NetApp 바이러스 백신 보호 정보

ONTAP 9

NetApp
February 12, 2026

목차

NetApp 바이러스 백신 보호 정보 . . . 1
- ONTAP Vscan을 사용한 NetApp 바이러스 검사에 대해 알아보세요 . . . 1
  - 바이러스 검사 작동 방식 . . . 1
- ONTAP Vscan을 사용한 바이러스 검사 워크플로 . . . 2
- ONTAP Vscan을 활용한 안티바이러스 아키텍처 . . . 3
  - Vscan 서버 소프트웨어 . . . 4
  - Vscan 소프트웨어 설정 . . . 4
- ONTAP Vscan 파트너 솔루션에 대해 알아보세요 . . . 6

NetApp 바이러스 백신 보호 정보

ONTAP Vscan을 사용한 NetApp 바이러스 검사에 대해 알아보세요

Vscan은 NetApp에서 개발한 바이러스 백신 검사 솔루션으로, 고객이 바이러스나 기타 악성 코드에 의해 데이터가 손상되는 것을 방지할 수 있습니다. 파트너가 제공하는 바이러스 백신 소프트웨어와 ONTAP 기능을 결합하여 고객이 파일 검사를 관리하는 데 필요한 유연성을 제공합니다.

바이러스 검사 작동 방식

스토리지 시스템은 타사 공급업체의 안티바이러스 소프트웨어를 호스팅하는 외부 서버로 검사 작업을 오프로드합니다.

활성 스캐닝 모드에 따라 ONTAP는 클라이언트가 SMB(온액세스)를 통해 파일에 액세스하거나 특정 위치, 스케줄 또는 즉시(온디맨드)에 있는 파일에 액세스할 때 스캔 요청을 전송합니다.

- 액세스 시 검사 _ 를 사용하여 클라이언트가 SMB를 통해 파일을 열거나 읽거나 이름을 바꾸거나 닫을 때 바이러스를 검사할 수 있습니다. 외부 서버가 파일의 스캔 상태를 보고할 때까지 파일 작업이 일시 중단됩니다. 파일이 이미 스캔되면 ONTAP에서 파일 작업을 허용합니다. 그렇지 않으면 서버에서 스캔을 요청합니다.

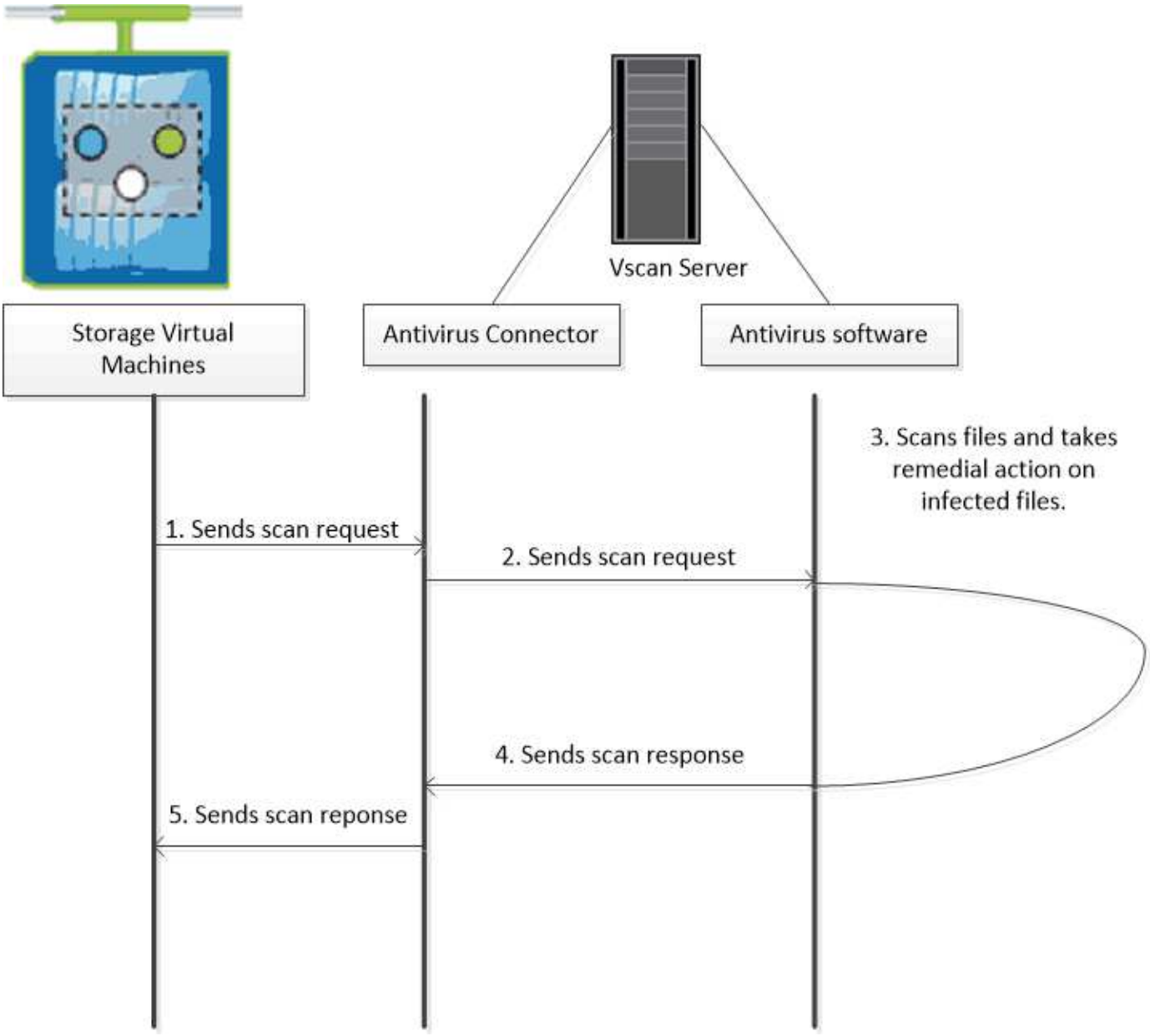
  액세스 시 스캐닝은 NFS에서 지원되지 않습니다.

