NetAppのウイルス対策保護について

ONTAP 9

NetApp
March 11, 2026

目次

NetAppのウイルス対策保護について

NetApp ONTAP Vscanによるウイルススキャンについて学ぶ

Vscanは、NetAppが開発したウイルス対策スキャン ソリューションで、ウイルスやその他の悪意のあるコードからデータを守れます。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て、柔軟にファイル スキャンを管理できます。

ウイルススキャンの仕組み

スキャン処理は、サードパーティ ベンダーのウイルス対策ソフトウェアをホストする外部サーバで実行されます。

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

- _オンアクセススキャン_を使用すると、クライアントがSMB経由でファイルを開く、読み込む、名前を変更する、または閉じる際にウイルスチェックを行うことができます。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、ファイル操作は一時停止されます。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。そうでない場合は、サーバにスキャンを要求します。

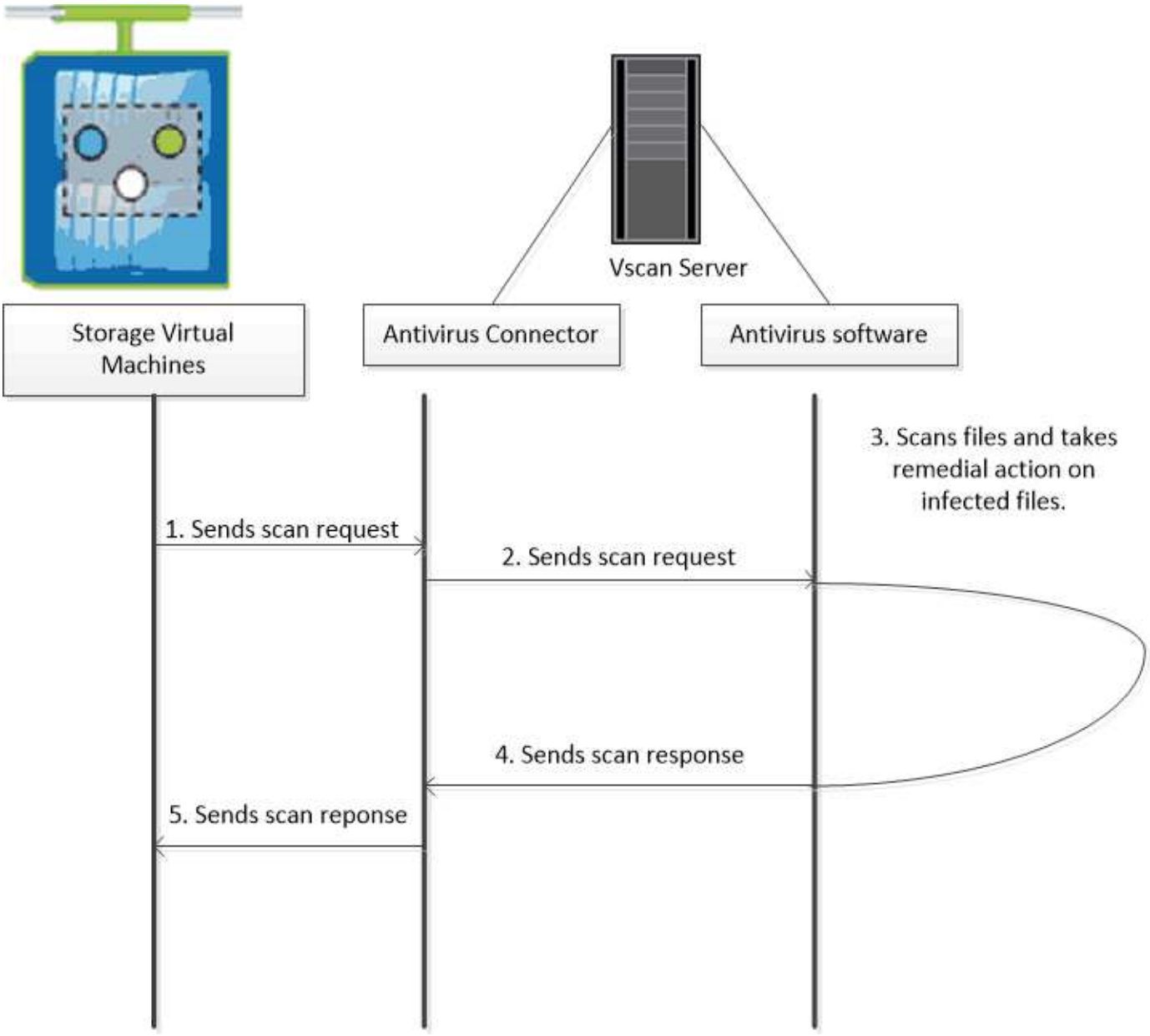
  オンアクセス スキャンは、NFSではサポートされません。

- _オンデマンドスキャン_を使用すると、ファイルのウイルスチェックを即時またはスケジュールに従って実行できます。既存のAVインフラストラクチャは通常、オンアクセススキャン用にサイズ調整されているため、オンデマンドスキャンはオフピーク時にのみ実行することをお勧めします。外部サーバーは、チェックされたファイルのスキャンステータスを更新することで、SMB経由のファイルアクセスの遅延を削減します。ファイルの変更やソフトウェアバージョンの更新があった場合は、外部サーバーに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すべてのパスに対して使用できます。

通常、SVMに対してオンアクセス スキャン 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、感染したファイルにはウイルス対策ソフトウェアで設定した処理が実行されます。

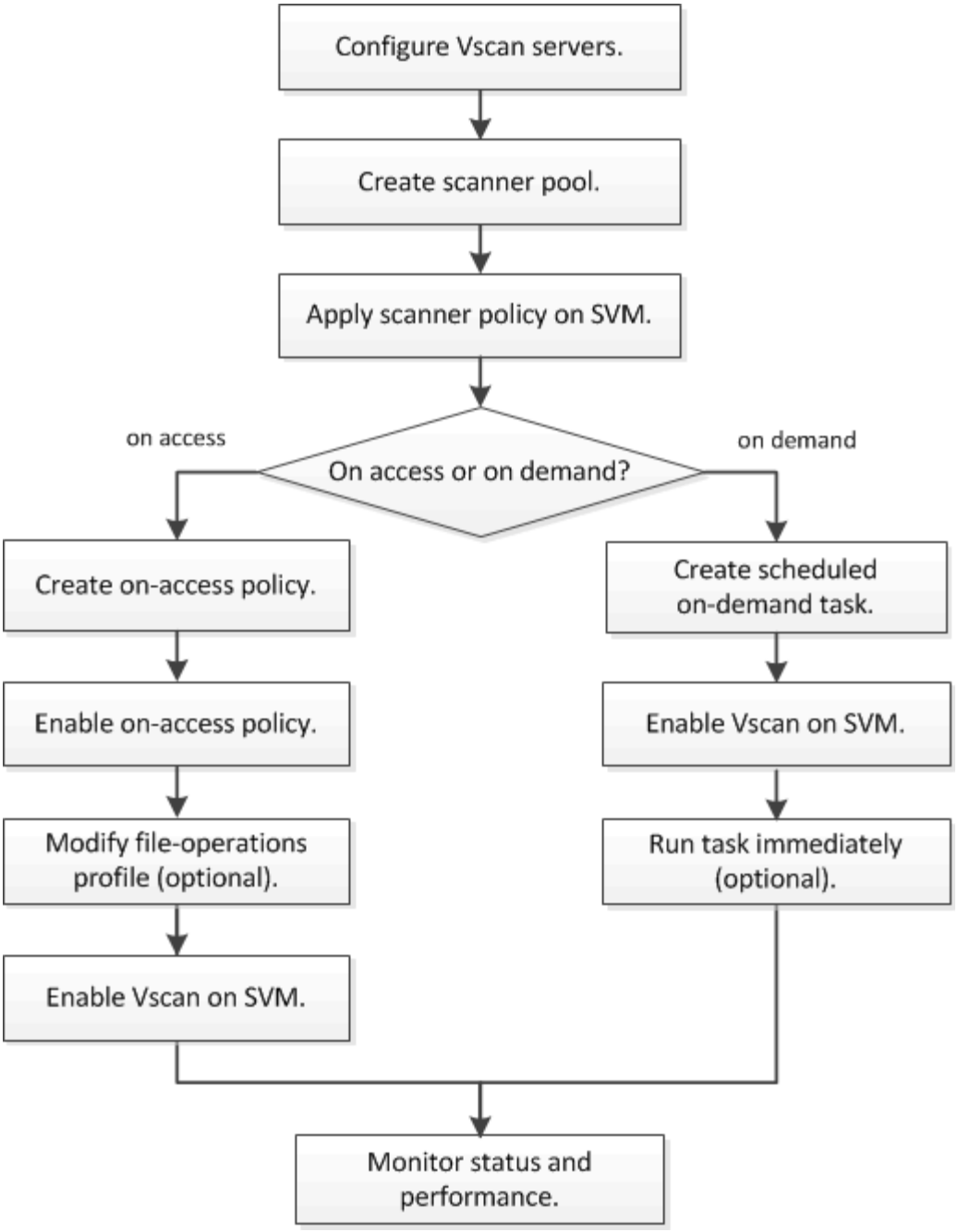
NetAppが提供し、外部サーバにインストールされるONTAP Antivirus Connectorが、ストレージ システムとウイルス対策ソフトウェア間の通信を処理します。



