Vscanによるウイルス保護

ONTAP 9

NetApp

February 13, 2026

目次

Vscanによるウイルス保護

ONTAP Vscanを使用したウイルス対策設定について学ぶ

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。

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イルス スキャンを実行します。Vscanは、オンデマンドで、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）や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"

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。

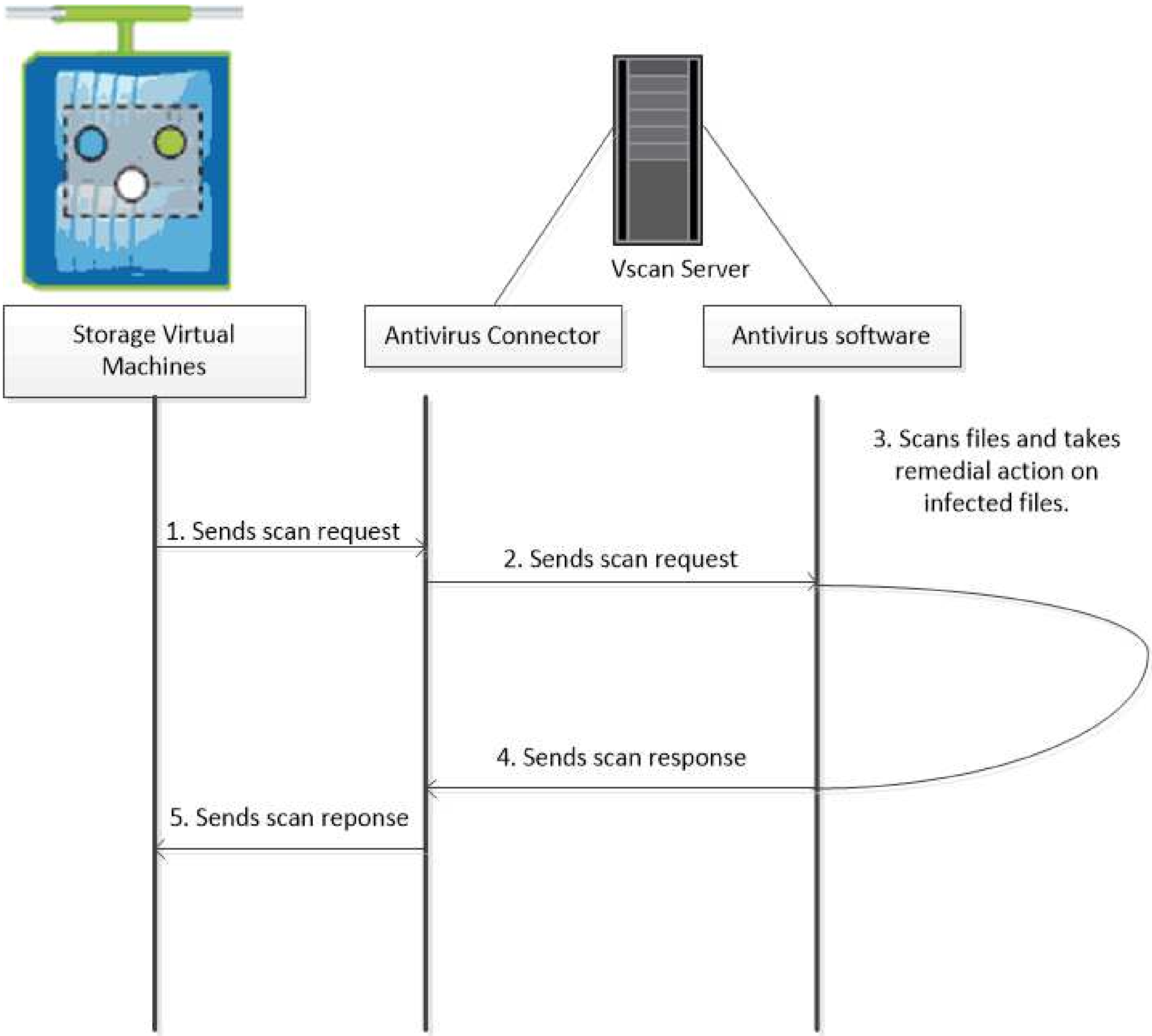
  オンアクセス スキャンは、NFSではサポートされません。

- _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。

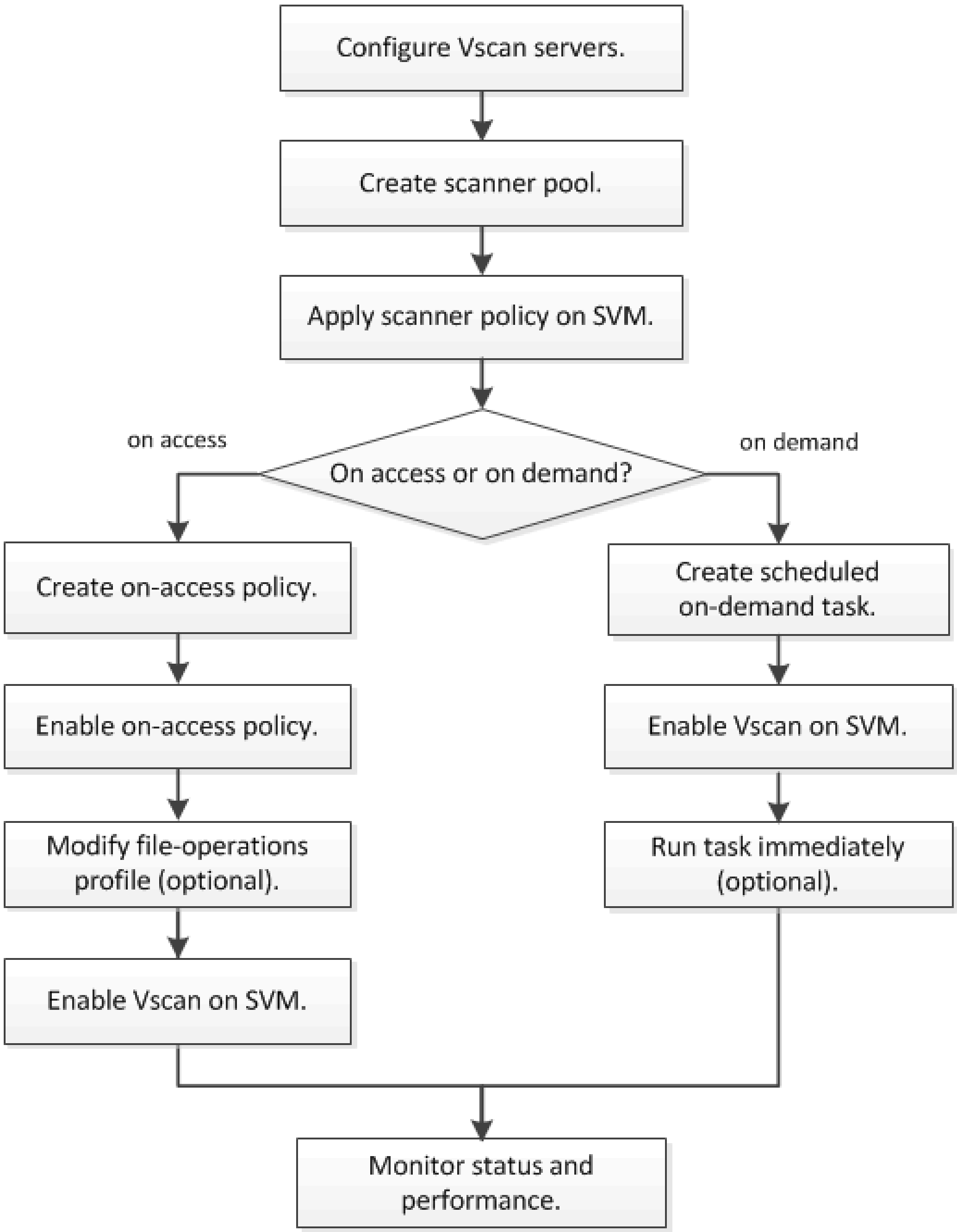
NetAppが提供し、外部サーバにインストールされるONTAP Antivirus Connectorが、ストレージ システムとウイルス対策ソフトウェア間の通信を処理します。



