관리 및 모니터링

ASA r2

NetApp
September 26, 2024

목차

관리 및 모니터링

ASA R2 스토리지 시스템에서 스토리지 VM에 대한 클라이언트 액세스를 관리합니다

ASA R2 시스템의 스토리지 유닛은 스토리지 가상 머신(VM) 내에 포함됩니다. 스토리지 VM은 SAN 클라이언트에 데이터를 제공하는 데 사용됩니다. ONTAP System Manager를 사용하여 SAN 클라이언트가 스토리지 VM에 연결하고 스토리지 유닛의 데이터에 액세스할 수 있도록 LIF(네트워크 인터페이스)를 생성합니다. 선택적으로 서브넷을 사용하여 LIF 생성을 단순화하고 IPspace를 사용하여 스토리지 VM에 자체적인 보안 스토리지, 관리 및 라우팅을 제공할 수 있습니다.

IPspace 생성

IPspace는 스토리지 VM이 상주하는 별개의 IP 주소 공간입니다. IPspace를 생성하면 스토리지 VM이 자체적인 보안 스토리지, 관리 및 라우팅을 확보할 수 있습니다. 또한 관리자가 분리된 네트워크 도메인의 클라이언트가 동일한 IP 주소 서브넷 범위의 겹치는 IP 주소를 사용할 수 있도록 합니다.

서브넷을 생성하기 전에 IPspace를 생성해야 합니다.

단계

1. 네트워크 > 개요 * 를 선택합니다.
2. IPspaces * 아래에서 를 선택합니다 + Add .
3. IPspace의 이름을 입력하거나 기본 이름을 그대로 사용합니다.

   "ALL"은 시스템이 예약된 이름이므로 IPspace 이름은 "ALL"일 수 없습니다.

4. 저장 * 을 선택합니다.

다음 단계

이제 IPspace를 생성했으므로 이 IPspace를 사용하여 서브넷을 만들 수 있습니다.

서브넷을 생성합니다

서브넷을 사용하면 LIF(네트워크 인터페이스)를 생성할 때 사용할 IPv4 또는 IPv6 주소의 특정 블록을 할당할 수 있습니다. 서브넷을 사용하면 각 LIF에 대한 특정 IP 주소 및 네트워크 마스크 대신 서브넷 이름을 지정할 수 있어 LIF 생성이 단순화됩니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- "브로드캐스트 도메인"서브넷을 추가하려는 및 IPspace가 이미 있어야 합니다.

단계

1. 네트워크 > 개요 * 를 선택합니다.
2. 서브넷 * 을 선택한 다음 을 + Add 선택합니다.

3. 서브넷 이름을 입력합니다.

   모든 서브넷 이름은 IPspace 내에서 고유해야 합니다.

4. 서브넷 IP 주소와 서브넷 마스크를 입력합니다.
5. 서브넷의 IP 주소 범위를 지정합니다.

   서브넷의 IP 주소 범위를 지정할 때 IP 주소를 다른 서브넷과 겹치지 마십시오. 네트워크 문제는 서브넷 IP 주소가 중복되고 다른 서브넷이나 호스트가 동일한 IP 주소를 사용하려고 할 때 발생할 수 있습니다.

6. 서브넷의 브로드캐스트 도메인을 선택합니다.
7. 추가 * 를 선택합니다.

다음 단계

LIF 생성을 단순화하는 데 사용할 수 있는 서브넷을 생성했습니다.

LIF(네트워크 인터페이스) 생성

LIF(네트워크 인터페이스)는 물리적 포트 또는 논리적 포트와 연결된 IP 주소입니다. 데이터에 액세스하는 데 사용할 포트에 LIF를 생성합니다. 스토리지 VM은 하나 이상의 LIF를 통해 클라이언트에 데이터를 제공합니다. 구성 요소 장애가 발생하는 경우 LIF가 페일오버되거나 다른 물리적 포트로 마이그레이션되어 네트워크 통신이 중단되지 않습니다.

IP 데이터 LIF가 생성되면 기본적으로 iSCSI 및 NVMe/TCP 트래픽을 모두 처리할 수 있습니다. FC 및 NVMe/FC 트래픽에는 대해 별도의 데이터 LIF를 생성해야 합니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 기본 물리적 또는 논리적 네트워크 포트가 관리 `up` 상태로 구성되어야 합니다.
- 서브넷 이름을 사용하여 LIF에 대한 IP 주소 및 네트워크 마스크 값을 할당하려는 경우, 서브넷이 이미 존재해야 합니다.
- 클러스터 간 노드 트래픽을 처리하는 LIF는 LIF가 관리 트래픽을 처리하거나 데이터 트래픽을 처리하는 LIF와 같은 서브넷에 있으면 안 됩니다.

단계

1. 네트워크 > 개요 * 를 선택합니다.
2. 네트워크 인터페이스 * 를 선택한 다음 를 + Add 선택합니다.
3. 인터페이스 유형과 프로토콜을 선택한 다음 스토리지 VM을 선택합니다.
4. LIF의 이름을 입력하거나 기본 이름을 그대로 사용합니다.
5. 네트워크 인터페이스의 홈 노드를 선택한 다음 IP 주소와 서브넷 마스크를 입력합니다.
6. 저장 * 을 선택합니다.

결과

데이터 액세스를 위한 LIF를 생성했습니다.

