System Manager로 클러스터 성능을 모니터링합니다

ONTAP 9

NetApp
September 12, 2024

목차

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, 체크박스에 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 FPolicy를 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.