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。

下表に示すように、Trellix、Symantec、Trend Microの相互運用性に関する詳細はNetApp相互運用性マトリックスに掲載されています。Trellix、Symantec、Deep Instinct、OPSWATの相互運用性に関する詳細は、各パートナーのウェブサイトでもご確認いただけます。Sentinel One、Deep Instinct、OPSWAT、およびその他の新規パートナーの相互運用性に関する詳細は、各パートナーのウェブサイトでご確認いただけます。

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"	• "NetApp Interoperability Matrix Tool" • "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

Vscanサーバのインストールと設定

ONTAP Vscan サーバーのインストールと構成

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確実にウイルス スキャンされるようにします。ウイルス対策ソフトウェアのサーバへのインストールと設定については、各ベンダーの手順に従ってください。

NetApp が提供する README ファイルの指示に従って、ONTAP Antivirus Connector をインストールおよび設定してください。または、"ONTAP Antivirus Connectorのインストール ページ" の指示に従ってください。

> ディザスタ リカバリ構成およびMetroCluster構成では、プライマリ / ローカルONTAPクラスタとセカンダリ / パートナーONTAPクラスタのそれぞれに対してVscanサーバを個別に設定する必要があります。

ウイルス対策ソフトウェアの要件

- ウイルス対策ソフトウェアの要件については、ベンダー提供のドキュメントを参照してください。
- Vscan でサポートされているベンダー、ソフトウェア、バージョンについては、"Vscanパートナー ソリューション"ページを参照してください。

ONTAP Antivirus Connectorの要件

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

> クラスター内の異なる Vscan サーバーに異なるバージョンの Windows サーバーをインストールできます。

- Windows Server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 ServerでSMB 2.0が有効になっている必要があります。

ONTAP Vscan アンチウイルス コネクタをインストールする

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するには、ONTAP Antivirus ConnectorをVscanサーバにインストールします。ONTAP Antivirus Connectorをインストールすると、ウイルス対策ソフトウェアが1台以上のStorage Virtual Machine（SVM）と通信できるようになります。

タスク概要

- サポートされているプロトコル、ウイルス対策ベンダー 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サーバーの詳細については、"Vscanパートナー ソリューション"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、NetAppでは、パフォーマンスを最大限に高めるために、ウイルス対策スキャンに専用の物理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WindowsサーバでSMB 2.0が有効になっている必要があります。

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て、ハード ドライブ上の任意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. _Next_を選択します。Destination Folderダイアログボックスが開きます。
3. 次へ を選択して、リストされているフォルダーにウイルス対策コネクタをインストールするか、変更 を選択して別のフォルダーにインストールします。
4. [ONTAP AV Connector Windows Service Credentials]ダイアログ ボックスが開きます。
5. Windowsサービスの認証情報を入力するか、*追加*を選択してユーザーを選択してください。ONTAPシステムの場合、このユーザーは有効なドメインユーザーであり、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. **Next** を選択します。Ready to Install the Program 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*Install*を選択するか、設定を変更したい場合は*Back*を選択してください。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ます。その後、InstallShield Wizard Completedダイアログボックスが表示されます。
8. 続いてONTAP管理LIFまたはデータLIFの設定を行う場合は、[Configure ONTAP LIFs]チェック ボックスをオンにします。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 Installer ログ*を表示する] チェック ボックスをオンにします。
10. *完了*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*ONTAP LIFの設定*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。Antivirus ConnectorにSVMを追加するには、データLIFのリストを取得するためにポーリングするONTAP管理LIFを追加するか、1つ以上のデータLIFを直接設定します。ONTAP管理LIFを設定する場合は、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。
    - 管理LIFまたはSVMのIPアドレスが `management-https`に対して有効になっていることを確認してください。データLIFのみを設定する場合は、この手順は必要ありません。
    - HTTP アプリケーションのユーザー アカウントを作成し、 `/api/network/ip/interfaces` REST API への（少なくとも読み取り専用の）アクセス権を持つロールを割り当てたことを確認します。
    - `security login role create`および `security login create`の詳細については、 "ONTAPコマンド リファレンス"をご覧ください。

管理SVMに認証トンネルSVMを追加することで、ドメインユーザーをアカウントとして使用することもできます。"ONTAPコマンド リファレンス"の `security login domain-tunnel create`の詳細をご覧ください。

手順

1. Antivirus Connector のインストールを完了したときにデスクトップに保存された **Configure ONTAP LIFs** 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。

このタイプの LIF を作成するには…	次の手順を実行します。
Data LIF	a. [role]を[data]に設定する b. [data protocol]を[cifs]に設定する c. [firewall policy]を[data]に設定する d. [service policy]を[default-data-files]に設定する
管理 LIF	a. 「role*」を「data」に設定する b. [data protocol]を[none]に設定する c. [firewall policy]を[mgmt]に設定する d. [service policy]を[default-management]に設定する

"LIFの作成"についての詳細を読む。

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、そのクラスタ内にある、SMBを提供するすべてのSVMで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に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。一意のDNS名が各データLIFに使用できない場合、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名やSPNを追加または変更した場合は、変更を適用するために、VscanサーバでAntivirus Connectorサービスを再起動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。ポーリング期間とは、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期間は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. *Test*をクリックして接続を確認し、認証を検証します。認証は管理LIF構成に対してのみ検証されます。
6. **Update** をクリックして、ポーリングまたは接続する LIF のリストに LIF を追加します。
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. 接続リストをレジストリインポートファイル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には、*エクスポート*をクリックします。これは、複数のVscanサーバーが同じ管理LIFまたはデータLIF

セットを使用している場合に便利です。

設定オプションについては"ONTAP Antivirus Connectorページを設定する"を参照してください。

ONTAP Vscan ウイルス対策コネクタを構成する

ONTAP Antivirus Connectorを設定して、接続するStorage Virtual Machine（SVM）を1つまたは複数指定します。この設定では、ONTAP管理LIF、ポーリング情報、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のみを入力します。また、SVM接続の詳細を変更するか、SVM接続自体を削除することもできます。デフォルトでは、ONTAP管理LIFが設定済みの場合、ONTAP Antivirus ConnectorはREST APIを使用してデータLIFの一覧を取得します。

