Subscription Central 1-latest

Discovery 사용

Discovery 이해

Last Updated: 2024-10-05

Subscription Central 1-latest Discovery 사용

Discovery 이해

법적 공지

초록

차례

1장. DISCOVERY 정보

Discovery는 사용자가 특정 Red Hat 소프트웨어 사용에 대한 데이터를 수집할 수 있도록 설계되었습니다. Discovery를 사용하면 해당 Red Hat 제품의 사용량을 계산하고 보고하는 데 필요한 시간과 노력을 줄일 수 있습니다.

더 알아보기

Discovery의 목적, 이점 및 특성에 대한 자세한 내용은 다음 정보를 참조하십시오.

- Discovery란 무엇인가?

Discovery에서 찾고 검사할 수 있는 제품 및 제품 버전에 대한 자세한 내용은 다음 정보를 참조하십시오.

- Discovery는 어떤 제품을 찾을 수 있습니까?

Discovery가 올바른 솔루션인지 여부를 평가하려면 다음 정보를 참조하십시오.

- Discovery가 사용 적합합니까?

1.1. DISCOVERY란 무엇인가?

Discovery는 검사 및 보고 도구입니다. 이는 네트워크, 운영 체제 및 기타 구성 데이터에서 물리적 시스템 및 가상 시스템 수와 같은 환경 데이터 또는 팩트를 찾고, 식별하고, 보고하도록 설계되었습니다. 또한 해당 네트워크의 IT 리소스에 대한 일부 주요 Red Hat 패키지 및 제품에 대한 자세한 정보를 찾아 식별하고 보고하도록 설계되었습니다.

네트워크에서 실행 중인 소프트웨어 및 시스템을 검사할 수 있으므로 서브스크립션 사용량을 이해하고 보고하는 기능이 향상됩니다. 궁극적으로 이러한 검사 및 보고 프로세스는 인벤토리를 관리하는 대규모 시스템 관리 작업의 일부입니다.

Discovery는 IT 리소스에 액세스하고 검사 프로세스를 실행하기 위해 두 가지 기본 구조를 구성해야 합니다. *인증 정보*에는 특정 소스에서 검사 프로세스를 실행하거나 해당 소스의 일부 자산을 실행할 수 있는 충분한 권한이 있는 사용자의 사용자 액세스 데이터(예: 사용자 이름 및 암호 또는 SSH 키)가 포함되어 있습니다. 소스에는 검사할 단일 자산 또는 여러 자산에 대한 데이터가 포함되어 있습니다. 이러한 자산은 호스트 이름, IP 주소, IP 범위 또는 서브넷으로 식별되는 물리적 시스템, 가상 시스템 또는 컨테이너일 수 있습니다. 이러한 자산은 vCenter Server 또는 Red Hat Satellite Server와 같은 시스템 관리 솔루션이거나 Red Hat OpenShift Container Platform에 배포된 클러스터일 수도 있습니다.

참고

현재 가상화 인프라 전용 소스를 사용하여 Discovery에서 검색할 수 있는 유일한 가상화된 배포는 VMware vCenter입니다. Red Hat에서 지원하는 다른 가상화 인프라는 특수 검사를 통해 검색할 수 없습니다. 특수 검사에서 정확한 메타데이터를 반환하지 않더라도 네트워크 일반 검색은 여전히 이러한 자산을 검색할 수 있습니다.

검사 프로세스를 실행하거나 *스캔*할 때 Discovery와 함께 사용할 여러 인증 정보 및 소스를 저장할 수 있습니다. 검사를 완료한 경우 출력에서 이러한 팩트를 형식화된 데이터 모음으로 액세스하거나 *보고서*를 작성하여 결과를 검토할 수 있습니다.

기본적으로 Discovery를 사용하는 동안 생성된 인증 정보 및 소스는 데이터베이스에서 암호화됩니다. 값은 AES-256을 사용하여 암호화됩니다. 이러한 암호는 Discovery 서버가 볼트 암호를 사용하여 검색을 실행하여 데이터베이스에 저장된 암호화된 값에 액세스하면 해독됩니다.

Discovery는 에이전트가 없는 검사 도구이므로 검사해야 하는 모든 소스에 툴을 설치할 필요가 없습니다. 그러나 Discovery가 설치된 시스템은 검색 및 검사할 시스템에 액세스할 수 있어야 합니다.

1.2. DISCOVERY는 어떤 제품을 찾을 수 있습니까?

Discovery는 다음 Red Hat 제품을 검색합니다. 각 버전 또는 릴리스에 대해 초기 버전이 나열되며 이후 버전은 검색 대상으로 표시됩니다.

최근에 이름이 변경된 경우 해당 제품의 현재 이름에 더 익숙한 경우 해당 이름이 추가 정보로 제공됩니다. 새 제품 이름이 나열되어 있지만 해당 제품의 특정 버전이 함께 표시되지 않는 한 이후 버전은 적용되지 않습니다.

Red Hat Enterprise Linux

- Red Hat Enterprise Linux 버전 5 이상
- Red Hat Enterprise Linux 버전 6 이상
- Red Hat Enterprise Linux 버전 7 이상
- Red Hat Enterprise Linux 버전 8 이상
- Red Hat Enterprise Linux 버전 9 이상

Red Hat Application Services 제품 (이전 Red Hat Middleware)

- JBoss Enterprise Web Server 버전 1 이상; Red Hat JBoss Web Server 3.0.1 이상
- Red Hat JBoss Enterprise Application Platform 버전 4.2 이상, 버전 4.3 이상, 버전 5 이상, 버전 6 이상, 버전 7 이상
- Red Hat Fuse 버전 6.0 이상

Red Hat Ansible Automation Platform

- Ansible Automation Platform 버전 2 이상

Red Hat OpenShift Container Platform

- Red Hat OpenShift Container Platform 버전 4 이상

Red Hat Advanced Cluster Security for Kubernetes

- Red Hat Advanced Cluster Security for Kubernetes 버전 4 이상

Red Hat Advanced Cluster Security for Kubernetes

- Red Hat Advanced Cluster Management for Kubernetes 버전 2 이상

1.3. DISCOVERY가 사용 적합합니까?

Discovery는 복잡한 네트워크에서 알 수 없는 제품 사용량을 포함하여 Red Hat 제품 인벤토리를 찾고 이해할 수 있도록 하기 위한 것입니다. Discovery에서 생성한 보고서는 Red Hat Solution Architect(SA) 또는 TAM(Technical Account Manager)과의 파트너십을 통해 또는 SEAP(Subscription and Awareness

Program)에서 제공하는 분석 및 지원을 통해 가장 잘 이해할 수 있습니다.

별도로 Discovery를 설치하고 사용한 다음 보고서 데이터를 생성하고 볼 수 있지만 검색 설명서는 보고서 결과를 해석하는 데 도움이 되는 정보를 제공하지 않습니다. 또한 Red Hat 지원은 Discovery 설치 및 사용과 관련된 몇 가지 기본 지원을 제공하지만 보고서를 이해하기 위한 지원은 제공하지 않습니다.

Discovery 툴은 Red Hat과 직접 데이터를 자동으로 공유하지 않습니다. 대신 Red Hat 툴 및 서비스에 통합하기 위해 보고서 데이터를 준비하고 Red Hat으로 보낼지 여부를 선택할 수 있습니다. Discovery 툴을 로컬로 사용하여 Discovery가 현재 지원하는 Red Hat 제품의 네트워크를 스캔한 다음 생성된 보고서를 내부 용도로 사용할 수 있습니다.

2장. DISCOVERY 사용자 인터페이스에 액세스

브라우저를 통해 Discovery 그래픽 사용자 인터페이스에 액세스합니다.

더 알아보기

Discovery 그래픽 사용자 인터페이스에 로그인하거나 로그아웃하는 요구 사항 및 단계에 대한 자세한 내용은 다음 정보를 참조하십시오.

- Discovery 사용자 인터페이스에 로그인
- Discovery 사용자 인터페이스에서 로그아웃

2.1. DISCOVERY 사용자 인터페이스에 로그인

Discovery 사용자 인터페이스에 로그인하려면 Discovery 서버가 설치된 시스템의 IP 주소, 서버 설치 중에 기본 포트가 변경된 경우 연결의 포트 번호, 로그인할 때 사용할 서버 관리자 사용자 이름과 암호가 필요합니다. 이 정보가 없는 경우 Discovery 서버를 설치한 관리자에게 문의하십시오.

사전 요구 사항

- Discovery 그래픽 사용자 인터페이스를 사용하려면 사용자 인터페이스를 실행할 시스템을 Discovery 서버가 설치된 시스템과 통신할 수 있어야 합니다.

프로세스

1. 브라우저에서 Discovery 서버의 URL을 **https://*IPaddress*:*server_port*** 형식으로 입력합니다. 여기서 ***IPaddress*** 는 Discovery 서버의 IP 주소이고 ***server_port*** 는 노출된 서버 포트입니다.
   다음 예제에서는 로그인 중인 시스템과 기본 포트가 사용되는지 여부에 따라 URL을 입력하는 두 가지 방법을 보여줍니다.
   - 서버가 설치되어 있고 기본 포트 **9443** 이 사용되는 시스템에서 로그인하는 경우 다음 예와 같이 루프백 주소(localhost라고도 함)를 IP 주소로 사용할 수 있습니다.

     ```
     https://127.0.0.1:9443
     ```

   - 서버에서 원격인 시스템에서 로그인하는 경우 서버는 IP 주소 **192.0.2.0** 에서 실행 중이며 설치 중에 기본 포트가 **8443** 으로 변경되었습니다. 다음 예와 같이 로그인합니다.

     ```
     https://192.0.2.0:8443
     ```

   서버의 URL을 입력하면 Discovery 로그인 페이지가 표시됩니다.
2. 로그인 페이지에서 Discovery 서버 관리자 계정의 사용자 이름과 암호를 입력한 다음 **로그인**을 클릭하여 서버에 로그인합니다.

검증 단계

Discovery에 처음 로그인한 경우 welcome 페이지가 표시됩니다. 검사에 사용할 수 있는 소스 및 인증 정보를 추가하여 시작할 수 있습니다. 이전에 Discovery에 로그인한 경우 welcome 페이지를 건너뛰고 이전에 생성한 소스, 인증 정보 및 스캔과 상호 작용할 수 있습니다.

2.2. DISCOVERY 사용자 인터페이스에서 로그아웃

프로세스

1. 애플리케이션 도구 모음에서 사용자 아이콘 또는 사용자 이름을 클릭합니다.
2. **Logout**을 클릭합니다.

3장. 소스 및 인증 정보 추가

검색을 실행하도록 Discovery를 준비하려면 검사하려는 IT 인프라의 일부를 하나 이상의 소스로 추가해야 합니다. 하나 이상의 인증 정보로 해당 소스에 액세스하는 데 필요한 사용자 이름 및 암호 또는 SSH 키와 같은 인증 정보도 추가해야 합니다. 구성 요구 사항이 다르기 때문에 검사하려는 소스 유형에 따라 소스 및 인증 정보를 추가합니다.

더 알아보기

IT 인프라의 다른 부분을 포함하는 소스 및 인증 정보를 추가하는 일반적인 프로세스의 일부로 여러 작업을 완료해야 할 수 있습니다.

네트워크 소스 및 인증 정보를 추가하여 네트워크의 물리적 시스템, 가상 시스템 또는 컨테이너와 같은 자산을 스캔합니다. 자세한 내용은 다음 정보를 참조하십시오.

- 네트워크 소스 및 인증 정보 추가

Red Hat Satellite Server 배포를 스캔하여 관리하는 자산을 찾기 위해 Satellite 소스 및 인증 정보를 추가합니다. 자세한 내용은 다음 정보를 참조하십시오.

- Satellite 소스 및 인증 정보 추가

vcenter 소스 및 인증 정보를 추가하여 vCenter Server 배포를 검사하여 관리하는 자산을 찾습니다. 자세한 내용은 다음 정보를 참조하십시오.

- vCenter 소스 및 인증 정보 추가

OpenShift 소스 및 인증 정보를 추가하여 Red Hat OpenShift Container Platform 클러스터 배포를 스캔합니다. 자세한 내용은 다음 정보를 참조하십시오.

- OpenShift 소스 및 인증 정보 추가

Ansible 소스 및 인증 정보를 추가하여 Ansible Automation Platform 배포를 검사하여 관리하는 보안 클러스터를 찾습니다. 자세한 내용은 다음 정보를 참조하십시오.

- Ansible 소스 및 인증 정보 추가

RHACS 소스 및 인증 정보를 추가하여 Red Hat Advanced Cluster Security for Kubernetes 배포를 검사하여 RHACS에서 관리하는 보안 클러스터를 찾습니다. 자세한 내용은 다음 정보를 참조하십시오.

- RHACS 소스 및 인증 정보 추가

3.1. 네트워크 소스 및 인증 정보 추가

네트워크에서 하나 이상의 물리적 시스템, 가상 머신 또는 컨테이너에서 검사를 실행하려면 검사할 각 자산을 식별하는 소스를 추가해야 합니다. 그런 다음 인증 데이터가 포함된 인증 정보를 추가하여 각 자산에 액세스해야 합니다.

더 알아보기

하나 이상의 네트워크 소스 및 인증 정보를 추가하여 네트워크의 자산을 검사하는 데 필요한 정보를 제공합니다. 자세한 내용은 다음 정보를 참조하십시오.

- 네트워크 소스를 추가하려면 네트워크 소스 추가를 참조하십시오.
- 네트워크 인증 정보를 추가하려면 네트워크 인증 정보 추가를 참조하십시오.

소스 및 인증 정보 및 Discovery가 이를 사용하는 방법에 대한 자세한 내용은 다음 정보를 참조하십시오.

- 소스 및 인증 정보 정보

Discovery가 네트워크에서 자산으로 인증하는 방법에 대한 자세한 내용은 다음 정보를 참조하십시오. 이 정보에는 승격된 권한으로 명령을 실행하는 방법에 대한 지침, 네트워크 인증 정보 구성 중에 수행해야 할 선택 사항이 포함되어 있습니다:

- 네트워크 인증
- 원격 네트워크 자산 검사에 사용되는 명령

3.1.1. 네트워크 소스 추가

초기 welcome 페이지 또는 소스 보기에서 소스를 추가할 수 있습니다.

프로세스

1. 위치를 기반으로 새 인증 정보를 추가하려면 옵션을 클릭합니다.
   - welcome 페이지에서 **소스 추가** 를 클릭합니다.
   - 소스 보기에서 **추가** 를 클릭합니다.

   소스 추가 마법사가 열립니다.
2. 유형 페이지에서 소스 유형으로 **네트워크 범위**를 선택하고 **다음**을 클릭합니다.
3. 인증 정보 페이지에서 다음 정보를 입력합니다.
   a. **이름** 필드에 설명이 포함된 이름을 입력합니다.
   b. **검색 주소** 필드에 쉼표로 구분된 하나 이상의 네트워크 식별자를 입력합니다. 호스트 이름, IP 주소 및 IP 범위를 입력할 수 있습니다.
      - DNS 호스트 이름으로 호스트 이름을 입력합니다(예: **server1.example.com**).
      - CIDR 또는 Ansible 표기법에 IP 범위를 입력합니다(예: CIDR 표기법의 경우 **192.168.1.0/24** 또는 Ansible 표기법의 경우 **192.168.1.[1:254]**).
   c. 선택 사항: 이 소스에 대한 검사를 기본 포트 22에서 실행하지 않으려면 **포트** 필드에 다른 포트를 입력합니다.
   d. **인증 정보** 목록에서 이 소스의 네트워크 리소스에 액세스하는 데 필요한 인증 정보를 선택합니다. 필요한 인증 정보가 없는 경우 **인증 정보 추가** 아이콘을 클릭하여 인증 정보 추가 마법사를 엽니다.
   e. 네트워크 리소스에 Ansible 연결 방법이 기본 OpenSSH 구현 대신 Python SSH 구현인 Paramiko가 되도록 하려면 **OpenSSH 확인란 대신 Paramiko를 사용하여** 연결을 선택합니다.
4. **저장을** 클릭하여 소스를 저장한 다음 **닫기** 를 클릭하여 소스 추가 마법사를 종료합니다.

3.1.2. 네트워크 인증 정보 추가

소스 생성 중에 인증 정보 보기 또는 소스 추가 마법사에서 인증 정보를 추가할 수 있습니다. 단일 소스에 포함된 모든 자산에 인증하기 위해 여러 인증 정보를 추가해야 할 수 있습니다.

사전 요구 사항

- 네트워크 인증 정보에 SSH 키 인증 유형을 사용하려면 사용할 각 SSH 개인 키를 Discovery 서버 설치 중에 **/sshkeys**에 매핑된 디렉터리로 복사해야 합니다. 이 디렉터리의 기본 경로는 **"${HOME}"/.local/share/discovery/sshkeys** 입니다.
  /sshkeys 디렉터리에서 사용할 수 있는 SSH 키에 대한 자세한 내용은 해당 디렉터리에 키 추가를 요청하려면 Discovery 서버를 관리하는 관리자에게 문의하십시오.

