이벤트, 성능 및 상태 모니터링

ONTAP 9

NetApp
September 12, 2024

목차

이벤트, 성능 및 상태 모니터링

System Manager로 클러스터 성능을 모니터링합니다

System Manager를 사용하여 클러스터 성능을 모니터링합니다

이 섹션의 항목에서는 ONTAP 9.7 이상 릴리즈의 System Manager에서 클러스터 상태 및 성능을 관리하는 방법을 보여 줍니다.

System Manager 대시보드에서 시스템에 대한 정보를 확인하여 클러스터 성능을 모니터링할 수 있습니다. 대시보드에는 중요한 알림, 스토리지 계층 및 볼륨의 효율성 및 용량, 클러스터에서 사용 가능한 노드, HA Pair의 노드 상태, 가장 활성화된 애플리케이션 및 개체에 대한 정보가 표시됩니다. 클러스터 또는 노드의 성능 메트릭과

대시보드를 통해 다음 정보를 확인할 수 있습니다.

- * 상태 *: 클러스터가 얼마나 양호합니까?
- * 용량 *: 클러스터에서 사용할 수 있는 용량은 무엇입니까?
- * 성능 *: 지연 시간, IOPS 및 처리량을 기준으로 클러스터의 성능은 어떻습니까?
- * 네트워크 *: 포트, 인터페이스 및 스토리지 VM과 같은 호스트 및 스토리지 객체로 네트워크를 구성하는 방법은 무엇입니까?

Health and Capacity 개요에서 을 클릭하여 추가 정보를 보고 작업을 수행할 수 있습니다 → .

성과 개요에서는 시간, 일, 주, 월 또는 연도를 기준으로 메트릭을 볼 수 있습니다.

네트워크 개요에서 네트워크의 각 개체 수가 표시됩니다(예: "8개의 NVMe/FC 포트"). 번호를 클릭하여 각 네트워크 개체에 대한 세부 정보를 볼 수 있습니다.

System Manager 대시보드에서 클러스터 개요를 확인합니다

System Manager 대시보드를 이용하면 단일 위치에서 ONTAP 클러스터를 빠르고 포괄적으로 확인할 수 있습니다.

System Manager 대시보드를 사용하면 중요한 경고와 알림, 스토리지 계층 및 볼륨의 효율성 및 용량, 클러스터에서 사용 가능한 노드, 고가용성(HA) 쌍의 노드 상태, 가장 활발한 애플리케이션 및 오브젝트의 상태에 대한 정보를 한눈에 볼 수 있습니다. 클러스터 또는 노드의 성능 메트릭을 파악할 수 있습니다.

대시보드에는 다음과 같이 설명된 4개의 패널이 포함되어 있습니다.

상태

상태 보기에는 클러스터에서 검색할 수 있는 모든 노드의 전반적인 상태에 대한 정보가 표시됩니다.

또한 상태 보기에는 구성되지 않은 노드 세부 정보와 같은 클러스터 레벨의 오류 및 경고가 표시되며, 클러스터 성능을 높이기 위해 수정할 수 있는 특성을 나타냅니다.

클러스터 이름, 버전, 클러스터 생성 날짜 및 시간 등과 같은 클러스터의 개요를 보려면 → 상태 보기를 클릭하여 확장합니다. 클러스터와 연결된 노드의 상태와 관련된 통계를 모니터링할 수도 있습니다. 환경에서 리소스를 그룹화하고

식별할 수 있는 태그를 관리할 수 있습니다. Insights 섹션은 시스템의 용량, 보안 규정 준수 및 구성을 최적화하는 데 도움이 됩니다.

용량

Capacity 보기에는 클러스터의 스토리지 공간이 표시됩니다. 사용된 총 논리적 공간, 사용된 총 물리적 공간 및 사용 가능한 디스크 공간을 볼 수 있습니다.

ActiveIQ에 등록하여 클러스터 데이터의 기간별 데이터를 볼 수 있습니다. →Capacity 뷰를 확장하면 클러스터와 관련된 계층의 개요를 볼 수 있습니다. 총 공간, 사용된 공간 및 사용 가능한 공간 등 각 계층에 대한 용량 정보를 볼 수 있습니다. 처리량, IOPS, 지연 시간에 대한 세부 정보가 표시됩니다. "이러한 용량 측정에 대한 자세한 내용은 System Manager를 참조하십시오"..

용량 보기를 사용하여 로컬 계층 또는 클라우드 계층을 추가할 수 있습니다. 용량 보기에 대한 자세한 내용은 을 참조하십시오 "클러스터의 용량을 봅니다".

네트워크

네트워크 보기에는 네트워크의 일부인 물리적 포트, 네트워크 인터페이스 및 스토리지 VM이 표시됩니다.

네트워크 보기에는 네트워크에 연결된 클라이언트 유형이 표시됩니다. 네트워크에 연결된 각 클라이언트는 숫자로 표시됩니다(예: "NVMe/FC 16"). 각 네트워크 요소에 대한 특정 세부 정보를 보려면 번호를 선택하십시오.

네트워크의 포트, 네트워크 인터페이스, 스토리지 VM 및 호스트를 포함하는 네트워크의 전체 페이지 보기를 보려면 → 클릭하십시오.

성능

성능 보기에는 ONTAP 클러스터의 상태와 효율성을 모니터링하는 데 도움이 되는 성능 통계가 표시됩니다. 통계에는 지연 시간, 처리량, IOPS 등 주요 클러스터 성능 표시기가 포함되어 있으며 그래프로 표시됩니다.

성능 보기에는 일, 시, 주 또는 연도별로 서로 다른 시간 간격의 성능 통계가 표시됩니다. 다양한 그래프를 사용하여 클러스터 성능을 빠르게 분석하고 최적화가 필요한 특성을 파악할 수 있습니다. 이 빠른 분석을 통해 워크로드를 추가 또는 이동하는 방법을 결정할 수 있습니다. 또한 최대 사용 시간을 살펴보고 잠재적 변경 사항을 계획할 수 있습니다.

성능 보기에는 지연 시간, 처리량 및 IOPS와 관련된 총 성능 메트릭이 표시됩니다.

9.15.1부터 성능 뷰가 향상되어 지연 시간, 처리량, IOPS와 관련된 읽기, 쓰기, 기타 및 총 성능 메트릭에 대한 그래프를 표시할 수 있습니다. 다른 메트릭에는 읽기 또는 쓰기가 아닌 작업이 포함됩니다.

성능 값은 3초마다 새로 고쳐지고 성능 그래프는 15초마다 새로 고쳐집니다. 클러스터 성능에 대한 정보를 사용할 수 없는 경우에는 그래프가 표시되지 않습니다.

시간, 일, 주, 월 및 연도별로 성능 메트릭을 전체 페이지 보기로 보려면 ↙↗ 클릭합니다. 로컬 시스템에서 성능 메트릭 보고서를 다운로드할 수도 있습니다.

핫 볼륨 및 기타 개체를 식별합니다

자주 액세스하는 볼륨(핫 볼륨) 및 데이터(핫 오브젝트)를 식별하여 클러스터 성능을 가속화합니다.

ONTAP 9.10.1부터 파일 시스템 분석의 활동 추적 기능을 사용하여 볼륨의 핫 객체를 모니터링할 수 있습니다.

단계

1. 스토리지 > 볼륨 * 을 클릭합니다.
2. 자주 액세스하는 볼륨 및 데이터를 보려면 IOPS, 지연 시간 및 처리량 열을 필터링합니다.

QoS를 수정합니다

ONTAP 9.8부터 스토리지를 프로비저닝할 때 서비스 품질(QoS) 기본적으로 활성화되어 있습니다. 프로비저닝 프로세스 중에 QoS를 비활성화하거나 사용자 지정 QoS 정책을 선택할 수 있습니다. 스토리지에 프로비저닝된 후 QoS를 수정할 수도 있습니다.

단계

1. System Manager에서 * Storage * 와 * Volumes * 를 차례로 선택합니다.
2. QoS를 수정할 볼륨 옆에 있는 * 편집 * 을 선택합니다 ⋮ .

위험 모니터링

ONTAP 9.10.0부터 시스템 관리자를 사용하여 Active IQ 디지털 어드바이저가 보고한 위험을 모니터링할 수 있습니다. ONTAP 9.10.1부터 System Manager를 사용하여 위험을 확인할 수도 있습니다.

NetApp Active IQ Digital Advisor는 위험을 줄이고 스토리지 환경의 성능과 효율성을 향상할 수 있는 기회를 보고합니다. System Manager를 사용하면 Active IQ에서 보고하는 위험에 대해 알아보고 실행 가능한 인텔리전스를 확보하여 스토리지를 관리하고 가용성을 높이고 보안을 강화하고 스토리지 성능을 향상할 수 있습니다.

Active IQ 계정에 대한 링크입니다

Active IQ의 위험에 대한 정보를 수신하려면 먼저 시스템 관리자에서 Active IQ 계정에 연결해야 합니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 클릭합니다.
2. Active IQ 등록 * 에서 * 등록 * 을 클릭합니다.
3. Active IQ에 대한 자격 증명을 입력합니다.
4. 자격 증명이 인증되면 * 확인을 클릭하여 Active IQ를 System Manager*와 연결합니다.

위험 수를 확인합니다

ONTAP 9.10.0부터 System Manager의 대시보드에서 Active IQ가 보고한 위험 수를 확인할 수 있습니다.

시작하기 전에

System Manager와 Active IQ 계정 간의 연결을 설정해야 합니다. 을 참조하십시오 Active IQ 계정에 대한 링크입니다.

단계

1. System Manager에서 * 대시보드 * 를 클릭합니다.
2. 상태 * 섹션에서 보고된 위험 수를 확인합니다.

> 위험 수를 보여 주는 메시지를 클릭하여 각 위험에 대한 자세한 정보를 볼 수 있습니다. 을 참조하십시오 위험에 대한 세부 정보를 봅니다.

위험에 대한 세부 정보를 봅니다

ONTAP 9.10.0부터 Active IQ에서 보고한 위험이 영향 영역별로 분류되는 방식을 시스템 관리자에서 확인할 수 있습니다. 또한 보고된 각 위험, 시스템에 미치는 잠재적 영향 및 취할 수 있는 수정 조치에 대한 자세한 정보를 볼 수 있습니다.

시작하기 전에

System Manager와 Active IQ 계정 간의 연결을 설정해야 합니다. 을 참조하십시오 Active IQ 계정에 대한 링크입니다.

단계

1. 이벤트 > 모든 이벤트 * 를 클릭합니다.
2. 개요 * 섹션의 * Active IQ 제안 * 아래에서 각 영향 영역 범주의 위험 수를 봅니다. 위험 범주는 다음과 같습니다.
   - 성능 및 효율성
   - 가용성 및 보호
   - 용량
   - 구성
   - 보안
3. Active IQ 제안 * 탭을 클릭하여 다음을 포함한 각 위험에 대한 정보를 확인하십시오.
   - 시스템에 미치는 영향 수준
   - 위험의 범주입니다
   - 영향을 받는 노드입니다
   - 필요한 완화 조치 유형
   - 수행할 수 있는 수정 조치

위험을 인정합니다

ONTAP 9.10.1부터 System Manager를 사용하여 열려 있는 위험을 확인할 수 있습니다.

단계

1. System Manager에서 의 절차를 수행하여 위험 목록을 표시합니다 위험에 대한 세부 정보를 봅니다.
2. 승인하려는 공개 위험의 위험 이름을 클릭합니다.
3. 다음 필드에 정보를 입력합니다.
   - 미리 알림(날짜)
   - 양쪽 맞춤
   - 설명

4. 확인 * 을 클릭합니다.

> 위험을 인지한 후 Active IQ 제안 목록에 변경이 반영되려면 몇 분 정도 걸립니다.

위험 확인 취소

ONTAP 9.10.1부터 System Manager를 사용하여 이전에 승인되었던 모든 위험을 확인할 수 있습니다.

단계

1. System Manager에서 의 절차를 수행하여 위험 목록을 표시합니다 위험에 대한 세부 정보를 봅니다.
2. 확인 취소할 확인된 위험의 위험 이름을 클릭합니다.
3. 다음 필드에 정보를 입력합니다.
   - 양쪽 맞춤
   - 설명
4. 승인 취소 * 를 클릭합니다.

> 위험을 인지하지 못한 후 Active IQ 제안 목록에 변경이 반영되려면 몇 분 정도 걸립니다.

System Manager 인사이트

ONTAP 9.11.1부터 System Manager는 시스템의 성능과 보안을 최적화하는 데 도움이 되는 _insights_를 표시합니다.

> 통찰력을 보고, 사용자 정의하고, 응답하려면 을 참조하십시오 "시스템 최적화를 위한 통찰력 확보"

용량 인사이트

System Manager에서는 시스템의 용량 조건에 대응하여 다음과 같은 인사이트를 표시할 수 있습니다.

통찰력	심각도입니다	조건	수정
로컬 계층에 공간이 부족합니다	위험 개선	하나 이상의 로컬 계층이 95% 이상 차 있고 빠르게 성장하고 있습니다. 기존 워크로드를 확장할 수 없거나, 기존 워크로드의 공간 부족과 장애가 발생할 수 있습니다.	• 권장 해결 방법 *: 다음 옵션 중 하나를 수행합니다. • 볼륨 복구 대기열을 지웁니다. • 씩 프로비저닝된 볼륨에서 씬 프로비저닝을 사용하여 트래핑된 스토리지를 제거합니다. • 볼륨을 다른 로컬 계층으로 이동 • 불필요한 스냅샷 복사본을 삭제합니다. • 볼륨에서 불필요한 디렉토리 또는 파일을 삭제합니다. • Fabric Pool을 사용하여 데이터를 클라우드에 계층화하십시오.

애플리케이션에 공간이 부족합니다	주의가 필요합니다	하나 이상의 볼륨이 95%를 초과하지만 자동 확장 기능이 사용되지 않습니다.	• 권장 *: 현재 용량의 150%까지 자동 확장 가능. • 기타 옵션 *: • 스냅샷 복사본을 삭제하여 공간을 재확보할 수 있습니다. • 볼륨 크기를 조정합니다. • 디렉터리 또는 파일을 삭제합니다.
FlexGroup 볼륨 용량이 불균형 상태입니다	스토리지 최적화	하나 이상의 FlexGroup 볼륨의 구성 볼륨의 크기가 시간이 지남에 따라 균일하지 않게 증가함에 따라 용량 사용량이 불균형 상태가 됩니다. 구성 볼륨이 꽉 차면 쓰기 장애가 발생할 수 있습니다.	• 권장 *: FlexGroup 볼륨 재조정.
스토리지 VM의 용량이 부족합니다	스토리지 최적화	하나 이상의 스토리지 VM이 최대 용량에 근접했습니다. 스토리지 VM이 최대 용량에 도달한 경우 새 볼륨 또는 기존 볼륨에 더 많은 공간을 프로비저닝할 수 없습니다.	• 권장 *: 가능한 경우 스토리지 VM의 최대 용량 제한을 늘리십시오.

보안 인사이트

System Manager에서는 데이터 또는 시스템의 보안을 위태롭게 할 수 있는 상황에 대응하여 다음과 같은 인사이트를 표시할 수 있습니다.

통찰력	심각도입니다	조건	수정
볼륨은 여전히 안티 랜섬웨어 학습 모드에 있습니다	주의가 필요합니다	하나 이상의 볼륨이 90일 동안 안티 랜섬웨어 학습 모드에 있었습니다.	• 권장 * : 해당 볼륨에 대한 안티 랜섬웨어 활성 모드를 활성화합니다.
스냅샷 복사본의 자동 삭제가 볼륨에 활성화되어 있습니다	주의가 필요합니다	스냅샷 자동 삭제가 하나 이상의 볼륨에 설정되어 있습니다.	• 권장 * : 스냅샷 복사본의 자동 삭제를 비활성화합니다. 그렇지 않으면 랜섬웨어 공격의 경우 이러한 볼륨에 대한 데이터 복구가 불가능할 수 있습니다.

볼륨에 스냅샷 정책이 없습니다	주의가 필요합니다	하나 이상의 볼륨에 적절한 스냅샷 정책이 연결되어 있지 않습니다.	• 권장 *: 스냅샷 정책을 없는 볼륨에 첨부하십시오. 그렇지 않으면 랜섬웨어 공격의 경우 이러한 볼륨에 대한 데이터 복구가 불가능할 수 있습니다.
기본 FPolicy가 구성되지 않았습니다	모범 사례	기본 FPolicy가 하나 이상의 NAS 스토리지 VM에 구성되지 않았습니다.	• 권장 * : * 중요 * : 확장자를 차단하면 예기치 않은 결과가 발생할 수 있습니다. 9.11.1부터는 스토리지 VM에 대한 기본 FPolicy를 활성화할 수 있는데, 이 FPolicy는 랜섬웨어 공격에 사용되는 것으로 알려진 3,000개 이상의 파일 확장자를 차단합니다. "기본 FPolicy를 구성합니다" NAS 스토리지 VM에서 사용자 환경의 볼륨에 쓸 수 있거나 허용되지 않는 파일 확장자를 제어합니다.
텔넷이 활성화되었습니다	모범 사례	보안 원격 액세스에는 SSH(Secure Shell)를 사용해야 합니다.	• 권장 * : 텔넷을 비활성화하고 SSH를 사용하여 원격 액세스를 안전하게 하십시오.
구성된 NTP 서버가 너무 적습니다	모범 사례	NTP에 대해 구성된 서버 수가 3개 미만입니다.	• 권장 *: 3개 이상의 NTP 서버를 클러스터에 연결합니다. 그렇지 않으면 클러스터 시간의 동기화에 문제가 발생할 수 있습니다.
원격 셸(RSH)이 활성화되었습니다	모범 사례	보안 원격 액세스에는 SSH(Secure Shell)를 사용해야 합니다.	• 권장 * : RSH를 비활성화하고 SSH를 사용하여 원격 액세스를 안전하게 하십시오.
로그인 배너가 구성되지 않았습니다	모범 사례	로그인 메시지는 클러스터, 스토리지 VM 또는 둘 다에 대해 구성되지 않습니다.	• 권장 *: 클러스터 및 스토리지 VM에 대한 로그인 배너를 설정하고 사용을 활성화합니다.
AutoSupport는 안전하지 않은 프로토콜을 사용하고 있습니다	모범 사례	AutoSupport가 HTTPS를 통해 통신하도록 구성되지 않았습니다.	• 권장 *: AutoSupport 메시지를 기술 지원 부서에 전송하기 위한 기본 전송 프로토콜로 HTTPS를 사용하는 것이 좋습니다.
기본 관리자 사용자가 잠겨 있지 않습니다	모범 사례	아무도 기본 관리 계정(admin 또는 diag)을 사용하여 로그인하지 않았으며 이러한 계정은 잠겨 있지 않습니다.	• 권장 * : 사용하지 않을 때 기본 관리 계정을 잠급니다.

SSH(Secure Shell)에서 비보안 암호를 사용하고 있습니다	모범 사례	현재 구성은 비보안 CBC 암호를 사용합니다.	• 권장 * : 방문자와의 안전한 통신을 보호하기 위해 웹 서버에 보안 암호화만 허용해야 합니다. "ais128-CBC", "AES192-CBC", "AES256-CBC" 및 "3DES-CBC"와 같이 "CBC"가 포함된 이름이 있는 암호를 제거합니다.
글로벌 FIPS 140-2 규정 준수가 비활성화되었습니다	모범 사례	클러스터에서 글로벌 FIPS 140-2 규정 준수가 비활성화되었습니다.	• 권장 *: 보안상의 이유로 ONTAP가 외부 클라이언트 또는 서버 클라이언트와 안전하게 통신할 수 있도록 글로벌 FIPS 140-2 호환 암호화를 활성화해야 합니다.
볼륨은 랜섬웨어 공격을 모니터링하지 않습니다	주의가 필요합니다	하나 이상의 볼륨에서 랜섬웨어 방지 기능이 비활성화되었습니다.	• 권장 * : 볼륨에서 안티 랜섬웨어 활성화. 그렇지 않으면 볼륨이 위협받거나 공격을 받고 있는 경우를 알 수 없습니다.
스토리지 VM이 안티 랜섬웨어용으로 구성되지 않았습니다	모범 사례	하나 이상의 스토리지 VM이 안티 랜섬웨어 보호를 위해 구성되지 않았습니다.	• 권장 * : 스토리지 VM에서 안티 랜섬웨어 활성화. 그렇지 않으면 스토리지 VM이 위협되거나 공격 당하는 시기를 모를 수 있습니다.

구성 인사이트

System Manager에서는 시스템 구성과 관련된 우려 사항에 대한 다음과 같은 인사이트를 표시할 수 있습니다.

통찰력	심각도입니다	조건	수정
클러스터가 알림에 대해 구성되지 않았습니다	모범 사례	이메일, Webhook 또는 SNMP Traphost는 클러스터 문제에 대한 알림을 받을 수 있도록 구성되어 있지 않습니다.	• 권장 *: 클러스터에 대한 알림을 구성합니다.
클러스터가 자동 업데이트를 위해 구성되지 않았습니다.	모범 사례	클러스터가 최신 디스크 검증 패키지, 디스크 펌웨어, 쉘프 펌웨어 및 SP/BMC 펌웨어 파일을 사용할 수 있는 경우 자동 업데이트를 수신하도록 구성되지 않았습니다.	• 권장 * : 이 기능을 활성화합니다.

클러스터 펌웨어가 최신 상태가 아닙니다	모범 사례	시스템에 향상된 성능, 보안 패치 또는 클러스터를 보호하는 데 도움이 되는 새로운 기능이 있을 수 있는 최신 펌웨어 업데이트가 없습니다.	• 권장 *: ONTAP 펌웨어를 업데이트합니다.

시스템 최적화를 위한 통찰력 확보

System Manager를 사용하면 시스템 최적화를 위한 통찰력을 얻을 수 있습니다.

이 작업에 대해

ONTAP 9.11.0부터 시스템 용량 및 보안 규정 준수를 최적화하는 데 도움이 되는 시스템 관리자에 대한 정보를 볼 수 있습니다.

ONTAP 9.11.1부터 시스템의 용량, 보안 준수 및 구성을 최적화하는 데 도움이 되는 추가 정보를 볼 수 있습니다.

> • 확장 차단으로 인해 예기치 않은 결과가 발생할 수 있습니다. * ONTAP 9.11.1부터 시스템 관리자를 사용하여 스토리지 VM에 대한 기본 FPolicy를 활성화할 수 있습니다. 자신에게 권장되는 System Manager Insight 메시지를 받을 수 있습니다 "기본 FPolicy를 구성합니다" Insight 설문조사에 응답해 주세요.
>
> FPolicy 기본 모드를 사용하면 특정 파일 확장자를 허용하거나 허용하지 않을 수 있습니다. System Manager는 과거 랜섬웨어 공격에 사용되었던 허용되지 않는 파일 확장자를 3000개 이상 권장합니다. 이러한 확장자 중 일부는 사용자 환경의 합법적인 파일에 의해 사용될 수 있으며 이러한 파일을 차단하면 예기치 않은 문제가 발생할 수 있습니다.
>
> 따라서 사용자 환경의 요구에 맞게 확장 목록을 수정하는 것이 좋습니다. 을 참조하십시오 "System Manager를 사용하여 System Manager에서 생성된 기본 FPolicy 구성에서 파일 확장명을 제거하여 정책을 재생성하는 방법".
>
> 기본 FPolicy에 대한 자세한 내용은 를 참조하십시오"FPolicy 구성 유형".

모범 사례에 따라 이러한 통찰력은 한 페이지에 표시되어 즉시 조치를 시작하여 시스템을 최적화할 수 있습니다. 각 통찰력에 대한 자세한 내용은 을 참조하십시오 "System Manager 인사이트".

최적화 인사이트 보기

단계

1. System Manager의 왼쪽 탐색 열에서 * Insights * 를 클릭합니다.

   Insights * 페이지에는 인사이트 그룹이 표시됩니다. 각 인사이트 그룹에는 하나 이상의 통찰력이 포함될 수 있습니다. 다음 그룹이 표시됩니다.

   - 주의가 필요합니다
   - 위험 개선
   - 스토리지를 최적화하십시오

2. (선택 사항) 페이지의 오른쪽 위 모서리에 있는 다음 단추를 클릭하여 표시되는 통찰력을 필터링합니다.
    - 보안 관련 인사이트를 표시합니다.
    - 용량 관련 인사이트를 표시합니다.
    - 구성 관련 인사이트를 표시합니다.
    - All 모든 정보를 표시합니다.

인사이트를 활용하여 시스템을 최적화합니다

System Manager에서 통찰력을 손실, 문제 해결을 위한 다양한 방법 모색 또는 문제 해결을 위한 프로세스 시작을 통해 통찰력을 얻을 수 있습니다.

단계

1. System Manager의 왼쪽 탐색 열에서 * Insights * 를 클릭합니다.
2. Insight 위로 마우스를 가져가면 다음 작업을 수행할 수 있는 버튼이 표시됩니다.
    - * Dismiss *: 뷰에서 통찰력을 제거합니다. 통찰력을 "해제"하려면 을 참조하십시오 [customize-settings-insights].
    - * Explore *: 통찰력에 언급된 문제를 해결하는 다양한 방법을 알아보십시오. 이 버튼은 둘 이상의 교정 방법이 있는 경우에만 나타납니다.
    - * 수정 *: 통찰력에 언급된 문제를 해결하는 프로세스를 시작합니다. 수정 사항을 적용하는 데 필요한 조치를 취할지 여부를 확인하는 메시지가 표시됩니다.

> 이러한 작업 중 일부는 System Manager의 다른 페이지에서 시작할 수 있지만 * Insights * 페이지에서는 이 한 페이지에서 이러한 작업을 시작할 수 있으므로 일상적인 작업을 간소화할 수 있습니다.

통찰력을 위한 설정을 사용자 지정합니다

System Manager에서 알림을 받을 인사이트를 사용자 지정할 수 있습니다.

단계

1. System Manager의 왼쪽 탐색 열에서 * Insights * 를 클릭합니다.
2. 페이지의 오른쪽 위 모서리에서 을 클릭한 ⋮다음 * 설정 * 을 선택합니다.
3. 설정 * 페이지에서 알림을 받을 인사이트 옆에 있는 확인란이 있는지 확인합니다. 이전에 통찰력을 거부했다면, 체크 박스에 체크 표시를 하여 "해제"할 수 있습니다.
4. 저장 * 을 클릭합니다.

통찰력을 **PDF** 파일로 내보냅니다

해당하는 모든 통찰력을 PDF 파일로 내보낼 수 있습니다.

단계

1. System Manager의 왼쪽 탐색 열에서 * Insights * 를 클릭합니다.
2. 페이지의 오른쪽 위 모서리에서 을 클릭한 ⋮다음 * 내보내기 * 를 선택합니다.

기본 **FPolicy**를 구성합니다

ONTAP 9.11.1부터 기본 FPolicy 구현을 제안하는 System Manager Insight를 수신하면 스토리지 VM 및 볼륨에서 구성할 수 있습니다.

시작하기 전에

System Manager Insights의 * 모범 사례 적용 * 에 액세스하면 기본 FPolicy가 구성되지 않았다는 메시지가 표시될 수 있습니다.

FPolicy 구성 유형에 대한 자세한 내용은 을 "FPolicy 구성 유형"참조하십시오.

단계

1. System Manager의 왼쪽 탐색 열에서 * Insights * 를 클릭합니다.
2. Apply 모범 사례 * 에서 * 기본 FPolicy가 구성되지 않음 * 을 찾습니다.
3. 조치를 취하기 전에 다음 메시지를 읽으십시오.

   - 확장 차단으로 인해 예기치 않은 결과가 발생할 수 있습니다. * ONTAP 9.11.1부터 시스템 관리자를 사용하여 스토리지 VM에 대한 기본 FPolicy를 활성화할 수 있습니다. FPolicy 기본 모드를 사용하면 특정 파일 확장자를 허용하거나 허용하지 않을 수 있습니다. System Manager는 과거 랜섬웨어 공격에 사용되었던 허용되지 않는 파일 확장자를 3000개 이상 권장합니다. 이러한 확장자 중 일부는 사용자 환경의 합법적인 파일에 의해 사용될 수 있으며 이러한 파일을 차단하면 예기치 않은 문제가 발생할 수 있습니다.

   따라서 사용자 환경의 요구에 맞게 확장 목록을 수정하는 것이 좋습니다. 을 참조하십시오 "System Manager를 사용하여 System Manager에서 생성된 기본 FPolicy 구성에서 파일 확장명을 제거하여 정책을 재생성하는 방법".

4. 수정 * 을 클릭합니다.
5. 기본 FPolicy를 적용할 스토리지 VM을 선택합니다.
6. 각 스토리지 VM에 대해 기본 FPolicy를 받을 볼륨을 선택합니다.
7. 구성 * 을 클릭합니다.

CLI를 사용하여 클러스터 성능을 모니터링하고 관리합니다

성능 모니터링 및 관리 개요

기본적인 성능 모니터링 및 관리 작업을 설정하고 일반적인 성능 문제를 식별하고 해결할 수 있습니다.

다음과 같은 가정이 상황에 적용되는 경우 이 절차를 사용하여 클러스터 성능을 모니터링하고 관리할 수 있습니다.

- 사용 가능한 모든 옵션을 탐색하는 것이 아니라 모범 사례를 사용하려고 합니다.

- ONTAP 명령줄 인터페이스 외에 Active IQ Unified Manager(이전의 OnCommand Unified Manager)를 사용하여 시스템 상태 및 경고를 표시하고, 클러스터 성능을 모니터링하고, 근본 원인 분석을 수행하려고 합니다.
- ONTAP 명령줄 인터페이스를 사용하여 스토리지 QoS(서비스 품질)를 구성합니다. QoS는 다음을 통해서도 사용할 수 있습니다.
  - 시스템 관리자
  - ONTAP REST API를 참조하십시오
  - VMware vSphere용 ONTAP 툴
  - NetApp 서비스 수준 관리자(NSLM)
  - OnCommand Workflow Automation(WFA)
- Linux 또는 Windows 기반 설치 대신 가상 어플라이언스를 사용하여 Unified Manager를 설치하려는 경우.
- 소프트웨어를 설치하는 데 DHCP가 아닌 정적 구성을 사용할 수 있습니다.
- 고급 권한 수준에서 ONTAP 명령에 액세스할 수 있습니다.
- "admin" 역할을 가진 클러스터 관리자입니다.

관련 정보

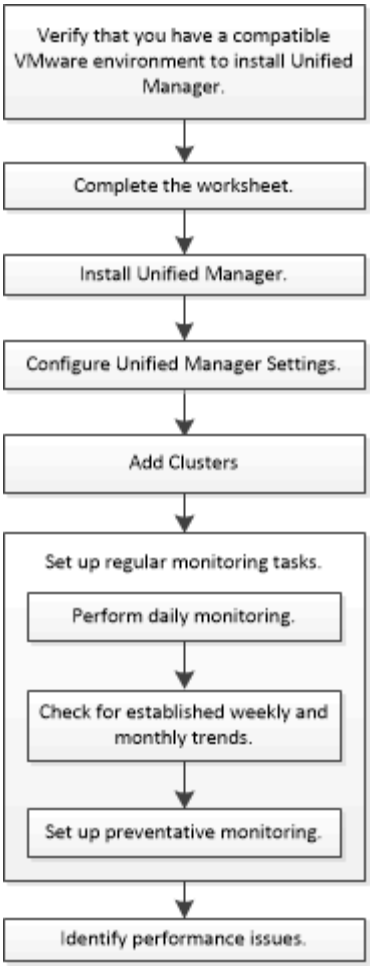
이러한 가정이 현재 상황에 맞지 않는 경우 다음 리소스를 참조하십시오.

- "Active IQ Unified Manager 9.8 설치"
- "시스템 관리"

성능을 모니터링합니다

성능 모니터링 및 유지 관리 워크플로우 개요

클러스터 성능을 모니터링하고 유지하려면 Active IQ Unified Manager 소프트웨어 설치, 기본 모니터링 작업 설정, 성능 문제 식별 및 필요에 따라 조정 작업이 필요합니다.



사용 중인 **VMware** 환경이 지원되는지 확인합니다

Active IQ Unified Manager를 성공적으로 설치하려면 VMware 환경이 필요한 요구 사항을 충족하는지 확인해야 합니다.

단계

1. VMware 인프라가 Unified Manager 설치를 위한 사이징 요구 사항을 충족하는지 확인합니다.
2. 로 이동합니다 "상호 운용성 매트릭스" 지원되는 다음 구성 요소 조합이 있는지 확인하려면 다음을 수행합니다.
   - ONTAP 버전입니다
   - ESXi 운영 체제 버전입니다
   - VMware vCenter Server 버전입니다
   - VMware Tools 버전입니다
   - 브라우저 유형 및 버전

   ⓘ `http://mysupport.netapp.com/matrix["상호 운용성 매트릭스"^]에는 Unified Manager에 대해 지원되는 구성이 나와 있습니다.`

3. 선택한 설정의 설정 이름을 클릭합니다.

해당 구성에 대한 세부 정보가 구성 세부 정보 창에 표시됩니다.

4. 다음 탭의 정보를 검토합니다.
   - 참고

     에는 사용자의 구성에 특정한 중요한 경고 및 정보가 나와 있습니다.

   - 정책 및 지침

     모든 구성에 대한 일반 지침을 제공합니다.

Active IQ Unified Manager 워크시트

Active IQ Unified Manager를 설치, 구성 및 연결하기 전에 사용자 환경에 대한 특정 정보를 즉시 사용할 수 있어야 합니다. 워크시트에 정보를 기록할 수 있습니다.

Unified Manager 설치 정보

소프트웨어가 구축된 가상 머신입니다	귀사의 가치
ESXi 서버 IP 주소입니다	
호스트 정규화된 도메인 이름입니다	
호스트 IP 주소입니다	
네트워크 마스크	
게이트웨이 IP 주소입니다	
기본 DNS 주소입니다	
보조 DNS 주소입니다	
도메인 검색	
유지보수 사용자 이름입니다	
유지보수 사용자 암호입니다	

Unified Manager 구성 정보

설정	귀사의 가치
유지보수 사용자 이메일 주소	

NTP 서버	
SMTP 서버 호스트 이름 또는 IP 주소입니다	
SMTP 사용자 이름입니다	
SMTP 암호	
SMTP 기본 포트	25(기본값)
알림 알림이 전송되는 이메일입니다	
LDAP 바인딩 고유 이름입니다	
LDAP 바인딩 암호입니다	
Active Directory 관리자 이름입니다	
Active Directory 암호입니다	
인증 서버 기본 고유 이름입니다	
인증 서버 호스트 이름 또는 IP 주소입니다	

클러스터 정보

Unified Manager의 각 클러스터에 대해 다음 정보를 수집합니다.

클러스터 1/N	귀사의 가치
호스트 이름 또는 클러스터 관리 IP 주소입니다	
ONTAP 관리자 사용자 이름입니다 관리자는 "admin" 역할을 할당해야 합니다.	
ONTAP 관리자 암호입니다	
프로토콜(HTTP 또는 HTTPS)	

관련 정보

"관리자 인증 및 RBAC"

Active IQ Unified Manager를 설치합니다

Active IQ Unified Manager 다운로드 및 배포

소프트웨어를 설치하려면 가상 어플라이언스(VA) 설치 파일을 다운로드한 다음 VMware vSphere Client를 사용하여 VMware ESXi 서버에 파일을 구축해야 합니다. VA는 OVA 파일에서 사용할 수 있습니다.

단계

1. NetApp Support 사이트 소프트웨어 다운로드 * 페이지로 이동하여 Active IQ Unified Manager을 찾으십시오.

   https://mysupport.netapp.com/products/index.html

2. Select Platform * (플랫폼 선택 *) 드롭다운 메뉴에서 * VMware vSphere * 를 선택하고 * Go! * (이동! *)를 클릭합니다
3. VMware vSphere Client에서 액세스할 수 있는 로컬 또는 네트워크 위치에 ""OVA"" 파일을 저장합니다.
4. VMware vSphere Client에서 * File * > * Deploy OVF Template * 을 클릭합니다.
5. ""OVA" 파일을 찾아 마법사를 사용하여 ESXi 서버에 가상 어플라이언스를 구축합니다.

   마법사의 * 속성 * 탭을 사용하여 정적 구성 정보를 입력할 수 있습니다.

6. VM의 전원을 켭니다.
7. 초기 부팅 프로세스를 보려면 * Console * 탭을 클릭합니다.
8. 프롬프트에 따라 VM에 VMware Tools를 설치합니다.
9. 시간대를 구성합니다.
10. 유지보수 사용자 이름과 암호를 입력합니다.
11. VM 콘솔에 표시된 URL로 이동합니다.

초기 Active IQ Unified Manager 설정을 구성합니다

Active IQ Unified Manager 초기 설정 대화 상자는 웹 UI에 처음 액세스할 때 나타나며, 이 대화 상자에서 일부 초기 설정을 구성하고 클러스터를 추가할 수 있습니다.

단계

1. 기본 AutoSupport 사용 설정을 적용합니다.
2. NTP 서버 세부 정보, 유지보수 사용자 이메일 주소, SMTP 서버 호스트 이름 및 추가 SMTP 옵션을 입력한 다음 * 저장 * 을 클릭합니다.

작업을 마친 후

초기 설정이 완료되면 클러스터 세부 정보를 추가할 수 있는 클러스터 데이터 소스 페이지가 표시됩니다.

모니터링할 클러스터를 지정합니다

클러스터를 모니터링하고, 클러스터 검색 상태를 확인하고, 성능을 모니터링하려면 Active IQ Unified Manager 서버에 클러스터를 추가해야 합니다.

필요한 것

- 다음 정보가 있어야 합니다.
  - 호스트 이름 또는 클러스터 관리 IP 주소입니다

    호스트 이름은 Unified Manager에서 클러스터에 연결하는 데 사용하는 FQDN(정규화된 도메인 이름) 또는 짧은 이름입니다. 이 호스트 이름은 클러스터 관리 IP 주소로 확인되어야 합니다.

  클러스터 관리 IP 주소는 관리 스토리지 가상 시스템(SVM)의 클러스터 관리 LIF여야 합니다. 노드 관리 LIF를 사용하면 작업이 실패합니다.

  - ONTAP 관리자 사용자 이름 및 암호
  - 클러스터에서 구성할 수 있는 프로토콜 유형(HTTP 또는 HTTPS) 및 클러스터의 포트 번호입니다
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- ONTAP 관리자는 ONTAPI 및 SSH 관리자 역할이 있어야 합니다.
- Unified Manager FQDN이 ONTAP을 ping할 수 있어야 합니다.

