액세스 시 스캔을 구성합니다

ONTAP 9

NetApp
February 14, 2026

This PDF was generated from https://docs.netapp.com/ko-kr/ontap/antivirus/create-on-access-policy-task.html on February 14, 2026. Always check docs.netapp.com for the latest.

목차

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.

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 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.