프로세스

1. 위치를 기반으로 새 인증 정보를 추가하려면 옵션을 클릭합니다.
   - 인증 정보 보기에서 **네트워크 인증 정보+추가** 를 클릭합니다.
   - 소스 추가 마법사에서 **인증 정보** 필드에 대한 **인증 정보 추가** 아이콘을 클릭합니다.

   인증 정보 추가 마법사가 열립니다.
2. **인증 정보 이름** 필드에 설명하는 이름을 입력합니다.
3. **인증 유형** 필드에서 사용할 인증 유형을 선택합니다. **사용자 이름 및 암호** 또는 **SSH 키** 중 하나를 선택할 수 있습니다.
4. 인증 유형에 따라 적절한 필드에 인증 데이터를 입력합니다.
   - 사용자 이름 및 암호 인증에 사용자의 사용자 이름과 암호를 입력합니다. 이 사용자에게는 네트워크 또는 검사하려는 네트워크의 하위 집합에 대한 루트 수준 액세스 권한이 있어야 합니다. 또는 이 사용자는 선택한 become 메서드를 사용하여 root 수준 액세스 권한을 얻을 수 있어야 합니다.
   - SSH 키 인증의 경우 사용자 이름과 Discovery 서버 컨테이너에 로컬인 SSH 키 파일의 경로를 입력합니다. 예를 들어 키 파일이 서버의 **"${HOME}"/.local/share/discovery/sshkeys** 기본 경로에 있는 경우 **SSH 키 파일** 필드에 해당 경로를 입력합니다. 암호를 입력하는 것은 선택 사항입니다.
5. 권한 상승을 위한 방법을 입력합니다. 네트워크 검사 중에 일부 명령을 실행하려면 권한 상승이 필요합니다. become 메서드의 사용자 이름과 암호를 입력하는 것은 선택 사항입니다.
6. **저장**을 클릭하여 인증 정보를 저장하고 인증 정보 추가 마법사를 종료합니다.

3.1.3. 소스 및 인증 정보

검사를 실행하려면 소스 및 인증 정보 두 가지 기본 구조에 대한 데이터를 구성해야 합니다. 검사 중에 검사할 소스 유형에 따라 소스 및 인증 정보 구성에 필요한 데이터 유형이 결정됩니다.

소스에는 스캔 중에 검사할 단일 자산 또는 여러 자산 세트가 포함되어 있습니다. 다음 유형의 소스를 구성할 수 있습니다.

네트워크 소스

하나 이상의 물리적 시스템, 가상 시스템 또는 컨테이너 이러한 자산은 호스트 이름, IP 주소, IP 범위 또는 서브넷으로 표시할 수 있습니다.

vCenter 소스

IT 인프라의 전체 또는 일부를 관리하는 vCenter Server 시스템 관리 솔루션입니다.

Satellite 소스

IT 인프라의 전체 또는 일부를 관리하는 Satellite 시스템 관리 솔루션입니다.

Red Hat OpenShift 소스

Red Hat OpenShift Container Platform 노드 및 워크로드를 모두 관리하거나 일부로 관리하는 Red Hat OpenShift Container Platform 클러스터입니다.

Ansible 소스

Ansible 노드 및 워크로드를 관리하는 Ansible 관리 솔루션입니다.

Red Hat Advanced Cluster Security for Kubernetes 소스

Kubernetes 환경을 보호하는 RHACS 보안 플랫폼 솔루션입니다.

네트워크 소스로 작업할 때 단일 소스 내에서 그룹화해야 하는 개별 자산 수를 결정합니다. 현재 네트워크 소스의 소스에 여러 자산을 추가할 수 있습니다. 다음 목록에는 소스를 추가할 때 고려해야 할 몇 가지 다른 요소가 포함되어 있습니다.

- 자산이 개발, 테스트 또는 프로덕션 환경의 일부인지 여부와 컴퓨팅 능력에 대한 요구와 유사한 우려가 해당 자산에 대한 고려 사항인지 여부.
- 설치된 소프트웨어로의 빈번한 변경과 같은 내부 비즈니스 관행을 위해 특정 엔티티 또는 엔티티 그룹을 더 자주 스캔할지 여부.

*인증 정보*에는 해당 소스에 포함된 자산의 전체 또는 일부에서 검사를 실행할 수 있는 충분한 권한이 있는 사용자의 사용자 이름 및 암호 또는 SSH 키와 같은 데이터가 포함되어 있습니다. 소스와 마찬가지로 인증 정보는 네트워크, vCenter, Satellite, OpenShift, Ansible 또는 RHACS 유형으로 구성됩니다. 일반적으로 네트워크 소스에는 광범위한 IP 범위의 모든 자산에 액세스하는 데 필요한 많은 인증 정보가 필요할 것으로 예상되므로 여러 네트워크 인증 정보가 필요할 수 있습니다. 반대로 vCenter 또는 satellite 소스는 일반적으로 단일 vCenter 또는 Satellite 인증 정보를 사용하여 특정 시스템 관리 솔루션 서버에 액세스하고 OpenShift, Ansible 또는 RHACS 소스를 사용하면 단일 클러스터에 액세스할 수 있습니다.

소스 뷰에서 새 소스를 추가하고 인증 정보 뷰에서 새 인증 정보를 추가할 수 있습니다. 소스 생성 중에 새로 인증 정보를 추가하거나 기존 인증 정보를 선택할 수도 있습니다. 소스 생성 중에 소스와 직접 인증 정보를 연결합니다. 소스 및 인증 정보에 일치하는 유형이 있어야 하므로 소스 생성 중에 추가한 모든 인증 정보는 소스와 동일한 유형을 공유합니다. 또한 소스 생성 중에 기존 인증 정보를 사용하려는 경우 사용 가능한 인증 정보 목록에는 동일한 유형의 인증 정보만 포함됩니다. 예를 들어, 네트워크 소스 생성 중에 선택 시 네트워크 인증 정보만 사용할 수 있습니다.

3.1.4. 네트워크 인증

Discovery 애플리케이션은 Ansible의 SSH 원격 연결 기능을 사용하여 네트워크 검사에서 원격 시스템을 검사합니다. 네트워크 인증 정보를 추가할 때 사용자 이름 및 암호 또는 사용자 이름 및 SSH 키 파일 쌍을 사용하여 SSH 연결을 구성합니다. SSH 키 인증을 사용하여 원격 시스템에 액세스하는 경우 SSH 키의 암호를 제공할 수도 있습니다.

네트워크 인증 정보 구성 중에도 become 메서드를 활성화할 수 있습니다. become 메서드는 권한 승격을 위해 검사 중에 사용됩니다. 이러한 승격된 권한은 명령을 실행하고 검사 중인 시스템에서 데이터를 얻으려면 필요합니다. 검사 중에 권한 승격이 필요하지 않고 명령에 대한 자세한 내용은 원격 네트워크 자산 스캔에 사용되는 명령을 참조하십시오.

3.1.4.1. 원격 네트워크 자산 검사에 사용되는 명령

네트워크 검사를 실행하는 경우 Discovery는 사용자가 제공한 인증 정보를 사용하여 네트워크의 원격 시스템에서 특정 명령을 실행해야 합니다. 이러한 명령 중 일부는 승격된 권한으로 실행해야 합니다. 이 액세스는 일반적으로 **sudo** 명령 또는 유사한 명령을 사용하여 검색됩니다. Discovery가 설치된 제품에 대한 보고서를 작성하는 데 사용하는 팩트 유형을 수집하려면 승격된 권한이 필요합니다.

승격된 권한 없이도 네트워크 소스 검사를 실행할 수 있지만 그렇게 검사하면 결과가 불완전합니다. 네트워크 검사 결과가 불완전하면 생성되는 검사 보고서의 품질에 영향을 줍니다.

다음 정보에는 네트워크 스캔 중에 Discovery가 원격 호스트에서 실행되는 명령이 나열되어 있습니다. 이 정보에는 승격된 권한 없이 실행할 수 있는 기본 명령과 보고서의 가장 정확하고 완전한 정보를 수집하기 위해 승격된 권한으로 실행해야 하는 명령이 포함됩니다.

참고

다음 명령 외에도 Discovery는 **bash** 쉘에서 제공하는 표준 쉘 기능에 따라 달라집니다.

3.1.4.1.1. 승격된 권한이 필요하지 않은 기본 명령

다음 명령에는 검사 중에 팩트를 수집하기 위해 승격된 권한이 필요하지 않습니다.

- cat
- egrep
- sort
- uname
- ctime
- grep
- rpm
- virsh
- date
- id
- test
- whereis
- echo
- sed
- tune2fs
- xargs

3.1.4.1.2. 승격된 권한이 필요한 명령

다음 명령에는 검사 중에 팩트를 수집하기 위해 승격된 권한이 필요합니다. 각 명령에는 검사 중에 Discovery가 검색하려고 시도하는 개별 팩트 또는 팩트 카테고리가 포함되어 있습니다. 이러한 팩트는 해당 명령에서 승격된 권한을 사용할 수 없는 경우 보고서에 포함될 수 없습니다.

- **awk**
- **cat**
- **chkconfig**
- **command**

- df
- dirname
- dmidecode
- echo
- egrep
- fgrep
- find
- ifconfig
- ip
- java
- locate
- ls
- ps
- readlink
- sed
- sort
- stat
- subscription-manager
- systemctl
- tail
- test
- tr
- unzip
- virt-what
- xargs
- yum

3.2. SATELLITE 소스 및 인증 정보 추가

Red Hat Satellite Server 배포에서 스캔을 실행하려면 검사할 Satellite Server 서버를 식별하는 소스를 추가해야 합니다. 그런 다음 해당 서버에 액세스하기 위해 인증 데이터가 포함된 인증 정보를 추가해야 합니다.

더 알아보기

Satellite Server 스캔에 필요한 정보를 제공하기 위해 Satellite 소스 및 인증 정보를 추가합니다. 자세한 내용은 다음 정보를 참조하십시오.

- Satellite 소스를 추가하려면 Satellite 소스 추가 를 참조하십시오.
- Satellite 인증 정보를 추가하려면 Satellite 인증 정보 추가 를 참조하십시오.

소스 및 인증 정보 및 Discovery가 이를 사용하는 방법에 대한 자세한 내용은 다음 정보를 참조하십시오.

- 소스 및 인증 정보

Satellite Server 서버에서 Discovery가 인증하는 방법에 대한 자세한 내용은 다음 정보를 참조하십시오. 이 정보에는 Satellite 인증 정보를 구성하는 동안 수행해야 하는 인증서 검증 및 SSL 통신 옵션에 대한 지침이 포함되어 있습니다.

- Satellite 서버 인증

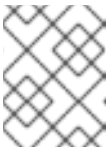
3.2.1. Satellite 소스 추가

초기 welcome 페이지 또는 소스 보기에서 소스를 추가할 수 있습니다.

프로세스

1. 위치를 기반으로 새 인증 정보를 추가하려면 옵션을 클릭합니다.
   - welcome 페이지에서 **소스 추가** 를 클릭합니다.
   - 소스 보기에서 **추가** 를 클릭합니다.

   소스 추가 마법사가 열립니다.
2. 유형 페이지에서 소스 유형으로 **Satellite** 를 선택하고 **다음**을 클릭합니다.
3. 인증 정보 페이지에서 다음 정보를 입력합니다.
   a. **이름** 필드에 설명이 포함된 이름을 입력합니다.
   b. **IP 주소 또는 호스트 이름** 필드에 이 소스의 Satellite 서버의 IP 주소 또는 호스트 이름을 입력합니다. 이 소스가 기본 포트 443에서 실행되도록 하려면 다른 포트를 입력합니다. 예를 들어 Satellite 서버의 IP 주소가 192.0.2.15이고 포트를 80으로 변경하려면 **192.0.2.15:80** 을 입력합니다.
   c. **인증 정보** 목록에서 이 소스의 Satellite 서버에 액세스하는 데 필요한 인증 정보를 선택합니다. 필요한 인증 정보가 없는 경우 **인증 정보 추가** 아이콘을 클릭하여 인증 정보 추가 마법사를 엽니다.
   d. **연결** 목록에서 이 소스를 검사하는 동안 보안 연결에 사용할 SSL 프로토콜을 선택합니다.



참고

Satellite Server는 SSL 비활성화를 지원하지 않습니다. **SSL 비활성화** 옵션을 선택하면 이 옵션이 무시됩니다.

e. 인증 기관에서 확인된 SSL 인증서를 확인하기 위해 Satellite 서버의 SSL 검증을 업그레이드해야 하는 경우 **Verify SSL Certificate** 확인란을 선택합니다.

4. **저장을** 클릭하여 소스를 저장한 다음 **닫기** 를 클릭하여 소스 추가 마법사를 종료합니다.

3.2.2. Satellite 인증 정보 추가

소스 생성 중에 인증 정보 보기 또는 소스 추가 마법사에서 인증 정보를 추가할 수 있습니다.

프로세스

1. 위치를 기반으로 새 인증 정보를 추가하려면 옵션을 클릭합니다.
   - 인증 정보 보기에서 **Satellite 인증 정보+추가** 를 클릭합니다.
   - 소스 추가 마법사에서 **인증 정보** 필드에 대한 **인증 정보 추가** 아이콘을 클릭합니다.

   인증 정보 추가 마법사가 열립니다.
2. **인증 정보 이름** 필드에 설명하는 이름을 입력합니다.
3. Satellite 서버 관리자의 사용자 이름과 암호를 입력합니다.
4. **저장**을 클릭하여 인증 정보를 저장하고 인증 정보 추가 마법사를 종료합니다.

3.2.3. 소스 및 인증 정보

검사를 실행하려면 소스 및 인증 정보 두 가지 기본 구조에 대한 데이터를 구성해야 합니다. 검사 중에 검사할 소스 유형에 따라 소스 및 인증 정보 구성에 필요한 데이터 유형이 결정됩니다.

소스에는 스캔 중에 검사할 단일 자산 또는 여러 자산 세트가 포함되어 있습니다. 다음 유형의 소스를 구성할 수 있습니다.

네트워크 소스

하나 이상의 물리적 시스템, 가상 시스템 또는 컨테이너 이러한 자산은 호스트 이름, IP 주소, IP 범위 또는 서브넷으로 표시할 수 있습니다.

vCenter 소스

IT 인프라의 전체 또는 일부를 관리하는 vCenter Server 시스템 관리 솔루션입니다.

Satellite 소스

IT 인프라의 전체 또는 일부를 관리하는 Satellite 시스템 관리 솔루션입니다.

Red Hat OpenShift 소스

Red Hat OpenShift Container Platform 노드 및 워크로드를 모두 관리하거나 일부로 관리하는 Red Hat OpenShift Container Platform 클러스터입니다.

Ansible 소스

Ansible 노드 및 워크로드를 관리하는 Ansible 관리 솔루션입니다.

Red Hat Advanced Cluster Security for Kubernetes 소스

Kubernetes 환경을 보호하는 RHACS 보안 플랫폼 솔루션입니다.

네트워크 소스로 작업할 때 단일 소스 내에서 그룹화해야 하는 개별 자산 수를 결정합니다. 현재 네트워크 소스의 소스에 여러 자산을 추가할 수 있습니다. 다음 목록에는 소스를 추가할 때 고려해야 할 몇 가지 다른 요소가 포함되어 있습니다.

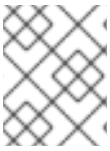
- 자산이 개발, 테스트 또는 프로덕션 환경의 일부인지 여부와 컴퓨팅 능력에 대한 요구와 유사한 우려가 해당 자산에 대한 고려 사항인지 여부.
- 설치된 소프트웨어로의 빈번한 변경과 같은 내부 비즈니스 관행을 위해 특정 엔티티 또는 엔티티 그룹을 더 자주 스캔할지 여부.

*인증 정보*에는 해당 소스에 포함된 자산의 전체 또는 일부에서 검사를 실행할 수 있는 충분한 권한이 있는 사용자의 사용자 이름 및 암호 또는 SSH 키와 같은 데이터가 포함되어 있습니다. 소스와 마찬가지로 인증 정보는 네트워크, vCenter, Satellite, OpenShift, Ansible 또는 RHACS 유형으로 구성됩니다. 일반적으로 네트워크 소스에는 광범위한 IP 범위의 모든 자산에 액세스하는 데 필요한 많은 인증 정보가 필요할 것으로 예상되므로 여러 네트워크 인증 정보가 필요할 수 있습니다. 반대로 vCenter 또는 satellite 소스는 일반적으로 단일 vCenter 또는 Satellite 인증 정보를 사용하여 특정 시스템 관리 솔루션 서버에 액세스하고 OpenShift, Ansible 또는 RHACS 소스를 사용하면 단일 클러스터에 액세스할 수 있습니다.