  ONTAP 명령 'ping-node_node_name_-destination_Unified_Manager_FQDN_'을 사용하여 이를 확인할 수 있습니다.

이 작업에 대해

MetroCluster 구성의 경우 로컬 클러스터와 원격 클러스터를 모두 추가해야 하며 클러스터가 올바르게 구성되어야 합니다.

단계

1. 구성 * > * 클러스터 데이터 소스 * 를 클릭합니다.
2. 클러스터 페이지에서 * 추가 * 를 클릭합니다.
3. 클러스터 추가 * 대화 상자에서 클러스터의 호스트 이름 또는 IP 주소(IPv4 또는 IPv6), 사용자 이름, 암호, 통신 프로토콜 및 포트 번호와 같은 필수 값을 지정합니다.

   기본적으로 HTTPS 프로토콜이 선택됩니다.

   클러스터 관리 IP 주소를 IPv6에서 IPv4로, 또는 IPv4에서 IPv6로 변경할 수 있습니다. 새 IP 주소는 다음 모니터링 주기가 완료된 후 클러스터 그리드 및 클러스터 구성 페이지에 반영됩니다.

4. 추가 * 를 클릭합니다.
5. HTTPS를 선택한 경우 다음 단계를 수행하십시오.

   a. 호스트 인증 * 대화 상자에서 * 인증서 보기 * 를 클릭하여 클러스터에 대한 인증서 정보를 봅니다.

   b. 예 * 를 클릭합니다.

      Unified Manager는 처음에 클러스터가 추가된 경우에만 인증서를 검사하지만 ONTAP에 대한 각 API 호출에서는 인증서를 확인하지 않습니다.

   인증서가 만료된 경우 클러스터를 추가할 수 없습니다. SSL 인증서를 갱신한 다음 클러스터를 추가해야 합니다.

6. * 선택 사항 *: 클러스터 검색 상태 보기:

a. Cluster Setup * 페이지에서 클러스터 검색 상태를 검토합니다.

기본 모니터링 간격 약 15분이 지나면 클러스터가 Unified Manager 데이터베이스에 추가됩니다.

기본 모니터링 작업을 설정합니다

매일 모니터링을 수행합니다

매일 모니터링을 수행하여 즉각적인 성능 문제가 발생하지 않도록 주의할 수 있습니다.

단계

1. Active IQ Unified Manager UI에서 * 이벤트 인벤토리 * 페이지로 이동하여 현재 이벤트와 사용되지 않는 이벤트를 모두 봅니다.
2. View* 옵션에서 "활성 성능 이벤트"를 선택하고 필요한 조치를 결정합니다.

매주 및 매월 성과 추세를 사용하여 성과 문제를 식별합니다

성능 추세를 파악하면 볼륨 지연 시간을 분석하여 클러스터가 과도하게 사용되고 있는지 또는 제대로 사용되고 있지 않는지를 파악하는 데 도움이 됩니다. 유사한 단계를 사용하여 CPU, 네트워크 또는 기타 시스템 병목 현상을 식별할 수 있습니다.

단계

1. 사용량이 적거나 과용되고 있다고 의심되는 볼륨을 찾습니다.
2. 볼륨 세부 정보 * 탭에서 * 30 d * 를 클릭하여 기록 데이터를 표시합니다.
3. "데이터 구분 기준" 드롭다운 메뉴에서 * 지연 시간 * 을 선택한 다음 * 제출 * 을 클릭합니다.
4. 클러스터 구성 요소 비교 차트에서 * Aggregate * 를 선택 취소한 다음 클러스터 지연 시간을 볼륨 지연 시간 차트와 비교합니다.
5. 클러스터 구성 요소 비교 차트에서 * Aggregate * 를 선택하고 다른 모든 구성 요소를 선택 취소한 다음, 애그리게이트 지연 시간과 볼륨 지연 시간 차트를 비교합니다.
6. 읽기/쓰기 지연 시간 차트를 볼륨 지연 시간 차트와 비교합니다.
7. 클라이언트 애플리케이션 로드로 인해 워크로드 경합이 발생했는지 확인하고 필요에 따라 워크로드를 재조정합니다.
8. Aggregate가 초과 사용되고 있는지 확인하고 필요에 따라 경합 및 워크로드 균형을 조정합니다.

성능 임계값을 사용하여 이벤트 알림을 생성합니다

이벤트는 미리 정의된 조건이 발생하거나 성능 카운터 값이 임계값을 초과할 때 Active IQ Unified Manager에서 자동으로 생성되는 알림입니다. 이벤트는 모니터링 중인 클러스터에서 성능 문제를 식별하는 데 도움이 됩니다. 특정 심각도 유형의 이벤트가 발생할 때 전자 메일 알림을 자동으로 보내도록 알림을 구성할 수 있습니다.

성능 임계값을 설정합니다

성능 임계값을 설정하여 중요한 성능 문제를 모니터링할 수 있습니다. 사용자 정의 임계값은 시스템이 정의된 임계값에 접근하거나 이를 초과할 경우 경고 또는 중요 이벤트 알림을

트리거합니다.

단계

1. 경고 및 위험 이벤트 임계값을 생성합니다.
   a. 구성 * > * 성능 임계값 * 을 선택합니다.
   b. Create * 를 클릭합니다.
   c. 객체 유형을 선택하고 정책의 이름과 설명을 지정합니다.
   d. 개체 카운터 조건을 선택하고 경고 및 위험 이벤트를 정의하는 제한 값을 지정합니다.
   e. 이벤트를 전송할 때 제한 값을 위반해야 하는 기간을 선택한 다음 * 저장 * 을 클릭합니다.
2. 스토리지 객체에 임계값 정책을 할당합니다.
   a. 이전에 선택한 것과 동일한 클러스터 객체 유형에 대한 인벤토리 페이지로 이동하여 보기 옵션에서 * 성능 * 을 선택합니다.
   b. 임계값 정책을 할당할 개체를 선택한 다음 * 임계값 정책 할당 * 을 클릭합니다.
   c. 이전에 생성한 정책을 선택한 다음 * 정책 할당 * 을 클릭합니다.

예

사용자 정의 임계값을 설정하여 중요한 성능 문제를 확인할 수 있습니다. 예를 들어, Microsoft Exchange Server가 있는데 볼륨 지연 시간이 20밀리초를 초과하면 오류가 발생하는 경우 경고 임계값을 12밀리초로 설정하고 임계치를 15밀리초로 설정할 수 있습니다. 이 임계값 설정을 사용하면 볼륨 지연 시간이 제한을 초과할 때 알림을 받을 수 있습니다.

알림을 추가합니다

특정 이벤트가 생성될 때 알림을 표시하도록 알림을 구성할 수 있습니다. 단일 리소스, 리소스 그룹 또는 특정 심각도 유형의 이벤트에 대한 알림을 구성할 수 있습니다. 알림을 받을 빈도를 지정하고 스크립트를 알림에 연결할 수 있습니다.

필요한 것

- Active IQ Unified Manager 서버가 이러한 설정을 사용하여 이벤트가 생성될 때 사용자에게 알림을 보낼 수 있도록 하려면 사용자 e-메일 주소, SMTP 서버 및 SNMP 트랩 호스트와 같은 알림 설정을 구성해야 합니다.
- 알림을 트리거할 리소스 및 이벤트와 알림을 보낼 사용자의 사용자 이름 또는 이메일 주소를 알고 있어야 합니다.
- 이벤트를 기반으로 스크립트를 실행하려면 스크립트 페이지를 사용하여 Unified Manager에 스크립트를 추가해야 합니다.
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이 작업에 대해

여기서 설명하는 대로 알림 설정 페이지에서 알림을 생성할 뿐만 아니라 이벤트를 수신한 후 이벤트 세부 정보 페이지에서 직접 알림을 생성할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 경고 설정 * 을 클릭합니다.
2. Alert Setup * 페이지에서 * Add * 를 클릭합니다.
3. 경고 추가 * 대화 상자에서 * 이름 * 을 클릭하고 경고의 이름과 설명을 입력합니다.
4. 리소스 * 를 클릭하고 경고에 포함되거나 제외될 리소스를 선택합니다.

   이름 포함 * 필드에서 텍스트 문자열을 지정하여 리소스 그룹을 선택하여 필터를 설정할 수 있습니다. 지정한 텍스트 문자열을 기준으로 사용 가능한 자원 목록에는 필터 규칙과 일치하는 자원만 표시됩니다. 지정하는 텍스트 문자열은 대/소문자를 구분합니다.

   자원이 지정한 포함 및 제외 규칙을 모두 준수하는 경우 제외 규칙이 포함 규칙보다 우선하며 제외된 리소스와 관련된 이벤트에 대해서는 알림이 생성되지 않습니다.

5. 이벤트 * 를 클릭하고 알림을 트리거할 이벤트 이름 또는 이벤트 심각도 유형을 기반으로 이벤트를 선택합니다.

   둘 이상의 이벤트를 선택하려면 Ctrl 키를 누른 상태에서 원하는 항목을 선택합니다.

6. Actions * 를 클릭하고 알릴 사용자를 선택하고, 알림 빈도를 선택하고, SNMP 트랩을 트랩 수신기로 전송할지 여부를 선택한 다음, 경고가 생성될 때 실행할 스크립트를 할당합니다.

   사용자에 대해 지정된 전자 메일 주소를 수정하고 편집을 위해 알림을 다시 열면 수정된 전자 메일 주소가 이전에 선택한 사용자에게 더 이상 매핑되지 않으므로 이름 필드가 비어 있습니다. 또한 사용자 페이지에서 선택한 사용자의 전자 메일 주소를 수정한 경우 선택한 사용자에 대해 수정된 전자 메일 주소가 업데이트되지 않습니다.

   SNMP 트랩을 통해 사용자에게 알리도록 선택할 수도 있습니다.

7. 저장 * 을 클릭합니다.

알림 추가 예

이 예제에서는 다음 요구 사항을 충족하는 알림을 생성하는 방법을 보여 줍니다.

- 알림 이름: 상태 테스트
- 리소스: 이름에 "abc"가 포함된 모든 볼륨을 포함하며 이름에 "xyz"가 포함된 모든 볼륨을 제외합니다.
- 이벤트: 모든 중요한 상태 이벤트를 포함합니다
- 작업: "sample@domain.com", "테스트" 스크립트를 포함하며 사용자에게 15분마다 알림을 받아야 합니다

경고 추가 대화 상자에서 다음 단계를 수행합니다.

1. 이름 * 을 클릭하고 * 알림 이름 * 필드에 '상태 테스트'를 입력합니다.
2. 리소스 * 를 클릭하고 포함 탭의 드롭다운 목록에서 * 볼륨 * 을 선택합니다.
   a. 이름에 abc가 포함된 볼륨을 표시하려면 * Name Contains * 필드에 abc를 입력합니다.
   b. 를 선택합니다[All Volumes whose name contains 'abc']Available Resources 영역에서 + * 를 선택한 다음 Selected Resources 영역으로 이동합니다.
   c. 제외 * 를 클릭하고 * 이름 포함 * 필드에 'xyz'를 입력한 다음 * 추가 * 를 클릭합니다.
3. 이벤트 * 를 클릭하고 이벤트 심각도 필드에서 * 긴급 * 을 선택합니다.

4. Matching Events 영역에서 * All Critical Events * 를 선택하고 Selected Events 영역으로 이동합니다.
5. [동작] * 을 클릭하고 다음 사용자에게 알림 필드에 'ample@domain.com'을 입력합니다.
6. 15분마다 사용자에게 알리려면 * 15분마다 알림 * 을 선택합니다.

   지정된 시간 동안 수신자에게 반복적으로 알림을 보내도록 알림을 구성할 수 있습니다. 알림에 대해 이벤트 알림이 활성화되는 시간을 결정해야 합니다.

7. 실행할 스크립트 선택 메뉴에서 * 테스트 * 스크립트를 선택합니다.
8. 저장 * 을 클릭합니다.

경고 설정을 구성합니다

Active IQ Unified Manager에서 알림을 트리거할 이벤트, 해당 알림의 e-메일 받는 사람 및 알림 빈도를 지정할 수 있습니다.

필요한 것

애플리케이션 관리자 역할이 있어야 합니다.

이 작업에 대해

다음 유형의 성능 이벤트에 대해 고유한 알림 설정을 구성할 수 있습니다.

- 사용자 정의 임계값 위반으로 인해 발생하는 중요 이벤트입니다
- 경고 이벤트는 사용자 정의 임계값, 시스템 정의 임계값 또는 동적 임계값 위반으로 인해 발생합니다

기본적으로 모든 새 이벤트에 대해 Unified Manager 관리 사용자에게 이메일 경고가 전송됩니다. 해당 사용자의 전자 메일 주소를 추가하여 다른 사용자에게 전자 메일 알림을 보낼 수 있습니다.

> 특정 유형의 이벤트에 대해 알림이 전송되지 않도록 하려면 이벤트 범주의 모든 확인란의 선택을 해제해야 합니다. 이 작업을 수행해도 이벤트가 사용자 인터페이스에 나타나지 않습니다.

단계

1. 왼쪽 탐색 창에서 * Storage Management * > * Alert Setup * 을 선택합니다.

   경고 설정 페이지가 표시됩니다.

2. 추가 * 를 클릭하고 각 이벤트 유형에 적절한 설정을 구성합니다.

   여러 사용자에게 전자 메일 알림을 보내려면 각 전자 메일 주소 사이에 쉼표를 입력합니다.

3. 저장 * 을 클릭합니다.

Active IQ Unified Manager의 성능 문제를 식별합니다

성능 이벤트가 발생하면 Active IQ Unified Manager에서 문제의 원인을 찾아 다른 도구를 사용하여 문제를 해결할 수 있습니다. 매일 모니터링하는 동안 이벤트에 대한 이메일 알림을 받거나 이벤트를 알릴 수 있습니다.

단계

1. e-메일 알림의 링크를 클릭하면 성능 이벤트가 있는 스토리지 객체로 직접 이동됩니다.

만약…	그러면…
이벤트에 대한 이메일 알림을 받습니다	링크를 클릭하여 이벤트 세부 정보 페이지로 직접 이동합니다.
이벤트 인벤토리 페이지를 분석하는 동안 이벤트를 확인합니다	이벤트 세부 정보 페이지로 직접 이동할 이벤트를 선택합니다.

2. 이벤트가 시스템 정의 임계값을 초과한 경우 UI에서 제안된 작업을 수행하여 문제를 해결하십시오.
3. 이벤트가 사용자 정의 임계값을 초과한 경우 이벤트를 분석하여 조치를 취해야 하는지 결정합니다.
4. 문제가 지속되면 다음 설정을 확인하십시오.
   - 스토리지 시스템의 프로토콜 설정입니다
   - 이더넷 또는 패브릭 스위치의 네트워크 설정
   - 스토리지 시스템의 네트워크 설정입니다
   - 스토리지 시스템의 디스크 레이아웃 및 애그리게이트 메트릭
5. 문제가 지속되면 기술 지원 팀에 지원을 요청하십시오.

Active IQ 디지털 어드바이저를 사용하여 시스템 성능을 확인합니다

AutoSupport 툴을 NetApp으로 전송하는 모든 ONTAP 시스템에서 포괄적인 성능 및 용량 데이터를 볼 수 있습니다. Active IQ는 System Manager에서 볼 수 있는 것보다 더 오랜 기간 동안의 시스템 성능을 보여 줍니다.

CPU 활용률, 지연 시간, IOPS, 프로토콜별 IOPS, 네트워크 처리량을 보여주는 그래프를 볼 수 있습니다. 다른 도구에서 분석할 수 있도록 이 데이터를 .csv 형식으로 다운로드할 수도 있습니다.

이 성능 데이터 외에도 Active IQ은 워크로드별 스토리지 효율성을 제공하고 해당 효율성을 해당 유형의 워크로드에 대한 예상 효율성과 비교할 수 있습니다. 용량 추세를 보고 특정 기간에 추가해야 할 추가 스토리지 양을 예측할 수 있습니다.

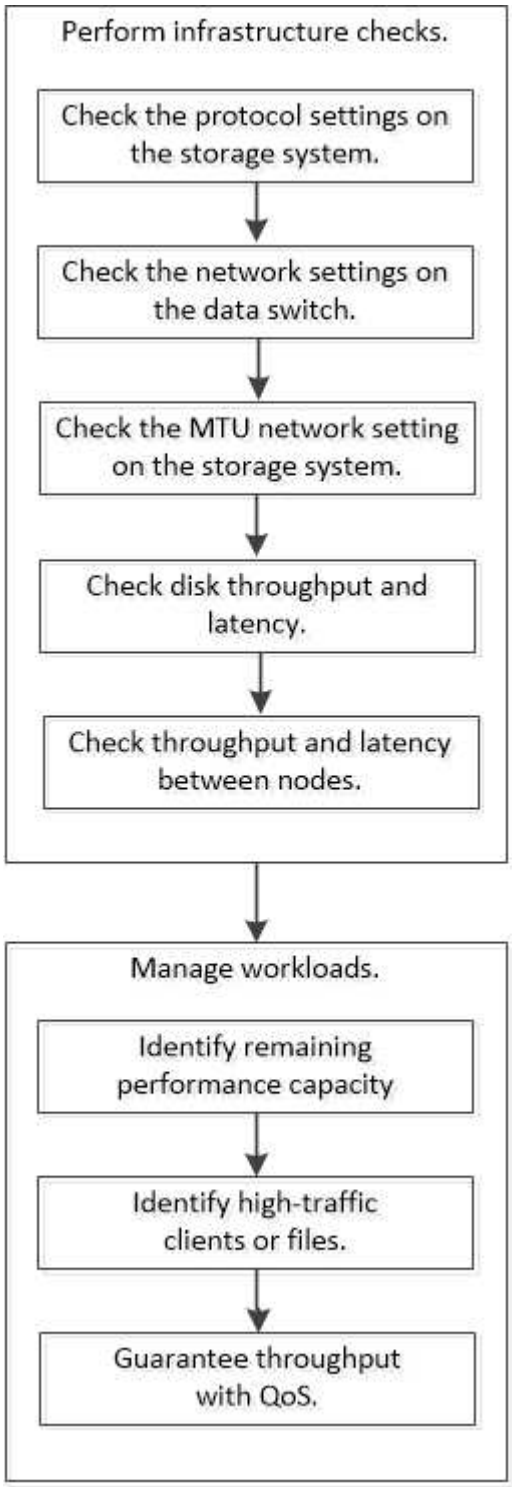
- 스토리지 효율성은 기본 대시보드 왼쪽의 고객, 클러스터 및 노드 레벨에서 사용할 수 있습니다.
- 성능은 메인 대시보드 왼쪽의 클러스터 및 노드 레벨에서 사용할 수 있습니다.

관련 정보

- "Active IQ 디지털 자문 문서"
- "Active IQ 디지털 자문 비디오 재생 목록"
- "Active IQ 웹 포털"

성능 문제 관리

성능 문제를 식별한 후 인프라에 대한 몇 가지 기본적인 진단 검사를 수행하여 명백한 구성 오류를 배제할 수 있습니다. 정확히 찾아내지 못하는 문제라면 워크로드 관리 문제를 살펴보는 것이 좋습니다.



기본 인프라 검사를 수행합니다

NFS TCP 최대 전송 크기를 확인합니다

NFS의 경우 읽기 및 쓰기에 대한 TCP 최대 전송 크기가 성능 문제를 일으킬 수 있는지 확인할 수 있습니다. 크기가 성능을 저하한다고 생각되면 크기를 늘릴 수 있습니다.

필요한 것

- 이 작업을 수행하려면 클러스터 관리자 권한이 있어야 합니다.
- 이 작업에는 고급 권한 레벨 명령을 사용해야 합니다.

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

2. TCP 최대 전송 크기를 확인합니다.

   'vserver nfs show -vserver_vserver_name_-instance'

3. TCP 최대 전송 크기가 너무 작은 경우 크기를 늘립니다.

   'vserver nfs modify -vserver_vserver_name_-tcp-max -xfer-size_integer_'

4. 관리 권한 수준으로 돌아가기:

   'Set-Privilege admin'입니다

예

다음 예에서는 'VM1'의 TCP 최대 전송 크기를 1048576으로 변경합니다.

```
cluster1::*> vserver nfs modify -vserver SVM1 -tcp-max-xfer-size 1048576
```

iSCSI TCP 읽기/쓰기 크기를 확인합니다

iSCSI의 경우 TCP 읽기/쓰기 크기를 확인하여 크기 설정이 성능 문제를 생성하고 있는지 확인할 수 있습니다. 크기가 문제의 원인이면 수정할 수 있습니다.

필요한 것

이 작업에는 고급 권한 레벨 명령이 필요합니다.

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

2. TCP 윈도우 크기 설정을 확인합니다.

'vserver iscsi show-vserv, er_vserver_name_-instance'

3. TCP 창 크기 설정을 수정합니다.

   'vserver iscsi modify -vserver_vserver_name_-tcp-window-size_integer_'

4. 관리 권한으로 돌아가기:

   'Set-Privilege admin'입니다

예

다음 예에서는 'VM1'의 TCP 윈도우 크기를 131,400바이트로 변경합니다.

```
cluster1::*> vserver iscsi modify -vserver vs1 -tcp-window-size 131400
```

CIFS 다중통신 설정을 점검하십시오

느린 CIFS 네트워크 성능으로 인해 성능 문제가 발생하는 경우 멀티플렉스 설정을 수정하여 성능을 개선하고 수정할 수 있습니다.

단계

1. CIFS 다중통신 설정을 점검한다.

   'vserver cifs options show -vserver_-vserver_name_-instance'

2. CIFS 다중통신 설정을 수정합니다.

   'vserver cifs options modify – vserver_-vserver_name_ – max-MPX_integer _'

예

다음 예에서는 'VM1'의 최대 다중통신 횟수를 255로 변경한다.

```
cluster1::> vserver cifs options modify -vserver SVM1 -max-mpx 255
```

FC 어댑터의 포트 속도를 확인합니다

어댑터 대상 포트 속도는 성능을 최적화하기 위해 연결된 장치의 속도와 일치해야 합니다. 포트가 autonegotiation으로 설정된 경우 테이크오버 및 반환 또는 기타 중단이 발생한 후 다시 연결하는 데 시간이 더 오래 걸릴 수 있습니다.

필요한 것

이 어댑터를 홈 포트로 사용하는 모든 LIF는 오프라인 상태여야 합니다.

단계

1. 어댑터를 오프라인 상태로 전환:

'network fcp adapter modify -node_nodename_-adapter_adapter_-state_down_'

2. 포트 어댑터의 최대 속도를 확인합니다.

   FCP 어댑터 show-instance(FCP 어댑터 show-instance)

3. 필요한 경우 포트 속도를 변경합니다.

   'network fcp adapter modify -node_nodename_-adapter_adapter_-speed{1|2|4|8|10|16|auto}'

4. 어댑터를 온라인으로 전환합니다.

   'network fcp adapter modify -node_nodename_-adapter_adapter_ - state up'

5. 어댑터에 있는 모든 LIF를 온라인으로 전환합니다.

   'network interface modify -vserver * -lif * {-home-node node1 -home-port e0c} -status -admin up'

예

다음 예에서는 node1의 어댑터 0d의 포트 속도를 2Gbps로 변경합니다.

```
cluster1::> network fcp adapter modify -node node1 -adapter 0d -speed 2
```

데이터 스위치의 네트워크 설정을 확인합니다

클라이언트, 서버 및 스토리지 시스템(즉, 네트워크 엔드포인트)에서 동일한 MTU 설정을 유지해야 하지만 성능에 영향을 주지 않도록 NIC 및 스위치와 같은 중간 네트워크 디바이스를 최대 MTU 값으로 설정해야 합니다.

최상의 성능을 얻으려면 네트워크의 모든 구성 요소가 점보 프레임(9000바이트 IP, 9022바이트 이더넷 포함)을 포워드할 수 있어야 합니다. 데이터 스위치는 최소 9022바이트로 설정해야 하지만 대부분의 스위치에서 일반적인 값 9216을 사용할 수 있습니다.

절차를 참조하십시오

데이터 스위치의 경우 MTU 크기가 9022 이상으로 설정되어 있는지 확인합니다.

자세한 내용은 스위치 공급업체 설명서를 참조하십시오.

스토리지 시스템에서 **MTU** 네트워크 설정을 확인합니다

스토리지 시스템의 네트워크 설정이 클라이언트 또는 다른 네트워크 엔드포인트와 동일하지 않은 경우 변경할 수 있습니다. 관리 네트워크 MTU 설정은 1500으로 설정되어 있지만 데이터 네트워크 MTU 크기는 9000이어야 합니다.

이 작업에 대해

브로드캐스트 도메인 내의 모든 포트는 MTU 크기가 동일하며 e0M 포트 처리 관리 트래픽을 제외하고 있습니다. 포트가 broadcast-domain의 일부인 경우 broadcast-domain modify 명령을 사용하여 수정된 broadcast-domain 내의 모든 포트에 대한 MTU를 변경한다.

NIC 및 데이터 스위치와 같은 중간 네트워크 장치는 네트워크 엔드포인트보다 더 높은 MTU 크기로 설정할 수 있습니다. 자세한 내용은 을 참조하십시오 "데이터 스위치의 네트워크 설정을 확인합니다".

단계

1. 스토리지 시스템에서 MTU 포트 설정을 확인합니다.

   네트워크 포트 show-instance

2. 포트에서 사용하는 브로드캐스트 도메인의 MTU를 변경합니다.

   'network port broadcast-domain modify -IPSpace_IPSpace_-broadcast-domain_broadcast_domain_ -MTU_new_MTU_'

예

다음 예에서는 MTU 포트 설정을 9000으로 변경합니다.

```
network port broadcast-domain modify -ipspace Cluster -broadcast-domain
Cluster -mtu 9000
```

디스크 처리량 및 지연 시간 확인

클러스터 노드의 디스크 처리량 및 지연 시간 메트릭을 확인하여 문제 해결을 지원할 수 있습니다.

이 작업에 대해

이 작업에는 고급 권한 레벨 명령이 필요합니다.

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

2. 디스크 처리량 및 지연 시간 메트릭을 확인합니다.

   '디스크 표시 정렬 키 지연'

예

다음 예제는 'cluster1'의 'node2'에 대한 각 사용자의 읽기 또는 쓰기 작업의 합계를 표시합니다.

```
::*> statistics disk show -sort-key latency
cluster1 : 8/24/2015 12:44:15
                     Busy Total Read  Write  Read    Write   *Latency
  Disk       Node   (%)   Ops   Ops   Ops   (Bps)    (Bps)       (us)
------------ ----   ---- ----   ----- ----- ------   -----    -----

1.10.20      node2     4    5       3     2  95232  367616    23806
1.10.8       node2     4    5       3     2 138240  386048    22113

1.10.6       node2     3    4       2     2  48128  371712    19113
1.10.19      node2     4    6       3     2 102400  443392    19106

1.10.11      node2     4    4       2     2 122880  408576    17713
```

노드 간 처리량과 지연 시간을 확인합니다

'network test-path' 명령을 사용하여 네트워크 병목 현상을 식별하거나 노드 간 네트워크 경로를 다시 확인할 수 있습니다. 클러스터 간 노드 또는 클러스터 내 노드 간에 명령을 실행할 수 있습니다.

필요한 것

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 이 작업에는 고급 권한 레벨 명령이 필요합니다.
- 인터클러스터 경로의 경우 소스 클러스터와 대상 클러스터를 피어링해야 합니다.

이 작업에 대해

노드 간 네트워크 성능이 경로 구성에 대한 기대치를 충족하지 못하는 경우가 있습니다. 예를 들어, SnapMirror 복제 작업에서 볼 수 있는 대규모 데이터 전송 유형에 대한 1Gbps의 전송 속도는 소스 클러스터와 대상 클러스터 간의 10GbE 링크와 일치하지 않습니다.

network test-path 명령을 사용하여 노드 간 처리량과 대기 시간을 측정할 수 있습니다. 클러스터 간 노드 또는 클러스터 내 노드 간에 명령을 실행할 수 있습니다.

> 이 테스트는 데이터가 네트워크 경로를 포화시키기 때문에, 시스템이 사용 중이 아닐 때나 노드 간 네트워크 트래픽이 과도하지 않을 때는 명령을 실행해야 합니다. 10초 후 테스트 시간이 초과됩니다. 명령은 ONTAP 9 노드 간에만 실행할 수 있습니다.

'세션 유형' 옵션은 네트워크 경로를 통해 실행 중인 작업 유형을 식별합니다(예: 원격 대상에 대한 SnapMirror 복제를 위한 "AsyncMirrorRemote"). 유형은 테스트에 사용되는 데이터의 양을 나타냅니다. 다음 표에서는 세션 유형을 정의합니다.

세션 유형	설명
AsyncMirrorLocal 을 선택합니다	동일한 클러스터의 노드 간에 SnapMirror가 사용하는 설정입니다

AsyncMirrorRemote 를 참조하십시오	서로 다른 클러스터 노드 간에 SnapMirror가 사용하는 설정(기본 유형)
RemoteDataTransfer를 참조하십시오	ONTAP에서 동일한 클러스터의 노드 간 원격 데이터 액세스를 위해 사용하는 설정(예: 다른 노드의 볼륨에 저장된 파일에 대해 노드에 NFS 요청)

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

2. 노드 간 처리량 및 지연 시간 측정:

   'network test-path-source-node_source_nodename_|local-destination-cluster_destination_clustername_-destination-node_destination_nodename_-session-type Default|AsyncMirrorLocal|AsyncMirrorRemote|SyncMirrorRemote|RemoteDataTransfer'

   소스 노드는 로컬 클러스터에 있어야 합니다. 대상 노드는 로컬 클러스터 또는 피어링된 클러스터에 있을 수 있습니다. '-source-node'의 "local" 값은 명령을 실행하는 노드를 지정합니다.

   다음 명령을 실행하면 로컬 클러스터의 노드1과 클러스터2의 노드3의 SnapMirror 유형 복제 작업에 대한 처리량과 지연 시간이 측정됩니다.

   ```
   cluster1::> network test-path -source-node node1 -destination-cluster
   cluster2 -destination-node node3 -session-type AsyncMirrorRemote
   Test Duration:      10.88 secs
   Send Throughput:    18.23 MB/sec
   Receive Throughput: 18.23 MB/sec
   MB sent:            198.31
   MB received:        198.31
   Avg latency in ms:  2301.47
   Min latency in ms:  61.14
   Max latency in ms:  3056.86
   ```

3. 관리 권한으로 돌아가기:

   'Set-Privilege admin'입니다

작업을 마친 후

성능이 경로 구성에 대한 기대를 충족하지 않는 경우 노드 성능 통계를 확인하고, 사용 가능한 툴을 사용하여 네트워크에서 문제를 격리하고, 스위치 설정을 확인하는 등의 작업을 수행해야 합니다.

워크로드 관리

성능 용량, 즉_FLO여유_는 리소스의 워크로드 성능이 지연 시간의 영향을 받기 전에 노드나 애그리게이트에 배치할 수 있는 작업의 양을 측정합니다. 클러스터에서 사용 가능한 성능 용량을 파악하면 워크로드를 프로비저닝하고 조정할 수 있습니다.

필요한 것

이 작업에는 고급 권한 레벨 명령이 필요합니다.

이 작업에 대해

'-object' 옵션에 다음 값을 사용하여 여유 공간 통계를 수집하고 표시할 수 있습니다.

- CPU의 경우 resource_refLO여유_cpu’입니다.
- Aggregate의 경우 RESOURCE_LOBLO여유_aggr입니다.

System Manager 및 Active IQ Unified Manager를 사용하여 이 작업을 완료할 수도 있습니다.

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

2. 실시간 여유 공간 통계 수집 시작:

   '통계 시작 – object resource_refo여유_cpu|aggr'

   전체 명령 구문은 man 페이지를 참조하십시오.

3. 실시간 여유 공간 통계 정보 표시:

   'tortistics show-object resource_fre여유_cpu|aggr'

   전체 명령 구문은 man 페이지를 참조하십시오.

4. 관리 권한으로 돌아가기:

   'Set-Privilege admin’입니다

예

다음 예제에는 클러스터 노드의 평균 사용 시간 여유 공간 통계가 표시됩니다.

Optimal_point_Utilization 카운터에서 Current_Utilization 카운터를 빼서 노드에 대해 사용 가능한 성능 용량을 계산할 수 있습니다. 이 예에서는 CPU_sti2520-213의 사용률 용량이 -14%(72%-86%)로, 이는 CPU가 지난 1시간 동안 평균 초과 사용되었음을 나타냅니다.

같은 정보를 더 오랜 기간 평균한 값으로 얻기 위해 'ewma_daily', 'ewma_weekly', 'ewma_monthly’를 지정할 수도 있습니다.

```
sti2520-2131454963690::*> statistics show -object resource_headroom_cpu
-raw -counter ewma_hourly
  (statistics show)

Object: resource_headroom_cpu
Instance: CPU_sti2520-213
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-213

    Counter                                                     Value
    -------------------------------- ---------------------------------
    ewma_hourly                                                     -
                         current_ops                             4376
                     current_latency                            37719
                current_utilization                               86
                  optimal_point_ops                             2573
              optimal_point_latency                             3589
           optimal_point_utilization                              72
     optimal_point_confidence_factor                               1

Object: resource_headroom_cpu
Instance: CPU_sti2520-214
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-214

    Counter                                                     Value
    -------------------------------- ---------------------------------
    ewma_hourly                                                     -
                         current_ops                                0
                     current_latency                                0
                current_utilization                                 0
                  optimal_point_ops                                 0
              optimal_point_latency                                 0
           optimal_point_utilization                               71
     optimal_point_confidence_factor                               1
2 entries were displayed.
```

트래픽이 높은 클라이언트 또는 파일을 식별합니다

ONTAP 활성 개체 기술을 사용하여 불균형적으로 많은 양의 클러스터 트래픽을 담당하는 클라이언트 또는 파일을 식별할 수 있습니다. 이러한 "상위" 클라이언트 또는 파일을 식별한 후에는 클러스터 워크로드를 재조정하거나 다른 단계를 수행하여 문제를 해결할 수 있습니다.

필요한 것

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 클러스터에 액세스하는 상위 클라이언트 보기:

   'tortistics top client show -node_name_-sort-key_sort_column_-interval_seconds_between_updates_ -iterations_-max_number_of_instances_'

   전체 명령 구문은 man 페이지를 참조하십시오.

   다음 명령을 실행하면 'cluster1'에 액세스하는 상위 클라이언트가 표시됩니다.

```
cluster1::> statistics top client show

cluster1 : 3/23/2016 17:59:10


                                                 *Total
        Client Vserver           Node Protocol    Ops
-------------- ------- -------------- -------- ------
172.17.180.170     vs4 siderop1-vsim4      nfs    668
172.17.180.169     vs3 siderop1-vsim3      nfs    337
172.17.180.171     vs3 siderop1-vsim3      nfs    142
172.17.180.170     vs3 siderop1-vsim3      nfs    137
172.17.180.123     vs3 siderop1-vsim3      nfs    137
172.17.180.171     vs4 siderop1-vsim4      nfs     95
172.17.180.169     vs4 siderop1-vsim4      nfs     92
172.17.180.123     vs4 siderop1-vsim4      nfs     92
172.17.180.153     vs3 siderop1-vsim3      nfs      0
```

2. 클러스터에서 액세스하는 상위 파일을 봅니다.

   'tortistics top file show -node_node_name_-sort-key_sort_column_-interval_seconds_between_updates_ -iterations_-max_number_of_instances_'

   전체 명령 구문은 man 페이지를 참조하십시오.

   다음 명령을 실행하면 'cluster1'에서 액세스되는 최상위 파일이 표시됩니다.

```
cluster1::> statistics top file show

cluster1 : 3/23/2016 17:59:10

                                    *Total
                     File Volume Vserver          Node    Ops
------------------------ ------ ------- -------------- ------
/vol/vol1/vm170-read.dat   vol1     vs4 siderop1-vsim4     22
/vol/vol1/vm69-write.dat   vol1     vs3 siderop1-vsim3      6
     /vol/vol2/vm171.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol2/vm169.dat   vol2     vs3 siderop1-vsim3      2
      /vol/vol2/p123.dat   vol2     vs4 siderop1-vsim4      2
      /vol/vol2/p123.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol1/vm171.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim3      2
      /vol/vol1/p123.dat   vol1     vs4 siderop1-vsim4      2
```

QoS로 처리량 보장

QoS 개요를 통해 처리량 보장

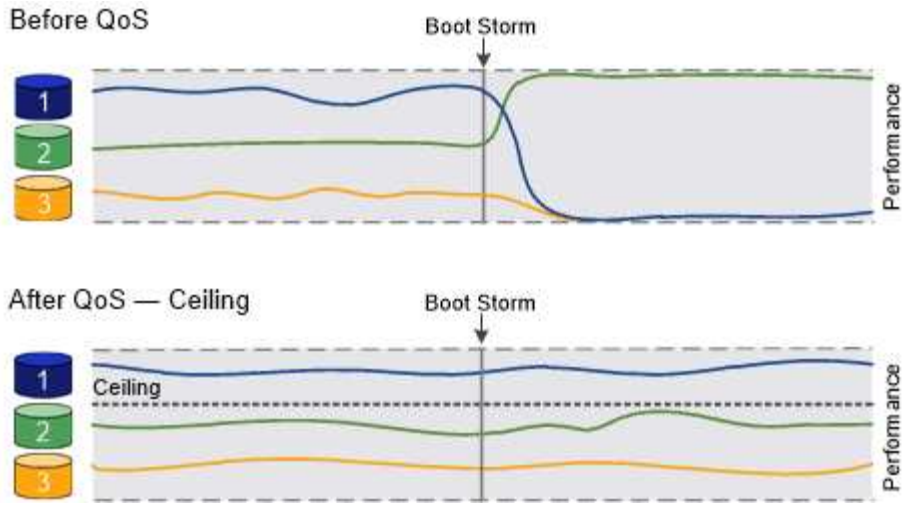
스토리지 QoS(서비스 품질)를 사용하여 주요 워크로드의 성능이 다른 워크로드에 의해 저하되지 않도록 보장할 수 있습니다. 경쟁 워크로드에 대한 throughput_ceiling_을 설정하여 시스템 리소스에 미치는 영향을 제한하거나 중요한 워크로드에 대한 throughput_floor_를 설정하여 경쟁 워크로드의 요구에 관계없이 최소 처리량 목표를 달성할 수 있습니다. 동일한 워크로드에 대해 천장과 바닥을 설정할 수도 있습니다.

