# Vscan 服务器安装和配置

ONTAP 9

NetApp
April 24, 2024

# 目录

# Vscan 服务器安装和配置

## Vscan 服务器安装和配置

设置一个或多个Vscan服务器、以确保系统上的文件已进行病毒扫描。按照供应商提供的说明在服务器上安装和配置防病毒软件。

按照NetApp提供的自述文件中的说明安装和配置ONTAP防病毒连接器。或者、按照上的说明进行操作 "安装ONTAP防病毒连接器页面"。

> 对于灾难恢复和MetroCluster配置、您必须为主/本地和二级/配对ONTAP集群设置和配置单独的Vscan服务器。

### 防病毒软件要求

- 有关防病毒软件要求的信息，请参见供应商文档。
- 有关 Vscan 支持的供应商，软件和版本的信息，请参见 "Vscan合作伙伴解决方案" 页面。

### ONTAP 防病毒连接器要求

- 您可以从NetApp 支持站点 上的*软件下载*页面下载ONTAP防病毒连接器。 "NetApp 下载：软件"
- 有关ONTAP防病毒连接器支持的Windows版本和互操作性要求的信息、请参阅 "Vscan合作伙伴解决方案"。

  > 您可以为集群中的不同 Vscan 服务器安装不同版本的 Windows 服务器。

- Windows 服务器上必须安装 .NET 3.0 或更高版本。
- 必须在 Windows 服务器上启用 SMB 2.0 。

## 安装ONTAP防病毒连接器

在Vscan服务器上安装ONTAP防病毒连接器、以启用运行ONTAP的系统与Vscan服务器之间的通信。安装ONTAP防病毒连接器后、防病毒软件可以与一个或多个Storage Virtual Machine (SVM)进行通信。

关于此任务

- 请参见 "Vscan合作伙伴解决方案" 页面、了解有关支持的协议、防病毒供应商软件版本、ONTAP版本、互操作性要求和Windows服务器的信息。
- 必须安装.NET 4.5.1或更高版本。
- ONTAP防病毒连接器可以在虚拟机上运行。但是、为了获得最佳性能、NetApp建议使用专用虚拟机进行防病毒扫描。
- 必须在要安装和运行ONTAP防病毒连接器的Windows服务器上启用SMB 2.0。

开始之前

- 从支持站点下载ONTAP防病毒连接器安装文件、并将其保存到硬盘驱动器上的目录中。
- 确认您满足安装ONTAP防病毒连接器的要求。
- 验证您是否具有安装防病毒连接器的管理员权限。

步骤

1. 运行相应的安装文件以启动防病毒连接器安装向导。
2. 选择_Next_。此时将打开目标文件夹对话框。
3. 选择_Next_将防病毒连接器安装到列出的文件夹中，或选择_Change_to install to a next folder。
4. 此时将打开ONTAP AV Connector Windows服务凭据对话框。
5. 输入您的Windows服务凭据或选择*Add*以选择用户。对于ONTAP系统、此用户必须是有效的域用户、并且必须位于SVM的扫描程序池配置中。
6. 选择 * 下一步 * 。此时将打开准备安装程序对话框。
7. 选择*Install*开始安装，或者如果要对设置进行任何更改，选择*Back*。 此时将打开一个状态框，并显示安装进度，然后显示InstallShield向导已完成对话框。
8. 如果要继续配置ONTAP管理或数据、请选中配置ONTAP LUN复选框。 要使用此Vscan服务器、必须至少配置一个ONTAP管理或数据LIF。
9. 如果要查看安装日志，请选中显示*Windows Installer log*复选框。
10. 选择*完成*以结束安装并关闭InstallShield向导。 配置ONTAP Lifs*图标保存在桌面上以配置ONTAP Lifs。
11. 将SVM添加到防病毒连接器。 您可以通过添加ONTAP管理LIF (轮询以检索数据LIF列表)或直接配置一个或多个数据LIF来将SVM添加到防病毒连接器。 如果配置了ONTAP管理LIF、则还必须提供轮询信息和ONTAP管理员帐户凭据。
    - 验证是否已为启用管理LIF或SVM的IP地址 `management-https`。仅在配置数据生命周期时、不需要执行此操作。
    - 验证是否已为HTTP应用程序创建用户帐户、并分配了对具有(至少是只读)访问权限的角色 `/api/network/ip/interfaces` REST API。 有关创建用户的详细信息、请参见 "创建安全登录角色" 和 "创建安全登录" ONTAP手册页。