소스 뷰에서 새 소스를 추가하고 인증 정보 뷰에서 새 인증 정보를 추가할 수 있습니다. 소스 생성 중에 새로 인증 정보를 추가하거나 기존 인증 정보를 선택할 수도 있습니다. 소스 생성 중에 소스와 직접 인증 정보를 연결합니다. 소스 및 인증 정보에 일치하는 유형이 있어야 하므로 소스 생성 중에 추가한 모든 인증 정보는 소스와 동일한 유형을 공유합니다. 또한 소스 생성 중에 기존 인증 정보를 사용하려는 경우 사용 가능한 인증 정보 목록에는 동일한 유형의 인증 정보만 포함됩니다. 예를 들어, 네트워크 소스 생성 중에 선택 시 네트워크 인증 정보만 사용할 수 있습니다.

3.2.4. Satellite 서버 인증

Satellite 스캔의 경우 Satellite Server에 대한 연결 및 액세스는 HTTPS를 통해 암호화된 기본 인증(사용자 이름 및 암호)에서 파생됩니다. 기본적으로 Satellite 스캔은 SSL(Secure Sockets Layer) 프로토콜을 통해 인증서 검증 및 보안 통신으로 실행됩니다. 소스 생성 중에 인증서 검증 및 보안 통신에 사용할 여러 다른 SSL 및 TLS(Transport Layer Security) 프로토콜을 선택할 수 있습니다.



참고

Satellite 스캔에 사용하는 Satellite Server 인증 정보는 호스트, 서브스크립션 및 조직에 대한 보기 권한이 포함된 역할이어야 합니다.

스캔 중에 Satellite 서버에 올바르게 연결하도록 인증서 검증 수준을 조정해야 할 수 있습니다. 예를 들어 Satellite 서버는 인증 기관의 확인된 SSL 인증서를 사용할 수 있습니다. 소스 생성 중에 SSL 인증서 검증을 업그레이드하여 해당 소스를 검사하는 동안 해당 인증서를 확인할 수 있습니다. 반대로 Satellite 서버에서 자체 서명된 인증서를 사용할 수 있습니다. 소스 생성 중에 해당 소스의 검사에서 인증서를 확인하지 않도록 SSL 검증을 기본값으로 유지할 수 있습니다. 이 옵션을 선택한 경우 자체 서명된 인증서의 기본값을 그대로 두려면 검사 오류가 발생하지 않을 수 있습니다.

SSL을 비활성화하는 옵션은 현재 인터페이스에서 사용할 수 있지만 Satellite Server는 SSL 비활성화를 지원하지 않습니다. Satellite 소스를 생성할 때 **SSL 비활성화** 옵션을 선택하면 이 옵션이 무시됩니다.

3.3. VCENTER 소스 및 인증 정보 추가

vCenter Server 배포에서 검사를 실행하려면 검사할 vCenter Server 서버를 식별하는 소스를 추가해야 합니다. 그런 다음 해당 서버에 액세스하기 위해 인증 데이터가 포함된 인증 정보를 추가해야 합니다.

더 알아보기

vcenter 소스 및 인증 정보를 추가하여 vCenter Server 스캔에 필요한 정보를 제공합니다. 자세한 내용은 다음 정보를 참조하십시오.

- vcenter 소스를 추가하려면 vcenter 소스 추가를 참조하십시오.

- vcenter 인증 정보를 추가하려면 vcenter 인증 정보 추가를 참조하십시오.

소스 및 인증 정보 및 Discovery가 이를 사용하는 방법에 대한 자세한 내용은 다음 정보를 참조하십시오.

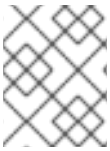
- 소스 및 인증 정보

vCenter Server 서버에서 Discovery가 인증하는 방법에 대한 자세한 내용은 다음 정보를 참조하십시오. 이 정보에는 vcenter 인증 정보를 구성하는 동안 수행해야 하는 인증서 검증 및 SSL 통신 옵션에 대한 지침이 포함되어 있습니다

- vCenter Server 인증

3.3.1. vcenter 소스 추가

초기 welcome 페이지 또는 소스 보기에서 소스를 추가할 수 있습니다.



참고

vCenter 소스는 vCenter 배포와만 호환됩니다. 이 소스를 사용하여 Red Hat에서 지원하는 다른 가상화 인프라도 스캔할 수 없습니다.

프로세스

1. 위치를 기반으로 새 인증 정보를 추가하려면 옵션을 클릭합니다.
   - welcome 페이지에서 **소스 추가** 를 클릭합니다.
   - 소스 보기에서 **추가** 를 클릭합니다.

   소스 추가 마법사가 열립니다.
2. 유형 페이지에서 소스 유형으로 **vCenter Server** 를 선택하고 **다음**을 클릭합니다.
3. 인증 정보 페이지에서 다음 정보를 입력합니다.
   a. **이름** 필드에 설명이 포함된 이름을 입력합니다.
   b. **IP 주소 또는 호스트 이름** 필드에 이 소스에 대한 vCenter Server의 IP 주소 또는 호스트 이름을 입력합니다. 이 소스가 기본 포트 443에서 실행되도록 하려면 다른 포트를 입력합니다. 예를 들어 vCenter Server의 IP 주소가 192.0.2.15이고 포트를 80으로 변경하려면 **192.0.2.15:80** 을 입력합니다.
   c. **인증 정보** 목록에서 이 소스의 vCenter Server에 액세스하는 데 필요한 인증 정보를 선택합니다. 필요한 인증 정보가 없는 경우 **인증 정보 추가** 아이콘을 클릭하여 인증 정보 추가 마법사를 엽니다.
   d. **연결** 목록에서 이 소스를 검사하는 동안 보안 연결에 사용할 SSL 프로토콜을 선택합니다. 이 소스를 검사하는 동안 보안 통신을 비활성화하려면 **SSL 비활성화** 를 선택합니다.
   e. 인증 기관에서 확인된 SSL 인증서를 확인하기 위해 vCenter Server에 대한 SSL 검증을 업그레이드해야 하는 경우 **Verify SSL Certificate** 확인란을 선택합니다.
4. **저장을** 클릭하여 소스를 저장한 다음 **닫기** 를 클릭하여 소스 추가 마법사를 종료합니다.

3.3.2. vcenter 인증 정보 추가

소스 생성 중에 인증 정보 보기 또는 소스 추가 마법사에서 인증 정보를 추가할 수 있습니다.

프로세스

1. 위치를 기반으로 새 인증 정보를 추가하려면 옵션을 클릭합니다.
   - 인증 정보 보기에서 **VCenter 인증정보+추가** 를 클릭합니다.
   - 소스 추가 마법사에서 **인증 정보** 필드에 대한 **인증 정보 추가** 아이콘을 클릭합니다.

   인증 정보 추가 마법사가 열립니다.
2. **인증 정보 이름** 필드에 설명하는 이름을 입력합니다.
3. vCenter Server 관리자의 사용자 이름과 암호를 입력합니다.
4. **저장**을 클릭하여 인증 정보를 저장하고 인증 정보 추가 마법사를 종료합니다.

3.3.3. 소스 및 인증 정보

검사를 실행하려면 소스 및 인증 정보 두 가지 기본 구조에 대한 데이터를 구성해야 합니다. 검사 중에 검사할 소스 유형에 따라 소스 및 인증 정보 구성에 필요한 데이터 유형이 결정됩니다.

소스에는 스캔 중에 검사할 단일 자산 또는 여러 자산 세트가 포함되어 있습니다. 다음 유형의 소스를 구성할 수 있습니다.

네트워크 소스

하나 이상의 물리적 시스템, 가상 시스템 또는 컨테이너 이러한 자산은 호스트 이름, IP 주소, IP 범위 또는 서브넷으로 표시할 수 있습니다.

vCenter 소스

IT 인프라의 전체 또는 일부를 관리하는 vCenter Server 시스템 관리 솔루션입니다.

Satellite 소스

IT 인프라의 전체 또는 일부를 관리하는 Satellite 시스템 관리 솔루션입니다.

Red Hat OpenShift 소스

Red Hat OpenShift Container Platform 노드 및 워크로드를 모두 관리하거나 일부로 관리하는 Red Hat OpenShift Container Platform 클러스터입니다.

Ansible 소스

Ansible 노드 및 워크로드를 관리하는 Ansible 관리 솔루션입니다.

Red Hat Advanced Cluster Security for Kubernetes 소스

Kubernetes 환경을 보호하는 RHACS 보안 플랫폼 솔루션입니다.

네트워크 소스로 작업할 때 단일 소스 내에서 그룹화해야 하는 개별 자산 수를 결정합니다. 현재 네트워크 소스의 소스에 여러 자산을 추가할 수 있습니다. 다음 목록에는 소스를 추가할 때 고려해야 할 몇 가지 다른 요소가 포함되어 있습니다.

- 자산이 개발, 테스트 또는 프로덕션 환경의 일부인지 여부와 컴퓨팅 능력에 대한 요구와 유사한 우려가 해당 자산에 대한 고려 사항인지 여부.
- 설치된 소프트웨어로의 빈번한 변경과 같은 내부 비즈니스 관행을 위해 특정 엔티티 또는 엔티티 그룹을 더 자주 스캔할지 여부.

*인증 정보*에는 해당 소스에 포함된 자산의 전체 또는 일부에서 검사를 실행할 수 있는 충분한 권한이 있는 사용자의 사용자 이름 및 암호 또는 SSH 키와 같은 데이터가 포함되어 있습니다. 소스와 마찬가지로 인증

정보는 네트워크, vCenter, Satellite, OpenShift, Ansible 또는 RHACS 유형으로 구성됩니다. 일반적으로 네트워크 소스에는 광범위한 IP 범위의 모든 자산에 액세스하는 데 필요한 많은 인증 정보가 필요할 것으로 예상되므로 여러 네트워크 인증 정보가 필요할 수 있습니다. 반대로 vCenter 또는 satellite 소스는 일반적으로 단일 vCenter 또는 Satellite 인증 정보를 사용하여 특정 시스템 관리 솔루션 서버에 액세스하고 OpenShift, Ansible 또는 RHACS 소스를 사용하면 단일 클러스터에 액세스할 수 있습니다.

소스 뷰에서 새 소스를 추가하고 인증 정보 뷰에서 새 인증 정보를 추가할 수 있습니다. 소스 생성 중에 새로 인증 정보를 추가하거나 기존 인증 정보를 선택할 수도 있습니다. 소스 생성 중에 소스와 직접 인증 정보를 연결합니다. 소스 및 인증 정보에 일치하는 유형이 있어야 하므로 소스 생성 중에 추가한 모든 인증 정보는 소스와 동일한 유형을 공유합니다. 또한 소스 생성 중에 기존 인증 정보를 사용하려는 경우 사용 가능한 인증 정보 목록에는 동일한 유형의 인증 정보만 포함됩니다. 예를 들어, 네트워크 소스 생성 중에 선택 시 네트워크 인증 정보만 사용할 수 있습니다.

3.3.4. vCenter Server 인증

vCenter 검사의 경우 vCenter Server에 대한 연결과 액세스는 HTTPS를 통해 암호화된 기본 인증(사용자 이름 및 암호)에서 파생됩니다. 기본적으로 vCenter 검사는 SSL(Secure Sockets Layer) 프로토콜을 통해 인증서 검증 및 보안 통신으로 실행됩니다. 소스 생성 중에 인증서 검증 및 보안 통신에 사용할 여러 다른 SSL 및 TLS(Transport Layer Security) 프로토콜을 선택할 수 있습니다.

검사 중에 vCenter 서버에 올바르게 연결하도록 인증서 검증 수준을 조정해야 할 수 있습니다. 예를 들어 vCenter 서버는 인증 기관의 확인된 SSL 인증서를 사용할 수 있습니다. 소스 생성 중에 SSL 인증서 검증을 업그레이드하여 해당 소스를 검사하는 동안 해당 인증서를 확인할 수 있습니다. 반대로 vCenter 서버에서 자체 서명된 인증서를 사용할 수 있습니다. 소스 생성 중에 소스 검사에서 인증서를 확인하지 않도록 SSL 검증을 기본값으로 유지할 수 있습니다. 이 옵션을 선택한 경우 자체 서명된 인증서의 기본값을 그대로 두려면 검사 오류가 발생하지 않을 수 있습니다.

vCenter 서버가 웹 애플리케이션에 SSL 통신을 사용하도록 구성되지 않은 경우 검사 중에 SSL을 보안 통신 방법으로 비활성화해야 할 수도 있습니다. 예를 들어 vCenter 서버는 포트 80과 HTTP를 사용하여 웹 애플리케이션과 통신하도록 구성할 수 있습니다. 이 경우 소스 생성 중에 해당 소스의 검사에 대한 SSL 통신을 비활성화할 수 있습니다.

3.4. OPENSHIFT 소스 및 인증 정보 추가

Red Hat OpenShift Container Platform 배포에서 검사를 실행하려면 검사할 Red Hat OpenShift Container Platform 클러스터를 식별하는 소스를 추가해야 합니다. 그런 다음 해당 클러스터에 액세스하려면 인증 데이터가 포함된 인증 정보를 추가해야 합니다.

더 알아보기

Red Hat OpenShift Container Platform 클러스터를 검사하는 데 필요한 정보를 제공하기 위해 OpenShift 소스 및 인증 정보를 추가합니다. 자세한 내용은 다음 정보를 참조하십시오.

- OpenShift 소스를 추가하려면 OpenShift 소스 추가를 참조하십시오.
- OpenShift 인증 정보를 추가하려면 OpenShift 인증 정보 추가를 참조하십시오.

소스 및 인증 정보 및 Discovery가 이를 사용하는 방법에 대한 자세한 내용은 다음 정보를 참조하십시오.

- 소스 및 인증 정보

Red Hat OpenShift Container Platform 클러스터에서 Discovery가 인증하는 방법에 대한 자세한 내용은 다음 정보를 참조하십시오. 이 정보에는 OpenShift 인증 정보를 구성하는 동안 수행해야 하는 인증서 검증 및 SSL 통신 옵션에 대한 지침이 포함되어 있습니다.

- Red Hat OpenShift Container Platform 인증

3.4.1. Red Hat OpenShift Container Platform 소스 추가

초기 welcome 페이지 또는 소스 보기에서 소스를 추가할 수 있습니다.

사전 요구 사항

- API 주소와 토큰 값을 얻으려면 Red Hat OpenShift Container Platform 웹 콘솔 관리자 화면에 액세스해야 합니다.

프로세스

1. 위치를 기반으로 새 인증 정보를 추가하려면 옵션을 클릭합니다.
   - welcome 페이지에서 **소스 추가** 를 클릭합니다.
   - 소스 보기에서 **추가** 를 클릭합니다.

   소스 추가 마법사가 열립니다.
2. 유형 페이지에서 소스 유형으로 **OpenShift** 를 선택하고 **다음을** 클릭합니다.
3. 인증 정보 페이지에서 다음 정보를 입력합니다.
   a. **이름** 필드에 설명이 포함된 이름을 입력합니다.
   b. **IP 주소 또는 호스트 이름** 필드에 이 소스의 Red Hat OpenShift Container Platform 클러스터 API 주소를 입력합니다. 웹 콘솔에서 클러스터의 개요 세부 정보를 확인하여 클러스터 API 주소를 찾을 수 있습니다.
   c. **인증 정보** 목록에서 이 소스의 클러스터에 액세스하는 데 필요한 인증 정보를 선택합니다. 필요한 인증 정보가 없는 경우 **인증 정보 추가** 아이콘을 클릭하여 인증 정보 추가 마법사를 엽니다.
   d. **연결** 목록에서 이 소스를 검사하는 동안 보안 연결에 사용할 SSL 프로토콜을 선택합니다. 이 소스를 검사하는 동안 보안 통신을 비활성화하려면 **SSL 비활성화** 를 선택합니다.
   e. 인증 기관에서 확인된 SSL 인증서를 확인하기 위해 클러스터의 SSL 검증을 업그레이드해야 하는 경우 **Verify SSL Certificate** 확인란을 선택합니다.
4. **저장을** 클릭하여 소스를 저장한 다음 **닫기** 를 클릭하여 소스 추가 마법사를 종료합니다.

3.4.2. Red Hat OpenShift Container Platform 인증 정보 추가

소스 생성 중에 인증 정보 보기 또는 소스 추가 마법사에서 인증 정보를 추가할 수 있습니다.

사전 요구 사항

- API 주소와 토큰 값을 얻으려면 Red Hat OpenShift Container Platform 웹 콘솔 관리자 화면에 액세스해야 합니다.

프로세스

1. 위치를 기반으로 새 인증 정보를 추가하려면 옵션을 클릭합니다.
   - 인증 정보 보기에서 **OpenShift+추가** 를 클릭합니다.

- 소스 추가 마법사에서 **인증 정보** 필드에 대한 **인증 정보 추가** 아이콘을 클릭합니다.

