FPolicy 이해

ONTAP 9

NetApp
May 09, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/ontap/nas-audit/two-parts-fpolicy-solution-concept.html on May 09, 2024. Always check docs.netapp.com for the latest.

목차

FPolicy 이해

FPolicy 솔루션의 두 부분은 무엇입니까

FPolicy는 파트너 솔루션을 통해 SVM(스토리지 가상 머신)의 파일 액세스 이벤트를 모니터링 및 관리하는 데 사용되는 파일 액세스 알림 프레임워크입니다. 파트너 솔루션을 사용하면 데이터 거버넌스 및 규정 준수, 랜섬웨어 보호 및 데이터 이동성과 같은 다양한 사용 사례를 해결할 수 있습니다.

파트너 솔루션에는 NetApp 지원 타사 솔루션과 NetApp 제품 워크로드 보안 및 클라우드 데이터 센스 가 모두 포함됩니다.

FPolicy 솔루션에는 두 가지 부품이 있습니다. ONTAP FPolicy 프레임워크는 클러스터의 활동을 관리하고 파트너 애플리케이션(일명 외부 FPolicy 서버)에 알림을 보냅니다. 외부 FPolicy 서버는 ONTAP FPolicy에서 보낸 알림을 처리하여 고객 사용 사례를 이행합니다.

ONTAP 프레임워크는 FPolicy 구성을 생성하고 유지하며 파일 이벤트를 모니터링하고 외부 FPolicy 서버에 알림을 보냅니다. ONTAP FPolicy는 외부 FPolicy 서버와 SVM(스토리지 가상 머신) 노드 간의 통신을 허용하는 인프라를 제공합니다.

FPolicy 프레임워크는 외부 FPolicy 서버에 연결되며, 클라이언트 액세스의 결과로 특정 파일 시스템 이벤트에 대한 알림을 FPolicy 서버로 보냅니다. 외부 FPolicy 서버에서 알림을 처리하고 응답을 노드로 다시 보냅니다. 알림 처리 결과로 발생하는 작업은 응용 프로그램과 노드와 외부 서버 간의 통신이 비동기 또는 동기인지 여부에 따라 달라집니다.

동기식 및 비동기식 알림입니다

FPolicy는 FPolicy 인터페이스를 통해 외부 FPolicy 서버에 알림을 보냅니다. 알림은 동기 또는 비동기 모드로 전송됩니다. 알림 모드는 FPolicy 서버에 알림을 보낸 후 ONTAP에서 수행하는 작업을 결정합니다.

- * 비동기 알림 *

  비동기 알림을 사용할 경우 노드는 FPolicy 서버의 응답을 기다리지 않으므로 시스템의 전반적인 처리량이 향상됩니다. 이 유형의 알림은 FPolicy 서버에서 알림 평가의 결과로 어떤 작업도 수행할 필요가 없는 애플리케이션에 적합합니다. 예를 들어, 스토리지 가상 시스템(SVM) 관리자가 파일 액세스 활동을 모니터링하고 감사하려고 할 때 비동기 알림이 사용됩니다.

  비동기 모드에서 작동하는 FPolicy 서버에서 네트워크 중단이 발생하는 경우, 정전 중에 생성된 FPolicy 알림은 스토리지 노드에 저장됩니다. FPolicy 서버가 온라인 상태로 돌아오면 저장된 알림에 대한 알림이 표시되고 스토리지 노드에서 가져올 수 있습니다. 정전 중에 알림을 저장할 수 있는 시간은 최대 10분까지 구성할 수 있습니다.

  ONTAP 9.14.1부터 FPolicy를 사용하면 SVM의 비동기적 정책에 대한 파일 액세스 이벤트를 캡처하는 영구 저장소를 설정할 수 있습니다. 영구 저장소는 클라이언트 I/O 처리를 FPolicy 알림 처리와 분리하여 클라이언트 지연 시간을 줄여 줍니다. 동기(필수 또는 비필수) 및 비동기 필수 구성은 지원되지 않습니다.

- * 동기식 알림 *

  동기식 모드에서 실행하도록 구성된 경우 FPolicy 서버는 클라이언트 작업을 계속하기 전에 모든 알림을 확인해야

합니다. 이 유형의 알림은 알림 평가 결과에 따라 조치가 필요한 경우에 사용됩니다. 예를 들어, SVM 관리자가 외부 FPolicy 서버에 지정된 기준에 따라 요청을 허용하거나 거부하려는 경우 동기식 알림이 사용됩니다.