SVM接続の詳細の変更

Antivirus Connectorに追加済みのStorage Virtual Machine（SVM）の詳細を更新するには、ONTAP管理LIFおよびポーリング情報を変更します。追加済みのデータLIFを更新することはできません。データLIFを更新するには、まず該当のLIFを削除してから、新しいLIFまたはIPアドレスで追加し直す必要があります。

開始する前に

HTTP アプリケーションのユーザー アカウントを作成し、 `/api/network/ip/interfaces` REST API への（少なくとも読み取り専用の）アクセス権を持つロールを割り当てたことを確認します。

```
`security login role create`および `security login create`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-
login-create.html["ONTAPコマンド リファレンス"^]をご覧ください。
```

管理SVMに認証トンネルSVMを追加することで、ドメインユーザーをアカウントとして使用することもできます。 `security login domain-tunnel create`の詳細については、"ONTAPコマンド リファレンス"を参照してください。

手順

1. Antivirus Connectorのインストール完了時にデスクトップに保存された*Configure ONTAP LIFs*アイコンを右クリックし、*管理者として実行*を選択します。Configure ONTAP LIFsダイアログボックスが開きます。
2. SVM 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、レジストリ内の接続の詳細を更新します。
5. 接続リストをレジストリインポートファイル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のセットを使用している場合に便利です。

Antivirus ConnectorからのSVM接続の削除

不要になったSVM接続は削除できます。

手順

1. Antivirus Connectorのインストール完了時にデスクトップに保存された*Configure ONTAP LIFs*アイコンを右クリックし、*管理者として実行*を選択します。Configure ONTAP LIFsダイアログボックスが開きます。
2. 1 つ以上の SVM IP アドレスを選択し、*削除*をクリックします。
3. 保存 をクリックして、レジストリ内の接続の詳細を更新します。
4. 接続リストをレジストリ インポート ファイルまたはレジストリ エクスポート ファイルにエクスポートするには、*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セットを使用している場合に便利です。

トラブルシューティング

開始する前に

この手順でレジストリ値を作成する際は、右側ペインを使用してください。

診断のために、Antivirus Connectorログの有効と無効を切り替えることができます。デフォルトでは、このログは無効になっています。高いパフォーマンスが必要な場合は、普段はAntivirus Connectorログを無効化しておき、重大イベントの発生時にのみ有効化することを推奨します。

手順

1. *スタート*を選択し、検索ボックスに「regedit」と入力して、プログラムの一覧から `regedit.exe`を選択します。
2. レジストリ エディター で、ONTAP Antivirus Connectorの次のサブキーを見つけます。
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. 次の表に示す型、名前、値を指定してレジストリ値を作成します。

タイプ	Name	値
文字列	Tracepath	c:\avshim.log

   このレジストリ値には、任意の有効なパスを指定できます。

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

タイプ	Name	重大なログ記録	中間ロギング	詳細ログ
DWORD	Tracelevel	1	2または3	4

   これにより、手順3でTracepath値に指定したパスに保存されているAntivirus Connectorログが有効化されます。

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ログを無効化します。
6. 「MULTI_SZ」タイプの別のレジストリ値を「LogRotation」（引用符なし）という名前で作成します。「LogRotation」には、ローテーションサイズ（1は1MBを表す）のエントリとして「logFileSize：1」を指定し、次の行にはローテーション制限（5が制限値）のエントリとして「logFileCount：5」を指定します。

> これらの値は省略可能です。値を指定しない場合、ローテーション サイズとローテーション制限には、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。整数値に小数値および分数値を指定することはできません。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. ユーザ設定のログ ローテーションを無効化する場合は、手順6で作成したレジストリ値を削除します。

カスタム バナー

カスタム バナーを使用すると、[*Configure ONTAP LIF API*] ウィンドウに法的拘束力のある声明とシステム アクセスの免責事項を配置できます。

手順

1. インストール ディレクトリ内の `banner.txt`ファイルの内容を更新し、変更を保存することで、デフォルトのバナーを変更します。バナーに変更が反映されていることを確認するには、Configure ONTAP LIF APIウィンドウを再度開く必要があります。

Extended Ordinance（**EO**）モードの有効化

安全な処理のために、Extended Ordinance（EO）モードの有効と無効を切り替えることができます。

手順

1. *スタート*を選択し、検索ボックスに「regedit」と入力して、プログラムの一覧から `regedit.exe`を選択します。
2. レジストリ エディター で、ONTAP Antivirus Connector の次のサブキーを見つけます：
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. 右側のペインで、「DWORD」型のレジストリ値を新しく作成し、名前を「EO_Mode」（「」は不要）として、EOモードを有効にする場合は値を「1」（「」は不要）に、EOモードを無効にする場合は値を「0」（「」は不要）に設定します。

   > デフォルトでは、 `EO_Mode`レジストリエントリが存在しない場合、EO モードは無効になります。EO モードを有効にする場合は、外部 syslog サーバー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

開始する前に

この手順でレジストリ値を作成する際は、右側ペインを使用してください。

手順

1. *スタート*を選択し、検索ボックスに「regedit」と入力して、プログラムの一覧から `regedit.exe`を選択します。
2. レジストリ エディター で、syslog 構成用の ONTAP Antivirus Connector 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. 次の表に示す型、名前、値を指定してレジストリ値を作成します。

タイプ	Name	Value
DWORD	syslog_enabled	1または0

「1」の値はsyslogを有効にし、「0」の値は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。

タイプ	Name
REG_SZ	Syslog_host

[値]フィールドには、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。

タイプ	Name
REG_SZ	Syslog_port

[値]フィールドには、syslogサーバが稼働し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。

タイプ	Name
REG_SZ	Syslog_protocol

[値]フィールドには、syslogサーバで使用しているプロトコル（「tcp」または「udp」）を入力します。

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。

タイプ	Name	LOG_CRIT	LOG_NOTICE	LOG_INFO	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。

タイプ	Name	Value
DWORD	syslog_tls	1または0

値が「1」の場合、Transport Layer Security（TLS）を使用した syslog が有効になり、値が「0」の場合、TLS を使用した syslog が無効になることに注意してください。

* キーが存在しない場合、または値が「null」の場合：
    * プロトコルはデフォルトの「tcp」に設定されます。
    * ポートはデフォルトの「514」（プレーン「TCP / UDP」の場合）または「6514」（TLSの場合）に設定されます。
    * syslogレベルはデフォルトの5（LOG_NOTICE）に設定されます。
* syslogが有効になっていることを確認するには、 `syslog_enabled`値が「1」であることを確認します。 `syslog_enabled`値が「1」の場合、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るはずです。
* EO モードが「1」に設定されていて、 `syslog_enabled` 値を「1」から「0」に変更すると、次のようになります：
    * EOモードでsyslogが無効になると、サービスを開始できなくなります。
    * システムの実行状態が安定している場合、警告が表示され、EOモードではsyslogを無効にできないのでsyslogが強制的に「1」に設定されたと通知されます（この結果はレジストリで確認できます）。この場合は、まずEOモードを無効にしてから、syslogを無効化する必要があります。
* EOモードとsyslogが有効な状態でsyslogサーバを正常に実行できない場合、サービスが停止します。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ない。
    * UDPとTCP以外の無効なプロトコルが設定されている。
    * ポート番号が無効である。
* TCP設定またはTCP経由のTLS設定の場合、サーバでIPポートがリスンされていないと、接続に失敗しサービスが終了します。