인증 정보 추가 마법사가 열립니다.

2. **인증 정보 이름** 필드에 설명하는 이름을 입력합니다.

3. 관리자 콘솔에서 Red Hat OpenShift Container Platform 클러스터의 API 토큰을 입력합니다. 콘솔에서 사용자 이름을 클릭하고 토큰 **표시** 옵션을 클릭하고 API 토큰에 표시된 값을 복사하여 **API 토큰** 을 찾을 수 있습니다.

4. **저장**을 클릭하여 인증 정보를 저장하고 인증 정보 추가 마법사를 종료합니다.

3.4.3. 소스 및 인증 정보

검사를 실행하려면 소스 및 인증 정보 두 가지 기본 구조에 대한 데이터를 구성해야 합니다. 검사 중에 검사할 소스 유형에 따라 소스 및 인증 정보 구성에 필요한 데이터 유형이 결정됩니다.

소스에는 스캔 중에 검사할 단일 자산 또는 여러 자산 세트가 포함되어 있습니다. 다음 유형의 소스를 구성할 수 있습니다.

네트워크 소스

하나 이상의 물리적 시스템, 가상 시스템 또는 컨테이너 이러한 자산은 호스트 이름, IP 주소, IP 범위 또는 서브넷으로 표시할 수 있습니다.

vCenter 소스

IT 인프라의 전체 또는 일부를 관리하는 vCenter Server 시스템 관리 솔루션입니다.

Satellite 소스

IT 인프라의 전체 또는 일부를 관리하는 Satellite 시스템 관리 솔루션입니다.

Red Hat OpenShift 소스

Red Hat OpenShift Container Platform 노드 및 워크로드를 모두 관리하거나 일부로 관리하는 Red Hat OpenShift Container Platform 클러스터입니다.

Ansible 소스

Ansible 노드 및 워크로드를 관리하는 Ansible 관리 솔루션입니다.

Red Hat Advanced Cluster Security for Kubernetes 소스

Kubernetes 환경을 보호하는 RHACS 보안 플랫폼 솔루션입니다.

네트워크 소스로 작업할 때 단일 소스 내에서 그룹화해야 하는 개별 자산 수를 결정합니다. 현재 네트워크 소스의 소스에 여러 자산을 추가할 수 있습니다. 다음 목록에는 소스를 추가할 때 고려해야 할 몇 가지 다른 요소가 포함되어 있습니다.

- 자산이 개발, 테스트 또는 프로덕션 환경의 일부인지 여부와 컴퓨팅 능력에 대한 요구와 유사한 우려가 해당 자산에 대한 고려 사항인지 여부.

- 설치된 소프트웨어로의 빈번한 변경과 같은 내부 비즈니스 관행을 위해 특정 엔티티 또는 엔티티 그룹을 더 자주 스캔할지 여부.

*인증 정보*에는 해당 소스에 포함된 자산의 전체 또는 일부에서 검사를 실행할 수 있는 충분한 권한이 있는 사용자의 사용자 이름 및 암호 또는 SSH 키와 같은 데이터가 포함되어 있습니다. 소스와 마찬가지로 인증 정보는 네트워크, vCenter, Satellite, OpenShift, Ansible 또는 RHACS 유형으로 구성됩니다. 일반적으로 네트워크 소스에는 광범위한 IP 범위의 모든 자산에 액세스하는 데 필요한 많은 인증 정보가 필요할 것으로 예상되므로 여러 네트워크 인증 정보가 필요할 수 있습니다. 반대로 vCenter 또는 satellite 소스는 일반적으로 단일 vCenter 또는 Satellite 인증 정보를 사용하여 특정 시스템 관리 솔루션 서버에 액세스하고 OpenShift, Ansible 또는 RHACS 소스를 사용하면 단일 클러스터에 액세스할 수 있습니다.

소스 뷰에서 새 소스를 추가하고 인증 정보 뷰에서 새 인증 정보를 추가할 수 있습니다. 소스 생성 중에 새로 인증 정보를 추가하거나 기존 인증 정보를 선택할 수도 있습니다. 소스 생성 중에 소스와 직접 인증 정보를 연결합니다. 소스 및 인증 정보에 일치하는 유형이 있어야 하므로 소스 생성 중에 추가한 모든 인증 정보는 소스와 동일한 유형을 공유합니다. 또한 소스 생성 중에 기존 인증 정보를 사용하려는 경우 사용 가능한 인증 정보 목록에는 동일한 유형의 인증 정보만 포함됩니다. 예를 들어, 네트워크 소스 생성 중에 선택 시 네트워크 인증 정보만 사용할 수 있습니다.

3.4.4. Red Hat OpenShift Container Platform 인증

OpenShift 검사의 경우 OpenShift 클러스터 API 주소에 대한 연결 및 액세스는 클러스터 API 주소와 HTTPS를 통해 암호화된 API 토큰을 사용하여 기본 인증에서 파생됩니다. 기본적으로 OpenShift 검사는 SSL(Secure Sockets Layer) 프로토콜을 통해 인증서 검증 및 보안 통신으로 실행됩니다. 소스 생성 중에 인증서 검증 및 보안 통신에 사용할 여러 다른 SSL 및 TLS(Transport Layer Security) 프로토콜을 선택할 수 있습니다.

검사 중에 Red Hat OpenShift Container Platform 클러스터 API 주소에 올바르게 연결하도록 인증서 검증 수준을 조정해야 할 수 있습니다. 예를 들어 OpenShift 클러스터 API 주소는 인증 기관의 확인된 SSL 인증서를 사용할 수 있습니다. 소스 생성 중에 SSL 인증서 검증을 업그레이드하여 해당 소스를 검사하는 동안 해당 인증서를 확인할 수 있습니다. 반대로 클러스터 API 주소가 자체 서명된 인증서를 사용할 수 있습니다. 소스 생성 중에 소스 검사에서 인증서를 확인하지 않도록 SSL 검증을 기본값으로 유지할 수 있습니다. 이 옵션을 선택한 경우 자체 서명된 인증서의 기본값을 그대로 두려면 검사 오류가 발생하지 않을 수 있습니다.

OpenShift 클러스터 API 주소가 웹 애플리케이션에 SSL 통신을 사용하도록 구성되지 않은 경우 스캔 중에 SSL을 보안 통신 방법으로 비활성화해야 할 수도 있습니다. 예를 들어 HTTP와 포트 80을 사용하여 웹 애플리케이션과 통신하도록 OpenShift 서버를 구성할 수 있습니다. 이 경우 소스 생성 중에 해당 소스의 검사에 대한 SSL 통신을 비활성화할 수 있습니다.

3.5. ANSIBLE 소스 및 인증 정보 추가

Ansible 배포에서 검사를 실행하려면 검사할 Ansible Automation Platform을 식별하는 소스를 추가해야 합니다. 그런 다음 해당 클러스터에 액세스하기 위해 인증 데이터가 포함된 인증 정보를 추가해야 합니다.

더 알아보기

Ansible 소스 및 인증 정보를 추가하여 Ansible Automation Platform 배포를 검사하는 데 필요한 정보를 제공합니다. 자세한 내용은 다음 정보를 참조하십시오.

- Ansible 소스를 추가하려면 Ansible 소스 추가를 참조하십시오.
- Ansible 인증 정보를 추가하려면 Ansible 인증 정보 추가를 참조하십시오.

소스 및 인증 정보 및 Discovery가 이를 사용하는 방법에 대한 자세한 내용은 다음 정보를 참조하십시오.

- 소스 및 인증 정보

Ansible 배포를 통해 Discovery가 인증하는 방법에 대한 자세한 내용은 다음 정보를 참조하십시오. 이 정보에는 Ansible 인증 정보 구성 중에 수행해야 할 수 있는 인증서 검증 및 SSL 통신 옵션에 대한 지침이 포함되어 있습니다.

- Ansible Automation Platform

3.5.1. Red Hat Ansible Automation Platform 소스 추가

초기 welcome 페이지 또는 소스 보기에서 소스를 추가할 수 있습니다.

프로세스

1. 위치를 기반으로 새 인증 정보를 추가하려면 옵션을 클릭합니다.
   - welcome 페이지에서 **소스 추가** 를 클릭합니다.
   - 소스 보기에서 **소스 추가**를 클릭합니다.

   소스 추가 마법사가 열립니다.
2. 유형 페이지에서 소스 유형으로 **Ansible Controller** 를 선택하고 **다음을** 클릭합니다.
3. 인증 정보 페이지에서 다음 정보를 입력합니다.
   a. **이름** 필드에 설명이 포함된 이름을 입력합니다.
   b. **IP 주소 또는 호스트 이름** 필드에 이 소스의 Ansible 호스트 IP 주소를 입력합니다. 포털에서 컨트롤러의 개요 세부 정보를 확인하여 호스트 IP 주소를 찾을 수 있습니다.
   c. **인증 정보** 목록에서 이 소스의 클러스터에 액세스하는 데 필요한 인증 정보를 선택합니다. 필요한 인증 정보가 없는 경우 **인증 정보 추가** 아이콘을 클릭하여 인증 정보 추가 마법사를 엽니다.
   d. **연결** 목록에서 이 소스를 검사하는 동안 보안 연결에 사용할 SSL 프로토콜을 선택합니다. 이 소스를 검사하는 동안 보안 통신을 비활성화하려면 **SSL 비활성화** 를 선택합니다.
   e. 인증 기관에서 확인된 SSL 인증서를 확인하기 위해 클러스터의 SSL 검증을 업그레이드해야 하는 경우 **Verify SSL Certificate** 확인란을 선택합니다.
4. **저장을** 클릭하여 소스를 저장한 다음 **닫기** 를 클릭하여 소스 추가 마법사를 종료합니다.

3.5.2. Red Hat Ansible Automation Platform 인증 정보 추가

소스 생성 중에 인증 정보 보기 또는 소스 추가 마법사에서 인증 정보를 추가할 수 있습니다.

프로세스

1. 위치를 기반으로 새 인증 정보를 추가하려면 옵션을 클릭합니다.
   - 인증 정보 보기에서 **Ansible 인증 정보+추가** 를 클릭합니다.
   - 소스 추가 마법사에서 **인증 정보** 필드에 대한 **인증 정보 추가** 아이콘을 클릭합니다.

   인증 정보 추가 마법사가 열립니다.
2. **인증 정보 이름** 필드에 설명하는 이름을 입력합니다.
3. **사용자 이름** 필드에 Ansible 컨트롤러 인스턴스의 사용자 이름을 입력합니다.
4. **암호** 필드에 Ansible Controller 인스턴스의 암호를 입력합니다.
5. **저장을** 클릭하여 인증 정보를 저장합니다. 인증 정보 추가 마법사가 종료됩니다.

3.5.3. 소스 및 인증 정보

검사를 실행하려면 소스 및 인증 정보 두 가지 기본 구조에 대한 데이터를 구성해야 합니다. 검사 중에 검사할 소스 유형에 따라 소스 및 인증 정보 구성에 필요한 데이터 유형이 결정됩니다.

소스에는 스캔 중에 검사할 단일 자산 또는 여러 자산 세트가 포함되어 있습니다. 다음 유형의 소스를 구성할 수 있습니다.

네트워크 소스

하나 이상의 물리적 시스템, 가상 시스템 또는 컨테이너 이러한 자산은 호스트 이름, IP 주소, IP 범위 또는 서브넷으로 표시할 수 있습니다.

vCenter 소스

IT 인프라의 전체 또는 일부를 관리하는 vCenter Server 시스템 관리 솔루션입니다.

Satellite 소스

IT 인프라의 전체 또는 일부를 관리하는 Satellite 시스템 관리 솔루션입니다.

Red Hat OpenShift 소스

Red Hat OpenShift Container Platform 노드 및 워크로드를 모두 관리하거나 일부로 관리하는 Red Hat OpenShift Container Platform 클러스터입니다.

Ansible 소스

Ansible 노드 및 워크로드를 관리하는 Ansible 관리 솔루션입니다.

Red Hat Advanced Cluster Security for Kubernetes 소스

Kubernetes 환경을 보호하는 RHACS 보안 플랫폼 솔루션입니다.

네트워크 소스로 작업할 때 단일 소스 내에서 그룹화해야 하는 개별 자산 수를 결정합니다. 현재 네트워크 소스의 소스에 여러 자산을 추가할 수 있습니다. 다음 목록에는 소스를 추가할 때 고려해야 할 몇 가지 다른 요소가 포함되어 있습니다.

- 자산이 개발, 테스트 또는 프로덕션 환경의 일부인지 여부와 컴퓨팅 능력에 대한 요구와 유사한 우려가 해당 자산에 대한 고려 사항인지 여부.
- 설치된 소프트웨어로의 빈번한 변경과 같은 내부 비즈니스 관행을 위해 특정 엔티티 또는 엔티티 그룹을 더 자주 스캔할지 여부.

*인증 정보*에는 해당 소스에 포함된 자산의 전체 또는 일부에서 검사를 실행할 수 있는 충분한 권한이 있는 사용자의 사용자 이름 및 암호 또는 SSH 키와 같은 데이터가 포함되어 있습니다. 소스와 마찬가지로 인증 정보는 네트워크, vCenter, Satellite, OpenShift, Ansible 또는 RHACS 유형으로 구성됩니다. 일반적으로 네트워크 소스에는 광범위한 IP 범위의 모든 자산에 액세스하는 데 필요한 많은 인증 정보가 필요할 것으로 예상되므로 여러 네트워크 인증 정보가 필요할 수 있습니다. 반대로 vCenter 또는 satellite 소스는 일반적으로 단일 vCenter 또는 Satellite 인증 정보를 사용하여 특정 시스템 관리 솔루션 서버에 액세스하고 OpenShift, Ansible 또는 RHACS 소스를 사용하면 단일 클러스터에 액세스할 수 있습니다.

소스 뷰에서 새 소스를 추가하고 인증 정보 뷰에서 새 인증 정보를 추가할 수 있습니다. 소스 생성 중에 새로 인증 정보를 추가하거나 기존 인증 정보를 선택할 수도 있습니다. 소스 생성 중에 소스와 직접 인증 정보를 연결합니다. 소스 및 인증 정보에 일치하는 유형이 있어야 하므로 소스 생성 중에 추가한 모든 인증 정보는 소스와 동일한 유형을 공유합니다. 또한 소스 생성 중에 기존 인증 정보를 사용하려는 경우 사용 가능한 인증 정보 목록에는 동일한 유형의 인증 정보만 포함됩니다. 예를 들어, 네트워크 소스 생성 중에 선택 시 네트워크 인증 정보만 사용할 수 있습니다.

3.5.4. Ansible 인증

Ansible 스캔의 경우 Ansible 호스트 IP 주소에 대한 연결 및 액세스는 호스트 IP 주소와 HTTPS를 통해 암호화된 암호를 사용하여 기본 인증에서 파생됩니다. 기본적으로 Ansible 스캔은 SSL(Secure Sockets Layer) 프로토콜을 통해 인증서 검증 및 보안 통신으로 실행됩니다. 소스 생성 중에 인증서 검증 및 보안 통신에 사용할 여러 다른 SSL 및 TLS(Transport Layer Security) 프로토콜을 선택할 수 있습니다.

스캔 중에 Ansible 호스트 IP 주소에 올바르게 연결하도록 인증서 검증 수준을 조정해야 할 수 있습니다. 예를 들어 Ansible 호스트 Ip 주소는 인증 기관의 확인된 SSL 인증서를 사용할 수 있습니다. 소스 생성 중

에 SSL 인증서 검증을 업그레이드하여 해당 소스를 검사하는 동안 해당 인증서를 확인할 수 있습니다. 반대로 호스트 IP 주소는 자체 서명된 인증서를 사용할 수 있습니다. 소스 생성 중에 소스 검사에서 인증서를 확인하지 않도록 SSL 검증을 기본값으로 유지할 수 있습니다. 이 옵션을 선택한 경우 자체 서명된 인증서의 기본값을 그대로 두려면 검사 오류가 발생하지 않을 수 있습니다.

Ansible 호스트 IP 주소가 웹 애플리케이션에 SSL 통신을 사용하도록 구성되지 않은 경우 스캔 중에 SSL을 보안 통신 방법으로 비활성화해야 할 수도 있습니다. 예를 들어 포트 80에서 HTTP를 사용하여 웹 애플리케이션과 통신하도록 Ansible 호스트 IP 주소를 구성할 수 있습니다. 이 경우 소스 생성 중에 해당 소스의 검사에 대한 SSL 통신을 비활성화할 수 있습니다.

3.6. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 소스 및 인증 정보 추가

RHACS(Red Hat Advanced Cluster Security for Kubernetes) 배포에서 검사를 실행하려면 검사할 RHACS 인스턴스를 식별하는 소스를 추가해야 합니다. 그런 다음 해당 인스턴스에 액세스하려면 인증 데이터가 포함된 인증 정보를 추가해야 합니다.

