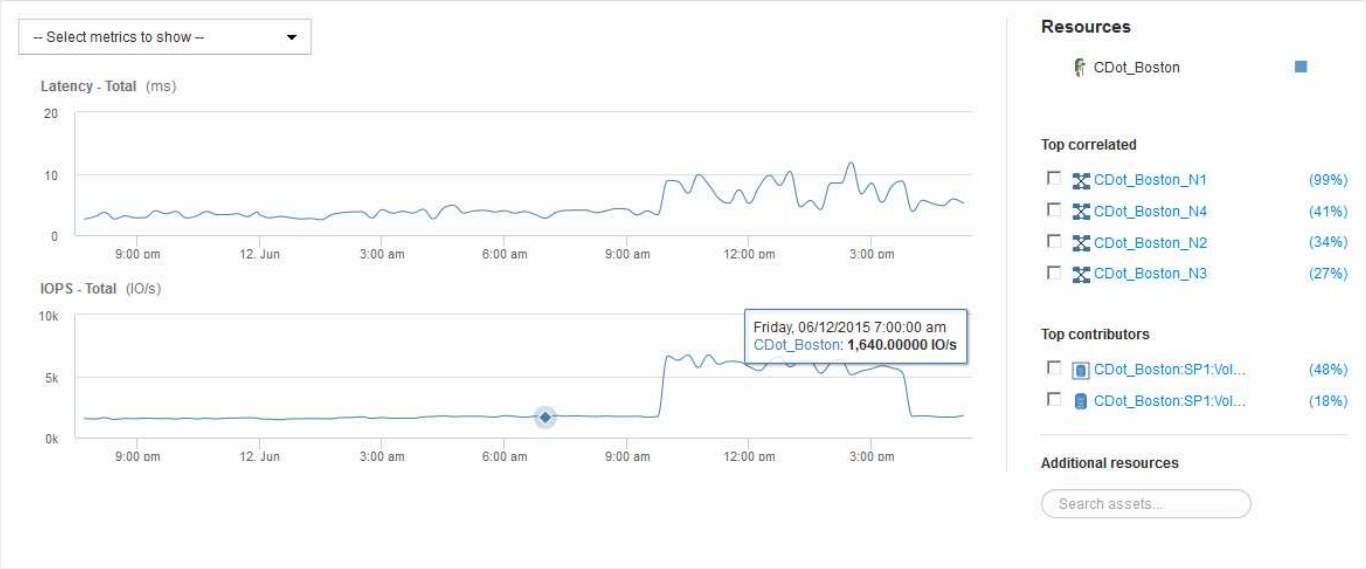
   주석이 자산에 할당됩니다. 나중에 쿼리를 사용하여 주석을 기준으로 자산을 필터링할 수 있습니다.
7. 주석을 지정한 후 주석 값을 변경하려면 을 클릭합니다 다른 값을 선택합니다.

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

전문가 뷰

자산 페이지의 전문가 보기 섹션에서는 선택한 기간(3시간, 24시간, 3일, 7일, 또는 사용자 지정 기간)을 성능 차트 및 관련 자산에 입력합니다.

다음은 볼륨 자산 페이지의 전문가 보기 섹션의 예입니다.



선택한 기간의 성능 차트에서 확인할 메트릭을 선택할 수 있습니다.

자원 섹션에는 기본 자산의 이름과 성능 차트의 기본 자산을 나타내는 색상이 표시됩니다. 상호 연결된 최상위 섹션에 성능 차트에서 보려는 자산이 없는 경우 추가 리소스 섹션의 * 자산 검색 * 상자를 사용하여 자산을 찾고 성능 차트에 추가할 수 있습니다. 자원을 추가하면 추가 자원 섹션에 나타납니다.

또한 리소스 섹션에 표시된 대로 다음 범주의 기본 자산과 관련된 자산이 있을 수 있습니다.

- 상호 연관성

  에는 기본 자산에 대한 하나 이상의 성능 메트릭과 높은 상관 관계(백분율)가 있는 자산이 나와 있습니다.

- 최고 기여자

  기본 자산에 기여하는 자산(백분율)을 표시합니다.

- 탐욕심

  에는 호스트, 네트워크 및 스토리지와 같은 동일한 리소스를 공유하여 자산에서 시스템 리소스를 빼앗는 자산이 나와 있습니다.

- 성능 저하

  이 자산으로 인해 시스템 리소스가 고갈된 자산을 표시합니다.

자산 페이지의 전문가 보기 섹션에는 자산에 대해 선택한 기간에 따라 몇 가지 메트릭이 표시됩니다. 각 메트릭은 자체 성능 차트에 표시됩니다. 보려는 데이터에 따라 차트에서 메트릭 및 관련 자산을 추가하거나 제거할 수 있습니다.

미터	설명
BB 크레딧 제로 Rx, Tx	샘플링 기간 동안 수신/전송 버퍼 대 버퍼 크레딧 수가 0으로 전환된 횟수입니다. 이 메트릭은 제공할 크레딧이 없기 때문에 연결된 포트의 전송을 중지해야 하는 횟수를 나타냅니다.
BB 크레딧 없음 기간 Tx	샘플링 간격 동안 전송 BB 크레딧이 0인 시간(밀리초)입니다.
캐시 적중률(총, 읽기, 쓰기) %	캐시 적중으로 인한 요청의 비율입니다. 적중 횟수와 볼륨 액세스 횟수가 많을수록 성능이 향상됩니다. 캐시 적중 정보를 수집하지 않는 스토리지 시스템의 경우 이 열이 비어 있습니다.
캐시 활용률(총) %	캐시 적중으로 인한 캐시 요청의 총 비율입니다
클래스 3이 삭제됩니다	Fibre Channel Class 3 데이터 전송 폐기 횟수
CPU 사용률(총) %	사용 가능한 총 CPU(모든 가상 CPU)의 백분율로 사용 중인 CPU 리소스의 양입니다.
CRC 오류입니다	샘플링 기간 동안 포트에서 감지된 잘못된 CRC(Cyclic Redundancy Check)의 프레임 수입니다
프레임 속도	초당 프레임 수(FPS)로 프레임 속도 전송
프레임 크기 평균(Rx, Tx)	프레임 크기에 대한 트래픽 비율입니다. 이 메트릭을 통해 Fabric에 오버헤드 프레임이 있는지 여부를 확인할 수 있습니다.
프레임 크기가 너무 깁니다	너무 긴 Fibre Channel 데이터 전송 프레임 수입니다.
프레임 크기가 너무 짧습니다	너무 짧은 Fibre Channel 데이터 전송 프레임 수입니다.
I/O 밀도(Total, Read, Write)	볼륨, 내부 볼륨 또는 스토리지 요소에 대한 IOPS를 사용된 용량(데이터 소스의 최신 인벤토리 폴에서 얻은 값)으로 나눈 값입니다. TB당 초당 I/O 작업 수로 측정

