NetAppアンチウイルスによる保護について

ONTAP 9

NetApp
December 20, 2024

目次

NetAppアンチウイルスによる保護について

NetAppウィルススキャンについて

Vscanは、NetAppが開発したウィルススキャンソリューションです。ウィルスやその他の悪意のあるコードからデータを保護できます。パートナーが提供するウイルス対策ソフトウェアとONTAPの機能を組み合わせることで、お客様はファイルスキャンの管理に必要な柔軟性を得ることができます。

ウィルススキャンの仕組み

スキャン処理は、サードパーティベンダーのウィルス対策ソフトウェアをホストする外部サーバにオフロードされます。

ONTAPは、アクティブなスキャンモードに基づいて、クライアントがSMB経由でファイルにアクセスする場合（オンアクセス）、または特定の場所にあるファイルにスケジュールに従ってアクセスする場合、またはただちに（オンデマンドで）アクセスする場合にスキャン要求を送信します。

- クライアントが SMB 経由でファイルを開く、読み取る、名前を変更する、閉じるたびにウィルスチェックを行うには、 _on_access scanning_to を使用します。ファイル操作は、外部サーバからファイルのスキャンステータスが報告されるまで中断されます。ファイルがすでにスキャンされている場合、ONTAPはファイル操作を許可します。それ以外の場合は、サーバからのスキャンを要求します。

