



# オンアクセススキャンの設定

## ONTAP 9

NetApp  
December 20, 2024

# 目次

オンアクセススキャンの設定	1
オンアクセスポリシーを作成する	1
オンアクセスポリシーを有効にする	3
SMB共有のVscanファイル処理プロファイルを変更する	4
オンアクセスポリシーの管理用コマンド	4

# オンアクセススキヤンの設定

## オンアクセスポリシーを作成する

オンアクセスポリシーはオンアクセススキヤンの範囲を定義します。オンアクセスポリシーは、個々のSVMまたはクラスタ内のすべてのSVMに対して作成できます。クラスタ内のすべてのSVM用のオンアクセスポリシーを作成した場合は、各SVMでポリシーを個別に有効にする必要があります。

### タスクの内容

- スキャンする最大ファイルサイズ、スキャンに含めるファイル拡張子とパス、およびスキャンから除外するファイル拡張子とパスを指定できます。
- このオプションをoffに設定する `scan-mandatory` と、ウィルススキャンに使用できるVscanサーバがない場合にファイルアクセスを許可します。
- デフォルトでは、ONTAPは「default\_cifs」という名前のオンアクセスポリシーを作成し、クラスタ内のすべてのSVMに対して有効にします。
- `file-ext-to-exclude`、または `max-file-size` パラメータに基づいてスキャン除外の対象となるファイル `paths-to-exclude` は、オプションがonに設定されていてもスキャン対象とみなされません `scan-mandatory`。 (オプションに関連する接続の問題については、このセクションを `scan-mandatory` 確認してください"[トラブルシューティング](#)")。
- デフォルトでは、読み取り/書き込みボリュームのみがスキャンされます。読み取り専用ボリュームのスキャンを有効にするフィルタや、実行アクセス権で開かれたファイルのみにスキャンを制限するフィルタを指定することができます。
- continuously-availableパラメータがYesに設定されているSMB共有ではウィルススキャンは実行されません。
- `_vscan`ファイル処理プロファイルの詳細については、セクションを参照してください"[ウィルス対策アーキテクチャ](#)"。
- SVMごとに最大10個のオンアクセスポリシーを作成できます。ただし、一度に有効にできるオンアクセスポリシーは1つだけです。
  - オンアクセスポリシーでは、最大100個のパスとファイル拡張子をウィルススキャンの対象から除外できます。
- ファイル除外の推奨事項：
  - 大容量ファイル（ファイルサイズを指定可能）は、CIFSユーザの応答に時間がかかるか、スキャン要求がタイムアウトする可能性があるため、ウィルススキャンの対象から除外することを検討してください。除外するデフォルトのファイルサイズは2GBです。
  - や `.tmp` などのファイル拡張子は除外することを検討してください `.vhd`。これらの拡張子のファイルはスキャンに適していない可能性があります。
  - 隔離ディレクトリなどのファイルパスや、仮想ハードドライブまたはデータベースのみが格納されているパスを除外することを検討してください。
  - 一度に有効にできるポリシーは1つだけであるため、すべての除外が同じポリシーに指定されていることを確認します。NetAppでは、アンチウイルスエンジンで指定されているのと同じ除外を設定することを強く推奨します。
- にはオンアクセスポリシーが必要[オンデマンドスキャン](#)です。のオンアクセススキヤンを実行しないよう

にするには、`false`と `-file-ext-to-exclude*`をに設定し ``-scan-files-with-no-ext``ですべての拡張子を除外します。

## 手順

### 1. オンアクセスポリシーを作成します。

```
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 extensions_of_files_to_include -file-ext-to-exclude
extensions_of_files_to_exclude -scan-files-with-no-ext true|false -paths-to
-exclude paths_of_files_to_exclude -scan-mandatory on|off
```

