Vscan을 통한 바이러스 보호

ONTAP 9

NetApp
February 14, 2026

목차

Vscan을 통한 바이러스 보호

ONTAP Vscan을 사용한 바이러스 백신 구성에 대해 알아보세요

Vscan은 NetApp에서 개발한 바이러스 백신 검사 솔루션으로, 고객이 바이러스나 기타 악성 코드에 의해 데이터가 손상되는 것을 방지할 수 있습니다.

Vscan은 클라이언트가 SMB를 통해 파일에 액세스할 때 바이러스 검사를 수행합니다. 주문형 또는 일정에 따라 스캔을 수행하도록 Vscan을 구성할 수 있습니다. ONTAP CLI(명령줄 인터페이스) 또는 ONTAP API(응용 프로그래밍 인터페이스)를 사용하여 Vscan과 상호 작용할 수 있습니다.

관련 정보

"Vscan 파트너 솔루션"

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.

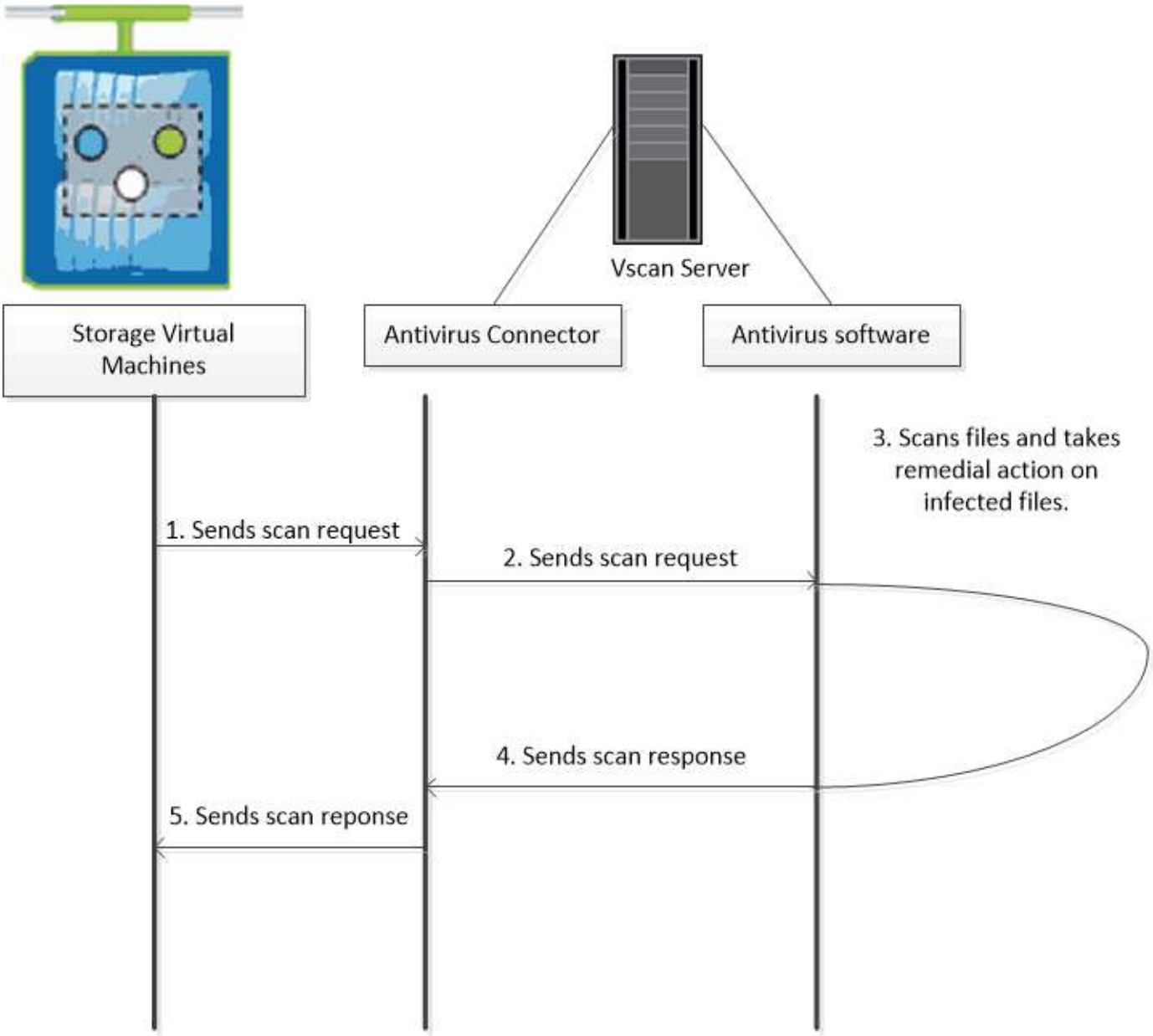
  액세스 시 스캐닝은 NFS에서 지원되지 않습니다.

- 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.

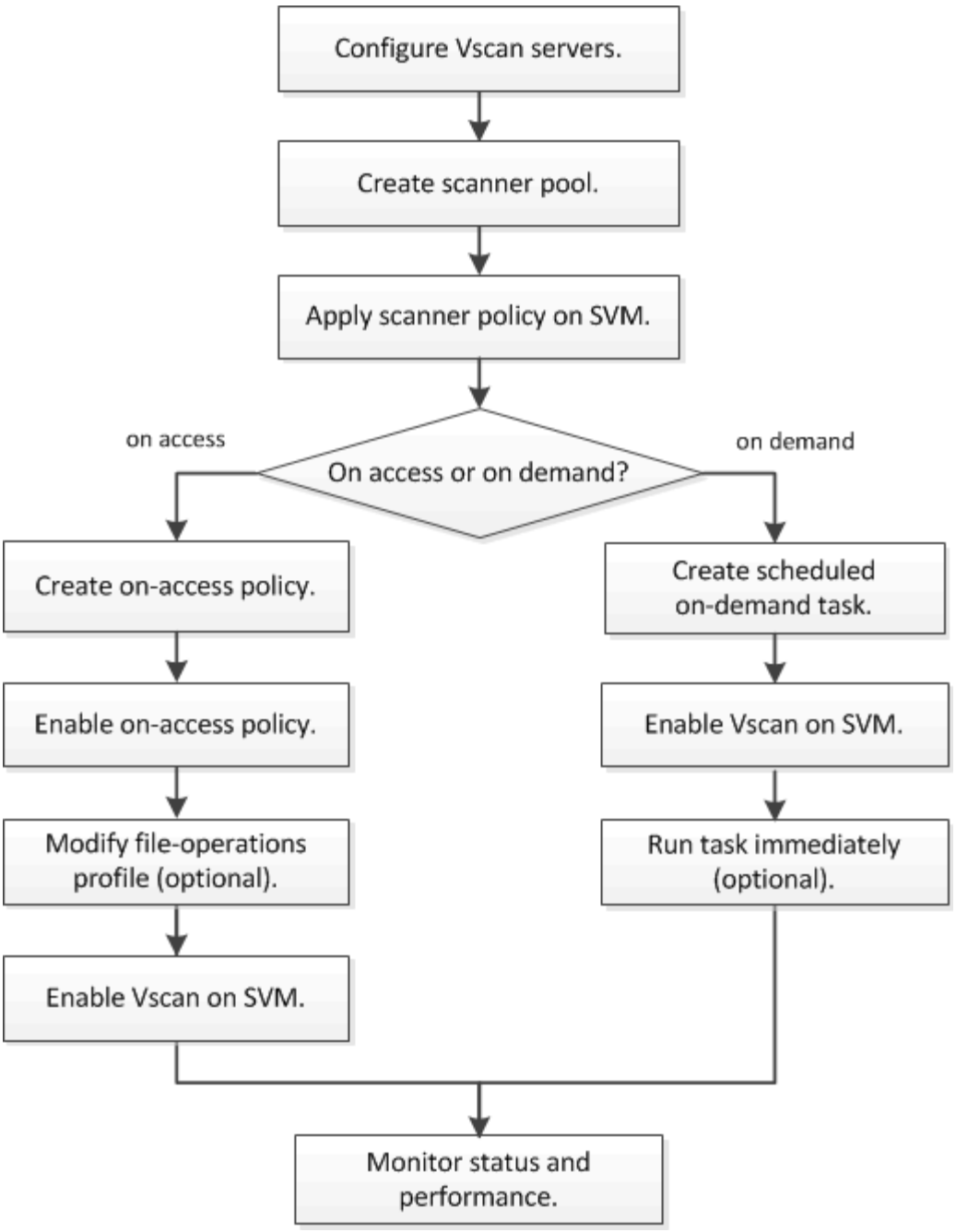
NetApp에서 제공하고 외부 서버에 설치된 ONTAP 바이러스 백신 커넥터는 스토리지 시스템과 바이러스 백신 소프트웨어 간의 통신을 처리합니다.



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

Vscan 서버 설치 및 구성

ONTAP Vscan 서버 설치 및 구성

하나 이상의 Vscan 서버를 설정하여 시스템의 파일에 바이러스가 있는지 검사합니다. 공급업체에서 제공한 지침에 따라 서버에 바이러스 백신 소프트웨어를 설치하고 구성합니다.

NetApp에서 제공하는 README 파일의 지침에 따라 ONTAP 안티바이러스 커넥터를 설치하고 구성합니다. 또는 의 지침을 따릅니다 "ONTAP 안티바이러스 커넥터 설치 페이지를 참조하십시오".

재해 복구 및 MetroCluster 구성의 경우 기본/로컬 및 보조/파트너 ONTAP 클러스터에 대해 별도의 Vscan 서버를 설정 및 구성해야 합니다.

안티바이러스 소프트웨어 요구 사항

- 안티바이러스 소프트웨어 요구 사항에 대한 자세한 내용은 공급업체 설명서를 참조하십시오.
- Vscan에서 지원하는 공급업체, 소프트웨어 및 버전에 대한 자세한 내용은 "Vscan 파트너 솔루션"페이지를 참조하십시오.

ONTAP 안티바이러스 커넥터 요구 사항

- ONTAP 안티바이러스 커넥터는 NetApp Support 사이트의 * 소프트웨어 다운로드 * 페이지에서 다운로드할 수 있습니다. "NetApp 다운로드: 소프트웨어"
- ONTAP 안티바이러스 커넥터에서 지원되는 Windows 버전 및 상호 운용성 요구 사항에 대한 자세한 내용은 을 참조하십시오"Vscan 파트너 솔루션".

하나의 클러스터에 다른 Vscan 서버용으로 다양한 버전의 Windows 서버를 설치할 수 있습니다.

- Windows 서버에 .NET 3.0 이상이 설치되어 있어야 합니다.
- Windows 서버에서 SMB 2.0을 활성화해야 합니다.

ONTAP Vscan Antivirus 커넥터 설치

Vscan 서버에 ONTAP 안티바이러스 커넥터를 설치하여 ONTAP를 실행하는 시스템과 Vscan 서버 간의 통신을 활성화합니다. ONTAP 안티바이러스 커넥터가 설치되면 안티바이러스 소프트웨어는 하나 이상의 SVM(스토리지 가상 머신)과 통신할 수 있습니다.

이 작업에 대해

- "Vscan 파트너 솔루션"지원되는 프로토콜, 안티바이러스 공급업체 소프트웨어 버전, ONTAP 버전, 상호 운용성 요구 사항 및 Windows 서버에 대한 자세한 내용은 페이지를 참조하십시오.
- NET 4.5.1 이상이 설치되어 있어야 합니다.
- ONTAP 안티바이러스 커넥터는 가상 머신에서 실행할 수 있습니다. 그러나 최상의 성능을 위해 NetApp에서는 바이러스 백신 검사에 전용 물리적 시스템을 사용할 것을 권장합니다.
- ONTAP 안티바이러스 커넥터를 설치하고 실행하는 Windows 서버에서 SMB 2.0을 활성화해야 합니다.

