# ウイルスから保護
## ONTAP 9

NetApp
April 24, 2024

# 目次

# ウイルスから保護

## ウィルス対策の設定の概要

Vscanは、NetAppが開発したウィルス対策スキャン解決策です。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。

Vscan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にウィルススキャンを実行します。Vscanは、オンデマンドまたはスケジュールに基づいてスキャンするように設定できます。Vscanは、ONTAPのコマンドラインインターフェイス（CLI）またはONTAPのアプリケーションプログラミングインターフェイス（API）を使用して操作できます。

関連情報

"Vscanパートナーソリューション"

## ネットアップのウィルス対策機能について

### ネットアップのウィルススキャンについて

Vscanは、NetAppが開発したウィルス対策スキャン解決策です。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で実行されます。

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。

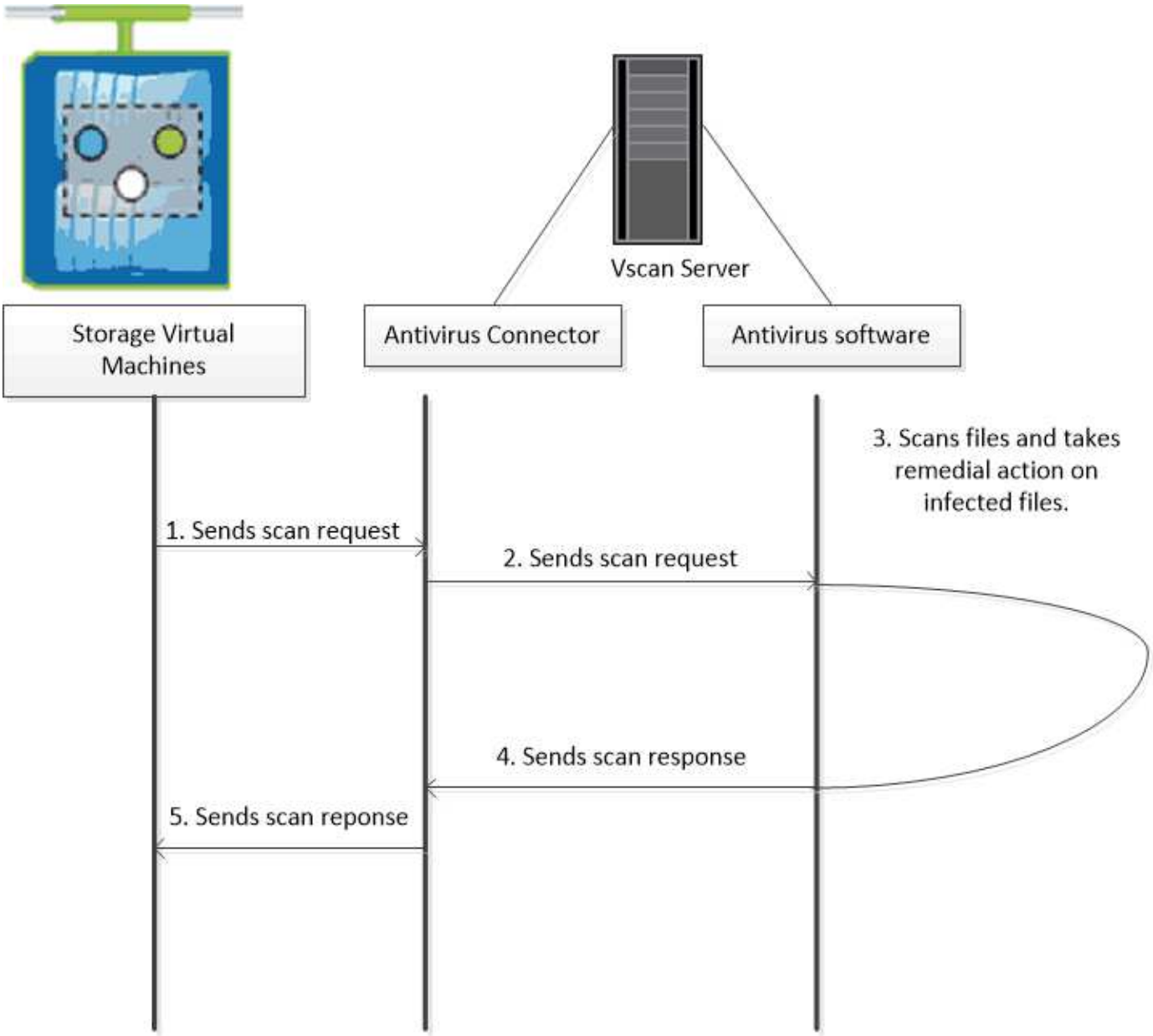
  オンアクセススキャンは NFS ではサポートされていません。

- 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すべて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。

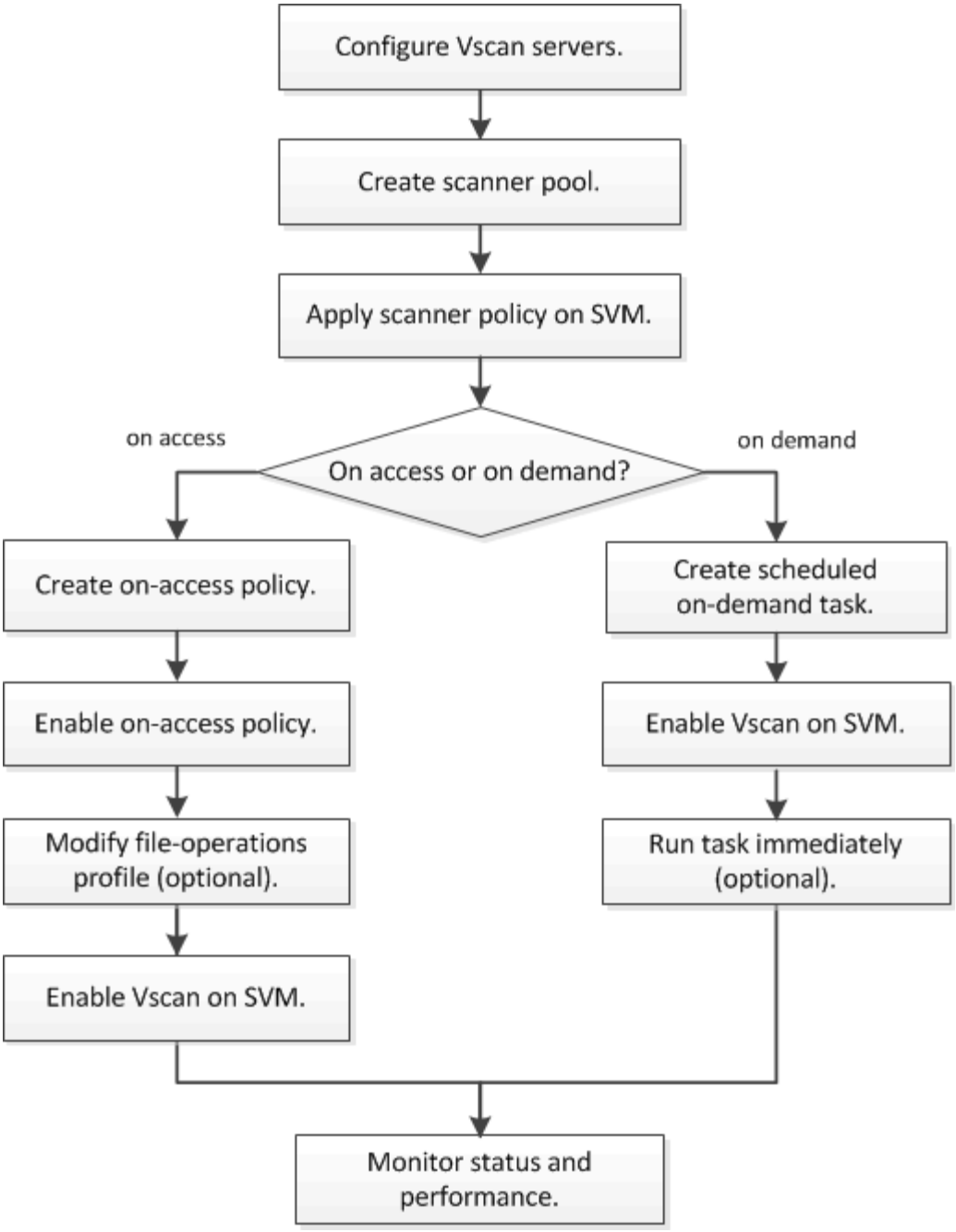
ネットアップが提供し、外部サーバにインストールされる ONTAP Antivirus Connector が、ストレージシステムとウィルス対策ソフトウェア間の通信を処理します。




## 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、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 の設定を完了しておく必要があります。




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します

## 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 *

  ネットアップ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 Support Site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。

を設定できます `scan-mandatory` オフにすると、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が許可されます。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いつタスクを実行するかを指定できます。を使用できます `vserver vscan on-demand-task run` タスクをすぐに実行するコマンド。

* * 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） *

。 `vscan-fileop-profile` のパラメータ `vserver cifs share create` コマンドは、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、パラメータはに設定されています `standard`NetAppのベストプラクティスです。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。