동기 및 비동기 애플리케이션

FPolicy 애플리케이션은 비동기식 및 동기식 모두에서 사용할 수 있습니다.

비동기식 애플리케이션은 외부 FPolicy 서버가 파일 또는 디렉토리에 대한 액세스를 변경하거나 SVM(스토리지 가상 머신)의 데이터를 수정하지 않는 애플리케이션입니다. 예를 들면 다음과 같습니다.

- 파일 액세스 및 감사 로깅
- 스토리지 리소스 관리

동기식 애플리케이션은 데이터 액세스가 변경되거나 외부 FPolicy 서버에 의해 데이터가 수정된 애플리케이션입니다. 예를 들면 다음과 같습니다.

- 할당량 관리
- 파일 액세스 차단
- 파일 아카이빙 및 계층적 스토리지 관리
- 암호화 및 암호 해독 서비스
- 압축 및 압축 해제 서비스

FPolicy 영구 저장소

ONTAP 9.14.1부터 FPolicy를 사용하면 SVM의 비동기적 정책에 대한 파일 액세스 이벤트를 캡처하는 영구 저장소를 설정할 수 있습니다. 영구 저장소는 클라이언트 I/O 처리를 FPolicy 알림 처리와 분리하여 클라이언트 지연 시간을 줄여 줍니다. 동기(필수 또는 비필수) 및 비동기 필수 구성은 지원되지 않습니다.

이 기능은 FPolicy 외부 모드에서만 사용할 수 있습니다. 사용하는 파트너 응용 프로그램이 이 기능을 지원해야 합니다. 파트너와 협력하여 이 FPolicy 구성이 지원되도록 해야 합니다.

모범 사례

클러스터 관리자는 FPolicy가 활성화된 각 SVM에서 영구 저장소의 볼륨을 구성해야 합니다. 구성된 영구 저장소는 일치하는 모든 FPolicy 이벤트를 캡처하며, FPolicy 파이프라인에서 추가로 처리되어 외부 서버로 전송됩니다.

영구 저장소는 예상치 못한 재부팅이 발생하거나 FPolicy가 비활성화되었다가 다시 활성화되었을 때 마지막 이벤트가 수신된 때처럼 유지됩니다. 테이크오버 작업 후 새 이벤트는 파트너 노드에서 저장하고 처리합니다. 반환 작업 후 영구 저장소는 노드 테이크오버 발생 시 계속 처리될 수 있는 처리되지 않은 이벤트의 처리를 다시 시작합니다. 라이브 이벤트는 처리되지 않은 이벤트보다 우선 순위가 부여됩니다.

영구 저장소 볼륨이 한 노드에서 동일한 SVM의 다른 노드로 이동하는 경우 아직 처리되지 않은 알림도 새 노드로 이동됩니다. 를 다시 실행해야 합니다 `fpolicy persistent-store create` 보류 중인 알림이 외부 서버로 전달되도록 볼륨을 이동한 후 두 노드 중 하나에서 명령을 실행합니다.

영구 저장소 볼륨은 SVM별로 설정됩니다. 각 FPolicy가 활성화된 SVM에 대해 영구 저장소 볼륨을 생성해야 합니다.

Fpolicy에서 최대 트래픽을 모니터링할 것으로 예상되는 LIF로 노드에 영구 저장소 볼륨을 생성합니다.

영구 저장소에 누적된 알림이 프로비저닝된 볼륨 크기를 초과하면 FPolicy가 적절한 EMS 메시지와 함께 수신 알림을 삭제하기 시작합니다.

영구 저장소 볼륨 이름과 볼륨 생성 시 지정된 접합 경로가 일치해야 합니다.

스냅샷 정책을 로 설정합니다 `none` 에 대해 이야기해 보려고 합니다 `default`. 이는 스냅샷을 실수로 복구하여 현재 이벤트가 손실되지 않도록 하고 중복 이벤트 처리를 방지하기 위한 것입니다.

영구 저장소 볼륨을 외부 사용자 프로토콜 액세스(CIFS/NFS)에 액세스할 수 없도록 하여 영구 이벤트 레코드가 실수로 손상되거나 삭제되지 않도록 합니다. 이를 위해 FPolicy를 활성화한 후 ONTAP에서 볼륨을 마운트 해제하여 접합 경로를 제거하면 사용자 프로토콜 액세스에 액세스할 수 없게 됩니다.

