Vscanサーバのインストールと設定

ONTAP 9

NetApp
December 20, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/ontap/antivirus/vscan-server-install-config-concept.html on December 20, 2024. Always check docs.netapp.com for the latest.

目次

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、の手順に従います"[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、"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サポートサイトの*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。"NetApp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サーバごとに異なるバージョンのWindowsサーバをインストールできます。

- 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。

タスクの内容

- "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、最高のパフォーマンスを得るために、NetAppではアンチウイルス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、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。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。
    - SVMの管理LIFまたはIPアドレスがで有効になっていることを確認します `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、REST APIへの（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`。
    - リンクの詳細については、ONTAPコマンドリファレンスを参照してください。https://docs NetAppONTAP .com /us-ja/cli/ security-login-role-create.htmlおよびlink：https://docs NetApp .com /us-

ja/cli/ security-login-create.html[`security login create`コマンドについては、「ONTAP[`security login role create`コマンドリファレンス」を参照してください。

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。リンクhttps://docs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。NetApp .com /us-en/ ONTAP -CLI/ security-login-domain-tunnel-create.html[`security login domain-tunnel create`^]コマンドを参照してください。

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
Data LIF	a. 「role」を「data」に設定 b. 「data protocol」を「cifs」に設定 c. 「firewall policy」を「data」に設定する d. 「service policy」を「default-data-files」に設定
管理LIF	a. 「role *」を「data」に設定 b. 「data protocol」を「none」に設定します。 c. 「firewall policy」を「mgmt」に設定 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. [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。

設定オプションについては、を参照してください"ONTAP Antivirus Connectorページの設定"。

ONTAP Antivirus Connectorの設定

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アプリケーション用のユーザアカウントを作成し、REST APIへの（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`。

リンクの詳細については、『ONTAPコマンドリファレンス』を参照してください。https://docs NetApp .com /us-en/ ONTAP -cli/security-login-role-create.html#description^][`security login role create`および`link：https://docs NetApp .com /us-en/ ONTAP -cli/ security-login-create.html[`security login create^]コマンドを参照してください。

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。リンクhttps://docs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。NetApp .com /us-en/ ONTAP -CLI/ security-login-domain-tunnel-create.html[`security login domain-tunnel create^]コマンドを参照してください。

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

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、[プログラム]リストでを選択します `regedit.exe`。
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。

タイプ	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。

タイプ	名前	重要なロギング	中間ロギング	詳細なロギング
DWORD	Tracelevel	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（1は1MB）のエントリとして「logFileSize:1」を指定し、次の行でローテーションの制限（5は制限）のエントリとして「logFileCount:5」を指定します。

> 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、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. インストールディレクトリのファイルの内容を更新して変更を保存することで、デフォルトバナーを変更し `banner.txt`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、[プログラム]リストでを選択します `regedit.exe`。
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、レジストリエントリが存在しない場合、 `EO_Mode`EOモードは無効になっています。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

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、[プログラム]リストでを選択します `regedit.exe`。

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。

タイプ	名前	値
DWORD	syslog_enabled	1または0

値「1」を指定するとsyslogが有効になり、値「0」を指定するとsyslogが無効になります。

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	名前
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	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。

タイプ	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。

タイプ	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。

タイプ	名前	値
DWORD	syslog_tls	1または0

値が「1」の場合はTransport Layer Security（TLS）でsyslogが有効になり、値が「0」の場合はTLSでsyslogが無効になります。

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、値が「1」であることを確認し `syslog_enabled`ます。値が「1」の場合は `syslog_enabled`、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、値を「1」から「0」に変更すると、 `syslog_enabled`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、ONTAP拡張メール（PEM）形式で「PEM_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。

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。