  。 `strict` プロファイルを使用すると、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状況でセキュリティが強化されます。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、別のクライアントで同じファイルが開いたままになっている場合は、 `strict` 2番目のクライアントでの読み取り処理で、ファイルが閉じる前にスキャンがトリガーされるようにします。

  の制限に注意する必要があります `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設定します。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。

以来 `writes-only` 生成されるスキャン要求が少なくなり、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、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、そのファイルにアクセスしたクライアントが修復、削除、または隔離されていない `without` それへの書き込みは感染します。

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。このような処理がセキュリティ上の問題になる場合は、を使用してください `standard` または `strict` プロファイル（Profile）：

## 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 | 解決策のドキュメント | 相互運用性の詳細 |
| --- | --- | --- |
| Trellix（旧McAfee） | "Trellix製品ドキュメント" | • "NetApp Interoperability Matrix Tool で確認できます"<br>• "Endpoint Security Storage Protectionでサポートされるプラットフォーム（trellix.com）" |
| シマンテック | "Symantec Protection Engine 9.0.0" | • "NetApp Interoperability Matrix Tool で確認できます"<br>• "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"<br>• "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 で確認できます" |

| パートナー | 解決策のドキュメント | 相互運用性の詳細 |
| --- | --- | --- |
| センチネル1 | • "SentinelOne Singularityクラウドデータセキュリティ"<br>• "SentinelOneのサポート"<br><br>このリンクにはユーザーログインが必要です。Sentinel Oneからアクセス権をリクエストできます。 | 深い本能 |

# Vscan サーバのインストールと設定

## Vscan サーバのインストールと設定

1つ以上のVscanサーバを設定して、システム上のファイルがウィルススキャンされるようにします。サーバにウィルス対策ソフトウェアをインストールして設定するには、ベンダーからの指示に従ってください。

NetAppが提供するREADMEファイルの手順に従って、ONTAP Antivirus Connectorをインストールして設定します。または、 "[Install ONTAP Antivirus Connectorページ"]。

> ディザスタリカバリおよびMetroCluster構成の場合は、プライマリ/ローカルおよびセカンダリ/パートナーのONTAPクラスタ用に個別のVscanサーバをセットアップして設定する必要があります。

ウィルス対策ソフトウェアの要件

- ウィルス対策ソフトウェアの要件については、ベンダーのドキュメントを参照してください。
- Vscan でサポートされるベンダー、ソフトウェア、およびバージョンについては、を参照してください "Vscanパートナーソリューション" ページ

**ONTAP Antivirus Connector** の要件

- ONTAP Antivirus Connectorは、NetApp Support Siteの*ソフトウェアダウンロード*ページからダウンロードできます。 "ネットアップのダウンロード：ソフトウェア"
- ONTAP Antivirus ConnectorでサポートされるWindowsのバージョンと相互運用性の要件については、を参照してください。 "Vscanパートナーソリューション"。

> クラスタ内の Vscan サーバによってインストールする Windows サーバのバージョンは同じでなくても構いません。

- Windows サーバに .NET 3.0 以降がインストールされている必要があります。
- Windows サーバで SMB 2.0 が有効になっている必要があります。

## ONTAP Antivirus Connectorのインストール

ONTAP Antivirus ConnectorをVscanサーバにインストールして、ONTAPを実行しているシステムとVscanサーバの間の通信を有効にします。ONTAP Antivirus Connectorをインストールすると、ウィルス対策ソフトウェアは1つ以上のStorage Virtual Machine（SVM）と通信できるようになります。

このタスクについて

- を参照してください "Vscanパートナーソリューション" サポートされるプロトコル、ウィルス対策ベンダーのソフトウェアのバージョン、ONTAPのバージョン、相互運用性の要件、およびWindowsサーバについては、ページを参照してください。
- .NET 4.5.1以降がインストールされている必要があります。
- ONTAP Antivirus Connectorは仮想マシンで実行できます。ただし、パフォーマンスを最大限に高めるために、NetAppではアンチウイルススキャンに専用の仮想マシンを使用することを推奨しています。
- ONTAP Antivirus ConnectorをインストールしてSMB 2.0が有効になっている必要があります。

作業を開始する前に

- サポートサイトからONTAP Antivirus Connectorセットアップファイルをダウンロードし、ハードドライブのディレクトリに保存します。
- ONTAP Antivirus Connectorをインストールするための要件を満たしていることを確認します。
- Antivirus Connectorをインストールするための管理者権限があることを確認します。

手順

1. 適切なセットアップファイルを実行して、Antivirus Connectorインストールウィザードを開始します。
2. ［次へ］を選択します。[インストール先フォルダ]ダイアログボックスが開きます。
3. 表示されているフォルダにAntivirus Connectorをインストールするには、_Next_を選択します。別のフォルダにインストールするには、_Change__を選択します。
4. [Windows AV Connector ONTAPサービスのクレデンシャル]ダイアログボックスが開きます。
5. Windowsサービスのクレデンシャルを入力するか、*[追加]*を選択してユーザを選択します。ONTAPシステムの場合、このユーザは有効なドメインユーザであり、SVMのスキャナプール設定に存在している必要があります。
6. 「 * 次へ * 」を選択します。[プログラムをインストールする準備ができました]ダイアログボックスが開きます。
7. インストールを開始するには*を選択します。設定を変更する場合は[戻る]*を選択します。 ステータス・ボックスが開き'インストールの進行状況が表示され'InstallShield Wizard Completedダイアログ・ボックスが表示されます
8. ONTAP ONTAP管理LIFまたはデータLIFの設定を続行する場合は、[LIFの設定]チェックボックスを選択します。 このVscanサーバを使用するには、ONTAP管理LIFまたはデータLIFを少なくとも1つ設定する必要があります。
9. インストールログを表示する場合は、[Windowsインストーラログを表示する]チェックボックスをオンにします。
10. を選択してインストールを終了し、**InstallShield**ウィザードを閉じます。 **ONTAP LIF**を設定するための[Configure ONTAP LIFs]*アイコンがデスクトップに保存されます。

11. Antivirus ConnectorにSVMを追加します。 SVMをAntivirus Connectorに追加するには、データLIFのリストを取得するようにポーリングされるONTAP管理LIFを追加するか、またはデータLIFを直接設定します。ONTAP管理LIFが設定されている場合は、ポーリング情報とONTAP管理者アカウントのクレデンシャルも指定する必要があります。
    - SVMの管理LIFまたはIPアドレスが `management-https`。これは、データLIFのみを設定する場合は必要ありません。
    - HTTPアプリケーション用のユーザアカウントを作成し、（少なくとも読み取り専用）アクセスを持つロールを割り当てたことを確認します。 `/api/network/ip/interfaces` REST API： ユーザの作成の詳細については、を参照してください。 "Security login role create を実行します" および "security login create を実行します" ONTAPのマニュアルページ

> 管理SVM用に認証トンネルSVMを追加して、ドメインユーザをアカウントとして使用することもできます。詳細については、を参照してください "security login domain-tunnel createのように設定します" ONTAPのマニュアルページまたは `/api/security/acccounts` および `/api/security/roles` adminアカウントとロールを設定するためのREST API。

手順

1. Antivirus Connectorのインストールの完了時にデスクトップに保存されていた*アイコンを右クリックし、[Run as Administrator]*を選択します。
2. [Configure ONTAP LIFs]ダイアログボックスで、優先する設定タイプを選択し、次の操作を実行します。

| 作成するLIFのタイプ | 実行する手順 |
|---|---|
| データ LIF | a. 「role」を「data」に設定<br>b. 「data protocol」を「cifs」に設定<br>c. 「firewall policy」を「data」に設定する<br>d. 「service policy」を「default-data-files」に設定 |
| 管理LIF | a. 「role *」を「data」に設定<br>b. 「data protocol」を「none」に設定します。<br>c. 「firewall policy」を「mgmt」に設定<br>d. 「service policy」を「default-management」に設定 |

詳細については、をご覧ください "LIFの作成"。

LIFを作成したら、追加するSVMのデータLIF、管理LIF、またはIPアドレスを入力します。クラスタ管理LIFを入力することもできます。クラスタ管理LIFを指定すると、そのクラスタ内でSMBを提供しているすべてのSVMがVscanサーバを使用できます。

> VscanサーバでKerberos認証が必要な場合は、各SVMデータLIFに一意のDNS名を付ける必要があり、その名前をWindows Active DirectoryでServer Principal Name（SPN；サーバプリンシパル名）として登録する必要があります。各データLIFで一意のDNS名を使用できない場合、またはSPNとして登録されていない場合、VscanサーバはNT LAN Managerメカニズムを使用して認証します。Vscanサーバを接続したあとにDNS名とSPNを追加または変更した場合は、VscanサーバでAntivirus Connectorサービスを再起動して変更を適用する必要があります。