더 알아보기

RHACS 소스 및 인증 정보를 추가하여 RHACS 인스턴스를 검사하는 데 필요한 정보를 제공합니다. 자세한 내용은 다음 정보를 참조하십시오.

- RHACS 소스를 추가하려면 RHACS 소스 추가를 참조하십시오.
- RHACS 인증 정보를 추가하려면 RHACS 인증 정보 추가를 참조하십시오.

소스 및 인증 정보 및 Discovery가 이를 사용하는 방법에 대한 자세한 내용은 다음 정보를 참조하십시오.

- 소스 및 인증 정보

Red Hat Advanced Cluster Security for Kubernetes 인스턴스에서 Discovery가 인증하는 방법에 대한 자세한 내용은 다음 정보를 참조하십시오. 이 정보에는 RHACS 인증 정보 구성 중에 수행해야 할 수 있는 인증서 검증 및 SSL 통신 옵션에 대한 지침이 포함되어 있습니다.

- Red Hat Advanced Cluster Security for Kubernetes

3.6.1. Red Hat Advanced Cluster Security for Kubernetes 소스 추가

초기 welcome 페이지 또는 소스 보기에서 소스를 추가할 수 있습니다.

사전 요구 사항

- 관리 API 토큰 값을 생성하려면 RHACS(Red Hat Advanced Cluster Security for Kubernetes) 포털에 액세스할 수 있어야 합니다.
- RHACS 중앙 끝점을 찾으려면 RHACS 포털에 액세스하거나 RHACS 구성 관리 클라우드 서비스 인스턴스 세부 정보에 액세스해야 합니다.

프로세스

1. 위치를 기반으로 새 인증 정보를 추가하려면 옵션을 클릭합니다.
   - welcome 페이지에서 **소스 추가** 를 클릭합니다.
   - 소스 보기에서 **추가** 를 클릭합니다.

소스 추가 마법사가 열립니다.

2. 유형 페이지에서 소스 유형으로 **RHACS** 를 선택하고 **다음을** 클릭합니다.

3. 인증 정보 페이지에서 다음 정보를 입력합니다.

   a. **이름** 필드에 설명이 포함된 이름을 입력합니다.

   b. **IP 주소 또는 호스트 이름** 필드에 이 소스의 Red Hat Advanced Cluster Security for Kubernetes Central 주소를 입력합니다.

      - RHACS가 OpenShift에 배포된 경우 클러스터의 네트워크 경로를 확인하여 주소를 찾을 수 있습니다.

      - RHACS가 클라우드에 배포된 경우 인스턴스 세부 정보에서 이 정보를 찾을 수 있습니다.

   c. **인증 정보** 목록에서 이 소스의 클러스터에 액세스하는 데 필요한 인증 정보를 선택합니다. 필요한 인증 정보가 없는 경우 **인증 정보 추가** 아이콘을 클릭하여 인증 정보 추가 마법사를 엽니다.

   d. **연결** 목록에서 이 소스를 검사하는 동안 보안 연결에 사용할 SSL 프로토콜을 선택합니다. 이 소스를 검사하는 동안 보안 통신을 비활성화하려면 **SSL 비활성화** 를 선택합니다.

   e. 인증 기관에서 확인된 SSL 인증서를 확인하기 위해 클러스터의 SSL 검증을 업그레이드해야 하는 경우 **Verify SSL Certificate** 확인란을 선택합니다.

4. **저장을** 클릭하여 소스를 저장한 다음 **닫기** 를 클릭하여 소스 추가 마법사를 종료합니다.

3.6.2. RHACS 인증 정보 추가

소스 생성 중에 인증 정보 보기 또는 소스 추가 마법사에서 인증 정보를 추가할 수 있습니다.

사전 요구 사항

- 관리 API 토큰 값을 생성하려면 RHACS(Red Hat Advanced Cluster Security for Kubernetes) 포털에 액세스할 수 있어야 합니다.

- RHACS 중앙 끝점을 찾으려면 RHACS 포털에 액세스하거나 RHACS 구성 관리 클라우드 서비스 인스턴스 세부 정보에 액세스해야 합니다.

프로세스

1. 위치를 기반으로 새 인증 정보를 추가하려면 옵션을 클릭합니다.

   - 인증 정보 보기에서 **RHACS+추가** 를 클릭합니다.

   - 소스 추가 마법사에서 **인증 정보** 필드에 대한 **인증 정보 추가** 아이콘을 클릭합니다.

   인증 정보 추가 마법사가 열립니다.

2. **인증 정보 이름** 필드에 설명하는 이름을 입력합니다.

3. RHACS 포털에서 RHACS의 API 토큰을 입력합니다. 토큰이 아직 없는 경우 RHACSConfiguration Management Cloud Service 포털에서 토큰을 생성할 수 있습니다.

4. **저장**을 클릭하여 인증 정보를 저장하고 인증 정보 추가 마법사를 종료합니다.

3.6.3. 소스 및 인증 정보

검사를 실행하려면 소스 및 인증 정보 두 가지 기본 구조에 대한 데이터를 구성해야 합니다. 검사 중에 검사할 소스 유형에 따라 소스 및 인증 정보 구성에 필요한 데이터 유형이 결정됩니다.

*소스*에는 스캔 중에 검사할 단일 자산 또는 여러 자산 세트가 포함되어 있습니다. 다음 유형의 소스를 구성할 수 있습니다.

네트워크 소스

하나 이상의 물리적 시스템, 가상 시스템 또는 컨테이너 이러한 자산은 호스트 이름, IP 주소, IP 범위 또는 서브넷으로 표시할 수 있습니다.

vCenter 소스

IT 인프라의 전체 또는 일부를 관리하는 vCenter Server 시스템 관리 솔루션입니다.

Satellite 소스

IT 인프라의 전체 또는 일부를 관리하는 Satellite 시스템 관리 솔루션입니다.

Red Hat OpenShift 소스

Red Hat OpenShift Container Platform 노드 및 워크로드를 모두 관리하거나 일부로 관리하는 Red Hat OpenShift Container Platform 클러스터입니다.

Ansible 소스

Ansible 노드 및 워크로드를 관리하는 Ansible 관리 솔루션입니다.

Red Hat Advanced Cluster Security for Kubernetes 소스

Kubernetes 환경을 보호하는 RHACS 보안 플랫폼 솔루션입니다.

네트워크 소스로 작업할 때 단일 소스 내에서 그룹화해야 하는 개별 자산 수를 결정합니다. 현재 네트워크 소스의 소스에 여러 자산을 추가할 수 있습니다. 다음 목록에는 소스를 추가할 때 고려해야 할 몇 가지 다른 요소가 포함되어 있습니다.

- 자산이 개발, 테스트 또는 프로덕션 환경의 일부인지 여부와 컴퓨팅 능력에 대한 요구와 유사한 우려가 해당 자산에 대한 고려 사항인지 여부.
- 설치된 소프트웨어로의 빈번한 변경과 같은 내부 비즈니스 관행을 위해 특정 엔티티 또는 엔티티 그룹을 더 자주 스캔할지 여부.

*인증 정보*에는 해당 소스에 포함된 자산의 전체 또는 일부에서 검사를 실행할 수 있는 충분한 권한이 있는 사용자의 사용자 이름 및 암호 또는 SSH 키와 같은 데이터가 포함되어 있습니다. 소스와 마찬가지로 인증 정보는 네트워크, vCenter, Satellite, OpenShift, Ansible 또는 RHACS 유형으로 구성됩니다. 일반적으로 네트워크 소스에는 광범위한 IP 범위의 모든 자산에 액세스하는 데 필요한 많은 인증 정보가 필요할 것으로 예상되므로 여러 네트워크 인증 정보가 필요할 수 있습니다. 반대로 vCenter 또는 satellite 소스는 일반적으로 단일 vCenter 또는 Satellite 인증 정보를 사용하여 특정 시스템 관리 솔루션 서버에 액세스하고 OpenShift, Ansible 또는 RHACS 소스를 사용하면 단일 클러스터에 액세스할 수 있습니다.

소스 뷰에서 새 소스를 추가하고 인증 정보 뷰에서 새 인증 정보를 추가할 수 있습니다. 소스 생성 중에 새로 인증 정보를 추가하거나 기존 인증 정보를 선택할 수도 있습니다. 소스 생성 중에 소스와 직접 인증 정보를 연결합니다. 소스 및 인증 정보에 일치하는 유형이 있어야 하므로 소스 생성 중에 추가한 모든 인증 정보는 소스와 동일한 유형을 공유합니다. 또한 소스 생성 중에 기존 인증 정보를 사용하려는 경우 사용 가능한 인증 정보 목록에는 동일한 유형의 인증 정보만 포함됩니다. 예를 들어, 네트워크 소스 생성 중에 선택 시 네트워크 인증 정보만 사용할 수 있습니다.

3.6.4. Red Hat Advanced Cluster Security for Kubernetes 인증

RHACS(Red Hat Advanced Cluster Security for Kubernetes) 검사의 경우 RHACS API에 대한 연결 및 액세스는 TLS(Transport Layer Security)를 통해 암호화된 API 토큰 인증을 사용하여 전달자 토큰 인증에서

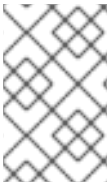
파생됩니다. 기본적으로 RHACS 검사는 인증서 검증 및 TLS 프로토콜을 통해 보안 통신으로 실행됩니다. 소스 생성 중에 인증서 검증 및 보안 통신에 사용할 여러 다른 SSL(Secure Sockets Layer) 및 TLS 프로토콜을 선택할 수 있습니다.

스캔 중에 RHACS 포털에 연결하기 위해 인증서 검증 수준을 조정해야 할 수 있습니다. 예를 들어 RHACS 인스턴스에서 인증 기관의 확인된 TLS 인증서를 사용할 수 있습니다. 소스 생성 중에 TLS 인증서 검증을 업그레이드하여 해당 소스를 검사하는 동안 해당 인증서를 확인할 수 있습니다. 반대로 RHACS 인스턴스에서 자체 서명된 인증서를 사용할 수 있습니다. 소스 생성 중에 소스 검사에서 인증서를 확인하지 않도록 TLS 검증을 기본값으로 유지할 수 있습니다. 이 옵션을 선택한 경우 자체 서명된 인증서의 기본값을 그대로 두려면 검사 오류가 발생하지 않을 수 있습니다.

RHACS 인스턴스가 웹 애플리케이션에 TSL 통신을 사용하도록 구성되지 않은 경우 스캔 중에 TSL을 보안 통신 방법으로 비활성화해야 할 수도 있습니다. 예를 들어, RHACS 인스턴스는 포트 80과 HTTP를 사용하여 웹 애플리케이션과 통신하도록 구성할 수 있습니다. 이 경우 소스 생성 중에 해당 소스의 검사에 대한 TSL 통신을 비활성화할 수 있습니다.

4장. 검사 실행 및 관리

검사하려는 IT 인프라 부분에 대한 소스 및 인증 정보를 추가한 후 스캔을 생성하고 실행할 수 있습니다. 검사를 생성할 때 단일 소스를 스캔하거나 다양한 소스 유형의 여러 소스를 결합하도록 선택할 수 있습니다. 또한 기본 설치 프로세스 및 위치에 설치된 제품의 표준 검사를 수행하거나 비표준 프로세스 또는 위치에서 제품이 설치된 경우 딥 스캔을 수행할 수 있습니다.



참고

현재 검사에서 OpenShift, Ansible 또는 RHACS 검사를 다른 유형의 소스와 결합할 수 없습니다. 그러나 단일 OpenShift, Ansible 또는 RHACS 검사에는 동일한 유형의 여러 소스가 포함될 수 있으며 각 소스는 단일 클러스터와만 연결됩니다.

검사가 생성되면 해당 검사를 여러 번 실행할 수 있습니다. 해당 검사의 각 인스턴스는 검사 작업으로 저장됩니다.

더 알아보기

제품에 대한 딥 스캔을 사용하지 않는 표준 검사를 실행하는 방법에 대한 자세한 내용은 다음 정보를 참조하십시오.

- 표준 검사 실행 및 관리

딥 스캔(비표준 프로세스 또는 비표준 위치에 설치될 수 있는 제품을 검색할 수 있는 스캔) 실행에 대한 자세한 내용은 다음 정보를 참조하십시오.

- 딥 스캔 실행 및 관리

4.1. 표준 검사 실행 및 관리

검사하려는 IT 인프라 부분에 대한 소스 및 인증 정보를 추가한 후 검사 실행을 시작할 수 있습니다. 대부분의 경우 표준 검사를 실행하여 Red Hat 제품을 보고하는 데 필요한 환경 및 제품 데이터를 찾을 수 있습니다.

더 알아보기

표준 검사를 실행하여 표준 위치에서 제품을 찾습니다. 자세한 내용은 다음 정보를 참조하십시오.

- 표준 검사 실행

검사 실행을 시작하면 검사를 관리하기 위해 수행할 수 있는 몇 가지 작업이 있습니다. 이러한 작업에는 새 검사 작업을 실행하고 일시 중지, 다시 시작 및 취소하여 활성 검사를 관리하여 검사 데이터를 업데이트하는 작업이 포함됩니다. 검사를 완료하면 해당 검사를 삭제할 수 있습니다. 자세한 내용은 다음 정보를 참조하십시오.

- 새 스캔 작업 실행
- 스캔 일시 중지, 다시 시작, 취소
- 스캔 삭제

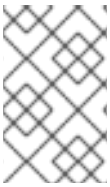
Discovery를 통해 스캔 작업을 처리하는 방법과 스캔 작업이 진행되는 상태를 포함하여 스캔 및 스캔 작업이 작동하는 방법에 대한 자세한 내용은 다음 정보를 참조하십시오.

- 스캔 및 스캔 작업 정보

- 작업 처리 스캔
- 작업 라이프 사이클 스캔

4.1.1. 표준 검사 실행

소스 뷰에서 새 스캔을 수행할 수 있습니다. 단일 소스 스캔을 수행하거나 여러 소스를 선택하여 단일 스캔으로 통합할 수 있습니다. 소스 보기를 사용하여 스캔을 실행할 때마다 새 스캔으로 저장하라는 메시지가 표시됩니다.



참고

현재 검사에서 OpenShift, Ansible 또는 RHACS 검사를 다른 유형의 소스와 결합할 수 없습니다. 그러나 단일 OpenShift, Ansible 또는 RHACS 검사에는 동일한 유형의 여러 소스가 포함될 수 있으며 각 소스는 단일 클러스터와만 연결됩니다.

스캔을 처음 실행하면 스캔이 스캔 뷰에 저장됩니다. 해당 보기에서 다시 스캔을 수행하여 데이터를 업데이트할 수 있습니다. 스캔 보기에서 스캔을 실행할 때마다 스캔의 새 스캔 작업으로 저장됩니다.

사전 요구 사항

- 스캔을 실행하려면 먼저 스캔하려는 소스와 해당 소스에 액세스할 인증 정보를 추가해야 합니다.

프로세스

1. 소스 보기에서 하나 이상의 소스를 선택합니다. 다양한 유형의 소스를 선택하여 단일 스캔으로 결합할 수 있습니다.
2. 선택한 소스에 적합한 **스캔** 버튼을 클릭합니다.
   - 단일 소스의 경우 해당 소스의 행에서 **스캔**을 클릭합니다. 소스에 대한 확인란을 선택하는 것은 선택 사항입니다.
   - 여러 소스를 선택한 경우 툴바에서 **스캔** 을 클릭합니다.

   스캔 마법사가 열립니다.
3. **이름** 필드에 스캔에 대한 설명이 포함된 이름을 입력합니다.
4. 기본 최대 동시 스캔 수를 변경하려면 **최대 동시 스캔** 필드에 새 값을 설정합니다. 이 값은 스캔 중에 병렬로 스캔되는 물리적 머신 또는 가상 머신의 최대 수입니다.
5. 기본 스캔 프로세스를 사용하려면 **이러한 제품에 대해 딥스캔** 이 기본으로 선택 해제된 상태로 유지되도록 합니다.
6. 스캔 프로세스를 시작하려면 **스캔**을 클릭합니다.

검증 단계

스캔 프로세스가 시작되면 소스 보기에 알림이 표시됩니다. 실행 중인 스캔도 스캔 보기에 표시되고 스캔 진행 상황에 대한 메시지가 표시됩니다.

4.1.2. 새 스캔 작업 실행

스캔 이름을 지정하고 처음 실행하면 스캔 보기에 추가됩니다. 그런 다음 스캔 작업이라는 해당 스캔의 새 인스턴스를 실행하여 해당 스캔에 대해 수집된 데이터를 업데이트할 수 있습니다.

프로세스

1. 스캔 보기에서 스캔 세부 정보에서 **스캔 실행** 아이콘을 클릭합니다.

참고

스캔 세부 정보에서 가장 최근 스캔 작업이 성공적으로 완료되지 않으면 이 아이콘에 **스캔 다시시도**라는 레이블이 지정됩니다.

