스토리지 시스템을 검색합니다

SANtricity 11.6

NetApp
February 12, 2024

목차

스토리지 시스템을 검색합니다 1
개념 1
방법 2

스토리지 시스템을 검색합니다

개념

스토리지 검색 시 고려 사항

SANtricity Unified Manager가 스토리지 리소스를 표시하고 관리하기 전에 먼저 조직의 네트워크에서 관리할 스토리지 어레이를 검색해야 합니다. 여러 어레이를 검색할 수도 있고 단일 어레이를 검색할 수도 있습니다.

여러 스토리지 시스템을 검색하는 중입니다

여러 어레이를 검색하도록 선택한 경우 네트워크 IP 주소 범위를 입력한 다음 Unified Manager가 해당 범위의 각 IP 주소에 대한 개별 연결을 시도합니다. 성공적으로 도달한 스토리지 배열이 * Discover * 페이지에 나타나고 관리 도메인에 추가될 수 있습니다.

단일 스토리지 시스템 검색

단일 어레이를 검색하도록 선택한 경우 스토리지 어레이에서 컨트롤러 중 하나에 대한 단일 IP 주소를 입력한 다음 개별 스토리지 어레이가 추가됩니다.

> Unified Manager는 컨트롤러에 할당된 범위 내에서 단일 IP 주소 또는 IP 주소만 검색하여 표시합니다. 이 단일 IP 주소 또는 IP 주소 범위를 벗어나는 컨트롤러에 할당된 대체 컨트롤러 또는 IP 주소가 있는 경우 Unified Manager는 이를 검색 또는 표시하지 않습니다. 그러나 스토리지 배열을 추가하면 연결된 모든 IP 주소가 검색되어 * Manage * (관리 *) 보기에 표시됩니다.

사용자 자격 증명

검색 프로세스 중에 추가할 각 스토리지 배열에 대해 관리자 암호를 제공해야 합니다.

웹 서비스 인증서

검색 프로세스의 일부로 Unified Manager는 검색된 스토리지 시스템이 신뢰할 수 있는 소스의 인증서를 사용하고 있는지 확인합니다. Unified Manager에서는 브라우저에 설정한 모든 연결에 대해 두 가지 유형의 인증서 기반 인증을 사용합니다.

- * 신뢰할 수 있는 인증서 *

  Unified Manager에서 검색된 스토리지의 경우 인증 기관에서 제공하는 신뢰할 수 있는 인증서를 추가로 설치해야 할 수 있습니다.

  이러한 인증서를 가져오려면 * 가져오기 * 버튼을 사용합니다. 이전에 이 어레이에 연결한 경우 하나 또는 두 컨트롤러 인증서 중 하나가 만료되었거나 해지되었거나 인증서 체인에 루트 인증서 또는 중간 인증서가 누락되었습니다. 스토리지 배열을 관리하기 전에 만료되었거나 해지된 인증서를 교체하거나 누락된 루트 인증서 또는 중간 인증서를 추가해야 합니다.

- * 자체 서명된 인증서 *

  자체 서명된 인증서도 사용할 수 있습니다. 관리자가 서명된 인증서를 가져오지 않고 어레이를 검색하려고 하면

Unified Manager에 관리자가 자체 서명된 인증서를 수락할 수 있는 오류 대화 상자가 표시됩니다. 스토리지 시스템의 자체 서명된 인증서가 신뢰할 수 있는 것으로 표시되고 스토리지 시스템이 Unified Manager에 추가됩니다.

스토리지 배열에 대한 연결을 신뢰하지 않는 경우, Unified Manager에 스토리지 배열을 추가하기 전에 * Cancel * 을 선택하고 스토리지 배열의 보안 인증서 전략을 확인합니다.

방법

여러 스토리지 시스템을 검색합니다

여러 어레이를 검색하여 관리 서버가 있는 서브넷에서 모든 스토리지 어레이를 검색하고 검색된 어레이를 관리 도메인에 자동으로 추가합니다.

이 작업에 대해

여러 어레이를 검색하려면 다음 단계를 수행하십시오.

1단계**:** 네트워크 주소를 입력합니다

로컬 하위 네트워크에서 검색할 네트워크 주소 범위를 입력합니다. 성공적으로 도달한 스토리지 배열이 * Discover * 페이지에 나타나고 관리 도메인에 추가될 수 있습니다.