시작하기 전에

- 지원 사이트에서 ONTAP 안티바이러스 커넥터 설치 파일을 다운로드하여 하드 드라이브의 디렉터리에 저장합니다.
- ONTAP 안티바이러스 커넥터를 설치하기 위한 요구 사항을 충족하는지 확인합니다.
- Antivirus Connector를 설치할 수 있는 관리자 권한이 있는지 확인합니다.

단계

1. 적절한 설치 파일을 실행하여 Antivirus Connector 설치 마법사를 시작합니다.
2. 다음 _ 을(를) 선택합니다. 대상 폴더 대화 상자가 열립니다.
3. 목록에 있는 폴더에 Antivirus Connector를 설치하려면 _Next_를 선택하고 다른 폴더에 설치하려면 _Change_를 선택하십시오.
4. ONTAP AV 커넥터 Windows 서비스 자격 증명 대화 상자가 열립니다.
5. Windows 서비스 자격 증명을 입력하거나 * 추가 * 를 선택하여 사용자를 선택합니다. ONTAP 시스템의 경우 이 사용자는 유효한 도메인 사용자여야 하며 SVM의 스캐너 풀 구성에 있어야 합니다.
6. 다음 * 을 선택합니다. 프로그램 설치 준비 완료 대화 상자가 열립니다.
7. 설치를 시작하려면 * 설치 * 를 선택하고 설정을 변경하려면 * 뒤로 * 를 선택하십시오. 상태 상자가 열리고 설치 진행률을 차트로 표시한 다음 InstallShield 마법사 완료 대화 상자가 나타납니다.
8. ONTAP 관리 또는 데이터 LIF 구성을 계속하려면 ONTAP LIF 구성 확인란을 선택합니다. 이 Vscan 서버를 사용하려면 먼저 하나 이상의 ONTAP 관리 또는 데이터 LIF를 구성해야 합니다.
9. 설치 로그를 보려면 * Windows Installer 로그 표시 * 확인란을 선택합니다.
10. 설치를 종료하고 InstallShield 마법사를 닫으려면 * 마침 * 을 선택하십시오. ONTAP LIF 구성 * 아이콘이 바탕 화면에 저장되어 ONTAP LIF를 구성합니다.
11. 바이러스 백신 커넥터에 SVM을 추가합니다. 데이터 LIF 목록을 검색하기 위해 폴링되는 ONTAP 관리 LIF를 추가하거나 데이터 LIF 또는 LIF를 직접 구성하여 SVM을 바이러스 백신 커넥터에 추가할 수 있습니다. ONTAP

관리 LIF가 구성된 경우 폴링 정보와 ONTAP 관리자 계정 자격 증명도 제공해야 합니다.

- 에 대해 관리 LIF 또는 SVM의 IP 주소가 활성화되었는지 확인합니다 `management-https`. 데이터 LIF만 구성하는 경우에는 이러한 변경이 필요하지 않습니다.
- HTTP 응용 프로그램에 대한 사용자 계정을 만들고 REST API에 대한 액세스(읽기 전용) 권한이 있는 역할을 할당했는지 확인합니다 `/api/network/ip/interfaces`.
- 및 `security login create` 에 대한 자세한 `security login role create` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

> 관리 SVM에 대한 인증 터널 SVM을 추가하여 도메인 사용자를 계정으로 사용할 수도 있습니다. 에 대한 자세한 내용은 `security login domain-tunnel create` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 안티바이러스 커넥터 설치를 완료하면 바탕 화면에 저장된 * ONTAP LIF 구성 * 아이콘을 마우스 오른쪽 단추로 클릭한 다음 * 관리자 권한으로 실행 * 을 선택합니다.
2. ONTAP LIF 구성 대화 상자에서 기본 구성 유형을 선택하고 다음 작업을 수행합니다.

이 유형의 LIF를 생성하려면…	다음 단계를 수행합니다.
데이터 LIF	a. "역할"을 "데이터"로 설정 b. "데이터 프로토콜"을 "CIFS"로 설정합니다. c. "방화벽 정책"을 "데이터"로 설정합니다. d. "서비스 정책"을 "default-data-files"로 설정합니다.
관리 LIF	a. "역할 * 을 "데이터"로 설정 b. "데이터 프로토콜"을 "없음"으로 설정합니다. c. "방화벽 정책"을 "관리"로 설정 d. "서비스 정책"을 "default-management"로 설정합니다.

에 대해 자세히 "LIF 생성"알아보세요.

LIF를 생성한 후 추가하려는 SVM의 데이터 또는 관리 LIF 또는 IP 주소를 입력합니다. 클러스터 관리 LIF를 입력할 수도 있습니다. 클러스터 관리 LIF를 지정하면 SMB를 제공하는 클러스터 내의 모든 SVM이 Vscan 서버를 사용할 수 있습니다.

> Vscan 서버에 Kerberos 인증이 필요한 경우 각 SVM 데이터 LIF는 고유한 DNS 이름을 가져야 하며, Windows Active Directory에 SPN(Server Principal Name)으로 등록해야 합니다. 각 데이터 LIF에 대해 고유한 DNS 이름을 사용할 수 없거나 SPN으로 등록된 경우 Vscan 서버는 NT LAN Manager 메커니즘을 사용하여 인증을 수행합니다. Vscan 서버가 연결된 후 DNS 이름 및 SPN을 추가하거나 수정하는 경우 변경 사항을 적용하려면 Vscan 서버에서 Antivirus Connector 서비스를 다시 시작해야 합니다.

3. 관리 LIF를 구성하려면 폴링 기간을 초 단위로 입력합니다. 폴링 기간은 Antivirus Connector가 SVM 또는 클러스터의 LIF 구성의 변경 사항을 확인하는 빈도입니다. 기본 폴링 간격은 60초입니다.

4. 관리 LIF를 구성하려면 ONTAP admin 계정 이름 및 암호를 입력합니다.
5. Test * 를 클릭하여 연결을 확인하고 인증을 확인합니다. 관리 LIF 구성에 대해서만 인증이 검증됩니다.
6. 업데이트 * 를 클릭하여 폴링하거나 연결할 LIF 목록에 LIF를 추가합니다.
7. 저장 * 을 클릭하여 레지스트리에 대한 연결을 저장합니다.
8. 연결 목록을 레지스트리 가져오기 또는 레지스트리 내보내기 파일로 내보내려면 * 내보내기 * 를 클릭합니다. 여러 Vscan 서버가 동일한 관리 또는 데이터 LIF 세트를 사용하는 경우 이 기능이 유용합니다.

를 참조하십시오 "ONTAP 안티바이러스 커넥터 페이지를 구성합니다" 를 클릭합니다.

ONTAP Vscan Antivirus 커넥터 구성

ONTAP 관리 LIF, 폴링 정보 및 ONTAP 관리자 계정 자격 증명을 입력하거나 데이터 LIF만 입력하여 연결하려는 하나 이상의 SVM(스토리지 가상 머신)을 지정하도록 ONTAP 바이러스 백신 커넥터를 구성합니다. SVM 연결의 세부 정보를 수정하거나 SVM 연결을 제거할 수도 있습니다. 기본적으로 ONTAP 바이러스 백신 커넥터는 ONTAP 관리 LIF가 구성된 경우 REST API를 사용하여 데이터 LIF 목록을 검색합니다.

SVM 연결의 세부 정보를 수정합니다

ONTAP 관리 LIF 및 폴링 정보를 수정하여 안티바이러스 커넥터에 추가된 SVM(스토리지 가상 머신) 연결의 세부 정보를 업데이트할 수 있습니다. 데이터 LIF를 추가한 후에는 업데이트할 수 없습니다. 데이터 LIF를 업데이트하려면 먼저 이러한 LIF를 제거한 다음 새 LIF 또는 IP 주소를 사용하여 다시 추가해야 합니다.

시작하기 전에

HTTP 응용 프로그램에 대한 사용자 계정을 만들고 REST API에 대한 액세스(읽기 전용) 권한이 있는 역할을 할당했는지 확인합니다 `/api/network/ip/interfaces`.

및 `security login create` 에 대한 자세한 `security login role create` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

관리 SVM에 대한 인증 터널 SVM을 추가하여 도메인 사용자를 계정으로 사용할 수도 있습니다. 에 대한 자세한 내용은 `security login domain-tunnel create` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 안티바이러스 커넥터 설치를 완료하면 바탕 화면에 저장된 * ONTAP LIF 구성 * 아이콘을 마우스 오른쪽 단추로 클릭한 다음 * 관리자 권한으로 실행 * 을 선택합니다. ONTAP LIF 구성 대화 상자가 열립니다.
2. SVM IP 주소를 선택한 다음 * Update * 를 클릭합니다.
3. 필요에 따라 정보를 업데이트합니다.
4. 저장 * 을 클릭하여 레지스트리에서 연결 세부 정보를 업데이트합니다.
5. 연결 목록을 레지스트리 가져오기 또는 레지스트리 내보내기 파일로 내보내려면 * 내보내기 * 를 클릭합니다. 여러 Vscan 서버가 동일한 관리 또는 데이터 LIF 세트를 사용하는 경우 이 기능이 유용합니다.

안티바이러스 커넥터에서 SVM 연결을 제거합니다

더 이상 SVM 연결이 필요하지 않은 경우 제거할 수 있습니다.

단계

1. 안티바이러스 커넥터 설치를 완료하면 바탕 화면에 저장된 * ONTAP LIF 구성 * 아이콘을 마우스 오른쪽 단추로 클릭한 다음 * 관리자 권한으로 실행 * 을 선택합니다. ONTAP LIF 구성 대화 상자가 열립니다.
2. 하나 이상의 SVM IP 주소를 선택한 다음 * 제거 * 를 클릭합니다.
3. 저장 * 을 클릭하여 레지스트리에서 연결 세부 정보를 업데이트합니다.
4. 연결 목록을 레지스트리 가져오기 또는 레지스트리 내보내기 파일로 내보내려면 * 내보내기 * 를 클릭합니다. 여러 Vscan 서버가 동일한 관리 또는 데이터 LIF 세트를 사용하는 경우 이 기능이 유용합니다.

문제 해결

시작하기 전에

이 절차에서 레지스트리 값을 만들 때는 오른쪽 창을 사용합니다.

진단 목적으로 바이러스 백신 커넥터 로그를 활성화하거나 비활성화할 수 있습니다. 기본적으로 이러한 로그는 비활성화되어 있습니다. 성능을 향상시키려면 Antivirus Connector 로그를 사용하지 않도록 설정하고 중요 이벤트에 대해서만 활성화해야 합니다.

단계

1. 시작 * 을 선택하고 검색 상자에 "regedit"를 입력한 다음 를 선택합니다 `regedit.exe` 를 선택합니다.
2. 레지스트리 편집기 * 에서 ONTAP 안티바이러스 커넥터의 다음 하위 키를 찾습니다. `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. 다음 표에 나와 있는 형식, 이름 및 값을 제공하여 레지스트리 값을 만듭니다.

유형	이름	값
문자열	Tracepath(추적 경로)	C:\avshim.log 으로 문의하십시오

   이 레지스트리 값은 다른 유효한 경로일 수 있습니다.

4. 다음 표에 나와 있는 형식, 이름, 값 및 로깅 정보를 제공하여 다른 레지스트리 값을 만듭니다.