3. 管理LIFを設定するには、ポーリング期間を秒単位で入力します。ポーリング期間は、Antivirus ConnectorがSVMまたはクラスタのLIF設定に対する変更をチェックする頻度です。デフォルトのポーリング間隔は60秒です。
4. ONTAP管理者アカウント名とパスワードを入力して、管理LIFを設定します。
5. [テスト]*をクリックして接続を確認し、認証を確認します。認証は管理LIFの設定でのみ検証されます。
6. ポーリングまたは接続先のLIFのリストにLIFを追加するには、*[更新]*をクリックします。
7. [保存]*をクリックして、レジストリへの接続を保存します。
8. 接続のリストをレジストリインポートまたはレジストリエクスポートファイルにエクスポートする場合は、*エクスポート*をクリックします。これは、複数のVscanサーバが同じ管理LIFまたはデータLIFのセットを使用する場合に便利です。

を参照してください "ONTAP Antivirus Connectorページの設定" を参照してください。

## ONTAP Antivirus Connectorの設定

ONTAP管理LIF、ポーリング情報、およびONTAP管理者アカウントのクレデンシャルを入力するか、データLIFだけを入力して、接続先のStorage Virtual Machine（SVM）を指定するようにONTAP Antivirus Connectorを設定します。また、SVM接続の詳細を変更したり、SVM接続を削除したりすることもできます。ONTAP管理LIFが設定されている場合、デフォルトでは、ONTAP Antivirus ConnectorはREST APIを使用してデータLIFのリストを取得します。

### SVM接続の詳細を変更する

Antivirus Connectorに追加されたStorage Virtual Machine（SVM）接続の詳細を更新するには、ONTAP管理LIFとポーリング情報を変更します。データLIFの追加後に更新することはできません。データLIFを更新するには、まずデータLIFを削除してから、新しいLIFまたはIPアドレスを使用して再度追加する必要があります。

作業を開始する前に

HTTPアプリケーション用のユーザアカウントを作成し、（少なくとも読み取り専用）アクセスを持つロールを割り当てたことを確認します。 `/api/network/ip/interfaces` REST API： ユーザの作成の詳細については、を参照してください。 "Security login role create を実行します" および "security login create を実行します" コマンド 管理SVM用に認証トンネルSVMを追加して、ドメインユーザをアカウントとして使用することもできます。 詳細については、を参照してください "security login domain-tunnel createのように設定します" ONTAPのマニュアルページ

手順

1. Antivirus Connectorのインストールの完了時にデスクトップに保存されていた*アイコンを右クリックし、[Run as Administrator]*を選択します。[Configure ONTAP LIF]ダイアログボックスが開きます。

2. SVMのIPアドレスを選択し、*[更新]*をクリックします。
3. 必要に応じて情報を更新します。
4. [保存]*をクリックして、レジストリの接続の詳細を更新します。
5. 接続のリストをレジストリインポートまたはレジストリエクスポートファイルにエクスポートする場合は、*エクスポート*をクリックします。 これは、複数のVscanサーバが同じ管理LIFまたはデータLIFのセットを使用する場合に便利です。

**Antivirus Connector**から**SVM**接続を削除する

不要になったSVM接続は削除できます。

手順

1. Antivirus Connectorのインストールの完了時にデスクトップに保存されていた*アイコンを右クリックし、[Run as Administrator]*を選択します。[Configure ONTAP LIF]ダイアログボックスが開きます。
2. SVMのIPアドレスを1つ以上選択し、*[削除]*をクリックします。
3. [保存]*をクリックして、レジストリの接続の詳細を更新します。
4. 接続のリストをレジストリインポートまたはレジストリエクスポートファイルにエクスポートする場合は、*エクスポート*をクリックします。 これは、複数のVscanサーバが同じ管理LIFまたはデータLIFのセットを使用する場合に便利です。

トラブルシューティングを行う

作業を開始する前に

この手順でレジストリ値を作成する場合は、右側のペインを使用します。

診断目的でAntivirus Connectorログを有効または無効にすることができます。デフォルトでは、これらのログは無効になっています。パフォーマンスを強化するには、Antivirus Connectorのログを無効なままにし、重大イベントに対してのみ有効にする必要があります。

手順

1. [スタート]*を選択し、検索ボックスに「regedit」と入力して、 `regedit.exe` をクリックします。
2. レジストリエディタ*で、ONTAP Antivirus Connectorの次のサブキーを探します。
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. 次の表に示すタイプ、名前、および値を指定して、レジストリ値を作成します。

| を入力します | 名前 | 値 |
|---|---|---|
| 文字列 | トレースパス | C：\ avshim.log |

   このレジストリ値には、他の有効なパスを指定できます。

4. 次の表に示すタイプ、名前、値、およびログ情報を指定して、別のレジストリ値を作成します。

| を入力します | 名前 | 重要なロギング | 中間ロギング | 詳細なロギング |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| DWORD | トレースレベル | 1. | 2または3 | 4. |

これにより、手順3でTracePathに指定したパス値に保存されるAntivirus Connectorログが有効になります。

5. 手順3および4で作成したレジストリ値を削除して、Antivirus Connectorログを無効にします。
6. 「LogRotation」という名前でタイプ「multi_sz」の別のレジストリ値を作成します（引用符なし）。"LogRotation"で、 ローテーションサイズのエントリとして「logFileSize:1」を指定し（1は1MBを表します）、次の行では「logFileCount:5」を ローテーションの制限（5が制限）を入力します。

> これらの値はオプションです。指定しない場合は、ローテーションサイズとローテーションの上限にそれぞれデフォルト値の20MBと10ファイルが使用されます。指定された整数値には、小数または小数の値は指定されません。デフォルト値よりも大きい値を指定した場合は、代わりにデフォルト値が使用されます。

7. ユーザー設定のログローテーションを無効にするには、手順6で作成したレジストリ値を削除します。

カスタマイズ可能なバナー

カスタムバナーを使用すると、法的拘束力のあるステートメントとシステムアクセスに関する免責事項を_Configure ONTAP LIFAPI_windowに配置できます。

ステップ

1. の内容を更新してデフォルトバナーを変更します。 `banner.txt` ファイルをインストールディレクトリに保存し、変更を保存します。 変更内容がバナーに反映されるようにするには、[Configure ONTAP LIF] ウィンドウを再度開いてください。

**Extended Ordinance（EO）モードを有効にする**

セキュアな運用のために、拡張規則（EO）モードを有効または無効にすることができます。

手順

1. [スタート]*を選択し、検索ボックスに「regedit」と入力して、 `regedit.exe` をクリックします。
2. レジストリエディタ*で、ONTAP Antivirus Connectorの次のサブキーを探します。
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. 右側のペインで、EOモードを有効にするには「EO_Mode」（引用符なし）と値「1」（引用符なし）という名前の「DWORD」タイプの新しいレジストリ値を作成し、EOモードを無効にするには「0」（引用符なし）を作成します。

> デフォルトでは、 `EO_Mode` レジストリエントリがありません。EOモードは無効です。EOモードをイネーブルにする場合は、外部syslogサーバと相互証明書認証の両方を設定する必要があります。

外部**syslog**サーバの設定

作業を開始する前に

この手順でレジストリ値を作成する場合は、右側のペインを使用することに注意してください。

手順

1. [スタート]*を選択し、検索ボックスに「regedit」と入力して、 `regedit.exe` をクリックします。
2. レジストリエディタ*で、syslog設定用のONTAP Antivirus Connector用の次のサブキーを作成します。
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
3. 次の表に示すように、タイプ、名前、および値を指定してレジストリ値を作成します。

   | を入力します | 名前 | 価値 |
   | --- | --- | --- |
   | DWORD | syslog_enabled | 1または0 |

   値「1」はsyslogを有効にし、値「0」はsyslogを無効にすることに注意してください。

4. 次の表に示す情報を指定して、別のレジストリ値を作成します。

   | を入力します | 名前 |
   | --- | --- |
   | REG_SZ | syslog_host |

   [Value]フィールドにsyslogホストのIPアドレスまたはドメイン名を入力します。

5. 次の表に示す情報を指定して、別のレジストリ値を作成します。

   | を入力します | 名前 |
   | --- | --- |
   | REG_SZ | syslog_port |

   [Value]フィールドに、syslogサーバが実行されているポート番号を入力します。

6. 次の表に示す情報を指定して、別のレジストリ値を作成します。

   | を入力します | 名前 |
   | --- | --- |
   | REG_SZ | syslog_protocol |

   syslogサーバで使用中のプロトコル（「tcp」または「udp」）を[Value]フィールドに入力します。

7. 次の表に示す情報を指定して、別のレジストリ値を作成します。

   | を入力します | 名前 | LOG_CRIT | LOG_NOTICE | ログ情報 | LOG_DEBUG |
   | --- | --- | --- | --- | --- | --- |
   | DWORD | syslog_level | 2. | 5. | 6. | 7. |

