Vscanサーバのインストールと設定

ONTAP 9

NetApp
February 12, 2026

目次

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。

設定した外部**syslog**サーバの動作の確認

- 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。

著作権に関する情報

商標に関する情報