유형	이름	중요한 로깅	중간 로깅	자세한 로깅
DWORD를 클릭합니다	TraceLevel 을 선택합니다	1	2 또는 3	4

   이렇게 하면 3단계의 TracePath에 제공된 경로 값으로 저장되는 Antivirus Connector 로그가 활성화됩니다.

5. 3단계와 4단계에서 만든 레지스트리 값을 삭제하여 Antivirus Connector 로그를 비활성화합니다.
6. 이름이 "LogRotation"(따옴표 제외)인 "multi_sz" 유형의 다른 레지스트리 값을 만듭니다. "LogRotation"에서 회전 크기 항목으로 "logFileSize:1"을 제공하고(1은 1MB를 나타냄) 다음 줄에서는 로 "logFileCount:5"를 제공합니다 회전 한계 입력(5가 한계)

이러한 값은 선택 사항입니다. 이 옵션이 제공되지 않으면 회전 크기 및 회전 제한에 각각 20MB와 10개의 파일이 사용됩니다. 제공된 정수 값은 10진수 또는 분수 값을 제공하지 않습니다. 기본값보다 높은 값을 제공하면 기본값이 대신 사용됩니다.

7. 사용자 구성 로그 회전을 사용하지 않으려면 6단계에서 만든 레지스트리 값을 삭제합니다.

사용자 지정 가능한 배너

사용자 지정 배너를 사용하면 _ Configure ONTAP LIF api_ 창에 법적 구속력 있는 문구와 시스템 액세스 고지 사항을 배치할 수 있습니다.

단계

1. 의 내용을 업데이트하여 기본 배너를 수정합니다 `banner.txt` 파일을 설치 디렉토리에 저장한 다음 변경 내용을 저장합니다. 배너에 반영된 변경 사항을 보려면 Configure ONTAP LIF API 창을 다시 열어야 합니다.

확장 조례**(EO)** 모드를 활성화합니다

보안 작동을 위해 EO(Extended Ordinance) 모드를 활성화하거나 비활성화할 수 있습니다.

단계

1. 시작 * 을 선택하고 검색 상자에 "regedit"를 입력한 다음 를 선택합니다 `regedit.exe` 를 선택합니다.
2. 레지스트리 편집기 * 에서 ONTAP 안티바이러스 커넥터의 다음 하위 키를 찾습니다. `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. 오른쪽 창에서 "DWORD" 유형의 새 레지스트리 값을 만들어 EO 모드를 사용하지 않도록 설정하려면 "EO_Mode"(따옴표 제외) 및 값 "1"(따옴표 제외)을 사용합니다.

기본적으로 이 인 경우 `EO_Mode` 레지스트리 항목이 없습니다. EO 모드가 비활성화됩니다. EO 모드를 활성화할 때 외부 syslog 서버와 상호 인증서 인증을 모두 구성해야 합니다.

외부 **syslog** 서버를 구성합니다

시작하기 전에

이 절차에서 레지스트리 값을 만들 때는 오른쪽 창을 사용합니다.

단계

1. 시작 * 을 선택하고 검색 상자에 "regedit"를 입력한 다음 를 선택합니다 `regedit.exe` 를 선택합니다.
2. 레지스트리 편집기 * 에서 syslog 구성에 대한 ONTAP 안티바이러스 커넥터 하위 키를 생성합니다. `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
3. 다음 표와 같이 유형, 이름 및 값을 제공하여 레지스트리 값을 만듭니다.

유형	이름	값
DWORD를 클릭합니다	syslog_enabled	1 또는 0

"1" 값은 syslog를 활성화하고 "0" 값은 syslog를 비활성화합니다.

4. 다음 표에 표시된 정보를 제공하여 다른 레지스트리 값을 만듭니다.

유형	이름
등록_SZ	syslog_host입니다

값 필드에 syslog 호스트 IP 주소 또는 도메인 이름을 입력합니다.

5. 다음 표에 표시된 정보를 제공하여 다른 레지스트리 값을 만듭니다.

유형	이름
등록_SZ	syslog_port

값 필드에 syslog 서버가 실행 중인 포트 번호를 제공합니다.

6. 다음 표에 표시된 정보를 제공하여 다른 레지스트리 값을 만듭니다.

유형	이름
등록_SZ	Syslog_프로토콜

syslog 서버에서 사용 중인 프로토콜을 값 필드에 "TCP" 또는 "UDP"로 입력합니다.

7. 다음 표에 표시된 정보를 제공하여 다른 레지스트리 값을 만듭니다.

유형	이름	로그_CRIT	로그_통지	Log_Info(로그 정보)	log_debug 를 참조하십시오
DWORD를 클릭합니다	syslog_레벨	2	5	6	7

8. 다음 표에 표시된 정보를 제공하여 다른 레지스트리 값을 만듭니다.

유형	이름	값
DWORD를 클릭합니다	Syslog_TLS	1 또는 0

"1" 값은 TLS(Transport Layer Security)를 사용하여 syslog를 활성화하고 "0" 값은 TLS를 사용하는 syslog를 비활성화합니다.

구성된 외부 **syslog** 서버가 원활하게 실행되는지 확인합니다

- 키가 없거나 null 값이 있는 경우:
  - 프로토콜은 기본적으로 "TCP"로 설정됩니다.
  - 일반 "TCP/UDP"의 경우 기본적으로 "514"이고 TLS의 경우 기본적으로 "6514"입니다.
  - syslog 레벨의 기본값은 5(log_notice)입니다.

- syslog가 활성화되어 있는지 확인하려면 를 확인하십시오 `syslog_enabled` 값은 "1"입니다. 를 누릅니다 `syslog_enabled` 값은 "1"입니다. EO 모드의 활성화 여부에 관계없이 구성된 원격 서버에 로그인할 수 있어야 합니다.
- EO 모드가 "1"로 설정된 경우 를 변경합니다 `syslog_enabled` "1"에서 "0"까지의 값은 다음과 같습니다.
  - EO 모드에서 syslog가 활성화되지 않은 경우 서비스를 시작할 수 없습니다.
  - 시스템이 안정 상태에서 실행 중인 경우, EO 모드에서 syslog를 비활성화할 수 없으며 syslog가 강제로 "1"로 설정된다는 경고가 나타납니다. 이 경고는 레지스트리에서 확인할 수 있습니다. 이 경우 먼저 EO 모드를 비활성화한 다음 syslog를 비활성화해야 합니다.
- EO 모드 및 syslog를 사용할 때 syslog 서버가 성공적으로 실행되지 않으면 서비스 실행이 중지됩니다. 이 문제는 다음과 같은 이유 중 하나로 인해 발생할 수 있습니다.
  - 유효하지 않거나 syslog_host가 구성되지 않았습니다.
  - UDP 또는 TCP와 별도로 잘못된 프로토콜이 구성되었습니다.
  - 포트 번호가 잘못되었습니다.
- TCP 또는 TLS over TCP 구성의 경우 서버가 IP 포트에서 수신 대기하지 않으면 연결이 실패하고 서비스가 종료됩니다.

X.509 상호 인증서 인증을 구성합니다

X.509 인증서 기반 상호 인증은 관리 경로에서 바이러스 백신 커넥터와 ONTAP 간의 SSL(Secure Sockets Layer) 통신에 사용할 수 있습니다. EO 모드가 활성화되어 있고 인증서를 찾을 수 없는 경우 AV 커넥터가 종료됩니다. 안티바이러스 커넥터에 대해 다음 절차를 수행하십시오.

단계

1. 안티바이러스 커넥터는 안티바이러스 커넥터가 설치 디렉토리를 실행하는 디렉토리 경로에서 NetApp 서버의 안티바이러스 커넥터 클라이언트 인증서 및 CA(인증 기관) 인증서를 검색합니다. 인증서를 이 고정 디렉토리 경로에 복사합니다.
2. 클라이언트 인증서와 개인 키를 PKCS12 형식으로 포함하고 이름을 "AV_CLIENT.P12"로 지정합니다.
3. NetApp 서버의 인증서에 서명하는 데 사용된 CA 인증서(루트 CA까지의 모든 중간 서명 기관 포함)가 PEM(Privacy Enhanced Mail) 형식이고 "Ontap_CA.pem"이라는 이름을 가지고 있는지 확인하세요. Antivirus Connector 설치 디렉토리에 넣으세요. ONTAP 시스템에서 "ONTAP"의 Antivirus Connector에 대한 클라이언트 인증서에 서명하는 데 사용되는 CA 인증서(루트 CA까지의 모든 중간 서명 기관 포함)를 "client-ca" 유형 인증서로 설치합니다.

스캐너 풀을 구성합니다

ONTAP Vscan 스캐너 풀 구성에 대해 알아보세요

스캐너 풀은 SVM에 연결할 수 있는 Vscan 서버 및 특별 권한 사용자를 정의합니다. 스캐너 정책은 스캐너 풀이 활성 상태인지 여부를 결정합니다.

SMB 서버에서 내보내기 정책을 사용하는 경우 각 Vscan 서버를 엑스포트 정책에 추가해야 합니다.

단일 클러스터에 **ONTAP Vscan** 스캐너 풀을 만듭니다.

스캐너 풀은 SVM에 연결할 수 있는 Vscan 서버 및 특별 권한 사용자를 정의합니다.

시작하기 전에

- SVM과 Vscan 서버는 동일한 도메인 또는 신뢰할 수 있는 도메인에 있어야 합니다.
- 클러스터 관리 LIF를 사용하여 ONTAP 바이러스 백신 커넥터를 구성합니다.
- 권한이 있는 사용자 목록에는 Vscan 서버가 SVM에 연결하는 데 사용하는 도메인 및 사용자 이름이 포함되어야 합니다.
- 스캐너 풀이 구성되면 서버에 대한 연결 상태를 확인합니다.

단계

1. 스캐너 풀 생성:

   ```
   vserver vscan scanner-pool create -vserver cluster_admin_SVM -scanner-pool
   scanner_pool -hostnames Vscan_server_hostnames -privileged-users
   privileged_users
   ```

   - 클러스터 관리자 SVM을 지정합니다.
   - 각 Vscan 서버 호스트 이름에 대한 IP 주소 또는 FQDN을 지정합니다.
   - 권한이 있는 각 사용자의 도메인 및 사용자 이름을 지정합니다.

   에 대한 자세한 내용은 `vserver vscan scanner-pool create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 스캐너 풀이 생성되었는지 확인합니다.

   ```
   vserver vscan scanner-pool show -vserver cluster_admin_SVM -scanner-pool
   scanner_pool
   ```

   다음 명령을 실행하면 'S' 스캐너 풀에 대한 세부 정보가 표시됩니다.

   ```
   cluster1::> vserver vscan scanner-pool show -vserver cluster_admin_SVM
   -scanner-pool SP

                                       Vserver: cluster_admin_SVM
                                  Scanner Pool: SP
                                Applied Policy: idle
                                Current Status: off
            Cluster on Which Policy Is Applied: -
                    Scanner Pool Config Owner: cluster
          List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
   List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
   27.fsct.nb
                     List of Privileged Users: cifs\u1, cifs\u2
   ```

명령을 사용하여 클러스터의 모든 스캐너 풀을 볼 수도 `vserver vscan scanner-pool show` 있습니다. 에 대한 자세한 내용은 `vserver vscan scanner-pool show` "ONTAP 명령 참조입니다"을 참조하십시오.

MetroCluster 구성에서 ONTAP Vscan 스캐너 풀 생성

클러스터의 운영 및 2차 SVM에 해당하는 MetroCluster 구성의 각 클러스터에 기본 및 2차 스캐너 풀을 생성해야 합니다.