8. 次の表に示す情報を指定して、別のレジストリ値を作成します。

| を入力します | 名前 | 価値 |
| --- | --- | --- |
| DWORD | syslog_tls | 1または0 |

値「1」はTransport Layer Security（TLS）でsyslogを有効にし、値「0」はTLSでsyslogを無効にすることに注意してください。

設定された外部**syslog**サーバがスムーズに動作することを確認する

- キーが存在しない場合、またはnull値がある場合は、次の手順を実行します。
  - プロトコルのデフォルトは「TCP」です。
  - ポートのデフォルトは、プレーンな「TCP/UDP」の場合は「514」、TLSの場合は「6514」です。
  - syslogレベルのデフォルト値は5（log_notice）です。
- syslogが有効になっていることを確認するには、 `syslog_enabled` 値は「1」です。をクリックします `syslog_enabled` 値は「1」です。EOモードが有効かどうかに関係なく、設定されたリモートサーバにログインできます。
- EOモードが「1」に設定されていて、 `syslog_enabled` 「1」から「0」までの値。以下が適用されます。
  - syslogがEOモードでイネーブルになっていない場合は、サービスを開始できません。
  - システムが安定した状態で実行されている場合は、EOモードでsyslogを無効にできず、syslogが強制的に「1」に設定されていることを示す警告が表示されます。これはレジストリに表示されます。この場合は、まずEOモードをディセーブルにしてから、syslogをディセーブルにする必要があります。
- EOモードおよびsyslogが有効になっているときにsyslogサーバが正常に実行できない場合、サービスの実行は停止します。これは、次のいずれかの理由で発生する可能性があります。
  - syslog_hostが無効であるか、設定されていません。
  - UDPまたはTCP以外の無効なプロトコルが設定されています。
  - ポート番号が無効です。
- TCPまたはTLS over TCP構成では、サーバがIPポートをリッスンしていない場合、接続は失敗し、サービスはシャットダウンします。

**X.509**相互証明書認証の設定

管理パス内のAntivirus ConnectorとONTAP間のSecure Sockets Layer（SSL）通信では、X.509証明書ベースの相互認証が可能です。EOモードが有効になっていて証明書が見つからない場合、AVコネクタは終了します。Antivirus Connectorで次の手順を実行します。

手順

1. Antivirus Connectorは、Antivirus Connectorのインストールディレクトリを実行するディレクトリパスで、Antivirus Connectorクライアント証明書とNetAppサーバの認証局（CA）証明書を検索します。証明書をこの固定ディレクトリパスにコピーします。
2. クライアント証明書とその秘密鍵をPKCS12形式で埋め込み、「av_client.p12」という名前を付けます。
3. NetAppサーバの証明書への署名に使用したCA証明書（およびルートCAまでの中間署名機関）が、Privacy Enhanced Mail（PEM）形式で「ontap_CA.pem」という名前のものであることを確認します。Antivirus Connectorインストールディレクトリに配置します。NetApp ONTAPシステムで、Antivirus

Connectorのクライアント証明書に「client-ca」タイプの証明書として署名するためのCA証明書（およびルートCAまでの中間署名機関）を「ONTAP」にインストールします。

# スキャナプールを設定

## スキャナプールの概要の設定

スキャナプールは、 SVM に接続できる Vscan サーバと特権ユーザを定義します。スキャナポリシーは、スキャナプールがアクティブかどうかを決定します。

> SMBサーバでエクスポートポリシーを使用する場合は、各Vscanサーバをエクスポートポリシーに追加する必要があります。

## 単一クラスタにスキャナプールを作成する

スキャナプールは、 SVM に接続できる Vscan サーバと特権ユーザを定義します。個 々のSVM用またはクラスタ内のすべてのSVM用のスキャナプールを作成できます。

必要なもの

- SVM と Vscan サーバは同じドメインに属しているか、信頼されたドメインに属している必要があります。
- 個 々 のSVM用のスキャナプールを定義する場合は、SVM管理LIFまたはSVMデータLIFにONTAP Antivirus Connectorを設定しておく必要があります。
- クラスタ内のすべてのSVM用のスキャナプールを定義する場合は、クラスタ管理LIFにONTAP Antivirus Connectorを設定しておく必要があります。
- 特権ユーザのリストには、 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が含まれている必要があります。
- スキャナプールの設定が完了したら、サーバへの接続ステータスを確認します。

手順

1. スキャナプールを作成します。

   ```
   vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
   privileged_users
   ```

   - 個々の SVM 用のプールの場合はデータ SVM 、クラスタ内のすべての SVM 用のプールの場合はクラスタ管理 SVM を指定します。
   - 各 Vscan サーバのホスト名には IP アドレスまたは FQDN を指定します。
   - 各特権ユーザのドメイン名とユーザ名を指定します。 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、という名前のスキャナプールを作成します `SP` をクリックします `vs1` SVM：

```
cluster1::> vserver vscan scanner-pool create -vserver vs1 -scanner-pool
SP -hostnames 1.1.1.1,vmwin204-27.fsct.nb -privileged-users
cifs\u1,cifs\u2
```

2. スキャナプールが作成されたことを確認します。

   `vserver vscan scanner-pool show -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner -pool` *`scanner_pool`*

   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、の詳細を表示します `SP` スキャナプール：

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                    Vserver: vs1
                              Scanner Pool: SP
                            Applied Policy: idle
                            Current Status: off
         Cluster on Which Policy Is Applied: -
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                    List of Privileged Users: cifs\u1, cifs\u2
```

   を使用することもできます `vserver vscan scanner-pool show` コマンドを使用してSVMのすべてのスキャナプールを表示します。コマンド構文全体については、コマンドのマニュアルページを参照してください。

## MetroCluster 構成でスキャナプールを作成

MetroCluster 構成の各クラスタには、クラスタのプライマリとセカンダリの SVM に対応するプライマリとセカンダリのスキャナプールを作成する必要があります。

必要なもの

- SVM と Vscan サーバは同じドメインに属しているか、信頼されたドメインに属している必要があります。
- 個 々 のSVM用のスキャナプールを定義する場合は、SVM管理LIFまたはSVMデータLIFにONTAP Antivirus Connectorを設定しておく必要があります。
- クラスタ内のすべてのSVM用のスキャナプールを定義する場合は、クラスタ管理LIFにONTAP Antivirus Connectorを設定しておく必要があります。
- 特権ユーザのリストには、 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が含まれ

ている必要があります。

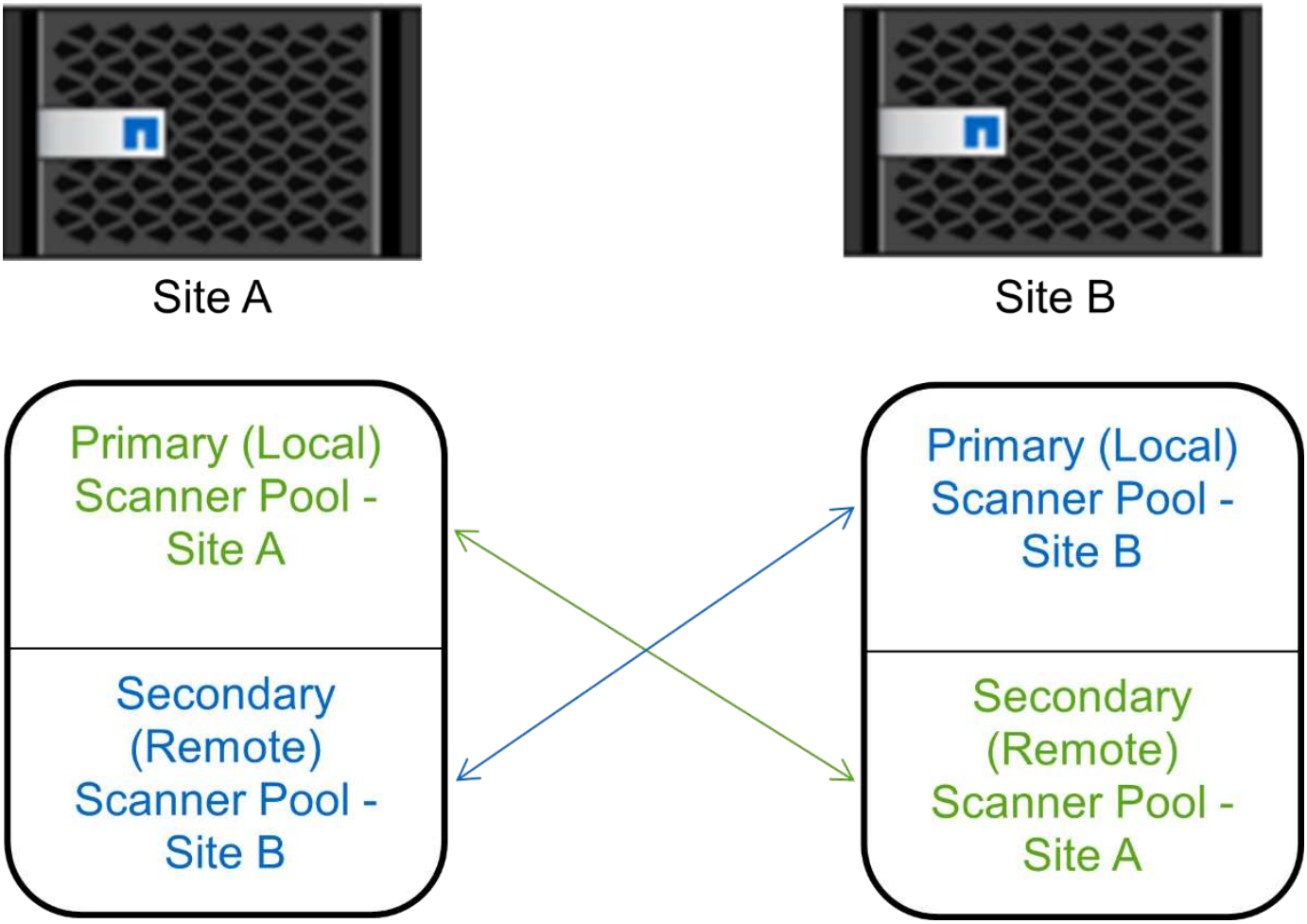
- スキャナプールの設定が完了したら、サーバへの接続ステータスを確認します。

このタスクについて

MetroCluster 構成は、物理的に分離された 2 つのミラークラスタを実装することでデータを保護します。各クラスタが、もう一方のクラスタのデータおよび SVM 設定を同期的にレプリケートします。クラスタがオンラインのときは、ローカルクラスタのプライマリ SVM がデータを提供します。リモートクラスタがオフラインのときは、ローカルクラスタのセカンダリ SVM がデータを提供します。

つまり、MetroCluster構成の各クラスタにプライマリとセカンダリのスキャナプールを作成する必要があり、クラスタがセカンダリSVMからデータの提供を開始すると、セカンダリプールがアクティブになります。ディザスタリカバリ（DR）の設定はMetroClusterと同様です。

この図は、一般的なMetroCluster / DR構成を示しています。




手順

1. スキャナプールを作成します。

   ```
   vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
   privileged_users
   ```

   - 個々の SVM 用のプールの場合はデータ SVM 、クラスタ内のすべての SVM 用のプールの場合はクラスタ管理 SVM を指定します。

- 各 Vscan サーバのホスト名には IP アドレスまたは FQDN を指定します。
- 各特権ユーザのドメイン名とユーザ名を指定します。

> スキャナプールの作成は、すべてプライマリ SVM を含むクラスタから実行する必要があります。

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、 MetroCluster 構成の各クラスタにプライマリとセカンダリのスキャナプールを作成します。

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

2. スキャナプールが作成されたことを確認します。

   `vserver vscan scanner-pool show -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner -pool` *`scanner_pool`*

   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、スキャナプールの詳細を表示します `pool1`：

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                              Scanner Pool: pool1_for_site1
                            Applied Policy: idle
                            Current Status: off
         Cluster on Which Policy Is Applied: -
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                   List of Privileged Users: cifs\u1,cifs\u2
```