- 주문형 검사 _ 을(를) 사용하여 파일에 바이러스가 있는지 즉시 또는 일정에 따라 확인할 수 있습니다. 일반적으로 온액세스 스캐닝에 적합한 크기인 기존 AV 인프라가 과부하되지 않도록 사용량이 적은 시간에만 온디맨드 검사를 실행하는 것이 좋습니다. 외부 서버는 선택한 파일의 스캔 상태를 업데이트하므로 SMB에 비해 파일 액세스 지연 시간이 줄어듭니다. 파일 수정이나 소프트웨어 버전 업데이트가 있는 경우 외부 서버에서 새 파일 검사를 요청합니다.

  NFS를 통해서만 내보낸 볼륨에서도 SVM 네임스페이스에서 모든 경로에 대해 온디맨드 스캐닝을 사용할 수 있습니다.

일반적으로 SVM에서 액세스 시 스캐닝 모드와 온디맨드 스캐닝 모드를 모두 사용할 수 있습니다. 어느 모드에서든 바이러스 백신 소프트웨어는 소프트웨어 설정에 따라 감염된 파일에 대한 치료 조치를 취합니다.

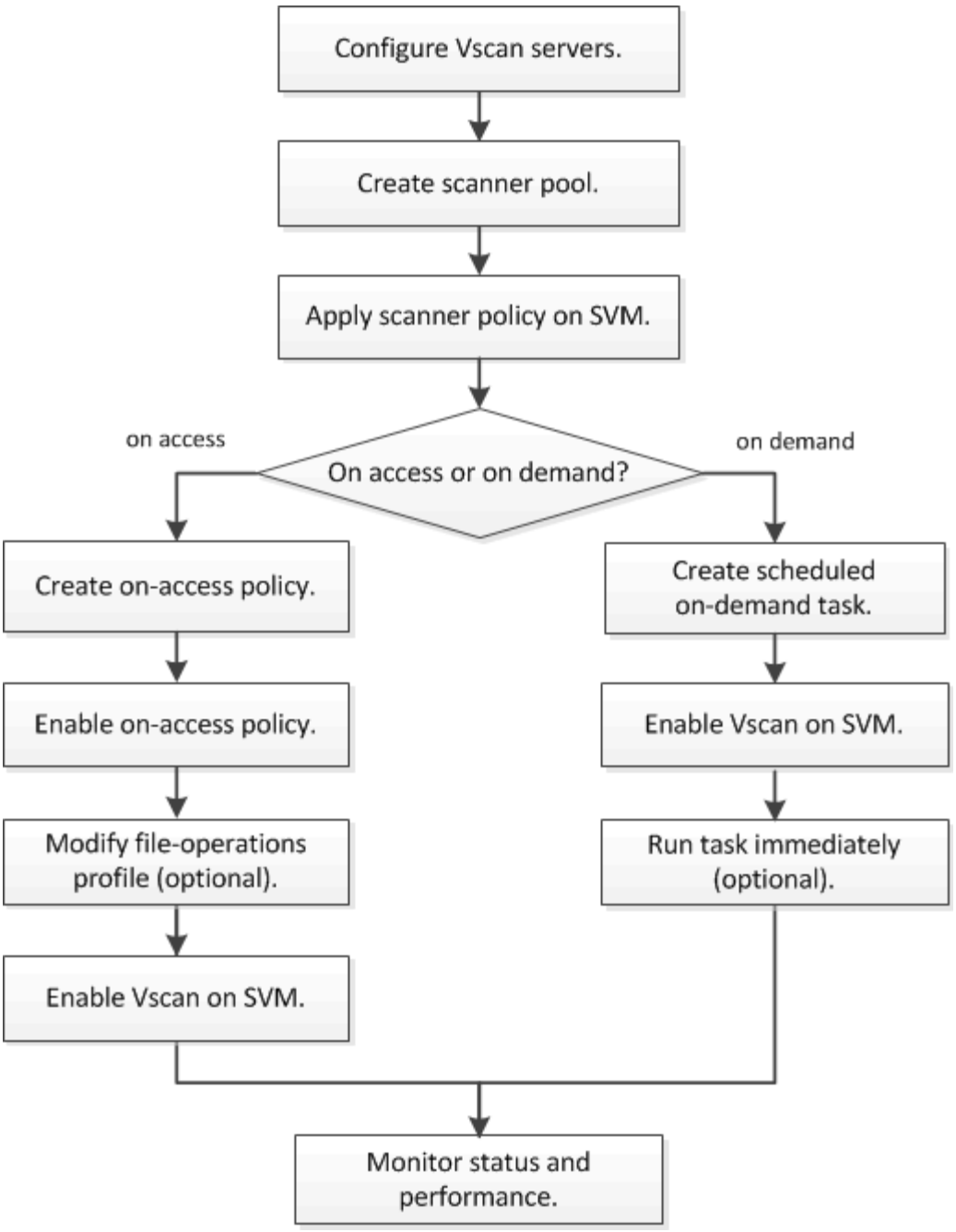
NetApp에서 제공하고 외부 서버에 설치된 ONTAP 바이러스 백신 커넥터는 스토리지 시스템과 바이러스 백신 소프트웨어 간의 통신을 처리합니다.



ONTAP Vscan을 사용한 바이러스 검사 워크플로

스캔을 활성화하기 전에 스캐너 풀을 생성하고 스캐너 정책을 적용해야 합니다. 일반적으로 SVM에서 액세스 시 스캐닝 모드와 온디맨드 스캐닝 모드를 모두 사용할 수 있습니다.

CIFS 구성을 완료해야 합니다.