시작하기 전에

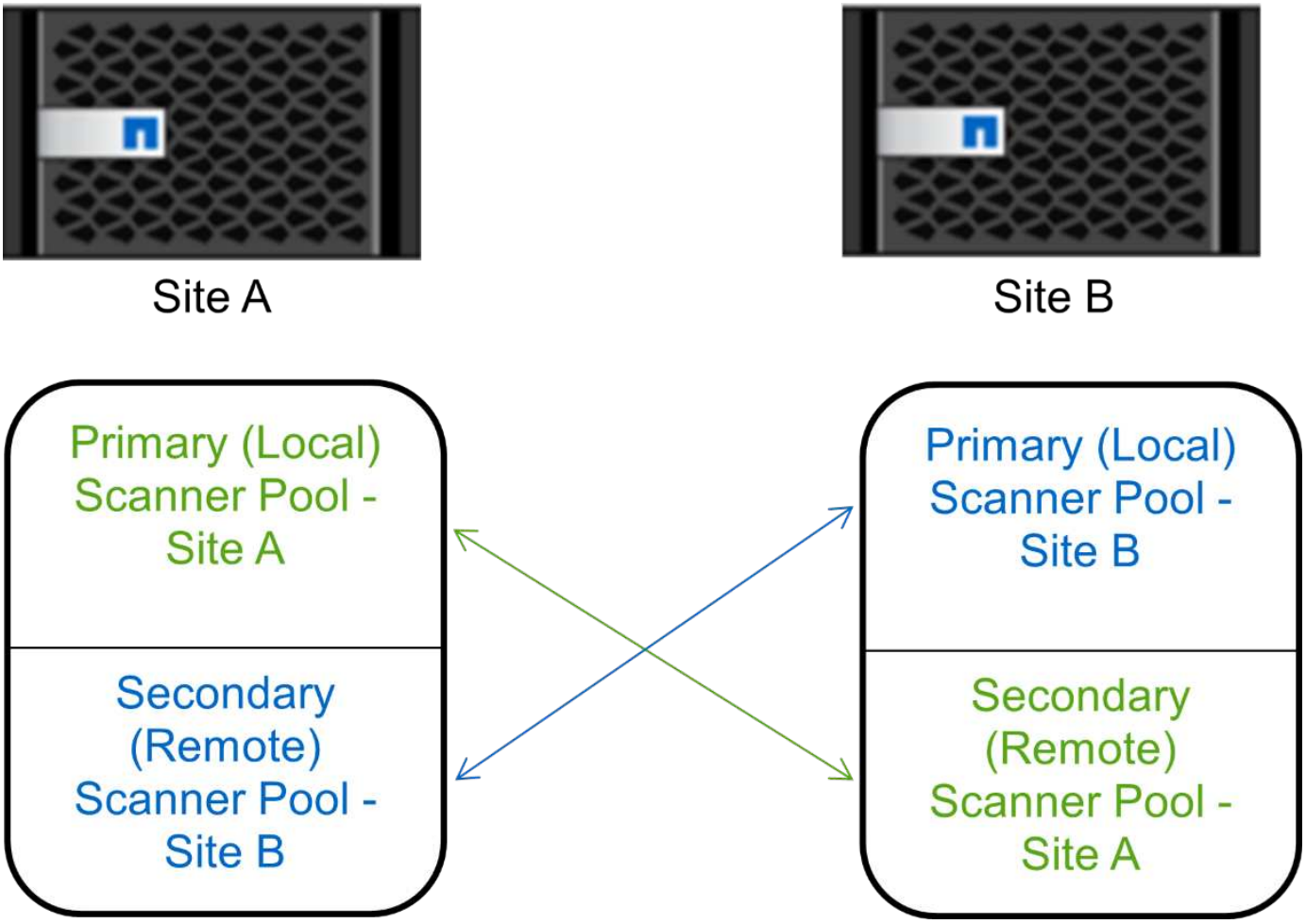
- SVM과 Vscan 서버는 동일한 도메인 또는 신뢰할 수 있는 도메인에 있어야 합니다.
- 개별 SVM용으로 정의된 스캐너 풀의 경우 ONTAP 바이러스 백신 커넥터를 SVM 관리 LIF 또는 SVM 데이터 LIF와 함께 구성해야 합니다.
- 클러스터의 모든 SVM에 대해 정의된 스캐너 풀의 경우 클러스터 관리 LIF에서 ONTAP 바이러스 백신 커넥터를 구성해야 합니다.
- 권한이 있는 사용자 목록에는 Vscan 서버가 SVM에 연결하는 데 사용하는 도메인 사용자 계정이 포함되어야 합니다.
- 스캐너 풀이 구성되면 서버에 대한 연결 상태를 확인합니다.

이 작업에 대해

MetroCluster 구성은 물리적으로 분리된 2개의 미러링된 클러스터를 구현하여 데이터를 보호합니다. 각 클러스터는 다른 클러스터의 데이터와 SVM 구성을 동기식으로 복제합니다. 로컬 클러스터의 1차 SVM은 클러스터가 온라인 상태일 때 데이터를 제공합니다. 로컬 클러스터의 2차 SVM은 원격 클러스터가 오프라인일 때 데이터를 제공합니다.

즉, MetroCluster 구성에서 각 클러스터에 기본 및 보조 스캐너 풀을 생성해야 하며, 클러스터가 2차 SVM에서 데이터 제공을 시작하면 2차 풀이 활성화됩니다. DR(재해 복구)의 경우 구성은 MetroCluster와 비슷합니다.

이 그림은 일반적인 MetroCluster/DR 구성을 보여 줍니다.



단계

1. 스캐너 풀 생성:

   'vserver vscan scanner -pool create -vserver_data_SVM|cluster_admin_SVM_-scanner -pool_scanner_pool_-hostname_vscan_server_hostname_-privileged-users_privileged_users_'

   - 개별 SVM용으로 정의된 풀에 대해 데이터 SVM을 지정하고, 클러스터의 모든 SVM에 대해 정의된 풀에 대해 클러스터 관리 SVM을 지정합니다.
   - 각 Vscan 서버 호스트 이름에 대한 IP 주소 또는 FQDN을 지정합니다.
   - 권한이 있는 각 사용자의 도메인 및 사용자 이름을 지정합니다.

   운영 SVM이 포함된 클러스터에서 모든 스캐너 풀을 생성해야 합니다.

   에 대한 자세한 내용은 `vserver vscan scanner-pool create` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 MetroCluster 구성의 각 클러스터에 운영 및 2차 스캐너 풀이 생성됩니다.

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

2. 스캐너 풀이 생성되었는지 확인합니다.

   `vserver vscan scanner-pool show -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner -pool` *`scanner_pool`*

   다음 명령을 실행하면 스캐너 풀 'pool1'에 대한 세부 정보가 표시됩니다.

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                                Scanner Pool: pool1_for_site1
                              Applied Policy: idle
                              Current Status: off
         Cluster on Which Policy Is Applied: -
                   Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                    List of Privileged Users: cifs\u1,cifs\u2
```

   또한 명령을 사용하여 SVM에 있는 모든 스캐너 풀을 볼 수도 있습니다 `vserver vscan scanner-pool show`. 에 대한 자세한 내용은 `vserver vscan scanner-pool show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP Vscan을 사용하여 단일 클러스터에 스캐너 정책 적용

스캐너 정책은 스캐너 풀이 활성 상태인지 여부를 결정합니다. 정의된 Vscan 서버가 SVM에 연결할 수 있으려면 먼저 스캐너 풀을 활성화해야 합니다.

이 작업에 대해

- 스캐너 풀에는 하나의 스캐너 정책만 적용할 수 있습니다.
- 클러스터에서 모든 SVM에 대해 스캐너 풀을 생성한 경우 각 SVM에 개별적으로 스캐너 정책을 적용해야 합니다.

단계

1. 스캐너 정책 적용:

   'vserver vscan scanner -pool apply -policy -vserver data_SVM -scanner -pool scanner_pool -scanner -policy primary | secondary|idle -cluster cluster_to_apply_policy_on'

   스캐너 정책은 다음 값 중 하나를 가질 수 있습니다.

   - "기본"은 스캐너 풀이 활성화되도록 지정합니다.
   - '2차'는 기본 스캐너 풀에 Vscan 서버가 연결되어 있지 않은 경우에만 스캐너 풀이 활성화되도록 지정합니다.
   - "유휴"는 스캐너 풀이 비활성 상태라고 지정합니다.

     다음 예제는 이름이 인 스캐너 풀을 보여 줍니다 `SP` 를 누릅니다 `vs1` SVM 활성화:

```
cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
-scanner-pool SP  -scanner-policy primary
```

2. 스캐너 풀이 활성화되었는지 확인합니다.

   'vserver vscan scanner -pool show -vserver data_SVM|cluster_admin_SVM-scanner -pool scanner_pool'

   이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

   다음 명령을 실행하면 'S' 스캐너 풀에 대한 세부 정보가 표시됩니다.

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                    Vserver: vs1
                               Scanner Pool: SP
                             Applied Policy: primary
                             Current Status: on
          Cluster on Which Policy Is Applied: cluster1
                    Scanner Pool Config Owner: vserver
        List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                     List of Privileged Users: cifs\u1, cifs\u2
```

   명령을 사용하여 SVM에서 활성 스캐너 풀을 볼 수 있습니다 `vserver vscan scanner-pool show-active`. 에 대한 자세한 내용은 `vserver vscan scanner-pool show-active` "ONTAP 명령 참조입니다"을 참조하십시오.

MetroCluster ONTAP Vscan 구성에 스캐너 정책 적용

스캐너 정책은 스캐너 풀이 활성 상태인지 여부를 결정합니다. MetroCluster 구성에서 각 클러스터의 기본 및 보조 스캐너 풀에 스캐너 정책을 적용해야 합니다.

이 작업에 대해

- 스캐너 풀에는 하나의 스캐너 정책만 적용할 수 있습니다.
- 클러스터에서 모든 SVM에 대해 스캐너 풀을 생성한 경우 각 SVM에 개별적으로 스캐너 정책을 적용해야 합니다.
- 재해 복구 및 MetroCluster 구성의 경우 로컬 클러스터 및 원격 클러스터의 모든 스캐너 풀에 스캐너 정책을 적용해야 합니다.
- 로컬 클러스터에 대해 생성하는 정책에서 에서 로컬 클러스터를 지정해야 합니다 `cluster` 매개 변수. 원격 클러스터에 대해 생성한 정책에서 에서 원격 클러스터를 지정해야 합니다 `cluster` 매개 변수. 그런 다음 재해 발생 시 원격 클러스터가 바이러스 검사 작업을 대신 수행할 수 있습니다.

단계

1. 스캐너 정책 적용:

   'vserver vscan scanner -pool apply -policy -vserver_data_SVM_ -scanner -pool_scanner_pool_ -scanner -policy primary|secondary|idle -cluster_cluster_to_apply_policy_on_'

   에 대한 자세한 내용은 `vserver vscan scanner-pool apply-policy` "ONTAP 명령 참조입니다"을 참조하십시오.

   스캐너 정책은 다음 값 중 하나를 가질 수 있습니다.

   - "기본"은 스캐너 풀이 활성화되도록 지정합니다.
   - '2차'는 기본 스캐너 풀에 Vscan 서버가 연결되어 있지 않은 경우에만 스캐너 풀이 활성화되도록 지정합니다.
   - "유휴"는 스캐너 풀이 비활성 상태라고 지정합니다.