LIF(네트워크 인터페이스) 수정

LIF는 필요에 따라 사용하지 않도록 설정하거나 이름을 바꿀 수 있습니다. LIF IP 주소 및 서브넷 마스크를 변경할 수도 있습니다.

단계

1. 네트워크 > 개요 * 를 선택한 다음 * 네트워크 인터페이스 * 를 선택합니다.
2. 편집할 네트워크 인터페이스 위로 마우스를 가져간 다음 을 선택합니다.
3. 편집 * 을 선택합니다.
4. 네트워크 인터페이스를 비활성화하거나, 네트워크 인터페이스의 이름을 바꾸거나, IP 주소를 변경하거나, 서브넷 마스크를 변경할 수 있습니다.
5. 저장 * 을 선택합니다.

결과

LIF가 수정되었습니다.

ASA R2 스토리지 시스템에서 클러스터 네트워킹을 관리합니다

ONTAP System Manager를 사용하여 ASA R2 시스템에서 기본적인 스토리지 네트워크 관리를 수행할 수 있습니다. 예를 들어 브로드캐스트 도메인을 추가하거나 다른 브로드캐스트 도메인에 포트를 재할당할 수 있습니다.

브로드캐스트 도메인을 추가합니다

브로드캐스트 도메인을 사용하면 동일한 계층 2 네트워크에 속하는 네트워크 포트를 그룹화하여 클러스터 네트워크 관리를 간소화할 수 있습니다. 그러면 VM(스토리지 가상 머신)이 데이터 또는 관리 트래픽에 그룹의 포트를 사용할 수 있습니다.

클러스터 설정 중에 "기본" 브로드캐스트 도메인 및 "클러스터" 브로드캐스트 도메인이 생성됩니다. "기본" 브로드캐스트 도메인에는 "기본" IPspace에 있는 포트가 포함되어 있습니다. 이러한 포트는 주로 데이터를 제공하는 데 사용됩니다. 클러스터 관리 및 노드 관리 포트도 이 브로드캐스트 도메인에 있습니다. "클러스터" 브로드캐스트 도메인에는 "클러스터" IPspace에 있는 포트가 포함되어 있습니다. 이러한 포트는 클러스터 통신에 사용되며 클러스터의 모든 노드에 있는 모든 클러스터 포트를 포함합니다.

클러스터가 초기화된 후 추가 브로드캐스트 도메인을 생성할 수 있습니다. 브로드캐스트 도메인을 생성하면 동일한 포트가 포함된 페일오버 그룹이 자동으로 생성됩니다.

이 작업에 대해

브로드캐스트 도메인에 추가된 포트의 MTU(Maximum Transmission Unit)가 브로드캐스트 도메인에 설정된 MTU 값으로 업데이트됩니다.

단계

1. System Manager에서 * 네트워크 > 개요 * 를 선택합니다.
2. 브로드캐스트 * 도메인 아래에서 를 선택합니다 + Add .
3. 브로드캐스트 도메인의 이름을 입력하거나 기본 이름을 그대로 사용합니다.

   모든 브로드캐스트 도메인 이름은 IPspace 내에서 고유해야 합니다.

4. 브로드캐스트 도메인의 IPspace를 선택합니다.

   IPspace 이름을 지정하지 않으면 브로드캐스트 도메인이 "기본" IPspace에 만들어집니다.

5. MTU(Maximum Transmission Unit)를 입력합니다.

   MTU는 브로드캐스트 도메인에서 허용할 수 있는 가장 큰 데이터 패킷입니다.

6. 원하는 포트를 선택한 다음 * 저장 * 을 선택합니다.

결과

새 브로드캐스트 도메인을 추가했습니다.

포트를 다른 브로드캐스트 도메인에 재할당합니다

포트는 하나의 브로드캐스트 도메인에만 속할 수 있습니다. 포트가 속한 브로드캐스트 도메인을 변경하려면 포트를 기존 브로드캐스트 도메인에서 새 브로드캐스트 도메인으로 재할당해야 합니다.

단계

1. System Manager에서 * 네트워크 > 개요 * 를 선택합니다.
2. 브로드캐스트 도메인 * 에서 ⋮ 도메인 이름 옆에 있는 을 선택한 다음 * 편집 * 을 선택합니다.
3. 다른 도메인에 재할당할 이더넷 포트의 선택을 취소합니다.
4. 포트를 재할당할 브로드캐스트 도메인을 선택한 다음 * 재할당 * 을 선택합니다.
5. 저장 * 을 선택합니다.

결과

포트를 다른 브로드캐스트 도메인에 다시 할당했습니다.

VLAN을 생성합니다

VLAN은 브로드캐스트 도메인으로 그룹화된 스위치 포트로 구성됩니다. VLAN을 사용하면 보안을 강화하고, 문제를 격리하고, IP 네트워크 인프라 내에서 사용 가능한 경로를 제한할 수 있습니다.

시작하기 전에

네트워크에 배포된 스위치는 IEEE 802.1Q 표준을 준수하거나 공급업체별로 VLAN을 구현해야 합니다.