처리량 천장 정보**(QoS Max)**

처리량 상한은 워크로드의 처리량을 최대 IOPS 또는 MBps, 즉 IOPS 및 MBps로 제한합니다. 아래 그림에서는 워크로드 2의 처리량 상한을 통해 워크로드 1과 3이 "괴롭지" 않도록 합니다.

policy group_은 하나 이상의 워크로드에 대한 처리량 한도를 정의합니다. 워크로드는 _ 스토리지 객체에 대한 입출력 작업을 나타냅니다. _ 볼륨, 파일, qtree 또는 LUN 또는 SVM의 모든 볼륨, 파일, Qtree 또는 LUN입니다. 정책 그룹을 생성할 때 상한을 지정하거나 워크로드를 모니터링하여 지정할 때까지 기다릴 수 있습니다.

> 워크로드에 대한 처리량이 지정된 상한을 최대 10% 초과할 수 있습니다. 특히, 작업 부하에 대한 처리량이 급격하게 변경될 경우 더욱 그렇습니다. 천장은 버스트를 처리하기 위해 최대 50%까지 초과될 수 있습니다. 토큰이 최대 150%까지 누적되면 단일 노드에서 버스트가 발생합니다



처리량 기준**(QoS Min)**

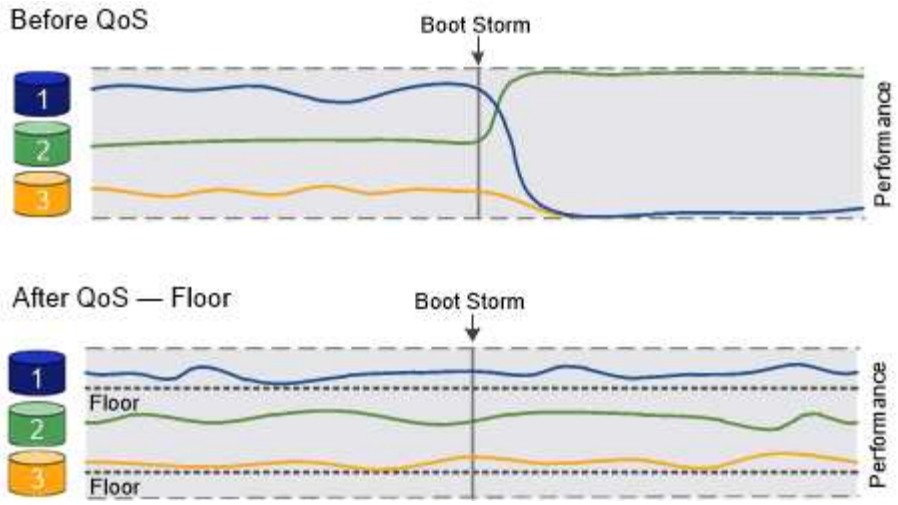
처리량 한도 에서는 워크로드의 처리량이 최소 IOPS 또는 MBps, 즉 IOPS 및 MBps 미만으로 떨어지지 않도록 보장합니다. 아래 그림에서 워크로드 1과 워크로드 3의 처리량 플로어는 워크로드 2의 수요에 관계없이 최소 처리량 목표를 충족할 수 있도록 합니다.

> 예를 들어, 처리량 상한은 처리량을 직접 조절합니다. 처리량 플로어에서는 플로어가 설정된 워크로드에 우선 순위를 부여하여 간접적으로 처리량을 조절합니다.

정책 그룹을 생성할 때 층을 지정하거나 워크로드를 모니터링하여 지정할 때까지 기다릴 수 있습니다.

ONTAP 9.13.1 부터는 을 사용하여 SVM 범위에서 처리량 플로어를 설정할 수 있습니다 [adaptive-qos-templates]. 9.13.1 이전의 ONTAP 릴리즈에서는 처리량 플로어를 정의하는 정책 그룹을 SVM에 적용할 수 없습니다.

> ONTAP 9.7 이전의 릴리즈에서는 사용 가능한 성능 용량이 충분한 경우 처리량 바닥이 보장됩니다.
>
> ONTAP 9.7 이상에서는 사용 가능한 성능 용량이 부족하더라도 처리량 플로어를 보장할 수 있습니다. 이러한 새로운 바닥 동작을 바닥 v2라고 합니다. 보장 사항을 충족하기 위해 v2층은 처리량 공간 또는 바닥 설정을 초과하는 작업 환경에서 작업 부하에 대한 대기 시간이 더 길어질 수 있습니다. 버전 v2는 QoS 및 적응형 QoS에 모두 적용됩니다.
>
> ONTAP 9.7P6 이상에서 새로운 바닥 v2의 동작을 활성화/비활성화하는 옵션을 사용할 수 있습니다. 과 같은 중요한 작업 중에는 워크로드가 지정된 설치 공간 아래로 떨어질 수 있습니다 `volume move trigger-cutover`. 충분한 용량을 사용할 수 있고 중요한 작업이 마련되어 있지 않더라도 워크로드의 처리량은 지정된 바닥 미만으로 최대 5% 떨어질 수 있습니다. 바닥이 초과 프로비저닝되고 성능 용량이 없는 경우 일부 워크로드가 지정된 설치 공간 아래로 떨어질 수 있습니다.



공유 및 비공유 **QoS** 정책 그룹에 대한 정보를 제공합니다

ONTAP 9.4부터 _non-shared_QoS 정책 그룹을 사용하여 정의된 처리량 상한 또는 최저가 각 구성원 워크로드에 개별적으로 적용되도록 지정할 수 있습니다. shared_policy 그룹의 동작은 정책 유형에 따라 달라집니다.

- 처리량 천장의 경우 공유 정책 그룹에 할당된 워크로드의 총 처리량은 지정된 한도를 초과할 수 없습니다.
- 처리량 플로어의 경우 공유 정책 그룹을 단일 워크로드에만 적용할 수 있습니다.

적응형 **QoS**에 대해 알아보십시오

일반적으로 스토리지 객체에 할당한 정책 그룹의 값은 고정됩니다. 스토리지 오브젝트의 크기가 변경되면 값을 수동으로 변경해야 합니다. 예를 들어, 볼륨에 사용된 공간의 양을 늘리려면 일반적으로 볼륨에 지정된 처리량 상한을 늘려야 합니다.

_Adaptive QoS_는 워크로드 크기에 따라 정책 그룹 값을 자동으로 확장하며 워크로드 크기 변화에 따라 IOPS와 TB|GB의 비율을 유지합니다. 이는 대규모 구축 환경에서 수백 또는 수천 개의 워크로드를 관리할 때 큰 이점입니다.

일반적으로 적응형 QoS를 사용하여 처리량 한도를 조정할 수 있지만 워크로드 크기가 증가하는 경우 이를 사용하여 처리량 플로어를 관리할 수도 있습니다. 워크로드 크기는 스토리지 객체에 할당된 공간 또는 스토리지 객체가 사용하는 공간으로 표시됩니다.

> ONTAP 9.5 이상의 처리량 층에서는 사용된 공간을 사용할 수 있습니다. ONTAP 9.4 및 이전 버전의 처리량 바닥재에서는 지원되지 않습니다.

- allocated space_policy는 스토리지 객체의 공칭 크기에 따라 IOPS/TB|GB 비율을 유지합니다. 비율이 100 IOPS/GB인 경우, 볼륨이 해당 크기로 유지되는 한 150 GB 볼륨의 처리량은 최대 15,000 IOPS입니다. 볼륨의 크기를 300GB로 변경하면 적응형 QoS는 처리량의 상한을 30,000 IOPS로 조정합니다.
- a_used space_policy(기본값)는 스토리지 효율성 이전에 저장된 실제 데이터의 양에 따라 IOPS/TB|GB 비율을 유지합니다. 비율이 100 IOPS/GB인 경우 100GB 데이터가 저장된 150GB 볼륨의 처리량은 최대 10,000 IOPS입니다. 사용된 공간의 양이 변경되면 적응형 QoS는 비율에 따라 처리량 상한을 조정합니다.

ONTAP 9.5부터 IOPS 및 MBPS 모두에서 처리량 제한을 나타낼 수 있도록 응용 프로그램에 대한 I/O 블록 크기를 지정할 수 있습니다. MBPS 제한은 블록 크기에 IOPS 제한을 곱하여 계산됩니다. 예를 들어, 6144IOPS/TB의 IOPS 한계 32K의 I/O 블록 크기는 192MBps의 MBPS 제한을 생성합니다.

처리량 천장과 바닥에 대해 다음과 같은 동작을 예상할 수 있습니다.

- 워크로드가 적응형 QoS 정책 그룹에 할당되면 상한 또는 하한 이 즉시 업데이트됩니다.
- 적응형 QoS 정책 그룹의 워크로드 크기를 조정하면 최대 또는 최저값이 약 5분 내에 업데이트됩니다.

업데이트를 적용하기 전에 처리량이 최소 10 IOPS 이상 증가해야 합니다.

적응형 QoS 정책 그룹은 항상 공유되지 않습니다. 정의된 처리량 상한 또는 최저값은 각 구성원 워크로드에 개별적으로 적용됩니다.

ONTAP 9.6부터 SSD가 장착된 ONTAP Select 프리미엄에서 처리량 플로어를 지원합니다.

적응형 정책 그룹 템플릿입니다

ONTAP 9.13.1 부터는 SVM에 적응형 QoS 템플릿을 설정할 수 있습니다. 적응형 정책 그룹 템플릿을 사용하면 SVM에서 모든 볼륨의 처리량 플로어 및 한도를 설정할 수 있습니다.

적응형 정책 그룹 템플릿은 SVM이 생성된 후에만 설정할 수 있습니다. 를 사용합니다 `vserver modify` 명령과 함께 `-qos-adaptive-policy-group-template` 매개 변수를 사용하여 정책을 설정합니다.

적응형 정책 그룹 템플릿을 설정하면 정책을 설정한 후 생성되거나 마이그레이션된 볼륨이 정책을 자동으로 상속합니다. 정책 템플릿을 할당할 때 SVM에 존재하는 볼륨은 영향을 받지 않습니다. SVM에서 정책을 사용하지 않도록 설정하면 이후에 SVM으로 마이그레이션되거나 SVM에서 생성된 모든 볼륨에서 정책을 받지 않습니다. 적응형 정책 그룹 템플릿을 사용하지 않도록 설정해도 정책 템플릿을 상속한 볼륨에는 영향을 주지 않습니다.

자세한 내용은 을 참조하십시오 적응형 정책 그룹 템플릿을 설정합니다.

일반 지원

다음 표에는 처리량 천장, 처리량 바닥 및 적응형 QoS 지원 차이의 차이가 나와 있습니다.

리소스 또는 기능	처리량 한도	처리량 플로어	처리량 플로어 **v2**	적응형 **QoS**
ONTAP 9 버전	모두	9.2 이상	9.7 이상	9.3 이상
플랫폼	모두	• AFF • C190 * • SSD * 가 포함된 ONTAP Select 프리미엄	• AFF • C190 • SSD가 포함된 ONTAP Select 프리미엄	모두
프로토콜	모두	모두	모두	모두
FabricPool	예	예. 계층화 정책이 "없음"으로 설정되고 클라우드에 블록이 없는 경우	예. 계층화 정책이 "없음"으로 설정되고 클라우드에 블록이 없는 경우	아니요
SnapMirror Synchronous	예	아니요	아니요	예

C190 및 ONTAP Select 지원은 ONTAP 9.6 릴리스부터 시작되었습니다.

처리량 상한에 대해 지원되는 워크로드

다음 표에서는 ONTAP 9 버전별 처리량 천장에 대한 워크로드 지원을 보여 줍니다. 루트 볼륨, 로드 공유 미러 및 데이터 보호 미러는 지원되지 않습니다.

워크로드 지원 - 최고	**ONTAP 9.0**	**ONTAP 9.1**	**ONTAP 9.2**	**ONTAP 9.3**	**ONTAP 9.4-9.7**	**ONTAP 9.8** 이상
볼륨	예	예	예	예	예	예
파일	예	예	예	예	예	예
LUN을 클릭합니다	예	예	예	예	예	예
SVM	예	예	예	예	예	예
FlexGroup 볼륨	아니요	아니요	아니요	예	예	예
Qtree *	아니요	아니요	아니요	아니요	아니요	예
정책 그룹당 워크로드가 여러 개일 수 있습니다	예	예	예	예	예	예
비공유 정책 그룹입니다	아니요	아니요	아니요	아니요	예	예

ONTAP 9.8부터 NFS 액세스가 지원되는 FlexVol 및 FlexGroup 볼륨의 qtree에서 NFS 액세스가 지원됩니다. ONTAP 9.9.1부터 SMB가 활성화된 FlexVol 및 FlexGroup 볼륨의 qtree에서도 SMB 액세스가 지원됩니다.

처리량 플로어에 대해 지원되는 워크로드

다음 표에는 ONTAP 9 버전별 처리량 플로어에 대한 워크로드 지원이 나와 있습니다. 루트 볼륨, 로드 공유 미러 및 데이터 보호 미러는 지원되지 않습니다.

워크로드 지원 - 현장	**ONTAP 9.2**	**ONTAP 9.3**	**ONTAP 9.4-9.7**	**ONTAP 9.8-9.13.0**	**ONTAP 9.13.1** 이상
볼륨	예	예	예	예	예
파일	아니요	예	예	예	예
LUN을 클릭합니다	예	예	예	예	예
SVM	아니요	아니요	아니요	아니요	예

워크로드 지원 - 현장	ONTAP 9.2	ONTAP 9.3	ONTAP 9.4-9.7	ONTAP 9.8-9.13.0	ONTAP 9.13.1 이상
FlexGroup 볼륨	아니요	아니요	예	예	예
Qtree *	아니요	아니요	아니요	예	예
정책 그룹당 워크로드가 여러 개일 수 있습니다	아니요	아니요	예	예	예
비공유 정책 그룹입니다	아니요	아니요	예	예	예

\ * ONTAP 9.8부터 NFS 액세스가 지원되는 FlexVol 및 FlexGroup 볼륨의 qtree에서 NFS 액세스가 지원됩니다. ONTAP 9.9.1부터 SMB가 활성화된 FlexVol 및 FlexGroup 볼륨의 qtree에서도 SMB 액세스가 지원됩니다.

적응형 **QoS**에 지원되는 워크로드

다음 표는 ONTAP 9 버전별 적응형 QoS에 대한 워크로드 지원을 보여줍니다. 루트 볼륨, 로드 공유 미러 및 데이터 보호 미러는 지원되지 않습니다.

워크로드 지원 - 적응형 QoS	ONTAP 9.3	ONTAP 9.4-9.13.0	ONTAP 9.13.1 이상
볼륨	예	예	예
파일	아니요	예	예
LUN을 클릭합니다	아니요	예	예
SVM	아니요	아니요	예
FlexGroup 볼륨	아니요	예	예
정책 그룹당 워크로드가 여러 개일 수 있습니다	예	예	예
비공유 정책 그룹입니다	예	예	예

최대 워크로드 및 정책 그룹 수

다음 표에는 ONTAP 9 버전별 최대 워크로드 및 정책 그룹 수가 나와 있습니다.

워크로드 지원	ONTAP 9.3 및 이전 버전	ONTAP 9.4 이상
클러스터당 최대 워크로드	12,000	40,000개
노드당 최대 워크로드	12,000	40,000개
최대 정책 그룹 수	12,000	12,000

처리량 플로어 **v2**를 활성화 또는 비활성화합니다

AFF에서 Throughput Floor v2를 활성화 또는 비활성화할 수 있습니다. 기본값은 ENABLED입니다. v2를 지원하는 경우, 컨트롤러가 다른 워크로드에 지연 시간이 길어지는 대신

사용량이 많은 경우 처리량 플로어를 충족할 수 있습니다. 버전 v2는 QoS 및 Adaptive QoS 모두에 적용됩니다.

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

2. 다음 명령 중 하나를 입력합니다.

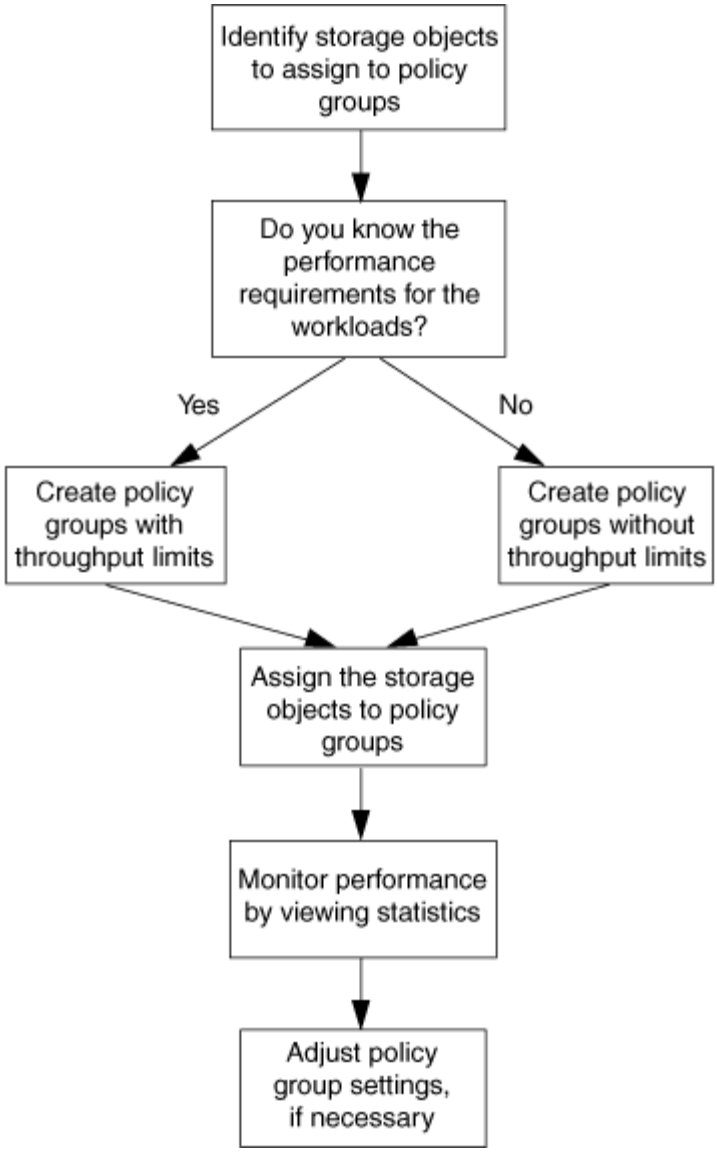
원하는 작업	다음 명령을 사용합니다.
Floor v2를 비활성화합니다	QoS 설정 처리량-층-v2-활성화 거짓
Floor v2를 활성화합니다	QoS 설정 처리량-층-v2-활성화 true

> MetroCluster 클러스터에서 처리량 층 v2를 비활성화하려면 를 실행해야 합니다
>
> QoS 설정 처리량-층-v2-활성화 거짓
>
> 소스 클러스터와 대상 클러스터 모두에서 명령을 내립니다.

```
cluster1::*> qos settings throughput-floors-v2 -enable false
```

스토리지 **QoS** 워크플로우

QoS를 사용하여 관리할 워크로드의 성능 요구사항을 이미 알고 있는 경우 정책 그룹을 생성할 때 처리량 한도를 지정할 수 있습니다. 그렇지 않으면 워크로드를 모니터링하여 한도를 지정할 때까지 기다릴 수 있습니다.



QoS를 사용하여 처리량 한도를 설정합니다

정책 그룹에 대해 '최대 처리량' 필드를 사용하여 스토리지 오브젝트 워크로드의 처리량 한도(QoS Max)를 정의할 수 있습니다. 스토리지 객체를 생성하거나 수정할 때 정책 그룹을 적용할 수 있습니다.

필요한 것

- 정책 그룹을 생성하려면 클러스터 관리자여야 합니다.
- SVM에 정책 그룹을 적용하려면 클러스터 관리자여야 합니다.

이 작업에 대해

- ONTAP 9.4부터 _non-shared_QoS 정책 그룹을 사용하여 정의된 처리량 상한이 각 구성원 워크로드에 개별적으로 적용되도록 지정할 수 있습니다. 그렇지 않으면 정책 그룹이 _ 공유: _ 입니다. 정책 그룹에 할당된 워크로드의 총 처리량은 지정된 한도를 초과할 수 없습니다.

  QoS policy-group create 명령에 대해 set '-is-shared=false'를 설정하여 비공유 정책 그룹을 지정합니다.

- 천장에 대한 처리량 제한을 IOPS, MB/s 또는 IOPS, MB/s로 지정할 수 있습니다 IOPS와 MB/s를 모두 지정하는 경우, 어느 한쪽의 제한에 먼저 도달하더라도 적용됩니다.

> 동일한 워크로드에 대해 천장과 바닥을 설정하는 경우 IOPS만 사용하여 천장에 대한 처리량 제한을 지정할 수 있습니다.

- QoS 제한이 적용되는 스토리지 개체는 정책 그룹이 속한 SVM에 포함되어 있어야 합니다. 여러 정책 그룹이 동일한 SVM에 속할 수 있습니다.
- 포함하는 객체 또는 해당 하위 객체가 정책 그룹에 속해 있는 경우 스토리지 객체를 정책 그룹에 할당할 수 없습니다.
- 정책 그룹을 동일한 유형의 스토리지 객체에 적용하는 것은 QoS 모범 사례입니다.

단계

1. 정책 그룹 생성:

   "QoS policy-group create-policy-group_policy_group_-vserver_SVM_-max-throughput_number_of_IOPS_|MB/S|IOPS, MB/S-is-shared true|false

   전체 명령 구문은 man 페이지를 참조하십시오. 'QoS policy-group modify' 명령을 사용하여 처리량 한도를 조정할 수 있습니다.

   다음 명령을 실행하면 최대 5,000 IOPS의 처리량을 갖는 공유 정책 그룹 'pg-vs1'이 생성됩니다.

   ```
   cluster1::> qos policy-group create -policy-group pg-vs1 -vserver vs1
   -max-throughput 5000iops -is-shared true
   ```

   다음 명령을 실행하면 비공유 정책 그룹 'pg-vs3'이 생성되고 최대 처리량은 100IOPS, 400KB/S입니다.

   ```
   cluster1::> qos policy-group create -policy-group pg-vs3 -vserver vs3
   -max-throughput 100iops,400KB/s -is-shared false
   ```

   다음 명령을 실행하면 처리량 제한 없이 비공유 정책 그룹 'pg-vs4'가 생성됩니다.

   ```
   cluster1::> qos policy-group create -policy-group pg-vs4 -vserver vs4
   -is-shared false
   ```

2. SVM, 파일, 볼륨 또는 LUN에 정책 그룹 적용:

   '*storage_object_create-vserver_SVM*-QoS-policy-group_policy_group_'

   전체 명령 구문은 man 페이지를 참조하십시오. '_storage_object_modify' 명령을 사용하여 스토리지 객체에 다른 정책 그룹을 적용할 수 있습니다.

   다음 명령은 SVM 'VS1'에 정책 그룹 'pg-vs1'을 적용합니다.

```
cluster1::> vserver create -vserver vs1 -qos-policy-group pg-vs1
```

다음 명령은 정책 그룹 pg-app을 볼륨 app1과 app2에 적용합니다.

```
cluster1::> volume create -vserver vs2 -volume app1 -aggregate aggr1
-qos-policy-group pg-app
```

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
-qos-policy-group pg-app
```

3. 정책 그룹 성능 모니터링:

   QoS 통계 성능 표시

   전체 명령 구문은 man 페이지를 참조하십시오.

   > 클러스터의 성능 모니터링 호스트의 툴을 사용하여 성능을 모니터링하지 마십시오.

   다음 명령을 실행하면 정책 그룹 성능이 표시됩니다.

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput   Latency
-------------------- -------- --------------- ----------
-total-                 12316       47.76MB/s  1264.00us
pg_vs1                   5008       19.56MB/s     2.45ms
_System-Best-Effort        62       13.36KB/s     4.13ms
_System-Background         30           0KB/s        0ms
```

4. 워크로드 성능 모니터링:

   QoS 통계 워크로드 성능 표시

   전체 명령 구문은 man 페이지를 참조하십시오.

   > 클러스터의 성능 모니터링 호스트의 툴을 사용하여 성능을 모니터링하지 마십시오.

   다음 명령을 실행하면 워크로드 성능이 표시됩니다.

```
cluster1::> qos statistics workload performance show
Workload          ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-              -    12320        47.84MB/s  1215.00us
app1-wid7967      7967     7219        28.20MB/s   319.00us
vs1-wid12279     12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS     14       55        10.92KB/s   236.00us
_Scan_Backgro..   5688       20            0KB/s        0ms
```

'QoS statistics workload latency show' 명령을 사용하여 QoS 워크로드에 대한 상세한 지연 시간 통계를 볼 수 있습니다.

QoS를 사용하여 처리량 기반 설정

정책 그룹의 '처리량' 필드를 사용하여 스토리지 오브젝트 워크로드의 처리량(QoS Min)을 정의할 수 있습니다. 스토리지 객체를 생성하거나 수정할 때 정책 그룹을 적용할 수 있습니다. ONTAP 9.8부터는 처리량(IOPS 또는 MBps, IOPS 및 MBps)을 지정할 수 있습니다.

시작하기 전에

- ONTAP 9.2 이상을 실행해야 합니다. ONTAP 9.2부터 처리량 플로어를 사용할 수 있습니다.
- 정책 그룹을 생성하려면 클러스터 관리자여야 합니다.
- ONTAP 9.13.1 부터는 를 사용하여 SVM 레벨에서 처리량 플로어를 적용할 수 있습니다 적응형 정책 그룹 템플릿입니다. QoS 정책 그룹을 갖는 SVM에서는 적응형 정책 그룹 템플릿을 설정할 수 없습니다.

이 작업에 대해

- ONTAP 9.4부터 _non-shared_QoS 정책 그룹을 사용하여 각 구성원 작업 부하에 대해 정의된 처리 층을 개별적으로 적용할 수 있습니다. 이는 처리량 플로어의 정책 그룹을 여러 워크로드에 적용할 수 있는 유일한 조건입니다.

  비공유 정책 그룹을 지정하기 위해 QoS policy-group create 명령에 대해 -is-shared=false를 설정합니다.

- 노드나 애그리게이트에 성능 용량(여유 공간)이 충분하지 않은 경우 워크로드에 대한 처리량이 지정된 플로어에 아래로 떨어질 수 있습니다.
- QoS 제한이 적용되는 스토리지 개체는 정책 그룹이 속한 SVM에 포함되어 있어야 합니다. 여러 정책 그룹이 동일한 SVM에 속할 수 있습니다.
- 정책 그룹을 동일한 유형의 스토리지 객체에 적용하는 것은 QoS 모범 사례입니다.
- 처리량 플로어를 정의하는 정책 그룹은 SVM에 적용할 수 없습니다.

단계

1. 에 설명된 대로 노드 또는 애그리게이트에서 적절한 성능 용량이 있는지 확인합니다 "남은 성능 용량 식별".
2. 정책 그룹 생성:

   'QoS policy-group create-policy group_policy_group_-vserver_SVM_-min-throughput_QoS_target_-is-shared true|false'

전체 명령 구문은 ONTAP 릴리즈의 man 페이지를 참조하십시오. 'QoS policy-group modify' 명령을 사용하여 처리량 층을 조정할 수 있습니다.

다음 명령을 실행하면 공유 정책 그룹 'pg-vs2'가 최소 1,000 IOPS의 처리량으로 생성됩니다.

```
cluster1::> qos policy-group create -policy group pg-vs2 -vserver vs2
-min-throughput 1000iops -is-shared true
```

다음 명령을 실행하면 처리량 제한 없이 비공유 정책 그룹 'pg-vs4'가 생성됩니다.

```
cluster1::> qos policy-group create -policy group pg-vs4 -vserver vs4
-is-shared false
```

3. 볼륨 또는 LUN에 정책 그룹 적용:

   '*storage_object_create-vserver_SVM*-QoS-policy-group_policy_group_'

   전체 명령 구문은 man 페이지를 참조하십시오. '_storage_object_modify' 명령을 사용하여 스토리지 객체에 다른 정책 그룹을 적용할 수 있습니다.

   다음 명령은 정책 그룹 pg-app2를 볼륨 app2에 적용합니다.

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
-qos-policy-group pg-app2
```

4. 정책 그룹 성능 모니터링:

   QoS 통계 성능 표시

   전체 명령 구문은 man 페이지를 참조하십시오.

   > 클러스터의 성능 모니터링 호스트의 툴을 사용하여 성능을 모니터링하지 마십시오.

   다음 명령을 실행하면 정책 그룹 성능이 표시됩니다.

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput   Latency
-------------------- -------- --------------- ----------
-total-                 12316       47.76MB/s  1264.00us
pg_app2                  7216       28.19MB/s   420.00us
_System-Best-Effort        62       13.36KB/s     4.13ms
_System-Background         30           0KB/s        0ms
```

5. 워크로드 성능 모니터링:

QoS 통계 워크로드 성능 표시

전체 명령 구문은 man 페이지를 참조하십시오.

> 클러스터의 성능 모니터링 호스트의 툴을 사용하여 성능을 모니터링하지 마십시오.

다음 명령을 실행하면 워크로드 성능이 표시됩니다.

```
cluster1::> qos statistics workload performance show
Workload           ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-              -    12320        47.84MB/s  1215.00us
app2-wid7967      7967     7219        28.20MB/s   319.00us
vs1-wid12279     12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS     14       55        10.92KB/s   236.00us
_Scan_Backgro..   5688       20            0KB/s        0ms
```

> 'QoS statistics workload latency show' 명령을 사용하여 QoS 워크로드에 대한 상세한 지연 시간 통계를 볼 수 있습니다.

적응형 **QoS** 정책 그룹을 사용합니다

adaptive QoS_policy 그룹을 사용하면 볼륨 크기가 변경될 때 IOPS와 TB|GB의 비율을 유지하면서 처리량 상한 또는 하한 크기를 자동으로 확장할 수 있습니다. 이는 대규모 구축 환경에서 수백 또는 수천 개의 워크로드를 관리할 때 큰 이점입니다.

시작하기 전에

- ONTAP 9.3 이상을 실행해야 합니다. 적응형 QoS 정책 그룹은 ONTAP 9.3부터 사용할 수 있습니다.
- 정책 그룹을 생성하려면 클러스터 관리자여야 합니다.

이 작업에 대해

스토리지 개체는 적응형 정책 그룹 또는 비적응 정책 그룹의 구성원일 수 있지만 둘 다 속할 수는 없습니다. 스토리지 오브젝트 및 정책의 SVM은 동일해야 합니다. 스토리지 객체가 온라인 상태여야 합니다.

적응형 QoS 정책 그룹은 항상 공유되지 않습니다. 정의된 처리량 상한 또는 최저값은 각 구성원 워크로드에 개별적으로 적용됩니다.

스토리지 오브젝트 크기에 대한 처리량 제한의 비율은 다음 필드의 상호 작용에 의해 결정됩니다.

- 'expected-IOPS'는 할당된 TB|GB당 예상되는 최소 IOPS입니다.

`expected-iops` 는 AFF 플랫폼에서만 보장됩니다. `expected-iops` 계층화 정책이 "없음"으로 설정되어 있고 클라우드에 블록이 없는 경우에만 FabricPool에 대해 보장됩니다. `expected-iops` SnapMirror 동기식 관계에 없는 볼륨에 대해 보장합니다.

- 'peak-IOPS'는 할당 또는 사용된 TB|GB당 가능한 최대 IOPS입니다.
- 'expected-IOPS-allocation'은 할당된 공간(기본값)이나 사용된 공간을 예상 IOPS에 사용할지 여부를 지정합니다.

ONTAP 9.5 이상에서 '예상 IOPS 할당'을 사용할 수 있습니다. ONTAP 9.4 이하 버전에서는 지원되지 않습니다.

- peak-IOPS-allocation은 peak-IOPS를 위해 할당된 공간과 사용된 공간(기본값)을 사용할지 여부를 지정한다.
- 절대 최소 IOPS는 절대 최소 IOPS의 수입니다. 이 필드는 매우 작은 스토리지 객체와 함께 사용할 수 있습니다. 절대분 IOPS가 계산된 예상 IOPS보다 크면 peak-IOPS와 expected-IOPS를 모두 재정의합니다.

  예를 들어, 'expected-IOPS'를 1,000 IOPS/TB로 설정하고 볼륨 크기가 1GB 미만인 경우 계산된 'expected-IOPS'는 IOP가 분수 값이 됩니다. 계산된 피크 IOPS는 이보다 훨씬 적은 비율입니다. 절대-최소-IOPS를 실제 값으로 설정하면 이러한 문제를 방지할 수 있습니다.

- 블록 크기 는 애플리케이션 입출력 블록 크기를 지정합니다. 기본값은 32K입니다. 유효한 값은 8K, 16K, 32K, 64K, any입니다. Any는 블록 크기가 적용되지 않음을 의미합니다.

다음 표에 나와 있는 것처럼 세 가지 기본 적응형 QoS 정책 그룹을 사용할 수 있습니다. 이러한 정책 그룹을 볼륨에 직접 적용할 수 있습니다.

기본 정책 그룹입니다	예상 IOPS/TB	최대 IOPS/TB	절대 최소 IOPS
"익스트림"	6,144	12,288	1000입니다
'퍼포먼스'	2,048	4,096개	500입니다
값	128	512	75를

포함하는 객체 또는 해당 하위 객체가 정책 그룹에 속하는 경우 스토리지 객체를 정책 그룹에 할당할 수 없습니다. 다음 표에는 제한 사항이 나와 있습니다.

다음을 할당하는 경우...	지정할 수 없는 경우...
SVM을 정책 그룹으로 이동합니다	SVM에 포함된 스토리지 오브젝트를 정책 그룹으로 이동
볼륨을 정책 그룹에	SVM이나 하위 LUN을 포함하는 볼륨을 정책 그룹에 포함하는 볼륨
정책 그룹에 LUN을 지정합니다	볼륨 또는 SVM을 포함하는 LUN을 정책 그룹으로 묶습니다

다음을 할당하는 경우...	지정할 수 없는 경우...
파일을 정책 그룹에 저장합니다	파일에서 볼륨 또는 SVM을 포함하는 정책 그룹으로 묶습니다

단계

1. 적응형 QoS 정책 그룹을 생성합니다.

   'QOS adaptive-policy-group create-policy group_group_-vserver_SVM_-expected-IOPS_number_of_IOPS_/TB|GB-peak-IOPS_number_of_IOPS_/TB|GB-expected-IOPS-allocation-space|used-space-peak-peak-IOPS-allocation-space|used-space-space-absolute-min-64K_K_number_K_number_K_number_K_K_number|K_K_K_number|K_MB|K_

   전체 명령 구문은 man 페이지를 참조하십시오.

   > ONTAP 9.5 이상에서 '-expected-IOPS-allocation' 및 '-block-size를 사용할 수 있다. 이러한 옵션은 ONTAP 9.4 이전 버전에서는 지원되지 않습니다.

   다음 명령을 실행하면 300 IOPS/TB로 설정된 adpg-app1 Adaptive QoS 정책 그룹, 1,000 IOPS/TB로 설정된 -peak-IOPS, 사용된 공간으로 설정된 -peak-IOPS-allocation, 50 IOPS로 설정된 -absolute-min-IOPS 정책 그룹,

   ```
   cluster1::> qos adaptive-policy-group create -policy group adpg-app1
   -vserver vs2 -expected-iops 300iops/tb -peak-iops 1000iops/TB -peak-iops
   -allocation used-space -absolute-min-iops 50iops
   ```

2. 적응형 QoS 정책 그룹을 볼륨에 적용합니다.

   'volume create-vserver SVM-volume_volume_-aggregate_aggregate_-size_number_of_TB|GB-QoS-adaptive-policy-group_policy_group_'

   전체 명령 구문은 man 페이지를 참조하십시오.

   다음 명령은 Adaptive QoS 정책 그룹 'adpg-app1'을 볼륨 'app1'에 적용합니다.

   ```
   cluster1::> volume create -vserver vs1 -volume app1 -aggregate aggr1
   -size 2TB -qos-adaptive-policy-group adpg-app1
   ```

   다음 명령은 새 볼륨 app4와 기존 볼륨 app5에 기본 적응형 QoS 정책 그룹 "extreme"을 적용합니다. 정책 그룹에 대해 정의된 처리량 상한은 볼륨 app4 및 app5에 개별적으로 적용됩니다.

   ```
   cluster1::> volume create -vserver vs4 -volume app4 -aggregate aggr4
   -size 2TB -qos-adaptive-policy-group extreme
   ```

```
cluster1::> volume modify -vserver vs5 -volume app5 -qos-adaptive-policy
-group extreme
```

적응형 정책 그룹 템플릿을 설정합니다

ONTAP 9.13.1 부터는 적응형 정책 그룹 템플릿을 사용하여 SVM 레벨에서 처리량 플로와 천장을 적용할 수 있습니다.

이 작업에 대해

- 적응형 정책 그룹 템플릿은 기본 정책입니다 `apg1`. 정책은 언제든지 수정할 수 있습니다. CLI 또는 ONTAP REST API에서만 설정할 수 있고 기존 SVM에만 적용할 수 있습니다.
- 적응형 정책 그룹 템플릿은 정책을 설정한 후 SVM에서 생성되거나 SVM으로 마이그레이션된 볼륨에만 영향을 줍니다. SVM의 기존 볼륨은 기존 상태를 유지합니다.

  적응형 정책 그룹 템플릿을 비활성화하면 SVM의 볼륨은 기존 정책을 그대로 유지합니다. 이후에 SVM에서 생성하거나 SVM으로 마이그레이션한 볼륨만 지원 해제에 의해 영향을 받습니다.
- QoS 정책 그룹을 갖는 SVM에서는 적응형 정책 그룹 템플릿을 설정할 수 없습니다.
- 적응형 정책 그룹 템플릿은 AFF 플랫폼용으로 설계되었습니다. 적응형 정책 그룹 템플릿은 다른 플랫폼에 설정할 수 있지만 정책이 최소 처리량을 적용하지 않을 수 있습니다. 마찬가지로, FabricPool 최소 처리량을 지원하지 않는 애그리게이트의 SVM에 적응형 정책 그룹 템플릿 을 추가할 수도 있지만, 처리량 수준이 적용되지 않습니다.
- SVM이 MetroCluster 구성 또는 SnapMirror 관계에 있는 경우 적응형 정책 그룹 템플릿이 미러링된 SVM에 적용됩니다.