を使用することもできます `vserver vscan scanner-pool show` コマンドを使用してSVMのすべてのスキャナプールを表示します。コマンド構文全体については、コマンドのマニュアルページを参照してください。

## 単一のクラスタにスキャナポリシーを適用する

スキャナポリシーは、スキャナプールがアクティブかどうかを決定します。スキャナプールが定義するVscanサーバがSVMに接続できるようにするには、スキャナプールをアクティブ化する必要があります。

このタスクについて

- 1 つのスキャナプールに適用できるスキャナポリシーは 1 つだけです。
- クラスタ内のすべてのSVM用のスキャナプールを作成した場合は、各SVMにスキャナポリシーを個別に適用する必要があります。

手順

1. スキャナポリシーを適用します。

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   cluster_to_apply_policy_on
   ```

   スキャナポリシーには次のいずれかの値が設定されます。

   - `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。

   次の例は、というスキャナプールを示しています `SP` をクリックします `vs1` SVMがアクティブ：

```
cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
-scanner-pool SP  -scanner-policy primary
```

2. スキャナプールがアクティブであることを確認します。

   `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool`

   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、の詳細を表示します `SP` スキャナプール：

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                    Vserver: vs1
                              Scanner Pool: SP
                            Applied Policy: primary
                            Current Status: on
         Cluster on Which Policy Is Applied: cluster1
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                   List of Privileged Users: cifs\u1, cifs\u2
```

   を使用できます `vserver vscan scanner-pool show-active` コマンドを使用して、SVMのアクティブなスキャナプールを表示します。コマンド構文全体については、コマンドのマニュアルページを参照してください。

## MetroCluster 構成でスキャナポリシーを適用

スキャナポリシーは、スキャナプールがアクティブかどうかを決定します。MetroCluster 構成では、各クラスタのプライマリとセカンダリのスキャナプールにスキャナポリシーを適用する必要があります。

このタスクについて

- 1 つのスキャナプールに適用できるスキャナポリシーは 1 つだけです。
- クラスタ内のすべてのSVM用のスキャナプールを作成した場合は、各SVMにスキャナポリシーを個別に適用する必要があります。
- ディザスタリカバリおよびMetroCluster構成では、ローカルクラスタとリモートクラスタ内のすべてのスキャナプールにスキャナポリシーを適用する必要があります。
- ローカルクラスタ用に作成するポリシーでは、でローカルクラスタを指定する必要があります `cluster` パラメータリモートクラスタ用に作成するポリシーでは、 `cluster` パラメータこれにより、災害発生時

にリモートクラスタがウィルススキャン処理をテイクオーバーできるようになります。

手順

1. スキャナポリシーを適用します。

   `vserver vscan scanner-pool apply-policy -vserver` *`data_SVM`* `-scanner-pool` *`scanner_pool`* `-scanner-policy primary|secondary|idle -cluster` *`cluster_to_apply_policy_on`*

   スキャナポリシーには次のいずれかの値が設定されます。

   - `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。

   > スキャナポリシーの適用は、すべてプライマリ SVM を含むクラスタから実行する必要があります。

   次のコマンドは、 MetroCluster 構成の各クラスタのプライマリとセカンダリのスキャナプールにスキャナポリシーを適用します。

```
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site1 -scanner-policy secondary -cluster
cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site2 -scanner-policy primary -cluster cluster2

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site2 -scanner-policy secondary -cluster
cluster2
```

2. スキャナプールがアクティブであることを確認します。

   `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool`

   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、スキャナプールの詳細を表示します `pool1`：

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                              Scanner Pool: pool1_for_site1
                            Applied Policy: primary
                            Current Status: on
         Cluster on Which Policy Is Applied: cluster1
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                   List of Privileged Users: cifs\u1,cifs\u2
```

を使用できます `vserver vscan scanner-pool show-active` コマンドを使用して、SVMのアクティブなスキャナプールを表示します。コマンド構文全体については、コマンドのマニュアルページを参照してください。

## スキャナプールの管理用コマンド

スキャナプールを変更および削除し、スキャナプールの特権ユーザと Vscan サーバを管理できます。また、スキャナプールに関する概要情報を確認することもできます。

| 状況 | 入力するコマンド |
|---|---|
| スキャナプールを変更 | `vserver vscan scanner-pool modify` |
| スキャナプールを削除します | `vserver vscan scanner-pool delete` |
| スキャナプールに特権ユーザを追加する | `vserver vscan scanner-pool privileged-users add` |
| スキャナプールから特権ユーザを削除します | `vserver vscan scanner-pool privileged-users remove` |
| スキャナプールに Vscan サーバを追加する | `vserver vscan scanner-pool servers add` |
| スキャナプールから Vscan サーバを削除します | `vserver vscan scanner-pool servers remove` |
| スキャナプールの概要と詳細を表示します | `vserver vscan scanner-pool show` |
| スキャナプールの特権ユーザを表示します | `vserver vscan scanner-pool privileged-users show` |

| | |
|---|---|
| すべてのスキャナプールの Vscan サーバを表示します | `vserver vscan scanner-pool servers 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。

# オンアクセススキャンを設定します

## オンアクセスポリシーを作成します

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 用またはクラスタ内のすべての SVM 用に作成できます。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。

このタスクについて

- 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。
- を設定できます `scan-mandatory` オフにすると、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が許可されます。
- 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。
- に基づいてスキャン除外の対象となるすべてのファイル `paths-to-exclude`、 `file-ext-to-exclude`または `max-file-size` パラメータは、 `scan-mandatory` オプションがonに設定されている。（これをチェックしてください "トラブルシューティング" セクションに関連する接続の問題 `scan-mandatory` オプション）
- 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。
- を参照してください "ウィルス対策アーキテクチャ" セクションで、_vscanファイル処理プロファイル_の詳細を確認してください。
- 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。
  - 次のようなファイル拡張子を除外することを検討 `.vhd` および `.tmp` これらの拡張子を持つファイルはスキャンに適していない可能性があるためです。
  - 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。

- オンアクセスポリシーは、 オンデマンドスキャン。のオンアクセススキャンを回避するには、 `-scan -files-with-no-ext` をfalseに設定し、 `-file-ext-to-exclude` すべての拡張子を除外するには、を指定します。

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` を設定すると、が上書きされます `-file-ext-to-include` 設定：
   - 設定 `-scan-files-with-no-ext` trueに設定すると、拡張子のないファイルがスキャンされます。次のコマンドは、という名前のオンアクセスポリシーを作成します `Policy1` をクリックします `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. 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、の詳細を表示します `Policy1` ポリシー：