ONTAP Vscanによるウイルススキャンワークフロー

スキャンを有効にする前に、スキャナ プールを作成し、スキャナ ポリシーを適用する必要があります。通常、SVMに対してオンアクセス スキャン 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の設定を完了しておく必要があります。



オンデマンド タスクを作成するには、オンアクセス ポリシーが少なくとも1つ有効になっている必要があります。オンアクセス ポリシーは、デフォルト ポリシーでも、ユーザが作成したものでもかまいません。

次の手順

- 単一クラスタでのスキャナ プールの作成
- 単一クラスタへのスキャナ ポリシーの適用
- オンアクセス ポリシーの作成

ONTAP Vscanを使用したウイルス対策アーキテクチャ

NetAppのウイルス対策アーキテクチャは、Vscanサーバ ソフトウェアと、それに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**アンチウイルスコネクタ

  これはNetAppが提供するソフトウェアで、SVMとウイルス対策ソフトウェアの間のスキャン要求と応答のやり取りを処理します。仮想マシン上でも実行できますが、最大限のパフォーマンスを実現するには、物理マシンを使用する必要があります。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）。

- ウイルス対策ソフトウェア

  これはパートナーが提供するソフトウェアで、ファイルをスキャンしてウイルスやその他の悪意のあるコードを検出します。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ソフトウェアの設定

これらのソフトウェアは、Vscanサーバで設定を行う必要があります。

- スキャナープール

  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、代わりの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サーバ上のウイルス対策ソフトウェアのタイムアウト時間は、スキャナ プールのスキャン要求のタイムアウト時間より5秒短く設定するようにしてください。こうすると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くなるので、ファイル アクセスが遅延したり、完全に拒否されたりする状況を回避できます。

- 特権ユーザー

  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 プールの特権ユーザ リスト内に存在するアカウントである必要があります。

- スキャナーポリシー

  スキャナ プールがアクティブかどうかを定義します。スキャナ ポリシーはシステムで定義されるので、カスタム スキャナ ポリシーは作成できません。使用できるポリシーは、次の3つのみです。

  - `Primary`スキャナープールがアクティブであることを指定します。
  - `Secondary`プライマリスキャナプール内のVscanサーバーがいずれも接続されていない場合にのみ、スキャナプールがアクティブであることを指定します。

- `Idle`スキャナープールが非アクティブであることを指定します。

- オンアクセスポリシー

  オンアクセス スキャンの範囲を定義します。スキャンするファイルの最大サイズ、スキャン対象に含めるファイルの拡張子とパス、スキャンから除外するファイルの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`は、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`実行アクセスで開かれたファイルへのスキャンを制限します。

  > 「Execute access」は「execute permission.」とは異なります。特定のクライアントは、ファイルが「execute intent.」で開かれた場合にのみ、実行可能ファイルに対する「Execute access」を持ちます。

  `scan-mandatory`
  オプションをオフに設定すると、ウイルススキャンに使用できるVscanサーバがない場合でもファイルアクセスが許可されるように指定できます。オンアクセスモード内では、次の2つの相互排他的なオプションから選択できます：