X.509相互証明書認証の設定

管理パス内でのAntivirus ConnectorとONTAP間のSecure Sockets Layer（SSL）通信には、X.509証明書ベースの相互認証を使用できます。EOモードが有効な状態で証明書が見つからない場合、AV Connectorは強制終了します。Antivirus Connectorで次の手順を実行します。

手順

1. Antivirus Connectorは、Antivirus Connectorがインストール ディレクトリを実行するディレクトリ パス内で、Antivirus Connectorクライアント証明書およびNetAppサーバの認証局（CA）証明書を検索します。この固定ディレクトリ パスにこれらの証明書をコピーします。
2. PKCS12形式ファイルにクライアント証明書と秘密鍵を埋め込み、「AV_client.P12」と名付けます。
3. NetAppサーバの証明書に署名するために使用した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」という名前になっていることを確認してください。この証明書をAntivirus Connectorのインストールディレクトリに配置してください。ONTAPシステムでは、「ONTAP」のAntivirus Connectorのクライアント証明書に署名するために使用したCA証明書（およびルートCAまでの中間署名機関）を「client-ca」タイプの証明書としてインストールしてください。

スキャナ プールの設定

ONTAP Vscanスキャナ プールの設定について学ぶ

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定義します。

> 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**ONTAP Vscan**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。

開始する前に

- SVMとVscanサーバは同じドメインに属しているか、相互に信頼されたドメインに属している必要があります。
- クラスタ管理LIFを使用してONTAPウイルス対策コネクタを設定します。
- 特権ユーザーのリストには、Vscan サーバーが SVM に接続するために使用するドメインとユーザー名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 cluster_admin_SVM -scanner-pool
   scanner_pool -hostnames Vscan_server_hostnames -privileged-users
   privileged_users
   ```

   - クラスタ管理 SVM を指定します。
   - 各 Vscan サーバホスト名に IP アドレスまたは FQDN を指定します。
   - 各特権ユーザーのドメインとユーザー名を指定します。

   ```
   `vserver vscan scanner-pool create`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-vscan-scanner-pool-create.html["ONTAPコマンド リファレンス
   "^]をご覧ください。
   ```

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 cluster_admin_SVM -scanner-pool
   scanner_pool
   ```

   次のコマンドは、`SP`スキャナープールの詳細を表示します：

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

                                    Vserver: cluster_admin_SVM
                               Scanner Pool: SP
                             Applied Policy: idle
                             Current Status: off
         Cluster on Which Policy Is Applied: -
                  Scanner Pool Config Owner: cluster
       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
```

```
`vserver vscan scanner-pool
show`コマンドを使用して、クラスター上のすべてのスキャナープールを表示することもできます。link:https://docs.netapp.com/us-en/ontap-cli/vserver-vscan-scanner-pool-show.html["ONTAPコマンド リファレンス"^]の `vserver vscan scanner-pool
show`の詳細を確認してください。
```

MetroCluster構成でONTAP Vscanスキャナプールを作成する

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。

開始する前に

- SVMとVscanサーバは同じドメインに属しているか、相互に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。

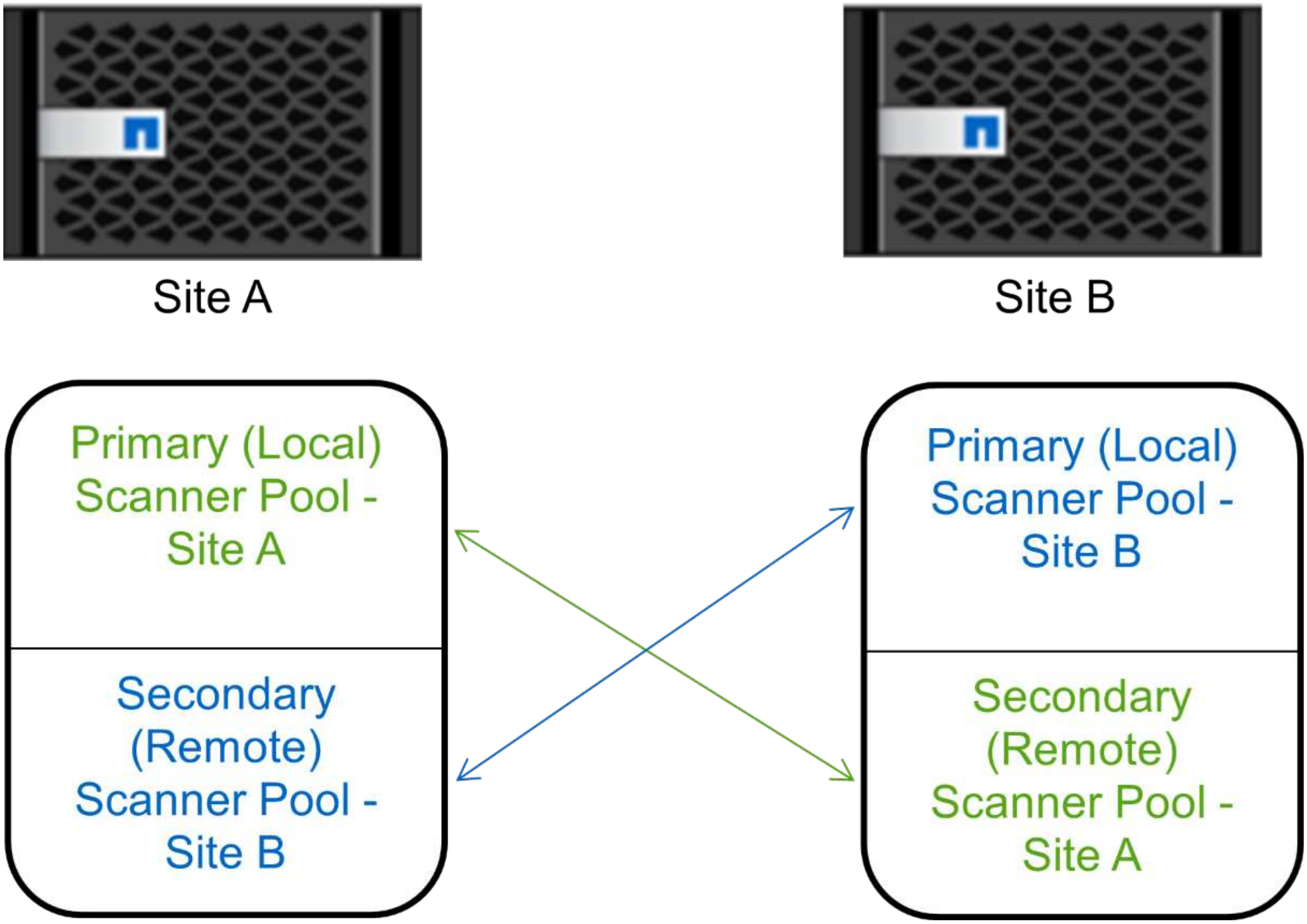
タスク概要

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。

したがって、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

あります。セカンダリSVMが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）については、MetroClusterと同様の構成になります。

この図は、代表的な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 に対して定義されたプールにはデータ SVM を指定し、クラスタ内のすべての SVM に対して定義されたプールにはクラスタ管理 SVM を指定します。
   ◦ 各 Vscan サーバホスト名に IP アドレスまたは FQDN を指定します。
   ◦ 各特権ユーザーのドメインとユーザー名を指定します。

   ⓘ スキャナ プールの作成は、いずれもプライマリSVMを含むクラスタから実行する必要があります。