IOPS(총, 읽기, 쓰기)	I/O 채널을 통해 전달되는 읽기/쓰기 I/O 서비스 요청 수 또는 시간 단위당 해당 채널의 일부(초당 I/O로 측정)
IP 처리량(총, 읽기, 쓰기)	총계: 초당 메가바이트 단위의 IP 데이터가 전송 및 수신된 총 속도입니다. 읽기: IP 처리량(수신): IP 데이터가 수신된 평균 속도(MB/초)입니다. 쓰기: IP 처리량(전송): IP 데이터가 전송된 평균 속도(MB/초)입니다.
지연 시간(총, 읽기, 쓰기)	지연 시간(R&W): 고정된 시간 내에 데이터를 가상 시스템에 읽거나 쓰는 비율. 이 값은 초당 메가바이트로 측정됩니다. 지연 시간: 데이터 저장소의 가상 머신에서 평균 응답 시간입니다. 최고 지연 시간: 데이터 저장소의 가상 머신에서 응답 시간이 가장 긴 경우
링크 실패	샘플링 기간 동안 포트에서 감지된 링크 장애 수입니다.
Link Reset Rx, Tx(링크 재설정 Rx, Tx	샘플링 기간 동안 수신 또는 전송 링크 재설정 횟수 이 메트릭은 이 포트에 연결된 포트에서 실행된 링크 재설정의 수를 나타냅니다.
메모리 사용률(총) %	호스트에서 사용하는 메모리의 임계값입니다.
부분 R/W(총) %	읽기/쓰기 작업이 RAID 5, RAID 1/0 또는 RAID 0 LUN의 디스크 모듈에서 스트라이프 경계를 교차하는 총 횟수입니다. 일반적으로 스트라이프 크로싱은 각 LUN에 추가 I/O가 필요하기 때문에 유용하지 않습니다 비율이 낮다면 효율적인 스트라이프 요소 크기를 나타내며 볼륨(또는 NetApp LUN)이 잘못 정렬되었음을 나타냅니다. CLARiX의 경우 이 값은 총 IOPS 수로 나눈 스트라이프 크로싱 수입니다.
포트 오류	샘플링 기간/지정된 기간 동안의 포트 오류 보고.
신호 손실 카운트	신호 손실 오류 수입니다. 신호 손실 오류가 발생하면 전기 연결이 없고 물리적 문제가 있는 것입니다.
스왑 속도(총 속도, 속도, 아웃 속도)	샘플링 기간 동안 메모리를 디스크에서 활성 메모리로 스왑하거나, 스왑 아웃하거나, 둘 다 활성 메모리로 스왑하는 속도입니다. 이 카운터는 가상 머신에 적용됩니다.

동기화 손실 카운트	동기화 손실 오류 수입니다. 동기화 손실 오류가 발생하면 하드웨어가 트래픽을 감지하거나 해당 트래픽을 잠글 수 없습니다. 모든 장비가 동일한 데이터 속도를 사용하지 않거나, 광학 또는 물리적 연결의 품질이 저하될 수 있습니다. 이러한 각 오류 후에 포트가 재동기화되어야 하며, 이는 시스템 성능에 영향을 줍니다. KB/초 단위로 측정됩니다
처리량(총, 읽기, 쓰기)	입출력 서비스 요청에 대한 응답으로 데이터가 전송, 수신 또는 모두 고정된 시간(MB/sec 단위로 측정)으로 전송되는 속도입니다.
시간 초과 폐기 프레임 - Tx	시간 초과로 인해 폐기된 전송 프레임 수입니다.
트래픽 속도(합계, 읽기, 쓰기)	샘플링 기간 동안 전송, 수신 또는 두 가지 모두 수신된 트래픽(초당 메비바이트)입니다.
트래픽 사용률(총, 읽기, 쓰기)	샘플링 기간 동안 수신/전송/총 수신/전송/총 용량의 비율입니다.
사용률(총, 읽기, 쓰기) %	전송(Tx) 및 수신(Rx)에 사용되는 가용 대역폭의 비율입니다.
쓰기 보류(총)	보류 중인 쓰기 입출력 서비스 요청 수입니다.

전문가 보기 섹션을 사용합니다

전문가 보기 섹션에서는 선택한 기간 동안 원하는 수의 해당 메트릭을 기준으로 자산에 대한 성능 차트를 보고, 서로 다른 기간 동안 자산 및 관련 자산 성과를 비교 및 대조할 수 있도록 관련 자산을 추가할 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 다음 중 하나를 수행하여 자산 페이지를 찾습니다.
   - Insight 도구 모음에서 를 클릭합니다 을 클릭하고 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
   - 대시보드 * 를 클릭하고 * 자산 대시보드 * 를 선택한 다음 자산 이름을 찾아 클릭합니다. 자산 페이지가 표시됩니다. 기본적으로 성능 차트는 자산 페이지에 대해 선택한 기간에 대해 두 가지 메트릭을 보여 줍니다. 예를 들어, 스토리지의 경우 성능 차트에는 기본적으로 지연 시간과 총 IOPS가 표시됩니다. 자원 섹션에는 자원 이름과 자산을 검색할 수 있는 추가 자원 섹션이 표시됩니다. 자산에 따라 Top Correlated, Top Contributor, greedy 및 Degraded 섹션에도 자산이 표시될 수 있습니다.
3. 표시할 메트릭 선택 * 을 클릭하고 메트릭을 선택하여 메트릭에 대한 성능 차트를 추가할 수 있습니다.

   선택한 메트릭에 대한 성능 차트가 추가됩니다. 선택한 기간의 데이터가 차트에 표시됩니다. 자산 페이지의 왼쪽 상단 모서리에 있는 다른 기간을 클릭하여 기간을 변경할 수 있습니다.

단계를 다시 수행하고 클릭하여 메트릭을 지울 수 있습니다. 메트릭에 대한 성능 차트가 제거됩니다.

4. 커서를 차트 위에 놓고 자산에 따라 다음 중 하나를 클릭하여 표시되는 메트릭 데이터를 변경할 수 있습니다.
   - * 읽기 * 또는 * 쓰기 *
   - **Tx** 또는 * Rx * * Total * 이 기본값입니다.
5. 선택한 기간 동안 메트릭 값이 어떻게 변경되는지 확인하려면 차트의 데이터 요소 위로 커서를 끌어다 놓습니다.
6. Resources * 섹션에서 다음 중 하나를 수행하여 해당되는 경우 성능 차트에 관련 자산을 추가할 수 있습니다.
   - Top Correlated, Top 컨트리뷰터, greedy 또는 Degraded 섹션에서 관련 자산을 선택하여 해당 자산의 데이터를 선택한 각 메트릭의 성능 차트에 추가할 수 있습니다. 자산에는 최소 15%의 상관 관계 또는 기여도가 표시되어야 합니다.

     자산을 선택하면 자산 옆에 색상 블록이 표시되어 차트의 데이터 요소 색상을 나타냅니다.

   - 표시된 자산의 경우 자산 이름을 클릭하여 해당 자산 페이지를 표시하거나, 자산이 상호 연관되거나 기본 자산에 기여하는 비율을 클릭하여 기본 자산에 대한 자산 관계에 대한 추가 정보를 볼 수 있습니다.