이 작업에 대해

- 구성원 포트가 없는 인터페이스 그룹 포트에는 VLAN을 만들 수 없습니다.
- 처음으로 포트를 통해 VLAN을 구성할 때 포트가 다운되어 일시적으로 네트워크 연결이 끊길 수 있습니다. 이후에 동일한 포트에 VLAN을 추가해도 포트 상태는 영향을 받지 않습니다.
- 스위치의 네이티브 VLAN과 ID가 동일한 네트워크 인터페이스에 VLAN을 생성해서는 안 됩니다. 예를 들어, 네트워크 인터페이스 e0b가 네이티브 VLAN 10에 있는 경우 해당 인터페이스에 VLAN e0b-10을 생성할 수 없습니다.

단계

1. System Manager에서 * 네트워크 > 이더넷 포트 * 를 선택한 다음 를 선택합니다 + VLAN.

2. VLAN에 대한 노드와 브로드캐스트 도메인을 선택합니다.
3. VLAN의 포트를 선택합니다.

   클러스터 LIF를 호스팅하는 포트 또는 클러스터 IPspace에 할당된 포트에 VLAN을 연결할 수 없습니다.

4. VLAN ID를 입력합니다.
5. 저장 * 을 선택합니다.

결과

보안을 강화하고, 문제를 격리하고, IP 네트워크 인프라 내에서 사용 가능한 경로를 제한하기 위해 VLAN을 만들었습니다.

사용량을 모니터링하고 용량을 늘립니다

ASA R2 스토리지 시스템에서 클러스터 및 스토리지 유닛 성능을 모니터링합니다

ONTAP System Manager를 사용하여 클러스터의 전반적인 성능과 특정 스토리지 유닛의 성능을 모니터링하여 지연 시간, IOPS 및 처리량이 중요 비즈니스 애플리케이션에 미치는 영향을 파악할 수 있습니다. 성능은 1시간에서 1년까지 다양한 기간 동안 모니터링할 수 있습니다.

예를 들어, 중요한 애플리케이션에서 높은 지연 시간과 낮은 처리량이 발생한다고 가정합니다. 지난 5일(영업일 기준) 동안 클러스터 성능을 볼 때 매일 동시에 성능이 저하된다는 것을 알 수 있습니다. 이 정보를 사용하여 중요하지 않은 프로세스가 백그라운드에서 실행되기 시작할 때 중요한 애플리케이션이 클러스터 리소스를 두고 경합하고 있는지 확인합니다. 그런 다음 QoS 정책을 수정하여 중요하지 않은 워크로드가 시스템 리소스에 미치는 영향을 제한하고 중요 워크로드가 최소 처리량 목표를 충족하도록 할 수 있습니다.

클러스터 성능을 모니터링합니다

클러스터 성능 메트릭을 사용하여 지연 시간을 최소화하고 중요 애플리케이션의 IOPS 및 처리량을 극대화하기 위해 워크로드를 이동해야 하는지 여부를 결정할 수 있습니다.

단계

1. System Manager에서 * 대시보드 * 를 선택합니다.
2. Performance * 에서 클러스터의 지연 시간, IOPS 및 처리량을 시간, 일, 주, 월 또는 연도별로 확인합니다.
3. 성능 데이터를 다운로드하려면 선택합니다.

다음 단계

클러스터 성능 메트릭을 사용하여 QoS 정책을 수정하거나 애플리케이션 워크로드를 조정할 필요가 있는지 분석하여 전체 클러스터 성능을 극대화할 수 있습니다.

스토리지 유닛 성능을 모니터링합니다

스토리지 유닛 성능 메트릭을 사용하여 특정 애플리케이션이 지연 시간, IOPS 및 처리량에 미치는 영향을 확인합니다.

단계

1. System Manager에서 * Storage * 를 선택합니다.
2. 모니터링할 스토리지 유닛을 선택한 다음 * Overview * 를 선택합니다.
3. Performance * 에서 시간, 일, 주, 월 또는 연도별로 스토리지 유닛의 지연 시간, IOPS 및 처리량을 확인합니다.
4. 성능 데이터를 다운로드하려면 선택합니다.

다음 단계

스토리지 유닛 성능 메트릭을 사용하여 스토리지 유닛에 할당된 QoS 정책을 수정해야 하는지 여부를 분석하여 지연 시간을 줄이고 IOPS 및 처리량을 극대화합니다.

ASA R2 스토리지 시스템에서 클러스터 및 스토리지 유닛 활용도를 모니터링합니다

ONTAP System Manager를 사용하여 스토리지 활용률을 모니터링하여 현재 및 미래의 워크로드를 처리하는 데 필요한 스토리지 용량을 확보하십시오.

클러스터 활용률을 모니터링합니다

클러스터에서 사용하는 스토리지 양을 정기적으로 모니터링하여 필요한 경우 공간이 부족해지기 전에 클러스터 용량을 확장할 준비가 되었는지 확인합니다.

단계

1. System Manager에서 * 대시보드 * 를 선택합니다.
2. Capacity * 에서 클러스터에서 사용된 물리적 공간의 양과 사용 가능한 공간의 양을 확인합니다.

   데이터 축소율은 스토리지 효율성을 통해 절약되는 공간의 양을 나타냅니다.

다음 단계

클러스터에 공간이 부족하거나 향후 요구 사항을 충족할 수 있는 용량이 없는 경우 "새 드라이브를 추가합니다"ASA R2 시스템을 구축하여 스토리지 용량을 늘려야 합니다.