```
`vserver vscan scanner-pool create`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-vscan-scanner-pool-create.html["ONTAPコマンド リファレンス"^]をご覧ください。
```

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`*

次のコマンドは、スキャナプール `pool1`の詳細を表示します：

```
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
```

```
`vserver vscan scanner-pool show`コマンドを使用して、
SVM上のすべてのスキャナプールを表示することもできます。link:https://docs.netapp.
com/us-en/ontap-cli/vserver-vscan-scanner-pool-show.html["ONTAPコマンド
リファレンス"^]の `vserver vscan scanner-pool show`の詳細を確認してください。
```

ONTAP Vscanを使用して単一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定義します。スキャナ プールによって定義されるVscanサーバがSVMに接続できるようにするには、先にスキャナ プールをアクティブにする必要があります。

タスク概要

- 1つのスキャナ プールには1つのスキャナ ポリシーのみを適用できます。
- 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になるように指定します。
   - `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。

     次の例は、 `vs1` SVM上の `SP`という名前のスキャナプールがアクティブであることを示しています：

   ```
   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なことを確認します。

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

   この手順で説明されているコマンドの詳細については、"ONTAPコマンド リファレンス"を参照してください。

   次のコマンドは、 `SP`スキャナープールの詳細を表示します：

```
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
```

```
`vserver vscan scanner-pool show-active`コマンドを使用して、
SVM上のアクティブなスキャナプールを表示できます。link:https://docs.netapp.com/u
s-en/ontap-cli/vserver-vscan-scanner-pool-show-active.html["ONTAPコマンド
リファレンス"^]の `vserver vscan scanner-pool show-
active`の詳細をご覧ください。
```

MetroCluster ONTAP Vscan構成で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定義します。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。

タスク概要

- 1つのスキャナ プールには1つのスキャナ ポリシーのみを適用できます。
- 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 リカバリ構成および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、`cluster`パラメータにローカルクラスタを指定する必要があります。リモートクラスタ用に作成するポリシーでは、`cluster`パラメータにリモートクラスタを指定する必要があります。これにより、災害発生時にリモートクラスタがウイルススキャン処理を引き継ぐことができます。

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*

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

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になるように指定します。

◦ `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。

> 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 pool2_for_site2 -scanner-policy primary -cluster cluster2

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

2. スキャナ プールがアクティブなことを確認します。

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

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

次のコマンドは、スキャナプール `pool1`の詳細を表示します：

```
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
```

```
`vserver vscan scanner-pool show-active`コマンドを使用して、
SVM上のアクティブなスキャナプールを表示できます。link:https://docs.netapp.com/u
s-en/ontap-cli/vserver-vscan-scanner-pool-show-active.html["ONTAPコマンド
リファレンス"^]の `vserver vscan scanner-pool show-
active`の詳細をご覧ください。
```

Vscan でスキャナ プールを管理するための ONTAP 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 プールを変更する	`vserver vscan scanner-pool modify`
スキャナ プールを削除する	`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する	`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サーバを削除する	`vserver vscan scanner-pool servers remove`
スキャナ プールの概要と詳細を表示する	`vserver vscan scanner-pool show`

スキャナ プールの特権ユーザを表示する	`vserver vscan scanner-pool privileged-users show`
すべてのスキャナ プールのVscanサーバを表示する	`vserver vscan scanner-pool servers show`

この手順で説明されているコマンドの詳細については、"ONTAPコマンド リファレンス"を参照してください。

オンアクセス スキャンの設定

ONTAP Vscan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。

タスク概要

- 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。
- `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 サーバーがない場合でもファイル アクセスを許可するように指定できます。
- デフォルトでは、「default_CIFS」という名前のオンアクセス ポリシーが作成され、クラスタ内のすべてのSVMに対して有効になります。
- `paths-to-exclude`、 `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は、 `scan-mandatory`オプションがオンに設定されている場合でも、スキャン対象として考慮されません。（ `scan-mandatory`オプションに関連する接続の問題については、この"トラブルシューティング"セクションを確認してください。）
- 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共有ではウイルス スキャンは実行されません。
- *Vscan* ファイル操作プロファイル の詳細については、"ウイルス対策アーキテクチャ" セクションを参照してください。
- 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イルス スキャンの対象から除外できます。
- 除外するファイルに関するいくつかの推奨事項：
    - 大容量ファイル（ファイル サイズは指定可能）は、応答に時間がかかったり、CIFSユーザのスキャン要求がタイムアウトになったりする可能性があるため、ウイルス スキャンの対象から除外することを検討します。除外されるファイルのサイズは、デフォルトでは2GBです。

◦ `.vhd`や `.tmp`などのファイル拡張子を持つファイルはスキャンに適さない可能性があるため、これらの拡張子を除外することを検討してください。

◦ 隔離ディレクトリなどのファイル パスや、仮想ハード ドライブやデータベースのみが格納されているパスは、除外することを検討します。

◦ 一度に有効にできるポリシーは1つだけなので、すべての除外が同じポリシーで指定されていることを確認します。NetAppは、除外する対象をウイルス対策エンジンで指定されているものと一致させることを強く推奨しています。

◦ ONTAP 9.14.1 以降では、ワイルドカードを使用して、除外するオンアクセス パスとファイル拡張子を指定できます。

- オンデマンド スキャンにはオンアクセス ポリシーが必要です。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`を*に設定してすべての拡張子を除外する必要があります。

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 に対して定義されたポリシーの場合はデータ SVM を指定し、クラスタ内のすべての SVM に対して定義された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 `-file-ext-to-include`設定を上書きします。

   ◦ `-scan-files-with-no-ext`を `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、 `vs1` SVM 上に `Policy1`という名前のオンアクセスポリシーを作成します：

```
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. on-access 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`*

```
`vserver vscan on-access-policy`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-
vscan-on-access-policy-show.html["ONTAPコマンド リファレンス
"^]をご覧ください。
```

   次のコマンドは、 `Policy1`ポリシーの詳細を表示します：

```
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
```

ONTAP Vscan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 `Policy1`という名前のオンアクセス ポリシーを有効にします：

   ```
   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`*

```
`vserver vscan on-access-policy show`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-vscan-on-access-policy-show.html["ONTAPコマンド リファレンス
"^]をご覧ください。
```