> 您还可以通过为管理SVM添加身份验证通道SVM来使用域用户作为帐户。有关详细信息，请参见 "安全登录域通道创建" ONTAP手册页或使用 `/api/security/acccounts` 和 `/api/security/roles` 用于配置管理员帐户和角色的REST API。

步骤

1. 右键单击完成防病毒连接器安装时保存在桌面上的*配置ONTAP Lifs*图标，然后选择*以管理员身份运行*。
2. 在配置ONTAP LUN对话框中、选择首选配置类型、然后执行以下操作：

| 要创建此类型的LIF… | 执行以下步骤 … |
| --- | --- |
| 数据 LIF | a. 将"Role"设置为"data"<br>b. 将"data protocol (数据协议)"设置为"CIFS (CIFS)"<br>c. 将"Firewall policy"设置为"data"<br>d. 将"service policy"设置为"default-data-files" |

| | |
|---|---|
| 管理LIF | a. 将"Role*设置为"data"<br>b. 将"data protocol (数据协议)"设置为"none (无)"<br>c. 将"Firewall policy"设置为"mgmt"<br>d. 将"service policy"设置为"default-management " |

了解更多信息 "正在创建LIF"。

创建LIF后、输入要添加的SVM的数据或管理LIF或IP地址。您也可以输入集群管理LIF。如果指定集群管理LIF、则该集群中提供SMB的所有SVM都可以使用Vscan服务器。

> 如果Vscan服务器需要Kerberos身份验证、则每个SVM数据LIF都必须具有唯一的DNS名称、并且您必须将该名称注册为Windows Active Directory中的服务器主体名称(SPN)。如果没有为每个数据LIF提供唯一的DNS名称或将其注册为SPN、则Vscan服务器将使用NT LAN Manager机制进行身份验证。如果在连接Vscan服务器后添加或修改DNS名称和SPN、则必须在Vscan服务器上重新启动防病毒连接器服务以应用更改。

3. 要配置管理LIF、请输入轮询持续时间(以秒为单位)。轮询持续时间是指防病毒连接器检查SVM或集群LIF配置是否发生更改的频率。默认轮询间隔为60秒。
4. 输入ONTAP管理员帐户名称和密码以配置管理LIF。
5. 单击*Test*以检查连接并验证身份验证。仅验证管理LIF配置的身份验证。
6. 单击*更新*将LIF添加到要轮询或连接到的LIF列表中。
7. 单击*保存*以保存与注册表的连接。
8. 如果要将连接列表导出到注册表导入或注册表导出文件，请单击*Export*。如果多个Vscan服务器使用一组相同的管理或数据生命周期、则此功能非常有用。

请参见 "配置ONTAP防病毒连接器页面" 了解配置选项。

# 配置ONTAP防病毒连接器

通过输入ONTAP管理LIF、轮询信息和ONTAP管理员帐户凭据或仅输入数据LIF、配置ONTAP防病毒连接器以指定要连接到的一个或多个Storage Virtual Machine (SVM)。您还可以修改SVM连接的详细信息或删除SVM连接。默认情况下、如果配置了ONTAP管理LIF、ONTAP防病毒连接器将使用REST API检索数据LIF列表。

## 修改SVM连接的详细信息

您可以通过修改ONTAP管理LIF和轮询信息来更新已添加到防病毒连接器的Storage Virtual Machine (SVM)连接的详细信息。添加数据LUN后、您将无法对其进行更新。要更新数据LIF、您必须先将其删除、然后使用新的LIF或IP地址重新添加。

开始之前

验证是否已为HTTP应用程序创建用户帐户、并分配了对具有(至少是只读)访问权限的角色 `/api/network/ip/interfaces` REST API。 有关创建用户的详细信息、请参见 "创建安全登录角色" 和 "创建安全登录" 命令 您还可以通过为管理SVM添加身份验证通道SVM来使用域用户作为帐户。 有关详细信息，请