이 작업에 대해

어떤 이유로든 검색 작업을 중지해야 하는 경우 * 검색 중지 * 를 클릭합니다.

단계

1. Manage * 페이지에서 * Add/Discover * 를 선택합니다.

   스토리지 시스템 추가/검색 대화 상자가 나타납니다.

2. 네트워크 범위 내의 모든 스토리지 배열 검색 * 라디오 버튼을 선택합니다.
3. 로컬 하위 네트워크를 검색할 시작 네트워크 주소와 끝 네트워크 주소를 입력한 다음 * 검색 시작 * 을 클릭합니다.

   검색 프로세스가 시작됩니다. 이 검색 프로세스를 완료하는 데 몇 분 정도 걸릴 수 있습니다. 스토리지 배열이 검색되면 * Discover * 페이지의 표가 채워집니다.

   관리 가능한 어레이가 검색되지 않으면 스토리지 어레이가 네트워크에 올바르게 연결되어 있고 할당된 주소가 범위 내에 있는지 확인합니다. 새 검색 매개변수 * 를 클릭하여 * 추가/검색 * 페이지로 돌아갑니다.

4. 검색된 스토리지 시스템의 목록을 검토합니다.
5. 관리 도메인에 추가할 스토리지 배열 옆의 확인란을 선택하고 * 다음 * 을 클릭합니다.

   SANtricity Unified Manager는 관리 도메인에 추가할 각 스토리지에 대해 자격 증명 검사를 수행합니다. 해당 배열과 연결된 자체 서명된 인증서 및 신뢰할 수 없는 인증서를 확인해야 할 수 있습니다.

6. 마법사의 다음 단계로 진행하려면 * Next * (다음 *)를 클릭합니다.
7. 로 이동합니다 2단계: 검색 중에 자체 서명된 인증서 해결.

2단계**:** 검색 중에 자체 서명된 인증서 해결

검색 프로세스의 일부로 시스템은 스토리지 어레이가 신뢰할 수 있는 소스의 인증서를 사용하고 있는지 확인합니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다.

단계

1. 다음 중 하나를 수행합니다.
   - 검색된 스토리지 배열에 대한 접속을 신뢰할 수 있는 경우 마법사의 다음 카드로 계속 진행합니다. 자체 서명된 인증서가 신뢰할 수 있는 것으로 표시되고 스토리지 시스템이 SANtricity Unified Manager에 추가됩니다.
   - 스토리지 어레이에 대한 연결을 신뢰할 수 없는 경우 * Cancel * 을 선택하고 각 스토리지 어레이의 보안 인증서 전략을 확인한 다음 Unified Manager에 추가합니다.
2. 마법사의 다음 단계로 진행하려면 * Next * (다음 *)를 클릭합니다.
3. 로 이동합니다 3단계: 검색 중에 신뢰할 수 없는 인증서를 해결합니다.

3단계**:** 검색 중에 신뢰할 수 없는 인증서를 해결합니다

신뢰할 수 없는 인증서는 스토리지 어레이에서 SANtricity Unified Manager에 대한 보안 연결을 설정하려고 시도하지만 연결이 보안으로 확인하지 못할 때 발생합니다. 어레이 검색 프로세스 중에 신뢰할 수 있는 타사에서 발급한 CA(인증 기관) 인증서 또는 CA 서명 인증서를 가져와 신뢰할 수 없는 인증서를 해결할 수 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다.
- 스토리지 배열의 각 컨트롤러에 대한 인증서 서명 요청(.csr 파일)을 생성하여 CA로 보냈습니다.
- CA가 신뢰할 수 있는 인증서 파일을 반환했습니다.
- 인증서 파일은 로컬 시스템에서 사용할 수 있습니다.

이 작업에 대해

다음 중 하나라도 해당되는 경우 신뢰할 수 있는 CA 인증서를 추가로 설치해야 할 수 있습니다.

- 최근에 스토리지 배열을 추가했습니다.
- 하나 이상의 인증서가 만료되었습니다.
- 하나 이상의 인증서가 해지되었습니다.
- 하나 이상의 인증서에 루트 또는 중간 인증서가 없습니다.

단계

1. 신뢰할 수 없는 인증서를 확인할 스토리지 배열 옆의 확인란을 선택한 다음 * 가져오기 * 버튼을 선택합니다.

   신뢰할 수 있는 인증서 파일을 가져올 수 있는 대화 상자가 열립니다.