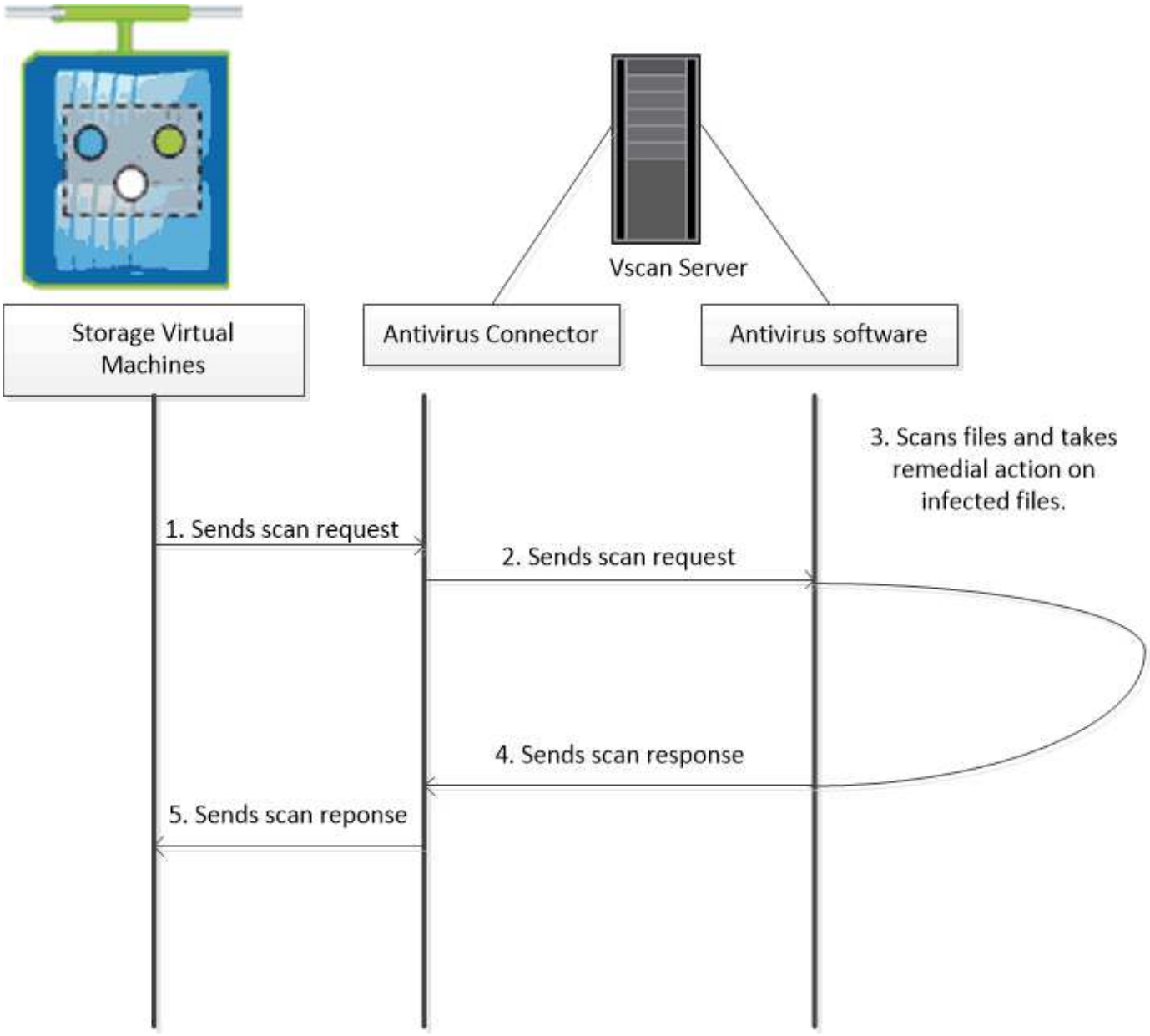
  NFSではオンアクセススキャンはサポートされていません。

- オンデマンドスキャン _ を使用すると、ファイルのウィルスチェックをただちにまたはスケジュールに基づいて実行できます。通常はオンアクセススキャン用にサイジングされている既存のAVインフラが過負荷にならないように、オンデマンドスキャンはオフピークの時間帯にのみ実行することを推奨します。外部サーバはチェックしたファイルのスキャンステータスを更新するため、SMB経由でのファイルアクセスのレイテンシが低減されます。ファイルの変更またはソフトウェアバージョンの更新があった場合は、外部サーバから新しいファイルスキャンを要求します。

  オンデマンドスキャンは、NFS経由でのみエクスポートされたボリュームも含め、SVMネームスペース内の任意のパスに対して使用できます。

通常は、SVMでオンアクセスモードとオンデマンドスキャンモードの両方を有効にします。どちらのモードでも、ウィルス対策ソフトウェアはソフトウェアの設定に基づいて感染したファイルに対して修復アクションを実行します。

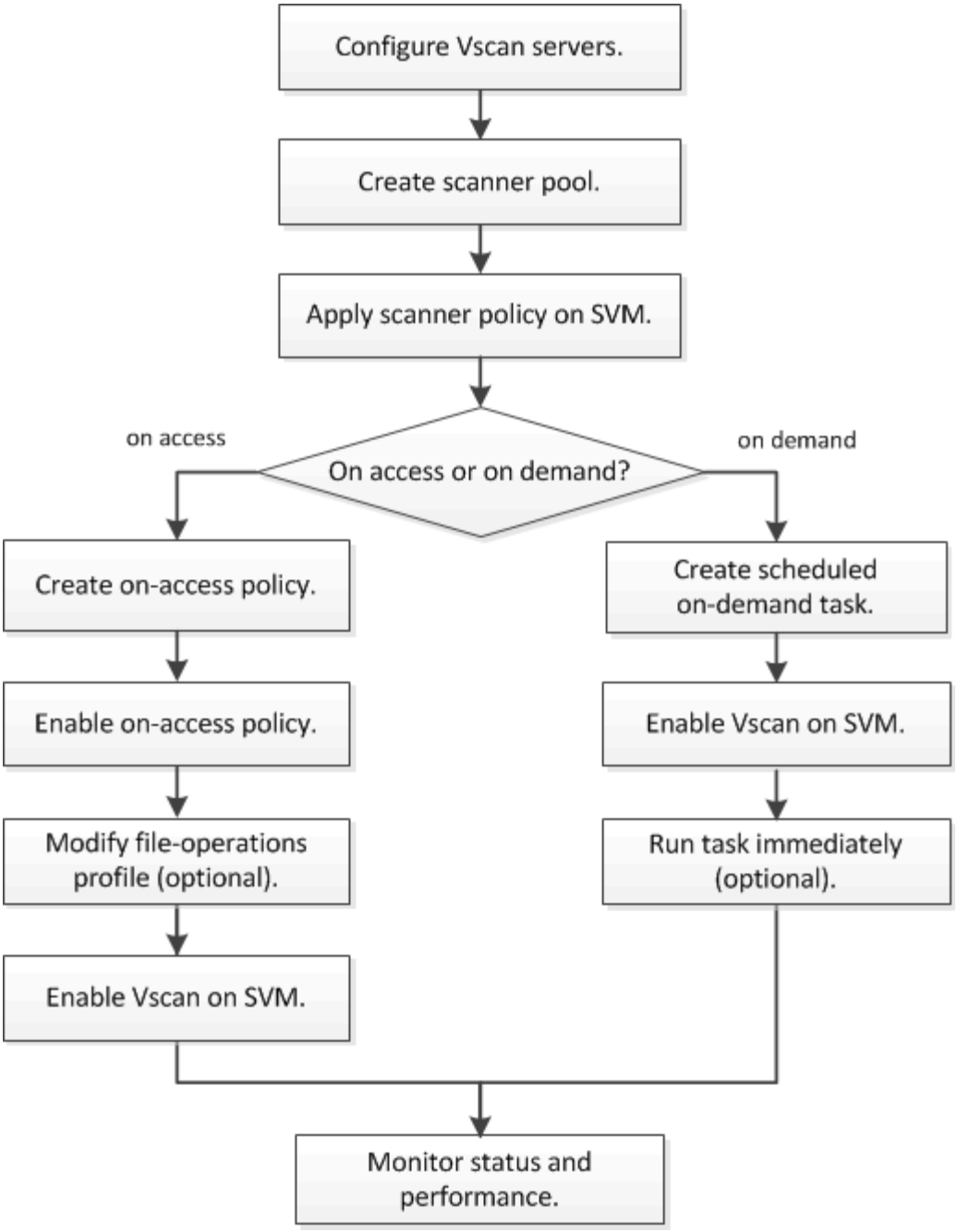
NetAppが提供し、外部サーバにインストールされるONTAP Antivirus Connectorは、ストレージシステムとウィルス対策ソフトウェア間の通信を処理します。