필요 시 작업을 생성하려면 액세스 시 정책을 하나 이상 활성화해야 합니다. 기본 정책이거나 사용자가 만든 액세스 시 정책일 수 있습니다.

다음 단계

- 단일 클러스터에 스캐너 풀을 생성합니다
- 단일 클러스터에 스캐너 정책을 적용합니다
- 액세스 시 정책을 생성합니다

ONTAP Vscan을 활용한 안티바이러스 아키텍처

NetApp 바이러스 백신 아키텍처는 Vscan 서버 소프트웨어와 관련 설정으로 구성됩니다.

Vscan 서버 소프트웨어

Vscan 서버에 이 소프트웨어를 설치해야 합니다.

- * ONTAP 안티바이러스 커넥터 *

  이 소프트웨어는 NetApp에서 제공하며 SVM과 바이러스 백신 소프트웨어 간의 스캔 요청 및 응답 통신을 처리합니다. 가상 시스템에서 실행할 수 있지만 최상의 성능을 위해서는 물리적 시스템을 사용해야 합니다. NetApp Support 사이트에서 이 소프트웨어를 다운로드할 수 있습니다(로그인 필요).

- * 안티바이러스 소프트웨어 *

  이 소프트웨어는 바이러스 또는 기타 악성 코드가 있는 파일을 검사하는 파트너 제공 소프트웨어입니다. 소프트웨어를 구성할 때 감염된 파일에 대해 수행할 치료 조치를 지정합니다.

Vscan 소프트웨어 설정

Vscan 서버에서 이러한 소프트웨어 설정을 구성해야 합니다.

- * 스캐너 풀 *

  이 설정은 SVM에 연결할 수 있는 Vscan 서버 및 특별 권한 사용자를 정의합니다. 또한 스캔 요청 시간 초과 기간을 정의하며, 이 기간이 지나면 스캔 요청이 다른 Vscan 서버로 전송됩니다(사용 가능한 경우).