     예를 들어 상호 연결된 최상위 자산 옆에 있는 연결된 백분율을 클릭하면 해당 자산의 상관 관계 유형과 기본 자산을 비교한 정보 메시지가 표시됩니다.

   - 비교 목적으로 성능 차트에 표시할 자산이 상관관계 섹션에 없는 경우 추가 리소스 섹션의 * 자산 검색 * 상자를 사용하여 다른 자산을 찾을 수 있습니다. 자산을 선택하면 추가 자원 섹션에 표시됩니다. 자산에 대한 정보를 더 이상 볼 수 없게 하려면 를 클릭합니다 .

관련 자산

해당하는 경우 자산 페이지에 관련 자산 섹션이 표시됩니다. 예를 들어, 볼륨 자산 페이지에는 스토리지 풀, 연결된 스위치 포트, 컴퓨팅 리소스 등의 자산에 대한 정보가 표시될 수 있습니다. 각 섹션은 해당 범주의 관련 자산 중 하나를 나열하고 각 자산 페이지에 대한 링크와 자산과 관련된 몇 가지 성능 통계를 나열하는 표로 구성됩니다.

관련 자산 섹션을 사용합니다

Related Assets(관련 자산) 섹션에서 기본 자산과 관련된 자산을 볼 수 있습니다. 각 관련 자산이 해당 자산에 대한 관련 통계와 함께 표에 표시됩니다. 자산 정보를 내보내거나 전문가 보기 성능 차트에서 자산 통계를 보거나 관련 자산에 대한 통계만 표시하는 차트를 표시할 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 다음 중 하나를 수행하여 자산 페이지를 찾습니다.
   - Insight 도구 모음에서 를 클릭합니다 을 클릭하고 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
   - 대시보드 * 를 클릭하고 * 자산 대시보드 * 를 선택한 다음 자산 이름을 찾아 클릭합니다. 자산 페이지가 표시됩니다.
3. 테이블에 에셋이 표시되는 방식을 제어하려면 다음을 수행합니다.
   - 자산 페이지를 표시하려면 자산 이름을 클릭합니다.

- 특정 자산만 표시하려면 * filter * 상자를 사용합니다.
- 테이블에 5개 이상의 자산이 있는 경우 페이지별로 자산을 찾아보려면 페이지 번호를 클릭합니다.
- 열 머리글의 화살표를 클릭하여 표에서 열의 정렬 순서를 오름차순(위쪽 화살표) 또는 내림차순(아래쪽 화살표)으로 변경합니다.
- 관련 자산 위에 커서를 놓고 을 클릭하여 전문가 보기 섹션의 성과 차트에 관련 자산을 추가합니다 .

4. 표에 표시된 정보를 로 내보냅니다 `.csv` 파일:
   a. 을 클릭합니다 .
   b. Open with * 를 클릭한 다음 * OK * 를 클릭하여 Microsoft Excel에서 파일을 열고 파일을 특정 위치에 저장하거나 * Save file * 을 클릭하고 * OK * 를 클릭하여 파일을 Downloads 폴더에 저장합니다.

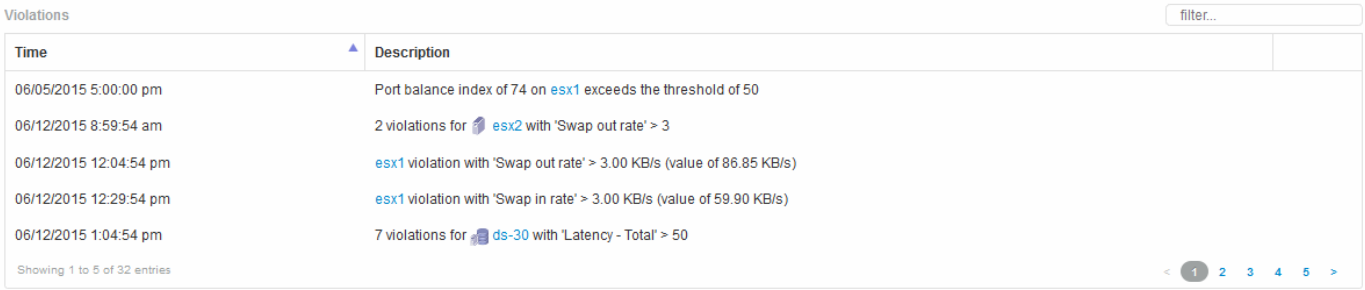
      표시를 위해 현재 선택된 컬럼의 모든 오브젝트 속성이 파일로 내보내집니다. 표시된 열의 속성만 내보내집니다. 표의 처음 10,000개 행만 내보내집니다.

5. 테이블 아래의 차트에 관련 자산 정보를 표시하려면 을 클릭합니다 다음 중 하나를 수행합니다.
   - 표시되는 메트릭 데이터를 변경하려면 * Read *, * Write * 또는 * Total * 을 클릭합니다. 기본값은 * Total * 입니다.
   - 을 클릭합니다 다른 메트릭을 선택합니다.
   - 을 클릭합니다 차트 종류를 변경하려면 다음을 수행합니다. 기본값은 * 꺾은선형 차트 * 입니다.
   - 차트의 데이터 요소 위로 커서를 이동하면 각 관련 자산에 대해 선택한 기간 동안 메트릭 값이 어떻게 변경되는지 확인할 수 있습니다.
   - 차트 범례에서 관련 자산을 클릭하여 차트에 추가하거나 차트에서 제거합니다.
   - 관련 자산 표에서 페이지 번호를 클릭하면 차트의 다른 관련 자산을 볼 수 있습니다.
   - 을 클릭합니다 를 눌러 차트를 닫습니다.

위반

자산 페이지의 위반 섹션을 사용하여 자산에 할당된 성능 정책의 결과로 사용자 환경에서 발생한 위반 사항을 확인할 수 있습니다. 성능 정책은 네트워크 임계값을 모니터링하고, 임계값 위반을 즉시 감지하고, 영향을 식별하고, 문제의 영향과 근본 원인을 빠르고 효과적으로 수정할 수 있는 방식으로 분석할 수 있도록 합니다.

다음 예제는 하이퍼바이저의 자산 페이지에 표시되는 보라색 섹션을 보여 줍니다.