ウィルススキャンのワークフロー

スキャンを有効にする前に、スキャナプールを作成してスキャナポリシーを適用する必要があります。通常は、SVMでオンアクセスモードとオンデマンドスキャンモードの両方を有効にします。

CIFSの設定が完了している必要があります。



オンデマンドタスクを作成するには、少なくとも1つのオンアクセスポリシーを有効にする必要があります。デフォルトポリシーまたはユーザが作成したオンアクセスポリシーを使用できます。

次のステップ

- 単一クラスタにスキャナプールを作成する
- 単一のクラスタにスキャナポリシーを適用する
- オンアクセスポリシーを作成する

ウィルス対策アーキテクチャ

NetAppウィルス対策アーキテクチャは、Vscanサーバソフトウェアと関連する設定で構成されます。

Vscanサーバソフトウェア

このソフトウェアはVscanサーバにインストールする必要があります。

- * ONTAP Antivirus Connector *

  NetAppが提供するソフトウェアで、SVMとウィルス対策ソフトウェアの間のスキャン要求と応答の通信を処理します。仮想マシン上で実行できますが、最高のパフォーマンスを得るには物理マシンを使用します。このソフトウェアはNetAppサポートサイトからダウンロードできます（ログインが必要です）。

- * アンチウイルスソフトウェア *

  これは、ウイルスやその他の悪意のあるコードのファイルをスキャンするパートナー提供のソフトウェアです。ソフトウェアを設定する際に、感染したファイルに対して実行する処理を指定します。

Vscanソフトウェア設定

これらのソフトウェアをVscanサーバで設定する必要があります。

- * スキャナプール *

  この設定では、SVMに接続できるVscanサーバと特権ユーザを定義します。また、スキャン要求のタイムアウト時間も定義します。この時間が経過すると、代替のVscanサーバがある場合はそのサーバにスキャン要求が送信されます。

  > Vscanサーバ上のウィルス対策ソフトウェアのタイムアウト時間は、scanner-poolのスキャン要求タイムアウト時間よりも5秒短く設定する必要があります。これにより、ソフトウェアのタイムアウト時間がスキャン要求のタイムアウト時間よりも長いため、ファイルアクセスが遅延または拒否される状況を回避できます。

- * 特権ユーザ *

  この設定は、VscanサーバがSVMへの接続に使用するドメインユーザアカウントです。スキャナプール内の特権ユーザのリストにアカウントが存在している必要があります。

- * スキャナポリシー *

  この設定では、スキャナプールをアクティブにするかどうかを指定します。スキャナポリシーはシステムで定義されるため、カスタムのスキャナポリシーを作成することはできません。次の3つのポリシーのみを使用できます。

  - `Primary`スキャナプールをアクティブにします。
  - `Secondary`プライマリスキャナプールのVscanサーバが1つも接続されていない場合にのみスキャナプールをアクティブにします。

- `Idle`スキャナプールを非アクティブにします。

- * オンアクセスポリシー *

  この設定では、オンアクセススキャンの範囲を定義します。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。

  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。

  - `scan-ro-volume`読み取り専用ボリュームのスキャンを有効にします。
  - `scan-execute-access`実行アクセス権で開かれたファイルにスキャンを制限します。

    「アクセスの実行」と「アクセスの実行」は「アクセスの実行」とは異なります。 指定されたクライアントは、実行ファイルが「実行意図」で開かれている場合にのみ、実行ファイルに対して「実行アクセス」を持つことになります。

  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。オンアクセスモードでは、次の2つのオプションのいずれかを選択できます。

  - 必須：このオプションを指定すると、タイムアウト時間が経過するまで、Vscanはサーバへのスキャン要求の配信を試みます。サーバがスキャン要求を受け入れなかった場合、クライアントアクセス要求は拒否されます。
  - 必須以外：このオプションを使用すると、Vscanサーバがウィルススキャンに使用できるかどうかに関係なく、Vscanでクライアントアクセスが常に許可されます。