단계

1. SVM을 수정하여 적응형 정책 그룹 템플릿을 적용합니다.
   `vserver modify -qos-adaptive-policy-group-template apg1`
2. 정책이 설정되었는지 확인합니다.
   `vserver show -fields qos-adaptive-policy-group`

Unified Manager로 클러스터 성능 모니터링

Active IQ Unified Manager를 사용하면 가용성을 최대화하고 NetApp AFF 및 FAS 스토리지 인프라에 대한 제어를 유지하여 확장성, 지원 가능성, 성능 및 보안을 향상할 수 있습니다.

Active IQ Unified Manager은 시스템 상태를 지속적으로 모니터링하고 알림을 전송하므로 조직에서 IT 직원 리소스를 여유 있게 사용할 수 있습니다. 단일 대시보드에서 스토리지 상태를 즉시 확인하고 권장 조치를 통해 문제를 빠르게 해결할 수 있습니다.

알림을 검색, 모니터링 및 수신하여 스토리지를 능동적으로 관리하고 신속하게 문제를 해결할 수 있으므로 데이터 관리가 간소화됩니다. 단일 대시보드에서 페타바이트급 데이터를 모니터링하고 규모에 맞게 데이터를 관리할 수 있으므로 관리 효율성이 향상됩니다.

Active IQ Unified Manager를 사용하면 변화하는 비즈니스 요구사항에 대응할 수 있으므로 성능 데이터 및 고급 분석을 사용하여 성능을 최적화할 수 있습니다. 보고 기능을 사용하면 표준 보고서에 액세스하거나 맞춤형 운영 보고서를 작성하여 비즈니스의 특정 요구를 충족할 수 있습니다.

관련 링크:

- "Active IQ Unified Manager에 대해 자세히 알아보십시오"
- "VMware용 Active IQ Unified Manager를 시작하십시오"
- "Linus용 Active IQ Unified Manager를 시작하십시오"
- "Active IQ Unified Manager for Windows를 시작합니다"

Cloud Insights로 클러스터 성능 모니터링

NetApp Cloud Insights는 전체 인프라에 대한 가시성을 제공하는 모니터링 툴입니다. Cloud Insights을 사용하면 퍼블릭 클라우드 및 프라이빗 데이터 센터를 비롯한 모든 리소스에 대한 모니터링, 문제 해결 및 최적화 등이 가능합니다.

Cloud Insights는 두 가지 버전으로 제공됩니다

Cloud Insights Basic Edition은 NetApp Data Fabric 자산을 모니터링하고 최적화하기 위해 특별히 설계되었습니다. HCI와 FAS(All Flash AFF)를 포함한 모든 NetApp 리소스 간의 연결을 무료로 제공하는 고급 분석 기능을 제공합니다.

Cloud Insights Standard Edition은 NetApp Data Fabric 지원 인프라 구성요소뿐만 아니라 멀티 벤더 및 멀티 클라우드 환경에 초점을 맞춥니다. 풍부한 기능을 통해 100개 이상의 서비스 및 리소스에 대한 지원을 이용할 수 있습니다.

온프레미스 데이터 센터에서 여러 퍼블릭 클라우드에 이르기까지 다양한 리소스를 활용하는 오늘날의 환경에서는 애플리케이션 자체에서 스토리지 어레이의 백엔드 디스크에 이르기까지 전체적인 상황을 파악하는 것이 중요합니다. 애플리케이션 모니터링을 위한 추가 지원(Kafka, MongoDB 및 Nginx 등)은 최적의 활용률 수준뿐 아니라 완벽한 위험 버퍼에서도 운영하는 데 필요한 정보와 지식을 제공합니다.

두 에디션(기본 및 표준) 모두 NetApp Active IQ Unified Manager와 통합할 수 있습니다. Active IQ Unified Manager를 사용하는 고객은 Cloud Insights 사용자 인터페이스 내에서 조인 정보를 볼 수 있습니다. Active IQ Unified Manager에 게시된 알림은 간과되지 않으며 Cloud Insights의 이벤트와 관련될 수 있습니다. 즉, 두 마리 토끼를 동시에 잡을 수 있습니다.

모든 리소스를 모니터링, 문제 해결 및 최적화합니다

Cloud Insights를 사용하면 문제 해결 시간을 크게 단축하고 최종 사용자에게 영향을 주지 않도록 방지할 수 있습니다. 또한 클라우드 인프라 비용을 줄일 수 있습니다. 실행 가능한 인텔리전스로 데이터를 보호하여 내부자 위협에 대한 노출을 줄입니다.

Cloud Insights를 사용하면 퍼블릭 클라우드에서 데이터 센터에 이르기까지 전체 하이브리드 인프라를 한 곳에서 확인할 수 있습니다. 필요에 따라 맞춤 구성할 수 있는 관련 대시보드를 즉시 만들 수 있습니다. 조직의 요구 사항에 따라 구체적이고 관련 있는 조건부 경고를 만들 수도 있습니다.

고급 이상 징후 탐지 기능을 통해 문제가 발생하기 전에 사전에 해결할 수 있습니다. 리소스 경합 및 성능 저하를 자동으로 확인하여 영향을 받는 워크로드를 신속하게 복원할 수 있습니다. 스택 내 여러 구성 요소 간의 관계를 자동으로 계층 구조로 만들어 문제 해결 작업을 더욱 빠르게 수행할 수 있습니다.

환경 전반에서 사용되지 않거나 버려진 리소스를 식별할 수 있으므로, 인프라의 크기를 적절하게 조정하고 전체 비용을 최적화할 기회를 찾을 수 있습니다.

Cloud Insights는 시스템 토폴로지를 시각화하여 Kubernetes 아키텍처를 파악합니다. 문제가 있는 노드를 비롯하여 Kubernetes 클러스터의 상태를 모니터링하고 문제가 발생하면 확장할 수 있습니다.

Cloud Insights는 고급 머신 러닝 및 이상 징후 탐지를 통해 악의적인 사용자 또는 침해를 입은 사용자가 조직 데이터를 악용하지 못하도록 보호하여 내부자 위협에 대해 실행 가능한 인텔리전스를 제공합니다.

Cloud Insights를 사용하면 Kubernetes 메트릭을 시각화하여 Pod, 노드, 클러스터 간의 관계를 완벽하게 파악할 수 있습니다. 현재 처리 중인 로드뿐만 아니라 클러스터 또는 작업 포드의 상태를 평가할 수 있으므로 K8S 클러스터의 명령을 수행하고 배포 상태와 비용을 모두 제어할 수 있습니다.

관련 링크

- "Cloud Insights에 대해 자세히 알아보십시오"
- "Cloud Insights과 함께 시작하십시오"

로깅 감사

ONTAP에서 감사 로깅을 구현하는 방법

감사 로그에 기록된 관리 작업은 표준 AutoSupport 보고서에 포함되며, 특정 로깅 작업은 EMS 메시지에 포함됩니다. 또한 지정한 대상에 감사 로그를 전달할 수 있으며 CLI 또는 웹 브라우저를 사용하여 감사 로그 파일을 표시할 수 있습니다.

ONTAP 9.11.1부터 시스템 관리자를 사용하여 감사 로그 내용을 표시할 수 있습니다.

ONTAP 9.12.1부터 ONTAP는 감사 로그에 대한 변조 경고를 제공합니다. ONTAP는 매일 백그라운드 작업을 실행하여 audit.log 파일의 변조를 확인하고 변경 또는 변조된 로그 파일이 발견되면 EMS 경고를 보냅니다.

ONTAP는 클러스터에서 수행된 관리 작업(예: 실행된 요청, 요청을 트리거한 사용자, 사용자의 액세스 방법 및 요청 시간)을 기록합니다.

관리 활동은 다음 유형 중 하나일 수 있습니다.

- 일반적으로 표시되지 않는 명령 또는 작업에 적용되는 요청 설정:
  - 예를 들어, 'create', 'modify', 'delete' 명령을 실행하면 이러한 요청이 실행됩니다.
  - 설정된 요청은 기본적으로 기록됩니다.
- GET requests, 정보를 검색하여 관리 인터페이스에 표시합니다.
  - 예를 들어 'show' 명령을 실행하면 이러한 요청이 실행됩니다.
  - GET 요청은 기본적으로 로깅되지 않지만 GET 요청이 ONTAP CLI에서 전송되는지 여부를 제어할 수 있습니다 (`-cliget`ONTAP API에서)를 클릭합니다 (-ontapiget`)를 선택하거나 REST API에서 가져옵니다 (`-httpget`)이 파일에 로그인되어 있습니다.

ONTAP는 노드의 `/mroot/etc/log/mlog/audit.log' 파일에 관리 활동을 기록합니다. CLI 명령(클러스터 셸, 노드 쉘, 비대화형 시스템 셸(대화형 시스템 셸 명령은 기록되지 않음))을 위한 세 개의 셸과 API 명령이 여기에 기록됩니다. 감사 로그에는 클러스터의 모든 노드가 시간 동기화되었는지 여부를 나타내는 타임스탬프가 포함됩니다.

Audit.log 파일은 AutoSupport Tool에 의해 지정된 수신인에게 전송된다. 또한 Splunk 또는 syslog 서버와 같이 지정한 외부 대상에 콘텐츠를 안전하게 전달할 수 있습니다.

Audit.log 파일은 매일 순환한다. 회전은 크기가 100MB에 도달하고 이전 48개 사본이 보존될 때도 발생합니다(최대 총 49개 파일). 감사 파일이 매일 회전을 수행하면 EMS 메시지가 생성되지 않습니다. 파일 크기 제한이 초과되어 Audit 파일이 회전하면 EMS 메시지가 발생한다.

ONTAP 9의 감사 로깅을 변경합니다

ONTAP 9부터는 Command-history.log 파일이 audit.log로 대체되고, mgwd.log 파일은 더 이상 Audit 정보를 포함하지 않는다. ONTAP 9로 업그레이드하는 경우 기존 파일과 해당 콘텐츠를 참조하는 스크립트나 도구를 검토해야 합니다.

ONTAP 9로 업그레이드한 후 기존 명령어 이력.log 파일을 보존한다. 새 감사.로그 파일이 (작성됨) 회전되면 해당 파일이 삭제(삭제)됩니다.

명령어-히스토리.로그 파일을 체크하는 툴과 스크립트는 업그레이드 시 명령어-히스토리.로그부터 audit.log로의 소프트 링크가 생성되기 때문에 계속 동작할 수 있다. 그러나 mgwd.log 파일을 확인하는 도구와 스크립트는 해당 파일에 더 이상 감사 정보가 없기 때문에 실패합니다.

또한 ONTAP 9 이상의 감사 로그에는 유용하지 않고 불필요한 로깅 활동을 유발하기 때문에 다음 항목이 더 이상 포함되지 않습니다.

- ONTAP에서 실행되는 내부 명령(즉, username=root)
- 명령 별칭(해당 명령이 가리키는 명령과는 별개)

ONTAP 9부터는 TCP 및 TLS 프로토콜을 사용하여 감사 로그를 외부 대상으로 안전하게 전송할 수 있습니다.

감사 로그 내용을 표시합니다

ONTAP CLI, System Manager 또는 웹 브라우저를 사용하여 클러스터의 `/mroot/etc/log/mlog/audit.log' 파일의 내용을 표시할 수 있습니다.

클러스터의 로그 파일 항목은 다음과 같습니다.

시간
: 로그 항목 타임 스탬프입니다.

응용 프로그램
: 클러스터에 연결하는 데 사용되는 애플리케이션입니다. 가능한 값의 예로는 'internal, console, ssh, http, ontapi, SNMP, rsh, telnet, service-processor 등이 있다.

사용자
: 원격 사용자의 사용자 이름입니다.

상태
: 성공, 보류, 오류 등 감사 요청의 현재 상태입니다.

메시지
: 명령 상태에 대한 오류 또는 추가 정보를 포함할 수 있는 선택적 필드입니다.

세션 **ID**입니다

요청이 수신된 세션 ID입니다. 각 SSH_SESSION_에는 세션 ID가 할당되고 각 HTTP, ONTAPI 또는 SNMP_REQUEST_에는 고유한 세션 ID가 할당됩니다.

스토리지 **VM**

사용자가 연결하는 데 사용되는 SVM.

범위

데이터 스토리지 VM에 요청이 있으면 'VM'을 표시하고, 그렇지 않으면 '클러스터'를 표시합니다.

명령 **ID**입니다

CLI 세션에서 수신한 각 명령의 ID입니다. 이렇게 하면 요청과 응답을 서로 연관시킬 수 있습니다. ZAPI, HTTP 및 SNMP 요청에는 명령 ID가 없습니다.

웹 브라우저에서 ONTAP CLI의 클러스터의 로그 항목을 표시하고 시스템 관리자에서 ONTAP 9.11.1로 시작할 수 있습니다.

시스템 관리자

- 인벤토리를 표시하려면 * 이벤트 및 작업 > 감사 로그 * 를 선택합니다. + 각 열에는 필터링, 정렬, 검색, 표시 및 인벤토리 범주를 제어하는 컨트롤이 있습니다. 재고 세부 정보는 Excel 통합 문서로 다운로드할 수 있습니다.
- 필터를 설정하려면 오른쪽 위에 있는 * Filter * (필터 *) 버튼을 클릭하고 원하는 필드를 선택합니다. +세션 ID 링크를 클릭하여 장애가 발생한 세션에서 실행된 모든 명령을 볼 수도 있습니다.

CLI를 참조하십시오

클러스터의 여러 노드에서 병합된 감사 항목을 표시하려면 +'보안 감사 로그 show_[parameters]_'를 입력합니다

'security audit log show' 명령을 사용하면 개별 노드의 감사 항목을 표시하거나 클러스터의 여러 노드에서 병합한 감사 항목을 표시할 수 있습니다. 웹 브라우저를 사용하여 단일 노드에 '/mroot/etc/log/mlog' 디렉토리의 컨텐츠를 표시할 수도 있습니다. 자세한 내용은 man 페이지를 참조하십시오.

웹 브라우저

웹 브라우저를 사용하여 단일 노드에 '/mroot/etc/log/mlog' 디렉토리의 내용을 표시할 수 있습니다. "웹 브라우저를 사용하여 노드의 로그, 코어 덤프 및 MIB 파일에 액세스하는 방법에 대해 알아보십시오".

감사 가져오기 요청 설정을 관리합니다

설정된 요청이 기본적으로 기록되지만 GET 요청은 기록되지 않습니다. 그러나 ONTAP HTML('-HttpGet'), ONTAP CLI('-cliget') 또는 ONTAP API('-ontapiget')에서 보낸 GET 요청이 파일에 기록되는지 여부를 제어할 수 있습니다.

시스템 관리자에서 감사 로깅 설정을 ONTAP CLI에서 수정할 수 있으며 ONTAP 9.11.1부터 시작할 수 있습니다.

시스템 관리자

1. 이벤트 및 작업 > 감사 로그 * 를 선택합니다.
2. ⚙오른쪽 상단 모서리를 클릭한 다음 추가 또는 제거할 요청을 선택합니다.

CLI를 참조하십시오

- ONTAP CLI 또는 API의 GET 요청을 감사 로그(audit.log 파일)에 기록하도록 지정하려면 기본 설정 요청 외에 + '보안 감사 수정[-cliget{on|off}][-HttpGet{ on|off}][-ontapiget{on|off}]'을 입력합니다
- 현재 설정을 표시하려면 + 보안 감사 표시 를 입력합니다

자세한 내용은 man 페이지를 참조하십시오.

감사 로그 대상을 관리합니다

감사 로그를 최대 10개의 대상으로 전달할 수 있습니다. 예를 들어, 모니터링, 분석 또는 백업을 위해 로그를 Splunk 또는 syslog 서버로 전달할 수 있습니다.

이 작업에 대해

전달을 구성하려면 syslog 또는 Splunk 호스트의 IP 주소, 포트 번호, 전송 프로토콜 및 전달된 로그에 사용할 syslog 기능을 제공해야 합니다. "syslog 기능에 대해 자세히 알아보십시오".

다음 전송 값 중 하나를 선택할 수 있습니다.

UDP 암호화되지 않음

보안이 없는 사용자 데이터그램 프로토콜(기본값)

TCP 암호화되지 않음

보안 기능이 없는 전송 제어 프로토콜

TCP 암호화

전송 계층 보안(TLS)이 있는 전송 제어 프로토콜 + A * 서버 확인 * 옵션은 TCP 암호화 프로토콜이 선택된 경우에 사용할 수 있습니다.

ONTAP CLI에서 감사 로그를 전달하고 ONTAP 9.11.1부터 System Manager에서 전달할 수 있습니다.

시스템 관리자

- 감사 로그 대상을 표시하려면 * 클러스터 > 설정 * 을 선택합니다. +로그 대상 수가 * 알림 관리 타일 * 에 표시됩니다. ⋮세부 정보를 표시하려면 클릭하십시오.
- 감사 로그 대상을 추가, 수정 또는 삭제하려면 * 이벤트 및 작업 > 감사 로그 * 를 선택한 다음 화면 오른쪽 상단의 * 감사 대상 관리 * 를 클릭합니다. + 를 + Add 클릭하거나 ⋮ * 호스트 주소 * 열을 클릭하여 항목을 편집하거나 삭제합니다.

CLI를 참조하십시오

1. 감사 로그를 전달할 각 대상에 대해 대상 IP 주소 또는 호스트 이름 및 보안 옵션을 지정합니다.

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 514 -protocol tcp-encrypted -facility user
```

   - "cluster log-forwarding create" 명령이 대상 호스트를 ping하여 연결을 확인할 수 없으면 명령이 실패하고 오류가 표시됩니다. 권장하지는 않지만 명령과 함께 '-force' 매개 변수를 사용하면 연결 확인이 생략됩니다.
   - '-verify-server' 매개 변수를 'true'로 설정하면 로그 전달 대상 ID가 인증서의 유효성을 확인하여 확인됩니다. 프로토콜 필드에서 TCP 암호화 값을 선택한 경우에만 이 값을 'true'로 설정할 수 있습니다.

2. cluster log-forwarding show 명령을 사용하여 대상 레코드가 올바른지 확인합니다.

```
cluster1::> cluster log-forwarding show

                                                    Verify Syslog
Destination Host           Port   Protocol         Server Facility
-------------------------- ------ --------         ------ --------
192.168.123.96             514    udp-unencrypted false  user
192.168.123.98             514    tcp-encrypted   true   user
2 entries were displayed.
```

자세한 내용은 man 페이지를 참조하십시오.

AutoSupport

AutoSupport에 대해 자세히 알아보십시오

AutoSupport 정보

AutoSupport는 시스템의 상태를 능동적으로 모니터링하고 NetApp 기술 지원, 내부 지원 조직 및 지원 파트너에게 메시지를 자동으로 보내는 메커니즘입니다. AutoSupport 기술 지원 메시지를 기본적으로 사용하도록 설정했지만 올바른 옵션을 설정하고 내부 지원 조직에 메시지를 보낼 수 있는 유효한 메일 호스트를 가지고 있어야 합니다.

클러스터 관리자만 AutoSupport 관리를 수행할 수 있습니다. 스토리지 가상 시스템(SVM) 관리자는 AutoSupport에 액세스할 수 없습니다.

스토리지 시스템을 처음 구성할 때 AutoSupport가 기본적으로 설정됩니다. AutoSupport는 AutoSupport가 활성화된 후 24시간 후에 기술 지원 부서에 메시지를 보내기 시작합니다. 시스템을 업그레이드 또는 되돌리거나, AutoSupport 구성을 수정하거나, 시스템 시간을 24시간 이외의 시간으로 변경하여 24시간을 단축할 수 있습니다.

> 언제든지 AutoSupport를 비활성화할 수 있지만, 이 기능을 활성 상태로 두어야 합니다. AutoSupport를 활성화하면 스토리지 시스템에서 문제가 발생할 경우 문제를 신속하게 확인하고 해결할 수 있습니다. 기본적으로 시스템에서는 AutoSupport를 사용하지 않도록 설정하더라도 AutoSupport 정보를 수집하여 로컬에 저장합니다.

AutoSupport에 대한 자세한 내용은 NetApp Support 사이트 를 참조하십시오.

관련 정보

- "NetApp 지원"
- "ONTAP 명령 참조입니다"

Active IQ Digital Advisor 및 AutoSupport 정보

ONTAP의 AutoSupport 구성 요소는 원격 측정을 수집하여 분석을 위해 전송합니다. Active IQ 디지털 어드바이저는 AutoSupport의 데이터를 분석하고 능동적인 관리 및 최적화를 제공합니다. Active IQ은 인공 지능을 사용하여 잠재적인 문제를 파악하고 비즈니스에 영향을 미치기 전에 이를 해결하도록 지원합니다.

Active IQ을 사용하면 클라우드 기반 포털 및 모바일 앱을 통해 실행 가능한 예측 분석과 능동적 지원을 제공하여 글로벌 하이브리드 클라우드 전반에서 데이터 인프라를 최적화할 수 있습니다. SupportEdge의 데이터 중심 인사이트와 권장사항은 Active IQ 계약이 체결된 모든 NetApp 고객(기능은 제품 및 지원 계층에 따라 다름)에게 제공됩니다.

다음은 Active IQ에서 수행할 수 있는 몇 가지 사항입니다.

- 업그레이드 계획 Active IQ는 사용자 환경에서 최신 버전의 ONTAP로 업그레이드하여 해결할 수 있는 문제를 식별하며, 업그레이드 관리자 구성 요소는 성공적인 업그레이드를 계획하는 데 도움이 됩니다.
- 시스템 상태 보기 Active IQ 대시보드에서 웰빙과 관련된 모든 문제를 보고하고 문제를 해결할 수 있습니다. 시스템 용량을 모니터링하여 스토리지 공간이 부족하지 않도록 하십시오. 시스템에 대한 지원 케이스를 봅니다.
- 성능 관리 Active IQ는 System Manager에서 볼 수 있는 것보다 더 오랜 기간 동안의 시스템 성능을 보여 줍니다. 성능에 영향을 주는 구성 및 시스템 문제를 식별합니다.
- 효율성 극대화 스토리지 효율성 메트릭을 확인하고 더 적은 공간에 더 많은 데이터를 저장하는 방법을 알아보십시오.
- 인벤토리 및 구성을 봅니다. Active IQ는 전체 인벤토리 및 소프트웨어 및 하드웨어 구성 정보를 표시합니다. 서비스 계약이 만료되는 시기를 확인하고 서비스 계약을 갱신하여 계속 지원을 받을 수 있도록 합니다.

관련 정보

"NetApp 설명서: Active IQ 디지털 자문업체"

"Active IQ를 시작합니다"

"SupportEdge 서비스"

AutoSupport 메시지가 전송되는 시기 및 위치

AutoSupport는 메시지 유형에 따라 다른 수신자에게 메시지를 보냅니다. AutoSupport에서 메시지를 보내는 시기와 위치를 이해하면 전자 메일을 통해 받는 메시지를 이해하거나 Active IQ(이전의 My AutoSupport) 웹 사이트에서 볼 수 있습니다.

별도로 지정하지 않는 한 다음 표의 설정은 'system node AutoSupport modify' 명령의 매개 변수입니다.

이벤트가 트리거된 메시지입니다

시스템에서 수정 조치가 필요한 이벤트가 발생하면 AutoSupport는 자동으로 이벤트 트리거 메시지를 전송합니다.

메시지가 전송될 때	메시지가 전송되는 위치입니다
AutoSupport는 EMS에서 트리거 이벤트에 응답합니다	"to"와 "noteto"에 지정된 주소. (서비스에 영향을 주는 중요 이벤트만 전송됩니다.) '-PARTNER-ADDRESS'에 명시된 주소 기술 지원, 만약 '-support'가 'enable'로 설정되어 있으면

예약된 메시지입니다

AutoSupport는 정기적으로 여러 메시지를 자동으로 보냅니다.

메시지가 전송될 때	메시지가 전송되는 위치입니다
매일(기본적으로 오전 12:00 사이에 전송됨 오전 1시 로그 메시지로 사용)	'-PARTNER-ADDRESS'에 명시된 주소 기술 지원, 만약 '-support'가 'enable'로 설정되어 있으면
매일(기본적으로 오전 12:00 사이에 전송됨 오전 1시 성능 메시지로서 -perf 매개 변수가 true로 설정되어 있으면	'파트너 주소'에 지정된 주소 기술 지원, 만약 '-support'가 'enable'로 설정되어 있으면
매주(기본적으로 일요일 오전 12:00 사이에 전송됨 및 오전 1:00)	'-PARTNER-ADDRESS'에 명시된 주소 기술 지원, 만약 '-support'가 'enable'로 설정되어 있으면

수동으로 트리거된 메시지입니다

AutoSupport 메시지를 수동으로 시작하거나 다시 보낼 수 있습니다.

메시지가 전송될 때	메시지가 전송되는 위치입니다
'system node AutoSupport invoke' 명령어를 이용하여 수동으로 메시지를 시작한다	System node AutoSupport invoke 명령에 '-Uri' 파라미터를 사용하여 URI를 지정하면 해당 URI로 메시지가 전송됩니다. 만약 '-Uri'를 생략하면 '-to', '-partner-address'에 지정된 주소로 메시지가 전송됩니다. 이 메시지는 '-support'가 'enable'로 설정되어 있는 경우 기술 지원부에도 전송됩니다.
'system node AutoSupport invoke-core-upload' 명령어를 이용하여 수동으로 메시지를 시작한다	System node AutoSupport invoke-core-upload 명령에서 '-Uri' 매개 변수를 사용하여 URI를 지정하면 해당 URI로 메시지가 전송되고 core dump 파일이 URI로 업로드된다. system node AutoSupport invoke-core-upload 명령에서 -uri를 생략하면 기술 지원 부서에 메시지가 전송되고 코어 덤프 파일이 기술 지원 사이트에 업로드됩니다. 두 시나리오 모두 '-support'가 'enable'로 설정되어 있고 'transport'가 'https' 또는 'http'로 설정되어 있어야 합니다. 코어 덤프 파일의 크기가 크기 때문에 '-to' 및 '-partner-addresses' 매개 변수에 지정된 주소로 메시지가 전송되지 않습니다.
'system node AutoSupport invoke-performance-archive' 명령어를 사용하여 수동으로 메시지를 시작한다	System node AutoSupport invoke-performance-archive 명령에서 '-Uri' 매개 변수를 사용하여 URI를 지정하면 해당 URI로 메시지가 전송되고 성능 아카이브 파일이 URI로 업로드됩니다. System node AutoSupport invoke-performance-archive에서 -Uri를 생략하면 기술 지원 부서에 메시지가 전송되고 성능 아카이브 파일이 기술 지원 사이트에 업로드됩니다. 두 시나리오 모두 '-support'가 'enable'로 설정되어 있고 'transport'가 'https' 또는 'http'로 설정되어 있어야 합니다. 대용량 성능 아카이브 파일로 인해 '-to' 및 '-partner-addresses' 매개 변수에 지정된 주소로 메시지가 전송되지 않습니다.
'시스템 노드 AutoSupport history retransmit' 명령어를 이용하여 수동으로 과거 메시지를 재전송한다	System node AutoSupport history retransmit 명령의 '-Uri' 파라미터에 지정하는 URI에만 해당

기술 지원 부서에서 트리거하는 메시지

기술 지원 부서는 AutoSupport OnDemand 기능을 사용하여 AutoSupport로부터 메시지를 요청할 수 있습니다.

메시지가 전송될 때	메시지가 전송되는 위치입니다
AutoSupport가 새 AutoSupport 메시지를 생성하기 위한 전달 지침을 얻는 경우	'-PARTNER-ADDRESS'에 명시된 주소 기술 지원인 -support가 enable로 설정되어 있고 -transport가 https로 설정되어 있으면
AutoSupport가 지난 AutoSupport 메시지를 다시 보내기 위한 전달 지침을 얻는 경우	기술 지원인 -support가 enable로 설정되어 있고 -transport가 https로 설정되어 있으면
AutoSupport가 코어 덤프 또는 성능 아카이브 파일을 업로드하는 새 AutoSupport 메시지를 생성하기 위한 전달 지침을 얻는 경우	기술 지원인 -support가 enable로 설정되어 있고 -transport가 https로 설정되어 있으면. 코어 덤프 또는 성능 아카이브 파일이 기술 지원 사이트에 업로드됩니다.

AutoSupport에서 이벤트 트리거 메시지를 만들고 보내는 방법

AutoSupport는 EMS가 트리거 이벤트를 처리할 때 이벤트 트리거 AutoSupport 메시지를 생성합니다. 이벤트가 트리거된 AutoSupport 메시지는 수신자에게 수정 조치가 필요한 문제를 경고하고 문제와 관련된 정보만 포함합니다. 포함할 콘텐츠 및 메시지를 받는 사람을 사용자 지정할 수 있습니다.

AutoSupport는 다음 프로세스를 사용하여 이벤트 트리거 AutoSupport 메시지를 만들고 보냅니다.

1. EMS가 trigger event를 처리할 때, EMS는 AutoSupport에게 request를 보낸다.

   트리거 이벤트는 AutoSupport 대상 및 이름이 callhome으로 시작하는 EMS 이벤트입니다.

2. AutoSupport에서 이벤트 트리거 AutoSupport 메시지를 생성합니다.

   AutoSupport는 트리거와 연결된 하위 시스템으로부터 기본 및 문제 해결 정보를 수집하여 트리거 이벤트와 관련된 정보만 포함된 메시지를 생성합니다.

   기본 하위 시스템 세트는 각 트리거와 연결됩니다. 그러나 'system node AutoSupport trigger modify' 명령을 사용하여 추가 서브시스템을 트리거에 연결할 수 있습니다.

3. AutoSupport는 시스템 노드 AutoSupport modify 명령에 의해 정의된 수신자에게 -to, -noteto, -partner-address, -support 매개 변수를 사용하여 이벤트 트리거 AutoSupport 메시지를 보냅니다.

   '-to' 및 '-noteto' 매개 변수를 사용하여 'system node AutoSupport trigger modify' 명령을 사용하여 특정 트리거에 대한 AutoSupport 메시지 전달을 활성화 또는 비활성화할 수 있습니다.

특정 이벤트에 대해 전송된 데이터의 예

Storage shelf PSU failed EMS 이벤트는 Mandatory, Log Files, Storage, RAID, HA의 기본 데이터가 포함된 메시지를 플랫폼, 네트워킹 하위 시스템 및 필수, 로그 파일 및 스토리지 하위 시스템의 데이터 문제 해결

향후 '스토리지 셸프 PSU 실패' 이벤트에 대한 응답으로 전송된 AutoSupport 메시지에 NFS에 대한 데이터를 포함시키기로 결정합니다. callhome.shlf.ps.fault 이벤트에 대해 NFS에 대한 문제 해결 수준 데이터를 활성화하려면 다음 명령을 입력합니다.

```
        cluster1::\>
        system node autosupport trigger modify -node node1 -autosupport
-message shlf.ps.fault -troubleshooting-additional nfs
```

'system node AutoSupport trigger' 명령어를 사용하거나 CLI에서 AutoSupport 및 EMS 이벤트가 참조할 때 callhome.shlf.ps.fault 이벤트에서 callhome. 접두사가 삭제된다.

AutoSupport 메시지의 유형과 콘텐츠입니다

AutoSupport 메시지에는 지원되는 하위 시스템에 대한 상태 정보가 포함되어 있습니다. AutoSupport 메시지에 포함된 내용을 학습하면 전자 메일로 받거나 Active IQ(이전의 My AutoSupport) 웹 사이트에서 보는 메시지를 해석하거나 응답할 수 있습니다.

메시지 유형입니다	메시지에 포함된 데이터 유형입니다
이벤트가 트리거되었습니다	이벤트가 발생한 특정 하위 시스템에 대한 컨텍스트 기반 데이터를 포함하는 파일입니다
매일	로그 파일
성능	지난 24시간 동안 샘플링된 성능 데이터
매주	구성 및 상태 데이터
'system node AutoSupport invoke' 명령에 의해 발생한다	'-type' 파라미터에 지정된 값에 따라 다름: • "테스트"는 기본적인 데이터가 포함된 사용자 트리거 메시지를 보냅니다. 또한 이 메시지는 '-to' 옵션을 사용하여 기술 지원에서 특정 이메일 주소로 자동 이메일 응답을 트리거하여 AutoSupport 메시지가 수신되고 있는지 확인할 수 있도록 합니다. • '성능'은 성능 데이터를 전송합니다. • All은 서브시스템의 데이터 문제 해결 등 주간 메시지와 유사한 완전한 데이터 세트를 가진 사용자 트리거 메시지를 전송한다. 기술 지원 부서에서는 일반적으로 이 메시지를 요청합니다.
'system node AutoSupport invoke-core-upload' 명령에 의해 발생한다	노드의 코어 덤프 파일

메시지 유형입니다	메시지에 포함된 데이터 유형입니다
'system node AutoSupport invoke-performance-archive' 명령에 의해 트리거됩니다	지정된 기간 동안 성능 아카이브 파일
AutoSupport OnDemand에 의해 트리거됩니다	AutoSupport OnDemand는 새 메시지 또는 이전 메시지를 요청할 수 있습니다. • AutoSupport 수집 유형에 따라 테스트, 전체 또는 성능 중 새 메시지가 나타날 수 있습니다. • 지난 메시지는 다시 전송되는 메시지 유형에 따라 달라집니다. AutoSupport OnDemand에서는 다음 파일을 NetApp 지원 사이트 로 업로드하는 새 메시지를 요청할 수 있습니다 "mysupport.netapp.com". • 코어 덤프 • 성능 아카이브

AutoSupport 하위 시스템을 봅니다

각 하위 시스템은 AutoSupport가 해당 메시지에 사용하는 기본 및 문제 해결 정보를 제공합니다. 또한 각 하위 시스템은 트리거 이벤트와 관련된 하위 시스템에서만 AutoSupport가 수집하도록 허용하는 트리거 이벤트와도 연결됩니다.

AutoSupport는 상황에 맞는 콘텐츠를 수집합니다.

단계

1. 하위 시스템 및 트리거 이벤트에 대한 정보를 봅니다.