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

```
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ONTAP Vscanファイル操作プロファイルを変更する

SMB共有の_Vscanファイル操作プロファイル_は、共有上でスキャンをトリガーできる操作を定義します。デフォルトでは、パラメータは`standard`に設定されています。SMB共有を作成または変更する際に、必要に応じてパラメータを調整できます。

Vscan ファイル操作プロファイル の詳細については、"ウイルス対策アーキテクチャ" セクションを参照してください。

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

手順

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`

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

次のコマンドは、SMB 共有の Vscan ファイル操作プロファイルを `strict`に変更します：

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

オンアクセス ポリシーを管理するための **ONTAP Vscan** コマンド

オンアクセス ポリシーを変更、無効化、削除できます。また、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 ポリシーの作成	`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 ポリシーの有効化	`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する	`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`

この手順で説明されているコマンドの詳細については、"ONTAPコマンド リファレンス"を参照してください。

オンデマンド スキャンの設定

ONTAP Vscanオンデマンド スキャンの設定について学ぶ

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いつタスクを実行するかを指定できます。

> 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。

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、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。

ONTAP Vscanで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 ウイルス 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もスキャンされます。

タスク概要

- 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 タスクにより、スキャンに関連する統計が記載されたレポートが作成されます。このレポートを確認するには、コマンドを使用するか、定義済みの場所にタスクにより作成されたレポート ファイルをダウンロードします。
- ONTAP 9.14.1以降では、ワイルドカードを使用して、除外するオンデマンドパスとファイル拡張子を指定できます。

開始する前に

- オンアクセスポリシーを作成したが必要です。ポリシーはデフォルトまたはユーザーが作成したものを使用できます。on-access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`設定は `-file-ext-to-include`設定を上書きします。
   - `-scan-files-with-no-ext` を true に設定すると、拡張子のないファイルをスキャンします。

     > `vserver vscan on-demand-task create`
     > の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-vscan-on-demand-task-create.html["ONTAPコマンド リファレンス"^]をご覧ください。

   次のコマンドは、`vs1` SVM に `Task1`という名前のオンデマンド タスクを作成します：

```
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.
```

+

`job show`コマンドを使用してジョブのステータスを表示できます。 `job pause`コマンドと `job resume`コマンドを使用してジョブを一時停止および再開したり、 `job stop`コマンドを使用してジョブを終了したりできます。"ONTAPコマンド リファレンス"の `job`の詳細を確認してください。

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`

```
`vserver vscan on-demand-task show`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-vscan-on-demand-task-show.html["ONTAPコマンド リファレンス"^]をご覧ください。
```

次のコマンドは、 `Task1`タスクの詳細を表示します：

```
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: -
```

終了後の操作

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。

ONTAP Vscanでオンデマンドタスクをスケジュールする

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ことも、タスクの作成中にスケジュールを追加することもできます。

タスク概要

> `vserver vscan on-demand-task schedule`コマンドで割り当てられたスケジュールは、`vserver vscan on-demand-task create`コマンド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。

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、 `vs2` SVM で `Task2` 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：

```
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.
```

```
`vserver vscan on-demand-task schedule`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-
vscan-on-demand-task-schedule.html["ONTAPコマンド リファレンス
"^]をご覧ください。
```

ジョブのステータスを表示するには、 `job show`コマンドを使用します。 `job pause`コマンドと `job resume`コマンドはそれぞれジョブを一時停止および再開します。 `job stop`コマンドはジョブを終了します。"ONTAPコマンド リファレンス"の `job`の詳細をご覧ください。

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*

   ```
   `vserver vscan on-demand-task show`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-
   vscan-on-demand-task-show.html["ONTAPコマンド リファレンス"^]をご覧ください。
   ```

   次のコマンドは `Task 2`タスクの詳細を表示します：

```
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
```

終了後の操作

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。

ONTAP Vscanオンデマンドタスクをすぐに実行

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。

開始する前に

SVM でスキャンを有効にする必要があります。

手順

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、 `vs1` SVM 上で `Task1`という名前のオンアクセス タスクを実行します：