```
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します

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、という名前のオンアクセスポリシーを有効にします `Policy1` をクリックします `vs1` SVM：

   ```
   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、の詳細を表示します `Policy1` オンアクセスポリシー：

```
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します

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ます `standard`。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。

を参照してください "ウィルス対策アーキテクチャ" セクションで、_vscanファイル処理プロファイル_の詳細を確認してください。

> が含まれているSMB共有ではウィルススキャンは実行されません。 `continuously-available` パラメータをに設定します `Yes`。

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ます。 `strict`：

   ```
   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を管理するためのコマンド

オンアクセスポリシーは変更、無効化、または削除できます。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します | `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します | `vserver vscan on-access-policy enable` |
| オンアクセスポリシーを無効にします | `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します | `vserver vscan on-access-policy show` |
| 対象から除外するパスをリストに追加します | `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します | `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します | `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します | `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します | `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します | `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します | `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します | `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。

# オンデマンドスキャンを設定する

## オンデマンドスキャンの概要を設定する

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。

たとえば、ピーク時を避けてスキャンを実行する場合や、オンアクセススキャンの対象外の大容量ファイルのスキャンを実行する場合などに便利です。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できます。

このトピックについて

- スケジュールはタスクの作成時に割り当てることができます。
- SVM で同時にスケジュールできるタスクは 1 つだけです。
- オンデマンドスキャンでは、シンボリックリンクやストリームファイルのスキャンはサポートされません。

> オンデマンドスキャンでは、シンボリックリンクやストリームファイルのスキャンはサポートされません。

> 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。

## オンデマンドタスクを作成する

オンデマンドタスクは、オンデマンドウィル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、およびスキャン対象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がスキャンされます。

このタスクについて

- SVMごとに最大10個のオンデマンドタスクを作成できますが、アクティブにできるのは1つだけです。
- オンデマンドタスクは、スキャンに関連する統計情報を含むレポートを作成します。このレポートには、コマンドを使用するか、タスクによって作成されたレポートファイルを定義された場所にダウンロードしてアクセスできます。

作業を開始する前に

- が必要です オンアクセスポリシーを作成しました。。デフォルトのポリシーでもユーザが作成したポリシーでもかまいません。オンアクセスポリシーがないと、スキャンを有効にできません。

手順

1. オンデマンドタスクを作成します。

   ```
   vserver vscan on-demand-task create -vserver data_SVM -task-name task_name
   -scan-paths paths_of_files_to_scan -report-directory report_directory_path
   -report-expiry-time expiration_time_for_report -schedule cron_schedule -max
   -file-size max_size_of_files_to_scan -paths-to-exclude paths -file-ext-to
   -exclude file_extensions -file-ext-to-include file_extensions -scan-files-with
   -no-ext true|false -directory-recursion true|false
   ```

   - 。 `-file-ext-to-exclude` を設定すると、が上書きされます `-file-ext-to-include` 設定：
   - 設定 `-scan-files-with-no-ext` trueに設定すると、拡張子のないファイルがスキャンされます。

     すべてのオプションの一覧については、を参照してください。 "コマンドリファレンス"。

     次のコマンドは、という名前のオンデマンドタスクを作成します。 `Task1` vs1 VMで次の手順を実行します。

   ```
   cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name
   Task1 -scan-paths "/vol1/","/vol2/cifs/" -report-directory "/report"
   -schedule daily -max-file-size 5GB -paths-to-exclude "/vol1/cold-files/"
   -file-ext-to-include "vmdk?","mp*" -file-ext-to-exclude "mp3","mp4"
   -scan-files-with-no-ext false
   [Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
   command to view the status.
   ```

   +

   > を使用できます `job show` コマンドを使用してジョブのステータスを表示します。を使用できます `job pause` および `job resume` ジョブを一時停止および再開するコマンド、または `job stop` コマンドを使用してジョブを終了します。

2. オンデマンドタスクが作成されたことを確認します。

   ```
   vserver vscan on-demand-task show -instance data_SVM -task-name task_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、の詳細を表示します `Task1` タスク：

```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task-name
Task1

                            Vserver: vs1
                          Task Name: Task1
                 List of Scan Paths: /vol1/, /vol2/cifs/
              Report Directory Path: /report
                       Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk?, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                  Report Log Level: info
        Expiration Time for Report: -
```

完了後

タスクの実行をスケジュールする前に、 SVM でスキャンを有効にする必要があります。

## オンデマンドタスクのスケジュールを設定します

スケジュールを割り当てずにタスクを作成し、 `vserver vscan on-demand-task schedule` コマンドを使用してスケジュールを割り当てるか、タスクの作成時にスケジュールを追加します。

このタスクについて

で割り当てられたスケジュール `vserver vscan on-demand-task schedule` このコマンドは、ですでに割り当てられているスケジュールを上書きします `vserver vscan on-demand-task create` コマンドを実行します

手順

1. オンデマンドタスクのスケジュールを設定します。

   `vserver vscan on-demand-task schedule -vserver` *`data_SVM`* `-task-name` *`task_name`* `-schedule cron_schedule`

   次のコマンドは、という名前のオンアクセスタスクをスケジュールします `Task2` をクリックします `vs2` SVM：

```
cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task
-name Task2 -schedule daily
[Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142"
command to view the status.
```

ジョブのステータスを表示するには、 `job show` コマンドを実行します。 `job pause` および `job resume` ジョブをそれぞれ一時停止および再開するコマンド。 `job stop` コマンドを実行すると、ジョブが終了します。

2. オンデマンドタスクがスケジュールされていることを確認します。

   `vserver vscan on-demand-task show -instance` *`data_SVM`* `-task-name` *`task_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、の詳細を表示します `Task 2` タスク：