```
system node autosupport trigger show
```

AutoSupport 규모와 시간 예산이 있습니다

AutoSupport는 하위 시스템별로 정보를 수집하고 각 하위 시스템의 콘텐츠에 대한 크기 및 시간 예산을 적용합니다. 스토리지 시스템이 확장됨에 따라 AutoSupport 예산을 통해 AutoSupport 페이로드를 제어할 수 있으므로, AutoSupport 데이터를 확장 가능한 제공할 수 있습니다.

AutoSupport는 하위 시스템 컨텐츠가 크기 또는 시간 예산을 초과하는 경우 정보 수집을 중지하고 AutoSupport 콘텐츠를 잘라냅니다. 콘텐츠를 쉽게 자를 수 없는 경우(예: 이진 파일) AutoSupport에서 콘텐츠를 생략합니다.

NetApp Support에서 요청받은 경우에만 기본 크기 및 시간 예산을 수정해야 합니다. AutoSupport manifest show 명령을 사용하여 하위 시스템의 기본 크기 및 시간 예산을 검토할 수도 있습니다.

이벤트 트리거 **AutoSupport** 메시지로 전송된 파일입니다

이벤트 트리거 AutoSupport 메시지에는 AutoSupport가 메시지를 생성하도록 한 이벤트와 연결된 하위 시스템의 기본 및 문제 해결 정보만 포함됩니다. 특정 데이터는 NetApp 지원 및 지원 파트너가 문제를 해결하는 데 도움이 됩니다.

AutoSupport는 다음 기준을 사용하여 이벤트 트리거 AutoSupport 메시지의 콘텐츠를 제어합니다.

- 포함된 하위 시스템

  데이터는 로그 파일과 같은 공통 하위 시스템 및 RAID와 같은 특정 하위 시스템을 포함한 하위 시스템으로 그룹화됩니다. 각 이벤트는 특정 하위 시스템의 데이터만 포함하는 메시지를 트리거합니다.

- 포함된 각 하위 시스템의 세부 수준

  포함된 각 하위 시스템의 데이터는 기본 또는 문제 해결 수준에서 제공됩니다.

'system node AutoSupport trigger show' 명령을 사용하여 가능한 모든 이벤트를 보고 각 이벤트에 대한 메시지에 포함할 하위 시스템을 '-instance' 매개 변수와 함께 확인할 수 있습니다.

각 이벤트에 기본적으로 포함되는 하위 시스템 외에도 '시스템 노드 AutoSupport trigger modify' 명령어를 사용하여 기본 또는 문제 해결 수준에서 하위 시스템을 추가할 수 있습니다.

AutoSupport 메시지로 전송된 로그 파일

AutoSupport 메시지에는 기술 지원 직원이 최근 시스템 작업을 검토할 수 있도록 하는 몇 가지 주요 로그 파일이 포함될 수 있습니다.

로그 파일 하위 시스템이 활성화된 경우 모든 유형의 AutoSupport 메시지에 다음 로그 파일이 포함될 수 있습니다.

로그 파일	파일에 포함된 데이터의 양입니다
• '/mroot/etc/log/mlog/' 디렉토리에서 파일을 기록합니다 • 메시지 로그 파일입니다	마지막 AutoSupport 메시지 이후 로그에 추가된 새 줄만 지정된 최대값까지 추가됩니다. 이렇게 하면 AutoSupport 메시지에 중복되지 않는 고유한 관련 데이터가 포함됩니다. (파트너의 로그 파일은 예외입니다. 파트너의 경우 허용되는 최대 데이터가 포함됩니다.)
• '/mroot/etc/log/shelflog/' 디렉토리의 로그 파일 • '/mroot/etc/log/acp/' 디렉토리의 로그 파일 • EMS(Event Management System) 로그 데이터	지정된 최대값까지의 최근 데이터 줄.

AutoSupport 메시지의 내용은 ONTAP 릴리스 간에 변경될 수 있습니다.

주간 **AutoSupport** 메시지로 전송된 파일입니다

Weekly AutoSupport 메시지에는 시간에 따른 시스템 변경 사항을 추적하는 데 유용한 추가

구성 및 상태 데이터가 포함되어 있습니다.

다음 정보는 주간 AutoSupport 메시지로 전송됩니다.

- 모든 하위 시스템에 대한 기본 정보
- 선택한 '/mroot/etc' 디렉토리 파일의 내용입니다
- 로그 파일
- 시스템 정보를 제공하는 명령의 출력
- RDB(복제 데이터베이스) 정보, 서비스 통계 등을 비롯한 추가 정보

AutoSupport OnDemand가 기술 지원으로부터 제공 지침을 얻는 방법

AutoSupport OnDemand는 정기적으로 기술 지원 팀과 통신하여 AutoSupport 메시지 전송, 재전송 및 거부 방법과 대용량 파일을 NetApp Support 사이트에 업로드하는 방법에 대한 제공 지침을 얻습니다. AutoSupport OnDemand를 사용하면 AutoSupport 메시지가 주간 AutoSupport 작업이 실행되기를 기다리지 않고 필요 시 전송됩니다.

AutoSupport OnDemand는 다음과 같은 구성 요소로 이루어집니다.

- 각 노드에서 실행되는 AutoSupport OnDemand 클라이언트입니다
- 기술 지원에 상주하는 AutoSupport OnDemand 서비스입니다

AutoSupport OnDemand 클라이언트는 정기적으로 AutoSupport OnDemand 서비스를 폴링하여 기술 지원 부서의 제공 지침을 받습니다. 예를 들어 기술 지원 부서에서는 AutoSupport OnDemand 서비스를 사용하여 새 AutoSupport 메시지 생성이 요청될 수 있습니다. AutoSupport OnDemand 클라이언트가 AutoSupport OnDemand 서비스를 폴링하면 클라이언트는 배달 지침을 얻고 요청에 따라 새 AutoSupport 메시지를 보냅니다.

AutoSupport OnDemand는 기본적으로 사용하도록 설정됩니다. 그러나 AutoSupport OnDemand는 일부 AutoSupport 설정에 의존하여 기술 지원 팀과 계속 통신합니다. AutoSupport OnDemand는 다음 요구 사항이 충족되면 자동으로 기술 지원 팀과 통신합니다.

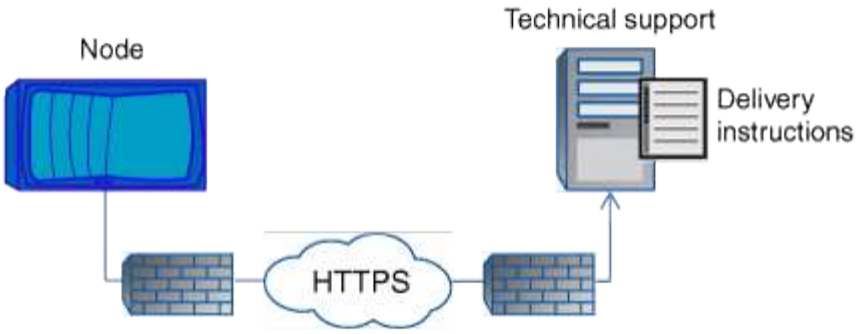
- AutoSupport가 활성화되었습니다.
- AutoSupport는 기술 지원 부서에 메시지를 전송하도록 구성되어 있습니다.
- AutoSupport는 HTTPS 전송 프로토콜을 사용하도록 구성되어 있습니다.

AutoSupport OnDemand 클라이언트는 AutoSupport 메시지가 전송되는 것과 동일한 기술 지원 위치로 HTTPS 요청을 보냅니다. AutoSupport OnDemand 클라이언트는 들어오는 연결을 허용하지 않습니다.

> AutoSupport OnDemand는 "AutoSupport" 사용자 계정을 사용하여 기술 지원 팀과 통신합니다. ONTAP에서는 이 계정을 삭제할 수 없습니다.

AutoSupport OnDemand를 사용하지 않도록 설정하고 AutoSupport를 계속 사용하도록 설정하려면 link:https://docs.netapp.com/us-en/ontap-cli/system-node-autosupport-modify.html#parameters 명령을 사용하십시오[`system node autosupport modify -ondemand-state disable`].

다음 그림에서는 AutoSupport OnDemand가 기술 지원 부서에 HTTPS 요청을 보내 전달 지침을 얻는 방법을 보여줍니다.



배송 지침에는 AutoSupport에서 다음을 수행하도록 요청하는 내용이 포함될 수 있습니다.

- 새 AutoSupport 메시지를 생성합니다.

  기술 지원 부서에서는 문제 선별을 위해 새 AutoSupport 메시지를 요청할 수 있습니다.

- 핵심 덤프 파일 또는 성능 아카이브 파일을 NetApp Support 사이트에 업로드하는 새 AutoSupport 메시지를 생성합니다.

  기술 지원 부서에서는 문제를 선별하기 위해 코어 덤프 또는 성능 아카이브 파일을 요청할 수 있습니다.

- 이전에 생성된 AutoSupport 메시지를 다시 전송합니다.

  이 요청은 배달 실패로 인해 메시지를 받지 못한 경우 자동으로 발생합니다.

- 특정 트리거 이벤트에 대한 AutoSupport 메시지 전달을 비활성화합니다.

  기술 지원 부서에서는 사용되지 않는 데이터의 제공을 비활성화할 수 있습니다.

전자 메일로 보낸 **AutoSupport** 메시지의 구조

AutoSupport 메시지를 전자 메일로 보내면 메시지에 표준 제목, 간단한 본문 및 데이터가 포함된 7z 파일 형식의 대용량 첨부 파일이 포함됩니다.

> AutoSupport가 개인 데이터를 숨기도록 구성된 경우 호스트 이름과 같은 특정 정보는 헤더, 제목, 본문 및 첨부 파일에서 생략되거나 마스킹됩니다.

제목

AutoSupport 메커니즘에서 보낸 메시지의 제목 줄에는 알림의 원인을 식별하는 텍스트 문자열이 포함됩니다. 제목 줄의 형식은 다음과 같습니다.

시스템_이름_(메시지)_심각도 _ 의 HA 그룹 알림

- _System_Name_은 AutoSupport 구성에 따라 호스트 이름 또는 시스템 ID입니다

바디

AutoSupport 메시지 본문에는 다음 정보가 포함됩니다.

- 메시지의 날짜 및 타임 스탬프입니다

- 메시지를 생성한 노드의 ONTAP 버전입니다
- 메시지를 생성한 노드의 시스템 ID, 일련 번호 및 호스트 이름입니다
- AutoSupport 시퀀스 번호
- SNMP 연락처 이름 및 위치(지정된 경우
- HA 파트너 노드의 시스템 ID 및 호스트 이름입니다

첨부 파일

AutoSupport 메시지의 주요 정보는 body.7z라는 7z 파일로 압축되어 메시지에 첨부되는 파일에 포함되어 있습니다.

첨부 파일에 포함된 파일은 AutoSupport 메시지 유형에 따라 다릅니다.

AutoSupport 심각도 유형

AutoSupport 메시지에는 각 메시지의 용도를 이해하는 데 도움이 되는 심각도 유형이 있습니다. 예를 들어 긴급 문제에 즉시 주의를 기울이거나 정보를 제공하는 용도로만 사용됩니다.

메시지에는 다음 심각도 중 하나가 있습니다.

- * 경고 *: 경고 메시지는 조치를 취하지 않을 경우 다음 단계의 이벤트가 발생할 수 있음을 나타냅니다.

  24시간 이내에 경고 메시지에 대해 조치를 취해야 합니다.

- * 비상 *: 중단이 발생했을 때 비상 메시지가 표시됩니다.

  긴급 메시지에 대해 즉시 조치를 취해야 합니다.

- * 오류 *: 오류 조건은 무시할 경우 발생할 수 있는 상황을 나타냅니다.
- * 알림 *: 정상이지만 심각한 상태입니다.
- * 정보 *: 무시할 수 있는 문제에 대한 세부 정보를 제공하는 정보 메시지입니다.
- **Debug**: 디버그 수준 메시지는 수행해야 하는 지침을 제공합니다.

내부 지원 조직이 이메일을 통해 AutoSupport 메시지를 수신하는 경우, 이메일 메시지의 제목 줄에 심각도가 표시됩니다.

AutoSupport 메시지 설명을 봅니다

수신하는 AutoSupport 메시지에 대한 설명은 ONTAP Syslog Translator를 통해 확인할 수 있습니다.

단계

1. 로 이동합니다 "Syslog 변환기".
2. [릴리스] 필드에 사용 중인 **ONTAP** 버전을 입력합니다. 검색 문자열** 필드에 "callhome"을 입력합니다. Translate * 를 선택합니다.
3. Syslog Translator는 사용자가 입력한 메시지 문자열과 일치하는 모든 이벤트를 알파벳 순으로 나열합니다.

AutoSupport 관리를 위한 명령입니다

'시스템 노드 AutoSupport' 명령어를 이용하여 AutoSupport 설정을 변경, 조회, 이전 AutoSupport 메시지 정보 표시, AutoSupport 메시지 전송, 재전송, 취소 등을 할 수 있다.

AutoSupport를 구성합니다

원하는 작업	이 명령 사용...
AutoSupport 메시지 전송 여부를 제어합니다	'system node AutoSupport modify'는 -state 매개 변수를 사용합니다
AutoSupport 메시지가 기술 지원 부서에 전송되는지 여부를 제어합니다	system node AutoSupport modify with the '-support' parameter
AutoSupport를 설정하거나 AutoSupport의 구성을 수정합니다	'시스템 노드 AutoSupport 수정
개별 트리거 이벤트에 대해 내부 지원 조직에 AutoSupport 메시지를 활성화 및 비활성화하고 개별 트리거 이벤트에 대한 응답으로 전송된 메시지에 포함할 추가 하위 시스템 보고서를 지정합니다	'시스템 노드 AutoSupport trigger modify

AutoSupport 구성에 대한 정보를 표시합니다

원하는 작업	이 명령 사용...
AutoSupport 설정을 표시합니다	'system node AutoSupport show'와 '-node' 매개 변수를 함께 사용합니다
AutoSupport 메시지를 수신하는 모든 주소 및 URL의 요약을 봅니다	'System node AutoSupport destinations show'가 나타납니다
개별 트리거 이벤트에 대해 내부 지원 조직에 전송되는 AutoSupport 메시지를 표시합니다	'시스템 노드 AutoSupport trigger show'
AutoSupport 구성 상태 및 다양한 대상에 대한 전송 상태를 표시합니다	'시스템 노드 AutoSupport check show'
AutoSupport 구성의 세부 상태와 다양한 대상에 대한 전송을 표시합니다	'시스템 노드 AutoSupport check show-details

지난 **AutoSupport** 메시지에 대한 정보를 표시합니다

원하는 작업	이 명령 사용...
최근 50개 AutoSupport 메시지 중 하나 이상에 대한 정보를 표시합니다	'시스템 노드 AutoSupport history show'
코어 덤프 또는 성능 아카이브 파일을 기술 지원 사이트나 지정된 URI에 업로드하기 위해 생성된 최근 AutoSupport 메시지에 대한 정보를 표시합니다	'시스템 노드 AutoSupport history show-upload-details'
메시지에 대해 수집된 각 파일의 이름과 크기를 비롯한 AutoSupport 메시지의 정보를 오류 메시지와 함께 확인합니다	'System node AutoSupport manifest show'

AutoSupport 메시지 보내기, 다시 보내기 또는 취소

원하는 작업	이 명령 사용...
AutoSupport 시퀀스 번호로 식별되는 로컬에 저장된 AutoSupport 메시지를 다시 전송합니다 AutoSupport 메시지를 다시 전송하고 해당 메시지를 이미 수신한 경우 지원 시스템에서 중복 케이스를 생성하지 않습니다. 반면에 지원부서에서 해당 메시지를 받지 못한 경우 AutoSupport 시스템은 메시지를 분석하고 필요한 경우 케이스를 생성합니다.	시스템 노드 AutoSupport history retransmit
AutoSupport 메시지 생성 및 전송 — 예를 들어, 테스트용으로 사용합니다	'시스템 노드 AutoSupport 호출' AutoSupport가 비활성화되었더라도 '-force' 매개 변수를 사용하여 메시지를 보냅니다. 구성된 대상 대신 지정한 대상으로 메시지를 보내려면 '-Uri' 매개 변수를 사용합니다.
AutoSupport 메시지를 취소합니다	'시스템 노드 AutoSupport history cancel

관련 정보

"ONTAP 명령 참조입니다"

AutoSupport 매니페스트에 포함된 정보입니다

AutoSupport 매니페스트는 각 AutoSupport 메시지에 대해 수집된 파일에 대한 자세한 보기를 제공합니다. AutoSupport 매니페스트에는 AutoSupport에서 필요한 파일을 수집할 수 없는 경우 컬렉션 오류에 대한 정보도 포함되어 있습니다.

AutoSupport 매니페스트에는 다음 정보가 포함됩니다.

- AutoSupport 메시지의 Sequence Number
- AutoSupport 메시지에 포함된 AutoSupport 파일
- 각 파일의 크기(바이트)입니다
- AutoSupport 매니페스트 컬렉션의 상태입니다
- AutoSupport가 하나 이상의 파일을 수집하지 못한 경우 오류 설명입니다

'system node AutoSupport manifest show' 명령을 사용하여 AutoSupport 매니페스트를 볼 수 있습니다.

AutoSupport 매니페스트는 모든 AutoSupport 메시지에 포함되어 있으며 XML 형식으로 표시됩니다. 즉, 일반 XML 뷰어를 사용하여 읽거나 Active IQ(이전의 My AutoSupport) 포털을 사용하여 볼 수 있습니다.

계획

AutoSupport 사용을 준비합니다

ONTAP 클러스터를 구성하여 AutoSupport 메시지를 NetApp에 전달할 수 있습니다. 또한 일반적으로 조직 내의 로컬 전자 메일 주소로 메시지 복사본을 보낼 수도 있습니다. 사용 가능한 옵션을 검토하여 AutoSupport를 구성할 준비를 해야 합니다.

AutoSupport 메시지를 **NetApp**에 전달합니다

AutoSupport 메시지는 HTTP 또는 SMTP 프로토콜을 사용하여 NetApp에 전달할 수 있습니다. 보안을 강화하기 위해 HTTP와 함께 TLS를 사용할 수 있습니다. ONTAP 9.15.1부터 SMTP와 함께 TLS를 사용할 수도 있습니다.

> 가능하면 항상 TLS와 함께 HTTP(HTTPS)를 사용합니다.

또한 다음 사항에 유의하십시오.

- NetApp AutoSupport 메시지에 대해 하나의 전달 채널만 구성할 수 있습니다. 두 프로토콜을 사용하여 AutoSupport 메시지를 NetApp에 전달할 수는 없습니다.
- AutoSupport는 각 프로토콜의 최대 파일 크기를 제한합니다. AutoSupport 메시지의 크기가 구성된 제한을 초과하는 경우 AutoSupport는 메시지를 최대한 많이 전달하지만 잘립니다.
- 필요한 경우 최대 파일 크기를 변경할 수 있습니다. 명령을 참조하십시오 `system node autosupport modify` 를 참조하십시오.
- 두 프로토콜 모두 이름이 확인되는 주소 패밀리에 따라 IPv4 또는 IPv6를 통해 전송할 수 있습니다.
- ONTAP에서 AutoSupport 메시지를 보내기 위해 설정한 TCP 연결은 일시적이며 단기간 동안 사용됩니다.

HTTP

가장 강력한 기능을 제공합니다. 다음 사항에 유의하십시오.

- AutoSupport OnDemand 및 대용량 파일 전송이 지원됩니다.
- HTTP PUT 요청이 먼저 시도됩니다. 전송 중에 요청이 실패하면 요청이 중지된 곳에서 다시 시작됩니다.
- 서버가 PUT를 지원하지 않으면 HTTP POST 메서드가 대신 사용됩니다.

- HTTP 전송의 기본 제한은 50MB입니다.
- 보안되지 않은 HTTP 프로토콜은 포트 80을 사용합니다.

SMTP

일반적으로 어떤 이유로 HTTPS/HTTP가 허용되지 않거나 지원되지 않는 경우에만 SMTP를 사용해야 합니다. 다음 사항에 유의하십시오.

- AutoSupport OnDemand 및 대용량 파일 전송은 지원되지 않습니다.
- SMTP 로그인 자격 증명이 구성된 경우 암호화되지 않은 상태로 전송됩니다.
- HTTP 전송의 기본 제한은 5MB입니다.
- 비보안 SMTP 프로토콜은 포트 25를 사용합니다.

TLS를 사용하여 보안을 향상합니다

HTTP 또는 SMTP를 사용할 경우 모든 트래픽이 암호화되지 않으므로 쉽게 가로채서 읽을 수 있습니다. HTTP를 사용할 때는 항상 TLS(HTTPS)도 사용하도록 프로토콜을 구성해야 합니다.

> ONTAP 9.15.1부터 SMTP(SMTPS)와 함께 TLS를 사용할 수도 있습니다. 이 경우 TCP 연결이 설정된 후 보안 채널을 활성화하는 _explicit TLS_가 사용됩니다.

보안 프로토콜용 포트

다음 포트는 일반적으로 이러한 프로토콜의 보안 버전에 사용됩니다.

- HTTPS 포트 443입니다
- SMTPS - 포트 587

인증서 검증

TLS를 사용하면 서버에서 다운로드한 인증서의 유효성을 루트 CA 인증서에 따라 ONTAP에서 확인합니다. HTTPS 또는 SMTPS를 사용하기 전에 루트 인증서가 ONTAP에 설치되어 있는지 확인해야 합니다. 을 참조하십시오 서버 인증서를 설치합니다 를 참조하십시오.

추가 구성 고려 사항

AutoSupport를 구성할 때 고려해야 할 몇 가지 추가 사항이 있습니다.

이메일을 사용하여 로컬 사본 보내기

AutoSupport 메시지를 NetApp에 전달하는 데 사용되는 프로토콜에 관계없이 각 메시지의 복사본을 하나 이상의 로컬 전자 메일 주소로 보낼 수도 있습니다. 예를 들어, 내부 지원 조직이나 파트너 조직에 메시지를 보낼 수 있습니다.

> SMTP(또는 SMTPS)를 사용하여 NetApp에 메시지를 전달하고 해당 메시지의 로컬 이메일 사본을 보내는 경우 동일한 이메일 서버 구성이 사용됩니다.

HTTP 프록시

네트워크 구성에 따라 HTTPS 프로토콜을 사용하려면 프록시 URL을 추가로 구성해야 할 수 있습니다. HTTPS를 사용하여 AutoSupport 메시지를 기술 지원 부서에 보내고 프록시가 있는 경우 프록시의 URL을 식별해야 합니다.

프록시가 기본 포트(포트 3128)가 아닌 다른 포트를 사용하는 경우 해당 프록시의 포트를 지정할 수 있습니다. 프록시 인증에 사용할 사용자 이름과 암호를 선택적으로 지정할 수도 있습니다.

서버 인증서를 설치합니다

TLS(HTTPS 또는 SMTPS)를 사용하는 경우 ONTAP에서 서버 인증서의 유효성을 검사할 수 있는지 확인해야 합니다. 이 유효성 검사는 서버 인증서에 서명한 CA를 기반으로 수행됩니다.

ONTAP에는 미리 설치된 루트 CA 인증서가 다수 포함되어 있습니다. 따라서 대부분의 경우 추가 구성 없이 ONTAP에서 서버의 인증서를 즉시 인식합니다. 그러나 서버 인증서 서명 방법에 따라 루트 CA 인증서와 중간 인증서를 설치해야 할 수도 있습니다.

필요한 경우 아래 제공된 지침에 따라 인증서를 설치합니다. 필요한 모든 인증서를 클러스터 수준에서 설치해야 합니다.

예 **1.** 단계

시스템 관리자

1. System Manager에서 * 클러스터 * > * 설정 * 을 선택합니다.
2. 아래로 스크롤하여 * 보안 * 섹션으로 이동합니다.
3. 인증서 * 옆에 있는 을 선택합니다 → .
4. 신뢰할 수 있는 인증 기관 * 탭에서 * 추가 * 를 클릭합니다.
5. 가져오기 * 를 클릭하고 인증서 파일을 선택합니다.
6. 사용자 환경에 대한 구성 매개 변수를 입력합니다.
7. 추가 * 를 클릭합니다.

CLI를 참조하십시오

1. 설치를 시작합니다.

   보안 인증서설치형 server-ca

2. 다음 콘솔 메시지를 찾습니다.

   ```
   Please enter Certificate: Press <Enter> when done
   ```

3. 텍스트 편집기로 인증서 파일을 엽니다.
4. 다음 행을 포함하여 전체 인증서를 복사합니다.

   ```
   -----BEGIN CERTIFICATE-----

   -----END CERTIFICATE-----
   ```

5. 명령 프롬프트 후 터미널에 인증서를 붙여 넣습니다.
6. Enter * 키를 눌러 설치를 완료합니다.
7. 다음 중 하나를 사용하여 인증서가 설치되었는지 확인합니다.

   ```
   security certificate show-user-installed

   security certificate show
   ```

AutoSupport를 설정합니다

ONTAP 클러스터를 구성하여 AutoSupport 메시지를 NetApp 기술 지원에 전달하고 이메일 복사본을 내부 지원 조직에 보낼 수 있습니다. 이러한 작업의 일부로 프로덕션 환경에서 사용하기 전에 구성을 테스트할 수도 있습니다.

이 작업에 대해

ONTAP 9.5부터 클러스터의 모든 노드에 대해 동시에 AutoSupport를 설정하고 구성할 수 있습니다. 새 노드가 클러스터에 추가되면 노드는 동일한 AutoSupport 구성을 자동으로 상속합니다. 이를 지원하기 위해 CLI 명령의 범위를

지정합니다 `system node autosupport modify` 클러스터 레벨입니다. 를 클릭합니다 `-node` 명령 옵션은 이전 버전과의 호환성을 위해 유지되지만 무시됩니다.

> ONTAP 9.4 이하 릴리즈에서는 명령을 사용합니다 `system node autosupport modify` 는 각 노드에 고유합니다. 클러스터에서 ONTAP 9.4 이하를 실행 중인 경우 클러스터의 각 노드에서 AutoSupport를 활성화하고 구성해야 합니다.

시작하기 전에

NetApp에 AutoSupport 메시지를 전달하기 위한 권장 전송 구성은 HTTPS(TLS 포함 HTTP)입니다. 이 옵션은 가장 강력한 기능과 최상의 보안을 제공합니다.

검토 "AutoSupport 사용을 준비합니다" 을 참조하십시오 ONTAP.

단계

1. AutoSupport가 활성화되어 있는지 확인합니다.

```
system node autosupport modify -state enable
```

2. NetApp 기술 지원 부서에서 AutoSupport 메시지를 받으려면 다음 명령을 사용하십시오.

```
system node autosupport modify -support enable
```

   AutoSupport를 AutoSupport OnDemand와 함께 사용하도록 설정하거나 코어 덤프 및 성능 아카이브 파일과 같은 대용량 파일을 기술 지원 또는 지정된 URL에 업로드하려면 이 옵션을 활성화해야 합니다.

3. NetApp 기술 지원 부서에서 AutoSupport 메시지를 받도록 설정한 경우 메시지에 사용할 전송 프로토콜을 지정합니다.

   다음 옵션 중에서 선택할 수 있습니다.

원하는 작업	그런 다음 'system node AutoSupport modify' 명령어의 다음 파라미터를 설정한다…
기본 HTTPS 프로토콜을 사용합니다	a. '-transport'를 'https'로 설정합니다. b. 프록시를 사용하는 경우 프록시 URL로 -proxy-url을 설정합니다. 이 구성은 AutoSupport OnDemand와의 통신 및 대용량 파일 업로드를 지원합니다.
SMTP를 사용합니다	'-transport'를 'MTP'로 설정합니다. 이 구성은 AutoSupport OnDemand 또는 대용량 파일 업로드를 지원하지 않습니다.

4. 내부 지원 조직 또는 지원 파트너가 AutoSupport 메시지를 받도록 하려면 다음 작업을 수행합니다.
   a. 'system node AutoSupport modify' 명령의 다음 매개 변수를 설정하여 조직의 수신자를 식별합니다.

이 매개 변수 설정…	이거면…
'-to'	내부 지원 조직에서 주요 AutoSupport 메시지를 받을 최대 5개의 쉼표로 구분된 개별 이메일 주소 또는 배포 목록
'-noteto'	내부 지원 조직에서 최대 5개의 쉼표로 구분된 개별 이메일 주소 또는 배포 목록을 통해 휴대폰과 기타 모바일 장치용으로 설계된 주요 AutoSupport 메시지의 축약된 버전을 받을 수 있습니다
파트너 주소	지원 파트너 조직에서 모든 AutoSupport 메시지를 쉼표로 구분하여 최대 5개의 개별 이메일 주소 또는 배포 목록을 받을 수 있습니다

b. 'system node AutoSupport destinations show' 명령을 사용하여 대상을 나열하여 주소가 올바르게 구성되었는지 확인합니다.

5. 내부 지원 조직에 메시지를 보내거나 기술 지원 메시지에 대해 SMTP 전송을 선택한 경우 'system node AutoSupport modify' 명령의 다음 매개 변수를 설정하여 SMTP를 구성합니다.

   - 메일 호스트를 쉼표로 구분하여 하나 이상의 메일 호스트로 설정합니다.

     최대 5개까지 설정할 수 있습니다.

   메일 호스트 이름 뒤에 콜론과 포트 번호를 지정하여 각 메일 호스트에 대한 포트 값을 구성할 수 있습니다. 예를 들어, mymailhost.example.com:5678`, 여기서 5678은 메일 호스트의 포트입니다.

   - AutoSupport 메시지를 보내는 e-메일 주소로 '-from'을 설정합니다.

6. DNS를 구성합니다.

7. 필요에 따라 특정 설정을 변경하려면 명령 옵션을 추가합니다.

이 작업을 수행하려면…	그런 다음 'system node AutoSupport modify' 명령어의 다음 파라미터를 설정한다…
메시지에서 중요한 데이터를 제거, 마스킹 또는 인코딩하여 개인 데이터를 숨깁니다	설정 `-remove-private-data` 를 선택합니다 `true`. 에서 변경한 경우 `false` 를 선택합니다 `true`모든 AutoSupport 기록 및 모든 관련 파일이 삭제됩니다.
Periodic AutoSupport 메시지로 성능 데이터 전송을 중지합니다	-perf를 false로 설정합니다.

8. SMTP를 사용하여 NetApp에 AutoSupport 메시지를 전달하는 경우 보안을 강화하기 위해 TLS를 선택적으로 활성화할 수 있습니다.

   a. 새 매개변수에 사용할 수 있는 값을 표시합니다.

```
cluster1::> system node autosupport modify -smtp-encryption ?
```

b. SMTP 메시지 배달을 위해 TLS 활성화:

```
cluster1::> system node autosupport modify -smtp-encryption start_tls
```

c. 현재 구성을 표시합니다.

```
cluster1::> system node autosupport show -fields smtp-encryption
```

9. 'system node AutoSupport show' 명령을 '-node' 매개변수와 함께 사용하여 전체 설정을 확인한다.
10. 'system node AutoSupport check show' 명령어를 사용해 AutoSupport 작동을 확인한다.

    문제가 보고되면 'system node AutoSupport check show-details' 명령어를 사용하여 더 많은 정보를 볼 수 있다.

11. AutoSupport 메시지가 전송 및 수신되고 있는지 테스트합니다.

    a. 를 사용합니다 `system node autosupport invoke` 명령과 함께 `-type` 매개 변수를 로 설정합니다 `test`:

    ```
    cluster1::> system node autosupport invoke -type test -node node1
    ```

    b. NetApp에서 AutoSupport 메시지를 수신하는지 확인합니다.

    ```
    system node autosupport history show -node local
    ```

    최근 나가는 AutoSupport 메시지의 상태는 모든 해당 프로토콜 대상에 대해 '성공적으로 완료'로 변경되어야 합니다.

    c. 필요에 따라 에 구성한 모든 주소의 이메일을 확인하여 AutoSupport 메시지가 내부 지원 조직 또는 지원 파트너에게 전송되는지 확인합니다 `-to`, `-noteto`, 또는 `-partner-address` 의 매개 변수 `system node autosupport modify` 명령.

구성

AutoSupport 설정을 관리합니다

System Manager를 사용하여 AutoSupport 계정의 설정을 관리할 수 있습니다.

다음 절차를 수행할 수 있습니다.

AutoSupport 설정을 봅니다

시스템 관리자를 사용하여 AutoSupport 계정의 설정을 볼 수 있습니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 클릭합니다.

   AutoSupport* 섹션에 다음 정보가 표시됩니다.

   - 상태
   - 전송 프로토콜
   - 프록시 서버
   - 보낸 사람 이메일 주소

2. AutoSupport * 섹션에서 을 선택한 다음 * 추가 옵션 * 을 ⋮선택합니다.

   AutoSupport 연결 및 전자 메일 설정에 대한 추가 정보가 표시됩니다. 또한 메시지의 전송 기록이 나열됩니다.

AutoSupport 데이터를 생성하고 전송합니다

System Manager에서 AutoSupport 메시지 생성을 시작하고 데이터가 수집되는 클러스터 노드 또는 노드를 선택할 수 있습니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. AutoSupport * 섹션에서 을 ⋮선택한 다음 * 생성 및 전송 * 을 선택합니다.
3. 제목을 입력합니다.
4. 데이터를 수집할 노드를 지정하려면 * 데이터 수집 위치 * 아래의 확인란을 선택합니다.

AutoSupport 연결을 테스트합니다

System Manager에서 테스트 메시지를 보내 AutoSupport에 대한 연결을 확인할 수 있습니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 클릭합니다.
2. AutoSupport * 섹션에서 을 ⋮선택한 다음 * Test Connectivity * 를 선택합니다.
3. 메시지의 제목을 입력합니다.

AutoSupport를 활성화 또는 비활성화합니다

AutoSupport는 가능한 구성 문제의 사전 식별 및 신속한 지원 케이스 해결을 포함하여 NetApp 고객에게 검증된 비즈니스 이점을 제공합니다. AutoSupport는 새로운 시스템에서 기본적으로 활성화되어 있습니다. 필요한 경우, System Manager를 사용하여 AutoSupport의 기능을 해제하여 스토리지 시스템의 상태를 모니터링하고 알림 메시지를 보낼 수 있습니다. AutoSupport를 비활성화한 후 다시 활성화할 수 있습니다.

이 작업에 대해

AutoSupport를 사용하지 않도록 설정하기 전에 NetApp Call-Home 시스템을 끄면 다음과 같은 이점을 얻을 수 있다는 점에 유의해야 합니다.

- * 상태 모니터링 *: AutoSupport는 스토리지 시스템의 상태를 모니터링하고 기술 지원 부서 및 내부 지원 부서에 알림을 전송합니다.
- * 자동화 *: AutoSupport는 지원 사례 보고를 자동화합니다. 대부분의 지원 케이스는 고객이 문제를 인지하기 전에 자동으로 열립니다.
- * 신속한 해결 *: AutoSupport 데이터를 전송하는 시스템은 AutoSupport 데이터를 보내지 않는 시스템에 비해 절반의 시간 내에 지원 사례를 해결할 수 있습니다.
- * 더 빠른 업그레이드 *: AutoSupport는 System Manager의 버전 업그레이드, 애드온, 갱신 및 펌웨어 업데이트 자동화와 같은 고객 셀프 서비스 워크플로를 지원합니다.
- * 더 많은 기능 *: 다른 툴의 특정 기능은 AutoSupport가 활성화된 경우(예: BlueXP의 일부 워크플로)에서만 작동합니다.

단계

1. 클러스터 > 설정 * 을 선택합니다.
2. AutoSupport * 섹션에서 을 선택한 다음 * 사용 안 함 * 을 ⋮선택합니다.
3. AutoSupport를 다시 활성화하려면 * AutoSupport * 섹션에서 를 선택한 다음 * 활성화 * 를 ⋮선택합니다.

지원 케이스 생성을 억제합니다

ONTAP 9.10.1부터 System Manager를 사용하여 AutoSupport에 요청을 보내 지원 케이스 생성을 억제할 수 있습니다.

이 작업에 대해

지원 케이스 생성을 억제하려면 노드 및 억제를 수행할 시간 수를 지정합니다.

시스템에서 유지 관리를 수행하는 동안 AutoSupport에서 자동화된 케이스를 생성하지 않으려는 경우 지원 케이스를 억제하면 특히 유용합니다.

단계

1. 클러스터 > 설정 * 을 선택합니다.
2. AutoSupport * 섹션에서 를 ⋮선택한 다음 * 지원 케이스 생성 안 함 * 을 선택합니다.
3. 억제가 발생할 시간을 입력합니다.
4. 기능 억제를 수행할 노드를 선택합니다.

지원 케이스 생성을 재개합니다

ONTAP 9.10.1부터 System Manager를 사용하면 AutoSupport에서 지원 케이스가 억제된 경우 해당 케이스를 다시 생성할 수 있습니다.

단계

1. 클러스터 > 설정 * 을 선택합니다.
2. AutoSupport * 섹션에서 를 ⋮선택한 다음 * 지원 케이스 생성 재개 * 를 선택합니다.
3. 생성을 재개할 노드를 선택합니다.

AutoSupport 설정을 편집합니다

시스템 관리자를 사용하여 AutoSupport 계정의 연결 및 이메일 설정을 수정할 수 있습니다.

단계

1. 클러스터 > 설정 * 을 선택합니다.
2. AutoSupport * 섹션에서 을 선택한 다음 * 추가 옵션 * 을 ⋮선택합니다.
3. 연결 * 섹션 또는 * 이메일 * 섹션에서 을 Edit 선택하여 어느 섹션의 설정을 수정합니다.

예약된 유지 관리 기간 동안 **AutoSupport** 케이스 생성을 억제합니다

AutoSupport 케이스 억제를 사용하면 예약된 유지 관리 기간 동안 트리거된 AutoSupport 메시지에 의해 불필요한 케이스가 생성되지 않도록 할 수 있습니다.

단계

1. 텍스트 문자열을 사용하여 AutoSupport 메시지를 수동으로 `MAINT=xh`호출합니다. 여기서 는 유지 보수 기간 (시간) 입니다. `x <node>를 AutoSupport 메시지를 보낼 노드의 이름으로 바꿉니다.

```
system node autosupport invoke -node <node> -message MAINT=xh
```

관련 정보

- "ONTAP 명령 참조입니다"
- "예약된 유지 보수 기간 동안 자동 케이스 생성을 억제하는 방법"

AutoSupport를 사용하여 파일을 업로드합니다

코어 덤프 파일을 업로드합니다

코어 덤프 파일이 저장되면 이벤트 메시지가 생성됩니다. AutoSupport 서비스가 활성화되어 NetApp 지원으로 메시지를 보내도록 구성된 경우 AutoSupport 메시지가 전송되고 자동 이메일 확인이 전송됩니다.

필요한 것

- 다음 설정으로 AutoSupport를 설정해야 합니다.
  - AutoSupport가 노드에서 활성화되어 있습니다.
  - AutoSupport는 기술 지원 부서에 메시지를 전송하도록 구성되어 있습니다.
  - AutoSupport는 HTTP 또는 HTTPS 전송 프로토콜을 사용하도록 구성됩니다.

    코어 덤프 파일과 같이 큰 파일이 포함된 메시지를 보낼 때는 SMTP 전송 프로토콜이 지원되지 않습니다.

이 작업에 대해

NetApp 지원 요청이 있을 경우 'system node AutoSupport invoke-core-upload' 명령을 사용하여 HTTPS를 통해 코어 덤프 파일을 업로드할 수도 AutoSupport 있습니다.

"NetApp에 파일을 업로드하는 방법"

단계

1. system node coredump show 명령을 사용하여 노드의 코어 덤프 파일을 봅니다.

   다음 예에서는 로컬 노드에 대해 코어 덤프 파일이 표시됩니다.

   ```
   cluster1::> system node coredump show -node local
   Node:Type Core Name Saved Panic Time
   --------- ------------------------------------------- -----
   -----------------
   node:kernel
   core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
   ```

2. 'system node AutoSupport invoke-core-upload' 명령어를 사용해 AutoSupport 메시지를 생성하고 core dump 파일을 업로드 한다.

   다음 예에서는 AutoSupport 메시지가 생성되어 기술 지원인 기본 위치로 전송되고 코어 덤프 파일이 NetApp Support 사이트인 기본 위치에 업로드됩니다.

   ```
   cluster1::> system node autosupport invoke-core-upload -core-filename
   core.4073000068.2013-09-11.15_05_01.nz -node local
   ```

   다음 예에서는 AutoSupport 메시지가 생성되어 URI에 지정된 위치로 전송되며 코어 덤프 파일이 URI에 업로드됩니다.

   ```
   cluster1::> system node autosupport invoke-core-upload -uri
   https//files.company.com -core-filename
   core.4073000068.2013-09-11.15_05_01.nz -node local
   ```

성능 아카이브 파일을 업로드합니다

성능 아카이브가 포함된 AutoSupport 메시지를 생성하고 보낼 수 있습니다. 기본적으로 NetApp 기술 지원에는 AutoSupport 메시지가 표시되고 성능 아카이브는 NetApp Support 사이트에 업로드됩니다. 메시지에 대한 대체 대상을 지정하고 업로드할 수 있습니다.

필요한 것

- 다음 설정으로 AutoSupport를 설정해야 합니다.
  - AutoSupport가 노드에서 활성화되어 있습니다.
  - AutoSupport는 기술 지원 부서에 메시지를 전송하도록 구성되어 있습니다.
  - AutoSupport는 HTTP 또는 HTTPS 전송 프로토콜을 사용하도록 구성됩니다.

    성능 아카이브 파일과 같은 대용량 파일이 포함된 메시지를 보낼 때는 SMTP 전송 프로토콜이 지원되지

않습니다.

이 작업에 대해

업로드할 성능 아카이브 데이터의 시작 날짜를 지정해야 합니다. 대부분의 스토리지 시스템은 성능 아카이브를 2주 동안 유지하여 시작 날짜를 최대 2주 전에 지정할 수 있습니다. 예를 들어 오늘이 1월 15일인 경우 1월 2일의 시작 날짜를 지정할 수 있습니다.

단계

1. 'system node AutoSupport invoke-performance-archive' 명령어를 사용하여 AutoSupport 메시지를 생성하고 성능 아카이브 파일을 업로드합니다.

   다음 예에서는 2015년 1월 12일부터 4시간 동안 성능 아카이브 파일이 AutoSupport 메시지에 추가되고 NetApp Support 사이트인 기본 위치에 업로드됩니다.

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h
   ```

   다음 예에서는 2015년 1월 12일부터 4시간 동안의 성능 아카이브 파일이 AutoSupport 메시지에 추가되고 URI에 의해 지정된 위치에 업로드됩니다.