검증 단계

스캔 프로세스가 시작되면 스캔 진행 상황에 대한 메시지와 함께 알림이 표시됩니다. 완료된 스캔을 보려면 스캔 세부 정보를 보고 **이전**을 클릭하여 이전 스캔 작업을 모두 볼 수 있습니다.

4.1.3. 스캔 일시 중지, 다시 시작, 취소

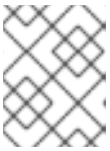
스캔 실행을 시작할 때 현재 실행 중인 스캔 작업을 중지해야 할 수 있습니다. 예를 들어 IT 상태 모니터링 시스템의 경고로 인해 긴급 수정을 수행해야 하거나 현재 실행 중인 더 낮은 우선 순위 검사보다 더 많은 CPU 리소스를 사용하는 우선 순위 검사를 실행해야 하는 여러 가지 비즈니스 이유가 있을 수 있습니다.

검사 작업을 일시 중지하거나 취소하여 중지할 수 있습니다. 일시 중지된 스캔 작업을 다시 시작할 수 있지만 취소된 스캔 작업을 다시 시작할 수 없습니다.

프로세스

실행 중인 스캔 작업을 일시 중지하려면 다음을 수행합니다.

1. 스캔 보기에서 일시 중지하려는 스캔 작업이 포함된 스캔을 찾습니다.
2. **스캔 일시 중지**를 클릭합니다.



참고

동시에 여러 스캔이 실행되는 경우 **스캔 일시 중지** 아이콘이 표시되기까지 몇 분 정도 걸릴 수 있습니다.

일시 중지된 스캔 작업을 다시 시작하려면 다음을 수행합니다.

1. 스캔 보기에서 다시 시작하려는 스캔 작업이 포함된 스캔을 찾습니다.
2. **스캔 다시 시작**을 클릭합니다.

실행 중인 스캔 작업을 취소하려면 다음을 수행합니다.

1. 스캔 보기에서 취소하려는 스캔 작업이 포함된 스캔을 찾습니다.
2. **스캔 취소** 를 클릭합니다.

4.1.4. 스캔 삭제

스캔을 삭제하는 것은 해당 스캔에 대한 검색 및 모든 스캔 작업을 삭제하는 되돌릴 수 없는 작업입니다. 삭제된 스캔을 검색할 수 없습니다.

사전 요구 사항

- 스캔을 삭제하려면 먼저 **스캔** 탐색에 표시되도록 스캔을 실행해야 합니다.

프로세스

1. 탐색에서 **스캔**을 클릭합니다.
2. 삭제하려는 스캔이 포함된 행을 찾습니다.
3. 해당 행의 **삭제** 아이콘을 클릭합니다.

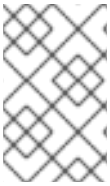
결과

- 스캔이 삭제됩니다.

4.1.5. 스캔 및 스캔 작업 정보

소스 및 인증 정보를 생성한 후 스캔을 생성할 수 있습니다. *스캔*은 재현 가능한 방식으로 스캔을 수행하거나 스캔할 수 있는 단위로 소스를 그룹화하는 오브젝트입니다. 저장된 스캔을 실행할 때마다 해당 인스턴스는 *스캔 작업*으로 저장됩니다. 스캔 작업의 출력은 해당 소스에 포함된 모든 IT 리소스에 대해 수집된 팩트 컬렉션 *보고서* 입니다.

스캔에는 하나 이상의 소스와 소스 생성 시 해당 소스와 연결된 인증 정보가 포함됩니다. 스캔 작업이 실행되면 제공된 인증 정보를 사용하여 소스에 포함된 자산에 연락한 다음 자산을 검사하여 보고서의 해당 자산에 대한 팩트를 수집합니다. 단일 스캔에 다양한 유형의 소스를 포함하여 단일 스캔에 여러 소스를 추가할 수 있습니다.



참고

현재 스캔의 다른 유형의 소스와 OpenShift 소스를 결합할 수 없습니다. 그러나 단일 OpenShift 검사에는 각각 단일 클러스터와만 연결된 OpenShift 소스가 여러 개 포함될 수 있습니다.

4.1.6. 작업 처리 스캔

스캔 작업은 처리되는 동안 두 단계 또는 작업을 통해 이동합니다. 이 두 작업은 연결 작업과 검사 작업입니다.

4.1.6.1. 작업 연결 및 검사 작업 스캔

스캔 작업 중에 실행되는 첫 번째 작업은 연결 작업입니다. *연결 작업은* 소스에 연결하는 기능을 결정하고 정의된 소스에 대해 검사할 수 있는 시스템 수를 찾습니다. 두 번째 실행 작업은 검사 작업입니다. *검사 작업은* 정의된 소스의 각 연결 가능한 시스템에서 데이터를 수집하여 검사 결과를 보고서로 출력하는 작업입니다.

스캔이 여러 소스를 포함하도록 구성된 경우 스캔 작업이 실행되면 각 소스에 대해 이러한 두 작업이 생성됩니다. 먼저 모든 소스에 대한 모든 연결 작업을 실행하여 소스에 대한 연결을 설정하고 검사할 수 있는 시스템을 찾습니다. 그런 다음 모든 소스에 대한 모든 검사 작업을 실행하여 소스에 포함된 액세스 가능한 시스템의 콘텐츠를 검사합니다.

4.1.6.2. 이러한 작업을 처리하는 방법

스캔 작업에서 소스에 대한 연결 작업을 실행하면 네트워크, 서버, 클러스터 또는 사용된 인스턴스에 연결을 시도합니다. 연결에 실패하면 연결 작업이 실패합니다. 네트워크 검사의 경우 네트워크에 연결할 수 없

거나 인증 정보가 유효하지 않은 경우 연결 작업에서 (0) 성공 시스템을 보고합니다. 네트워크 스캔용 일부 시스템만 연결할 수 있는 경우 연결 작업에서 연결할 수 있는 시스템에서 성공하고 연결 작업이 실패하지 않습니다.

스캔 보기에서 연결 작업의 상태에 대한 정보를 볼 수 있습니다. 스캔 행에는 가장 최근 검사 작업의 성공적인 시스템 연결 수로 연결 작업 결과가 표시됩니다. 이전 스캔 작업을 확장하여 이전 스캔 작업에 대한 연결 작업 결과를 확인할 수도 있습니다.

스캔 작업에서 소스에 대한 스캔 작업을 실행하면 연결 작업 상태를 확인합니다. 연결 작업이 실패 상태를 표시하거나 0(0)에 성공한 연결이 있는 경우 스캔 작업이 실패 상태로 전환됩니다. 그러나 연결 작업에서 하나 이상의 성공적인 연결을 보고하면 검사 작업이 계속됩니다. 그런 다음 스캔 작업의 결과에 각 개별 시스템의 성공 및 실패 데이터가 표시됩니다. 검사 작업이 성공한 시스템에서 결과를 수집할 수 없거나 검사 작업 중에 다른 예기치 않은 오류가 발생한 경우 스캔 작업이 실패 상태로 전환됩니다.

스캔에 여러 소스가 포함된 경우 각 소스에 고유한 연결 및 검사 작업이 있습니다. 이러한 작업은 다른 소스에 대한 작업과 독립적으로 처리됩니다. 소스에 대한 작업이 하나라도 실패하면 스캔 작업이 실패 상태로 전환됩니다. 스캔 작업은 모든 소스에 대한 모든 스캔 작업 작업이 성공적으로 완료된 경우에만 완료된 상태로 전환됩니다.

스캔 작업이 성공적으로 완료되면 해당 스캔 작업의 데이터가 보고서로 생성됩니다. 스캔 보기에서 성공적인 각 스캔 작업에 대한 보고서를 다운로드할 수 있습니다.

4.1.7. 작업 라이프 사이클 스캔

스캔 작업 또는 스캔의 개별 인스턴스는 라이프사이클 동안 여러 상태를 통해 이동합니다.

스캔을 시작하면 스캔 작업이 생성되고 스캔 작업이 *생성됨* 상태가 됩니다. 그런 다음 스캔 작업이 처리를 위해 대기열에 추가되고 스캔 작업이 *보류 중* 상태로 전환됩니다. 스캔 작업은 시작 순서대로 직렬로 실행됩니다.

Discovery 서버가 대기열의 특정 스캔 작업에 도달하면 해당 스캔 작업의 처리가 시작될 때 스캔 작업이 *보류* 상태에서 *실행* 상태로 전환됩니다. 스캔 프로세스가 성공적으로 완료되면 스캔 작업이 *완료* 상태로 전환되고 스캔 작업에서 보고서에서 볼 수 있는 결과를 생성합니다. 스캔 프로세스에서 스캔을 성공적으로 완료하지 못하는 오류가 발생하면 스캔 작업이 중지되고 스캔 작업이 *실패* 상태로 전환됩니다. 실패한 스캔에 대한 추가 상태 메시지에는 실패 원인을 결정하는 데 도움이 되는 정보가 포함되어 있습니다.

스캔 작업에서 수행된 사용자 작업으로 인한 스캔 작업의 기타 상태입니다. 보류 중이거나 실행 중인 동안 스캔 작업을 일시 중지하거나 취소할 수 있습니다. *일시 중지됨* 상태의 스캔 작업을 다시 시작할 수 있습니다. *취소됨* 상태의 스캔 작업은 다시 시작할 수 없습니다.

4.2. 딥 스캔 실행 및 관리

검사하려는 IT 인프라 부분에 대한 소스 및 인증 정보를 추가한 후 검사 실행을 시작할 수 있습니다. 몇 가지 상황에서는 표준 검사를 실행하는 것만으로는 Red Hat 제품을 보고하는 데 필요한 환경 및 제품 데이터를 찾는 데 충분하지 않습니다.

기본적으로 Discovery는 해당 제품과 관련된 알려진 메타데이터를 사용하여 제품을 검색하고 인쇄합니다. 그러나 이러한 제품을 프로세스 또는 설치 위치에 설치하여 검색 및 지문 알고리즘의 효과를 줄일 수 있습니다. 이 경우 해당 제품을 찾으려면 딥 스캔을 사용해야 합니다.

더 알아보기

딥 스캔을 실행하여 비표준 위치에서 제품을 찾습니다. 자세한 내용은 다음 정보를 참조하십시오.

- 딥 스캔으로 검사 실행

검사 실행을 시작하면 검사를 관리하기 위해 수행할 수 있는 몇 가지 작업이 있습니다. 이러한 작업에는 새 검사 작업을 실행하고 일시 중지, 다시 시작 및 취소하여 활성 검사를 관리하여 검사 데이터를 업데이트하는 작업이 포함됩니다. 검사를 완료하면 해당 검사를 삭제할 수 있습니다. 자세한 내용은 다음 정보를 참조하십시오.

- 새 스캔 작업 실행
- 스캔 일시 중지, 다시 시작, 취소
- 스캔 삭제

Discovery를 통해 스캔 작업을 처리하는 방법과 스캔 작업이 진행되는 상태를 포함하여 스캔 및 스캔 작업이 작동하는 방법에 대한 자세한 내용은 다음 정보를 참조하십시오.

- 스캔 및 스캔 작업 정보
- 작업 처리 스캔
- 작업 라이프 사이클 스캔

4.2.1. 딥 스캔으로 검사 실행

소스 뷰에서 새 스캔을 수행할 수 있습니다. 단일 소스 스캔을 수행하거나 여러 소스를 선택하여 단일 스캔으로 통합할 수 있습니다. 검사 구성의 일부로 딥 스캔 프로세스를 사용하여 비표준 위치의 제품을 검색하도록 선택할 수 있습니다.

참고

현재 검사에서 OpenShift, Ansible 또는 RHACS 검사를 다른 유형의 소스와 결합할 수 없습니다. 그러나 단일 OpenShift, Ansible 또는 RHACS 검사에는 각각 단일 클러스터에만 연결된 OpenShift, Ansible 또는 RHACS 소스가 여러 개 포함될 수 있습니다.

딥 스캔 프로세스에서는 **find** 명령을 사용하므로 검색 프로세스가 검사 중인 시스템에 CPU 리소스를 많이 사용할 수 있습니다. 따라서 프로덕션 시스템과 같이 지속적인 가용성이 필요한 시스템에 대한 깊은 검사를 선택할 때 재량에 따라 사용해야 합니다.

스캔을 처음 실행하면 스캔이 스캔 뷰에 저장됩니다. 해당 보기에서 검사를 다시 실행하여 데이터를 업데이트할 수 있습니다.

사전 요구 사항

- 스캔을 실행하려면 먼저 스캔하려는 소스와 해당 소스에 액세스할 인증 정보를 추가해야 합니다.

프로세스

1. 소스 보기에서 하나 이상의 소스를 선택합니다. 다양한 유형의 소스를 선택하여 단일 스캔으로 결합할 수 있습니다.
2. 선택한 소스에 적합한 **스캔** 버튼을 클릭합니다.
   - 단일 소스의 경우 해당 소스의 행에서 **스캔**을 클릭합니다. 소스에 대한 확인란을 선택하는 것은 선택 사항입니다.
   - 여러 소스를 선택한 경우 툴바에서 **스캔** 을 클릭합니다.

   스캔 마법사가 열립니다.

3. **이름** 필드에 스캔에 대한 설명이 포함된 이름을 입력합니다.

4. 기본 최대 동시 스캔 수를 변경하려면 **최대 동시 스캔** 필드에 새 값을 설정합니다. 이 값은 스캔 중에 병렬로 스캔되는 물리적 머신 또는 가상 머신의 최대 수입니다.

5. 하나 이상의 제품에서 딥 스캔 프로세스를 사용하려면 다음 정보를 제공하십시오.

   - **이러한 제품에 적용되는 딥 스캔** 확인란을 선택합니다.

   - 선택적으로 Discovery를 스캔할 디렉터리를 입력합니다. 딥 검사에 사용되는 기본 디렉터리는 **/** , **/opt**, **/ app**,**/home**, **/usr** 디렉토리입니다.

6. 스캔 프로세스를 시작하려면 **스캔**을 클릭합니다.

검증 단계

스캔 프로세스가 시작되면 소스 보기에 알림이 표시됩니다. 실행 중인 스캔도 스캔 보기에 표시되고 스캔 진행 상황에 대한 메시지가 표시됩니다.

4.2.2. 새 스캔 작업 실행

스캔 이름을 지정하고 처음 실행하면 스캔 보기에 추가됩니다. 그런 다음 스캔 작업이라는 해당 스캔의 새 인스턴스를 실행하여 해당 스캔에 대해 수집된 데이터를 업데이트할 수 있습니다.

프로세스

1. 스캔 보기에서 스캔 세부 정보에서 **스캔 실행** 아이콘을 클릭합니다.

참고

스캔 세부 정보에서 가장 최근 스캔 작업이 성공적으로 완료되지 않으면 이 아이콘에 **스캔 다시시도**라는 레이블이 지정됩니다.

검증 단계

스캔 프로세스가 시작되면 스캔 진행 상황에 대한 메시지와 함께 알림이 표시됩니다. 완료된 스캔을 보려면 스캔 세부 정보를 보고 **이전**을 클릭하여 이전 스캔 작업을 모두 볼 수 있습니다.

4.2.3. 스캔 일시 중지, 다시 시작, 취소

스캔 실행을 시작할 때 현재 실행 중인 스캔 작업을 중지해야 할 수 있습니다. 예를 들어 IT 상태 모니터링 시스템의 경고로 인해 긴급 수정을 수행해야 하거나 현재 실행 중인 더 낮은 우선 순위 검사보다 더 많은 CPU 리소스를 사용하는 우선 순위 검사를 실행해야 하는 여러 가지 비즈니스 이유가 있을 수 있습니다.

검사 작업을 일시 중지하거나 취소하여 중지할 수 있습니다. 일시 중지된 스캔 작업을 다시 시작할 수 있지만 취소된 스캔 작업을 다시 시작할 수 없습니다.

프로세스

실행 중인 스캔 작업을 일시 중지하려면 다음을 수행합니다.

1. 스캔 보기에서 일시 중지하려는 스캔 작업이 포함된 스캔을 찾습니다.

2. **스캔 일시 중지**를 클릭합니다.

참고

동시에 여러 스캔이 실행되는 경우 **스캔 일시 중지** 아이콘이 표시되기까지 몇 분 정도 걸릴 수 있습니다.

일시 중지된 스캔 작업을 다시 시작하려면 다음을 수행합니다.

1. 스캔 보기에서 다시 시작하려는 스캔 작업이 포함된 스캔을 찾습니다.
2. **스캔 다시 시작**을 클릭합니다.

실행 중인 스캔 작업을 취소하려면 다음을 수행합니다.

1. 스캔 보기에서 취소하려는 스캔 작업이 포함된 스캔을 찾습니다.
2. **스캔 취소**를 클릭합니다.