위반 섹션을 사용하십시오

위반 섹션에서는 자산에 할당된 성능 정책의 결과로 네트워크에서 발생하는 모든 위반 사항을 보고 관리할 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 다음 중 하나를 수행하여 자산 페이지를 찾습니다.
   - Insight 도구 모음에서 를 클릭합니다 을 클릭하고 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
   - 대시보드 * 를 클릭하고 * 자산 대시보드 * 를 선택한 다음 자산 이름을 찾아 클릭합니다. 자산 페이지가 표시됩니다. 위반 섹션에는 위반이 발생한 시간 및 발생한 임계값에 대한 설명과 함께 위반이 발생한 자산에 대한 하이퍼링크가 표시됩니다(예: "'지연 시간이 있는 2개의 위반 FIR DS-30, 총 > 50").
3. 다음과 같은 옵션 작업을 수행할 수 있습니다.
   - 특정 위반만 표시하려면 * filter * 상자를 사용합니다.
   - 표에 위반사항이 5개 이상 있는 경우 페이지 번호를 클릭하여 위반사항을 페이지별로 탐색합니다.
   - 열 머리글의 화살표를 클릭하여 표에서 열의 정렬 순서를 오름차순(위쪽 화살표) 또는 내림차순(아래쪽 화살표)으로 변경합니다.
   - 설명에서 자산 이름을 클릭하여 자산 페이지를 표시합니다. 빨간색 원은 추가 조사가 필요한 문제를 나타냅니다.

     정책 편집 대화 상자가 표시된 성능 정책을 클릭하여 성능 정책을 검토하고 필요한 경우 정책을 변경할 수 있습니다.

   - 을 클릭합니다 문제가 더 이상 문제의 원인이 아닌 것으로 판단될 경우 목록에서 위반 사항을 제거합니다.

사용자 지정 가능한 자산 페이지

추가 데이터는 각 자산 페이지의 사용자 지정 가능한 위젯에 표시될 수 있습니다. 자산에 대한 페이지를 사용자 지정하면 해당 유형의 모든 자산에 대한 사용자 지정이 페이지에 적용됩니다.

다음 작업을 수행하여 자산 페이지 위젯을 사용자 지정합니다.

1. 페이지에 위젯을 추가합니다
2. 원하는 데이터를 표시할 위젯에 대한 쿼리 또는 표현식을 생성합니다
3. 원하는 경우 필터를 선택합니다
4. 롤업 또는 그룹화 방법을 선택합니다
5. 위젯을 저장합니다
6. 원하는 모든 위젯에 대해 반복합니다
7. 자산 페이지를 저장합니다

위젯에서 표시된 데이터를 더욱 구체화하는 데 사용할 수 있는 변수를 사용자 지정 자산 페이지에 추가할 수도 있습니다. 각 자산 유형은 일반 변수 외에도 "$this" 변수 세트를 사용하여 현재 자산과 직접 관련된 리소스를 빠르게 식별할 수 있습니다. 예를 들어, 현재 가상 머신을 호스팅하는 동일한 하이퍼바이저에 의해 호스팅되는 모든 가상 머신을 확인할 수 있습니다.

이 사용자 지정 자산 페이지는 각 사용자뿐 아니라 각 자산 유형에 대해 고유합니다. 예를 들어 사용자 A가 가상 머신에 대한 사용자 지정 자산 페이지를 생성하는 경우 해당 사용자에 대한 모든 가상 머신 자산 페이지에 대해 해당 사용자 지정 페이지가 표시됩니다.

사용자는 자신이 만든 사용자 지정 자산 페이지만 보고, 편집하거나 삭제할 수 있습니다.

사용자 지정 자산 페이지는 Insight의 내보내기/가져오기 기능에 포함되지 않습니다.

"$이" 변수 이해

자산의 "추가 데이터" 사용자 지정 페이지에 있는 특수 변수를 사용하면 현재 자산과 직접 관련된 추가 정보를 쉽게 표시할 수 있습니다.

이 작업에 대해

자산의 사용자 지정 가능한 랜딩 페이지의 위젯에 ""$This"" 변수를 사용하려면 다음 단계를 따르십시오. 이 예에서는 테이블 위젯을 추가합니다.

> ""$This" 변수는 자산의 사용자 지정 가능한 랜딩 페이지에만 유효합니다. 다른 Insight 대시보드에는 사용할 수 없습니다. 사용 가능한 "$This" 변수는 자산 유형에 따라 다릅니다.

단계

1. 선택한 자산에 대한 자산 페이지로 이동합니다. 이 예에서는 가상 머신(VM) 자산 페이지를 선택하겠습니다. VM을 쿼리하거나 검색하고 링크를 클릭하여 해당 VM의 자산 페이지로 이동합니다.

   VM의 자산 페이지가 열립니다.

2. 해당 자산의 사용자 지정 가능한 랜딩 페이지로 이동하려면 * Change view: * > * Additional Virtual Machine data * 드롭다운을 클릭합니다.
3. Widget * 버튼을 클릭하고 * Table widget * 을 선택합니다.

   편집을 위해 테이블 위젯이 열립니다. 기본적으로 모든 스토리지가 테이블에 표시됩니다.

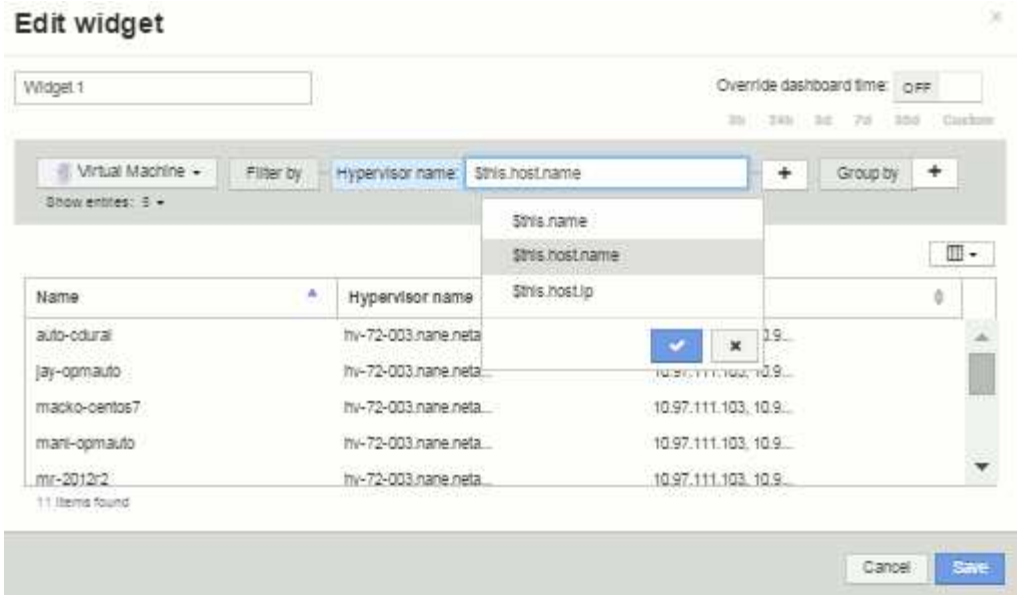
4. 모든 가상 시스템을 표시하려고 합니다. 자산 선택기를 클릭하고 * 스토리지 * 를 * 가상 머신 * 으로 변경합니다.

   이제 모든 가상 머신이 테이블에 표시됩니다.

5. 열 선택기 * 버튼을 클릭합니다 하이퍼바이저 이름 * 필드를 테이블에 추가합니다.

   하이퍼바이저 이름이 표에 각 VM에 대해 표시됩니다.