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h -uri
   https://files.company.com
   ```

문제 해결

메시지가 수신되지 않을 경우 **AutoSupport** 문제를 해결합니다

시스템에서 AutoSupport 메시지를 보내지 않는 경우 AutoSupport에서 메시지를 생성할 수 없거나 메시지를 전달할 수 없기 때문에 메시지를 보낼 수 있는지 여부를 확인할 수 있습니다.

단계

1. System node AutoSupport history show 명령을 사용하여 메시지의 delivery 상태를 확인한다.
2. 상태를 읽습니다.

이 상태입니다	의미합니다
초기화 중입니다	수집 프로세스가 시작됩니다. 이 상태가 일시적일 경우 모든 것이 좋습니다. 그러나 이 상태가 지속되면 문제가 있는 것입니다.
수집 실패	AutoSupport가 스풀 디렉터리에 AutoSupport 콘텐츠를 만들 수 없습니다. 'system node AutoSupport history show-detail' 명령어를 입력하여 AutoSupport가 수집하려는 정보를 확인할 수 있다.

이 상태입니다	의미합니다
수집 중입니다	AutoSupport가 AutoSupport 콘텐츠를 수집하고 있습니다. 'system node AutoSupport manifest show' 명령어를 입력하여 AutoSupport가 수집하는 정보를 확인할 수 있다.
대기열에 있습니다	AutoSupport 메시지는 전달 대기 상태이지만 아직 전달되지 않았습니다.
전송 중입니다	AutoSupport가 현재 메시지를 전달하고 있습니다.
전송됨 - 성공했습니다	AutoSupport가 메시지를 성공적으로 전달했습니다. 'system node AutoSupport history show-delivery' 명령어를 입력하여 AutoSupport가 메시지를 전달한 위치를 확인할 수 있다.
무시	AutoSupport에 메시지의 대상이 없습니다. 'system node AutoSupport history show-delivery' 명령어를 입력하여 전달 세부 정보를 볼 수 있다.
다시 대기 중입니다	AutoSupport가 메시지를 전달하려고 했지만 시도가 실패했습니다. 따라서 AutoSupport는 다른 시도를 위해 메시지를 배달 대기열에 다시 배치했습니다. System node AutoSupport history show 명령을 입력하여 오류를 확인할 수 있다.
전송 - 실패	AutoSupport가 지정된 횟수만큼 메시지를 배달하지 못하여 메시지 전달 시도를 중지했습니다. System node AutoSupport history show 명령을 입력하여 오류를 확인할 수 있다.
OnDemand - 무시	AutoSupport 메시지가 처리되었지만 AutoSupport OnDemand 서비스에서 무시하도록 선택했습니다.

3. 다음 작업 중 하나를 수행합니다.

이 상태를 표시합니다	이렇게 하십시오
초기화 또는 수집 실패	AutoSupport에서 메시지를 생성할 수 없으므로 NetApp 지원에 문의하십시오. 다음 기술 자료 문서를 언급합니다. "AutoSupport에서 전송 실패: 초기화 중에 상태가 고착됨"
무시, 다시 대기 중 또는 전송에 실패했습니다	AutoSupport에서 메시지를 전달할 수 없으므로 SMTP, HTTP 또는 HTTPS에 대해 대상이 올바르게 구성되었는지 확인합니다.

HTTP 또는 **HTTPS**를 통한 **AutoSupport** 메시지 전송 문제를 해결합니다

시스템이 예상 AutoSupport 메시지를 전송하지 않고 HTTP 또는 HTTPS를 사용하고 있거나 자동 업데이트 기능이 작동하지 않는 경우 여러 설정을 확인하여 문제를 해결할 수 있습니다.

필요한 것

기본 네트워크 연결 및 DNS 조회를 확인해야 합니다.

- 노드 관리 LIF가 운영 및 관리 상태이어야 합니다.
- 클러스터 관리 LIF(노드의 LIF가 아님)에서 동일한 서브넷에 있는 기능 호스트를 ping할 수 있어야 합니다.
- 클러스터 관리 LIF에서 서브넷 외부의 기능 호스트를 Ping할 수 있어야 합니다.
- IP 주소가 아닌 호스트의 이름을 사용하여 클러스터 관리 LIF에서 서브넷 외부의 기능 호스트를 Ping할 수 있어야 합니다.

이 작업에 대해

이러한 단계는 AutoSupport가 메시지를 생성할 수 있지만 HTTP 또는 HTTPS를 통해 메시지를 전달할 수 없는 경우에 적용됩니다.

오류가 발생하거나 이 절차의 단계를 완료할 수 없는 경우 다음 단계로 진행하기 전에 문제를 확인하고 해결하십시오.

단계

1. AutoSupport 하위 시스템의 세부 상태를 표시합니다.

   '시스템 노드 AutoSupport check show-details

   여기에는 테스트 메시지를 전송하고 AutoSupport 구성 설정에서 발생할 수 있는 오류 목록을 제공하여 AutoSupport 대상에 대한 연결을 확인하는 작업이 포함됩니다.

2. 노드 관리 LIF의 상태를 확인합니다.

   'network interface show-home-node local-role node-mgmt-fields vserver, lif, status-oper, status-admin, address, role'

   '돌격대'와 '상태-관리자' 필드는 '위로'가 되어야 합니다.

3. 나중에 사용할 수 있도록 SVM 이름, LIF 이름 및 LIF IP 주소를 기록합니다.
4. DNS가 올바르게 설정 및 구성되었는지 확인합니다.

   'vserver services name-service dns show'

5. AutoSupport 메시지가 반환한 모든 오류를 해결합니다.

   'System node AutoSupport history show -node * -fields node, seq -num, destination, last-update, status, error'

   반환된 오류에 대한 문제 해결에 대한 자세한 내용은 을 참조하십시오 "ONTAP AutoSupport(전송 HTTPS 및 HTTP) 해상도 안내서입니다".

6. 클러스터가 필요한 서버와 인터넷에 모두 액세스할 수 있는지 확인합니다.

   a. 'network traceroute-lif node-management_LIF-destination DNS server
   b. 네트워크 traceroute-lif node_management_LIF-destination support.netapp.com`

> 주소인 upport.netapp.com` 자체는 ping/traceroute에 응답하지 않지만, per-hop 정보는 가치가 있다.

c. '시스템 노드 AutoSupport show-fields proxy-url

d. 'network traceroute-node_management_LIF-destination proxy_url

이러한 경로 중 하나라도 작동하지 않는 경우, 대부분의 타사 네트워크 클라이언트에 있는 ""traceroute"" 또는 ""tracert""" 유틸리티를 사용하여 클러스터와 동일한 서브넷의 작동 호스트에서 동일한 경로를 시도해 보십시오. 이렇게 하면 문제가 네트워크 구성에 있는지 또는 클러스터 구성에 있는지 여부를 확인할 수 있습니다.

7. AutoSupport 전송 프로토콜에 HTTPS를 사용하는 경우 HTTPS 트래픽이 네트워크를 종료할 수 있는지 확인합니다.

   a. 클러스터 관리 LIF와 동일한 서브넷에 있는 웹 클라이언트를 구성합니다.

      동일한 프록시 서버, 사용자 이름, 암호 및 포트 사용을 포함하여 모든 구성 매개 변수가 AutoSupport 구성과 동일한 값인지 확인합니다.

   b. 웹 클라이언트를 사용하여 'https://support.netapp.com` 액세스합니다.

      액세스가 성공적으로 이루어져야 합니다. 그렇지 않은 경우 모든 방화벽이 HTTPS 및 DNS 트래픽을 허용하도록 올바르게 구성되어 있고 프록시 서버가 올바르게 구성되어 있는지 확인하십시오. support.netapp.com 에 대한 정적 이름 확인을 구성하는 방법에 대한 자세한 내용은 기술 자료 문서를 참조하십시오 "ONTAP for support.netapp.com? 에서 호스트 항목을 추가하는 방법은"

8. ONTAP 9.10.1부터 자동 업데이트 기능을 활성화한 경우 다음 추가 URL에 HTTPS 연결이 있는지 확인합니다.
   - https://support-sg-emea.netapp.com 으로 문의하십시오
   - https://support-sg-naeast.netapp.com 으로 문의하십시오
   - https://support-sg-nawest.netapp.com 으로 문의하십시오

SMTP를 통한 **AutoSupport** 메시지 전달 문제를 해결합니다

시스템이 SMTP를 통해 AutoSupport 메시지를 전달할 수 없는 경우 여러 설정을 확인하여 문제를 해결할 수 있습니다.

필요한 것

기본 네트워크 연결 및 DNS 조회를 확인해야 합니다.

- 노드 관리 LIF가 운영 및 관리 상태이어야 합니다.
- 클러스터 관리 LIF(노드의 LIF가 아님)에서 동일한 서브넷에 있는 기능 호스트를 ping할 수 있어야 합니다.
- 클러스터 관리 LIF에서 서브넷 외부의 기능 호스트를 Ping할 수 있어야 합니다.
- IP 주소가 아닌 호스트의 이름을 사용하여 클러스터 관리 LIF에서 서브넷 외부의 기능 호스트를 Ping할 수 있어야 합니다.

이 작업에 대해

다음 단계는 AutoSupport에서 메시지를 생성할 수 있지만 SMTP를 통해 메시지를 전달할 수 없는 경우를 위한 것입니다.

오류가 발생하거나 이 절차의 단계를 완료할 수 없는 경우 다음 단계로 진행하기 전에 문제를 확인하고 해결하십시오.

별도로 지정하지 않는 한 모든 명령은 ONTAP 명령줄 인터페이스에 입력됩니다.

단계

1. 노드 관리 LIF의 상태를 확인합니다.

   '* 네트워크 인터페이스 show-home-node local-role node-mgmt-fields vserver, lif, status-oper, status-admin, address, role *

   '돌격대'와 '상태-관리자' 필드는 '위로'가 되어야 합니다.

2. 나중에 사용할 수 있도록 SVM 이름, LIF 이름 및 LIF IP 주소를 기록합니다.
3. DNS가 올바르게 설정 및 구성되었는지 확인합니다.

   ``vserver services name-service dns show *''를 참조하십시오

4. AutoSupport에서 사용하도록 구성된 모든 서버를 표시합니다.

   ``시스템 노드 AutoSupport 표시 필드 메일-호스트*'

   표시된 모든 서버 이름을 기록합니다.

5. 이전 단계에서 표시한 각 서버 및 'upport.netapp.com` 에 대해 노드에서 서버 또는 URL에 연결할 수 있는지 확인합니다.

   '* network traceroute-node local-destination_server_name_*'

   이러한 경로 중 하나라도 작동하지 않는 경우, 대부분의 타사 네트워크 클라이언트에 있는 ""traceroute"" 또는 ""tracert""" 유틸리티를 사용하여 클러스터와 동일한 서브넷의 작동 호스트에서 동일한 경로를 시도해 보십시오. 이렇게 하면 문제가 네트워크 구성에 있는지 또는 클러스터 구성에 있는지 여부를 확인할 수 있습니다.

6. 메일 호스트로 지정된 호스트에 로그인하고 SMTP 요청을 처리할 수 있는지 확인합니다.

   ``netstat-Aan|grep 25 *'

   수신 SMTP 포트 번호는 25입니다.

   다음 텍스트와 유사한 메시지가 표시됩니다.

   ```
   ff64878c tcp        0      0  *.25    *.*    LISTEN.
   ```

7. 다른 호스트에서 메일 호스트의 SMTP 포트로 텔넷 세션을 엽니다.

   '* telnet_mailhost_25 * '

   다음 텍스트와 유사한 메시지가 표시됩니다.

```
220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
10:49:04 PST
```

8. 텔넷 프롬프트에서 메일 호스트로부터 메시지를 전달할 수 있는지 확인합니다.

   ' * HELO_DOMAIN_NAME_ * '

   (* 메일 보낸 사람: _ your_email_address_ *)

   (* RCPT to:autosupport@netapp.com *)

   domain_name은 네트워크의 도메인 이름입니다.

   Relaying이 denied로 되어 있는 오류가 반환되면 메일 호스트에서 relaying이 활성화되지 않습니다. 시스템 관리자에게 문의하십시오.

9. 텔넷 프롬프트에서 테스트 메시지를 보냅니다.

   ' * 데이터 * '

   시험대상자: 시험 *' 이것은 시험이다 *'

   `. * '

   > 줄의 마지막 기간(.)을 직접 입력해야 합니다. 이 기간은 메일 호스트에 메시지가 완료되었음을 나타냅니다.

   오류가 반환되면 메일 호스트가 올바르게 구성되지 않은 것입니다. 시스템 관리자에게 문의하십시오.

10. ONTAP 명령줄 인터페이스에서 AutoSupport 테스트 메시지를 액세스 권한이 있는 신뢰할 수 있는 전자 메일 주소로 보냅니다.

    '* 시스템 노드 AutoSupport invoke-node local-type test*'

11. 시도의 순서 번호를 찾습니다.

    ``시스템 노드 AutoSupport 이력 표시 노드 로컬 대상 SMTP*'

    타임 스탬프를 기준으로 시도 순서 번호를 찾습니다. 가장 최근에 시도한 시도일 것입니다.

12. 테스트 메시지 시도에 대한 오류를 표시합니다.

    '* system node AutoSupport history show -node local -seq -num seq_num -fields error *

    표시된 오류가 '로그인 거부'인 경우 SMTP 서버가 클러스터 관리 LIF의 전송 요청을 수락하지 않습니다. 전송 프로토콜로 HTTPS 사용을 변경하지 않으려면 사이트 네트워크 관리자에게 문의하여 이 문제를 해결할 SMTP 게이트웨이를 구성하십시오.

    이 테스트가 성공했지만 mailto:autosupport@netapp.com 으로 전송된 동일한 메시지가 없으면 모든 SMTP 메일 호스트에서 SMTP 릴레이가 활성화되어 있는지 확인하거나 HTTPS를 전송 프로토콜로 사용하십시오.

로컬로 관리되는 전자 메일 계정에 대한 메시지도 성공하지 못한 경우 SMTP 서버가 다음 두 특성을 모두 사용하여 첨부 파일을 전달하도록 구성되었는지 확인합니다.

- "7z" 접미사
- "application/x-7x-compressed" MIME 형식.

AutoSupport 하위 시스템 문제를 해결합니다

'system node check show' 명령어를 이용하여 AutoSupport 구성 및 제공과 관련된 모든 문제를 확인하고 해결할 수 있다.

단계

1. 다음 명령을 사용하여 AutoSupport 하위 시스템의 상태를 표시합니다.

이 명령 사용...	수행할 작업...
``시스템 노드 AutoSupport CHOK SHOW *'	AutoSupport HTTP 또는 HTTPS 대상, AutoSupport SMTP 대상, AutoSupport OnDemand 서버 및 AutoSupport 구성과 같은 AutoSupport 하위 시스템의 전체 상태를 표시합니다
``시스템 노드 AutoSupport CHOK SHOW-details *'	오류에 대한 자세한 설명과 수정 조치 등 AutoSupport 하위 시스템의 세부 상태를 표시합니다

상태 모니터링

시스템 상태 모니터링 개요

상태 모니터는 클러스터의 특정 중요한 상태를 능동적으로 모니터링하고 장애 또는 위험을 감지하는 경우 경고를 표시합니다. 활성 경고가 있는 경우 시스템 상태는 클러스터에 대한 성능 저하 상태를 보고합니다. 알림에는 저하된 시스템 상태에 응답하는 데 필요한 정보가 포함됩니다.

상태가 성능 저하인 경우 가능한 원인 및 권장 복구 조치를 포함하여 문제에 대한 세부 정보를 볼 수 있습니다. 문제를 해결한 후 시스템 상태는 자동으로 OK로 복귀합니다.

시스템 상태는 여러 개의 개별 상태 모니터를 반영합니다. 개별 상태 모니터의 성능 저하 상태는 전체 시스템 상태의 성능 저하 상태를 야기합니다.

ONTAP가 클러스터에서 시스템 상태 모니터링을 위해 클러스터 스위치를 지원하는 방법에 대한 자세한 내용은 _Hardware Universe_를 참조하십시오.

"Hardware Universe에서 지원되는 스위치입니다"

CSMM(Cluster Switch Health Monitor) AutoSupport 메시지의 원인과 이러한 경고를 해결하는 데 필요한 조치에 대한 자세한 내용은 기술 자료 문서를 참조하십시오.

"AutoSupport 메시지: 상태 모니터 프로세스 CSMM"

상태 모니터링 작동 방식

개별 상태 모니터에는 특정 조건이 발생할 때 알림을 트리거하는 일련의 정책이 있습니다. 상태 모니터링 작동 방식을 이해하면 문제에 대응하고 향후 경고를 제어하는 데 도움이 됩니다.

상태 모니터링은 다음과 같은 구성 요소로 이루어집니다.

- 개별 상태는 특정 서브시스템에 대한 모니터링을 하며, 각 하위 시스템은 자체 상태를 가지고 있습니다

  예를 들어, 스토리지 서브시스템에는 노드 연결 상태 모니터가 있습니다.

- 개별 상태 모니터의 상태를 통합하는 전체 시스템 상태 모니터입니다

  단일 서브시스템의 성능 저하 상태가 전체 시스템의 성능 저하 상태를 초래하게 됩니다. 하위 시스템에 경고가 없으면 전체 시스템 상태가 정상입니다.

각 상태 모니터는 다음과 같은 주요 요소로 구성됩니다.

- 상태 모니터에서 발생할 수 있는 경고입니다

  각 알림에는 알림의 심각도 및 가능한 원인과 같은 세부 정보가 포함된 정의가 있습니다.

- 각 알림이 트리거되는 시기를 식별하는 상태 정책입니다

  각 상태 정책에는 경고를 트리거하는 정확한 조건이나 변경 조건인 규칙 식이 있습니다.

상태 모니터는 서브시스템의 리소스에 대한 상태 또는 상태 변경을 지속적으로 모니터링 및 검증합니다. 상태 또는 상태 변경이 상태 정책의 규칙 식과 일치하면 상태 모니터에서 알림을 발생시킵니다. 알림을 통해 하위 시스템의 상태 및 전체 시스템 상태가 성능 저하 상태가 됩니다.

시스템 상태 알림에 응답하는 방법

시스템 상태 경고가 발생하면 이를 확인하고, 자세히 알아보고, 기본 상태를 수리하고, 문제가 다시 발생하지 않도록 할 수 있습니다.

상태 모니터에서 알림을 발생시키면 다음 방법 중 하나를 사용하여 응답할 수 있습니다.

- 영향을 받는 리소스, 경고 심각도, 가능한 원인, 가능한 영향 및 수정 조치가 포함된 알림에 대한 정보를 얻을 수 있습니다.
- 알림이 발생한 시간, 다른 사용자가 이미 알림을 확인했는지 여부 등 알림에 대한 자세한 정보를 확인합니다.
- 특정 쉘프 또는 디스크와 같은 영향을 받는 리소스 또는 하위 시스템의 상태에 대한 상태 관련 정보를 가져옵니다.
- 누군가 문제를 해결하고 있음을 알리고 자신을 "확인자"로 식별합니다.
- 연결 문제를 해결하기 위해 케이블 연결 문제 해결 등 알림에 제공된 수정 조치를 수행하여 문제를 해결합니다.
- 시스템에서 자동으로 경고를 지우지 않은 경우 해당 경고를 삭제합니다.
- 알림을 표시하지 않도록 하여 하위 시스템의 상태에 영향을 주지 않도록 합니다.

  기능 억제는 문제를 이해할 때 유용합니다. 경고를 표시하지 않으면 알림이 계속 발생할 수 있지만 하위 시스템

상태가 "ok-with-suppressed"로 표시됩니다.

시스템 상태 경고 사용자 지정

알림이 트리거되는 시기를 정의하는 시스템 상태 정책을 설정 및 해제하여 상태 모니터에서 생성되는 알림을 제어할 수 있습니다. 이를 통해 특정 환경에 맞게 상태 모니터링 시스템을 사용자 지정할 수 있습니다.

생성된 알림에 대한 세부 정보를 표시하거나 특정 상태 모니터, 노드 또는 알림 ID에 대한 정책 정의를 표시하여 정책의 이름을 확인할 수 있습니다.

상태 정책을 사용하지 않도록 설정하는 것은 알림을 표시하지 않는 것과 다릅니다. 알림을 표시하지 않으면 하위 시스템의 상태에 영향을 주지 않지만 알림은 계속 발생할 수 있습니다.

정책을 사용하지 않도록 설정하면 해당 정책 규칙 식에 정의된 조건이나 상태가 더 이상 알림을 트리거하지 않습니다.

비활성화하려는 알림의 예

예를 들어 사용자에게 유용하지 않은 경고가 발생한다고 가정합니다. 'system health alert show –instance' 명령을 사용하여 경고의 정책 ID를 가져옵니다. 'system health policy definition show' 명령에서 정책 ID를 사용하여 정책에 대한 정보를 확인할 수 있습니다. 규칙 식 및 정책에 대한 기타 정보를 검토한 후 정책을 사용하지 않도록 설정합니다. 'system health policy definition modify' 명령을 사용하여 정책을 사용하지 않도록 설정할 수 있습니다.

상태 알림이 **AutoSupport** 메시지 및 이벤트를 트리거하는 방식

시스템 상태 알림은 EMS(이벤트 관리 시스템)에서 AutoSupport 메시지 및 이벤트를 트리거하여, 상태 모니터링 시스템을 직접 사용하는 것 외에도 AutoSupport 메시지 및 EMS를 사용하여 시스템의 상태를 모니터링할 수 있습니다.

경고 후 5분 내에 AutoSupport 메시지가 전송됩니다. AutoSupport 메시지에는 이전 AutoSupport 메시지 이후에 생성된 모든 경고가 포함됩니다. 단, 이전 주 내에 동일한 리소스 및 가능한 원인에 대한 경고를 복제하는 알림은 제외됩니다.

일부 알림은 AutoSupport 메시지를 트리거하지 않습니다. 상태 정책에서 AutoSupport 메시지 전송을 사용하지 않도록 설정한 경우 알림은 AutoSupport 메시지를 트리거하지 않습니다. 예를 들어, 상태 정책은 기본적으로 AutoSupport 메시지를 사용하지 않도록 설정할 수 있습니다. 이 경우 문제가 발생할 때 AutoSupport에서 이미 메시지를 생성하므로 'system health policy definition modify' 명령을 사용하여 AutoSupport 메시지를 트리거하지 않도록 정책을 구성할 수 있습니다.

'system health AutoSupport trigger history show' 명령어를 사용해 지난 주에 보낸 모든 경고 트리거 AutoSupport 메시지의 목록을 볼 수 있다.

또한 알림은 EMS에 대한 이벤트 생성을 트리거합니다. 알림은 알림이 생성될 때마다 그리고 경고가 삭제될 때마다 생성됩니다.

사용 가능한 클러스터 상태 모니터

클러스터의 여러 부분을 모니터링하는 상태 모니터가 여러 개 있습니다. 상태 모니터는 이벤트를 감지하고, 사용자에게 경고를 보내고, 이벤트를 삭제하여 ONTAP 시스템 내의 오류를 복구할 수 있도록 도와줍니다.

상태 모니터 이름(식별자)	하위 시스템 이름(식별자)	목적
클러스터 스위치(클러스터 스위치)	스위치(스위치 - 상태)	클러스터 네트워크 스위치 및 관리 네트워크 스위치에서 온도, 사용률, 인터페이스 구성, 이중화(클러스터 네트워크 스위치만 해당) 및 팬 및 전원 공급 장치 작동을 모니터링합니다. 클러스터 스위치 상태 모니터는 SNMP를 통해 스위치와 통신합니다. SNMPv2c가 기본 설정입니다. ONTAP 9.2부터는 이 모니터가 마지막 폴링 기간 이후 클러스터 스위치가 재부팅된 경우를 감지하여 보고할 수 있습니다.
MetroCluster 패브릭	스위치	MetroCluster 구성 백엔드 Fabric 토폴로지를 모니터링하고 잘못된 케이블 연결 및 조닝, ISL 장애 등의 잘못된 구성을 감지합니다.
MetroCluster 상태	상호 연결, RAID 및 스토리지	FC-VI 어댑터, FC 이니시에이터 어댑터, 좌측 애그리게이트 및 디스크, 클러스터 간 포트를 모니터링합니다
노드 연결(노드 연결)	CIFS 무중단 운영(CIFS-NDO)	SMB 연결을 모니터링하여 Hyper-V 애플리케이션의 무중단 운영을 지원합니다.
스토리지(SAS-connect)	노드 레벨에서 쉘프, 디스크, 어댑터를 모니터링하여 적절한 경로와 연결을 설정합니다.	시스템
해당 없음	다른 상태 모니터의 정보를 집계합니다.	시스템 연결(시스템 연결)

시스템 상태 알림을 자동으로 받습니다

'system health alert show' 명령을 사용하여 시스템 상태 경고를 수동으로 볼 수 있습니다. 그러나 상태 모니터에서 알림을 생성할 때 알림을 자동으로 수신하려면 특정 EMS(이벤트 관리 시스템) 메시지에 가입해야 합니다.

이 작업에 대해

다음 절차에서는 모든 HM.ALERT.Raised 메시지 및 모든 HM.ALERT.clLEALEed 메시지에 대한 알림을 설정하는 방법을 보여 줍니다.

모든 HM.ALERT.Raised 메시지 및 모든 HM.ALERT.ALLEALEAN 메시지에는 SNMP 트랩이 포함됩니다. SNMP 트랩의 이름은 HealthMonitorAlertRaised와 HealthMonitorAlertCleared입니다. SNMP 트랩에 대한 자세한 내용은 _Network Management Guide_를 참조하십시오.

단계

1. 이벤트 목적지 작성 명령을 사용하여 EMS 메시지를 보낼 대상을 정의합니다.

```
cluster1::> event destination create -name health_alerts -mail
admin@example.com
```

2. event route add-destinations 명령을 사용하여 hm.alert.Raised 메시지와 hm.alert.clined 메시지를 목적지로 라우트한다.

```
cluster1::> event route add-destinations -messagename hm.alert*
-destinations health_alerts
```

관련 정보

"네트워크 관리"

저하된 시스템 상태에 응답합니다

시스템 상태가 성능 저하 상태일 때 경고를 표시하고 가능한 원인 및 수정 조치를 읽으면서 저하된 서브시스템에 대한 정보를 표시하고 문제를 해결할 수 있습니다. 억제된 알림도 표시되어 이를 수정하고 확인되었는지 확인할 수 있습니다.

이 작업에 대해

AutoSupport 메시지 또는 EMS 이벤트를 보거나 '시스템 상태' 명령을 사용하여 알림이 생성되었는지 확인할 수 있습니다.

단계

1. 'system health alert show' 명령을 사용하면 시스템 상태를 훼손하는 경고를 볼 수 있습니다.
2. 경고의 가능한 원인, 가능한 영향 및 수정 조치를 읽고 문제를 해결할 수 있는지 또는 추가 정보가 필요한지 확인하십시오.
3. 자세한 정보가 필요하면 'system health alert show-instance' 명령을 사용하여 경고에 사용할 수 있는 추가 정보를 확인하십시오.
4. '-ACKNOWLEDGE' 매개 변수와 함께 'system health alert modify' 명령을 사용하여 특정 경고를 작업 중임을 나타냅니다.
5. 경고의 "수정 조치" 필드에 설명된 대로 문제를 해결하기 위해 수정 조치를 취합니다.

   수정 조치에는 시스템 재부팅이 포함될 수 있습니다.

   문제가 해결되면 경고가 자동으로 지워집니다. 하위 시스템에 다른 경고가 없으면 하위 시스템의 상태가 'OK'로 바뀝니다. 모든 서브시스템의 상태가 정상이면 전체 시스템 상태가 정상(OK)으로 바뀝니다.

6. 'system status show' 명령을 사용하여 시스템 상태가 'OK'인지 확인합니다.

   시스템 상태가 '정상'이 아닌 경우 이 절차를 반복합니다.

저하된 시스템 상태에 응답하는 예

노드에 대한 경로가 2개인 셸프로 인해 성능이 저하된 시스템 상태의 특정 예를 검토하여 경고에 응답할 때 CLI가 표시되는 내용을 볼 수 있습니다.

ONTAP를 시작한 후 시스템 상태를 확인하고 성능이 저하되었습니다.

```
      cluster1::>system health status show
        Status
        ---------------
        degraded
```

경고를 표시하여 문제가 발생한 위치를 확인하고 쉘프 2에서 노드 1에 대한 경로가 2개 있지 않음을 확인할 수 있습니다.

```
      cluster1::>system health alert show
               Node: node1
           Resource: Shelf ID 2
           Severity: Major
       Indication Time: Mon Nov 10 16:48:12 2013
     Probable Cause: Disk shelf 2 does not have two paths to controller
                     node1.
    Possible Effect: Access to disk shelf 2 via controller node1 will be
                     lost with a single hardware component failure (e.g.
                     cable, HBA, or IOM failure).
 Corrective Actions: 1. Halt controller node1 and all controllers attached
to disk shelf 2.
                     2. Connect disk shelf 2 to controller node1 via two
paths following the rules in the Universal SAS and ACP Cabling Guide.
                     3. Reboot the halted controllers.
                     4. Contact support personnel if the alert persists.
```

경고 ID를 비롯한 추가 정보를 얻기 위해 알림에 대한 세부 정보를 표시합니다.

```
      cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
                  Node: node1
               Monitor: node-connect
              Alert ID: DualPathToDiskShelf_Alert
     Alerting Resource: 50:05:0c:c1:02:00:0f:02
             Subsystem: SAS-connect
       Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
        Probable Cause: Connection_establishment_error
           Description: Disk shelf 2 does not have two paths to controller
node1.
    Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert
persists.
       Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
 hardware component failure (e.g. cable, HBA, or IOM failure).
           Acknowledge: false
              Suppress: false
                Policy: DualPathToDiskShelf_Policy
          Acknowledger: -
            Suppressor: -
Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
Alerting Resource Name: Shelf ID 2
```

이 알림은 작업 중임을 나타냅니다.

```
      cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true
```

쉘프 2와 노드 1 사이의 케이블 연결을 수정한 다음 시스템을 재부팅합니다. 그런 다음 시스템 상태를 다시 확인하고 상태가 "OK"인지 확인합니다.