자세한 내용은 을 참조하십시오 "영구 저장소를 만듭니다".

FPolicy 구성 유형

기본 FPolicy 구성 유형은 두 가지입니다. 하나의 구성에서는 외부 FPolicy 서버를 사용하여 알림을 처리하고 처리합니다. 다른 구성에서는 외부 FPolicy 서버를 사용하지 않습니다. 대신 ONTAP 내부 기본 FPolicy 서버를 사용하여 확장자에 따라 간단한 파일 차단을 수행합니다.

- * 외부 FPolicy 서버 구성 *

  이 알림은 FPolicy 서버로 전송됩니다. FPolicy 서버는 요청을 심사하고 규칙을 적용하여 노드에서 요청된 파일 작업을 허용할 것인지 결정합니다. 그런 다음 동기식 정책의 경우 FPolicy 서버가 노드에 응답을 보내 요청된 파일 작업을 허용하거나 차단합니다.

- * 기본 FPolicy 서버 구성 *

  알림은 내부적으로 스크리닝됩니다. FPolicy 범위에 구성된 파일 확장명 설정에 따라 요청이 허용되거나 거부됩니다.

- 참고 *: 거부된 파일 확장 요청은 기록되지 않습니다.

기본 FPolicy 구성을 생성하는 경우

기본 FPolicy 구성에서는 ONTAP 내부 FPolicy 엔진을 사용하여 파일의 확장명에 따라 파일 작업을 모니터링하고 차단합니다. 이 솔루션에는 외부 FPolicy 서버(FPolicy 서버)가 필요하지 않습니다. 이 간단한 솔루션이 필요한 경우 기본 파일 차단 구성을 사용하는 것이 좋습니다.

기본 파일 차단을 사용하면 구성된 작업 및 필터링 이벤트와 일치하는 모든 파일 작업을 모니터링한 다음 특정 확장명을 가진 파일에 대한 액세스를 거부할 수 있습니다. 기본 구성입니다.

이 구성은 파일 확장자만을 기준으로 파일 액세스를 차단하는 방법을 제공합니다. 예를 들어, 'P3' 확장자가 포함된 파일을 차단하려면 'P3'의 대상 파일 확장자를 가진 특정 작업에 대한 알림을 제공하는 정책을 구성합니다. 이 정책은 알림을 생성하는 작업에 대한 mP3 파일 요청을 거부하도록 구성되어 있습니다.

다음은 기본 FPolicy 구성에 적용됩니다.

- FPolicy 서버 기반 파일 검사에서 지원되는 것과 동일한 필터 및 프로토콜 세트도 기본 파일 차단에 대해

지원됩니다.

- 기본 파일 차단 및 FPolicy 서버 기반 파일 검사 애플리케이션을 동시에 구성할 수 있습니다.

  이렇게 하려면 기본 파일 차단용으로 구성된 정책 하나와 FPolicy 서버 기반 파일 검사용으로 구성된 정책 하나를 사용하여 SVM(스토리지 가상 머신)에 대해 두 개의 개별 FPolicy 정책을 구성할 수 있습니다.

- 기본 파일 차단 기능은 파일 내용이 아닌 확장자에 따라 파일을 심사합니다.
- 심볼 링크의 경우 네이티브 파일 차단은 루트 파일의 파일 확장명을 사용합니다.

에 대해 자세히 알아보십시오 "FPolicy: 기본 파일 차단".

외부 **FPolicy** 서버를 사용하는 구성을 생성하는 시기

외부 FPolicy 서버를 사용하여 알림을 처리 및 관리하는 FPolicy 구성은 파일 확장자에 따라 단순한 파일 차단이 필요한 사용 사례에 적합한 강력한 솔루션을 제공합니다.

파일 액세스 이벤트를 모니터링 및 기록하고, 할당량 서비스를 제공하고, 단순 파일 확장자 이외의 기준에 따라 파일 차단을 수행하고, 계층적 스토리지 관리 애플리케이션을 사용하여 데이터 마이그레이션 서비스를 제공하려는 경우에 외부 FPolicy 서버를 사용하는 구성을 생성해야 합니다. 스토리지 가상 시스템(SVM)의 데이터 서브셋만 모니터링하는 세부적인 정책 세트를 제공할 수도 있습니다.

클러스터 구성 요소가 **FPolicy** 구현을 수행하는 역할을 합니다

클러스터와 포함된 SVM(스토리지 가상 머신) 및 데이터 LIF는 모두 FPolicy 구현에서 역할을 합니다.