6. 우리는 현재 VM을 호스팅하는 하이퍼바이저만 신경 쓸 뿐입니다. 필터 기준* 필드의 **+** 버튼을 클릭하고 * 하이퍼바이저 이름 * 을 선택합니다.
7. 아무 * 나 * 를 클릭하고 * $this.host.name * 변수를 선택합니다. 확인 버튼을 클릭하여 필터를 저장합니다.



8. 이제 이 표에는 현재 VM의 하이퍼바이저에 의해 호스팅되는 모든 VM이 표시됩니다. 저장 * 을 클릭합니다.

결과

이 가상 머신 자산 페이지에 대해 생성한 테이블이 표시되는 모든 VM 자산 페이지에 대해 표시됩니다. 위젯에서 * $this.host.name * 변수를 사용하면 현재 자산의 하이퍼바이저가 소유한 VM만 테이블에 표시됩니다.

네트워크 리소스 밸런싱

밸런싱 문제를 해결하려면 자산 페이지를 사용하여 문제를 찾고 사용량이 적은 고용량 볼륨을 식별합니다.

단계

1. 브라우저에서 자산 대시보드를 엽니다.
2. 가상 머신 IOPS 히트 맵에서 매우 큰 인쇄물에 VM 이름이 표시되므로 종종 문제를 보고할 수 있습니다.
3. VM 이름을 클릭하여 자산 페이지를 표시합니다.
4. 요약에서 오류 메시지를 확인합니다.
5. 성능 차트 및 특히 상호 연결된 최상위 리소스를 확인하여 경합 중인 볼륨을 찾습니다.
6. 성능 차트에 볼륨을 추가하여 활동 패턴을 비교하고 문제와 관련된 다른 리소스의 자산 페이지를 더 많이 표시합니다.
7. 자산 페이지 맨 아래로 스크롤하여 VM과 관련된 모든 리소스 목록을 확인합니다. 고용량 vmdks를 실행합니다. 이로 인해 경합이 발생할 수 있습니다.
8. 균형 조정 문제를 해결하려면 과도하게 사용되는 리소스로부터 로드를 받거나 사용량이 많은 리소스에서 덜 까다로운 애플리케이션을 제거하기 위해 활용도가 낮은 리소스를 파악합니다.

네트워크 성능 검사

스토리지 환경의 성능을 검사하고 활용률이 저조하거나 활용도가 높은 리소스를 식별하고 문제가 발생하기 전에 위험을 식별할 수 있습니다.

Insight는 수집된 스토리지 데이터를 통해 밝혀진 성능 및 가용성 문제를 해결합니다.

Insight를 사용하여 다음과 같은 성능 관리 작업을 수행할 수 있습니다.

- 환경 전체의 성능 모니터링
- 다른 장치의 성능에 영향을 미치는 리소스를 파악합니다

포트의 중요성

DWH(Insight Server and Data Warehouse) 서버는 안정적으로 작동하려면 많은 TCP 포트를 사용할 수 있어야 합니다. 이러한 포트 중 일부는 localhost 어댑터(127.0.0.1)에 바인딩된 프로세스에만 활용되지만 핵심 서비스가 안정적으로 작동하려면 여전히 필요합니다. 필요한 포트 수는 네트워크에서 사용되는 포트의 상위 집합입니다.

Insight 서버 포트

Insight Server에는 소프트웨어 방화벽이 설치되어 있을 수 있습니다. 열어야 할 "구멍"은 아래와 같습니다.

- 인바운드 HTTPS 443 * - TCP 443에서 Insight WebUI를 실행 중인 경우 다음 소비자 중 일부 및 모두를 허용하도록 해당 를 노출해야 합니다.
- WebUI의 Insight 사용자
- Insight 서버에 연결하려는 원격 획득 장치
- 이 Insight 서버에 대한 커넥터가 있는 OCI DWH 서버
- Insight REST API와의 프로그래밍 상호 작용

Insight 서버 호스트 레벨 방화벽 구축을 원하는 모든 사람에게 NetApp은 모든 기업 네트워크 IP 블록에 HTTPS 액세스를 허용하도록 권장합니다.

- 인바운드 MySQL(TCP 3306) *. 이 포트는 커넥터가 있는 Insight DWH 서버에만 노출되어야 합니다

Insight에는 수십 개의 데이터 수집기가 있지만 모두 폴링 기반 Insight로 인해 획득 장치(AUS)가 다양한 장치에 대한 아웃바운드 통신을 시작합니다. 호스트 기반 방화벽이 방화벽을 통해 반환 트래픽을 허용할 수 있도록 "상태 저장"되어 있는 한 Insight Server의 호스트 기반 방화벽은 데이터 획득에 영향을 주지 않습니다.

데이터 웨어하우스 포트

Insight DWH 서버의 경우:

- 인바운드 HTTPS 443 * - TCP 443에서 Insight WebUI를 실행 중인 경우 다음 소비자를 허용하도록 해당 를 노출해야 합니다.
- DWH 관리 포털의 Insight 관리 사용자
- 인바운드 HTTPS(TCP 9300) * - Cognos 보고 인터페이스입니다. 사용자가 Cognos 보고 인터페이스와 상호 작용할 경우 이 정보는 원격으로 노출되어야 합니다.

DWH를 노출할 필요가 없는 환경을 상상할 수 있습니다. 보고서 작성자는 DWH 서버에 RDP 연결을 만들고 보고서를 작성 및 예약하는 동시에 모든 보고서가 SMTP를 통해 전송되거나 원격 파일 시스템에 기록되도록 예약할 수 있습니다.

- 인바운드 MySQL(TCP 3306) *. 이 포트는 조직이 DWH 데이터와 MySQL 기반 통합을 수행하는 경우에만 노출되어야 합니다. - CMDB, 차지백 시스템 등과 같은 다른 애플리케이션에 대한 인제스트하기 위해 다양한 DWH 데이터 마트에서 데이터를 추출하는 경우

느린 **PC** 성능 분석

네트워크 사용자의 컴퓨터가 느리게 실행된다고 불평하는 전화를 받는 경우 호스트 성능을 분석하고 영향을 받는 리소스를 확인해야 합니다.

시작하기 전에

이 예제에서 호출자는 호스트 이름을 지정합니다.

단계

1. 브라우저에서 Insight를 엽니다.
2. Search assets * 상자에 호스트 이름을 입력하고 검색 결과에서 호스트 이름을 클릭합니다.

   리소스의 _asset 페이지_가 열립니다.

3. 호스트의 자산 페이지에서 페이지 중앙의 성능 차트를 확인합니다. 일반적으로 사전 선택된 지연 시간 및 IOPS 외에 다른 유형의 데이터를 표시할 수 있습니다. 장치 유형에 따라 처리량, 메모리, CPU 또는 IP 처리량 등 다른 유형의 데이터에 대한 확인란을 클릭합니다.
4. 차트에 점에 대한 설명을 표시하려면 마우스 포인터를 해당 점 위에 놓습니다.
5. 또한 페이지 맨 위에 있는 선택 항목의 시간 범위를 3시간~7일 또는 사용 가능한 모든 데이터로 변경할 수도 있습니다.
6. 상호 연결된 상위 리소스 * 의 목록을 검토하여 기본 리소스와 패턴이 동일한 다른 리소스가 있는지 확인합니다.