```
cluster1::>system health status show
  Status
  ---------------
  OK
```

클러스터 및 관리 네트워크 스위치 검색을 구성합니다

클러스터 스위치 상태 모니터는 CDP(Cisco Discovery Protocol)를 사용하여 클러스터 및 관리 네트워크 스위치를 자동으로 검색합니다. 스위치를 자동으로 검색할 수 없거나 자동 검색에 CDP를 사용하지 않으려는 경우 상태 모니터를 구성해야 합니다.

이 작업에 대해

'system cluster-switch show' 명령은 상태 모니터가 검색한 스위치를 나열합니다. 목록에 표시할 스위치가 없는 경우 상태 모니터에서 스위치를 자동으로 검색할 수 없습니다.

단계

1. 자동 검색에 CDP를 사용하려면 다음을 수행합니다.

   a. 스위치에서 CDP(Cisco Discovery Protocol)가 활성화되어 있는지 확인합니다.

      자세한 내용은 스위치 설명서를 참조하십시오.

   b. 클러스터의 각 노드에서 다음 명령을 실행하여 CDP가 설정되어 있는지 여부를 확인합니다.

      '* run-node_node_name_ - 명령 옵션 CDPD.enable *

      CDP가 활성화된 경우 d 단계로 이동합니다 CDP가 비활성화되어 있으면 c 단계로 이동합니다

   c. CDP를 사용하도록 설정하려면 다음 명령을 실행합니다.

      ' * run-node_node_name_ - 명령 옵션 CDPD.enable on * '

   5분 정도 기다린 후 다음 단계로 이동합니다.

   a. 'system cluster-switch show' 명령을 사용하여 ONTAP가 이제 스위치를 자동으로 검색할 수 있는지 확인합니다.

2. 상태 모니터가 스위치를 자동으로 검색할 수 없는 경우 'system cluster-switch create' 명령을 사용하여 스위치 검색을 구성합니다.

   ```
   cluster1::> system cluster-switch create -device switch1 -address
   192.0.2.250 -snmp-version SNMPv2c -community cshm1! -model NX5020 -type
   cluster-network
   ```

   5분 정도 기다린 후 다음 단계로 이동합니다.

3. 'system cluster-switch show' 명령을 사용하여 ONTAP에서 정보를 추가한 스위치를 검색할 수 있는지

확인합니다.

작업을 마친 후

상태 모니터에서 스위치를 모니터링할 수 있는지 확인합니다.

클러스터 및 관리 네트워크 스위치의 모니터링을 확인합니다

클러스터 스위치 상태 모니터는 검색된 스위치를 자동으로 모니터링하지만 스위치가 올바르게 구성되지 않은 경우 모니터링이 자동으로 실행되지 않을 수 있습니다. 스위치를 모니터링하도록 상태 모니터가 올바르게 구성되어 있는지 확인해야 합니다.

단계

1. 클러스터 스위치 상태 모니터에서 검색한 스위치를 식별하려면 다음 명령을 입력합니다.

   ONTAP 9.8 이상

   '시스템 스위치 이더넷 쇼

   ONTAP 9.7 이하

   'system cluster-switch show'

   Model 열에 Other 값이 표시되면 ONTAP에서 스위치를 모니터링할 수 없습니다. ONTAP에서 자동으로 검색하는 스위치가 상태 모니터링을 지원하지 않는 경우 이 값을 '기타'로 설정합니다.

   ⓘ 스위치가 명령 출력에 표시되지 않으면 스위치 검색을 구성해야 합니다.

2. 지원되는 최신 스위치 소프트웨어로 업그레이드하고 NetApp Support 사이트에서 RCF(구성 파일)를 참조합니다.

   "NetApp 지원 다운로드 페이지"

   스위치의 RCF에 있는 커뮤니티 문자열은 상태 모니터가 사용하도록 구성된 커뮤니티 문자열과 일치해야 합니다. 기본적으로 상태 모니터는 커뮤니티 문자열 "cshm1!"를 사용합니다.

   ⓘ 현재 상태 모니터는 SNMPv2만 지원합니다.

   클러스터에서 모니터링하는 스위치에 대한 정보를 변경해야 하는 경우 다음 명령을 사용하여 상태 모니터에서 사용하는 커뮤니티 문자열을 수정할 수 있습니다.

   ONTAP 9.8 이상

   '시스템 스위치 이더넷 수정

   ONTAP 9.7 이하

   '시스템 클러스터 스위치 수정

3. 스위치의 관리 포트가 관리 네트워크에 연결되어 있는지 확인합니다.

SNMP 쿼리를 수행하려면 이 연결이 필요합니다.

시스템 상태를 모니터링하는 명령입니다

시스템 상태 명령을 사용하여 시스템 리소스 상태에 대한 정보를 표시하고, 알림에 응답하고, 향후 경고를 구성할 수 있습니다. CLI 명령을 사용하면 상태 모니터링 구성 방법에 대한 자세한 정보를 볼 수 있습니다. 명령에 대한 man 페이지에는 자세한 정보가 포함되어 있습니다.

시스템 상태의 상태를 표시합니다

원하는 작업	이 명령 사용...
개별 상태 모니터의 전체 상태를 반영하는 시스템의 상태를 표시합니다	'시스템 상태 표시
상태 모니터링을 사용할 수 있는 서브시스템의 상태를 표시합니다	시스템 상태 하위 시스템이 표시됩니다

노드 접속 상태를 표시합니다

원하는 작업	이 명령 사용...
포트 정보, HBA 포트 속도, I/O 처리량, 초당 I/O 작업 속도 등 노드에서 스토리지 셸프로의 접속에 대한 세부 정보를 표시합니다	'Storage shelf show-connectivity '-instance' 매개 변수를 사용하여 각 쉘프에 대한 자세한 정보를 표시합니다.
사용 가능한 공간, 쉘프 및 베이 번호, 소유 노드 이름 등의 드라이브 및 어레이 LUN에 대한 정보를 표시합니다	스토리지 디스크 쇼 각 드라이브에 대한 자세한 정보를 표시하려면 '-instance' 매개 변수를 사용하십시오.
포트 유형, 속도 및 상태를 포함한 스토리지 쉘프 포트에 대한 자세한 정보를 표시합니다	'Storage port show' 각 어댑터에 대한 자세한 정보를 표시하려면 '-instance' 매개 변수를 사용하십시오.

클러스터, 스토리지 및 관리 네트워크 스위치의 검색 관리

원하는 작업	이 명령을 사용합니다. **(ONTAP 9.8 이상)**	이 명령을 사용합니다. **(ONTAP 9.7 이하)**
클러스터에서 모니터링하는 스위치를 표시합니다	'시스템 스위치 이더넷 쇼	'system cluster-switch show'

원하는 작업	이 명령을 사용합니다. **(ONTAP 9.8 이상)**	이 명령을 사용합니다. **(ONTAP 9.7 이하)**
명령 출력의 Reason 열에 표시된 스위치를 비롯하여 클러스터에서 현재 모니터링하는 스위치와 클러스터 및 관리 네트워크 스위치에 대한 네트워크 액세스에 필요한 구성 정보를 표시합니다. 이 명령은 고급 권한 수준에서 사용할 수 있습니다.	'시스템 스위치 이더넷 show-all'	'system cluster-switch show-all'
검색되지 않은 스위치의 검색을 구성합니다	'시스템 스위치 이더넷 생성	'system cluster-switch create
클러스터에서 모니터링하는 스위치에 대한 정보 수정(예: 장치 이름, IP 주소, SNMP 버전 및 커뮤니티 문자열)	'시스템 스위치 이더넷 수정	'시스템 클러스터 스위치 수정
스위치 모니터링을 비활성화합니다	'시스템 스위치 이더넷 수정-비활성화-모니터링	'system cluster-switch modify-disable-monitoring
스위치 검색 및 모니터링을 비활성화하고 스위치 구성 정보를 삭제합니다	'시스템 스위치 이더넷 삭제	'system cluster-switch delete
데이터베이스에 저장된 스위치 구성 정보를 영구적으로 제거합니다(이렇게 하면 스위치의 자동 검색이 다시 활성화됩니다).	'시스템 스위치 이더넷 삭제-강제	'system cluster-switch delete-force'를 선택합니다
AutoSupport 메시지와 함께 보내려면 자동 로깅을 활성화합니다.	'시스템 스위치 이더넷 로그	'시스템 클러스터-스위치 로그

생성된 알림에 응답합니다

원하는 작업	이 명령 사용...
알림이 트리거된 리소스 및 노드, 알림의 심각도 및 추정 원인과 같이 생성된 알림에 대한 정보를 표시합니다	'시스템 상태 경고 표시
생성된 각 알림에 대한 정보를 표시합니다	'시스템 상태 경고 표시 - 인스턴스'
다른 사용자가 알림을 작업 중임을 나타냅니다	시스템 상태 알림 수정
알림을 확인합니다	'시스템 상태 경고 수정 - 확인'

원하는 작업	이 명령 사용...
하위 시스템의 상태에 영향을 주지 않도록 후속 경고를 표시하지 않습니다	'시스템 상태 경고 수정 - 억제'
자동으로 지워지지 않은 알림을 삭제합니다	'시스템 상태 경고 삭제
예를 들어, 알림이 AutoSupport 메시지를 트리거했는지 여부와 같이 지난 주 내에 트리거된 알림을 표시하는 AutoSupport 메시지에 대한 정보를 표시합니다	'시스템 상태 AutoSupport 트리거 기록 표시

향후 알림을 구성합니다

원하는 작업	이 명령 사용...
특정 리소스 상태가 특정 경고를 발생시키는지 여부를 제어하는 정책을 사용하거나 사용하지 않도록 설정합니다	'시스템 상태 정책 정의 수정

상태 모니터링 구성 방법에 대한 정보를 표시합니다

원하는 작업	이 명령 사용...
노드, 이름, 하위 시스템 및 상태와 같은 상태 모니터에 대한 정보를 표시합니다	'시스템 상태 구성 쇼' 각 상태 모니터에 대한 세부 정보를 표시하려면 '-instance' 매개 변수를 사용합니다.
상태 모니터에서 잠재적으로 생성할 수 있는 알림에 대한 정보를 표시합니다	시스템 상태 경고 정의가 표시됩니다 각 경고 정의에 대한 자세한 정보를 표시하려면 '-instance' 매개 변수를 사용합니다.
알림이 발생하는 시기를 결정하는 상태 모니터링 정책에 대한 정보를 표시합니다	시스템 상태 정책 정의가 표시됩니다 각 정책에 대한 세부 정보를 표시하려면 '-instance' 매개 변수를 사용합니다. 다른 매개 변수를 사용하여 알림 목록을 정책 상태(사용 여부), 상태 모니터, 알림 등으로 필터링할 수 있습니다.

환경 정보를 표시합니다

센서를 통해 시스템의 환경 구성요소를 모니터링할 수 있습니다. 환경 센서에 대해 표시할 수 있는 정보에는 유형, 이름, 상태, 값 및 임계값 경고가 포함됩니다.

단계

1. 환경 센서에 대한 정보를 표시하려면 'system node environment sensors show' 명령을 사용합니다.

파일 시스템 분석

파일 시스템 분석 개요

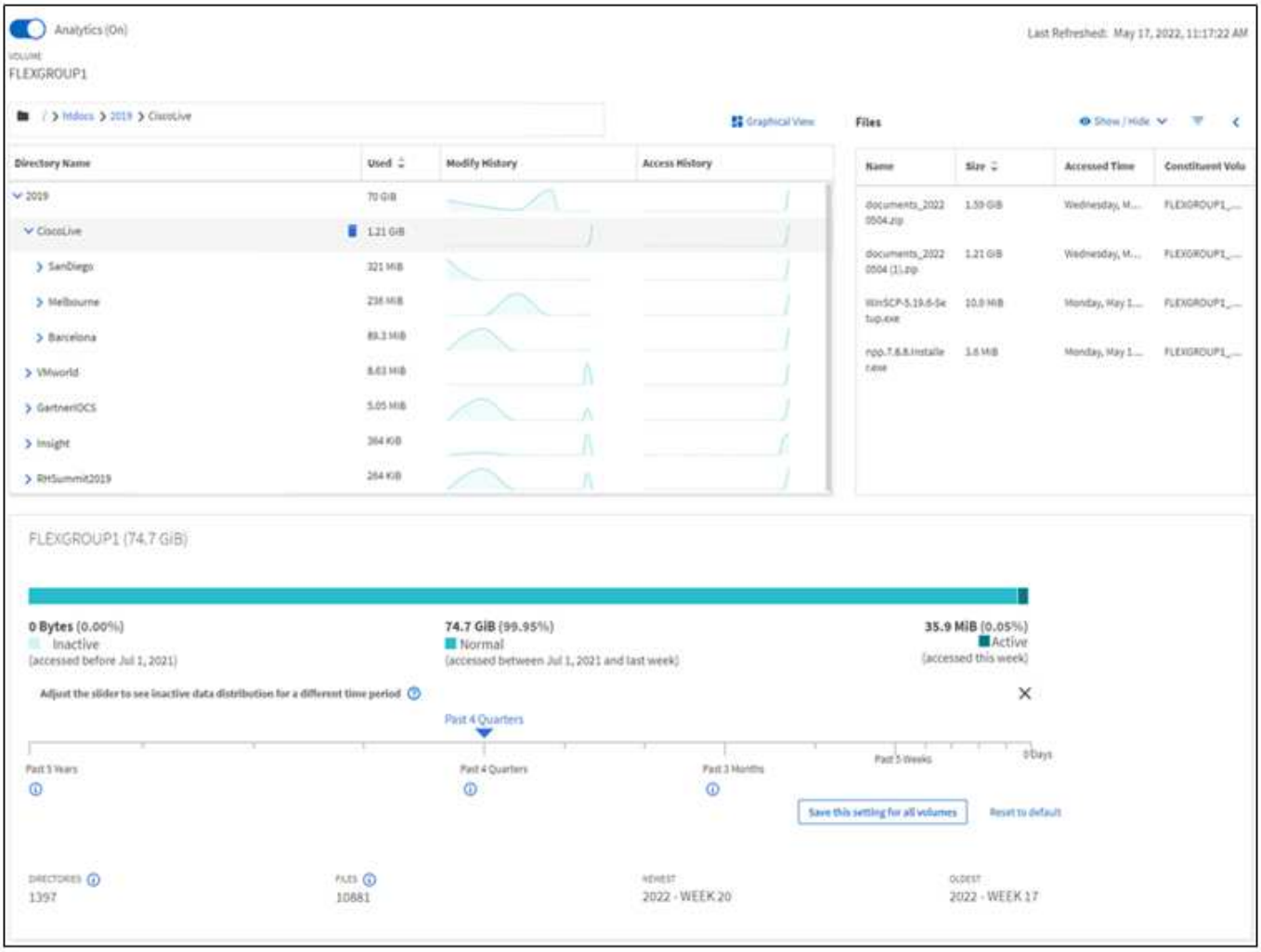
ONTAP 9.8에서 파일 시스템 분석(FSA)이 처음 도입되어 ONTAP FlexGroup 또는 FlexVol 볼륨 내의 파일 사용 및 스토리지 용량 추세를 실시간으로 파악할 수 있게 되었습니다. 이 기본 기능을 사용하면 외부 툴이 필요하지 않으며 스토리지 활용 방법과 비즈니스 요구 사항에 맞게 스토리지를 최적화할 수 있는 기회가 있는지 여부에 대한 주요 통찰력을 얻을 수 있습니다.

FSA를 사용하면 NAS에 있는 볼륨의 파일 시스템 계층 구조의 모든 수준에 대한 가시성을 확보할 수 있습니다. 예를 들어, SVM(Storage VM), 볼륨, 디렉토리, 파일 레벨에서 사용량 및 용량 인사이트를 얻을 수 있습니다. FSA를 사용하여 다음과 같은 질문에 답할 수 있습니다.

- 내 저장소를 채우는 것은 무엇이며, 다른 저장 위치로 이동할 수 있는 대용량 파일이 있습니까?
- 가장 활성화된 볼륨, 디렉토리 및 파일은 무엇입니까? 스토리지 성능이 사용자의 요구사항에 최적화되어 있습니까?
- 지난 달에 추가된 데이터의 양은 어느 정도입니까?
- 가장 활동적이거나 활동이 적은 스토리지 사용자는 누구입니까?
- 기본 스토리지에 얼마나 비활성 또는 휴면 데이터가 있습니까? 해당 데이터를 저비용 콜드 계층으로 이동할 수 있습니까?
- 계획된 서비스 품질 변경이 자주 액세스하는 중요한 파일에 대한 액세스에 부정적인 영향을 미칩니까?

파일 시스템 분석은 ONTAP 시스템 관리자에 통합됩니다. System Manager 내에서 제공되는 뷰:

- 실시간 가시성을 통해 데이터를 효과적으로 관리하고 운영할 수 있습니다
- 실시간 데이터 수집 및 집계
- 관련 성능 프로파일과 함께 하위 디렉토리와 파일 크기 및 개수를 계산합니다
- 수정 및 액세스 기록을 위한 파일 에이지 히스토그램



지원되는 볼륨 유형

파일 시스템 분석은 FlexCache 캐시 및 SnapMirror 대상 볼륨을 제외하고 활성 NAS 데이터가 있는 볼륨에 대한 가시성을 제공하도록 설계되었습니다.

파일 시스템 분석 기능 가용성

각 ONTAP 릴리즈는 파일 시스템 분석 범위를 확장합니다.

	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.8
System Manager의 시각화	✓	✓	✓	✓	✓	✓	✓	✓
용량 분석	✓	✓	✓	✓	✓	✓	✓	✓
비활성 데이터 정보	✓	✓	✓	✓	✓	✓	✓	✓
Data ONTAP 7-Mode에서 전환된 볼륨 지원	✓	✓	✓	✓	✓	✓	✓	
System Manager에서 비활성 기간을 사용자 지정할 수 있습니다	✓	✓	✓	✓	✓	✓	✓	

	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.8
볼륨 레벨 활동 추적	✓	✓	✓	✓	✓	✓		
활동 추적 데이터를 CSV로 다운로드합니다	✓	✓	✓	✓	✓	✓		
SVM 레벨의 활동 추적 을 참조하십시오	✓	✓	✓	✓	✓			
타임라인	✓	✓	✓	✓	✓			
사용 분석	✓	✓	✓	✓				
File System Analytics를 기본적으로 설정하는 옵션입니다	✓	✓	✓					
초기화 스캔 진행 모니터	✓	✓						

파일 시스템 분석에 대해 자세히 알아보십시오

추가 참고 자료

- "TR 4687: ONTAP 파일 시스템 분석에 대한 모범 사례 지침"
- "기술 자료: NetApp ONTAP 파일 시스템 분석을 켠 후 지연 시간이 길거나 변동이 심한 경우"

파일 시스템 분석 설정

용량 분석과 같은 사용 데이터를 수집하고 표시하려면 볼륨에 대해 File System Analytics를 활성화해야 합니다.

이 작업에 대해

- ONTAP 9.8부터 새 볼륨이나 기존 볼륨에서 파일 시스템 분석을 활성화할 수 있습니다. 시스템을 ONTAP 9.8 이상으로 업그레이드하는 경우 파일 시스템 분석을 활성화하기 전에 모든 업그레이드 프로세스가 완료되었는지 확인하십시오.
- 분석을 지원하는 데 걸리는 시간은 볼륨의 크기와 콘텐츠에 따라 다릅니다. System Manager에서 진행 상황을 표시하고 완료되면 분석 데이터를 표시합니다. 초기화 스캔 진행률에 대한 보다 정확한 정보가 필요한 경우 ONTAP CLI 명령을 사용할 수 있습니다 `volume analytics show`.
  - ONTAP 9.14.1부터 ONTAP는 스캔 진행률에 영향을 주는 임계치 조절 이벤트에 대한 알림과 더불어 초기화 스캔에 대한 진행률 추적을 제공합니다.
  - ONTAP 9.15.1부터 한 노드에서 4개의 초기화 스캔만 동시에 수행할 수 있습니다. 새 스캔을 시작하기 전에 스캔이 완료될 때까지 기다려야 합니다. 또한 ONTAP는 볼륨에 사용 가능한 공간이 충분한지 확인하고, 없는 경우 오류 메시지를 표시합니다. 볼륨의 사용 가능한 공간의 최소 5 ~ 8%가 사용 가능한지 확인합니다. 볼륨에 자동 크기 조정이 활성화되어 있는 경우 최대 자동 확장 크기를 기준으로 사용 가능한 크기를 계산합니다.
  - 초기화 스캔과 관련된 추가 고려 사항은 를 참조하십시오 스캔 고려 사항.

기존 볼륨에서 파일 시스템 분석을 활성화합니다

ONTAP System Manager 또는 CLI를 사용하여 파일 시스템 분석을 활성화할 수 있습니다.

예 **2.** 단계

시스템 관리자

ONTAP 9.8 및 **9.9.1**	**ONTAP 9.10.1**에서 시작합니다
스토리지 > 볼륨 * 을 선택합니다. 원하는 볼륨을 선택한 다음 * 탐색기 * 를 선택합니다. 분석 활성화 * 또는 * 분석 비활성화 * 를 선택합니다.	스토리지 > 볼륨 * 을 선택합니다. 원하는 볼륨을 선택합니다. 개별 볼륨 메뉴에서 * 파일 시스템 > 탐색기 * 를 선택합니다. 분석 활성화 * 또는 * 분석 비활성화 * 를 선택합니다.

CLI를 참조하십시오

CLI를 사용하여 **File System Analytics**를 설정합니다

1. 다음 명령을 실행합니다. 'volume analytics on-vserver_svm_name_-volume_volume_name_[-foreground{true|false}]' 명령은 기본적으로 포그라운드에서 실행되며, ONTAP는 진행률을 표시하고 완료되면 분석 데이터를 표시합니다. 보다 정확한 정보가 필요한 경우 '-foreground false' 옵션을 사용하여 백그라운드에서 명령을 실행한 다음 'volume analytics show' 명령을 사용하여 CLI에서 초기화 진행률을 표시할 수 있습니다.
2. 파일 시스템 분석을 성공적으로 활성화한 후 System Manager 또는 ONTAP REST API를 사용하여 분석 데이터를 표시할 수 있습니다.

기본 파일 시스템 분석 설정을 수정합니다

ONTAP 9.13.1 부터는 SVM 또는 클러스터 설정을 수정하여 새 볼륨에서 파일 시스템 분석을 기본적으로 사용하도록 설정할 수 있습니다.

예 **3.** 단계

시스템 관리자

System Manager를 사용하는 경우, 기본적으로 볼륨 생성 시 용량 분석 및 활동 추적을 사용하도록 스토리지 VM 또는 클러스터 설정을 수정할 수 있습니다. 기본 활성화는 기존 볼륨이 아니라 설정을 수정한 후에만 생성된 볼륨에만 적용됩니다.

클러스터에서 파일 시스템 분석 설정을 수정합니다

1. System Manager에서 클러스터 설정으로 이동합니다.
2. Cluster settings** 에서 File System Settings 탭을 검토합니다. 설정을 수정하려면 ⚙ 아이콘을 선택합니다.
3. [활동 추적**] 필드에 기본적으로 활동 추적을 활성화할 SVM의 이름을 입력합니다. 필드를 비워 두면 모든 SVM에서 활동 추적이 비활성화됩니다.

   새 스토리지 VM에서 기본적으로 활성 추적을 해제하려면 새 스토리지 **VM**에서 활성화 상자의 선택을 취소합니다.

4. 분석** 필드에 용량 분석을 기본적으로 활성화할 스토리지 VM의 이름을 입력합니다. 필드를 비워 두면 모든 SVM에서 용량 분석이 비활성화됩니다.

   새 스토리지 VM에서 기본적으로 용량 분석을 사용하지 않도록 설정하려면 **Enable on new storage VMs** 확인란의 선택을 취소합니다.

5. 저장을 선택합니다.

SVM에서 파일 시스템 분석 설정을 수정합니다

1. 수정할 SVM을 선택한 다음 스토리지 **VM** 설정을 선택합니다.
2. **File System Analytics** 카드에서 토글을 사용하여 스토리지 VM의 모든 새 볼륨에 대한 활동 추적 및 용량 분석을 활성화 또는 비활성화합니다.

CLI를 참조하십시오

ONTAP CLI를 사용하여 새 볼륨에서 파일 시스템 분석을 기본적으로 사용하도록 스토리지 VM을 구성할 수 있습니다.

SVM에서 기본적으로 파일 시스템 분석 지원

1. 새로 생성된 모든 볼륨에서 용량 분석 및 활동 추적을 기본적으로 사용하도록 SVM 수정:
   `vserver modify -vserver` *`svm_name`* `-auto-enable-activity-tracking true -auto -enable-analytics true`

파일 시스템 작업을 봅니다

FSA(File System Analytics)를 활성화한 후 선택한 볼륨의 루트 디렉토리 컨텐츠를 각 하위 트리에 사용된 공간으로 정렬할 수 있습니다.

파일 시스템 객체를 선택하여 파일 시스템을 탐색하고 디렉토리의 각 객체에 대한 세부 정보를 표시합니다. 디렉토리에 대한 정보도 그래픽으로 표시할 수 있습니다. 시간이 지남에 따라 각 하위 트리에 대한 기록 데이터가 표시됩니다. 사용된 공간은 3000 개가 넘는 디렉토리가 있는 경우 정렬되지 않습니다.

탐색기

파일 시스템 분석 * 탐색기 * 화면은 다음 세 가지 영역으로 구성됩니다.

- 디렉터리 및 하위 디렉터리의 트리 보기; 이름, 크기, 수정 기록 및 액세스 기록을 표시하는 확장 가능한 목록.
- 디렉토리 목록에서 선택한 객체에 대한 이름, 크기 및 액세스 시간을 표시하는 파일.
- 디렉토리 목록에서 선택한 객체에 대한 활성 및 비활성 데이터 비교

  ONTAP 9.9.1부터 보고할 범위를 사용자 지정할 수 있습니다. 기본값은 1년입니다. 이러한 사용자 지정을 기반으로 볼륨 이동 및 계층화 정책 수정 등의 수정 조치를 수행할 수 있습니다.

액세스 시간은 기본적으로 표시됩니다. 그러나 볼륨 기본값이 CLI에서 변경된 경우('볼륨 수정' 명령으로 '-atime-update' 옵션을 'false'로 설정) 마지막으로 수정한 시간만 표시됩니다. 예를 들면 다음과 같습니다.

- 트리 보기에는 * 액세스 기록 * 이 표시되지 않습니다.
- 파일 보기가 변경됩니다.
- 활성/비활성 데이터 뷰는 수정된 시간('시간')을 기준으로 합니다.

이러한 디스플레이를 사용하여 다음을 검사할 수 있습니다.

- 파일 시스템 위치는 공간을 가장 많이 소모합니다
- 디렉토리 및 하위 디렉토리 내의 파일 및 하위 디렉토리 수를 비롯한 디렉토리 트리에 대한 자세한 정보
- 이전 데이터가 포함된 파일 시스템 위치(예: 스크래치, 임시 또는 로그 트리)

FSA 출력을 해석할 때는 다음 사항을 염두에 두십시오.

- FSA는 데이터가 처리되는 양이 아니라 데이터의 사용 위치 및 시기를 보여 줍니다. 예를 들어, 최근에 액세스하거나 수정한 파일에 의한 대규모 공간 소비는 시스템 처리 부하가 높음을 나타내는 것은 아닙니다.
- Volume Explorer * 탭에서 FSA의 공간 소비를 계산하는 방식은 다른 도구와 다를 수 있습니다. 특히 볼륨에 스토리지 효율성 기능이 활성화되어 있는 경우 * 볼륨 개요 * 에 보고된 소비량과 비교하여 큰 차이가 있을 수 있습니다. 이는 * Volume Explorer * 탭에 효율성 절약 효과가 포함되지 않기 때문입니다.
- 디렉토리 표시의 공간 제한으로 인해 _List View_에서 8개 수준 이상의 디렉토리 깊이를 볼 수 없습니다. 8개 수준 이상의 디렉토리를 보려면 _Graphical View_로 전환하고 원하는 디렉토리를 찾은 다음 _List View_로 다시 전환해야 합니다. 그러면 디스플레이에 추가 화면 공간이 허용됩니다.

단계

1. 선택한 볼륨의 루트 디렉토리 컨텐츠를 봅니다.

ONTAP 9.8 및 **9.9.1**	**ONTAP 9.10.1**에서 시작합니다
Storage > Volumes * 를 클릭하고 원하는 볼륨을 선택한 다음 * Explorer * 를 클릭합니다.	Storage > Volumes * 를 선택하고 원하는 볼륨을 선택합니다. 개별 볼륨 메뉴에서 * 파일 시스템 > 탐색기 * 를 선택합니다.

활동 추적을 활성화합니다

ONTAP 9.10.1부터 파일 시스템 분석에는 핫 객체를 식별하고 데이터를 CSV 파일로

다운로드할 수 있는 활동 추적 기능이 포함되어 있습니다. ONTAP 9.11.1부터 활동 추적 기능이 SVM 범위로 확장됩니다. 또한 ONTAP 9.11.1부터 System Manager에서 활동 추적 타임라인을 제공하므로 활동 추적 데이터를 최대 5분 동안 살펴볼 수 있습니다.

Activity Tracking(활동 추적)을 사용하면 다음 네 가지 범주로 모니터링할 수 있습니다.

- 디렉토리
- 파일
- 클라이언트
- 사용자

모니터링되는 각 범주에 대해 작업 추적은 읽기 IOPS, 쓰기 IOPS, 읽기 처리량 및 쓰기 처리량을 표시합니다. 작업 추적에 대한 쿼리는 이전 5초 간격 동안 시스템에 표시되는 핫 스팟과 관련하여 10-15초마다 새로 고쳐집니다.

활동 추적 정보는 근사치이며, 데이터의 정확도는 수신되는 I/O 트래픽의 분포에 따라 달라집니다.

System Manager의 볼륨 레벨에서 활동 추적을 보면 확장된 볼륨의 메뉴만 활발하게 새로 고쳐집니다. 볼륨 보기가 축소되면 볼륨 표시가 확장될 때까지 볼륨이 새로 고쳐지지 않습니다. 새로 고침 일시 중지 * 버튼을 사용하여 새로 고침을 중지할 수 있습니다. 활동 데이터는 선택한 볼륨에 대해 캡처된 모든 시점 데이터를 표시하는 CSV 형식으로 다운로드할 수 있습니다.

ONTAP 9.11.1부터 일정 기능을 사용할 수 있으므로 볼륨 또는 SVM에서 핫스팟 활동 기록을 유지하고 약 5초마다 지속적으로 업데이트하며 이전 5분 동안의 데이터를 유지할 수 있습니다. 시간 표시 막대 데이터는 페이지의 표시 영역에 있는 필드에만 유지됩니다. 시간 표시 막대가 표시되지 않도록 추적 범주를 축소하거나 스크롤하면 시간 표시 막대가 데이터 수집을 중지합니다. 기본적으로 타임라인은 비활성화되어 있으며 활동 탭에서 멀리 이동하면 자동으로 비활성화됩니다.

단일 볼륨에 대해 활동 추적을 활성화합니다

ONTAP 시스템 관리자 또는 CLI를 사용하여 활동 추적을 설정할 수 있습니다.

이 작업에 대해

ONTAP REST API 또는 시스템 관리자와 함께 RBAC를 사용하는 경우 활동 추적에 대한 액세스를 관리하기 위해 사용자 지정 역할을 만들어야 합니다. 을 참조하십시오 역할 기반 액세스 제어 참조하십시오.

시스템 관리자

단계

1. 스토리지 > 볼륨 * 을 선택합니다. 원하는 볼륨을 선택합니다. 개별 볼륨 메뉴에서 파일 시스템 을 선택한 다음 활동 탭을 선택합니다.
2. 상위 디렉토리, 파일, 클라이언트 및 사용자에 대한 개별 보고서를 보려면 * Activity Tracking * 이 켜져 있어야 합니다.
3. 새로 고침 없이 보다 깊이 있는 데이터를 분석하려면 * 새로 고침 일시 중지 * 를 선택합니다. 데이터를 다운로드하여 보고서의 CSV 레코드도 가질 수 있습니다.

CLI를 참조하십시오

단계

1. 활동 추적 활성화:

   ```
   volume activity-tracking on -vserver svm_name -volume volume_name
   ```

2. 다음 명령을 사용하여 볼륨에 대한 Activity Tracking 상태가 On 또는 Off 인지 확인합니다.

   ```
   volume activity-tracking show -vserver svm_name -volume volume_name -state
   ```

3. 활성화되면 ONTAP 시스템 관리자 또는 ONTAP REST API를 사용하여 활동 추적 데이터를 표시합니다.

여러 볼륨에 대해 활동 추적을 활성화합니다

System Manager 또는 CLI를 사용하여 여러 볼륨의 활동 추적을 설정할 수 있습니다.

이 작업에 대해

ONTAP REST API 또는 시스템 관리자와 함께 RBAC를 사용하는 경우 활동 추적에 대한 액세스를 관리하기 위해 사용자 지정 역할을 만들어야 합니다. 을 참조하십시오 역할 기반 액세스 제어 참조하십시오.

시스템 관리자

특정 볼륨에 대해 활성화합니다

1. 스토리지 > 볼륨 * 을 선택합니다. 원하는 볼륨을 선택합니다. 개별 볼륨 메뉴에서 파일 시스템 을 선택한 다음 활동 탭을 선택합니다.
2. 활동 추적을 활성화할 볼륨을 선택합니다. 볼륨 목록 상단에서 * 추가 옵션 * 버튼을 선택합니다. 작업 추적 활성화 * 를 선택합니다.
3. SVM 레벨에서 활동 추적을 보려면 * 스토리지 > 볼륨 * 에서 보려는 특정 SVM을 선택합니다. File System(파일 시스템) 탭, Activity(활동) 로 이동하면 Activity Tracking(활동 추적)이 활성화된 볼륨에 대한 데이터가 표시됩니다.

모든 볼륨에 대해 활성화

1. 스토리지 > 볼륨 * 을 선택합니다. 메뉴에서 SVM을 선택합니다.
2. File System * 탭으로 이동하고 * More * 탭을 선택하여 SVM의 모든 볼륨에서 활동 추적을 활성화합니다.

CLI를 참조하십시오

ONTAP 9.13.1 부터는 ONTAP CLI를 사용하여 여러 볼륨의 활동 추적을 활성화할 수 있습니다.

단계

1. 활동 추적 활성화:

   ```
   volume activity-tracking on -vserver svm_name -volume [*|!volume_names]
   ```

   사용 * 지정된 스토리지 VM의 모든 볼륨에 대해 작업 추적을 설정하려면 다음을 수행합니다.

   사용 ! 볼륨 이름 다음에 볼륨 이름을 사용하여 SVM의 모든 볼륨에서 활동 추적을 활성화합니다. 단, 볼륨 이름은 예외입니다.

2. 작업이 성공했는지 확인합니다.

   ```
   volume show -fields activity-tracking-state
   ```

3. 활성화되면 ONTAP 시스템 관리자 또는 ONTAP REST API를 사용하여 활동 추적 데이터를 표시합니다.

사용 분석 지원

ONTAP 9.12.1부터 사용 분석을 통해 볼륨 내에서 공간이 가장 많은 디렉토리를 볼 수 있습니다. 볼륨의 총 디렉토리 수 또는 볼륨의 총 파일 수를 볼 수 있습니다. 보고는 가장 많은 공간을 사용하는 25개 디렉토리로 제한됩니다.

대규모 디렉토리에 대한 분석 기능은 15분마다 업데이트됩니다. 페이지 맨 위에서 마지막으로 새로 고친 타임스탬프를 확인하여 가장 최근 새로 고침을 모니터링할 수 있습니다. 다운로드 단추를 클릭하여 Excel 통합 문서로 데이터를 다운로드할 수도 있습니다. 다운로드 작업은 백그라운드에서 실행되며 선택한 볼륨에 대해 가장 최근에 보고된 정보를 제공합니다. 검사가 결과 없이 반환되는 경우 볼륨이 온라인 상태인지 확인합니다. SnapRestore와 같은 이벤트로 인해 파일 시스템 분석 시 대규모 디렉토리 목록이 재구축됩니다.

단계

1. 스토리지 > 볼륨 * 을 선택합니다. 원하는 볼륨을 선택합니다.
2. 개별 볼륨 메뉴에서 * 파일 시스템 * 을 선택합니다. 그런 다음 * Usage * 탭을 선택합니다.
3. 분석 * 스위치를 전환하여 사용 분석을 활성화합니다.
4. System Manager는 크기가 가장 큰 디렉토리를 내림차순으로 식별하는 막대 그래프를 표시합니다.

> 최상위 디렉토리 목록이 수집되는 동안 ONTAP는 부분 데이터를 표시하거나 데이터를 전혀 표시하지 않을 수 있습니다. 스캔 진행 상황은 스캔 중에 표시되는 * Usage * (사용 *) 탭에 있을 수 있습니다.

특정 디렉토리에 대한 더 많은 통찰력을 얻을 수 있습니다 파일 시스템에 대한 작업을 봅니다.

분석을 기반으로 수정 조치 수행

ONTAP 9.9.1부터 파일 시스템 분석 디스플레이에서 직접 현재 데이터와 원하는 결과를 기반으로 수정 조치를 수행할 수 있습니다.

디렉토리 및 파일을 삭제합니다

탐색기 디스플레이에서 삭제할 디렉터리 또는 개별 파일을 선택할 수 있습니다. 디렉토리는 지연 시간이 짧은 빠른 디렉토리 삭제 기능으로 삭제됩니다. (빠른 디렉토리 삭제는 분석이 활성화되지 않은 ONTAP 9.9.1부터 사용할 수도 있습니다.)

단계

1. 스토리지 > 볼륨 * 을 클릭한 다음 * 탐색기 * 를 클릭합니다.

   파일 또는 폴더 위로 마우스를 가져가면 삭제 옵션이 나타납니다. 한 번에 하나의 개체만 삭제할 수 있습니다.

> 디렉토리와 파일이 삭제되면 새 스토리지 용량 값이 즉시 표시되지 않습니다.

스토리지 계층에서 미디어 비용을 할당하여 비활성 데이터 스토리지 위치의 비용을 비교합니다

미디어 비용은 스토리지 비용 평가를 기준으로 할당한 값이며, 선택한 통화는 GB당 통화입니다. 설정할 경우 System Manager에서 볼륨을 이동할 때 할당된 미디어 비용을 사용하여 예상 절감액을 투영합니다.

설정한 미디어 비용은 지속적이지 않으며 단일 브라우저 세션에만 설정할 수 있습니다.

단계

1. Storage > Tiers * 를 클릭한 다음 원하는 로컬 계층(집계) 타일에서 * Set Media Cost * 를 클릭합니다.

   비교를 활성화하려면 활성 계층과 비활성 계층을 선택해야 합니다.

2. 통화 유형 및 금액을 입력합니다.

   미디어 비용을 입력하거나 변경하면 모든 미디어 유형에 변경 사항이 적용됩니다.

스토리지 비용을 줄이기 위해 볼륨을 이동합니다

분석 표시 및 미디어 비용 비교를 기반으로, 볼륨을 로컬 계층의 저렴한 스토리지로 이동할 수 있습니다.

한 번에 하나의 볼륨만 비교 및 이동할 수 있습니다.

단계

1. 미디어 비용 표시를 활성화한 후 * Storage > Tiers * 를 클릭하고 * Volumes * 를 클릭합니다.
2. 볼륨에 대한 대상 옵션을 비교하려면 볼륨에 대해 를 ⋮ 클릭한 다음 * Move * 를 클릭합니다.
3. 대상 로컬 계층 선택 * 디스플레이에서 대상 계층을 선택하여 예상 비용 차이를 표시합니다.
4. 옵션을 비교한 후 원하는 계층을 선택하고 * Move * (이동 *)를 클릭합니다.

파일 시스템 분석을 통한 역할 기반 액세스 제어

ONTAP 9.12.1부터 ONTAP에는 라는 사전 정의된 역할 기반 액세스 제어(RBAC) 역할이 포함되어 있습니다 `admin-no-fsa`. 를 클릭합니다 `admin-no-fsa` 역할은 관리자 수준의 권한을 부여하지만 사용자가 와 관련된 작업을 수행할 수 없습니다 `files` ONTAP CLI, REST API 및 System Manager의 엔드포인트(예: 파일 시스템 분석)

에 대한 자세한 내용은 를 참조하십시오 `admin-no-fsa` 역할, 을 참조하십시오 클러스터 관리자를 위한 사전 정의된 역할.

ONTAP 9.12.1 이전 버전의 ONTAP를 사용하는 경우 파일 시스템 분석에 대한 액세스를 제어하는 전용 역할을 만들어야 합니다. ONTAP 9.12.1 이전의 ONTAP 버전에서는 ONTAP CLI 또는 ONTAP REST API를 통해 RBAC 권한을 구성해야 합니다.

시스템 관리자

ONTAP 9.12.1부터는 System Manager를 사용하여 파일 시스템 분석에 대한 RBAC 권한을 구성할 수 있습니다.

단계

1. 클러스터 > 설정 * 을 선택합니다. 보안 * 에서 * 사용자 및 역할 * 로 이동하고 를 선택합니다 →.
2. 역할 * 에서 을 + Add 선택합니다.
3. 역할의 이름을 지정하십시오. 역할 속성 에서 적절한 를 제공하여 사용자 역할에 대한 액세스 또는 제한을 구성합니다 "API 엔드포인트". File System Analytics 액세스 또는 제한을 구성하기 위한 기본 경로 및 보조 경로는 아래 표를 참조하십시오.

제한	기본 경로	보조 경로
볼륨의 활동 추적	`/api/storage/volumes`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
SVM에서 활동 추적	`/api/svm/svms`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
모든 파일 시스템 분석 작업	`/api/storage/volumes`	`/:uuid/files`

   을 사용할 수 있습니다 `/*/` 엔드포인트에서 모든 볼륨 또는 SVM에 대한 정책을 설정할 UUID가 아닌

   각 엔드포인트에 대한 액세스 권한을 선택합니다.

4. 저장 * 을 선택합니다.
5. 사용자 또는 사용자에게 역할을 할당하려면 을 참조하십시오 관리자 액세스 제어.

CLI를 참조하십시오

ONTAP 9.12.1 이전 버전의 ONTAP를 사용하는 경우 ONTAP CLI를 사용하여 사용자 지정 역할을 만듭니다.

단계

1. 모든 기능에 액세스할 수 있는 기본 역할을 만듭니다.

이 작업은 제한된 역할을 생성하기 전에 수행해야 하며, 해당 역할이 활동 추적에서만 제한적인지 확인해야 합니다.

'Security login role create-cmddirname default-access all-role StorageAdmin

2. 제한적인 역할 생성:

   보안 로그인 역할 create-cmddirname "volume file show-disk-usage" -access none-role StorageAdmin"

3. SVM의 웹 서비스에 액세스할 수 있는 역할 승인:

   - REST API 호출의 경우 'st'입니다
   - 암호 보호를 위한 보안
   - System Manager 액세스를 위한 sysmgr입니다

     'vserver services web access create-vserver_svm-name_-name rest-role StorageAdmin'

     'vserver services web access create-vserver_svm-name_-name security-role StorageAdmin'

   'vserver services web access create-vserver_svm-name_-name sysmgr-role StorageAdmin'

4. 사용자를 생성합니다.

   사용자에게 적용하려는 각 응용 프로그램에 대해 고유한 create 명령을 실행해야 합니다. 같은 사용자에 대해 여러 번 만들기 를 호출하면 해당 사용자에게 모든 응용 프로그램이 적용되고 매번 새 사용자가 작성되지는 않습니다. 애플리케이션 유형에 대한 http 파라미터는 ONTAP REST API와 System Manager에 적용된다.

   보안 로그인 create-user-or-group-name storageUser-authentication-method password-application http-role StorageAdmin

5. 새로운 사용자 자격 증명을 사용하여 System Manager에 로그인하거나 ONTAP REST API를 사용하여 파일 시스템 분석 데이터에 액세스할 수 있습니다.

추가 정보

- 클러스터 관리자를 위한 사전 정의된 역할
- System Manager로 관리자 액세스 제어
- "RBAC 역할 및 ONTAP REST API에 대해 자세히 알아보십시오"

파일 시스템 분석을 위한 고려 사항

File System Analytics 구축과 관련된 특정 사용량 제한 및 잠재적 성능 영향을 알고 있어야 합니다.

SVM 보호 관계

SVM이 포함된 볼륨에서 파일 시스템 분석을 사용하도록 설정한 경우, 분석 데이터가 타겟 SVM에 복제되지 않습니다. 복구 작업에서 소스 SVM을 재동기화해야 하는 경우 복구 후 원하는 볼륨에 대한 분석을 수동으로 다시 활성화해야 합니다.

성능 고려 사항

경우에 따라 초기 메타데이터 수집 중에 파일 시스템 분석을 사용하도록 설정하면 성능에 부정적인 영향을 미칠 수 있습니다. 이는 일반적으로 최대 사용률이 있는 시스템에서 가장 많이 나타납니다. 이러한 시스템에 대한 분석을 사용하지 않으려면 ONTAP System Manager 성능 모니터링 툴을 사용하면 됩니다.

지연 시간이 현저하게 증가하는 경우 기술 자료 문서를 참조하십시오 "NetApp ONTAP 파일 시스템 분석을 켠 후 지연 시간이 높거나 변동이 심한 경우".

스캔 고려 사항

용량 분석을 활성화하면 ONTAP에서 용량 분석을 위한 초기화 스캔을 수행합니다. 이 스캔은 용량 분석이 활성화된 볼륨의 모든 파일에 대한 메타데이터에 액세스합니다. 스캔 중에 파일 데이터가 읽혀지지 않습니다. ONTAP 9.14.1부터 시스템 관리자의 탐색기 탭 또는 을 사용하여 REST API를 사용하여 스캔 진행률을 추적할 수 있습니다 `volume analytics show` CLI 명령: 임계치 조절 이벤트가 있는 경우 ONTAP에서 알림을 제공합니다.

볼륨에서 File System Analytics를 활성화할 때는 볼륨의 사용 가능한 공간의 5~8%가 사용 가능한지 확인하십시오. 볼륨에 자동 크기 조정이 활성화되어 있는 경우 최대 자동 확장 크기를 기준으로 사용 가능한 크기를 계산합니다. ONTAP 9.15.1부터 볼륨에서 파일 시스템 분석을 활성화할 때 사용 가능한 공간이 충분하지 않으면 ONTAP에 오류 메시지가 표시됩니다.

검사가 완료된 후 파일 시스템이 변경되면 File System Analytics는 실시간으로 계속 업데이트됩니다.

스캔에 필요한 시간은 볼륨의 디렉토리 및 파일 수에 비례합니다. 스캔은 메타데이터를 수집하므로 파일 크기는 스캔 시간에 영향을 주지 않습니다.

초기화 스캔에 대한 자세한 내용은 을 참조하십시오 "TR-4867: 파일 시스템 분석을 위한 모범 사례 지침".

모범 사례

애그리게이트를 공유하지 않는 볼륨에서 스캔을 시작해야 합니다. 명령을 사용하여 현재 어떤 애그리게이트가 어떤 볼륨을 호스팅하고 있는지 확인할 수 있습니다.