- * 클러스터 *

  클러스터는 FPolicy 관리 프레임워크를 포함하고 클러스터의 모든 FPolicy 구성에 대한 정보를 유지 관리하고 관리합니다.

- * SVM *

  FPolicy 구성은 SVM 레벨에서 정의됩니다. 구성 범위는 SVM 이며 SVM 리소스에서만 작동합니다. 한 SVM 구성은 다른 SVM에 상주하는 데이터에 대한 파일 액세스 요청을 모니터링하고 알림을 전송할 수 없습니다.

  FPolicy 구성은 관리 SVM에서 정의할 수 있습니다. 관리 SVM에서 구성을 정의하면 모든 SVM에서 구성을 확인하고 사용할 수 있습니다.

- 데이터 LIF *

  FPolicy 서버에 대한 연결은 FPolicy 구성을 사용하여 SVM에 속하는 데이터 LIF를 통해 이루어집니다. 이러한 연결에 사용되는 데이터 LIF는 일반 클라이언트 액세스에 사용되는 데이터 LIF와 같은 방법으로 페일오버할 수 있습니다.

FPolicy가 외부 **FPolicy** 서버에서 작동하는 방식

스토리지 가상 시스템(SVM)에서 FPolicy를 구성하고 사용하도록 설정한 후에는 SVM이 참여하는 모든 노드에서 FPolicy가 실행됩니다. FPolicy는 알림 처리를 위해 외부 FPolicy

서버(FPolicy 서버)와의 연결을 설정하고 유지하는 동시에 FPolicy 서버와 주고받는 알림 메시지를 관리하는 역할을 합니다.

또한 연결 관리의 일환으로 FPolicy는 다음과 같은 책임을 수행합니다.

- 파일 알림이 올바른 LIF를 통해 FPolicy 서버로 흐르도록 합니다.
- 여러 FPolicy 서버가 정책에 연결될 때 FPolicy 서버로 알림을 보낼 때 로드 밸런싱이 수행됩니다.
- FPolicy 서버에 대한 연결이 끊어지면 연결을 다시 설정하려고 시도합니다.
- 인증된 세션을 통해 FPolicy 서버에 알림을 보냅니다.
- 패스스루 읽기가 활성화된 경우 FPolicy 서버에서 클라이언트 요청을 처리하기 위해 설정하는 패스스루 읽기 데이터 연결을 관리합니다.

FPolicy 통신에는 제어 채널이 어떻게 사용됩니다

FPolicy는 스토리지 가상 머신(SVM)에 참여하는 각 노드의 데이터 LIF에서 외부 FPolicy 서버에 대한 제어 채널 연결을 시작합니다. FPolicy는 제어 채널을 사용하여 파일 알림을 전송합니다. 따라서 FPolicy 서버는 SVM 토폴로지를 기준으로 여러 개의 제어 채널 연결을 볼 수 있습니다.

동기 통신에 권한 있는 데이터 액세스 채널이 사용되는 방식

동기식 사용 사례에서 FPolicy 서버는 권한이 있는 데이터 액세스 경로를 통해 SVM(스토리지 가상 머신)에 있는 데이터에 액세스합니다. 권한 있는 경로를 통해 액세스하면 전체 파일 시스템이 FPolicy 서버에 노출됩니다. IT 부서는 데이터 파일에 액세스하여 정보를 수집하고, 파일을 스캔하거나, 파일을 읽거나, 파일에 쓸 수 있습니다.

외부 FPolicy 서버가 권한 있는 데이터 채널을 통해 SVM 루트에서 전체 파일 시스템에 액세스할 수 있으므로 권한이 있는 데이터 채널 연결이 보안되어야 합니다.

권한 있는 데이터 액세스 채널에서 **FPolicy** 연결 자격 증명을 사용하는 방법

FPolicy 서버는 FPolicy 구성과 함께 저장된 특정 Windows 사용자 자격 증명을 사용하여 클러스터 노드에 대한 권한 있는 데이터 액세스 연결을 만듭니다. SMB는 권한이 있는 데이터 액세스 채널 연결을 만들기 위해 지원되는 유일한 프로토콜입니다.

FPolicy 서버에 권한이 있는 데이터 액세스가 필요한 경우 다음 조건을 충족해야 합니다.