  > Vscan 서버의 바이러스 백신 소프트웨어에서 시간 초과 기간을 scanner-pool scan-request 시간 초과 기간보다 5초 이내로 설정해야 합니다. 따라서 소프트웨어의 시간 제한 기간이 스캔 요청의 시간 초과 기간보다 크기 때문에 파일 액세스가 모두 지연되거나 거부되는 상황을 피할 수 있습니다.

- * 특별 권한 사용자 *

  이 설정은 Vscan 서버에서 SVM에 연결하는 데 사용하는 도메인 사용자 계정입니다. 계정은 스캐너 풀의 권한이 있는 사용자 목록에 있어야 합니다.

- * 스캐너 정책 *

  이 설정은 스캐너 풀의 활성 여부를 결정합니다. 스캐너 정책은 시스템 정의이므로 사용자 정의 스캐너 정책을 만들 수 없습니다. 다음 세 가지 정책만 사용할 수 있습니다.

  - "기본"은 스캐너 풀이 활성화되도록 지정합니다.
  - `Secondary` 기본 스캐너 풀에 있는 Vscan 서버가 연결되어 있지 않을 때만 스캐너 풀이 활성화되도록 지정합니다.
  - "유휴"는 스캐너 풀이 비활성 상태라고 지정합니다.

- * 액세스 시 정책 *

  이 설정은 액세스 시 스캔의 범위를 정의합니다. 스캔할 최대 파일 크기, 스캔에 포함할 파일 확장명 및 경로, 스캔에서 제외할 파일 확장명 및 경로를 지정할 수 있습니다.

  기본적으로 읽기-쓰기 볼륨만 스캔됩니다. 읽기 전용 볼륨을 스캔할 수 있도록 하거나 실행 액세스 권한으로 연 파일로 스캔을 제한하는 필터를 지정할 수 있습니다.

◦ '스캔-볼륨'은 읽기 전용 볼륨을 스캔할 수 있게 해줍니다.

◦ '스캔 실행 액세스'는 실행 권한으로 연 파일로 스캔을 제한합니다.

> "접속 실행"은 "실행 권한"과 다릅니다. 특정 클라이언트는 파일이 "실행 의도"로 열린 경우에만 실행 파일에 "실행 액세스"를 가집니다.

를 설정할 수 있습니다 `scan-mandatory` 바이러스 검사에 사용할 수 있는 Vscan 서버가 없을 때 파일 액세스가 허용되도록 지정하는 옵션. 온액세스 모드에서는 다음 두 가지 상호 배타적인 옵션 중에서 선택할 수 있습니다.

◦ 필수: Vscan은 이 옵션을 사용하여 제한 시간이 만료될 때까지 서버에 스캔 요청을 전송하려고 합니다. 서버에서 스캔 요청을 수락하지 않으면 클라이언트 액세스 요청이 거부됩니다.

◦ 비필수: Vscan은 이 옵션을 통해 바이러스 스캔에 Vscan 서버를 사용할 수 있는지 여부에 관계없이 항상 클라이언트 액세스를 허용합니다.

- * 온디맨드 작업 *

  이 설정은 온디맨드 스캔의 범위를 정의합니다. 스캔할 최대 파일 크기, 스캔에 포함할 파일 확장명 및 경로, 스캔에서 제외할 파일 확장명 및 경로를 지정할 수 있습니다. 하위 디렉터리의 파일은 기본적으로 스캔됩니다.

  cron 일정을 사용하여 작업 실행 시간을 지정합니다. 명령을 사용하여 작업을 즉시 실행할 수 `vserver vscan on-demand-task run` 있습니다. 에 대한 자세한 내용은 `vserver vscan on-demand-task run` "ONTAP 명령 참조입니다"을 참조하십시오.

- * Vscan 파일 작업 프로필(액세스 시 스캔에만 해당) *

  를 클릭합니다 `vscan-fileop-profile` 에 대한 매개 변수입니다 `vserver cifs share create` 명령은 바이러스 검사를 트리거하는 SMB 파일 작업을 정의합니다. 기본적으로 매개 변수는 로 설정됩니다 `standard`NetApp 모범 사례입니다. SMB 공유를 생성하거나 수정할 때 필요에 따라 이 매개 변수를 조정할 수 있습니다.

  ◦ NO-SCAN은 공유에 대해 바이러스 검사가 트리거되지 않도록 지정합니다.

  ◦ `standard` 열기, 닫기 및 이름 바꾸기 작업을 통해 바이러스 검사가 트리거되도록 지정합니다.