스토리지 유닛 사용률을 모니터링합니다

스토리지 유닛에서 사용하는 스토리지 양을 모니터링하여 비즈니스 요구 사항에 따라 스토리지 유닛의 크기를 사전에 늘릴 수 있습니다.

단계

1. System Manager에서 * Storage * 를 선택합니다.
2. 모니터링할 스토리지 유닛을 선택한 다음 * Overview * 를 선택합니다.
3. 스토리지 * 에서 다음을 확인합니다.
   - 저장 장치의 크기입니다
   - 사용된 공간의 양입니다
   - 데이터 축소율

     데이터 축소율은 스토리지 효율성을 통해 절약된 공간의 양을 나타냅니다

◦ 스냅샷이 사용되었습니다

사용된 스냅샷은 스냅샷에 사용되는 스토리지의 양을 나타냅니다.

다음 단계

저장 장치 용량이 거의 다 되면 "스토리지 유닛을 수정합니다"크기를 늘려야 합니다.

ASA R2 스토리지 시스템에서 스토리지 용량을 늘립니다

노드나 쉘프에 드라이브를 추가하여 ASA R2 시스템의 스토리지 용량을 늘립니다.

NetApp Hardware Universe를 사용하여 새 드라이브 설치를 준비합니다

새 드라이브를 노드 또는 쉘프에 설치하기 전에 NetApp Hardware Universe를 사용하여 추가하려는 드라이브가 ASA R2 플랫폼에서 지원되는지 확인하고 새 드라이브에 대한 올바른 슬롯을 식별하십시오. 드라이브를 추가할 수 있는 올바른 슬롯은 플랫폼 모델과 ONTAP 버전에 따라 다릅니다. 경우에 따라 특정 슬롯에 순차적으로 드라이브를 추가해야 할 수도 있습니다.

단계

1. 로 이동합니다"NetApp Hardware Universe를 참조하십시오".
2. 제품 * 에서 하드웨어 구성을 선택합니다.
3. ASA R2 플랫폼을 선택합니다.
4. ONTAP 버전을 선택한 다음 * 결과 표시 * 를 선택합니다.
5. 그래픽 아래에서 * 대체 보기를 보려면 여기를 클릭하십시오 * 를 선택한 다음 구성과 일치하는 보기를 선택하십시오.
6. 구성 보기를 사용하여 새 드라이브가 지원되는지, 올바른 설치 슬롯이 지원되는지 확인합니다.

결과

새 드라이브가 지원되는지 확인했으며 설치에 적합한 슬롯을 알고 있습니다.

ASA R2에 새 드라이브를 설치합니다

단일 절차에서 추가해야 하는 최소 드라이브 수는 6개입니다. 단일 드라이브를 추가하면 성능이 저하될 수 있습니다.

이 작업에 대해

각 드라이브에 대해 이 절차의 단계를 반복해야 합니다.

단계

1. 적절하게 접지합니다.
2. 플랫폼 전면에서 베젤을 조심스럽게 분리합니다.
3. 새 드라이브를 올바른 슬롯에 삽입합니다.
   a. 캠 핸들이 열린 위치에 있는 상태에서 두 손을 사용하여 새 드라이브를 삽입합니다.
   b. 드라이브가 멈출 때까지 누릅니다.
   c. 드라이브가 중간 평면에 완전히 장착되고 핸들이 제자리에 고정되도록 캠 핸들을 닫습니다.

캠 핸들이 드라이브 면과 올바르게 정렬되도록 캠 핸들을 천천히 닫아야 합니다.

4. 드라이브의 작동 LED(녹색)가 켜져 있는지 확인합니다.
   - LED가 켜져 있으면 드라이브에 전원이 들어옵니다.
   - LED가 깜박이면 드라이브에 전원이 들어오고 I/O가 진행 중인 것입니다. 드라이브 펌웨어를 업데이트하는 경우에도 LED가 깜박입니다.

     현재 펌웨어 버전이 없는 새 드라이브에서 드라이브 펌웨어가 중단 없이 자동으로 업데이트됩니다.
5. 노드가 드라이브 자동 할당으로 구성되어 있는 경우 ONTAP가 새 드라이브를 노드에 자동으로 할당할 때까지 기다릴 수 있습니다. 노드가 드라이브 자동 할당으로 구성되지 않았거나 원하는 경우 드라이브를 수동으로 할당할 수 있습니다.

   새 드라이브는 노드에 할당될 때까지 인식되지 않습니다.

다음 단계

새 드라이브가 인식되면 드라이브가 추가되었고 소유권이 올바르게 지정되었는지 확인합니다.

ASA R2 스토리지 시스템에서 펌웨어를 업데이트합니다

ONTAP는 기본적으로 ASA R2 시스템에서 펌웨어 및 시스템 파일을 자동으로 다운로드하고 업데이트합니다. 권장 업데이트를 다운로드하여 설치하기 전에 유연하게 확인할 수 있는 경우 ONTAP System Manager를 사용하여 자동화된 업데이트를 사용하지 않도록 설정하거나 업데이트 매개 변수를 편집하여 작업을 수행하기 전에 사용 가능한 업데이트 알림을 표시할 수 있습니다.