```
volume show -volume comma-separated-list_of_volumes -fields aggr-list
```

검사가 실행되는 동안 볼륨은 계속해서 클라이언트 트래픽을 처리합니다. 클라이언트 트래픽이 낮을 것으로 예상되는 기간 동안 스캔을 시작하는 것이 좋습니다.

클라이언트 트래픽이 증가하면 시스템 리소스가 소모되고 스캔 시간이 길어집니다.

ONTAP 9.12.1부터 시스템 관리자 및 ONTAP CLI에서 데이터 수집을 일시 중지할 수 있습니다.

- ONTAP CLI를 사용하는 경우:
  - 다음 명령을 사용하여 데이터 수집을 일시 중지할 수 있습니다. `volume analytics initialization pause -vserver svm_name -volume volume_name`
  - 클라이언트 트래픽이 느려지면 다음 명령을 사용하여 데이터 수집을 다시 시작할 수 있습니다. `volume analytics initialization resume -vserver svm_name -volume volume_name`
- System Manager를 사용하는 경우 볼륨 메뉴의 * 탐색기 * 보기에서 * 데이터 수집 일시 중지 * 및 * 데이터 수집 다시 시작 * 버튼을 사용하여 스캔을 관리합니다.

EMS 구성

EMS 구성 개요

즉각적인 주의가 필요한 시스템 문제를 즉시 알 수 있도록 중요한 EMS(이벤트 관리 시스템) 이벤트 알림을 이메일 주소, syslog 서버, SNMP(Simple Management Network Protocol) 트라프호스트 또는 웹후크 애플리케이션에 직접 보내도록 ONTAP 9를 구성할 수 있습니다.

중요 이벤트 알림은 기본적으로 활성화되어 있지 않으므로 이메일 주소, syslog 서버, SNMP traphost 또는 webhook 애플리케이션에 알림을 보내도록 EMS를 구성해야 합니다.

의 릴리스 특정 버전을 검토합니다 "ONTAP 9 EMS 참조".

EMS 이벤트 매핑에 사용되지 않는 ONTAP 명령 집합(예: 이벤트 대상, 이벤트 경로)을 사용하는 경우 매핑을 업데이트하는 것이 좋습니다. "사용되지 않는 ONTAP 명령에서 EMS 매핑을 업데이트하는 방법을 알아보십시오"..

System Manager로 EMS 이벤트 알림 및 필터를 구성합니다

System Manager를 사용하면 즉각적인 주의가 필요한 시스템 문제를 알릴 수 있도록 이벤트 관리 시스템(EMS)에서 이벤트 알림을 보내는 방법을 구성할 수 있습니다.

ONTAP 버전입니다	System Manager를 사용하면…
ONTAP 9.12.1 이상	원격 syslog 서버로 이벤트를 보낼 때 TLS(Transport Layer Security) 프로토콜을 지정합니다.
ONTAP 9.10.1 이상	e-메일 주소, syslog 서버, webhook 애플리케이션 및 SNMP traphosts를 구성합니다.
ONTAP 9.7 ~ 9.10.0	SNMP traphosts만 구성합니다. ONTAP CLI로 다른 EMS 대상을 구성할 수 있다. 을 참조하십시오 "EMS 구성 개요".

다음 절차를 수행할 수 있습니다.

- [add-ems-destination]
- [create-ems-filter]
- [edit-ems-destination]
- [edit-ems-filter]
- [delete-ems-destination]
- [delete-ems-filter]

관련 정보

- "ONTAP EMS 참조"
- "CLI를 사용하여 이벤트 알림을 수신하도록 SNMP traphosts를 구성합니다"

EMS 이벤트 알림 대상을 추가합니다

System Manager를 사용하여 EMS 메시지를 보낼 위치를 지정할 수 있습니다.

ONTAP 9.12.1부터 EMS 이벤트는 TLS(Transport Layer Security) 프로토콜을 통해 원격 syslog 서버의 지정된 포트로 전송될 수 있습니다. 자세한 내용은 를 참조하십시오 `event notification destination create` Man 페이지.

단계

1. 클러스터 > 설정 * 을 클릭합니다.
2. 알림 관리 * 섹션에서 를 클릭한 ⋮다음 * 이벤트 대상 보기 * 를 클릭합니다.
3. 알림 관리 * 페이지에서 * 이벤트 대상 * 탭을 선택합니다.
4. 을 + Add 클릭합니다.
5. 이름, EMS 대상 유형 및 필터를 지정합니다.

   필요한 경우 새 필터를 추가할 수 있습니다. 새 이벤트 필터 추가 * 를 클릭합니다.

6. 선택한 EMS 대상 유형에 따라 다음을 지정합니다.

구성하려면…	지정 또는 선택…
SNMP traphost를 참조하십시오	• traphost 이름입니다
이메일 (9.10.1부터)	• 대상 이메일 주소입니다 • 메일 서버 • 보낸 사람 이메일 주소
Syslog 서버 (9.10.1부터)	• 서버의 호스트 이름 또는 IP 주소입니다 • Syslog 포트(9.12.1로 시작) • Syslog 전송(9.12.1로 시작) TCP 암호화 * 를 선택하면 TLS(Transport Layer Security) 프로토콜이 활성화됩니다. Syslog port * 에 대해 값을 입력하지 않으면 * Syslog transport * 선택 항목에 따라 기본값이 사용됩니다.
웹훅 (9.10.1부터)	• 웹후크 URL • 클라이언트 인증(클라이언트 인증서를 지정하려면 이 옵션 선택)

새 **EMS** 이벤트 알림 필터를 생성합니다

ONTAP 9.10.1부터 시스템 관리자를 사용하여 EMS 알림 처리 규칙을 지정하는 새로운 사용자 지정 필터를 정의할 수 있습니다.

단계

1. 클러스터 > 설정 * 을 클릭합니다.
2. 알림 관리 * 섹션에서 를 클릭한 ⋮다음 * 이벤트 대상 보기 * 를 클릭합니다.
3. 알림 관리 * 페이지에서 * 이벤트 필터 * 탭을 선택합니다.
4. 을 + Add 클릭합니다.
5. 이름을 지정하고 기존 이벤트 필터에서 규칙을 복사할지 또는 새 규칙을 추가할지 여부를 선택합니다.
6. 선택에 따라 다음 단계를 수행하십시오.

선택하십시오.	그런 다음 다음 다음 단계를 수행합니다.
• 기존 이벤트 필터에서 규칙 복사 *	1. 기존 이벤트 필터를 선택합니다. 2. 기존 규칙을 수정합니다. 3. 필요한 경우 을 클릭하여 다른 규칙을 + Add 추가합니다.
• 새 규칙 추가 *	각 새 규칙의 유형, 이름 패턴, 심각도 및 SNMP 트랩 유형을 지정합니다.

EMS 이벤트 알림 대상을 편집합니다

ONTAP 9.10.1부터 시스템 관리자를 사용하여 이벤트 알림 대상 정보를 변경할 수 있습니다.

단계

1. 클러스터 > 설정 * 을 클릭합니다.
2. 알림 관리 * 섹션에서 를 클릭한 ⋮다음 * 이벤트 대상 보기 * 를 클릭합니다.
3. 알림 관리 * 페이지에서 * 이벤트 대상 * 탭을 선택합니다.
4. 이벤트 대상의 이름 옆에 있는 을 ⋮클릭한 다음 * 편집 * 을 클릭합니다.
5. 이벤트 대상 정보를 수정한 다음 * 저장 * 을 클릭합니다.

EMS 이벤트 알림 필터를 편집합니다

ONTAP 9.10.1.1부터 시스템 관리자를 사용하여 사용자 지정된 필터를 수정하여 이벤트 알림의 처리 방법을 변경할 수 있습니다.

ⓘ 시스템 정의 필터는 수정할 수 없습니다.

단계

1. 클러스터 > 설정 * 을 클릭합니다.
2. 알림 관리 * 섹션에서 를 클릭한 ⋮다음 * 이벤트 대상 보기 * 를 클릭합니다.
3. 알림 관리 * 페이지에서 * 이벤트 필터 * 탭을 선택합니다.
4. 이벤트 필터 이름 옆에 있는 을 ⋮클릭한 다음 * 편집 * 을 클릭합니다.
5. 이벤트 필터 정보를 수정한 다음 * 저장 * 을 클릭합니다.

EMS 이벤트 알림 대상을 삭제한다

ONTAP 9.10.1부터 System Manager를 사용하여 EMS 이벤트 알림 대상을 삭제할 수 있습니다.

> SNMP 대상은 삭제할 수 없습니다.

단계

1. 클러스터 > 설정 * 을 클릭합니다.
2. 알림 관리 * 섹션에서 를 클릭한 ⋮다음 * 이벤트 대상 보기 * 를 클릭합니다.
3. 알림 관리 * 페이지에서 * 이벤트 대상 * 탭을 선택합니다.
4. 이벤트 대상의 이름 옆에 있는 을 클릭한 ⋮다음 * 삭제 * 를 클릭합니다.

EMS 이벤트 알림 필터를 삭제한다

ONTAP 9.10.1부터 시스템 관리자를 사용하여 사용자 정의 필터를 삭제할 수 있습니다.

> 시스템 정의 필터는 삭제할 수 없습니다.

단계

1. 클러스터 > 설정 * 을 클릭합니다.
2. 알림 관리 * 섹션에서 를 클릭한 ⋮다음 * 이벤트 대상 보기 * 를 클릭합니다.
3. 알림 관리 * 페이지에서 * 이벤트 필터 * 탭을 선택합니다.
4. 이벤트 필터 이름 옆에 있는 을 ⋮클릭한 다음 * 삭제 * 를 클릭합니다.

CLI로 EMS 이벤트 알림을 설정한다

EMS 구성 작업 흐름

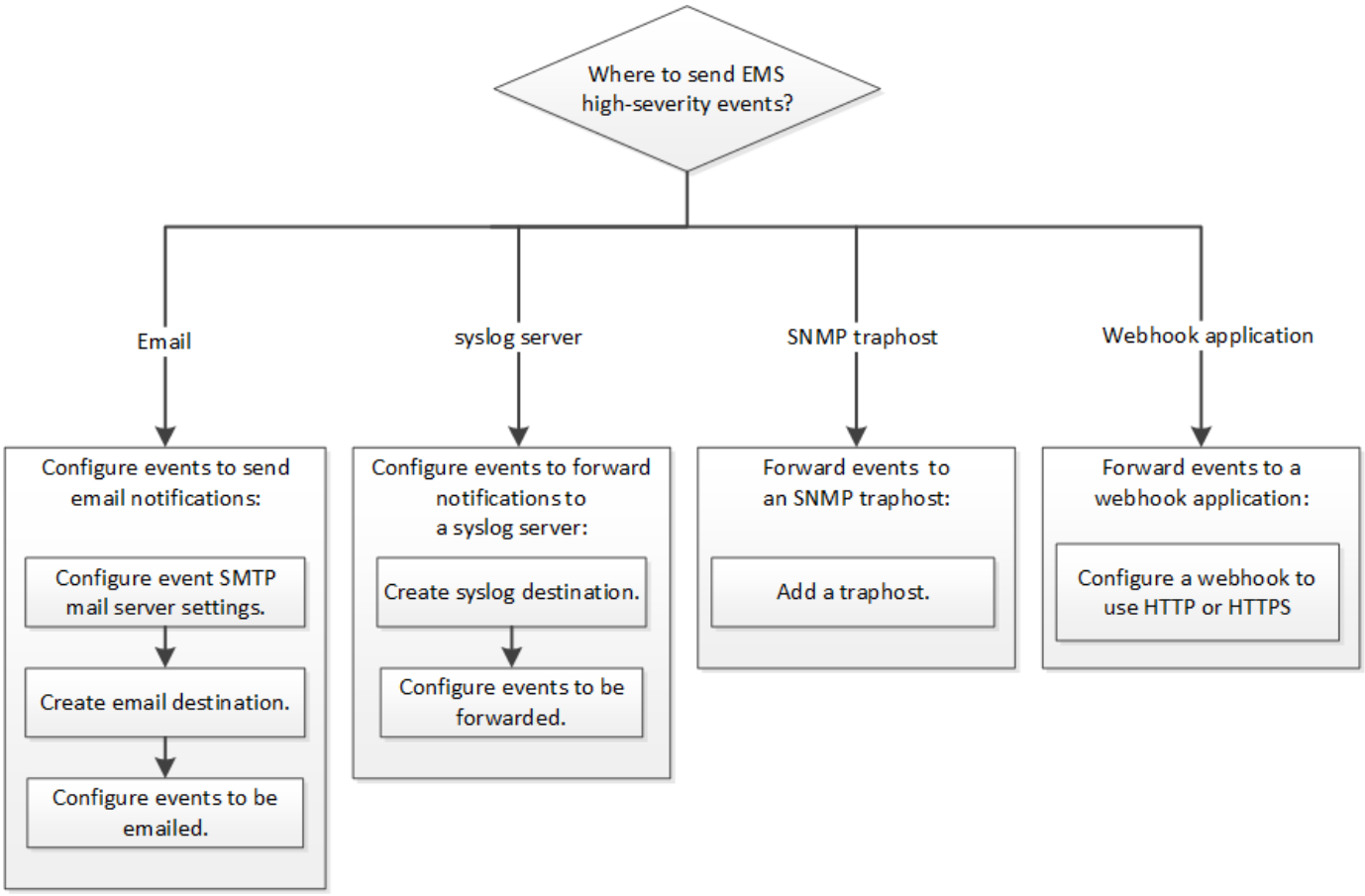
중요한 EMS 이벤트 알림을 e-메일로 보내거나, syslog 서버로 전달하거나, SNMP traphost로 전달하거나, webhook 애플리케이션으로 전달되도록 구성해야 합니다. 이를 통해 적시에 수정 조치를 취함으로써 시스템 중단을 방지할 수 있습니다.

이 작업에 대해

환경에 서버 및 애플리케이션과 같은 다른 시스템에서 기록된 이벤트를 집계하기 위한 syslog 서버가 이미 포함되어 있는 경우, 해당 syslog 서버를 사용하여 스토리지 시스템의 중요한 이벤트 알림도 쉽게 확인할 수 있습니다.

환경에 syslog 서버가 아직 포함되어 있지 않은 경우 중요한 이벤트 알림에 e-메일을 사용하는 것이 더 쉽습니다.

이벤트 알림을 SNMP traaphost에 이미 전달하는 경우 해당 traaphost에서 중요한 이벤트를 모니터링할 수 있습니다.



선택

- 이벤트 알림을 보내도록 EMS를 설정합니다.

원하는 작업	참조 항목...
EMS는 중요한 이벤트 알림을 이메일 주소로 전송합니다	e-메일 알림을 보내도록 중요한 EMS 이벤트를 구성합니다
중요한 이벤트 알림을 syslog 서버로 전달하는 EMS입니다	syslog 서버로 알림을 전달하도록 중요한 EMS 이벤트를 구성합니다
EMS에서 이벤트 알림을 SNMP traaphost로 전달하도록 하려는 경우	이벤트 알림을 수신하도록 SNMP traaphosts를 구성합니다
EMS에서 이벤트 알림을 Webhook 애플리케이션으로 전달하려는 경우	Webhook 애플리케이션에 알림을 전달하도록 중요한 EMS 이벤트를 구성합니다

e-메일 알림을 보내도록 중요한 **EMS** 이벤트를 구성합니다

가장 중요한 이벤트의 이메일 알림을 수신하려면 중요한 활동을 나타내는 이벤트에 대한 이메일 메시지를 보내도록 EMS를 구성해야 합니다.

필요한 것

클러스터에서 DNS를 구성하여 이메일 주소를 확인해야 합니다.

이 작업에 대해

ONTAP 명령줄에 명령을 입력하여 클러스터가 실행 중일 때마다 이 작업을 수행할 수 있습니다.

단계

1. 이벤트 SMTP 메일 서버 설정을 구성합니다.

   'event config modify-mail-server mailhost.your_domain-mail-from cluster_admin@your_domain'

2. 이벤트 알림을 위한 e-메일 대상 생성:

   '이벤트 알림 대상 create-name storage-admins-email@your_domain'으로 이메일을 보냅니다

3. e-메일 알림을 보내도록 중요한 이벤트를 구성합니다.

   이벤트 알림 create-filter-name important-events-destinations storage-admins입니다

syslog 서버로 알림을 전달하도록 중요한 **EMS** 이벤트 구성

syslog 서버에서 가장 심각한 이벤트의 알림을 기록하려면 중요한 활동을 나타내는 이벤트에 대한 알림을 전달하도록 EMS를 구성해야 합니다.

필요한 것

syslog 서버 이름을 확인하기 위해 클러스터에 DNS를 구성해야 합니다.

이 작업에 대해

환경에 이벤트 알림에 대한 syslog 서버가 아직 포함되어 있지 않은 경우 먼저 syslog 서버를 생성해야 합니다. 사용자 환경에 다른 시스템의 이벤트를 로깅하기 위한 syslog 서버가 이미 포함되어 있는 경우 중요한 이벤트 알림에 이 서버를 사용할 수 있습니다.

ONTAP CLI에서 명령을 입력하여 클러스터가 실행 중일 때마다 이 작업을 수행할 수 있습니다.

ONTAP 9.12.1부터 EMS 이벤트는 TLS(Transport Layer Security) 프로토콜을 통해 원격 syslog 서버의 지정된 포트로 전송될 수 있습니다. 두 가지 새로운 매개 변수를 사용할 수 있습니다.

`tcp-encrypted`

시기 `tcp-encrypted` 에 대해 지정됩니다 `syslog-transport`, ONTAP 는 해당 인증서를 검증하여 대상 호스트의 ID를 확인합니다. 기본값은 입니다 `udp-unencrypted`.

`syslog-port`

기본값입니다 `syslog-port` 매개 변수는 의 설정에 따라 다릅니다 `syslog-transport` 매개 변수. If(경우 `syslog-transport` 가 로 설정되어 있습니다 `tcp-encrypted`, `syslog-port` 기본값은 6514입니다.

자세한 내용은 를 참조하십시오 `event notification destination create` Man 페이지.

단계

1. 중요한 이벤트에 대한 syslog 서버 대상을 생성합니다.

```
event notification destination create -name syslog-ems -syslog syslog-server-address -syslog-transport {udp-unencrypted|tcp-unencrypted|tcp-encrypted}
```

ONTAP 9.12.1부터 에 대해 다음 값을 지정할 수 있습니다 `syslog-transport`:

- `udp-unencrypted` 보안 기능이 없는 사용자 데이터그램 프로토콜
- `tcp-unencrypted` 보안 기능이 없는 전송 제어 프로토콜
- `tcp-encrypted` 전송 계층 보안(TLS)이 있는 전송 제어 프로토콜

기본 프로토콜은 입니다 `udp-unencrypted`.

2. syslog 서버로 알림을 전달할 중요 이벤트를 구성합니다.

```
event notification create -filter-name important-events -destinations syslog-ems
```

이벤트 알림을 수신하도록 **SNMP traaphosts**를 구성합니다

SNMP traaphost에서 이벤트 알림을 수신하려면 traphost를 구성해야 합니다.

필요한 것

- 클러스터에서 SNMP 및 SNMP 트랩을 활성화해야 합니다.

  SNMP 및 SNMP 트랩은 기본적으로 사용하도록 설정됩니다.

- traphost 이름을 확인하기 위해 클러스터에서 DNS를 구성해야 합니다.

이 작업에 대해

이벤트 알림(SNMP 트랩)을 받도록 구성된 SNMP 트랩 호스트가 아직 없는 경우 이를 추가해야 합니다.

ONTAP 명령줄에 명령을 입력하여 클러스터가 실행 중일 때마다 이 작업을 수행할 수 있습니다.

단계

1. 환경에 이벤트 알림을 수신하도록 구성된 SNMP traaphost가 아직 없는 경우 다음 중 하나를 추가하십시오.

   'System snmp traphost add-peer-address_snmp_traphost_name_'

   기본적으로 SNMP에서 지원하는 모든 이벤트 알림은 SNMP traphost로 전달됩니다.

Webhook 애플리케이션에 알림을 전달하도록 중요한 **EMS** 이벤트를 구성합니다

중요한 이벤트 알림을 Webhook 애플리케이션에 전달하도록 ONTAP를 구성할 수 있습니다. 필요한 구성 단계는 선택한 보안 수준에 따라 다릅니다.

EMS 이벤트 전달을 구성할 준비를 합니다

이벤트 알림을 웹 후크 응용 프로그램으로 전달하도록 ONTAP를 구성하기 전에 고려해야 할 몇 가지 개념과 요구 사항이 있습니다.

Webhook 응용 프로그램

ONTAP 이벤트 알림을 받을 수 있는 웹 후크 응용 프로그램이 필요합니다. Webhook은 사용자가 정의한 콜백 루틴으로, 이 루틴이 실행되는 원격 응용 프로그램 또는 서버의 기능을 확장합니다. Webhook는 대상 URL로 HTTP 요청을 전송하여 클라이언트(이 경우 ONTAP)에 의해 호출되거나 활성화됩니다. 특히 ONTAP는 웹 후크 응용 프로그램을 호스팅하는 서버에 HTTP POST 요청을 보내고 XML로 포맷된 이벤트 알림 세부 정보를 보냅니다.

보안 옵션

TLS(Transport Layer Security) 프로토콜을 사용하는 방법에 따라 몇 가지 보안 옵션을 사용할 수 있습니다. 선택한 옵션에 따라 필요한 ONTAP 구성이 결정됩니다.

> TLS는 인터넷에서 널리 사용되는 암호화 프로토콜입니다. 하나 이상의 공개 키 인증서를 사용하여 개인 정보 보호와 데이터 무결성 및 인증을 제공합니다. 인증서는 신뢰할 수 있는 인증 기관에서 발급합니다.

HTTP

HTTP를 사용하여 이벤트 알림을 전송할 수 있습니다. 이 구성에서는 연결이 안전하지 않습니다. ONTAP 클라이언트 및 웹 후크 응용 프로그램의 ID가 확인되지 않습니다. 또한 네트워크 트래픽은 암호화되거나 보호되지 않습니다. 을 참조하십시오 "HTTP를 사용하도록 웹 후크 대상을 구성합니다" 를 참조하십시오.

HTTPS

추가 보안을 위해 Webhook 루틴을 호스팅하는 서버에 인증서를 설치할 수 있습니다. ONTAP는 HTTPS 프로토콜을 사용하여 웹 후크 응용 프로그램 서버의 ID와 네트워크 트래픽의 개인 정보 보호와 무결성을 보장합니다. 을 참조하십시오 "HTTPS를 사용하도록 웹 후크 대상을 구성합니다" 를 참조하십시오.

상호 인증을 사용하는 **HTTPS**

웹북 요청을 실행하는 ONTAP 시스템에 클라이언트 인증서를 설치하여 HTTPS 보안을 강화할 수 있습니다. webhook 응용 프로그램 서버의 ID를 확인하고 네트워크 트래픽을 보호하는 ONTAP 외에도 webhook 응용 프로그램은 ONTAP 클라이언트의 ID를 확인합니다. 이 양방향 피어 인증을 _Mutual TLS_라고 합니다. 을 참조하십시오 "상호 인증과 함께 HTTPS를 사용하도록 웹 후크 대상을 구성합니다" 를 참조하십시오.

관련 정보

- "TLS(Transport Layer Security) 프로토콜 버전 1.3"

HTTP를 사용하도록 웹 후크 대상을 구성합니다

HTTP를 사용하여 웹 후크 응용 프로그램에 이벤트 알림을 전달하도록 ONTAP를 구성할 수 있습니다. 이 옵션은 가장 안전하지는 않지만 가장 간단한 설치 방법입니다.

단계

1. 이벤트를 수신할 새 대상 'restapi-EMS'를 생성합니다.

   이벤트 알림 목적지 create-name restapi-ems-rest-api-url\http://<webhook-application>`

   위 명령에서 대상에 대해 * HTTP * 체계를 사용해야 합니다.

2. 중요 이벤트 필터를 "restapi-EMS" 대상으로 연결하는 알림 생성:

   이벤트 알림 create-filter-name important-events-destinations reapi-EMS

HTTPS를 사용하도록 웹 후크 대상을 구성합니다

HTTPS를 사용하여 이벤트 알림을 웹 후크 응용 프로그램으로 전달하도록 ONTAP를 구성할 수 있습니다. ONTAP는 서버 인증서를 사용하여 웹 후크 응용 프로그램의 ID를 확인하고 네트워크 트래픽을 보호합니다.

시작하기 전에

- Webhook 응용 프로그램 서버에 대한 개인 키와 인증서를 생성합니다
- ONTAP에 설치할 수 있는 루트 인증서를 가지고 있어야 합니다

단계

1. 웹 후크 응용 프로그램을 호스팅하는 서버에 적절한 서버 개인 키와 인증서를 설치합니다. 특정 구성 단계는 서버에 따라 다릅니다.
2. ONTAP에 서버 루트 인증서 설치:

   보안 인증서설치형 server-ca

   명령이 인증서를 요청합니다.

3. 이벤트를 수신할 'restapi-EMS' 대상을 생성합니다.

   이벤트 알림 목적지 create-name restapi-ems-rest-api-url\https://<webhook-application>`

   위의 명령에서 대상에 대해 * HTTPS * 구성표를 사용해야 합니다.

4. 중요 이벤트 필터를 새 restapi-EMS 대상과 연결하는 알림을 생성합니다.

   이벤트 알림 create-filter-name important-events-destinations reapi-EMS

상호 인증과 함께 HTTPS를 사용하도록 웹 후크 대상을 구성합니다

상호 인증을 사용하여 HTTPS를 사용하여 이벤트 알림을 웹 후크 응용 프로그램에 전달하도록 ONTAP를 구성할 수 있습니다. 이 구성에는 두 개의 인증서가 있습니다. ONTAP는 서버 인증서를 사용하여 webhook 응용 프로그램의 ID를 확인하고 네트워크 트래픽을 보호합니다. 또한 webhook를 호스팅하는 응용 프로그램은 클라이언트 인증서를 사용하여 ONTAP 클라이언트의 ID를 확인합니다.

시작하기 전에

ONTAP를 구성하기 전에 다음을 수행해야 합니다.

- Webhook 응용 프로그램 서버에 대한 개인 키와 인증서를 생성합니다
- ONTAP에 설치할 수 있는 루트 인증서를 가지고 있어야 합니다
- ONTAP 클라이언트에 대한 개인 키와 인증서를 생성합니다

단계

1. 작업의 처음 두 단계를 수행합니다 "HTTPS를 사용하도록 웹 후크 대상을 구성합니다" ONTAP가 서버의 ID를 확인할 수 있도록 서버 인증서를 설치합니다.
2. 웹 후크 응용 프로그램에 적절한 루트 및 중간 인증서를 설치하여 클라이언트 인증서를 확인합니다.
3. ONTAP에 클라이언트 인증서 설치:

보안 인증서 설치형 클라이언트

명령에서 개인 키와 인증서를 요청합니다.

4. 이벤트를 수신할 'restapi-EMS' 대상을 생성합니다.

   '이벤트 알림 대상 create-name restapi-EMS-REST-API-URL\https://<webhook-application> - certificate-authority <클라이언트 인증서 발급자> - certificate-serial <클라이언트 인증서 직렬>'

   위의 명령에서 대상에 대해 * HTTPS * 구성표를 사용해야 합니다.

5. 중요 이벤트 필터를 새 restapi-EMS 대상과 연결하는 알림을 생성합니다.

   이벤트 알림 create-filter-name important-events-destinations reapi-EMS

더 이상 사용되지 않는 **EMS** 이벤트 매핑을 업데이트합니다

EMS 이벤트 매핑 모델

ONTAP 9.0 이전에는 EMS 이벤트가 이벤트 이름 패턴 일치를 기준으로 이벤트 대상에만 매핑될 수 있었습니다. 이 모델을 사용하는 ONTAP 명령 집합('이벤트 대상', '이벤트 경로')은 최신 버전의 ONTAP에서 계속 사용할 수 있지만 ONTAP 9.0부터는 더 이상 사용되지 않습니다.

ONTAP 9.0부터 ONTAP EMS 이벤트 대상 매핑의 모범 사례는 이벤트 필터, 이벤트 알림, 이벤트 알림 대상 명령 집합을 사용하여 여러 필드에서 패턴 일치를 수행하는 보다 확장 가능한 이벤트 필터 모델을 사용하는 것입니다.

더 이상 사용되지 않는 명령어를 이용하여 EMS mapping을 설정한 경우, 'event filter', 'event notification', 'event notification destination' 명령어 세트를 사용하도록 mapping을 업데이트해야 한다.

이벤트 대상에는 두 가지 유형이 있습니다.

1. * 시스템 생성 대상 *: 기본적으로 5개의 시스템 생성 이벤트 대상이 있습니다.
   - '대들레부들'
   - "ASUP"
   - '비판들
   - 페이저
   - 트라프호스트

     시스템 생성 대상 중 일부는 특별한 목적으로 사용됩니다. 예를 들어, ASUP 대상은 callhome. * 이벤트를 ONTAP의 AutoSupport 모듈로 라우팅하여 AutoSupport 메시지를 생성합니다.

2. * 사용자 작성 대상 *: '이벤트 목적지 작성' 명령을 사용하여 수동으로 생성됩니다.

```
cluster-1::event*> destination show
                                                                    Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents        -                 -                  -
false
asup             -                 -                  -
false
criticals        -                 -                  -
false
pager            -                 -                  -
false
traphost         -                 -                  -
false
5 entries were displayed.
+
cluster-1::event*> destination create -name test -mail test@xyz.com
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
+
cluster-1::event*> destination show
+
Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents        -                 -                  -
false
asup             -                 -                  -
false
criticals        -                 -                  -
false
pager            -                 -                  -
false
test             test@xyz.com      -                  -
false
traphost         -                 -                  -
false
6 entries were displayed.
```

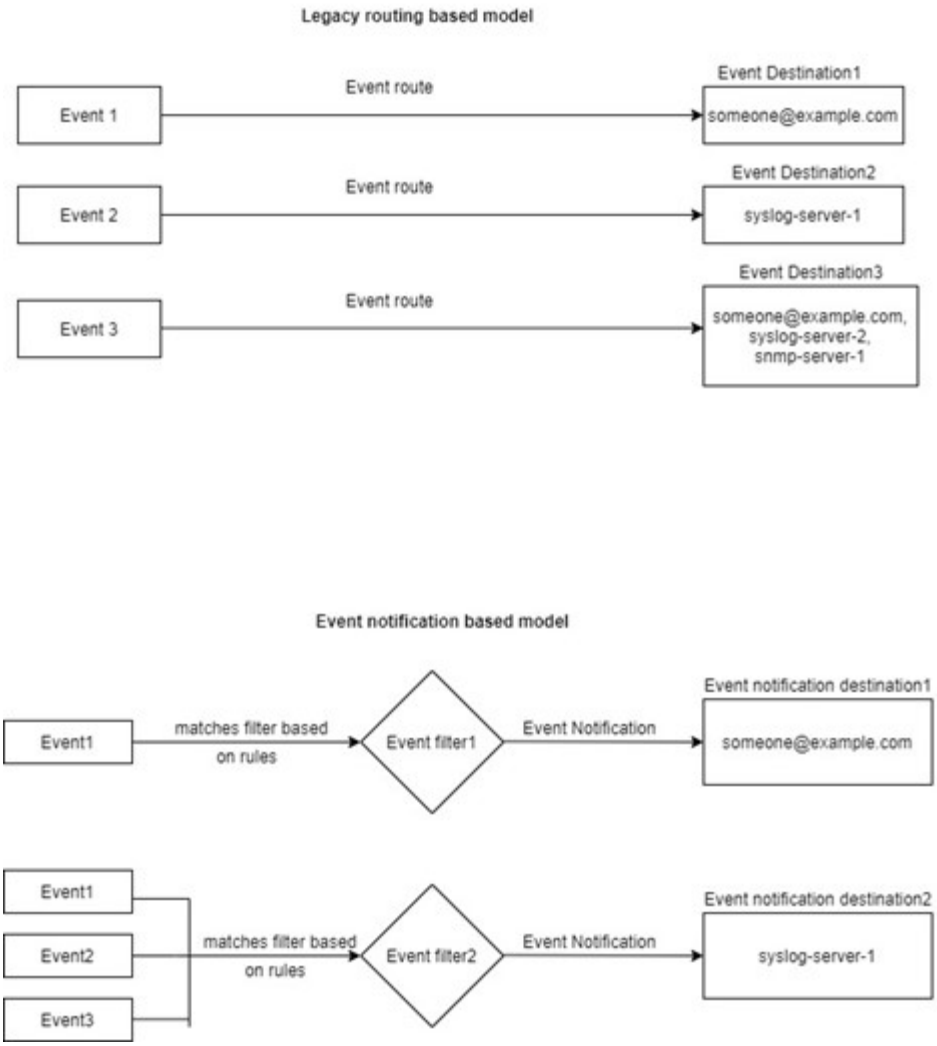
사용되지 않는 모델에서는 이벤트 라우트 add-destinations 명령을 사용하여 EMS 이벤트가 대상에 개별적으로 매핑됩니다.

```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.

cluster-1::event*> route show -message-name raid.aggr.*
                                                                    Freq
Time
Message                           Severity       Destinations   Threshd
Threshd
--------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort          NOTICE         test           0       0
raid.aggr.autoGrow.success        NOTICE         test           0       0
raid.aggr.lock.conflict           INFORMATIONAL  test           0       0
raid.aggr.log.CP.count            DEBUG          test           0       0
4 entries were displayed.
```

보다 확장성이 뛰어난 새로운 EMS 이벤트 알림 메커니즘은 이벤트 필터 및 이벤트 알림 대상을 기반으로 합니다. 새 이벤트 알림 메커니즘에 대한 자세한 내용은 다음 KB 문서를 참조하십시오.

- "ONTAP 9용 이벤트 관리 시스템 개요"



사용되지 않는 **ONTAP** 명령에서 **EMS** 이벤트 매핑을 업데이트합니다

EMS 이벤트 매핑이 사용되지 않는 ONTAP 명령 집합('이벤트 대상', '이벤트 경로')을 사용하여 현재 구성된 경우 다음 절차에 따라 매핑을 업데이트하여 '이벤트 필터', '이벤트 알림' 및 '이벤트 알림 대상' 명령 집합을 사용해야 합니다.

단계

1. 'event destination show' 명령을 사용하여 시스템의 모든 이벤트 대상을 나열합니다.

```
cluster-1::event*> destination show

Hide
Name              Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents         -                 -                  -
false
asup              -                 -                  -
false
criticals         -                 -                  -
false
pager             -                 -                  -
false
test              test@xyz.com      -                  -
false
traphost          -                 -                  -
false
6 entries were displayed.
```

2. 각 목적지에 대해 'event route show-destinations <destination name>' 명령어를 이용하여 해당 목적지에 맵핑되는 이벤트를 나열한다.

```
cluster-1::event*> route show -destinations test
                                                                  Freq
Time
Message                           Severity       Destinations   Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort          NOTICE         test           0       0
raid.aggr.autoGrow.success        NOTICE         test           0       0
raid.aggr.lock.conflict           INFORMATIONAL  test           0       0
raid.aggr.log.CP.count            DEBUG          test           0       0
4 entries were displayed.
```

3. 이러한 모든 이벤트 하위 집합을 포함하는 해당 이벤트 필터를 만듭니다. 예를 들어, 'raid.aggr.' * 이벤트만 포함하려면 필터를 생성할 때 'essage-name' 매개 변수에 와일드카드를 사용합니다. 단일 이벤트에 대한 필터를 만들 수도 있습니다.

> 최대 50개의 이벤트 필터를 만들 수 있습니다.

```
cluster-1::event*> filter create -filter-name test_events

cluster-1::event*> filter rule add -filter-name test_events -type
include -message-name raid.aggr.*

cluster-1::event*> filter show -filter-name test_events
Filter Name Rule     Rule      Message Name           SNMP Trap Type
Severity
            Position Type
----------- -------- --------- ---------------------- ---------------
--------
test_events
            1        include   raid.aggr.*            *               *
            2        exclude   *                      *               *
2 entries were displayed.
```

4. 각 '이벤트 대상' 엔드포인트(SMTP/SNMP/syslog)에 대해 '이벤트 알림 대상'을 생성한다.

```
cluster-1::event*> notification destination create -name dest1 -email
test@xyz.com

cluster-1::event*> notification destination show
Name            Type        Destination
--------------  ----------  ---------------------
dest1           email       test@xyz.com (via "localhost" from
"admin@localhost", configured in "event config")
snmp-traphost   snmp        - (from "system snmp traphost")
2 entries were displayed.
```

5. 이벤트 필터를 이벤트 알림 대상에 매핑하여 이벤트 알림을 생성합니다.

```
cluster-1::event*> notification create -filter-name asup_events
-destinations dest1

cluster-1::event*> notification show
ID   Filter Name                     Destinations
---- ------------------------------  -----------------
1    default-trap-events             snmp-traphost
2    asup_events                     dest1
2 entries were displayed.
```

6. 이벤트 경로 매핑이 있는 각 이벤트 대상에 대해 1-5단계를 반복합니다.

SNMP 대상으로 라우팅된 이벤트는 NMP-traphost 이벤트 알림 대상에 매핑되어야 합니다. SNMP traphost 대상은 시스템에서 구성한 SNMP traphost를 사용합니다.

```
cluster-1::event*> system snmp traphost add 10.234.166.135

cluster-1::event*> system snmp traphost show
        scspr2410142014.gdl.englab.netapp.com
(scspr2410142014.gdl.englab.netapp.com) <10.234.166.135>    Community:
public

cluster-1::event*> notification destination show -name snmp-traphost

                Destination Name: snmp-traphost
             Type of Destination: snmp
                     Destination: 10.234.166.135 (from "system snmp
traphost")
 Server CA Certificates Present?: -
   Client Certificate Issuing CA: -
Client Certificate Serial Number: -
       Client Certificate Valid?: -
```