  ◦ `strict` 열기, 읽기, 닫기 및 이름 바꾸기 작업을 통해 바이러스 검사가 트리거되도록 지정합니다.

  이 '사전' 프로필은 여러 클라이언트가 동시에 파일에 액세스하는 상황에 대해 향상된 보안을 제공합니다. 한 클라이언트에서 바이러스를 작성한 후 파일을 닫고 두 번째 클라이언트에서 동일한 파일을 열어 둘 경우 두 번째 클라이언트에서 읽기 작업을 수행하면 파일이 닫히기 전에 검사가 트리거됩니다.

  > `strict`동시에 액세스할 것으로 예상되는 파일이 포함된 공유로 프로필을 제한해야 합니다. 이 프로필은 더 많은 스캔 요청을 생성하므로 성능에 영향을 미칠 수 있습니다.

  ◦ `writes-only` 수정된 파일이 닫힐 때만 바이러스 검사가 트리거되도록 지정합니다.

  그 이후로 `writes-only` 스캔 요청을 적게 생성하여 일반적으로 성능을 향상시킵니다.

이 프로필을 사용하는 경우, 감염되지 않은 감염된 파일을 삭제하거나 격리하도록 스캐너를 구성해야 합니다. 예를 들어, 클라이언트가 바이러스에 감염된 후 파일을 닫고 파일이 복구, 삭제 또는 격리되지 않은 경우 파일에 액세스하는 모든 클라이언트가 파일을 닫습니다 `without` 쓰기 작업을 하면 감염됩니다.

클라이언트 응용 프로그램에서 이름 바꾸기 작업을 수행하면 파일이 새 이름으로 닫히고 스캔되지 않습니다. 이러한 작업이 환경에 보안 문제가 될 경우 '표준' 또는 '중독' 프로필을 사용해야 합니다.

에 대한 자세한 내용은 `vserver cifs share create` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP Vscan 파트너 솔루션에 대해 알아보세요

NetApp는 Trellix, Symantec, Trend Micro, Sentinel One, Deep 본능 및 OPSWAT와 협력하여 ONTAP Vscan 기술을 기반으로 하는 업계 최고의 맬웨어 방지 및 바이러스 방지 솔루션을 제공합니다. 이러한 솔루션을 통해 맬웨어에 대한 파일을 검사하고 영향을 받는 파일을 수정할 수 있습니다.

아래 표에 나와 있는 것처럼 Trellix, Symantec 및 Trend Micro의 상호 운용성 세부 정보는 NetApp 상호 운용성 매트릭스에 보관되어 있습니다. Trellix, Symantec, Deep 본능 및 OPSWAT에 대한 상호 운용성 세부 정보는 파트너 웹 사이트에서도 확인할 수 있습니다. Sentinel One, Deep 본능, OPSWAT 및 기타 신규 파트너에 대한 상호 운용성 세부 정보는 해당 웹 사이트에서 파트너가 관리합니다.

파트너	솔루션 설명서	상호 운용성 세부 정보
Trelix(이전 명칭 McAfee)	"Trelix 제품 설명서"	• "NetApp 상호 운용성 매트릭스 툴" • "엔드포인트 보안 스토리지 보호에 지원되는 플랫폼(trellix.com)"
시만텍	"Symantec Protection Engine 9.0.0"	• "NetApp 상호 운용성 매트릭스 툴" • "NAS(Network Attached Storage) 9.x.x용 Symantec Protection Engine(SPE)으로 인증된 파트너 장치 지원 매트릭스"
Trend Micro	"Trend Micro ServerProtect for Storage 6.0 시작 가이드"	"NetApp 상호 운용성 매트릭스 툴"
센티넬 원	• "SentinelOne 특이성 클라우드 데이터 보안" • "SentinelOne 지원" 이 링크를 사용하려면 사용자 로그인이 필요합니다. Sentinel One에서 액세스를 요청할 수 있습니다.	해당 없음

파트너	솔루션 설명서	상호 운용성 세부 정보
깊은 본능	NAS용 DSX • "문서 및 상호 운용성" 이 링크를 사용하려면 사용자 로그인이 필요합니다. 당신은 깊은 본능에서 액세스를 요청할 수 있습니다. • "데이터 시트"	해당 없음
OPSWAT	OPSWAT MetaDefender 스토리지 보안 • "MetaDefender 스토리지 보안과 NetApp의 통합" • "OPSWAT 파트너 페이지 를 참조하십시오" • "통합 솔루션 개요"	해당 없음