- 클러스터에서 SMB 라이센스를 활성화해야 합니다.
- FPolicy 서버는 FPolicy 구성에 구성된 자격 증명에서 실행해야 합니다.

데이터 채널을 연결할 때 FPolicy는 지정된 Windows 사용자 이름에 대한 자격 증명을 사용합니다. admin 공유 ONTAP_admin$에서 데이터 액세스가 가능합니다.

권한 있는 데이터 액세스를 위해 수퍼 사용자 자격 증명을 부여하는 것은 무엇을 의미하는지

ONTAP는 FPolicy 구성에 구성된 IP 주소와 사용자 자격 증명의 조합을 사용하여 수퍼 사용자 자격 증명을 FPolicy 서버에 부여합니다.

수퍼 사용자 상태는 FPolicy 서버가 데이터에 액세스할 때 다음 권한을 부여합니다.

- 권한 검사를 피하십시오

  사용자는 파일 및 디렉터리 액세스에 대한 검사를 피할 수 있습니다.

- 특수 잠금 권한

  ONTAP는 기존 잠금과 관계없이 모든 파일에 대한 읽기, 쓰기 또는 수정 액세스를 허용합니다. FPolicy 서버가 파일에서 바이트 범위 잠금을 사용하면 파일에서 기존 잠금을 즉시 제거할 수 있습니다.

- FPolicy 검사를 생략합니다

  FPolicy 알림을 생성하지 않습니다.

FPolicy가 정책 처리를 관리하는 방법입니다

스토리지 가상 시스템(SVM)에 여러 FPolicy 정책이 할당될 수 있으며 각 정책은 서로 다른 우선순위를 갖습니다. SVM에 적절한 FPolicy 구성을 생성하려면 FPolicy에서 정책 처리를 관리하는 방법을 이해하는 것이 중요합니다.

각 파일 액세스 요청은 처음에 평가하여 이 이벤트를 모니터링하는 정책을 결정합니다. 모니터링되는 이벤트인 경우 관심 있는 정책과 함께 모니터링되는 이벤트에 대한 정보가 FPolicy로 전달되어 FPolicy가 평가됩니다. 각 정책은 할당된 우선 순위에 따라 평가됩니다.

정책을 구성할 때는 다음 권장 사항을 고려해야 합니다.

- 다른 정책보다 먼저 정책을 항상 평가하려면 우선 순위가 더 높은 정책을 구성합니다.
- 모니터링되는 이벤트에 대해 요청된 파일 액세스 작업의 성공이 다른 정책에 대해 평가된 파일 요청에 대한 사전 요구 사항이면 첫 번째 파일 작업의 성공 또는 실패를 보다 높은 우선 순위로 제어하는 정책을 지정합니다.

  예를 들어, 하나의 정책이 FPolicy 파일 아카이빙 및 복원 기능을 관리하고 두 번째 정책이 온라인 파일의 파일 액세스 작업을 관리하는 경우, 파일 복원을 관리하는 정책은 우선 순위가 더 높아야 두 번째 정책에 의해 관리되는 작업을 허용하기 전에 파일을 복원할 수 있습니다.

- 파일 액세스 작업에 적용할 수 있는 모든 정책을 평가하려면 동기 정책을 낮은 우선 순위로 지정합니다.

정책 시퀀스 번호를 수정하여 기존 정책에 대한 정책 우선 순위를 다시 정렬할 수 있습니다. 하지만 FPolicy에서 수정된 우선 순위 순서에 따라 정책을 평가하도록 하려면 수정된 시퀀스 번호를 사용하여 정책을 사용하지 않도록 설정하고 다시 활성화해야 합니다.