- 個々の SVM 用のポリシーの場合はデータ SVM、クラスタ内のすべての SVM 用のポリシーの場合はクラスタ管理 SVM を指定します。
- ``-file-ext-to-exclude``設定は設定よりも優先され ``-file-ext-to-include``ます。
- 拡張子のないファイルをスキャンするには、`true`に設定し ``-scan-files-with-no-ext``ます。次のコマンドは、SVM上に ``vs1``という名前のオンアクセスポリシーを作成し ``Policy1``ます。

```
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. オンアクセスポリシーが作成されたことを確認します。 `vserver vscan on-access-policy show -instance data_SVM|cluster_admin_SVM -policy-name name`

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、ポリシーの詳細を表示し ``Policy1``ます。

```
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
```

# オンアクセスポリシーを有効にする

オンアクセスポリシーはオンアクセススキャンの範囲を定義します。SVMのファイルをスキャンするには、そのSVMでオンアクセスポリシーを有効にする必要があります。

クラスタ内のすべてのSVM用のオンアクセスポリシーを作成した場合は、各SVMでポリシーを個別に有効にする必要があります。SVMで一度に有効にできるオンアクセスポリシーは1つだけです。

## 手順

1. オンアクセスポリシーを有効にします。

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

次のコマンドは vs1、SVMでという名前のオンアクセスポリシーを有効にし `Policy1` ます。

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

2. オンアクセスポリシーが有効になっていることを確認します。

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

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、オンアクセスポリシーの詳細を表示し `Policy1` ます。

```
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共有のVscanファイル処理プロファイルを変更する

SMB共有の `_vscan` ファイル処理プロファイルは、スキャンをトリガーできる共有に対する処理を定義します。デフォルトでは、パラメータはに設定されてい `standard` ます。このパラメータは、SMB共有を作成または変更するときに必要に応じて調整できます。

`_vscan` ファイル処理プロファイルの詳細については、セクションを参照してください"[ウイルス対策アーキテクチャ](#)"。



パラメータがに設定され `Yes`` ているSMB共有ではウイルススキャンは実行されません ``continuously-available`。

### ステップ

1. SMB共有のVscanファイル処理プロファイルの値を変更します。

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

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、SMB共有のVscanファイル処理プロファイルをに変更し `strict` ます。

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

## オンアクセスポリシーの管理用コマンド

オンアクセスポリシーは変更、無効化、削除できます。ポリシーの概要と詳細を表示できます。

状況	入力するコマンド
オンアクセスポリシーを作成する	<code>vserver vscan on-access-policy create</code>
オンアクセスポリシーを変更する	<code>vserver vscan on-access-policy modify</code>
オンアクセスポリシーを有効にする	<code>vserver vscan on-access-policy enable</code>
オンアクセスポリシーを無効にする	<code>vserver vscan on-access-policy disable</code>
オンアクセスポリシーを削除する	<code>vserver vscan on-access-policy delete</code>
オンアクセスポリシーの概要と詳細を表示する	<code>vserver vscan on-access-policy show</code>

対象から除外するパスをリストに追加する	<code>vserver vscan on-access-policy paths-to-exclude add</code>
対象から除外するパスをリストから削除します。	<code>vserver vscan on-access-policy paths-to-exclude remove</code>
対象から除外するパスのリストを表示する	<code>vserver vscan on-access-policy paths-to-exclude show</code>
対象から除外するファイル拡張子をリストに追加する	<code>vserver vscan on-access-policy file-ext-to-exclude add</code>
対象から除外するファイル拡張子をリストから削除する	<code>vserver vscan on-access-policy file-ext-to-exclude remove</code>
対象から除外するファイル拡張子のリストを表示する	<code>vserver vscan on-access-policy file-ext-to-exclude show</code>
対象に含めるファイル拡張子をリストに追加する	<code>vserver vscan on-access-policy file-ext-to-include add</code>
対象に含めるファイル拡張子をリストから削除する	<code>vserver vscan on-access-policy file-ext-to-include remove</code>
対象に含めるファイル拡張子のリストを表示する	<code>vserver vscan on-access-policy file-ext-to-include show</code>

これらのコマンドの詳細については、マニュアルページを参照してください。

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。