   목록의 첫 번째 자원은 항상 기본 자원입니다.

   a. 연결된 리소스 옆의 연결된 백분율을 클릭하여 연결된 활동 패턴이 기본 리소스 및 다른 리소스의 IOPS 또는 CPU에 있는지 확인합니다.
   b. 연결된 리소스의 확인란을 클릭하여 해당 데이터를 성능 차트에 추가합니다.
   c. 연결된 리소스의 연결된 이름을 클릭하여 자산 페이지를 표시합니다.
7. 이 예에서 볼 수 있듯이 VM의 경우 * 상호 연결된 최상위 리소스 * 에서 스토리지 풀을 찾고 스토리지 풀 이름을 클릭합니다.

관련 리소스 분석 중

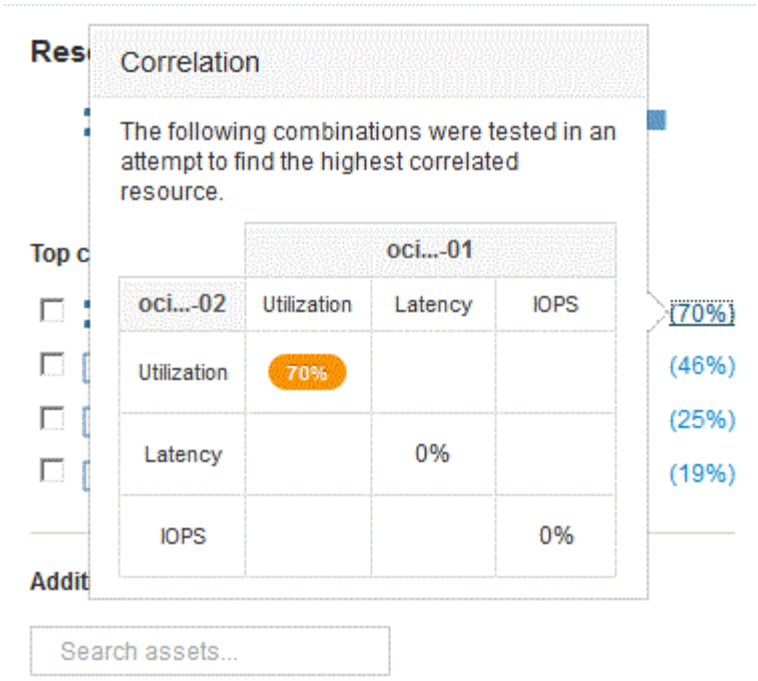
성능 문제를 조사하고 장치에 대한 _asset 페이지_를 여는 경우 상호 연결된 최상위 리소스 목록을 사용하여 성능 차트에 표시되는 데이터를 구체화해야 합니다. 백분율이 높은 자원은 기본 자원과 활동이 유사함을 나타냅니다.

이 작업에 대해

성능 문제를 조사 중이며 장치의 자산 페이지를 열었습니다.

단계

1. Top Correlated resources * 목록에서 첫 번째 리소스는 기본 리소스입니다. 목록의 상관 자원은 첫 번째 장치에 대한 상관 활동의 비율에 따라 순위가 매겨집니다. 연결된 상관 비율을 클릭하여 세부 정보를 봅니다. 이 예에서 70%의 상관관계는 사용률이므로 기본 리소스와 상호 연결된 리소스 모두 동일한 수준의 사용률을 가지고 있습니다.



2. 성능 차트에 연결된 리소스를 추가하려면 추가하려는 리소스의 * 상호 연결된 최상위 리소스 * 목록에서 확인란을 선택합니다. 기본적으로 각 자원에는 사용 가능한 전체 데이터가 제공되지만 확인란의 메뉴에서 읽기 또는 쓰기 데이터만 선택할 수 있습니다.

   차트의 각 리소스는 서로 다른 색을 사용하여 각 리소스의 성능 측정값을 비교할 수 있습니다. 선택한 측정 메트릭에는 적절한 유형의 데이터만 플롯됩니다. 예를 들어 CPU 데이터에는 읽기 또는 쓰기 메트릭이 없으므로 총 데이터만 사용할 수 있습니다.

3. 연결된 리소스의 연결된 이름을 클릭하여 자산 페이지를 표시합니다.
4. 분석에 고려되어야 한다고 생각하는 상호 연결된 최상위 리소스에 나열된 리소스가 표시되지 않으면 * 자산 검색 * 상자를 사용하여 해당 리소스를 찾을 수 있습니다.

파이버 채널 환경 모니터링

OnCommand Insight의 파이버 채널 자산 페이지를 사용하여 환경 내의 패브릭의 성능 및 인벤토리를 모니터링하고 문제를 일으킬 수 있는 변경 사항을 인지할 수 있습니다.

파이버 채널 자산 페이지

Insight의 자산 페이지에서는 리소스, 토폴로지(장치 및 연결), 성능 차트 및 관련 리소스 표에 대한 요약 정보를 제공합니다. 패브릭, 스위치 및 포트 자산 페이지를 사용하여 파이버 채널 환경을 모니터링할 수 있습니다. Fibre Channel 문제를 해결할 때 특히 유용하며, 각 포트 자산에 대한 성능 도표는 선택한 최상위 기여 포트의 트래픽을 보여줍니다. 또한 Insight에서 각 메트릭에 대한 별도의 성능 차트를 표시하면서 이 차트에 버퍼링까지 크레딧 메트릭과 포트 오류를 표시할 수도 있습니다.

포트 메트릭에 대한 성능 정책

Insight를 사용하면 성능 정책을 생성하여 네트워크를 모니터링하여 다양한 임계값을 파악하고 이러한 임계값을 초과할 때 경고를 표시할 수 있습니다. 사용 가능한 포트 메트릭을 기준으로 포트에 대한 성능 정책을 생성할 수 있습니다. 임계값 위반이 발생하면 Insight는 빨간색 실선 원을 표시하고, 이메일 알림을 구성하고, 위반 대시보드 또는 위반을 보고하는 사용자 지정 대시보드를 통해 관련 자산 페이지에서 이를 감지하여 보고합니다.

TTL(Time-to-Live) 및 다운샘플링 데이터

OnCommand Insight 7.3부터는 데이터 보존 또는 TTL(Time-to-Live)이 7일에서 90일로 증가했습니다. 즉, 차트 및 테이블에 대해 훨씬 더 많은 데이터가 처리되고 수만 개의 데이터 포인트(datapart)가 발생할 가능성이 있기 때문에 데이터가 표시되기 전에 다운샘플링됩니다.

다운샘플링은 차트에서 데이터의 통계적 근사치를 제공하여 수집된 데이터의 정확한 뷰를 유지하면서 모든 데이터 요소를 표시할 필요 없이 데이터를 효율적으로 개괄적으로 보여 줍니다.