노드-외부 FPolicy 서버 통신 프로세스는 무엇입니까

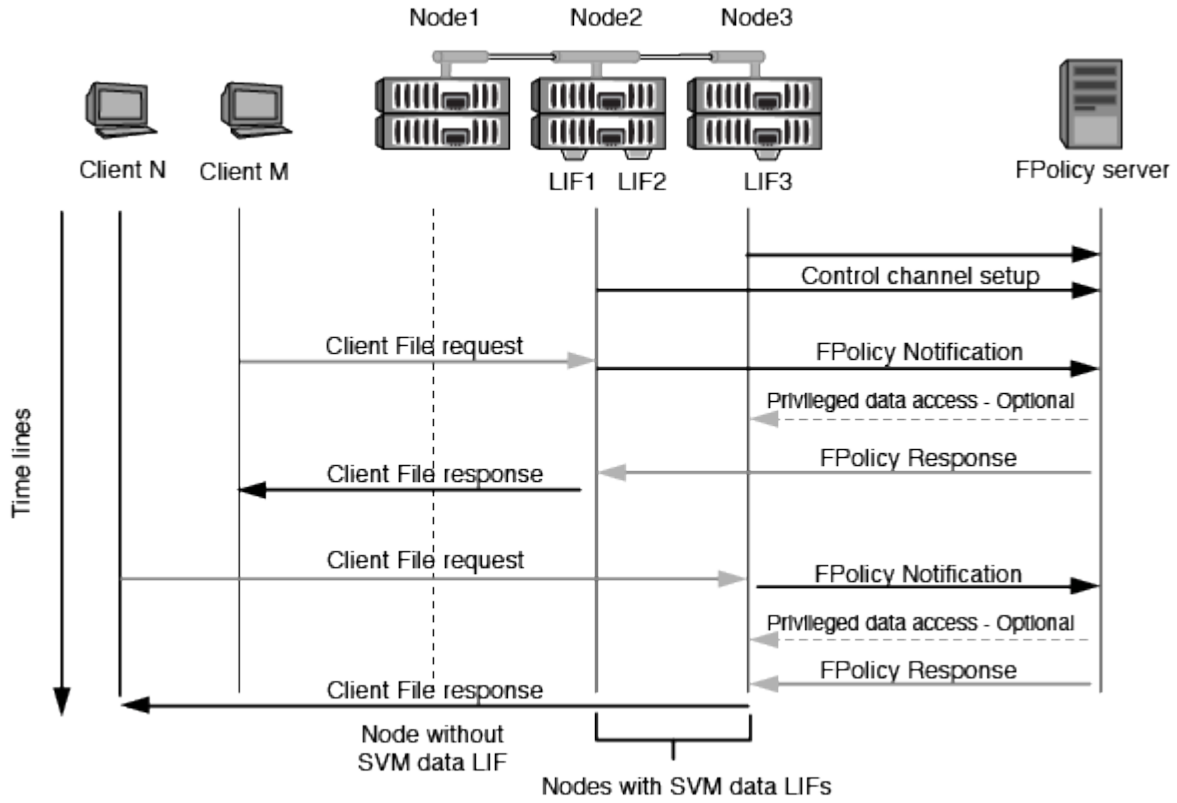
FPolicy 구성을 올바르게 계획하려면 노드-외부 FPolicy 서버 통신 프로세스가 무엇인지 이해해야 합니다.

각 스토리지 가상 머신(SVM)에 참여하는 모든 노드는 TCP/IP를 사용하여 외부 FPolicy 서버(FPolicy 서버)에 연결을 시작합니다. FPolicy 서버에 대한 연결은 노드 데이터 LIF를 사용하여 설정됩니다. 따라서 노드에 SVM을 위한 운영 데이터 LIF가 있는 경우에만 참여 노드가 연결을 설정할 수 있습니다.

참여 노드의 각 FPolicy 프로세스는 정책이 사용되도록 설정된 경우 FPolicy 서버에 연결을 설정하려고 시도합니다. 정책 구성에 지정된 FPolicy 외부 엔진의 IP 주소와 포트를 사용합니다.

이 연결을 통해 데이터 LIF를 통해 각 SVM에 참여하는 각 노드에서 FPolicy 서버로 제어 채널을 설정합니다. 또한 IPv4 및 IPv6 데이터 LIF 주소가 동일한 참여 노드에 있는 경우 FPolicy는 IPv4와 IPv6 모두에 대한 연결을 시도합니다. 따라서 SVM이 여러 노드로 확장되거나 IPv4 및 IPv6 주소가 둘 다 있는 경우 SVM에서 FPolicy 정책을 활성화한 후 FPolicy 서버에서 클러스터의 여러 제어 채널 설정 요청을 준비할 수 있어야 합니다.

예를 들어, 클러스터에 Node1, Node2, Node3와 같은 3개의 노드가 있고, SVM 데이터 LIF가 Node2와 Node3에만 분산되는 경우, 데이터 볼륨의 분산에 관계없이 제어 채널은 Node2와 Node3에서만 시작됩니다. Node2에는 SVM에 속하는 두 개의 데이터 LIF(LIF1 및 LIF2)가 있으며, 초기 접속은 LIF1입니다. LIF1에 장애가 발생하면 FPolicy는 LIF2에서 제어 채널을 설정하려고 시도합니다.