자동 업데이트를 활성화합니다

스토리지 펌웨어, SP/BMC 펌웨어 및 시스템 파일에 대한 권장 업데이트는 기본적으로 ASA R2 시스템에 자동으로 다운로드되고 설치됩니다. 자동 업데이트를 사용하지 않도록 설정한 경우 기본 동작을 복원하도록 설정할 수 있습니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 자동 업데이트 * 옆에 있는 * 를 선택한 ⋮ 다음 * 사용 * 을 선택합니다.
3. EULA를 읽고 동의합니다.
4. 기본값을 그대로 사용하여 펌웨어 및 시스템 파일을 자동으로 업데이트합니다. 필요한 경우 알림을 표시하거나 권장 업데이트를 자동으로 해제하려면 을 선택합니다.
5. 업데이트 수정이 모든 현재 및 향후 업데이트에 적용됨을 확인하려면 선택합니다.
6. 저장 * 을 선택합니다.

결과

업데이트 선택 항목에 따라 권장 업데이트가 자동으로 다운로드되고 ASA R2 시스템에 설치됩니다.

자동 업데이트를 비활성화합니다

권장 업데이트를 설치하기 전에 유연하게 볼 수 있도록 하려면 자동 업데이트를 사용하지 않도록 설정합니다. 자동 업데이트를 비활성화하는 경우 펌웨어 및 시스템 파일 업데이트를 수동으로 수행해야 합니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 자동 업데이트 * 옆에 있는 * 를 선택한 ⋮ 다음 * 사용 안 함 * 을 선택합니다.

결과

자동 업데이트를 사용할 수 없습니다. 권장 업데이트를 정기적으로 확인하고 수동 설치를 수행할지 결정해야 합니다.

자동 업데이트를 봅니다

클러스터에 다운로드되고 자동 설치가 예약된 펌웨어 및 시스템 파일 업데이트 목록을 봅니다. 이전에 자동으로 설치된 업데이트도 볼 수 있습니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 자동 업데이트 * 옆에 있는 * 를 선택한 ⋮ 다음 * 모든 자동 업데이트 보기 * 를 선택합니다.

자동 업데이트를 편집합니다

스토리지 펌웨어, SP/BMC 펌웨어 및 시스템 파일에 대한 권장 업데이트를 클러스터에 자동으로 다운로드하고 설치하도록 선택하거나 권장 업데이트를 자동으로 해제하도록 선택할 수 있습니다. 업데이트 설치 또는 해제를 수동으로 제어하려면 권장 업데이트가 있을 때 알림을 받도록 선택합니다. 그런 다음 수동으로 선택하여 설치하거나 해제할 수 있습니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 자동 업데이트 * 옆에 있는 * ⋮ 자동 업데이트 * 를 선택한 다음 * 자동 업데이트 편집 * 을 선택합니다.
3. 자동 업데이트 선택 사항을 업데이트합니다.
4. 저장 * 을 선택합니다.

결과

자동 업데이트는 사용자의 선택에 따라 수정됩니다.

펌웨어를 수동으로 업데이트합니다

권장 업데이트를 다운로드 및 설치하기 전에 유연하게 볼 수 있도록 하려면 자동 업데이트를 비활성화하고 펌웨어를 수동으로 업데이트할 수 있습니다.

단계

1. 펌웨어 업데이트 파일을 서버 또는 로컬 클라이언트에 다운로드합니다.
2. System Manager에서 * 클러스터 > 개요 * 를 선택한 다음 * 업데이트 * 를 선택합니다.
3. 펌웨어 업데이트 * 를 선택하고 선택합니다 + Update firmware .

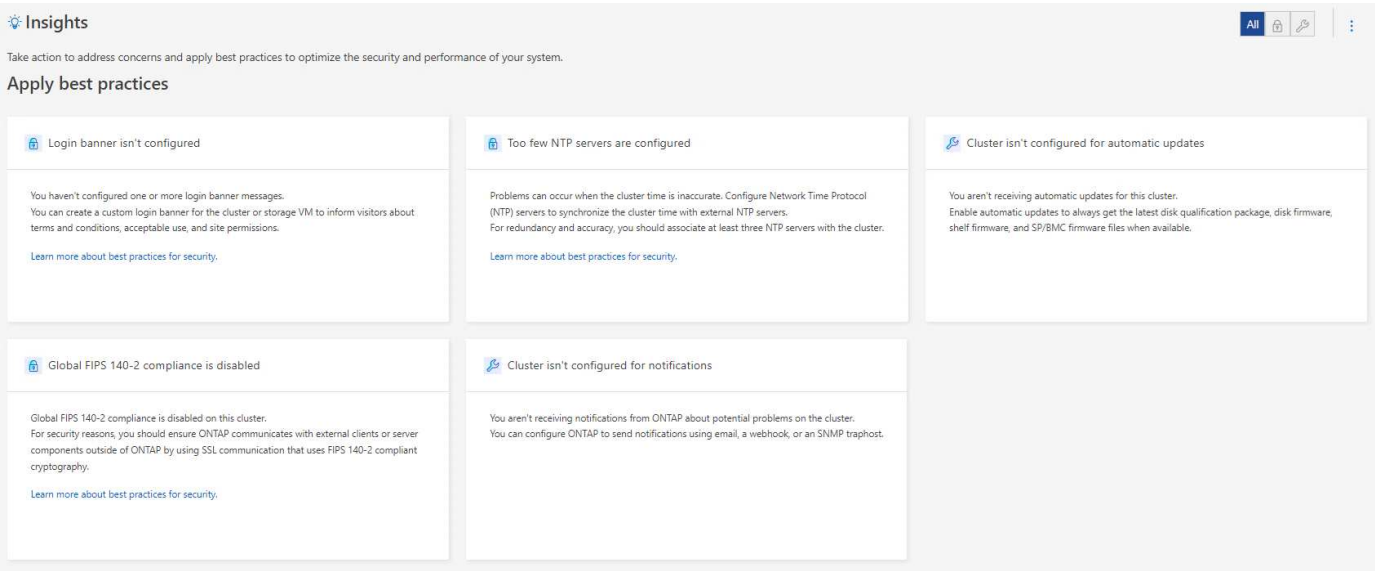
결과

펌웨어가 업데이트됩니다.