```
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.
```

```
`vserver vscan on-demand-task run`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-vscan-on-demand-task-run.html["ONTAPコマンド リファレンス"^]をご覧ください。
```

`job show`コマンドを使用してジョブのステータスを表示できます。 `job pause`コマンドと `job resume`コマンドを使用してジョブを一時停止および再開したり、 `job stop`コマンドを使用してジョブを終了したりできます。"ONTAPコマンド リファレンス"の `job`の詳細を確認してください。

オンデマンド タスクを管理するための **ONTAP Vscan** コマンド

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。また、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 タスクの作成	`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 タスクの実行	`vserver vscan on-demand-task run`
オンデマンド タスクのスケジュールの設定	`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する	`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 レポートを表示する	`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`

この手順で説明されているコマンドの詳細については、"ONTAPコマンド リファレンス"を参照してください。

ONTAP Vscanのオフボックスウイルス対策機能を設定するためのベストプラクティス

ONTAPで外部の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。

- ウイルス スキャン処理を特権ユーザに限定します。一般ユーザが、特権ユーザのクレデンシャルを使用できないようにします。これは、Active Directoryで特権ユーザのログイン権限をオフにすることで実現できます。
- 特権ユーザは、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 グループの一員である必要はありません。ただし、Vscanサーバ接続を作成したり、ウイルス スキャンのためにファイルにアクセスしたりできるように、ストレージ システムのみによって検証される必要があります。
- Vscanサーバが実行されているコンピュータは、ウイルス スキャンの目的でのみ使用します。一般的な用途で使用されるのを防ぐため、これらのマシンではWindows Terminal Servicesやその他のリモート アクセス プロビジョニングを無効にしておき、マシンに新しいソフトウェアをインストールするための権限は管理者のみに付与します。
- Vscanサーバはウイルス 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ようにします。Vscanサーバは、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に割り当てられたリソースが共有されておらず、ウイルス 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。
- リソースの過剰割り当てを回避するために、Vscanサーバには十分なCPU、メモリ、ディスク容量を提供します。ほとんどのVscanサーバは、マルチ コアCPUのサーバを使用して、CPU全体に負荷を分散する設計になっています。
- NetAppは、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 トラフィックから影響を受けないようにするため、プライベートVLANによる専用のネットワークを使用することを推奨しています。Vscanサーバ上のウイルス対策VLANとSVM上のデータLIFに、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。こうしておくと、ネットワークで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しやすくなります。プライベート ネットワークを使用して、ウイルス対策トラフィックを分離するようにします。ウイルス対策サーバを、次のいずれかの方法でドメイン コントローラ（DC）やONTAPと通信するように構成します。
  - DCとウイルス対策サーバが、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通信する。
  - DCとウイルス対策サーバが、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もの）を介して通信する。
  - ウイルス対策通信でKerberos認証を有効にする場合は、プライベートLIF用のDNSエントリと、プライベートLIF用に作成されたDNSエントリに対応するDC上のサービス プリンシパル名を作成する。このサービス プリンシパル名は、ウイルス対策コネクタにLIFを追加するときに使用します。DNSは、ウイルス対策コネクタに接続されている各プライベートLIFの一意の名前を返せるものである必要があります。

> 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と、ポート障害が発生した場合に、Vscan LIFがもう一方のノードにフェイルオーバーされる可能性があります。この変更によってVscanサーバが新規ノードから到達不能になり、ノードでのファイル処理に関するスキャン通知が失敗します。Vscanサーバがノード上の1つ以上のLIFを通じて到達可能であり、そのノードで実行されたファイル処理に関するスキャン要求を処理できるか確認してください。

* NetAppのストレージ システムとVscanサーバの接続には、1GbE以上のネットワークを使用します。
* 複数のVscanサーバがある環境では、接続パフォーマンスが高い同等のネットワークですべてのサーバを接続します。Vscanサーバを接続すると、負荷共有が可能になるのでパフォーマンスが向上します。
* NetAppは、リモート サイトやブランチ オフィスでは、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ています。これは、高レイテンシの環境にはローカルのVscanサーバが最適であるためです。コストを重視する場合は、ノートPCやデスクトップ コンピュータを使用して適度なウイルス対策を講じます。ボリュームやqtreeを共有してファイルシステム全体の定期スキャンのスケジュールを設定すると、それらをリモート サイトのシステムでスキャンできます。
* 負荷分散と冗長性を確保するため、複数のVscanサーバを使用してSVM上のデータをスキャンします。CIFSのワークロード量とそれに伴うウイルス対策トラフィック量はSVMごとに異なります。ストレージコントローラ上のCIFSおよびウイルススキャンのレイテンシを監視します。結果の傾向を経時的に監視します。VscanサーバのCPUまたはアプリケーションキューが原因でCIFSのレイテンシとウイルススキャンのレイテンシが傾向のしきい値を超えて増加すると、CIFSクライアントの待機時間が長くなる可能性があります。負荷を分散するために、Vscanサーバを追加してください。
* 最新バージョンのONTAP Antivirus Connectorをインストールします。
* ウイルス対策のエンジンと定義を常に最新の状態に保ちます。推奨される更新頻度については、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、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。ただし、VscanサーバとSVMが同じドメインか、信頼できるドメインに属していることが条件になります。
* 感染したファイルに関するウイルス対策ソフトウェア ポリシーは、大半のウイルス対策ベンダーが設定しているデフォルト値である「delete」または「quarantine」に設定します。「vscan-fileop-profile」が「write_only」に設定されていると、感染したファイルが検出された場合も、ファイルは共有に残り、開くことができます。これは、ファイルを開いただけではスキャンはトリガーされないためです。ウイルス対策スキャンは、ファイルを閉じるまでトリガーされません。
* `scan-engine timeout`値は `scanner-pool request-timeout`値よりも小さくする必要があります。値を大きくすると、ファイルへのアクセスが遅延し、最終的には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`を `scanner-pool request-timeout`値より5秒小さく設定してください。 `scan-engine timeout`設定の変更方法については、スキャンエンジンベンダーのドキュメントを参照してください。 `scanner-pool timeout`は、詳細モードで次のコマンドを使用し、 `request-timeout`パラメータに適切な値を指定することで変更できます：`vserver vscan scanner-pool modify
* NetAppは、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 スキャンを使用する必要がある環境では、既存のウイルス対策インフラに余計な負荷がかからないように、オンデマンド スキャンの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"をご覧ください。

SVM ONTAP Vscanでウイルススキャンを有効にする

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ためには、SVMでウイルス スキャンを有効にする必要があります。

手順

1. SVMでウイルス スキャンを有効にします。

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

```
`vserver vscan enable`の詳細については、link:https://docs.netapp.com/us-
en/ontap-cli/vserver-vscan-enable.html["ONTAPコマンド リファレンス
"^]をご覧ください。
```

> 必要に応じて、`vserver vscan disable`コマンドを使用してウイルススキャンを無効にすることができます。"ONTAPコマンド リファレンス"の `vserver vscan disable`の詳細をご覧ください。

次のコマンドは vs1 SVM でのウイルススキャンを有効にします：

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

2. SVMでウイルス 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`

```
`vserver vscan show`の詳細については、link:https://docs.netapp.com/us-
en/ontap-cli/vserver-vscan-show.html["ONTAPコマンド リファレンス
"^]をご覧ください。
```

次のコマンドは、 vs1 SVM の Vscan ステータスを表示します：

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

                          Vserver: vs1
                     Vscan Status: on
```

ONTAP Vscanでスキャンしたファイルのステータスをリセットする

SVM上で正常にスキャンされたファイルのスキャンステータスをリセットする必要がある場合があります。 `vserver vscan reset`コマンドを使用してファイルのキャッシュ情報を破棄します。例えば、スキャンの設定ミスがあった場合などに、このコマンドを使用してウイルススキャン処理を再開することができます。 `vserver vscan reset`の詳細については、"ONTAPコマンド リファレンス"をご覧ください。

タスク概要

```
`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は次回アクセス時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。

開始する前に

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`

   ```
   `set -privilege advanced`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/set.html["ONTAPコマンド リファレンス"^]をご覧ください。
   ```

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、 `vs1` SVM 上のスキャンされたファイルのステータスをリセットします：

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

ONTAPでVscanイベントログ情報を表示

```
`vserver vscan show-events`コマンドを使用すると、感染ファイル、
Vscanサーバの更新などに関するイベントログ情報を表示できます。クラスタ全体、または特定の
ノード、SVM、Vscanサーバのイベント情報を表示できます。
```

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`

```
`set`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/set.html["ONTAPコマンド リファレンス"^]をご覧ください。
```

2. Vscanイベント ログ情報を表示します。

   `vserver vscan show-events`

   ```
   `vserver vscan show-events`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-vscan-show-events.html["ONTAPコマンド リファレンス"^]をご覧ください。
   ```

   次のコマンドは、クラスターのイベント 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 オプションに関連する潜在的な **ONTAP Vscan** 接続の問題

```
`vserver vscan connection-status
show`コマンドを使用すると、接続の問題のトラブルシューティングに役立つ可能性のあるVscanサーバー接続に関する情報を表示できます。
```

デフォルトでは、 `scan-mandatory`オンアクセススキャンのオプションは、スキャンにVscanサーバー接続が利用できない場合、ファイルへのアクセスを拒否します。このオプションは重要な安全機能を提供しますが、いくつかの状況では問題を引き起こす可能性があります。

- クライアントアクセスを有効にする前に、LIFを持つ各ノードのSVMに少なくとも1台の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後にサーバをSVMに接続する必要がある場合は、Vscanサーバ接続が利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、SVMで `scan-mandatory`オプションをオフにする必要があります。サーバが接続されたら、このオプ

ションをオンに戻すことができます。

• ターゲットLIFがSVMのすべてのVscanサーバ接続をホストしている場合、LIFを移行するとサーバとSVM間の接続が失われます。Vscanサーバ接続が利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、LIFを移行する前に `scan-mandatory`オプションをオフにする必要があります。LIFの移行後、このオプションをオンに戻すことができます。

各SVMには少なくとも2台のVscanサーバを割り当てる必要があります。Vscanサーバをストレージシステムに接続する場合は、クライアントアクセスに使用するネットワークとは別のネットワークを使用するのがベストプラクティスです。

