Vscan 서버 설치 및 구성

ONTAP 9

NetApp
April 24, 2024

목차

Vscan 서버 설치 및 구성

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 를 참조하십시오 "Vscan 파트너 솔루션" 페이지.

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 안티바이러스 커넥터를 설치합니다

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

- 를 참조하십시오 "Vscan 파트너 솔루션" 지원되는 프로토콜, 안티바이러스 공급업체 소프트웨어 버전, ONTAP 버전, 상호 운용성 요구 사항 및 Windows 서버에 대한 정보를 제공합니다.
- 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 가상 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 에 대한 액세스(읽기 전용) 권한이 있는 역할을 할당했는지 확인합니다 `/api/network/ip/interfaces` REST API: 사용자 만들기에 대한 자세한 내용은 를 참조하십시오 "보안 로그인 역할이 생성됩니다" 및 "보안 로그인 생성" ONTAP Man 페이지.

> 관리 SVM에 대한 인증 터널 SVM을 추가하여 도메인 사용자를 계정으로 사용할 수도 있습니다. 자세한 내용은 를 참조하십시오 "보안 로그인 도메인 - 터널 생성" ONTAP man 페이지를 참조하거나 을 사용합니다 `/api/security/acccounts` 및 `/api/security/roles` REST API를 통해 admin 계정 및 역할을 구성합니다.

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 알아보십시오 "LIF 생성".

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 안티바이러스 커넥터를 구성합니다

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 에 대한 액세스(읽기 전용) 권한이 있는 역할을 할당했는지 확인합니다 `/api/network/ip/interfaces` REST API: 사용자 만들기에 대한 자세한 내용은 를 참조하십시오 "보안 로그인 역할이 생성됩니다" 및 "보안 로그인 생성" 명령. 관리 SVM에 대한 인증 터널 SVM을 추가하여 도메인 사용자를 계정으로 사용할 수도 있습니다. 자세한 내용은 를 참조하십시오 "보안 로그인 도메인 - 터널 생성" ONTAP man 페이지입니다.

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 인증서를 서명하는 데 사용되는 CA 인증서(루트 CA에 대한 중간 등록 권한 포함)가 PEM(개인 정보 보호 향상 메일) 형식이고 이름이 "ontap_ca.pem"인지 확인합니다. 바이러스 백신 커넥터 설치 디렉터리에 넣습니다. NetApp ONTAP 시스템에서 "ONTAP"의 안티바이러스 커넥터에 대한 클라이언트 인증서를 "client-ca" 유형 인증서로 서명하는 데 사용되는 CA 인증서(루트 CA에 대한 중간 서명 권한 포함)를 설치합니다.