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task-name
Task2

                            Vserver: vs2
                          Task Name: Task2
                List of Scan Paths: /vol1/, /vol2/cifs/
              Report Directory Path: /report
                       Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                  Report Log Level: info
```

完了後

タスクの実行をスケジュールする前に、 SVM でスキャンを有効にする必要があります。

## オンデマンドタスクをただちに実行します

オンデマンドタスクは、スケジュールが割り当てられているかどうかに関係なく、ただちに実行することもできます。

作業を開始する前に

SVM でスキャンを有効にしておく必要があります。

ステップ

1. オンデマンドタスクをただちに実行します。

   `vserver vscan on-demand-task run -vserver data_SVM -task-name task_name`

   次のコマンドは、という名前のオンアクセスタスクを実行します `Task1` をクリックします `vs1` SVM：

   ```
   cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name
   Task1
   [Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161"
   command to view the status.
   ```

   を使用できます `job show` コマンドを使用してジョブのステータスを表示します。を使用できます `job pause` および `job resume` ジョブを一時停止および再開するコマンド、または `job stop` コマンドを使用してジョブを終了します。

## オンデマンドタスクを管理するためのコマンドです

オンデマンドタスクを変更、削除、またはスケジュールを解除できます。タスクの概要と詳細を表示し、タスクのレポートを管理できます。

| 状況 | 入力するコマンド |
|---|---|
| オンデマンドタスクを作成する | `vserver vscan on-demand-task create` |
| オンデマンドタスクを変更する | `vserver vscan on-demand-task modify` |
| オンデマンドタスクを削除する | `vserver vscan on-demand-task delete` |
| オンデマンドタスクを実行する | `vserver vscan on-demand-task run` |
| オンデマンドタスクのスケジュールを設定します | `vserver vscan on-demand-task schedule` |
| オンデマンドタスクのスケジュールを解除します | `vserver vscan on-demand-task unschedule` |
| オンデマンドタスクの概要と詳細を表示する | `vserver vscan on-demand-task show` |
| オンデマンドレポートを表示します | `vserver vscan on-demand-task report show` |

| | |
|---|---|
| オンデマンドレポートを削除する | `vserver vscan on-demand-task report delete` |

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。

# ONTAPで外部接続式のウィルス対策機能を設定するためのベストプラクティス

ONTAPでオフボックス機能を設定する場合は、次の推奨事項を考慮してください。

- 特権ユーザのウィルススキャン処理を制限します。通常のユーザは、特権ユーザクレデンシャルを使用しないでください。この制限は、Active Directoryの特権ユーザのログイン権限を無効にすることで実現できます。
- AdministratorsグループやBackup Operatorsグループなど、ドメイン内で多数の権限を持つユーザグループには、特権ユーザを含める必要はありません。特権ユーザは、Vscanサーバ接続の確立およびウィルススキャン用ファイルへのアクセスを許可するために、ストレージシステムでのみ検証する必要があります。
- Vscanサーバを実行しているコンピュータは、ウィルススキャンの目的でのみ使用してください。一般的な使用を避けるには、これらのマシンのWindowsターミナルサービスおよびその他のリモートアクセスプロビジョニングを無効にし、これらのマシンに新しいソフトウェアをインストールする権利を管理者のみに付与します。
- Vscanサーバはウィルススキャン専用にし、バックアップなどの他の処理には使用しないでください。Vscanサーバを仮想マシン（VM）として実行することもできます。VscanサーバをVMとして実行する場合は、VMに割り当てられているリソースが共有されておらず、ウィルススキャンを実行するのに十分であることを確認してください。
- Vscanサーバに適切なCPU、メモリ、およびディスク容量を提供して、リソースの過剰割り当てを回避します。ほとんどのVscanサーバは、複数のCPUコアサーバを使用してCPU間で負荷を分散するように設計されています。
- SVMからVscanサーバへの接続には、スキャントラフィックが他のクライアントネットワークトラフィックの影響を受けないように、専用ネットワークとプライベートVLANを使用することを推奨します NetApp。Vscanサーバ上のウィルス対策VLAN専用およびSVM上のデータLIF専用の、独立したネットワークインターフェイスカード（NIC）を作成します。この手順により、ネットワークの問題が発生した場合の管理とトラブルシューティングが簡単になります。アンチウイルストラフィックは、プライベートネットワークを使用して分離する必要があります。ウィルス対策サーバは、次のいずれかの方法でドメインコントローラ（DC）およびONTAPと通信するように設定する必要があります。
  - DCは、トラフィックの分離に使用されるプライベートネットワークを介してアンチウイルスサーバと通信する必要があります。
  - DCサーバとウィルス対策サーバは、CIFSクライアントネットワークとは異なる別のネットワーク（前述のプライベートネットワークではない）を介して通信する必要があります。
  - ウィルス対策通信でKerberos認証を有効にするには、プライベートLIF用のDNSエントリと、プライベートLIF用に作成したDNSエントリに対応するサービスプリンシパル名をDC上に作成します。この名前は、Antivirus ConnectorにLIFを追加するときに使用します。DNSは、Antivirus Connectorに接続されている各プライベートLIFに対して一意の名前を返すことができる必要があります。

Vscanトラフィック用のLIFがクライアントトラフィック用のLIFとは別のポートに設定されている場合、ポート障害が発生したときにVscan LIFが別のノードにフェイルオーバーする可能性があります。変更によって新しいノードからVscanサーバに到達できなくなり、ノード上のファイル処理に関するスキャン通知が失敗します。ノード上の少なくとも1つのLIFを介してVscanサーバにアクセスできることを確認し、そのノードで実行されたファイル処理のスキャン要求を処理できるようにします。

- 少なくとも1GbEネットワークを使用して、NetAppストレージシステムとVscanサーバを接続します。
- 複数のVscanサーバがある環境では、同様の高パフォーマンスネットワーク接続があるすべてのサーバを接続します。Vscanサーバを接続すると、負荷を分散できるためパフォーマンスが向上します。
- リモートサイトやブランチオフィスには、NetAppではリモートのVscanサーバではなくローカルのVscanサーバを使用することを推奨します。これは、Vscanサーバが高レイテンシの場合に最適なサーバであるためです。コストが要因の場合は、中程度のウイルス保護のためにラップトップまたはPCを使用してください。ボリュームまたはqtreeを共有し、リモートサイトの任意のシステムからスキャンすることで、ファイルシステム全体の定期的なスキャンをスケジュールできます。
- 複数のVscanサーバを使用してSVM上のデータをスキャンし、ロードバランシングと冗長性を確保します。CIFSワークロードとその結果のウィルス対策トラフィックの量は、SVMごとに異なります。ストレージコントローラでCIFSとウィルススキャンのレイテンシを監視します。時間の経過に伴う結果の傾向を監視します。VscanサーバのCPUキューやアプリケーションキューが原因でCIFSのレイテンシやウィルススキャンのレイテンシがトレンドのしきい値を超えて上昇すると、CIFSクライアントの待機時間が長くなることがあります。Vscanサーバを追加する 負荷を分散するため。
- 最新バージョンのONTAP Antivirus Connectorをインストールします。
- ウィルス対策エンジンと定義を最新の状態に維持します。更新頻度に関する推奨事項については、パートナーにお問い合わせください。
- マルチテナンシー環境では、VscanサーバとSVMが同じドメインまたは信頼されたドメインに属している場合は、スキャナプール（Vscanサーバのプール）を複数のSVMで共有できます。
- 感染したファイルのウィルス対策ソフトウェアポリシーは、ほとんどのウィルス対策ベンダーで設定されているデフォルト値である「delete」または「quarantine」に設定する必要があります。「vscan-fileop-profile」が「write_only」に設定されていて、感染したファイルが見つかった場合、ファイルは共有に残り、ファイルを開いてもスキャンはトリガーされないため開くことができます。アンチウイルススキャンは、ファイルが閉じられた後にのみトリガーされます。
- 。 `scan-engine timeout` 値は次の値より小さくする必要があります： `scanner-pool request-timeout` 価値。 この値を大きい値に設定すると、ファイルへのアクセスに遅延が生じ、最終的にタイムアウトする可能性があります。 これを回避するには、 `scan-engine timeout` 5秒未満 `scanner-pool request-timeout` 価値。の変更方法については、スキャンエンジンベンダーのマニュアルを参照してください。 `scan-engine timeout` 設定：。 `scanner-pool timeout` 次のコマンドをアドバンスモードで使用し、 `request-timeout` パラメータ： `vserver vscan scanner-pool modify`。
- オンアクセススキャンのワークロード向けにサイジングされていて、オンデマンドスキャンの使用が必要な環境では、NetAppでは、既存のウィルス対策インフラへの負荷の増大を避けるために、オンデマンドスキャンジョブをオフピークの時間帯にスケジュールすることを推奨しています。

パートナー様固有のベストプラクティスの詳細については、 "Vscanパートナーソリューション"。

# SVM でウィルススキャンを有効にします

オンアクセススキャンまたはオンデマンドスキャンを実行するには、 SVM でウィルス

スキャンを有効にする必要があります。

手順

1. SVM でウィルススキャンを有効にします。

   ```
   vserver vscan enable -vserver data_SVM
   ```

   を使用できます `vserver vscan disable` ウィルススキャンを無効にするコマンド（必要な場合）。

   次のコマンドは、でウィルススキャンを有効にします `vs1` SVM：

   ```
   cluster1::> vserver vscan enable -vserver vs1
   ```

2. SVM でウィルススキャンが有効になっていることを確認します。

   ```
   vserver vscan show -vserver data_SVM
   ```

   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、のVscanステータスを表示します `vs1` SVM：

   ```
   cluster1::> vserver vscan show -vserver vs1

                              Vserver: vs1
                         Vscan Status: on
   ```

# スキャン済みファイルのステータスをリセットします

SVMでスキャンに成功したファイルのスキャンステータスををを使用してリセットすることもできます `vserver vscan reset` コマンドを使用して、ファイルのキャッシュされた情報を破棄します。このコマンドを使用すると、たとえばスキャン設定に誤りがあった場合にウィルススキャン処理を再開できます。

このタスクについて

を実行したあと `vserver vscan reset` コマンドを実行すると、対象となるすべてのファイルが次回アクセスされたときにスキャンされます。

このコマンドを使用すると、再スキャンするファイルの数やサイズによっては、パフォーマンスが低下する可能性があります。

必要なもの

このタスクを実行するには advanced 権限が必要です。

手順

1. advanced 権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. スキャン済みファイルのステータスをリセットします。

   ```
   vserver vscan reset -vserver data_SVM
   ```

   次のコマンドは、のスキャン済みファイルのステータスをリセットします `vs1` SVM：

   ```
   cluster1::> vserver vscan reset -vserver vs1
   ```

# Vscan イベントログ情報を表示します

を使用できます `vserver vscan show-events` コマンドを使用して、感染したファイル、Vscanサーバの更新などに関するイベントログ情報を表示します。クラスタ、特定のノード、 SVM 、または Vscan サーバについてのイベント情報を表示できます。

作業を開始する前に

Vscanイベントログを表示するにはadvanced権限が必要です。

手順

1. advanced 権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. Vscan イベントログ情報を表示します。

   ```
   vserver vscan show-events
   ```

   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、クラスタのイベントログ情報を表示します `cluster1`：