ASA R2 스토리지 시스템 인사이트를 통해 클러스터 보안 및 성능을 최적화합니다

ONTAP System Manager에서 View_Insights_를 사용하여 ASA R2 시스템에 구현할 수 있는 모범 사례와 구성 수정 사항을 파악하여 클러스터 보안 및 성능을 최적화할 수 있습니다.

예를 들어, 클러스터에 사용하도록 NTP(네트워크 시간 프로토콜) 서버가 구성되어 있다고 가정합니다. 그러나 최적의 클러스터 시간 관리에 필요한 NTP 서버의 수가 권장된 수보다 적다는 사실을 모르고 있습니다. 클러스터 시간이 정확하지 않을 때 발생할 수 있는 문제를 방지하기 위해 Insights에서는 NTP 서버가 너무 적게 구성되어 있음을 알리고 이 문제에 대해 자세히 알아보거나 수정하거나 무시할 수 있는 옵션을 제공합니다.



단계

1. System Manager에서 * Insights * 를 선택합니다.
2. 권장 사항을 검토합니다.

다음 단계

모범 사례를 구현하고 클러스터 보안 및 성능을 최적화하는 데 필요한 작업을 수행합니다.

ASA R2 스토리지 시스템에서 클러스터 이벤트 및 작업을 봅니다

ONTAP System Manager를 사용하면 시스템에서 발생한 오류 또는 경고 목록과 권장 수정 조치를 볼 수 있습니다. 또한 시스템 감사 로그 및 활성, 완료 또는 실패한 작업 목록을 볼 수 있습니다.

단계

1. System Manager에서 * Events & Jobs * 를 선택합니다.
2. 클러스터 이벤트 및 작업을 봅니다.

이 항목을 보려면...	수행할 작업...
클러스터 이벤트입니다	이벤트 * 를 선택한 다음 * 이벤트 로그 * 를 선택합니다.
Active IQ 제안	이벤트 * 를 선택한 다음 * Active IQ Suggestions * 를 선택합니다.
시스템 경고	a. 시스템 알림 * 을 선택합니다. b. 조치를 취할 시스템 알림을 선택합니다. c. 경고를 확인하거나 표시하지 않습니다.
클러스터 작업	작업 * 을 선택합니다.
감사 로그	Audit logs * 를 선택합니다.

클러스터 이벤트 및 감사 로그에 대한 이메일 알림을 보냅니다

클러스터 이벤트 또는 감사 로그 항목이 있을 때 특정 이메일 주소로 알림을 보내도록 시스템을 구성합니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. Notifications management * 옆에 있는 을 선택합니다⋮.
3. 이벤트 목적지를 구성하려면 * 이벤트 목적지 보기 * 를 선택한 다음 * 이벤트 목적지 * 를 선택하십시오. 감사 로그 대상을 구성하려면 * 감사 대상 보기 * 를 선택한 다음 * 감사 로그 대상 * 을 선택합니다.
4. 을 + Add 선택합니다.
5. 목적지 정보를 입력한 다음 * 추가 * 를 선택합니다.

결과

추가한 이메일 주소는 클러스터 이벤트 및 감사 로그에 대해 지정된 이메일 알림을 받습니다.

노드 관리

ASA R2 스토리지 시스템에서 노드를 재부팅합니다

유지보수, 문제 해결, 소프트웨어 업데이트 또는 기타 관리상의 이유로 노드를 재부팅해야 할 수 있습니다. 노드가 재부팅되면 HA 파트너가 자동으로 테이크오버를 실행합니다. 파트너 노드는 재부팅된 노드가 다시 온라인 상태가 된 후에 자동 반환을 수행합니다.

단계

1. System Manager에서 * 클러스터 > 개요 * 를 선택합니다.
2. ⋮재부팅하려는 노드 옆에 있는 을 선택한 다음 * 재부팅 * 을 선택합니다.
3. 노드를 재부팅하는 이유를 입력한 다음 * Reboot * 를 선택합니다.

재부팅 이유를 입력한 이유는 시스템 감사 로그에 기록됩니다.

다음 단계

노드가 재부팅 중인 동안 HA 파트너가 테이크오버를 수행하여 데이터 서비스가 중단되지 않도록 합니다. 재부팅이 완료되면 HA 파트너가 기브백을 수행합니다.

ASA R2 스토리지 시스템에서 노드 이름을 바꿉니다

ONTAP System Manager를 사용하여 ASA R2 시스템에서 노드 이름을 바꿀 수 있습니다. 조직의 명명 규칙에 맞게 또는 기타 관리 상의 이유로 노드 이름을 변경해야 할 수도 있습니다.