   > ⓘ 운영 SVM이 포함된 클러스터에서 모든 스캐너 정책을 적용해야 합니다.

   다음 명령은 MetroCluster 구성에서 각 클러스터의 기본 및 보조 스캐너 풀에 스캐너 정책을 적용합니다.

```
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site1 -scanner-policy secondary -cluster
cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site2 -scanner-policy primary -cluster cluster2

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site2 -scanner-policy secondary -cluster
cluster2
```

2. 스캐너 풀이 활성화되었는지 확인합니다.

   'vserver vscan scanner -pool show -vserver data_SVM|cluster_admin_SVM-scanner -pool scanner_pool'

   에 대한 자세한 내용은 `vserver vscan scanner-pool show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 스캐너 풀 'pool1'에 대한 세부 정보가 표시됩니다.

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                                Scanner Pool: pool1_for_site1
                             Applied Policy: primary
                             Current Status: on
          Cluster on Which Policy Is Applied: cluster1
                   Scanner Pool Config Owner: vserver
        List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                    List of Privileged Users: cifs\u1,cifs\u2
```

   명령을 사용하여 SVM에서 활성 스캐너 풀을 볼 수 있습니다 `vserver vscan scanner-pool show-active`. 에 대한 자세한 내용은 `vserver vscan scanner-pool show-active` "ONTAP 명령 참조입니다"을 참조하십시오.

Vscan에서 스캐너 풀을 관리하기 위한 ONTAP 명령

스캐너 풀을 수정 및 삭제하고, 스캐너 풀의 권한이 있는 사용자와 Vscan 서버를 관리할 수 있습니다. 스캐너 풀에 대한 요약 정보도 볼 수 있습니다.

원하는 작업	다음 명령을 입력합니다…
스캐너 풀을 수정합니다	'vserver vscan scanner-pool modify(가상 Vscan 스캐너 풀 수정)
스캐너 풀을 삭제합니다	'vserver vscan scanner -pool delete'(Vscan scanner -pool 삭제
스캐너 풀에 권한이 있는 사용자를 추가합니다	'vserver vscan scanner-pool privileged-users add'
스캐너 풀에서 권한이 있는 사용자를 삭제합니다	'vserver vscan scanner-pool privileged-users remove'(Vscan scanner-
Vscan 서버를 스캐너 풀에 추가합니다	'vserver vscan scanner-pool servers add'
스캐너 풀에서 Vscan 서버를 삭제합니다	'vserver vscan scanner-pool servers remove(Vscan scanner-pool 서버
스캐너 풀에 대한 요약 및 세부 정보를 봅니다	'vserver vscan scanner-pool show'
스캐너 풀에 대한 권한이 있는 사용자를 봅니다	'vserver vscan scanner-pool privileged-users show'(Vscan scanner-pool
모든 스캐너 풀에 대한 Vscan 서버를 봅니다	'vserver vscan scanner-pool servers show'

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

액세스 시 스캔을 구성합니다

ONTAP Vscan 온액세스 정책 생성

액세스 시 정책은 액세스 시 검사의 범위를 정의합니다. 개별 SVM 또는 클러스터의 모든 SVM에 대해 액세스 시 정책을 생성할 수 있습니다. 클러스터에서 모든 SVM에 대해 액세스 시 정책을 생성한 경우 각 SVM에 대해 개별적으로 정책을 활성화해야 합니다.

이 작업에 대해

- 스캔할 최대 파일 크기, 스캔에 포함할 파일 확장명 및 경로, 스캔에서 제외할 파일 확장명 및 경로를 지정할 수 있습니다.
- 바이러스 검사를 위해 Vscan 서버를 사용할 수 없는 경우 파일 액세스가 허용되도록 '스캔 필수' 옵션을 꺼짐으로 설정할 수 있습니다.
- 기본적으로 ONTAP는 "default_cifs"라는 액세스 시 정책을 생성하고 클러스터에 있는 모든 SVM에 대해 활성화합니다.
- 에 따라 스캔 제외 대상이 되는 모든 파일 `paths-to-exclude`, `file-ext-to-exclude`, 또는 `max-file-size` 매개 변수는 에도 스캔 대상으로 고려되지 않습니다 `scan-mandatory` 옵션이 켜짐으로 설정되어 있습니다. (이것을 확인하십시오 "문제 해결" 과 관련된 연결 문제에 대한 섹션입니다 `scan-mandatory` 옵션)

- 기본적으로 읽기-쓰기 볼륨만 스캔됩니다. 읽기 전용 볼륨을 스캔할 수 있도록 하거나 실행 권한으로 연 파일로 스캔을 제한하는 필터를 지정할 수 있습니다.
- 지속적으로 사용 가능한 매개 변수가 Yes로 설정된 SMB 공유에서는 바이러스 검사가 수행되지 않습니다.
- 를 참조하십시오 "안티바이러스 아키텍처" Vscan 파일 - 작업 프로필 _ 에 대한 자세한 내용은 섹션을 참조하십시오.
- SVM당 최대 10개의 액세스 정책을 생성할 수 있습니다. 그러나 한 번에 하나의 온액세스 정책만 활성화할 수 있습니다.
  - 액세스 시 정책에서 바이러스 검사에서 최대 100개의 경로 및 파일 확장명을 제외할 수 있습니다.
- 일부 파일 제외 권장 사항:
  - CIFS 사용자에 대한 응답 속도가 느려지거나 스캔 요청 시간 초과가 발생할 수 있으므로 바이러스 검사에서 큰 파일(파일 크기를 지정할 수 있음)을 제외하는 것이 좋습니다. 제외의 기본 파일 크기는 2GB입니다.
  - 과 같은 파일 확장명을 제외하는 것이 좋습니다 `.vhd` 및 `.tmp` 이러한 확장자가 있는 파일은 스캔에 적합하지 않을 수 있기 때문입니다.
  - 격리 디렉터리나 가상 하드 드라이브 또는 데이터베이스만 저장되는 경로와 같은 파일 경로를 제외하는 것이 좋습니다.
  - 한 번에 하나의 정책만 활성화할 수 있으므로 모든 제외가 동일한 정책에 지정되어 있는지 확인합니다. NetApp는 바이러스 백신 엔진에 지정된 것과 동일한 제외 세트를 사용할 것을 적극 권장합니다.
  - ONTAP 9.14.1부터 와일드카드를 사용하여 제외할 액세스 시 경로 및 파일 확장자를 지정할 수 있습니다.
- 의 경우 액세스 시 정책이 필요합니다 온디맨드 검사. 에 대한 액세스 시 스캔을 방지하려면 을 설정해야 합니다 `-scan-files-with-no-ext` 버튼을 눌러 false로 이동하고 `-file-ext-to-exclude` 모든 확장자를 제외하려면 * 를 선택합니다.

단계

1. 액세스 시 정책 생성:

   'vserver vscan on-access-policy create -vserver_data_SVM|cluster_admin_SVM_-policy -name_policy_name_-protocol cifs-max-file-size_max_size_of_files_to_scan_ – filters [scan-ro-volume,] [scan-execute-access] -file-ext-to -include_ext_ext_ext_ext_exclude_ext_ext_exclude_ext_ext_ext_ext_exclude_exclude_ext_ext_exclude_file_exclude_file_file_scan_exclude_exclude_exclude_file_file_file_file_file_file_max-max_max-max-max-max-max_

   - 개별 SVM에 정의된 정책에 따라 데이터 SVM을 지정하고, 클러스터의 모든 SVM에 정의된 정책에 따라 클러스터 관리 SVM을 지정합니다.
   - '-file-ext-to-exclude' 설정은 '-file-ext-to-include' 설정보다 우선합니다.
   - 설정 `-scan-files-with-no-ext` 를 true로 설정하면 확장자가 없는 파일을 스캔할 수 있습니다. 다음 명령을 실행하면 이라는 온액세스 정책이 생성됩니다 `Policy1` 를 누릅니다 `vs1` SVM:

   ```
   cluster1::> vserver vscan on-access-policy create -vserver vs1 -policy
   -name Policy1 -protocol CIFS -filters scan-ro-volume -max-file-size 3GB
   -file-ext-to-include "mp*","tx*" -file-ext-to-exclude "mp3","txt" -scan
   -files-with-no-ext false -paths-to-exclude "\vol\a b\","\vol\a,b\"
   ```

2. 다음과 같이 on-access 정책이 생성되었는지 확인합니다. `vserver vscan on-access-policy show`

`-instance data_SVM|cluster_admin_SVM -policy-name name`

에 대한 자세한 내용은 `vserver vscan on-access-policy` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 명령을 실행하면 Policy1 정책에 대한 세부 정보가 표시됩니다.

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                            Vserver: vs1
                             Policy: Policy1
                      Policy Status: off
                Policy Config Owner: vserver
               File-Access Protocol: CIFS
                            Filters: scan-ro-volume
                     Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
             File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

ONTAP Vscan 온액세스 정책 활성화

액세스 시 정책은 액세스 시 검사의 범위를 정의합니다. SVM의 파일을 스캔하려면 먼저 SVM에서 액세스 시 정책을 활성화해야 합니다.

클러스터에서 모든 SVM에 대해 액세스 시 정책을 생성한 경우 각 SVM에 대해 개별적으로 정책을 활성화해야 합니다. 한 번에 하나의 SVM에 대해 액세스 시 정책만 활성화할 수 있습니다.

단계

1. 액세스 시 정책 활성화:

   'vserver vscan on-access-policy enable-vserver data_SVM-policy-name policy_name'

   다음 명령을 실행하면 이라는 온액세스 정책이 설정됩니다 `Policy1` 를 누릅니다 `vs1` SVM:

   ```
   cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy
   -name Policy1
   ```

2. 액세스 시 정책이 활성화되어 있는지 확인합니다.

   `vserver vscan on-access-policy show -instance data_SVM -policy-name policy_name`

   에 대한 자세한 내용은 `vserver vscan on-access-policy show` "ONTAP 명령 참조입니다"을

참조하십시오.

다음 명령을 실행하면 "Policy1" 액세스 시 정책에 대한 세부 정보가 표시됩니다.

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                            Vserver: vs1
                             Policy: Policy1
                      Policy Status: on
                Policy Config Owner: vserver
               File-Access Protocol: CIFS
                            Filters: scan-ro-volume
                     Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
            File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

SMB 공유에 대한 ONTAP Vscan 파일 작업 프로필 수정

SMB 공유의 _ Vscan 파일 작업 프로필 _ 은(는) 스캔을 트리거할 수 있는 공유 작업을 정의합니다. 기본적으로 매개 변수는 로 설정됩니다 `standard`. SMB 공유를 생성하거나 수정할 때 필요에 따라 매개 변수를 조정할 수 있습니다.

를 참조하십시오 "안티바이러스 아키텍처" Vscan 파일 - 작업 프로필 _ 에 대한 자세한 내용은 섹션을 참조하십시오.

가 있는 SMB 공유에서는 바이러스 검사가 수행되지 않습니다 `continuously-available` 매개 변수를 로 설정합니다 `Yes`.

단계

1. SMB 공유에 대한 Vscan 파일 작업 프로필의 값을 수정합니다.

   ```
   vserver cifs share modify -vserver data_SVM -share-name share -path share_path
   -vscan-fileop-profile no-scan|standard|strict|writes-only
   ```

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

   다음 명령을 실행하면 SMB 공유에 대한 Vscan 파일 작업 프로필이 로 변경됩니다 `strict`:

   ```
   cluster1::> vserver cifs share modify -vserver vs1 -share-name
   SALES_SHARE -path /sales -vscan-fileop-profile strict
   ```

온액세스 정책을 관리하기 위한 **ONTAP Vscan** 명령

액세스 시 정책을 수정, 비활성화 또는 삭제할 수 있습니다. 정책의 요약 및 세부 정보를 볼 수 있습니다.

원하는 작업	다음 명령을 입력합니다…
액세스 시 정책을 생성합니다	`vserver vscan on-access-policy create`
액세스 시 정책을 수정합니다	'vserver Vscan on-access-policy modify'를 참조하십시오
액세스 시 정책을 설정합니다	`vserver vscan on-access-policy enable`
액세스 시 정책을 사용하지 않도록 설정합니다	'vserver Vscan on-access-policy disable'
액세스 시 정책을 삭제합니다	'vserver Vscan on-access-policy delete
액세스 시 정책에 대한 요약 및 세부 정보를 봅니다	'vserver vscan on-access-policy show'를 참조하십시오
제외할 경로 목록에 추가합니다	`vserver vscan on-access-policy paths-to-exclude add`
제외할 경로 목록에서 삭제합니다	`vserver vscan on-access-policy paths-to-exclude remove`
제외할 경로 목록을 봅니다	`vserver vscan on-access-policy paths-to-exclude show`
제외할 파일 확장명 목록에 추가합니다	`vserver vscan on-access-policy file-ext-to-exclude add`
제외할 파일 확장명 목록에서 삭제합니다	`vserver vscan on-access-policy file-ext-to-exclude remove`
제외할 파일 확장명 목록을 봅니다	`vserver vscan on-access-policy file-ext-to-exclude show`
포함할 파일 확장명 목록에 추가합니다	`vserver vscan on-access-policy file-ext-to-include add`
포함할 파일 확장명 목록에서 삭제합니다	`vserver vscan on-access-policy file-ext-to-include remove`

포함할 파일 확장명 목록을 봅니다	`vserver vscan on-access-policy file-ext-to-include show`

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

온디맨드 스캐닝 구성

ONTAP Vscan 온디맨드 스캐닝 구성에 대해 알아보세요

주문형 검사를 사용하여 파일에 바이러스가 있는지 즉시 또는 일정에 따라 확인할 수 있습니다.

예를 들어, 사용량이 적은 시간에만 스캔을 실행하거나 액세스 시 스캔에서 제외되었던 매우 큰 파일을 스캔할 수 있습니다. cron 일정을 사용하여 작업 실행 시간을 지정할 수 있습니다.

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

을 참조하십시오

- 작업을 만들 때 일정을 할당할 수 있습니다.
- SVM에서 한 번에 하나의 작업만 예약할 수 있습니다.
- 필요 시 스캐닝은 심볼 링크 또는 스트림 파일의 스캔을 지원하지 않습니다.

필요 시 스캐닝은 심볼 링크 또는 스트림 파일의 스캔을 지원하지 않습니다.

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

ONTAP Vscan으로 주문형 작업 만들기

주문형 작업은 주문형 바이러스 검사의 범위를 정의합니다. 스캔할 파일의 최대 크기, 스캔에 포함할 파일의 확장명 및 경로, 스캔에서 제외할 파일의 확장명 및 경로를 지정할 수 있습니다. 하위 디렉터리의 파일은 기본적으로 스캔됩니다.

이 작업에 대해

- 각 SVM에 대해 최대 10개의 온디맨드 작업이 존재할 수 있지만, 하나의 SVM만 활성화할 수 있습니다.
- 필요 시 작업에서는 스캔과 관련된 통계와 관련된 정보가 포함된 보고서를 생성합니다. 이 보고서는 명령을 사용하거나 정의된 위치에서 작업에 의해 생성된 보고서 파일을 다운로드하여 액세스할 수 있습니다.
- ONTAP 9.14.1부터 와일드카드를 사용하여 제외할 온디맨드 경로와 파일 확장자를 지정할 수 있습니다.

시작하기 전에

- 이(가) 있어야 합니다 액세스 시 정책을 생성했습니다. 정책은 기본 정책이거나 사용자가 만든 정책일 수 있습니다. On-access 정책이 없으면 검사를 활성화할 수 없습니다.

단계

1. 필요 시 작업 만들기:

   `vserver vscan on-demand-task create -vserver data_SVM -task-name task_name -scan-paths paths_of_files_to_scan -report-directory report_directory_path -report-expiry-time expiration_time_for_report -schedule cron_schedule -max -file-size max_size_of_files_to_scan -paths-to-exclude paths -file-ext-to -exclude file_extensions -file-ext-to-include file_extensions -scan-files-with -no-ext true|false -directory-recursion true|false`

   - '-file-ext-to-exclude' 설정은 '-file-ext-to-include' 설정보다 우선합니다.
   - 설정 `-scan-files-with-no-ext` 를 true로 설정하면 확장자가 없는 파일을 스캔할 수 있습니다.

     에 대한 자세한 내용은 `vserver vscan on-demand-task create` "ONTAP 명령 참조입니다"을 참조하십시오.

     다음 명령을 실행하면 이라는 On-Demand 작업이 생성됩니다 `Task1` VS1의 VM에서:

```
cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name
Task1 -scan-paths "/vol1/","/vol2/cifs/" -report-directory "/report"
-schedule daily -max-file-size 5GB -paths-to-exclude "/vol1/cold-files/"
-file-ext-to-include "vmdk?","mp*" -file-ext-to-exclude "mp3","mp4"
-scan-files-with-no-ext false
[Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
command to view the status.
```

+

> 명령을 사용하여 작업의 상태를 볼 수 `job show` 있습니다. 및 `job resume` 명령을 사용하여 작업을 일시 중지하고 다시 시작하거나 `job stop` 명령을 사용하여 작업을 종료할 수 `job pause` 있습니다. 에 대한 자세한 내용은 `job` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 주문형 작업이 생성되었는지 확인합니다.

   `vserver vscan on-demand-task show -instance data_SVM -task-name task_name`

   에 대한 자세한 내용은 `vserver vscan on-demand-task show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 'Task1' 작업에 대한 세부 정보가 표시됩니다.

```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task-name
Task1

                            Vserver: vs1
                          Task Name: Task1
                List of Scan Paths: /vol1/, /vol2/cifs/
              Report Directory Path: /report
                       Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
             File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk?, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                   Report Log Level: info
        Expiration Time for Report: -
```

작업을 마친 후

작업을 실행하도록 예약하기 전에 SVM에서 스캔을 활성화해야 합니다.

ONTAP Vscan을 사용하여 주문형 작업 일정을 예약하세요

일정을 할당하지 않고 작업을 만들고 를 사용할 수 있습니다 `vserver vscan on-demand-task schedule` 스케줄을 할당하거나 작업을 생성하는 동안 스케줄을 추가하는 명령입니다.

이 작업에 대해

'vserver vscan on-demand-task schedule' 명령으로 할당된 스케줄은 'vserver vscan on-demand-task create' 명령으로 이미 할당된 스케줄보다 우선합니다.

단계

1. 필요 시 작업 예약:

   `vserver vscan on-demand-task schedule -vserver` *`data_SVM`* `-task-name` *`task_name`* `-schedule cron_schedule`

   다음 명령을 실행하면 이라는 액세스 시 작업이 예약됩니다 `Task2` 를 누릅니다 `vs2` SVM:

```
cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task
-name Task2 -schedule daily
[Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142"
command to view the status.
```

에 대한 자세한 내용은 `vserver vscan on-demand-task schedule` "ONTAP 명령 참조입니다"을 참조하십시오.

> 작업 상태를 보려면 `job show` 명령을 사용하십시오. `job pause`및 `job resume` 명령은 각각 작업을 일시 중지하고 다시 시작합니다. 명령은 작업을 종료합니다. `job stop` 에 대한 자세한 내용은 `job` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 필요 시 작업이 예약되었는지 확인합니다.

   `vserver vscan on-demand-task show -instance` *`data_SVM`* `-task-name` *`task_name`*

   에 대한 자세한 내용은 `vserver vscan on-demand-task show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 '작업 2' 작업에 대한 세부 정보가 표시됩니다.

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task-name
Task2

                            Vserver: vs2
                          Task Name: Task2
                 List of Scan Paths: /vol1/, /vol2/cifs/
               Report Directory Path: /report
                        Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
              File Paths Not to Scan: /vol1/cold-files/
        File Extensions Not to Scan: mp3, mp4
            File Extensions to Scan: vmdk, mp*
       Scan Files with No Extension: false
            Request Service Timeout: 5m
                     Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                   Report Log Level: info
```

작업을 마친 후

작업을 실행하도록 예약하기 전에 SVM에서 스캔을 활성화해야 합니다.

ONTAP Vscan 온디맨드 작업을 즉시 실행하세요

일정을 할당했는지 여부에 관계없이 필요 시 작업을 즉시 실행할 수 있습니다.

시작하기 전에

SVM에서 스캔을 활성화해야 합니다.

단계

1. 필요 시 작업을 즉시 실행합니다.

   `vserver vscan on-demand-task run -vserver data_SVM -task-name task_name`

   다음 명령을 실행하면 이라는 온액세스 작업이 실행됩니다 `Task1` 를 누릅니다 `vs1` SVM:

   ```
   cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name
   Task1
   [Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161"
   command to view the status.
   ```

   에 대한 자세한 내용은 `vserver vscan on-demand-task run` "ONTAP 명령 참조입니다"을 참조하십시오.

   명령을 사용하여 작업의 상태를 볼 수 `job show` 있습니다. 및 `job resume` 명령을 사용하여 작업을 일시 중지하고 다시 시작하거나 `job stop` 명령을 사용하여 작업을 종료할 수 `job pause` 있습니다. 에 대한 자세한 내용은 `job` "ONTAP 명령 참조입니다"을 참조하십시오.

주문형 작업 관리를 위한 **ONTAP Vscan** 명령

필요 시 작업을 수정, 삭제 또는 예약 취소할 수 있습니다. 작업에 대한 요약 및 세부 정보를 보고 작업에 대한 보고서를 관리할 수 있습니다.

원하는 작업	다음 명령을 입력합니다...
주문형 작업을 만듭니다	`vserver vscan on-demand-task create`
필요 시 작업을 수정합니다	'vserver vscan on-demand-task modify(가상 Vscan 주문형 작업 수정)
필요 시 작업을 삭제합니다	'vserver vscan on-demand-task delete'(가상 Vscan 주문형 작업 삭제
주문형 작업을 실행합니다	`vserver vscan on-demand-task run`
필요 시 작업을 예약합니다	`vserver vscan on-demand-task schedule`
필요 시 작업 일정을 취소합니다	'vserver vscan on-demand-task unschedule'
필요 시 작업에 대한 요약 및 세부 정보를 봅니다	'vserver vscan on-demand-task show'
주문형 보고서 보기	'vserver vscan on-demand-task report show'(가상 Vscan 주문형 작업 보고서 표시
필요 시 보고서를 삭제합니다	'vserver Vscan 주문형 작업 보고서 삭제

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

ONTAP Vscan에서 오프박스 바이러스 백신 기능을 구성하기 위한 모범 사례

ONTAP에서 오프 박스 기능을 구성할 때는 다음 권장 사항을 고려하십시오.