4.2.4. 스캔 삭제

스캔을 삭제하는 것은 해당 스캔에 대한 검색 및 모든 스캔 작업을 삭제하는 되돌릴 수 없는 작업입니다. 삭제된 스캔을 검색할 수 없습니다.

사전 요구 사항

- 스캔을 삭제하려면 먼저 **스캔** 탐색에 표시되도록 스캔을 실행해야 합니다.

프로세스

1. 탐색에서 **스캔**을 클릭합니다.
2. 삭제하려는 스캔이 포함된 행을 찾습니다.
3. 해당 행의 **삭제** 아이콘을 클릭합니다.

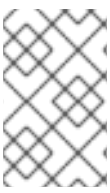
결과

- 스캔이 삭제됩니다.

4.2.5. 스캔 및 스캔 작업 정보

소스 및 인증 정보를 생성한 후 스캔을 생성할 수 있습니다. *스캔*은 재현 가능한 방식으로 스캔을 수행하거나 스캔할 수 있는 단위로 소스를 그룹화하는 오브젝트입니다. 저장된 스캔을 실행할 때마다 해당 인스턴스는 *스캔 작업*으로 저장됩니다. 스캔 작업의 출력은 해당 소스에 포함된 모든 IT 리소스에 대해 수집된 팩트 컬렉션 *보고서* 입니다.

스캔에는 하나 이상의 소스와 소스 생성 시 해당 소스와 연결된 인증 정보가 포함됩니다. 스캔 작업이 실행되면 제공된 인증 정보를 사용하여 소스에 포함된 자산에 연락한 다음 자산을 검사하여 보고서의 해당 자산에 대한 팩트를 수집합니다. 단일 스캔에 다양한 유형의 소스를 포함하여 단일 스캔에 여러 소스를 추가할 수 있습니다.



참고

현재 스캔의 다른 유형의 소스와 OpenShift 소스를 결합할 수 없습니다. 그러나 단일 OpenShift 검사에는 각각 단일 클러스터와만 연결된 OpenShift 소스가 여러 개 포함될 수 있습니다.

4.2.6. 작업 처리 스캔

스캔 작업은 처리되는 동안 두 단계 또는 작업을 통해 이동합니다. 이 두 작업은 연결 작업과 검사 작업입니다.

4.2.6.1. 작업 연결 및 검사 작업 스캔

스캔 작업 중에 실행되는 첫 번째 작업은 연결 작업입니다. *연결 작업은* 소스에 연결하는 기능을 결정하고 정의된 소스에 대해 검사할 수 있는 시스템 수를 찾습니다. 두 번째 실행 작업은 검사 작업입니다. *검사 작업은* 정의된 소스의 각 연결 가능한 시스템에서 데이터를 수집하여 검사 결과를 보고서로 출력하는 작업입니다.

스캔이 여러 소스를 포함하도록 구성된 경우 스캔 작업이 실행되면 각 소스에 대해 이러한 두 작업이 생성됩니다. 먼저 모든 소스에 대한 모든 연결 작업을 실행하여 소스에 대한 연결을 설정하고 검사할 수 있는 시스템을 찾습니다. 그런 다음 모든 소스에 대한 모든 검사 작업을 실행하여 소스에 포함된 액세스 가능한 시스템의 콘텐츠를 검사합니다.

4.2.6.2. 이러한 작업을 처리하는 방법

스캔 작업에서 소스에 대한 연결 작업을 실행하면 네트워크, 서버, 클러스터 또는 사용된 인스턴스에 연결을 시도합니다. 연결에 실패하면 연결 작업이 실패합니다. 네트워크 검사의 경우 네트워크에 연결할 수 없거나 인증 정보가 유효하지 않은 경우 연결 작업에서 (0) 성공 시스템을 보고합니다. 네트워크 스캔용 일부 시스템만 연결할 수 있는 경우 연결 작업에서 연결할 수 있는 시스템에서 성공하고 연결 작업이 실패하지 않습니다.

스캔 보기에서 연결 작업의 상태에 대한 정보를 볼 수 있습니다. 스캔 행에는 가장 최근 검사 작업의 성공적인 시스템 연결 수로 연결 작업 결과가 표시됩니다. 이전 스캔 작업을 확장하여 이전 스캔 작업에 대한 연결 작업 결과를 확인할 수도 있습니다.

스캔 작업에서 소스에 대한 스캔 작업을 실행하면 연결 작업 상태를 확인합니다. 연결 작업이 실패 상태를 표시하거나 0(0)에 성공한 연결이 있는 경우 스캔 작업이 실패 상태로 전환됩니다. 그러나 연결 작업에서 하나 이상의 성공적인 연결을 보고하면 검사 작업이 계속됩니다. 그런 다음 스캔 작업의 결과에 각 개별 시스템의 성공 및 실패 데이터가 표시됩니다. 검사 작업이 성공한 시스템에서 결과를 수집할 수 없거나 검사 작업 중에 다른 예기치 않은 오류가 발생한 경우 스캔 작업이 실패 상태로 전환됩니다.

스캔에 여러 소스가 포함된 경우 각 소스에 고유한 연결 및 검사 작업이 있습니다. 이러한 작업은 다른 소스에 대한 작업과 독립적으로 처리됩니다. 소스에 대한 작업이 하나라도 실패하면 스캔 작업이 실패 상태로 전환됩니다. 스캔 작업은 모든 소스에 대한 모든 스캔 작업 작업이 성공적으로 완료된 경우에만 완료된 상태로 전환됩니다.

스캔 작업이 성공적으로 완료되면 해당 스캔 작업의 데이터가 보고서로 생성됩니다. 스캔 보기에서 성공적인 각 스캔 작업에 대한 보고서를 다운로드할 수 있습니다.

4.2.7. 작업 라이프 사이클 스캔

스캔 작업 또는 스캔의 개별 인스턴스는 라이프사이클 동안 여러 상태를 통해 이동합니다.

스캔을 시작하면 스캔 작업이 생성되고 스캔 작업이 *생성됨* 상태가 됩니다. 그런 다음 스캔 작업이 처리를 위해 대기열에 추가되고 스캔 작업이 *보류 중* 상태로 전환됩니다. 스캔 작업은 시작 순서대로 직렬로 실행됩니다.

Discovery 서버가 대기열의 특정 스캔 작업에 도달하면 해당 스캔 작업의 처리가 시작될 때 스캔 작업이 *보류* 상태에서 *실행* 상태로 전환됩니다. 스캔 프로세스가 성공적으로 완료되면 스캔 작업이 *완료* 상태로 전환되고 스캔 작업에서 보고서에서 볼 수 있는 결과를 생성합니다. 스캔 프로세스에서 스캔을 성공적으로 완료하지 못하는 오류가 발생하면 스캔 작업이 중지되고 스캔 작업이 *실패* 상태로 전환됩니다. 실패한 스캔에 대한 추가 상태 메시지에는 실패 원인을 결정하는 데 도움이 되는 정보가 포함되어 있습니다.

스캔 작업에서 수행된 사용자 작업으로 인한 스캔 작업의 기타 상태입니다. 보류 중이거나 실행 중인 동안 스캔 작업을 일시 중지하거나 취소할 수 있습니다. *일시 중지된* 상태의 스캔 작업을 다시 시작할 수 있습니다. *취소된* 상태의 스캔 작업은 다시 시작할 수 없습니다.

5장. 보고서 다운로드

스캔을 실행한 후 해당 스캔에 대한 보고서를 다운로드하여 해당 스캔 중에 수집 및 처리된 데이터를 볼 수 있습니다.

더 알아보기

보고서 다운로드에 대한 자세한 내용은 다음 정보를 참조하십시오.

- 보고서 다운로드

5.1. 보고서 다운로드

스캔을 실행한 후 해당 스캔에 대한 보고서를 다운로드하여 해당 스캔 중에 수집 및 처리된 데이터를 볼 수 있습니다.

스캔 보고서는 CSV(콤마로 구분된 변수) 형식과 JSON(JavaScript Object Notation) 형식의 두 형식으로 사용할 수 있습니다. 또한 두 가지 콘텐츠 유형, 세부 정보 보고서로 스캔의 원시 출력 및 배포 보고서로 콘텐츠를 처리할 수 있습니다.

참고

세 번째 유형의 보고서를 사용할 수 있지만 이 보고서는 Discovery 명령줄 인터페이스를 통해서만 생성할 수 있습니다. Insights 보고서를 다운로드하면 cloud.redhat.com에서 하이브리드 클라우드 콘솔로 전송할 수 있는 **.tar.gz** 파일이 제공됩니다. 이 파일을 전송하면 Red Hat Insights 인벤토리 서비스 및 서브스크립션 서비스에서 보고서 데이터를 사용할 수 있습니다.

더 알아보기

보고서 병합 및 다운로드에 대한 자세한 내용은 다음 정보를 참조하십시오.

- 보고서 다운로드

보고서를 만드는 방법에 대한 자세한 내용은 다음 정보를 참조하십시오. 이 정보에는 보고서 생성 프로세스에 대한 추적이 포함됩니다. 이러한 프로세스는 세부 정보 보고서의 원시 사실을 지문 데이터로 변경한 다음 지문 데이터를 배포 보고서의 중복 및 병합 데이터로 변경합니다. 이 정보에는 검색 보고서를 만드는 데 사용되는 데이터 유형을 표시하는 부분 지문 예도 포함되어 있습니다.

- 보고서가 생성되는 방법
- 지문 예

5.1.1. 보고서 다운로드

스캔 보기에서 하나 이상의 보고서를 선택하고 다운로드하여 보고서 데이터를 볼 수 있습니다.

사전 요구 사항

스캔에 대한 보고서를 다운로드하려면 해당 스캔에 대한 최신 스캔 작업이 성공적으로 완료되어야 합니다.

프로세스

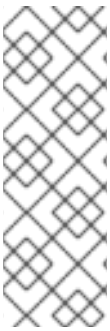
1. 스캔 보기에서 보고서를 다운로드할 스캔 행으로 이동합니다.

2. 해당 스캔에 대한 **다운로드**를 클릭합니다.

검증 단계

다운로드한 보고서는 브라우저의 다운로드 위치에 **.tar.gz** 파일(예: **report_id_224_20190702_173309.tar.gz**)로 저장됩니다. 파일 이름 형식은 **report_id_*ID_DATE_TIME*.tar.gz** 입니다. 여기서 ***ID*** 는 서버에서 할당한 고유한 보고서 ID이며, ***DATE***는 *yyyymmdd* 형식의 날짜이며, ***TIME*** 은 24시간 시스템을 기반으로 *hhmmss* 형식의 시간입니다. 날짜 및 시간 데이터는 클라이언트와 서버 API를 실행하는 브라우저의 상호 작용에 따라 결정됩니다.

보고서를 보려면 **.tar.gz** 파일을 **report_id_*ID*** 디렉터리로 압축 해제하십시오. 압축되지 않은 보고서 번들에는 CSV 및 JSON 형식의 두 가지 세부 정보 보고서와 CSV 및 JSON 형식의 배포 보고서 두 개가 포함되어 있습니다.



참고

이러한 보고서의 출력을 보고 내부 프로세스에 대해 사용할 수 있지만 Discovery 설명서에서는 보고서 결과를 해석하는 데 도움이 되는 정보를 제공하지 않습니다. 또한 Red Hat 지원팀은 Discovery 설치 및 사용과 관련된 몇 가지 기본 지원을 제공할 수 있지만 지원 팀은 보고서를 이해하는 데 도움을 주는 어떠한 도움도 제공하지 않습니다. 보고서 및 형식은 Red Hat Subscription Education and Awareness Program (SEAP) 팀에서 사용하고 다양한 하이브리드 클라우드 콘솔 서비스에 데이터를 제공하는 등의 기타 Red Hat 내부 프로세스를 위해 사용하도록 설계되었습니다.

5.1.2. 보고서가 생성되는 방법

스캔 프로세스는 IT 인프라의 시스템을 검색하고, 해당 시스템의 특성과 콘텐츠에 대한 정보를 검사 및 수집하고, 각 시스템을 검사하는 동안 수집하는 정보에서 보고서를 생성하는 데 사용됩니다.

*시스템*은 SSH 연결, vCenter Server 데이터, Satellite Server API 또는 Red Hat OpenShift 클러스터 API를 통해 검사 작업에서 상호 순환할 수 있는 엔터티입니다. 따라서 시스템은 물리적 또는 가상 머신과 같은 머신일 수 있으며 컨테이너 또는 클러스터와 같은 다른 유형의 엔터티일 수도 있습니다.

5.1.2.1. 팩트 및 지문

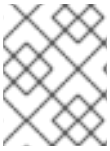
검사 중에 각 소스에 포함된 각 시스템에 대한 팩트 컬렉션이 수집됩니다. *팩트*는 운영 체제 버전, CPU 코어 수 또는 Red Hat 제품에 대한 소비 인타이틀먼트와 같은 시스템에 대한 단일 데이터입니다.

팩트는 각 시스템에 대한 요약된 데이터 세트, 지문이라고 하는 데이터 집합을 생성하기 위해 처리됩니다. *지문* 은 고유한 시스템과 아키텍처, 운영 체제, 해당 시스템 및 해당 버전에 설치된 다양한 제품, 해당 시스템에서 사용 중인 인타이틀먼트 등을 식별하는 팩트 세트입니다.

데이터 지문은 검사 작업을 실행할 때 생성되지만 데이터는 하나의 보고서 유형만 생성하는 데 사용됩니다. 세부 정보 보고서를 요청하면 지문 없이 해당 검사에 대한 원시 정보가 표시됩니다. 배포 보고서를 요청하면 중복 제거, 병합 및 후 처리 프로세스의 결과가 포함된 지문 데이터가 표시됩니다. 이러한 프로세스에는 원시 사실에서 설치된 제품 및 버전 식별, 소비된 인타이틀먼트 찾기, 다른 소스의 중복 제품 인스턴스를 검색 및 병합하고, 기본이 아닌 위치에 설치된 제품 찾기가 포함됩니다.

5.1.2.2. 시스템 중복 제거 및 시스템 병합

단일 시스템은 스캔 중에 여러 소스에서 찾을 수 있습니다. 예를 들어 vCenter Server의 가상 머신은 Satellite에서 관리하는 Red Hat Enterprise Linux 운영 체제 설치를 실행할 수 있습니다. 각 소스 유형, vcenter, satellite 및 network가 포함된 검사를 구성하는 경우 해당 단일 시스템은 스캔 중에 세 가지 소스 모두에 의해 보고됩니다.



참고

현재 검사에서 OpenShift 또는 Ansible 소스를 다른 유형의 소스와 결합할 수 없으므로 중복 제거 및 병합 프로세스는 OpenShift 또는 Ansible 검사에 적용되지 않습니다.

이 문제를 해결하고 정확한 지문을 구축하기 위해 Discovery는 처리되지 않은 시스템 팩트를 스캔에서 지문 엔진에 공급합니다. 지문 엔진은 중복 제거 및 병합 프로세스를 사용하여 둘 이상의 소스에서 발견된 시스템의 데이터를 일치시키고 병합합니다.

시스템 중복 제거 프로세스는 시스템에 대한 특정 팩트를 사용하여 중복 시스템을 식별합니다. 프로세스는 중복 시스템을 연속으로 결합하기 위해 이러한 사실을 사용하여 여러 단계로 이동합니다.

- 네트워크 소스의 모든 시스템은 단일 네트워크 시스템 세트로 결합됩니다. **subscription_manager_id** 또는 **bios_uuid** 팩트에 동일한 값이 있는 경우 시스템은 중복으로 간주됩니다.
- vcenter 소스의 모든 시스템은 단일 vcenter 시스템 세트로 결합됩니다. **vm_uuid** 팩트에 동일한 값이 있는 경우 시스템은 중복으로 간주됩니다.
- Satellite 소스의 모든 시스템은 단일 Satellite 시스템 세트로 결합됩니다. **subscription_manager_id** 팩트에 동일한 값이 있는 경우 시스템은 중복으로 간주됩니다.
- 네트워크 시스템 세트는 satellite 시스템 세트와 병합되어 단일 network-satellite 시스템 세트를 형성합니다. 시스템이 **subscription_manager** 팩트에 대해 동일한 값이 있거나 **mac_addresses** 팩트에서 일치하는 MAC 주소 값이 있는 경우 시스템은 중복으로 간주됩니다.
- network-satellite 시스템 세트는 vcenter 시스템 세트와 병합되어 전체 시스템 세트를 구성합니다. 시스템이 **mac_addresses** 팩트에서 MAC 주소 값과 일치하는 경우 또는 **vm_uuid** 팩트의 vcenter 값이 **bios_uuid** 팩트의 네트워크 값과 일치하는 경우 중복으로 간주됩니다.

5.1.2.2.1. 시스템 병합

중복 제거 프로세스에서 두 시스템이 중복되는 것을 확인한 후 다음 단계는 이 두 시스템을 병합하는 것입니다. 병합된 시스템에는 각 소스의 시스템 팩트가 통합됩니다. 두 시스템에 표시되는 팩트가 병합되면 병합 프로세스에서 우선순위의 다음 순서를 사용하여 가장 높은 것에서 가장 낮은 순으로 해당 사실을 병합합니다.