```
cluster1::*> vserver vscan show-events

Vserver     Node            Server          Event Type        Event Time
----------- --------------- --------------- -----------------
-----------------
vs1         Cluster-01      192.168.1.1     file-infected     9/5/2014
11:37:38
vs1         Cluster-01      192.168.1.1     scanner-updated   9/5/2014
11:37:08
vs1         Cluster-01      192.168.1.1     scanner-connected 9/5/2014
11:34:55
3 entries were displayed.
```

# 接続の問題の監視とトラブルシューティング

## **scan-mandatory** オプションの使用時に発生する可能性がある接続の問題

を使用できます `vserver vscan connection-status show` 接続の問題のトラブルシューティングに役立つVscanサーバ接続に関する情報を表示するコマンド。

デフォルトでは、が表示されます `scan-mandatory` オンアクセススキャンのオプションを指定すると、Vscanサーバ接続をスキャンに使用できない場合にファイルアクセスが拒否されます。このオプションは重要な安全機能を備えていますが、いくつかの状況で問題が発生する可能性があります。

- クライアントアクセスを有効にする前に、 LIF が設定された各ノードの SVM に少なくとも 1 つの Vscan サーバが接続されていることを確認する必要があります。クライアントアクセスを有効にしたあとにサーバをSVMに接続する必要がある場合は、をオフにする必要があります `scan-mandatory` オプションを使用して、Vscanサーバ接続を使用できないためにファイルアクセスが拒否されないようにします。サーバの接続が完了したら、オプションをオンに戻すことができます。
- 1 つのターゲット LIF で SVM のすべての Vscan サーバ接続をホストしている場合、その LIF を移行するとサーバと SVM の間の接続が失われます。Vscanサーバ接続を使用できないためにファイルアクセスが拒否されないようにするには、をオフにする必要があります `scan-mandatory` オプションを選択してください。LIF の移行が完了したら、オプションをオンに戻すことができます。

各 SVM に少なくとも 2 つの Vscan サーバを割り当てる必要があります。ストレージシステムへの Vscan サーバの接続には、クライアントアクセスとは別のネットワークを使用することを推奨します。

## **Vscan** サーバの接続ステータスを表示するコマンド

を使用できます `vserver vscan connection-status show` Vscanサーバの接続ステータスに関する概要と詳細情報を表示するコマンド。

| 状況 | 入力するコマンド |
|---|---|
| Vscan サーバ接続の概要を表示します | `vserver vscan connection-status show` |

| 状況 | 入力するコマンド |
| --- | --- |
| Vscan サーバ接続の詳細を表示します | `vserver vscan connection-status show-all` |
| 接続されている Vscan サーバの詳細を表示します | `vserver vscan connection-status show-connected` |
| 接続されていない使用可能な Vscan サーバの詳細を表示します | `vserver vscan connection-status show-not-connected` |

これらのコマンドの詳細については、を参照してください "ONTAP のマニュアルページ"。

## ウィルススキャンのトラブルシューティング

一般的なウイルススキャンの問題については、考えられる原因と解決方法があります。ウィルススキャンはVscanとも呼ばれます。

| 問題 | 解決方法 |
| --- | --- |
| Vscanサーバがに接続できない clustered ONTAPストレージシステム。 | スキャナプールの設定でVscanサーバのIPアドレスが指定されているかどうかを確認します。また、スキャナプールのリストで許可されている特権ユーザがアクティブかどうかも確認します。スキャナプールを確認するには、 `vserver vscan scanner-pool show` コマンドをストレージシステムのコマンドプロンプトで実行します。それでもVscanサーバが接続できない場合は、ネットワークに問題がある可能性があります。 |
| クライアントで高レイテンシが観察されます。 | スキャナプールにVscanサーバを追加するタイミングが来たと考えられます。 |
| トリガーされたスキャンが多すぎます。 | の値を変更します。 `vscan-fileop-profile` パラメータを指定して、ウィルススキャンの対象として監視するファイル操作の数を制限します。 |
| 一部のファイルがスキャンされていません。 | オンアクセスポリシーを確認します。これらのファイルのパスがパス除外リストに追加されているか、ファイルのサイズが除外の設定値を超えている可能性があります。オンアクセスポリシーを確認するには、 `vserver vscan on-access-policy show` コマンドをストレージシステムのコマンドプロンプトで実行します。 |

| | |
|---|---|
| ファイルアクセスが拒否されました。 | ポリシー設定で_scan-mandatory_settingが指定されているかどうかを確認します。この設定では、Vscanサーバが接続されていない場合にデータアクセスが拒否されます。必要に応じて設定を変更します。 |

## ステータスとパフォーマンスアクティビティの監視

## Vscanサーバの接続ステータス、 Vscanサーバの健常性、およびスキャンされたファイルの数。この情報は、 Vscanサーバに関連する問題を診断します。

### **Vscan**サーバの接続情報の表示

Vscanサーバの接続ステータスを表示して、使用中の接続を管理できます。 使用可能な接続が表示されます。 さまざまなコマンドで情報を表示 Vscanサーバの接続ステータスについて

| コマンド… | 表示される情報… |
|---|---|
| `vserver vscan connection-status show` | 接続ステータスの概要 |
| `vserver vscan connection-status show-all` | 接続ステータスに関する詳細情報 |
| `vserver vscan connection-status show-not-connected` | 使用可能だが接続されていない接続のステータス |
| `vserver vscan connection-status show-connected` | 接続されているVscanサーバに関する情報 |

これらのコマンドの詳細については、を参照してください "マニュアルページ"。

### **Vscan**サーバの統計の表示

Vscanサーバ固有の統計を表示して、パフォーマンスを監視し、関連する問題を診断できます。 ウィルススキャン：を使用する前に、データサンプルを収集する必要があります。 `statistics show` コマンドをに送信します Vscanサーバの統計を表示します。 データサンプルを完了するには、次の手順を実行します。

ステップ

1. を実行します `statistics start` コマンドとを実行します `optional statistics` 停止コマンド。

#### **Vscan**サーバ要求とレイテンシの統計を表示する

ONTAPを使用できます。 `offbox_vscan` SVM単位でカウンタを実行してVscan速度を監視 すべてのVscanで1秒あたりに送出および受信されるサーバ要求とサーバレイテンシ サーバ：これらの統計を表示するには、次の手順を実行します。

ステップ

1. statistics showを実行します。 `object offbox_vscan -instance SVM` コマンドにを指定します 次の

カウンタ

| カウンタ… | 表示される情報… |
| --- | --- |
| scan_request_dispatched_rate | ONTAPからVscanサーバに送信される1秒あたりのウィルススキャン要求数 |
| scan_noti_received_rate | ONTAPがVscanサーバから受信した1秒あたりのウィルススキャン要求数 |
| dispatch_latency | 使用可能なVscanサーバを特定してそのVscanサーバに要求を送信するためのONTAP内のレイテンシ |
| scan_latency | ONTAPからVscanサーバへのラウンドトリップレイテンシ（スキャンの実行時間を含む） |

**ONTAP外部Vscanカウンタから生成される統計の例**

```
Object: offbox_vscan
Instance: SVM
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 2 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_noti_received_rate 292
dispatch_latency 43986us
scan_latency 3433501us
-------------------------------------------------------------------
```

個 々 の**Vscan**サーバ要求とレイテンシの統計を表示する

ONTAPを使用できます。 `offbox_vscan_server` SVMごと、オフボックスのVscanサーバごとにカウンタノード単位で監視し、ディスパッチされたVscanサーバ要求の速度とサーバレイテンシを 各Vscanサーバを個別に指定します。この情報を収集するには、次の手順を実行します。

ステップ

1. を実行します `statistics show -object offbox_vscan -instance SVM:servername:nodename` 次のカウンタを指定してコマンドを実行します。

| カウンタ… | 表示される情報… |
| --- | --- |
| scan_request_dispatched_rate | ONTAPから送信されたウィルススキャン要求の数 |

| | |
|---|---|
| scan_latency | ONTAPからVscanサーバへのラウンドトリップレイテンシ（スキャンの実行時間を含む） 1秒あたりのVscanサーバへの転送 |

**ONTAP offbox_vscan_server**カウンタで生成される統計の例

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_latency 3433830us
-----------------------------------------------------------------
```

**Vscan**サーバ使用率の統計を表示する

ONTAPを使用することもできます。 `offbox_vscan_server` Vscanサーバ側の使用率を収集するカウンタ統計：これらの統計は、SVM単位、オフボックスのVscanサーバ単位、ノード単位で追跡されます。彼らはVscanサーバのCPU利用率、Vscanサーバでのスキャン処理のキュー深度を記載 （現在と最大の両方）、使用済みメモリ、および使用済みネットワーク。 これらの統計は、Antivirus ConnectorによってONTAP内の統計カウンタに転送されます。彼らは 20秒ごとにポーリングされ、正確性を保つために複数回収集する必要があるデータに基づいている。 それ以外の場合、統計に表示される値は最後のポーリングのみを反映します。CPUの利用率とキューは 特に監視と分析に重要です。平均キューの値が大きい場合、 Vscanサーバがボトルネックになります。 SVMごと、オフボックスVscanサーバごと、およびノードごとのVscanサーバの使用率の統計を収集するには Basisで、次の手順を実行します。

ステップ

1. Vscanサーバの使用率の統計を収集します。

   を実行します `statistics show -object offbox_vscan_server -instance SVM:servername:nodename` コマンドと次のコマンド `offbox_vscan_server` カウンタ：

| カウンタ… | 表示される情報… |
|---|---|
| scanner_stats_pct_cpu_used | VscanサーバのCPU利用率 |
| scanner_stats_pct_input_queue_avg | Vscanサーバ上のスキャン要求の平均キュー |
| scanner_stats_pct_input_queue_hiwatermark | Vscanサーバでのスキャン要求のピークキュー |

| | |
|---|---|
| scanner_stats_pct_mem_used | Vscanサーバで使用されているメモリ |
| scanner_stats_pct_network_used | Vscanサーバで使用されるネットワーク |

**Vscan**サーバの使用率統計の例

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scanner_stats_pct_cpu_used 51
scanner_stats_pct_dropped_requests 0
scanner_stats_pct_input_queue_avg 91
scanner_stats_pct_input_queue_hiwatermark 100
scanner_stats_pct_mem_used 95
scanner_stats_pct_network_used 4
---------------------------------------------------------------
```