- 권한이 있는 사용자를 바이러스 검사 작업으로 제한합니다. 일반 사용자는 권한이 있는 사용자 자격 증명을 사용하지 않도록 해야 합니다. 이러한 제한은 Active Directory에서 권한이 있는 사용자에 대한 로그인 권한을 해제하면 얻을 수 있습니다.
- 권한이 있는 사용자는 administrators 그룹 또는 backup operators 그룹과 같이 도메인에서 많은 권한이 있는 사용자 그룹에 속할 필요가 없습니다. 권한이 있는 사용자는 Vscan 서버 접속을 생성하고 바이러스 검사를 위한 파일에 액세스할 수 있도록 스토리지 시스템에서만 유효성을 검사해야 합니다.
- Vscan 서버를 실행하는 컴퓨터는 바이러스 검사 목적으로만 사용하십시오. 일반적인 사용을 방지하려면 이러한 컴퓨터에서 Windows 터미널 서비스 및 기타 원격 액세스 조항을 비활성화하고 관리자에게만 새 소프트웨어를 설치할 권한을 부여하십시오.
- Vscan 서버를 바이러스 검사 전용으로 사용하고 백업 등의 다른 작업에 사용하지 마십시오. Vscan 서버를 가상 머신(VM)으로 실행하기로 결정할 수 있습니다. Vscan 서버를 VM으로 실행하는 경우 VM에 할당된 리소스가 공유되지 않고 바이러스 검사를 수행하기에 충분한지 확인합니다.
- 리소스의 초과 할당을 방지하기 위해 Vscan 서버에 적절한 CPU, 메모리 및 디스크 용량을 제공합니다. 대부분의 Vscan 서버는 여러 CPU 코어 서버를 사용하고 CPU 전반에 로드를 분산하도록 설계되었습니다.
- NetApp는 다른 클라이언트 네트워크 트래픽의 영향을 받지 않도록 SVM에서 Vscan 서버로의 연결에 전용 VLAN을 사용하는 것이 좋습니다. Vscan 서버의 안티바이러스 VLAN 및 SVM의 데이터 LIF 전용 NIC(네트워크 인터페이스 카드)를 생성합니다. 이 단계는 네트워크 문제가 발생할 경우 관리 및 문제 해결을 간소화합니다. 바이러스 백신 트래픽은 개인 네트워크를 사용하여 분리해야 합니다. 다음 방법 중 하나를 사용하여 DC(도메인 컨트롤러) 및 ONTAP와 통신하도록 바이러스 백신 서버를 구성해야 합니다.
  - DC는 트래픽을 분리하는 데 사용되는 개인 네트워크를 통해 바이러스 백신 서버와 통신해야 합니다.
  - DC 및 안티바이러스 서버는 CIFS 클라이언트 네트워크와 동일하지 않은 다른 네트워크(앞에서 언급한 전용 네트워크가 아님)를 통해 통신해야 합니다.
  - 바이러스 백신 통신에 Kerberos 인증을 사용하려면 프라이빗 LIF에 대한 DNS 항목과 프라이빗 LIF에 대해 생성된 DNS 항목에 해당하는 DC에 서비스 사용자 이름을 생성해야 합니다. 바이러스 백신 커넥터에 LIF를 추가할 때 이 이름을 사용하십시오. DNS는 안티바이러스 커넥터에 연결된 각 전용 LIF에 대해 고유한 이름을 반환할 수 있어야 합니다.

> Vscan 트래픽용 LIF가 클라이언트 트래픽에 대한 LIF가 아닌 다른 포트에 구성되어 있는 경우, 포트 장애가 발생하면 Vscan LIF가 다른 노드로 페일오버될 수 있습니다. 변경 사항으로 인해 새 노드에서 Vscan 서버에 연결할 수 없으며 노드의 파일 작업에 대한 검색 알림이 실패합니다. Vscan 서버가 노드에서 수행된 파일 작업에 대한 스캔 요청을 처리할 수 있도록 노드에 있는 하나 이상의 LIF를 통해 연결할 수 있는지 확인합니다.

- 1GbE 네트워크 이상을 사용하여 NetApp 스토리지 시스템과 Vscan 서버를 연결합니다.
- 여러 Vscan 서버가 있는 환경의 경우 비슷한 고성능 네트워크 연결이 있는 모든 서버를 연결합니다. Vscan 서버를 연결하면 부하 공유를 허용하여 성능이 향상됩니다.
- 원격 사이트 및 지사의 경우 NetApp는 원격 Vscan 서버 대신 로컬 Vscan 서버를 사용할 것을 권장합니다. 이는 지연 시간이 길기 때문입니다. 비용이 중요한 경우 보통 수준의 바이러스 보호를 위해 노트북 또는 PC를 사용하십시오. 볼륨 또는 qtree를 공유하고 원격 사이트의 모든 시스템에서 스캔하여 전체 파일 시스템 검사를

주기적으로 예약할 수 있습니다.

- 여러 Vscan 서버를 사용하여 로드 밸런싱 및 이중화를 위해 SVM의 데이터를 스캔합니다. CIFS 워크로드 양과 그에 따른 바이러스 백신 트래픽은 SVM당 다릅니다. 스토리지 컨트롤러에서 CIFS 및 바이러스 검사 지연 시간을 모니터링합니다. 시간에 따른 결과 추세를 모니터링합니다. 추세 임계값을 초과하는 Vscan 서버의 CPU 또는 애플리케이션 큐로 인해 CIFS 지연 시간 및 바이러스 검사 지연 시간이 증가하면 CIFS 클라이언트가 대기 시간이 길어질 수 있습니다. Vscan 서버를 추가합니다 하중을 분산시킵니다.
- 최신 버전의 ONTAP 안티바이러스 커넥터를 설치합니다.
- 바이러스 백신 엔진과 정의를 최신 상태로 유지합니다. 업데이트 빈도에 대한 권장 사항은 파트너에게 문의하십시오.
- 멀티 테넌시 환경에서는 Vscan 서버와 SVM이 동일한 도메인 또는 신뢰할 수 있는 도메인에 속해 있는 경우 여러 SVM과 스캐너 풀(Vscan 서버 풀)을 공유할 수 있습니다.
- 감염된 파일에 대한 바이러스 백신 소프트웨어 정책은 대부분의 바이러스 백신 공급업체에서 설정한 기본값인 " 삭제" 또는 "격리"로 설정되어야 합니다. "vscan-fileop-profile"이 "write_only"로 설정되어 있고 감염된 파일이 발견되면 파일이 공유에 남아 있고 파일을 열면 검사가 트리거되지 않으므로 열 수 있습니다. 바이러스 백신 검사는 파일을 닫은 후에만 트리거됩니다.
- 를 클릭합니다 `scan-engine timeout` 값은 보다 작아야 합니다 `scanner-pool request-timeout` 값. 더 높은 값으로 설정하면 파일 액세스가 지연되고 결국 시간 초과될 수 있습니다. 이를 방지하려면 를 구성하십시오 `scan-engine timeout` 보다 5초 더 짧습니다 `scanner-pool request-timeout` 값. 를 변경하는 방법에 대한 지침은 스캔 엔진 공급업체의 설명서를 참조하십시오 `scan-engine timeout` 설정. 를 클릭합니다 `scanner-pool timeout` 고급 모드에서 다음 명령을 사용하고 에 적절한 값을 입력하여 변경할 수 있습니다 `request-timeout` 매개 변수: `vserver vscan scanner-pool modify`.
- 온-액세스 검사 워크로드에 적합한 크기로 주문형 검사를 사용해야 하는 환경의 경우, NetApp 기존 바이러스 백신 인프라에 추가 로드가 발생하지 않도록 사용량이 적은 시간에 온디맨드 검사 작업을 예약하는 것이 좋습니다.

파트너 관련 모범 사례에 대한 자세한 내용은 을 "Vscan 파트너 솔루션"참조하십시오.

SVM ONTAP Vscan에서 바이러스 검사 활성화

액세스 또는 온디맨드 검사를 실행하려면 SVM에서 바이러스 검사를 활성화해야 합니다.

단계

1. SVM에서 바이러스 검사 활성화:

   'vserver Vscan enable - vserver data_SVM'

   에 대한 자세한 내용은 `vserver vscan enable` "ONTAP 명령 참조입니다"을 참조하십시오.

   > 필요한 경우 명령을 사용하여 바이러스 검사를 비활성화할 수 `vserver vscan disable` 있습니다. 에 대한 자세한 내용은 `vserver vscan disable` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 에서 바이러스 검사가 활성화됩니다 `vs1` SVM:

   ```
   cluster1::> vserver vscan enable -vserver vs1
   ```

2. SVM에서 바이러스 검사가 활성화되었는지 확인합니다.

   'vserver vscan show -vserver data_SVM'

   에 대한 자세한 내용은 `vserver vscan show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 의 Vscan 상태가 표시됩니다 `vs1` SVM:

```
cluster1::> vserver vscan show -vserver vs1

                                Vserver: vs1
                          Vscan Status: on
```

ONTAP Vscan 스캔 파일 상태 재설정

경우에 따라 명령을 사용하여 파일에 대해 캐시된 정보를 삭제하여 SVM에서 성공적으로 스캔된 파일의 스캔 상태를 재설정해야 할 수 있습니다 `vserver vscan reset`. 예를 들어, 잘못 구성된 검사가 있는 경우 이 명령을 사용하여 바이러스 검사 처리를 다시 시작할 수 있습니다. 에 대한 자세한 내용은 `vserver vscan reset` "ONTAP 명령 참조입니다"을 참조하십시오.

이 작업에 대해

'vserver Vscan reset' 명령을 실행하면 다음에 액세스할 때 모든 유효한 파일이 스캔됩니다.

> 이 명령은 다시 스캔 대상 파일의 수와 크기에 따라 성능에 부정적인 영향을 미칠 수 있습니다.

시작하기 전에

이 작업에는 고급 권한이 필요합니다.

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

   에 대한 자세한 내용은 `set -privilege advanced` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 스캔한 파일의 상태 재설정:

   'vserver Vscan reset - vserver data_SVM'

   다음 명령을 실행하면 에서 스캔한 파일의 상태가 재설정됩니다 `vs1` SVM:

```
cluster1::> vserver vscan reset -vserver vs1
```

ONTAP를 사용하여 Vscan 이벤트 로그 정보를 봅니다

'vserver Vscan show-events' 명령을 사용하여 감염된 파일에 대한 이벤트 로그 정보, Vscan 서버에 대한 업데이트 등을 확인할 수 있습니다. 클러스터에 대한 이벤트 정보 또는 지정된 노드, SVM 또는 Vscan 서버에 대한 이벤트 정보를 볼 수 있습니다.

시작하기 전에

Vscan 이벤트 로그를 보려면 고급 권한이 필요합니다.

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

   에 대한 자세한 내용은 `set` "ONTAP 명령 참조입니다"을 참조하십시오.

2. Vscan 이벤트 로그 정보 보기:

   'vserver vscan show-events'

   에 대한 자세한 내용은 `vserver vscan show-events` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 클러스터 'cluster1'에 대한 이벤트 로그 정보가 표시됩니다.

```
cluster1::*> vserver vscan show-events

Vserver     Node              Server          Event Type         Event Time
----------- ---------------- --------------- ------------------
-----------------
vs1         Cluster-01      192.168.1.1     file-infected      9/5/2014
11:37:38
vs1         Cluster-01      192.168.1.1     scanner-updated    9/5/2014
11:37:08
vs1         Cluster-01      192.168.1.1     scanner-connected 9/5/2014
11:34:55
3 entries were displayed.
```

연결 문제를 모니터링하고 해결합니다

스캔 필수 옵션과 관련된 잠재적인 ONTAP Vscan 연결 문제

"vserver vscan connection-status show" 명령을 사용하면 연결 문제 해결에 도움이 될 수 있는 Vscan 서버 연결에 대한 정보를 볼 수 있습니다.

기본적으로, 액세스 시 스캔에 대한 '스캔 필수' 옵션은 Vscan 서버 연결을 스캐닝에 사용할 수 없을 때 파일 액세스를 거부합니다. 이 옵션은 중요한 안전 기능을 제공하지만 몇 가지 상황에서 문제가 발생할 수 있습니다.