다운샘플링이 필요한 이유는 무엇입니까?

Insight 7.3은 데이터의 TTL(Time-to-Live)을 90일로 늘립니다. 즉, 차트 및 그래프에 표시할 데이터를 준비하는 데 필요한 처리 양이 증가합니다. 차트를 빠르고 효율적으로 표시할 수 있도록 해당 차트의 모든 데이터 요소를 처리할 필요 없이 차트의 전체 모양을 유지하는 방식으로 데이터가 다운샘플링됩니다.

> 다운샘플링 중에는 실제 데이터가 손실되지 않습니다. 아래 그림에 표시된 단계를 따르면 다운샘플링된 데이터 대신 차트의 실제 데이터를 볼 수 있습니다.

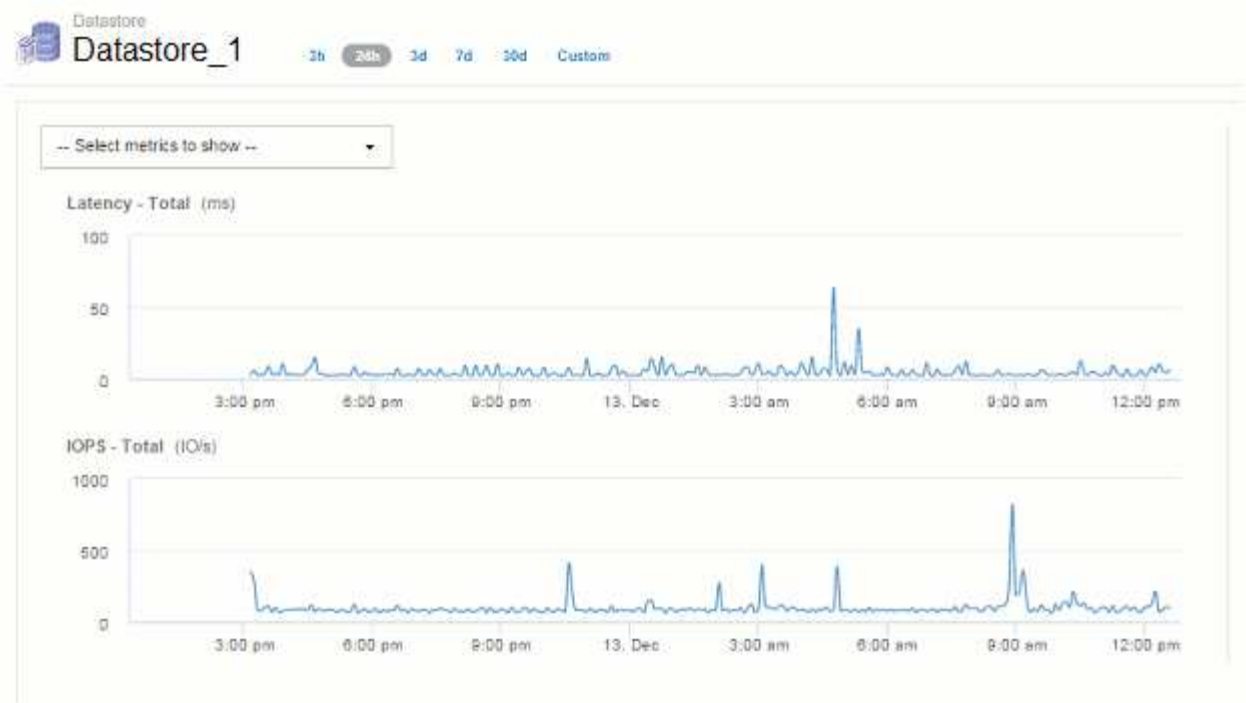
다운샘플링의 작동 방식

데이터는 다음 조건에서 다운샘플링됩니다.

- 선택한 시간 범위에 7일 이하의 데이터가 포함된 경우 다운샘플링이 발생하지 않습니다. 차트는 실제 데이터를 표시합니다.
- 선택한 시간 범위에 7일 이상의 데이터가 포함되어 있지만 데이터 요소가 1,000개 미만인 경우 다운샘플링이 발생하지 않습니다. 차트는 실제 데이터를 표시합니다.
- 선택한 시간 범위에 7일 이상의 데이터와 1,000개 이상의 데이터 요소가 포함된 경우 데이터가 다운샘플링됩니다. 차트는 근사화된 데이터를 표시합니다.

다음 예에서는 다운샘플링이 실제 작동 중인 것을 보여 줍니다. 첫 번째 그림에서는 데이터 저장소 자산 페이지의 시간 선택기에서 * 24h * 를 선택하여 24시간 동안 데이터 저장소 자산 페이지에 지연 시간 및 IOPS 차트를 보여 줍니다. 또한 * Custom * 을 선택하고 동일한 24시간 기간으로 시간 범위를 설정하여 동일한 데이터를 볼 수도 있습니다.

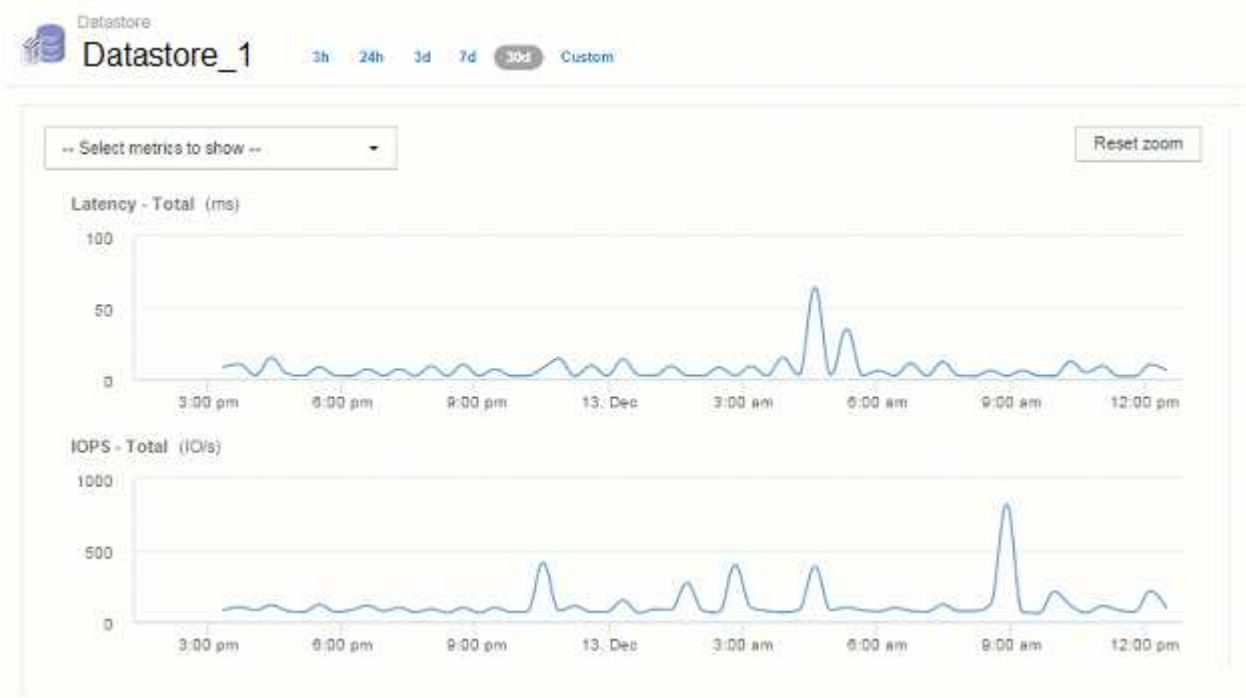
7일 미만의 시간 범위를 선택하고 차트에 사용할 데이터 요소가 1,000개 미만인 경우 표시되는 데이터는 실제 데이터입니다. 다운샘플링이 발생하지 않습니다.