参见 "安全登录域通道创建" ONTAP手册页。

步骤

1. 右键单击完成防病毒连接器安装时保存在桌面上的*配置ONTAP Lifs*图标，然后选择*以管理员身份运行*。此时将打开配置ONTAP LUN对话框。
2. 选择SVM IP地址，然后单击*Update*。
3. 根据需要更新此信息。
4. 单击*保存*以更新注册表中的连接详细信息。
5. 如果要将连接列表导出到注册表导入或注册表导出文件，请单击*Export*。 如果多个Vscan服务器使用一组相同的管理或数据生命周期、则此功能非常有用。

## 从防病毒连接器中删除SVM连接

如果您不再需要SVM连接、可以将其删除。

步骤

1. 右键单击完成防病毒连接器安装时保存在桌面上的*配置ONTAP Lifs*图标，然后选择*以管理员身份运行*。此时将打开配置ONTAP LUN对话框。
2. 选择一个或多个SVM IP地址，然后单击*Remove*。
3. 单击*保存*以更新注册表中的连接详细信息。
4. 如果要将连接列表导出到注册表导入或注册表导出文件，请单击*Export*。 如果多个Vscan服务器使用一组相同的管理或数据生命周期、则此功能非常有用。

## 故障排除

开始之前

在此操作步骤中创建注册表值时、请使用右侧窗格。

您可以启用或禁用防病毒连接器日志以进行诊断。默认情况下、这些日志处于禁用状态。为了提高性能、您应禁用防病毒连接器日志、并仅在发生严重事件时启用这些日志。

步骤

1. 选择*Start*，在搜索框中键入“regedit”，然后选择 `regedit.exe` 在程序列表中。
2. 在*Registry Editor*中，找到ONTAP防病毒连接器的以下项：
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. 通过提供下表所示的类型、名称和值来创建注册表值：

   | Type | Name | 值 |
   | --- | --- | --- |
   | string | 迹线 | C：\avshim.log |

   此注册表值可以是任何其他有效路径。

4. 通过提供下表所示的类型、名称、值和日志记录信息、创建另一个注册表值：

| Type | Name | 关键日志记录 | 中间日志记录 | 详细日志记录 |
| --- | --- | --- | --- | --- |
| DWORD | Tracellevel | 1. | 2或3 | 4. |

这将启用按照步骤3中的TracePath提供的路径值保存的防病毒连接器日志。

5. 通过删除在步骤3和4中创建的注册表值来禁用防病毒连接器日志。
6. 创建另一个类型为"multi_SZ"且名称为"LogRotation"(不带引号)的注册表值。在"LogRotation"中、 提供"logFileSize：1"作为轮换大小的条目(其中1表示1MB)、并在下一行中提供"logFileCount：5"作为 旋转限值条目(5为限值)。

> 这些值是可选的。如果未提供、则会分别使用默认值20 MB和10个文件作为轮换大小和轮换限制。提供的整数值不提供小数值或小数值。如果提供的值高于默认值、则会改用默认值。

7. 要禁用用户配置的日志轮换、请删除您在步骤6中创建的注册表值。

## 可自定义的横幅

自定义横幅允许您在_Configure ONTAP LIF API_窗口中放置具有法律约束力的声明和系统访问免责声明。

步骤

1. 通过更新中的内容来修改默认横幅 `banner.txt` 文件、然后保存所做的更改。 要查看横幅中反映的更改、必须重新打开配置ONTAP LIF API窗口。

## 启用扩展条例模式

您可以启用和禁用扩展法令(EO)模式以确保安全操作。

步骤

1. 选择*Start*，在搜索框中键入“regedit”，然后选择 `regedit.exe` 在程序列表中。
2. 在*Registry Editor*中，找到ONTAP防病毒连接器的以下项：
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. 在右侧窗格中、创建名为"EO_Mode"(不带引号)且值为"1"(不带引号)的新注册表值"DWORD"、以启用"EO模式"或值"0"(不带引号)禁用"EO模式"。