- 클라이언트 액세스를 활성화하기 전에 LIF가 있는 각 노드의 SVM에 하나 이상의 Vscan 서버가 연결되어 있는지 확인해야 합니다. 클라이언트 액세스를 활성화한 후 서버를 SVM에 연결해야 하는 경우 Vscan 서버 연결을 사용할 수 없기 때문에 파일 액세스가 거부되지 않도록 SVM에서 '필수' 옵션을 해제해야 합니다. 서버를 연결한 후 옵션을 다시 켤 수 있습니다.
- 대상 LIF가 SVM을 위한 모든 Vscan 서버 연결을 호스팅하는 경우 LIF가 마이그레이션되면 서버와 SVM 간 연결이 끊어집니다. Vscan 서버 연결을 사용할 수 없어 파일 액세스가 거부되지 않도록 하려면 LIF를 마이그레이션하기 전에 '필수' 옵션을 해제해야 합니다. LIF가 마이그레이션된 후 옵션을 다시 설정할 수 있습니다.

각 SVM에는 최소한 2개의 Vscan 서버가 할당되어 있어야 합니다. Vscan 서버를 클라이언트 액세스에 사용되는 네트워크와 다른 네트워크를 통해 스토리지 시스템에 연결하는 것이 가장 좋습니다.

에 대한 자세한 내용은 `vserver vscan connection-status show` "ONTAP 명령 참조입니다"을 참조하십시오.

Vscan 서버 연결 상태를 보기 위한 ONTAP 명령

'vserver vscan connection-status show' 명령을 사용하여 Vscan 서버 연결 상태에 대한 요약 및 세부 정보를 볼 수 있습니다.

원하는 작업	다음 명령을 입력합니다...
Vscan 서버 연결 요약 보기	'vserver vscan connection-status show'
Vscan 서버 연결에 대한 세부 정보를 봅니다	'vserver vscan connection-status show-all'을 선택합니다
연결된 Vscan 서버에 대한 세부 정보를 봅니다	'vserver Vscan connection-status show-connected'(가상 Vscan 연결 상태 표시 - 연결됨
연결되지 않은 사용 가능한 Vscan 서버에 대한 세부 정보를 봅니다	'vserver Vscan connection-status show-not-connected'(가상 Vscan 연결 상태 표시 - 연결되지 않음)

에 대한 자세한 내용은 `vserver vscan connection-status show` "ONTAP 명령 참조입니다"을 참조하십시오.

바이러스 ONTAP Vscan 스캐닝 문제 해결

일반적인 바이러스 검사 문제의 경우 가능한 원인과 해결 방법이 있습니다. 바이러스 검사는 Vscan이라고도 합니다.

문제	해결 방법

Vscan 서버는 에 연결할 수 없습니다 clustered ONTAP 스토리지 시스템을 활용할 수 있습니다.	스캐너 풀 구성에서 Vscan 서버 IP 주소를 지정하는지 확인합니다. 스캐너 풀 목록에서 허용된 권한이 있는 사용자가 활성 상태인지 확인합니다. 스캐너 풀을 확인하려면 를 실행합니다 `vserver vscan scanner-pool show` 스토리지 시스템 명령 프롬프트에서 명령을 입력합니다. 그래도 Vscan 서버에 연결할 수 없는 경우 네트워크에 문제가 있을 수 있습니다.
클라이언트에서 높은 지연 시간을 관찰합니다.	스캐너 풀에 Vscan 서버를 더 추가해야 할 때가 되었을 것입니다.
너무 많은 스캔이 트리거되었습니다.	의 값을 수정합니다 `vscan-fileop-profile` 바이러스 검사를 위해 모니터링되는 파일 작업의 수를 제한하는 매개 변수입니다.
일부 파일이 스캔되지 않습니다.	온액세스 정책을 확인합니다. 이러한 파일의 경로가 경로 제외 목록에 추가되었거나 파일 크기가 제외에 대해 구성된 값을 초과할 수 있습니다. On-access 정책을 확인하려면 를 실행합니다 `vserver vscan on-access-policy show` 스토리지 시스템 명령 프롬프트에서 명령을 입력합니다.
파일 액세스가 거부되었습니다.	정책 구성에 _scan-mandatory_setting이 지정되어 있는지 확인한다. 이 설정은 연결된 Vscan 서버가 없는 경우 데이터 액세스를 거부합니다. 필요에 따라 설정을 수정합니다.

관련 정보

- "Vscan vscan scanner -pool show를 선택합니다"
- "vserver Vscan on-access-policy show 를 참조하십시오"

ONTAP Vscan 상태 및 성능 활동 모니터링

Vscan 서버 연결 상태와 같은 Vscan 모듈의 중요한 측면을 모니터링할 수 있습니다. Vscan 서버의 상태 및 스캔된 파일 수 이 정보는 도움이 됩니다 Vscan 서버와 관련된 문제를 진단합니다.

Vscan 서버 연결 정보를 봅니다

Vscan 서버의 연결 상태를 보고 이미 사용 중인 연결을 관리할 수 있습니다 및 사용 가능한 연결입니다. 다양한 명령이 정보를 표시합니다 Vscan 서버의 연결 상태 정보

명령…	표시된 정보…
'vserver vscan connection-status show'	연결 상태 요약

'vserver vscan connection-status show-all'을 선택합니다	연결 상태에 대한 자세한 정보입니다
'vserver Vscan connection-status show-not-connected'(가상 Vscan 연결 상태 표시 - 연결되지 않음)	사용할 수 있지만 연결되지 않은 연결의 상태입니다
'vserver Vscan connection-status show-connected'(가상 Vscan 연결 상태 표시 - 연결됨	연결된 Vscan 서버에 대한 정보입니다

에 대한 자세한 내용은 `vserver vscan connection-status show` "ONTAP 명령 참조입니다"을 참조하십시오.

Vscan 서버 통계를 봅니다

Vscan 서버별 통계를 확인하여 성능을 모니터링하고 바이러스 검사 관련 문제를 진단할 수 있습니다. Vscan을 사용하려면 먼저 데이터 샘플을 수집해야 합니다. `statistics show` Vscan 서버 통계를 표시하는 명령입니다.

에 대한 자세한 내용은 `statistics show` "ONTAP 명령 참조입니다"을 참조하십시오.

데이터 샘플을 완료하려면 다음 단계를 완료하십시오.

단계

1. `statistics start`명령 및 선택적 `statistics stop` 명령을 실행합니다.

   자세히 알아보세요 `statistics start` 그리고 `statistics stop` 에서 "ONTAP 명령 참조입니다" .

Vscan 서버 요청 및 대기 시간에 대한 통계를 봅니다

ONTAP를 사용할 수 있습니다 `offbox_vscan` Vscan의 속도를 모니터링하기 위해 SVM 단위로 카운터를 사용합니다 모든 Vscan에 대해 1초에 발송 및 수신된 서버 요청 및 서버 지연 시간 서버. 이러한 통계를 보려면 다음 단계를 완료하십시오.

단계

1. 다음 카운터로 명령을 실행합니다 `statistics show -object offbox_vscan -instance SVM`.

카운터...	표시된 정보...
`scan_request_dispatched_rate`	ONTAP에서 초당 Vscan 서버로 보낸 바이러스 검사 요청 수입니다
`scan_noti_received_rate`	ONTAP가 초당 Vscan 서버로부터 받은 바이러스 검사 요청 수입니다
`dispatch_latency`	ONTAP 내의 대기 시간으로 사용 가능한 Vscan 서버를 식별하고 해당 Vscan 서버로 요청을 전송합니다

scan_latency	ONTAP에서 Vscan 서버로의 왕복 지연 시간(스캔 실행 시간 포함)

ONTAP 오프박스 **Vscan** 카운터에서 생성된 통계의 예

```
Object: offbox_vscan
Instance: SVM
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 2 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_noti_received_rate 292
dispatch_latency 43986us
scan_latency 3433501us
-------------------------------------------------------------------
```

개별 **Vscan** 서버 요청 및 대기 시간에 대한 통계를 봅니다

ONTAP를 사용할 수 있습니다 `offbox_vscan_server` Vscan 서버당, SVM당, 오프박스 Vscan 서버의 카운터, 및 노드별 기준으로 파견된 Vscan 서버 요청 비율 및 에 대한 서버 지연 시간을 모니터링합니다 각 Vscan 서버를 개별적으로 사용할 수 있습니다. 이 정보를 수집하려면 다음 단계를 완료하십시오.

단계

1. 를 실행합니다 `statistics show -object offbox_vscan -instance SVM:servername:nodename` 다음 카운터를 사용하여 명령을 실행합니다.

카운터…	표시된 정보…
scan_request_dispatched_rate	ONTAP에서 보낸 바이러스 검사 요청 수입니다
scan_latency	ONTAP에서 Vscan 서버로의 왕복 지연 시간(스캔 실행 시간 포함) 초당 Vscan 서버로

ONTAP offbox_Vscan_server 카운터에서 생성된 통계의 예

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_latency 3433830us
-------------------------------------------------------------------
```

Vscan 서버 활용도에 대한 통계를 봅니다

ONTAP를 사용할 수도 있습니다 `offbox_vscan_server` Vscan 서버 – 측면 활용 수집 카운터 통계. 이러한 통계는 SVM, Box가 없는 Vscan 서버별, 노드 단위로 추적됩니다. 있습니다 Vscan 서버의 CPU 사용률, Vscan 서버의 스캔 작업에 대한 대기열 깊이를 포함합니다 (현재 및 최대), 사용된 메모리 및 사용된 네트워크. 이러한 통계는 ONTAP 내의 통계 카운터로 Antivirus Connector에 의해 전달됩니다. 있습니다 20초마다 폴링되는 데이터를 기반으로 하며 정확성을 위해 여러 번 수집해야 합니다. 그렇지 않으면 통계에 표시되는 값은 마지막 폴링만 반영합니다. CPU 사용률 및 큐는 입니다 특히 모니터링 및 분석에 중요합니다. 평균 대기열의 값이 높으면 가 표시됩니다 Vscan 서버에 병목 현상이 있습니다. Vscan 서버에 대한 사용률을 SVM 단위, 오프박스 Vscan 서버 단위 및 노드별로 수집합니다 다음 단계를 완료합니다.

단계

1. Vscan 서버에 대한 활용도 통계를 수집합니다

   를 실행합니다 `statistics show –object offbox_vscan_server –instance SVM:servername:nodename` 명령을 입력합니다 `offbox_vscan_server` 카운터:

카운터…	표시된 정보…
`scanner_stats_pct_cpu_used`	Vscan 서버의 CPU 활용도입니다
`scanner_stats_pct_input_queue_avg`	Vscan 서버에 대한 스캔 요청의 평균 대기열
`scanner_stats_pct_input_queue_hiwatermark`	Vscan 서버에서 스캔 요청 최대 대기열
`scanner_stats_pct_mem_used`	Vscan 서버에서 사용되는 메모리입니다
`scanner_stats_pct_network_used`	Vscan 서버에서 사용되는 네트워크

Vscan 서버에 대한 사용률 통계의 예

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scanner_stats_pct_cpu_used 51
scanner_stats_pct_dropped_requests 0
scanner_stats_pct_input_queue_avg 91
scanner_stats_pct_input_queue_hiwatermark 100
scanner_stats_pct_mem_used 95
scanner_stats_pct_network_used 4
---------------------------------------------------------------
```

관련 정보

- "ONTAP 명령 참조입니다"