```
`vserver vscan connection-status show`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-vscan-connection-status-show.html["ONTAPコマンド リファレンス"^]をご覧ください。
```

Vscan サーバの接続ステータスを表示するための ONTAP コマンド

```
`vserver vscan connection-status show`コマンドを使用して、Vscan
サーバ接続ステータスに関する概要情報と詳細情報を表示できます。
```

状況	入力するコマンド
Vscanサーバ接続の概要を表示する	`vserver vscan connection-status show`
Vscanサーバ接続の詳細を表示する	`vserver vscan connection-status show-all`
接続されているVscanサーバの詳細を表示する	`vserver vscan connection-status show-connected`
未接続の使用可能なVscanサーバの詳細を表示する	`vserver vscan connection-status show-not-connected`

```
`vserver vscan connection-status show`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+vscan+connection-status+show["ONTAPコマンド
リファレンス"^]を参照してください。
```

ONTAPのVscanスキャンによるウイルスのトラブルシューティング

ウイルス スキャンに関する一般的な問題については、考えられる原因と解決方法があります。ウイルス スキャンはVscanとも呼ばれます。

問題	解決方法

Vscan サーバーは、クラスタ化された ONTAP ストレージ システムに接続できません。	scanner-pool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てください。また、scanner-poolリストで許可された特権ユーザーがアクティブになっているかどうかも確認してください。scanner-poolを確認するには、ストレージシステムのコマンドプロンプトで `vserver vscan scanner-pool show`コマンドを実行してください。それでもVscanサーバに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。
クライアントのレイテンシが高くなっている。	スキャナ プールにVscanサーバを追加すると解決する可能性があります。
トリガーされたスキャンの数が多すぎる。	`vscan-fileop-profile`パラメータの値を変更して、ウイルススキャンで監視され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ない。	オンアクセスポリシーを確認してください。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、ストレージシステムのコマンドプロンプトで `vserver vscan on-access-policy show`コマンドを実行してください。
ファイル アクセスが拒否される。	ポリシー設定で_scan-mandatory_設定が指定されているかどうかを確認してください。この設定は、Vscanサーバが接続されていない場合にデータアクセスを拒否します。必要に応じて設定を変更してください。

関連情報

- "vserver vscan scanner-pool show"
- "vserver vscan on-access-policy show"

ONTAP Vscanのステータスとパフォーマンスアクティビティを監視する

Vscanモジュールの重要な側面、例えばVscanサーバーの接続状態、Vscanサーバーの健全性、スキャンされたファイル数などを監視できます。これらの情報は、Vscanサーバーに関連する問題の診断に役立ちます。

Vscanサーバの接続情報の表示

Vscanサーバーの接続ステータスを表示して、すでに使用中の接続と使用可能な接続を管理できます。Vscanサーバーの接続ステータスに関する情報は、さまざまなコマンドで表示できます。

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`	使用可能だが未接続の接続のステータス
`vserver vscan connection-status show-connected`	接続されているVscanサーバに関する情報

```
`vserver vscan connection-status show`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-vscan-connection-status-show.html["ONTAPコマンド リファレンス"^]をご覧ください。
```

Vscanサーバに関する統計の表示

Vscanサーバ固有の統計情報を表示することで、パフォーマンスを監視し、ウイルススキャンに関連する問題を診断できます。 `statistics show`コマンドを使用してVscanサーバの統計情報を表示する前に、データサンプルを収集する必要があります。

```
`statistics show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/statistics-show.html["ONTAPコマンド リファレンス"^]をご覧ください。
```

データのサンプリングを完了するには、次の手順を実行します。

手順

1. `statistics start`コマンドとオプションの `statistics stop`コマンドを実行します。

   ```
   `statistics start`および `statistics stop`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=statistics["ONTAPコマンド リファレンス"^]をご覧ください。
   ```

Vscanサーバ要求とレイテンシに関する統計の表示

ONTAP `offbox_vscan`カウンタをSVMごとに使用することで、1秒あたりにディスパッチおよび受信されるVscanサーバ要求のレートと、すべてのVscanサーバにおけるサーバレイテンシを監視できます。これらの統計情報を表示するには、次の手順を実行します（：）

手順

1. `statistics show -object offbox_vscan –instance SVM`コマンドを次のカウンターで実行します：

カウンタ...	表示される情報...
`scan_request_dispatched_rate`	ONTAPからVscanサーバに送信されたウイルス スキャン要求の1秒あたりの数
`scan_noti_received_rate`	ONTAPがVscanサーバから受信したウイルス スキャン要求の1秒あたりの数
`dispatch_latency`	使用可能なVscanサーバを特定し、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`	スキャンの実行時間を含む、ONTAPからVscanサーバへのラウンドトリップ レイテンシ

ONTAP offbox_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に関する統計の表示

ONTAP `offbox_vscan_server`カウンタをSVMごと、オフボックスVscanサーバごと、ノードごとに使用することで、ディスパッチされたVscanサーバ要求のレートと各Vscanサーバのサーバレイテンシを個別に監視できます。この情報を収集するには、次の手順を実行します：

手順

1. `statistics show –object offbox_vscan –instance SVM:servername:nodename`コマンドを次のカウンターで実行します：

カウンタ...	表示される情報...
`scan_request_dispatched_rate`	ONTAPから送信されたウイルス スキャン要求の数

scan_latency	ONTAPからVscanサーバへの往復遅延（Vscanサーバへのスキャン実行時間を含む、1秒あたり）

ONTAP offbox_vscan_serverカウンタから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サーバの利用率に関する統計の表示

ONTAP `offbox_vscan_server`カウンタを使用して、Vscanサーバ側の使用率統計を収集することもできます。これらの統計は、SVMごと、オフボックスVscanサーバごと、およびノードごとに追跡されます。統計には、VscanサーバのCPU使用率、Vscanサーバでのスキャン操作のキュー深度（現在値と最大値の両方）、使用メモリ、使用ネットワークが含まれます。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。これらの統計は20秒ごとにポーリングされるデータに基づいており、正確性を保つには複数回収集する必要があります。そうでない場合、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使用率とキューは、監視および分析において特に重要です。平均キューの値が高い場合、Vscanサーバにボトルネックが発生している可能性があります。SVMごと、オフボックスVscanサーバごと、およびノードごとにVscanサーバの使用率統計を収集するには、次の手順を実行します：

手順

1. Vscanサーバの利用率に関する統計を収集します。

```
 `statistics show -object offbox_vscan_server -instance
SVM:servername:nodename`コマンドを次の
`offbox_vscan_server`カウンターで実行します：
```

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サーバのスキャン要求の平均キュー

scanner_stats_pct_input_queue_hiwatermark	Vscanサーバのスキャン要求のピーク キュー
scanner_stats_pct_mem_used	Vscanサーバの使用済みメモリ
scanner_stats_pct_network_used	Vscanサーバの使用済みネットワーク

Vscanサーバの利用率に関する統計の例

```
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
-------------------------------- --------------------------------
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
-----------------------------------------------------------------
```

関連情報

- "ONTAPコマンド リファレンス"