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

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ャ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ャ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`て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"ウィ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共有ではウィ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	`vserver vscan on-access-policy create`
オンアクセスポリシーを変更する	`vserver vscan on-access-policy modify`
オンアクセスポリシーを有効にする	`vserver vscan on-access-policy enable`
オンアクセスポリシーを無効にする	`vserver vscan on-access-policy disable`
オンアクセスポリシーを削除する	`vserver vscan on-access-policy delete`
オンアクセスポリシーの概要と詳細を表示する	`vserver vscan on-access-policy show`

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

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

商標に関する情報