FPolicy가 LIF 마이그레이션 또는 페일오버 중에 외부 통신을 관리하는 방법입니다

데이터 LIF는 동일한 노드의 데이터 포트 또는 원격 노드의 데이터 포트로 마이그레이션할 수 있습니다.

데이터 LIF가 페일오버되거나 마이그레이션되면 FPolicy 서버에 새 제어 채널 연결이 만들어집니다. 그런 다음 FPolicy는 시간이 초과된 SMB 및 NFS 클라이언트 요청을 다시 시도할 수 있습니다. 그 결과 새 알림이 외부 FPolicy 서버로 전송됩니다. 이 노드는 FPolicy 서버 응답을 원래의 제한 시간이 초과된 SMB 및 NFS 요청에 대해 거부합니다.

노드 페일오버 중에 FPolicy가 외부 통신을 관리하는 방법

FPolicy 통신에 사용되는 데이터 포트를 호스팅하는 클러스터 노드에 장애가 발생하면 ONTAP는 FPolicy 서버와 노드 간의 연결을 끊습니다.

FPolicy 통신에 사용되는 데이터 포트를 다른 활성 노드로 마이그레이션하도록 페일오버 정책을 구성하여 FPolicy 서버로 클러스터 페일오버가 미치는 영향을 완화할 수 있습니다. 마이그레이션이 완료되면 새 데이터 포트를 사용하여 새 연결이 설정됩니다.

데이터 포트를 마이그레이션하도록 페일오버 정책이 구성되지 않은 경우 FPolicy 서버가 장애가 발생한 노드가 시작될

때까지 기다려야 합니다. 노드가 가동되면 새 세션 ID가 있는 해당 노드에서 새 연결이 시작됩니다.

> FPolicy 서버에서 Keep-alive 프로토콜 메시지의 끊어진 연결을 감지합니다. FPolicy를 구성할 때 세션 ID를 제거하는 시간이 초과되었습니다. 기본 연결 유지 시간 초과는 2분입니다.

FPolicy 서비스가 SVM 네임스페이스 전체에서 작동하는 방식

ONTAP은 유니파이드 스토리지 가상 시스템(SVM) 네임스페이스를 제공합니다. 접합을 통해 클러스터 전체의 볼륨을 연결하여 하나의 논리적 파일 시스템을 제공합니다. FPolicy 서버는 네임스페이스 토폴로지를 인식하고 네임스페이스에서 FPolicy 서비스를 제공합니다.

네임스페이스는 SVM 내에서만 고유하며 SVM 내부에 포함되어 있습니다. 따라서 SVM 컨텍스트에서만 네임스페이스를 볼 수 있습니다. 네임스페이스에는 다음과 같은 특성이 있습니다.

- 각 SVM에는 네임스페이스 루트의 루트가 루트 볼륨으로, 네임스페이스에서 슬래시(/)로 표시되는 단일 네임스페이스가 있습니다.
- 다른 모든 볼륨에는 루트(/) 아래에 접합점이 있습니다.
- 볼륨 접합은 클라이언트에 영향을 미치지 않습니다.
- 단일 NFS 내보내기로 전체 네임스페이스에 대한 액세스를 제공할 수 있습니다. 그렇지 않으면 엑스포트 정책으로 특정 볼륨을 내보낼 수 있습니다.
- SMB 공유는 볼륨 내의 qtree 또는 네임스페이스 내의 모든 디렉토리에 생성할 수 있습니다.
- 네임스페이스 아키텍처는 유연합니다.

  일반적인 네임스페이스 아키텍처의 예는 다음과 같습니다.

  - 루트에서 단일 분기가 있는 네임스페이스
  - 루트에서 여러 개의 분기가 있는 네임스페이스입니다
  - 여러 개의 분기되지 않은 볼륨을 루트에서 벗어난 네임스페이스입니다

FPolicy 패스스루 읽기를 통해 어떻게 계층적 스토리지 관리의 사용성을 개선합니다

패스스루 읽기를 통해 FPolicy 서버(계층적 스토리지 관리(HSM) 서버로 작동)가 보조 스토리지 시스템에서 기본 스토리지 시스템으로 파일을 리콜하지 않고 오프라인 파일에 대한 읽기 액세스를 제공할 수 있습니다.