단계

1. System Manager에서 * 클러스터 > 개요 * 를 선택합니다.
2. ⋮ 이름을 바꾸려는 노드 옆에 있는 을 선택한 다음 * Rename * 을 선택합니다.
3. 노드의 새 이름을 입력한 다음 * Rename * 을 선택합니다.

결과

새 이름이 노드에 적용됩니다.

ASA R2 스토리지 시스템에서 사용자 계정 및 역할을 관리합니다

System Manager를 사용하여 사용자 계정에 대한 Active Directory 도메인 컨트롤러 액세스, LDAP 및 SAML 인증을 구성합니다. 사용자 계정 역할을 생성하여 역할에 할당된 사용자가 클러스터에서 수행할 수 있는 특정 기능을 정의합니다.

Active Directory 도메인 컨트롤러 액세스를 구성합니다

AD 계정 액세스를 설정할 수 있도록 클러스터 또는 스토리지 VM에 대한 AD(Active Directory) 도메인 컨트롤러 액세스를 구성합니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 섹션의 * Active Directory * 아래에서 * 구성 * 을 선택합니다.

다음 단계

이제 ASA R2 시스템에서 AD 계정 액세스를 활성화할 수 있습니다.

LDAP를 구성합니다

LDAP(Lightweight Directory Access Protocol) 서버를 구성하여 인증을 위한 사용자 정보를 중앙에서 관리합니다.

시작하기 전에

인증서 서명 요청을 생성하고 CA 서명 서버 디지털 인증서를 추가해야 합니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 섹션에서 * LDAP * 옆에 있는 를 선택합니다.
3. 필요한 LDAP 서버 및 바인딩 정보를 입력한 다음 * 저장 * 을 선택합니다.

다음 단계

이제 사용자 정보 및 인증에 LDAP를 사용할 수 있습니다.

SAML 인증을 구성합니다

SAML(Security Assertion Markup Language) 인증을 사용하면 Active Directory 및 LDAP와 같은 직접 서비스 공급자 대신 IDP(Secure Identity Provider)에서 사용자를 인증할 수 있습니다.

시작하기 전에

- 원격 인증에 사용하려는 IDP를 구성해야 합니다.

  구성에 대해서는 IDP 설명서를 참조하십시오.

- IDP의 URI가 있어야 합니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 에서 * SAML 인증 * 옆에 있는 를 선택합니다.
3. SAML 인증 활성화 * 를 선택합니다.
4. IDP URL 및 호스트 시스템 IP 주소를 입력한 다음 * 저장 * 을 선택합니다.

   확인 창에 메타데이터 정보가 표시되며, 이 정보는 클립보드에 자동으로 복사됩니다.

5. 지정한 IDP 시스템으로 이동한 다음 클립보드에서 메타데이터를 복사하여 시스템 메타데이터를 업데이트합니다.
6. System Manager의 확인 창으로 돌아가서 * I have configured the IDP with the host URI or metadata * 를 선택합니다.
7. SAML 기반 인증을 활성화하려면 * 로그아웃 * 을 선택합니다.

   IDP 시스템에 인증 화면이 표시됩니다.

다음 단계

이제 사용자 계정에 대해 SAML 인증을 사용할 수 있습니다.

사용자 계정 역할을 생성합니다

클러스터 관리자 및 스토리지 VM 관리자의 역할은 클러스터가 초기화될 때 자동으로 생성됩니다. 추가 사용자 계정 역할을 생성하여 역할에 할당된 사용자가 클러스터에서 수행할 수 있는 특정 기능을 정의합니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 섹션에서 * 사용자 및 역할 * 옆에 있는 를 선택합니다.

3. 역할 * 에서 을 + Add 선택합니다.
4. 역할 속성을 선택합니다.

   여러 속성을 추가하려면 을 선택합니다 + Add .

5. 저장 * 을 선택합니다.

결과

새 사용자 계정이 생성되어 ASA R2 시스템에서 사용할 수 있습니다.

관리자 계정을 만듭니다

계정 사용자가 계정에 할당된 역할에 따라 클러스터에서 특정 작업을 수행할 수 있도록 관리자 계정을 생성합니다. 계정 보안을 강화하려면 계정을 만들 때 MFA(다중 요소 인증)를 설정합니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 섹션에서 * 사용자 및 역할 * 옆에 있는 를 선택합니다 →.
3. 사용자 * 에서 을 선택합니다 + Add .
4. 사용자 이름을 입력한 다음 사용자에게 할당할 역할을 선택합니다.
5. 사용자 로그인 방법과 인증 방법을 선택합니다.
6. MFA를 활성화하려면 를 + Add 선택한 다음 보조 로그인 방법 및 인증 방법을 선택합니다
7. 사용자의 암호를 입력합니다.
8. 저장 * 을 선택합니다.

결과

새 관리자 계정이 생성되어 ASA R2 클러스터에서 사용할 수 있습니다.

ASA R2 스토리지 시스템에서 보안 인증서를 관리합니다

디지털 보안 인증서를 사용하여 원격 서버의 ID를 확인합니다.

OCSP(온라인 인증서 상태 프로토콜)는 SSL 및 TLS(전송 계층 보안) 연결을 사용하여 ONTAP 서비스에서 디지털 인증서 요청 상태를 검증합니다.