- * オンデマンドタスク *

  この設定では、オンデマンドスキャンの範囲を定義します。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。デフォルトでは、サブディレクトリ内のファイルがスキャンされます。

  cronスケジュールを使用して、タスクを実行するタイミングを指定します。コマンドを使用すると、タスクをすぐに実行できます `vserver vscan on-demand-task run`。

- * Vscan ファイル処理プロファイル（オンアクセススキャンのみ） *

  コマンドのパラメータ `vserver cifs share create`は、 `vscan-fileop-profile`ウィルススキャンをトリガーするSMBファイル処理を定義します。デフォルトでは、パラメータは（NetAppのベストプラクティス）に設定され `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。

  - `no-scan`共有に対してウィルススキャンを一切トリガーしません。
  - `standard`開く、閉じる、および名前変更の各処理でウィルススキャンをトリガーします。
  - `strict`開く、読み取る、閉じる、および名前変更の各処理でウィルススキャンをトリガーします。

    プロファイルを使用する `strict`と、複数のクライアントが同時に1つのファイルにアクセスする場合のセキュリティが強化されます。では、あるクライアントがウィルスを書き込んだあとにファイルを閉じたときに別のクライアントが同じファイルを開いていた場合、2番目のクライアントが `strict`ファイ

ルを閉じる前に読み取り処理を実行したときにスキャンがトリガーされます。

> `strict`同時にアクセスされる可能性があるファイルを含む共有にプロファイルを制限するように注意してください。このプロファイルはより多くのスキャン要求を生成するため、パフォーマンスに影響を与える可能性があります。

- `writes-only`変更されたファイルが閉じられたときにのみウィルススキャンをトリガーします。

> `writes-only`で生成されるスキャン要求が少なくなるため、通常はパフォーマンスが向上します。

このプロファイルを使用する場合は、修復不可能な感染ファイルを削除または隔離するようにスキャナを設定して、アクセスできないようにする必要があります。たとえば、あるクライアントがウィルスを書き込んだあとにファイルを閉じた場合、そのファイルが修復、削除、または隔離されていないと、書き込み先のファイルにアクセスしたすべてのクライアント `without`が感染します。

> クライアントアプリケーションが名前変更処理を実行すると、ファイルは新しい名前で閉じられ、スキャンされません。このような処理によってセキュリティが懸念される環境では、または `strict`プロファイルを使用する必要があり `standard`ます。

Vscanパートナーソリューション

NetAppは、Trellix、Symantec、Trend Micro、およびSentinel Oneと協力して、ONTAP Vscanテクノロジを基盤とする業界をリードするアンチマルウェアおよびアンチウイルスソリューションを提供しています。これらのソリューションは、ファイルをスキャンしてマルウェアを検出し、影響を受けるファイルを修正するのに役立ちます。

次の表に示すように、Trellix、Symantec、Trend Microの相互運用性の詳細については、NetAppのInteroperability Matrixを参照してください。TrellixとSymantecの相互運用性の詳細については、パートナーのWebサイトを参照してください。Sentinel Oneおよびその他の新しいパートナーの相互運用性の詳細は、パートナーのWebサイトで管理されます。

パートナー	ソリューションのドキュメント	相互運用性の詳細
Trellix（旧McAfee）	"Trellix製品ドキュメント"	• "NetApp Interoperability Matrix Tool" • "Endpoint Security Storage Protectionでサポートされるプラットフォーム（trellix.com）"

パートナー	ソリューションのドキュメント	相互運用性の詳細
シマンテック	"Symantec Protection Engine 9.0.0"	• "NetApp Interoperability Matrix Tool" • "Symantec Protection Engine（SPE）for Network Attached Storage（NAS）9.x.xと認定されたパートナーデバイスのサポートマトリックス" • "Symantec Protection Engine（SPE）for Network Attached Storage（NAS）8.x認定パートナーデバイスのサポートマトリックス（broadcom.com）"
トレンドマイクロ	"『Trend Micro ServerProtect for Storage 6.0 Getting Started Guide』"	"NetApp Interoperability Matrix Tool"
Sentinel One	• "SentinelOne Singularityクラウドデータセキュリティ" • "SentinelOneのサポート" このリンクにはユーザ ログインが必要です。SentinelOneにアクセス権をリクエストしてください。	Deep Instinct
ストレージに対する深い本能的な防止 • "ドキュメントと相互運用性" このリンクにはユーザ ログインが必要です。Deep Instinctにアクセス権をリクエストしてください。 • "データシート"	オプスワット	OPSWAT MetaDefenderストレージセキュリティ • "MetaDefenderストレージセキュリティとNetAppの統合" • "OPSWAPパートナーページ" • "統合ソリューション概要"

著作権に関する情報

商標に関する情報