그러나 자산 페이지 시간 선택기에서 * 30d * 를 선택하여 데이터를 보는 경우 또는 7일 이상의 사용자 지정 시간 범위를 설정하여(또는 Insight가 선택한 기간 동안 1,000개 이상의 데이터 샘플을 수집한 경우) 데이터가 표시되기 전에 다운샘플링됩니다. 다운샘플링된 차트를 확대하면 디스플레이에 근사화된 데이터가 계속 표시됩니다.

> 다운샘플링된 차트를 확대할 때 확대/축소는 디지털 확대/축소입니다. 디스플레이에 근사치 데이터가 계속 표시됩니다.

다음 그림에서 시간 범위가 처음 30d로 설정된 것을 볼 수 있으며, 그런 다음 차트를 확대하여 위와 동일한 24시간 기간을 표시할 수 있습니다.



다운샘플링된 차트는 위의 "실제" 차트와 동일한 24시간 기간을 보여 주므로 동일한 일반 셰이프를 따라 선이

표시되므로 성능 데이터에서 흥미로운 최고점 또는 최저점을 빠르게 찾을 수 있습니다.

> 다운샘플링을 위해 데이터가 근사화되기 때문에 다운샘플과 비교할 때 차트 선이 약간 꺼질 수 있습니다 실제 데이터를 사용하여 그래프를 더 잘 정렬할 수 있습니다. 그러나 차이는 크지 않으며 표시되는 데이터의 전체 정확도에는 영향을 미치지 않습니다.

다운샘플링된 차트에 대한 위반

다운샘플링된 차트를 볼 때는 위반 사항이 표시되지 않는다는 점에 유의하십시오. 위반 사항을 보려면 다음 두 가지 중 하나를 수행합니다.

- 자산 페이지 시간 선택기에서 사용자 정의를 선택하고 7일 미만의 시간 범위를 입력하여 해당 시간 범위의 실제 데이터를 봅니다. 각 빨간색 점 위로 마우스를 가져갑니다. 도구 설명에 발생한 위반이 표시됩니다.
- 시간 범위를 기록하고 위반 대시보드에서 위반 사항을 찾습니다.

재고 기록 정리

Insight는 버전 7.3.2부터 90일 동안 인벤토리(기반) 변경 기록을 유지합니다. 이전 버전의 Insight에서는 설치 시점의 모든 재고 변경 내역이 유지됩니다. 이전 버전의 Insight에서 업그레이드한 후 오래된 재고 기록은 로 정리된 후 90일 동안 유지됩니다.

최신 버전의 OnCommand Insight로 업그레이드한 후 가장 최근 90일 동안 기록이 정리됩니다. Insight는 가장 오래된 것부터 시작하여 90일 분량의 역사가 남아 있을 때까지 하루에 한 번 30일 단위로 역사를 정리합니다. 그런 다음, 매일 역사를 정리하여 90일 동안의 재고 변경 내역을 유지합니다.

VM의 **NAS** 경로입니다

OnCommand Insight 7.3은 가상 머신에서 스토리지 공유에 대한 NAS 경로를 지원합니다. 이러한 경로는 호스트에서 스토리지 공유에 대한 NAS 경로와 유사합니다. VM의 IP 주소가 공유에 액세스할 수 있으면 NAS 경로가 생성됩니다.

가상 머신의 NAS 경로는 내부 볼륨 랜딩 페이지에 표시됩니다. 이 페이지에는 VM이 액세스할 수 있는 내부 볼륨을 식별하는 게스트 마운트 스토리지 리소스 위젯이 포함되어 있습니다.

- NAS 경로는 가상 머신이 백엔드 공유에 액세스할 수 있을 때 생성됩니다. 가상 머신이 공유에 액세스하는지 여부에 대한 확인은 없습니다.
- 상관 관계 계산은 지연 시간과 IOPS를 기반으로 하며 VM에 백엔드 스토리지에 대한 NAS 경로가 있는 경우는 포함되지 않습니다.
- 사용자는 이니시에이터 IP 주소로 공유를 쿼리할 수 있지만, 경로로 쿼리하는 것은 지원되지 않습니다.

이제 내부 볼륨의 컴퓨팅 리소스 표에 NAS 경로가 있는 VM도 표시됩니다. 각 VM, CPU 및 메모리에 대해 사용률 및 성능 데이터가 제공됩니다.

데이터 웨어하우스에 미치는 영향

OnCommand Insight 7.3으로 업그레이드한 후 표시되는 데이터 웨어하우스의 변경 사항은 다음과 같습니다.

- dWh_inventory.nas_logical 테이블이 Inventory Data Mart에서 제거되고 보기로 교체됩니다.

NFS 경로 테이블이 포함된 Insight 7.2.x 보고서는 그대로 유지됩니다.

- dWh_inventory.nas_cr_logical 테이블이 Inventory Data Mart에 추가되고 다음 항목이 포함됩니다.
  - 컴퓨팅 리소스
  - 내부 볼륨
  - 스토리지
  - NAS 공유

시간 시리즈로서의 용량

OnCommand Insight 7.3.1에서는 용량 정보가 시간 시리즈 데이터로 보고되고 차트로 작성됩니다.

이전에는 데이터 소스에서 가져온 용량 정보가 "시점" 데이터(PIT)로만 제공되기 때문에 차트에서 시계열 데이터로 사용할 수 없었습니다. 이제 자산의 용량 값을 다음과 같은 방법으로 시계열 데이터로 사용할 수 있습니다.

- 표, 위젯, 전문가 뷰 및 시계열 데이터가 표시되는 모든 위치에 그래프로 표시됩니다
- 기존 의미를 사용하는 위반의 성능 임계값에 적용됩니다
- 필요한 경우 다른 성능 카운터와 함께 식에 사용됩니다

이전 버전의 Insight에서 업그레이드하는 경우 쿼리 또는 사용자 지정 대시보드의 필터에 사용된 이전 PIT 용량 값이 시계열 용량 데이터로 대체됩니다. 따라서 이전 Insight 버전의 동급 데이터와 비교할 때 용량 데이터가 보고되거나 필터링되는 방식이 약간 변경될 수 있습니다.