인증서 서명 요청을 생성합니다

인증서 서명 요청(CSR)을 생성하여 공용 인증서를 생성하는 데 사용할 수 있는 개인 키를 만듭니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 에서 * 인증서 * 옆에 있는 를 선택한 →다음 를 + Generate CSR 선택합니다.
3. 주체의 일반 이름을 입력한 다음 국가를 선택합니다.

4. GSR 기본값을 변경하려면 확장 키 사용을 선택하거나 제목 대체 이름을 추가한 More options다음 을 선택하고 원하는 업데이트를 수행합니다.
5. Generate * 를 선택합니다.

결과

공개 인증서를 생성하는 데 사용할 수 있는 CSR을 생성했습니다.

신뢰할 수 있는 인증 기관을 추가합니다

ONTAP TLS(전송 계층 보안)를 사용하는 응용 프로그램에 대해 신뢰할 수 있는 기본 루트 인증서 집합을 제공합니다. 필요에 따라 신뢰할 수 있는 인증 기관을 추가할 수 있습니다.

단계

1. 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 에서 * 인증서 * 옆에 있는 를 선택합니다 →.
3. 신뢰할 수 있는 인증 기관 * 을 선택합니다.
4. 인증서 세부 정보를 입력하거나 가져온 다음 을 + Add 선택합니다.

결과

신뢰할 수 있는 새 인증 기관을 ASA R2 시스템에 추가했습니다.

신뢰할 수 있는 인증 기관을 갱신하거나 삭제합니다

신뢰할 수 있는 인증 기관은 매년 갱신해야 합니다. 만료된 인증서를 갱신하지 않으려면 삭제해야 합니다.

단계

1. 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 에서 * 인증서 * 옆에 있는 를 선택합니다 →.
3. 신뢰할 수 있는 인증 기관 * 을 선택합니다.
4. 갱신하거나 삭제할 신뢰 인증 기관을 선택합니다.
5. 인증 기관을 갱신하거나 삭제합니다.

인증 기관을 갱신하려면 다음을 수행합니다.	인증 기관을 삭제하려면 다음을 수행합니다.
a. 을 ⋮ 선택한 다음 * 갱신 * 을 선택합니다. b. 인증서 정보를 입력하거나 가져온 다음 * 갱신 * 을 선택합니다.	a. 을 ⋮ 선택한 다음 * 삭제 * 를 선택합니다. b. 삭제를 확인한 다음 * Delete * 를 선택합니다.

결과

ASA R2 시스템에서 기존의 신뢰할 수 있는 인증 기관을 갱신하거나 삭제했습니다.

클라이언트/서버 인증서 또는 로컬 인증 기관을 추가합니다

클라이언트/서버 인증서 또는 로컬 인증 기관을 추가하여 보안 웹 서비스를 활성화합니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 에서 * 인증서 * 옆에 있는 를 선택합니다 →.
3. 클라이언트/서버 인증서 * 또는 * 로컬 인증 기관 * 을 선택합니다.
4. 인증서 정보를 추가한 다음 을 선택합니다 + Add .

결과

새 클라이언트/서버 인증서 또는 지역 기관을 ASA R2 시스템에 추가했습니다.

클라이언트/서버 인증서 또는 로컬 인증 기관을 갱신하거나 삭제합니다

클라이언트/서버 인증서 및 로컬 인증 기관은 매년 갱신해야 합니다. 만료된 인증서 또는 로컬 인증 기관을 갱신하지 않으려면 삭제해야 합니다.

단계

1. 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 에서 인증서 옆에 있는 를 →선택합니다.
3. 클라이언트/서버 인증서 * 또는 * 로컬 인증 기관 * 을 선택합니다.
4. 갱신 또는 삭제할 인증서를 선택합니다.
5. 인증 기관을 갱신하거나 삭제합니다.

인증 기관을 갱신하려면 다음을 수행합니다.	인증 기관을 삭제하려면 다음을 수행합니다.
a. 을 ⋮선택한 다음 * 갱신 * 을 선택합니다. b. 인증서 정보를 입력하거나 가져온 다음 * 갱신 * 을 선택합니다.	을 ⋮선택한 다음 * 삭제 * 를 선택합니다.

결과

ASA R2 시스템에서 기존 클라이언트/서버 인증서 또는 로컬 인증 기관을 갱신하거나 삭제했습니다.

ASA R2 스토리지 시스템에서 호스트 접속을 확인합니다

호스트 데이터 작업에 문제가 있는 경우 ONTAP System Manager를 사용하여 호스트에서 ASA R2 스토리지 시스템으로의 접속이 활성 상태인지 확인할 수 있습니다.

단계

1. System Manager에서 * Host * 를 선택합니다.

   호스트 접속 상태는 호스트 그룹 이름 옆에 다음과 같이 표시됩니다.

- * OK *: 모든 이니시에이터가 두 노드에 연결되었음을 나타냅니다.
- 부분적으로 연결됨: 초기자 중 일부가 두 노드에 연결되지 않았음을 나타냅니다.
- **None Connected**: 연결된 이니시에이터가 없음을 나타냅니다.

다음 단계

호스트에서 업데이트를 수행하여 연결 문제를 수정합니다. ONTAP는 15분마다 연결 상태를 다시 확인합니다.