FPolicy 서버가 SMB 서버에 상주하는 파일에 HSM을 제공하도록 구성된 경우, 파일이 보조 스토리지에 오프라인으로 저장되고 스텁 파일만 운영 스토리지에 남아 있는 경우 정책 기반 파일 마이그레이션이 발생합니다. 스텁 파일이 클라이언트에 일반 파일로 나타나지만 실제로는 원본 파일의 크기가 같은 스파스 파일입니다. 스파스 파일에는 SMB 오프라인 비트 세트가 있고 보조 스토리지로 마이그레이션된 실제 파일을 가리킵니다.

일반적으로 오프라인 파일에 대한 읽기 요청이 수신되면 요청된 콘텐츠를 운영 스토리지로 다시 리콜한 다음 운영 스토리지를 통해 액세스해야 합니다. 데이터를 기본 스토리지로 다시 불러내야 할 경우 좋지 않은 영향을 몇 가지 일으킬 수 있습니다. 원치 않는 결과 중 하나는 요청에 응답하기 전에 콘텐츠를 다시 불러와야 하는 필요성과 기본 스토리지의 리콜 대상 파일에 필요한 공간 소비가 증가했기 때문에 발생하는 클라이언트 요청에 대한 지연 시간이 늘어난 것입니다.

FPolicy 패스스루 읽기를 사용하면 HSM 서버(FPolicy 서버)에서 2차 스토리지 시스템에서 1차 스토리지 시스템으로 파일을 리콜하지 않고 마이그레이션된 오프라인 파일에 대한 읽기 액세스를 제공할 수 있습니다. 파일을 운영 스토리지로 다시 호출하는 대신 읽기 요청을 보조 스토리지에서 직접 처리할 수 있습니다.

> ODX(복사 오프로드)는 FPolicy 패스스루 읽기 작업에서 지원되지 않습니다.

PassThrough-read는 다음과 같은 이점을 제공하여 유용성을 향상시킵니다.

- 운영 스토리지에 요청된 데이터를 운영 스토리지로 다시 불러올 공간이 충분하지 않은 경우에도 읽기 요청을 처리할 수 있습니다.
- 스크립트 또는 백업 솔루션에서 많은 오프라인 파일에 액세스해야 하는 경우와 같이 데이터 리콜이 급증할 수 있는 경우 용량과 성능을 더욱 효과적으로 관리할 수 있습니다.
- 스냅샷 복사본의 오프라인 파일에 대한 읽기 요청을 처리할 수 있습니다.

  스냅샷 복사본은 읽기 전용이므로 스텁 파일이 스냅샷 복사본에 있는 경우 FPolicy 서버가 원래 파일을 복원할 수 없습니다. 패스스루 읽기를 사용하면 이 문제가 해결됩니다.

- 보조 스토리지의 파일에 대한 액세스를 통해 읽기 요청을 처리하고 오프라인 파일을 운영 스토리지로 리콜해야 하는 시기를 제어하는 정책을 설정할 수 있습니다.

  예를 들어, HSM 서버에서 파일을 운영 스토리지로 다시 마이그레이션하기 전에 지정된 시간 내에 오프라인 파일에 액세스할 수 있는 횟수를 지정하는 정책을 생성할 수 있습니다. 이 유형의 정책은 거의 액세스하지 않는 파일을 리콜하지 않습니다.

FPolicy 패스스루 읽기가 활성화된 경우 읽기 요청이 관리되는 방법입니다

FPolicy 패스스루 읽기를 사용하도록 설정한 경우 스토리지 가상 시스템(SVM)과 FPolicy 서버 간의 연결을 최적으로 구성할 수 있도록 읽기 요청이 관리되는 방식을 이해해야 합니다.

FPolicy 패스스루 읽기를 사용하고 SVM이 오프라인 파일에 대한 요청을 받으면 FPolicy가 표준 연결 채널을 통해 FPolicy 서버(HSM 서버)에 알림을 보냅니다.

알림을 수신한 FPolicy 서버는 알림에 전송된 파일 경로에서 데이터를 읽고, SVM과 FPolicy 서버 사이에 설정된 패스스루 읽기 전용 데이터 연결을 통해 SVM으로 요청된 데이터를 보냅니다.

데이터가 전송된 후 FPolicy 서버는 읽기 요청에 대해 허용 또는 거부로 응답합니다. 읽기 요청의 허용 또는 거부 여부에 따라 ONTAP는 요청된 정보를 보내거나 클라이언트에 오류 메시지를 보냅니다.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.