1. 네트워크 소스 팩트
2. Satellite 소스 팩트
3. vCenter 소스 팩트

시스템 지문에는 해당 시스템에 대한 각 사실의 원래 소스를 캡처하는 **metadata** 사전이 포함되어 있습니다.

5.1.2.3. 시스템 후 처리

중복 제거 및 병합이 완료되면 파생된 시스템 팩트를 작성하는 처리 후 단계가 있습니다. *파생된 시스템 팩트*는 둘 이상의 시스템 팩트의 평가에서 생성되는 팩트입니다. 파생된 시스템 팩트의 대부분은 특정 제품 및 해당 버전의 존재와 같은 제품 식별 데이터와 관련이 있습니다.

다음 예제에서는 파생 시스템 팩트 **system_creation_date** 가 생성되는 방법을 보여줍니다.

system_creation_date 팩트는 실제 시스템 생성 시간이 포함된 파생 시스템 팩트입니다. 이 팩트의 값은 다음 팩트의 평가에 의해 결정됩니다. 각 팩트의 값은 다음과 같은 우선 순위 순서로 검사되며 실제 시스템

생성 시간에 대한 일치의 정확성에 따라 우선순위 순서가 결정됩니다. 비어 있지 않은 가장 높은 값은 **system_creation_date** 팩트의 값을 결정하는 데 사용됩니다.

1. **date_machine_id**
2. **registration_time**
3. **date_anaconda_log**
4. **date_filesystem_create**
5. **date_yum_history**

5.1.2.4. 보고서 생성

보고서 데이터 처리가 완료되면 보고서 작성 프로세스는 JSON(JavaScript Object Notation)과 쉼표로 구분된 변수(CSV)의 두 가지 형식으로 보고서를 작성합니다. 각 형식에 대한 *세부 정보* 보고서에는 처리가 없는 원시 팩트가 포함되어 있으며 각 형식의 *배포* 보고서에는 지문, 중복 제거, 병합, 후처리 프로세스를 통해 원시 팩트가 전달된 후 출력이 포함됩니다.

보고서 형식은 Red Hat Subscription educational and Awareness Program (SEAP) 팀이 고객 참여 및 기타 Red Hat 내부 프로세스에 사용하도록 설계되었습니다.

참고

이러한 보고서의 출력을 보고 내부 프로세스에 대해 사용할 수 있지만 Discovery 설명서에서는 보고서 결과를 해석하는 데 도움이 되는 정보를 제공하지 않습니다. 또한 Red Hat 지원팀은 Discovery 설치 및 사용과 관련된 몇 가지 기본 지원을 제공할 수 있지만 지원 팀은 보고서를 이해하는 데 도움을 주는 어떠한 도움도 제공하지 않습니다. 보고서 및 형식은 Red Hat Subscription Education and Awareness Program (SEAP) 팀에서 사용하고 다양한 하이브리드 클라우드 콘솔 서비스에 데이터를 제공하는 등의 기타 Red Hat 내부 프로세스를 위해 사용하도록 설계되었습니다.

5.1.2.5. 지문 예

지문은 해당 시스템의 제품, 인타이틀먼트, 소스 및 메타데이터에 대한 사실 외에 단일 시스템에 대한 팩트 세트로 구성됩니다. 다음 예제에서는 지문 데이터를 보여줍니다. Red Hat 제품이 거의 설치되지 않은 경우에도 단일 시스템의 지문 행이 많을 수 있습니다. 따라서 이 예에서는 부분 지문만 사용됩니다.

예

```
{
   "os_release": "Red Hat Enterprise Linux Atomic Host 7.4",
   "cpu_count": 4,
   "products": [
      {
         "name": "JBoss EAP",
         "version": null,
         "presence": "absent",
         "metadata": {
            "source_id": 5,
            "source_name": "S62Source",
            "source_type": "satellite",
            "raw_fact_key": null
         }
```

```
        }
    ],
    "entitlements": [
        {
            "name": "Satellite Tools 6.3",
            "entitlement_id": 54,
            "metadata": {
                "source_id": 5,
                "source_name": "S62Source",
                "source_type": "satellite",
                "raw_fact_key": "entitlements"
            }
        }
    ],
    "metadata": {
        "os_release": {
            "source_id": 5,
            "source_name": "S62Source",
            "source_type": "satellite",
            "raw_fact_key": "os_release"
        },
        "cpu_count": {
            "source_id": 4,
            "source_name": "NetworkSource",
            "source_type": "network",
            "raw_fact_key": "os_release"
        }
    },
    "sources": [
        {
            "id": 4,
            "source_type": "network",
            "name": "NetworkSource"
        },
        {
            "id": 5,
            "source_type": "satellite",
            "name": "S62Source"
        }
    ]
}
```


지문의 처음 몇 줄은 운영 체제 및 CPU에 대한 팩트를 포함하여 시스템에 대한 팩트를 보여줍니다. 이 예제에서 **os_release** 팩트는 설치된 운영 체제를 설명하고 **Red Hat Enterprise Linux Atomic Host 7.4** 로 릴리스됩니다.

다음으로, 지문에 제품 섹션에 설치된 **제품이** 나열됩니다. 제품에는 name, version, presence, metadata 필드가 있습니다. JBoss EAP 섹션의 **presence** 필드에는 **absent** 가 값으로 표시되므로 이 예제의 시스템에는 Red Hat JBoss Enterprise Application Platform이 설치되지 않습니다.

지문에는 권한 섹션에서 해당 시스템에 사용된 **인타이틀먼트** 도 나열됩니다. 목록의 각 자격에는 해당 사실의 원래 소스를 설명하는 이름, ID 및 메타데이터가 있습니다. 예제 지문에서 시스템에는 **Satellite Tools 6.3** 인타이틀먼트가 있습니다.

products 및 **entitlements** 섹션에 있는 메타데이터 필드 외에도 지문에는 시스템 팩트 메타데이터에 사용되는 **metadata** 섹션이 포함되어 있습니다. 각 시스템 팩트에 대해 해당 시스템 팩트의 원래 소스를 식

별하는 지문의 **metadata** 섹션에 해당 항목이 있습니다. 이 예에서는 satellite 소스를 스캔하는 동안 Satellite Server에서 **os_release** 팩트가 감지되었습니다.

마지막으로, 지문은 **sources** 섹션에 이 시스템이 포함된 소스를 나열합니다. 시스템은 하나 이상의 소스에 포함될 수 있습니다. 예를 들어 네트워크 소스와 Satellite 소스를 모두 포함하는 검사의 경우 스캔의 두 부분에서 단일 시스템을 찾을 수 있습니다.

6장. 하이브리드 클라우드 콘솔에 보고서 전송

검사를 실행한 후 cloud.redhat.com의 하이브리드 클라우드 콘솔에 해당 검사에 대한 보고서를 보낼 수 있습니다. 생성 및 보내는 보고서는 세부 정보 보고서 또는 배포 보고서가 아닙니다. 대신 *Insights 보고서*로 알려진 세 번째 유형의 보고서입니다. 이러한 유형의 보고서는 특히 하이브리드 클라우드 콘솔 서비스의 수집에 대해 포맷됩니다.

하이브리드 클라우드 콘솔에 인사이트 보고서를 보낼 때 Red Hat Insights의 인벤토리 서비스와 같이 하이브리드 클라우드 콘솔 서비스에서 보고서 데이터를 수집하고 사용하여 호스트 기반 인벤토리 데이터 및 서브스크립션 사용 데이터를 표시할 수 있습니다.

더 알아보기

Insights 보고서 작업 방법에 대한 자세한 내용은 다음 정보를 참조하십시오.

- 하이브리드 클라우드 콘솔에 인사이트 보고서 다운로드 및 전송

Insights 보고서 개념에 대한 자세한 내용은 다음 정보를 참조하십시오.

- Insights 보고서란 무엇입니까?

6.1. 하이브리드 클라우드 콘솔에 인사이트 보고서 다운로드 및 전송

Red Hat Insights 인벤토리 서비스 및 서브스크립션 서비스와 같은 하이브리드 클라우드 콘솔 서비스에 보고서 데이터를 제공해야 하는 경우 Insights 보고서를 다운로드하여 보냅니다.

이러한 유형의 보고서는 세부 정보 보고서 또는 배포 보고서와 다릅니다. *Insights 보고서*는 배포 보고서와 유사한 데이터가 포함된 검색 보고서이지만 해당 내용과 형식은 하이브리드 클라우드 콘솔 서비스에서 수집 및 사용하도록 특별히 설계되었습니다. 또한 Discovery 그래픽 사용자 인터페이스에서 Insights 보고서를 생성할 수 없습니다. Discovery 명령줄 인터페이스를 사용하여 생성해야 합니다.

사전 요구 사항

Insights 보고서를 다운로드하여 보내려면 다음 요구 사항을 충족해야 합니다.

- 해당 검사에 대한 최신 스캔 작업이 성공적으로 완료되어야 합니다.
- 명령줄 인터페이스에서 다음 절차를 실행할 수 있도록 Discovery 서버와 동일한 시스템에 Discovery 명령줄 인터페이스를 설치해야 합니다. 그래픽 사용자 인터페이스에서 Insights 보고서를 다운로드하여 보낼 수 없습니다.

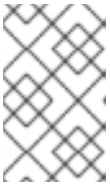
프로세스

1. 명령줄 인터페이스에 로그인합니다. 여기서 ***server_administrator_username*** 은 Discovery 서버 관리자의 사용자 이름이며 ***server_administrator_password*** 는 서버 관리자의 암호입니다.

```
dsc server login --username server_administrator_username --password
server_administrator_password
```

2. Insights 보고서를 만드는 데 사용할 검사 작업의 **report_identifier** (report ID) 값을 찾습니다. 다음 명령은 생성된 모든 검사 오브젝트에 대한 요약 세부 정보를 반환합니다.

```
dsc scan list
```



참고

사용하려는 검사의 이름을 알고 있지만 **report_identifier** 값을 모르는 경우 **qpc scan show --name *scan_name*** 명령을 사용하여 해당 검사에 대한 검사 작업만 표시할 수도 있습니다.

3. 발견한 **report_identifier** 값을 사용하여 검사 작업에 대한 Insights 보고서를 다운로드합니다. 다음 예제 명령에서 다운로드한 보고서에 할당된 파일 이름은 **report.tar.gz** 이지만 필요에 따라 이 파일 이름을 변경할 수 있습니다.

```
dsc report insights --report report_identifier --output-file report.tar.gz
```

4. 일반적으로 Red Hat Customer Portal 계정인 하이브리드 클라우드 콘솔에 로그인하는 데 사용하는 인증 정보를 명령줄 인터페이스 구성에 추가합니다. 다음 단계에서 이러한 인증 정보를 사용하여 Insights 보고서를 하이브리드 클라우드 콘솔에 보낼 수 있도록 하기 위해 이 단계가 필요합니다.

```
dsc insights login
```

5. **publish** 하위 명령을 사용하여 Insights 보고서 데이터를 하이브리드 클라우드 콘솔로 전송하고 인벤토리 서비스 및 서브스크립션 서비스와 같이 보고서를 사용할 수 있는 서비스를 보냅니다.

```
dsc insights publish --input-file report.tar.gz
```

참고

Insights 보고서의 출력을 볼 수 있지만 Discovery 설명서에서는 Insights 보고서 결과를 해석하는 데 도움이 되는 정보를 제공하지 않습니다. 또한 Red Hat 지원은 Discovery 설치 및 사용과 관련된 몇 가지 기본 지원을 제공할 수 있지만 지원 팀은 Insights 보고서를 이해하는 데 도움이 되지 않습니다. Insights 보고서 및 형식은 다양한 하이브리드 클라우드 콘솔 서비스에 데이터를 제공하는 등 Red Hat 내부 프로세스에서 사용하도록 설계되었습니다.

추가 리소스

- Discovery 명령줄 인터페이스 설치 및 구성에 대한 자세한 내용은 Discovery *설치 및 구성* 을 참조하십시오.

6.2. INSIGHTS 보고서란 무엇입니까?

IT 인프라 또는 IT 인프라의 일부를 검사를 실행한 후 Discovery를 사용하여 검사의 데이터로 인사이트 보고서를 생성할 수 있습니다. Insights 보고서는 호스트 기반 인벤토리 데이터 및 서브스크립션 사용 데이터를 표시하기 위해 Red Hat Insights의 인벤토리 서비스와 같이 하이브리드 클라우드 콘솔 서비스로 전송되도록 설계된 특수 보고서입니다.

Discovery는 연결 및 연결이 끊어진 IT 인프라의 모든 부분을 스캔하고 보고하는 데 유용하지만 하이브리드 클라우드 콘솔 서비스에 인사이트 보고서를 보내는 기능은 IT 인프라의 일부가 연결이 끊기거나 무선 적용 가능한 경우 특히 유용합니다. Discovery를 사용하여 네트워크의 해당 부분에 대한 데이터를 수집하면 전체 네트워크에 대한 보다 완전하고 큐레이션된 보기를 얻을 수 있습니다. Insights 보고서의 데이터가 하이브리드 클라우드 콘솔을 지원하는 툴의 다른 데이터 수집과 결합된 경우 통합 인벤토리와 서브스크립션 사용량을 Hybrid Cloud Console이라는 한 곳에서 확인할 수 있습니다.

6.2.1. 보고 빈도

오프라인 및 에어 갭이 있는 모든 시스템은 정기적으로 스캔하고 Insights 보고서를 통해 보고하여 정확한 데이터가 Hybrid Cloud Console에 도달했는지 확인해야 합니다. Insights 보고서를 매주 보내는 것이 현재 권장 사항입니다. 주간 주기로 하는 경우 서브스크립션 서비스의 서브스크립션 사용을 효과적으로 모니터링할 수 있는 충분한 이정표를 제공합니다.

6.2.2. 시스템 중복 방지

Insights 보고서에서 제공하는 데이터 유형에 따라 데이터 마스킹이 보고서의 품질에 영향을 줄 수 있습니다. 특히 보고의 중복 제거 및 병합 프로세스에서 두드러집니다.

예를 들어 Insights 보고서에 IT 인프라의 연결된 부분과 연결이 끊긴 부분에 대한 데이터가 포함되어 있고 해당 보고서에서 데이터를 마스킹하는 경우 Red Hat Satellite 또는 Red Hat Insights와 같은 다른 방법을 통해 보고되는 연결된 시스템이 중복됩니다. 따라서 Red Hat Insights, Satellite, Red Hat Subscription Management 또는 유사한 툴을 통해 직접 보고되는 시스템이 이미 있는 경우 인사이트 보고서를 생성할 때 시스템을 구분하는 데 도움이 되는 호스트 이름, IP 주소 및 유사한 사실을 마스킹하지 않아야 합니다.

일반적으로 IT 인프라의 연결이 끊긴 부분만 다루는 검사 또는 연결이 끊긴 고객의 경우 100 % 연결이 끊긴 고객의 경우 마스킹은 일관된 해시 값을 사용하는 경우 선택 사항입니다. 그러나 마스킹은 권장되지 않습니다. 마스킹은 개별 시스템을 구분하는 데 사용되는 정보 유형을 제거하므로 마스킹을 사용하면 Red Hat Insights 및 서브스크립션 서비스와 같은 기타 하이브리드 클라우드 콘솔 툴에서 제공하는 대부분의 이점을 얻을 수 없습니다.

RED HAT 문서에 관한 피드백 제공

문서 개선을 위한 의견에 감사드립니다. 피드백을 제공하려면 문제를 설명하는 Jira 문제를 엽니다. 요청을 신속하게 처리할 수 있도록 가능한 한 자세한 정보를 제공하십시오.

사전 요구 사항

- Red Hat 고객 포털 계정이 있어야 합니다. 이 계정을 사용하면 Red Hat Jira Software 인스턴스에 로그인할 수 있습니다. 계정이 없는 경우 계정을 생성하라는 메시지가 표시됩니다.

프로세스

피드백을 제공하려면 다음 단계를 수행합니다.

1. 다음 링크를 클릭합니다. 문제 만들기.
2. **요약** 텍스트 상자에 문제에 대한 간략한 설명을 입력합니다.
3. **설명** 텍스트 상자에 문제에 대한 자세한 내용을 제공합니다. 문제를 발견한 URL을 포함합니다.
4. 기타 필수 필드에 대한 정보를 제공합니다. 기본 정보가 포함된 모든 필드가 기본값으로 유지되도록 허용합니다.
5. **생성** 을 클릭하여 문서 팀에 대한 Jira 문제를 생성합니다.

문서 문제가 생성되고 적절한 문서 팀으로 라우팅됩니다. 피드백을 제공하기 위해 시간을 내어 주셔서 감사합니다.