  - 必須：このオプションを選択すると、Vscan はタイムアウト期間が終了するまでスキャン要求をサーバーに送信しようとします。スキャン要求がサーバーに受け入れられない場合、クライアントのアクセス要求は拒否されます。
  - 非必須：このオプションを使用すると、Vscanサーバーがウイルススキャンに使用できるかどうかに関係なく、Vscanは常にクライアントアクセスを許可します。

- オンデマンドタスク

  オンデマンド スキャンの範囲を定義します。スキャンするファイルの最大サイズ、スキャン対象に含めるファイルの拡張子とパス、スキャンから除外するファイルの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もスキャンされます。

  cronスケジュールを使用して、タスクの実行タイミングを指定します。 `vserver vscan on-demand-task run`コマンドを使用して、タスクを即時実行することもできます。"ONTAPコマンド リファレンス"の`vserver vscan on-demand-task run`の詳細をご覧ください。

- **Vscan** ファイル操作プロファイル（**on-access** スキャンのみ）

  `vserver cifs share create`コマンドの `vscan-fileop-profile`パラメータは、どのSMBファイル操作がウイルススキャンをトリガーするかを定義します。デフォルトでは、パラメータは `standard`に設定されており、これがNetAppのベストプラクティスです。SMB共有を作成または変更する際に、必要に応じてこのパラメータを調整できます：

  - `no-scan`共有に対してウイルススキャンがトリガーされないように指定します。

- `standard`は、開く、閉じる、名前の変更の操作によってウイルス スキャンがトリガーされることを指定します。
- `strict`開く、読む、閉じる、名前を変更する操作によってウイルス スキャンがトリガーされることを指定します。

> `strict`プロファイルは、複数のクライアントが同時にファイルにアクセスする状況において、セキュリティを強化します。あるクライアントがウイルスを書き込んだ後にファイルを閉じ、同じファイルが別のクライアントで開かれたままになっている場合、`strict`は、ファイルが閉じられる前に、別のクライアントでの読み取り操作によってスキャンが実行されるようにします。

> `strict`プロファイルを、同時にアクセスされることが予想されるファイルを含む共有に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 リクエストを生成するため、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イルス スキャンがトリガーされるように指定します。

> `writes-only`はスキャン要求の生成数が少ないため、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、修復不可能な感染ファイルにアクセスできないように、スキャナで削除または隔離するように設定する必要があります。例えば、クライアントがウイルスを書き込んだ後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、そのファイル `without`にアクセスするすべてのクライアントが感染します。

> クライアントアプリケーションが名前変更操作を実行した場合、ファイルは新しい名前で閉じられ、スキャンされません。このような操作が環境内でセキュリティ上の懸念となる場合は、`standard` または `strict` プロファイルを使用してください。

`vserver cifs share create`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-cifs-share-create.html["ONTAPコマンド リファレンス"^]を参照してください。

ONTAP Vscanパートナー解決策の詳細

NetAppは、Trellix、Symantec、Trend Micro、Sentinel One、Deep Instinct、OPSWATと連携し、ONTAP Vscanテクノロジーを基盤とした業界最先端のマルウェア対策およびウイルス対策解決策を提供しています。これらの解決策は、ファイルのマルウェアスキャンや、影響を受けたファイルの修復に役立ちます。

下の表に示すように、TrellixとTrend Microの相互運用性の詳細は、NetApp相互運用性マトリックスに記載さ

れています。Trellix、Deep Instinct、OPSWATの相互運用性に関する詳細は、パートナーのWebサイトでもご確認いただけます。Sentinel One、Symantec、Deep Instinct、OPSWAT、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 のサポート対象プラットフォーム（trellix.com）"
Symantec	"Symantec Protection Engine 9.0.0"	"Symantec Protection Engine (SPE) for Network Attached Storage (NAS) 9.x.x 認定パートナーデバイスのサポートマトリックス"
Trend Micro	"『Trend Micro ServerProtect for Storage 6.0 Getting Started Guide』"	"NetApp Interoperability Matrix Tool"
SentinelOne	• "SentinelOne Singularity Cloud Data Security" • "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。	該当なし
Deep Instinct	NAS用Deep Instinct DSX • "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"	該当なし
OPSWAT	OPSWAT MetaDefender ストレージセキュリティ • "MetaDefender Storage Security と NetApp の統合" • "OPSWAT パートナーページ" • "統合解決策概要"	該当なし