> 默认情况下、如果是 `EO_Mode` 缺少注册表条目、已禁用EO模式。启用EO模式后、必须同时配置外部系统日志服务器和相互证书身份验证。

## 配置外部系统日志服务器

开始之前

请注意、在此操作步骤中创建注册表值时、请使用右侧窗格。

步骤

1. 选择*Start*，在搜索框中键入“regedit”，然后选择 `regedit.exe` 在程序列表中。

2. 在*Registry Editor*中，为系统日志配置的ONTAP防病毒连接器创建以下项：
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
3. 通过提供类型、名称和值来创建注册表值、如下表所示：

| Type | Name | 价值 |
|---|---|---|
| DWORD | syslog_enabled | 1或0 |

请注意、使用"1"值启用系统日志、使用"0"值禁用系统日志。

4. 通过提供下表所示的信息创建另一个注册表值：

| Type | Name |
|---|---|
| REG_SZ | syslog_host |

为值字段提供系统日志主机IP地址或域名。

5. 通过提供下表所示的信息创建另一个注册表值：

| Type | Name |
|---|---|
| REG_SZ | syslog_port |

在Value字段中提供运行系统日志服务器的端口号。

6. 通过提供下表所示的信息创建另一个注册表值：

| Type | Name |
|---|---|
| REG_SZ | syslog_protocol |

在值字段中输入系统日志服务器上使用的协议、即"TCP"或"UDP"。

7. 通过提供下表所示的信息创建另一个注册表值：

| Type | Name | Log_Rert | log_notice | LOG_INFO | log_ddebug |
|---|---|---|---|---|---|
| DWORD | syslog_level | 2. | 5. | 6. | 7. |

8. 通过提供下表所示的信息创建另一个注册表值：

| Type | Name | 价值 |
|---|---|---|
| DWORD | syslog_tls. | 1或0 |

请注意、"1"值将启用采用传输层安全(Transport Layer Security、TLS)的系统日志、而"0"值将禁用采用TLS的系统日志。

确保已配置的外部系统日志服务器平稳运行

- 如果密钥不存在或具有空值：
  - 协议默认为"TCP"。
  - 对于纯"TCP/UDP"、此端口默认为"514"；对于TLS、此端口默认为"6514"。
  - 系统日志级别默认为5 (log_notice)。
- 您可以通过验证是否已启用系统日志来确认是否已启用 `syslog_enabled` 值为"1"。当 `syslog_enabled` 值为"1"、无论是否启用了EO模式、您都应该能够登录到已配置的远程服务器。
- 如果将EO模式设置为"1"、则更改 `syslog_enabled` 值从"1"到"0"、适用以下条件：
  - 如果未在EO模式下启用系统日志、则无法启动此服务。
  - 如果系统以稳定状态运行、则会显示一条警告、指出无法在EO模式下禁用系统日志、并且系统日志会强制设置为"1"、您可以在注册表中看到此信息。如果发生这种情况、您应先禁用EO模式、然后再禁用系统日志。
- 如果在启用了EO模式和系统日志后、系统日志服务器无法成功运行、则该服务将停止运行。出现此问题的原因可能如下：
  - 配置的syslog_host无效或未配置。
  - 配置的协议无效、而不是UDP或TCP。
  - 端口号无效。
- 对于TCP或基于TCP的TLS配置、如果服务器未侦听IP端口、则连接将失败、服务将关闭。

## 配置X.509相互证书身份验证

对于管理路径中防病毒连接器和ONTAP之间的安全套接字层(SSL)通信、可以使用基于X.509证书的相互身份验证。如果启用了EO模式、但未找到证书、AV Connector将终止。在防病毒连接器上执行以下操作步骤：

步骤

1. 防病毒连接器在其运行安装目录的目录路径中搜索NetApp服务器的防病毒连接器客户端证书和证书颁发机构(CA)证书。将证书复制到此固定目录路径中。
2. 以PKCS12格式嵌入客户端证书及其私钥、并将其命名为"AV_client.p12"。
3. 确保用于对NetApp服务器的证书签名的CA证书(以及任何中间签名颁发机构、直到根CA)采用隐私增强邮件(PEM)格式且名为"ONTAP CA。pEM"。将其放在防病毒连接器安装目录中。在NetApp ONTAP系统上、安装用于将ONTAP中的防病毒连接器客户端证书作为"client-ca"类型证书进行签名的CA证书(以及直到根CA的任何中间签名颁发机构)。