2. Browse * 를 클릭하여 스토리지 배열에 대한 인증서 파일을 선택합니다.

   대화 상자에 파일 이름이 표시됩니다.

3. 가져오기 * 를 클릭합니다.

파일이 업로드되고 검증됩니다.

신뢰할 수 없는 인증서 문제가 해결되지 않은 스토리지 어레이는 Unified Manager에 추가되지 않습니다.

4. 마법사의 다음 단계로 진행하려면 * Next * (다음 *)를 클릭합니다.
5. 로 이동합니다 4단계: 암호를 입력합니다.

4단계**:** 암호를 입력합니다

관리 도메인에 추가할 스토리지 배열에 대한 암호를 입력해야 합니다.

시작하기 전에

- 스토리지 배열이 올바르게 설정 및 구성되어 있어야 합니다.
- 스토리지 배열 암호는 SANtricity 시스템 관리자의 * 액세스 관리 * 타일을 사용하여 설정해야 합니다.

단계

1. SANtricity Unified Manager에 추가할 각 스토리지 어레이의 암호를 입력합니다.
2. * 선택 사항: * 그룹에 스토리지 어레이 연결: 드롭다운 목록에서 선택한 스토리지 어레이와 연결할 그룹을 선택합니다.
3. 마침 * 을 클릭합니다.

작업을 마친 후

스토리지 배열이 관리 도메인에 추가되고 선택한 그룹에 연결됩니다(지정된 경우).

Unified Manager가 지정된 스토리지 어레이에 연결하는 데 몇 분 정도 걸릴 수 있습니다.

단일 스토리지를 검색합니다

단일 스토리지 배열 추가/검색 옵션을 사용하여 조직의 네트워크에 단일 스토리지 배열을 수동으로 검색하고 추가합니다.

시작하기 전에

- 스토리지 배열이 올바르게 설정 및 구성되어 있어야 합니다.
- 스토리지 배열 암호는 SANtricity 시스템 관리자의 액세스 관리 타일을 사용하여 설정해야 합니다.

단계

1. Manage * 페이지에서 * Add/Discover * 를 선택합니다.

   스토리지 배열 추가/검색 * 대화 상자가 나타납니다.

2. Discover a single storage array * 라디오 버튼을 선택합니다.
3. 스토리지 배열에 있는 컨트롤러 중 하나의 IP 주소를 입력한 다음 * 검색 시작 * 을 클릭합니다.

   SANtricity Unified Manager가 지정된 스토리지 어레이에 연결하는 데 몇 분 정도 걸릴 수 있습니다.

지정된 컨트롤러의 IP 주소에 대한 연결이 실패하면 * 스토리지 어레이에 액세스할 수 없음 * 메시지가 나타납니다.

4. 메시지가 표시되면 자체 서명된 인증서를 모두 해결합니다.

   검색 프로세스의 일부로 검색된 스토리지 시스템이 신뢰할 수 있는 소스의 인증서를 사용하고 있는지 확인합니다. 스토리지 배열에 대한 디지털 인증서를 찾을 수 없는 경우 보안 예외를 추가하여 CA(인증 기관)에서 서명하지 않은 인증서를 확인하라는 메시지가 표시됩니다.

5. 메시지가 나타나면 신뢰할 수 없는 인증서를 모두 확인합니다.

   신뢰할 수 없는 인증서는 스토리지 어레이에서 SANtricity Unified Manager에 대한 보안 연결을 설정하려고 시도하지만 연결이 보안으로 확인하지 못할 때 발생합니다. 신뢰할 수 있는 제3자가 발급한 CA(인증 기관) 인증서를 가져와 신뢰할 수 없는 인증서를 해결합니다.

6. 다음 * 을 클릭합니다.
7. * 선택 사항: * 검색된 스토리지 배열을 그룹에 연결: 드롭다운 목록에서 스토리지 배열에 연결할 그룹을 선택합니다.

   기본적으로 "모두" 그룹이 선택됩니다.

8. 관리 도메인에 추가할 스토리지 배열의 관리자 암호를 입력한 다음 * 확인 * 을 클릭합니다.

작업을 마친 후

스토리지 어레이가 SANtricity Unified Manager에 추가되고 지정된 경우 선택한 그룹에 추가됩니다.

자동 지원 데이터 수집이 설정된 경우 추가하는 스토리지 배열에 대한 지원 데이터가 자동으로 수집됩니다.

저작권 정보

상표 정보