



防范病毒 ONTAP 9

NetApp
April 24, 2024

目录

- 防范病毒 1
 - 防病毒配置概述 1
 - 关于 NetApp 防病毒保护 1
 - Vscan 服务器安装和配置 6
 - 配置扫描程序池 13
 - 配置实时扫描 21
 - 配置按需扫描 25
 - 在ONTAP中配置机下防病毒功能的最佳实践 30
 - 在 SVM 上启用病毒扫描 32
 - 重置已扫描文件的状态 32
 - 查看 Vscan 事件日志信息 33
 - 监控连接问题并对其进行故障排除 34

防范病毒

防病毒配置概述

Vscan是NetApp开发的防病毒扫描解决方案、支持客户保护其数据免受病毒或其他恶意代码的危害。

当客户端通过SMB访问文件时、Vscan会执行病毒扫描。您可以将Vscan配置为按需或按计划进行扫描。您可以使用ONTAP命令行界面(CLI)或ONTAP应用程序编程接口(API)与Vscan进行交互。

相关信息

["Vscan合作伙伴解决方案"](#)

关于 NetApp 防病毒保护

关于 NetApp 病毒扫描

Vscan是NetApp开发的防病毒扫描解决方案、支持客户保护其数据免受病毒或其他恶意代码的危害。它将合作伙伴提供的防病毒软件与ONTAP功能相结合、为客户提供管理文件扫描所需的灵活性。

病毒扫描的工作原理

存储系统将扫描操作卸载到托管第三方供应商提供的防病毒软件的外部服务器。

根据活动扫描模式、当客户端按计划或立即(按需)通过SMB (实时)访问文件或访问特定位置的文件时、ONTAP会发送扫描请求。

- 当客户端通过 SMB 打开，读取，重命名或关闭文件时，您可以使用 `_on-access scanning` 来检查病毒。文件操作将暂停、直到外部服务器报告文件的扫描状态为止。如果文件已扫描，则 ONTAP 允许执行文件操作。否则，它将从服务器请求扫描。

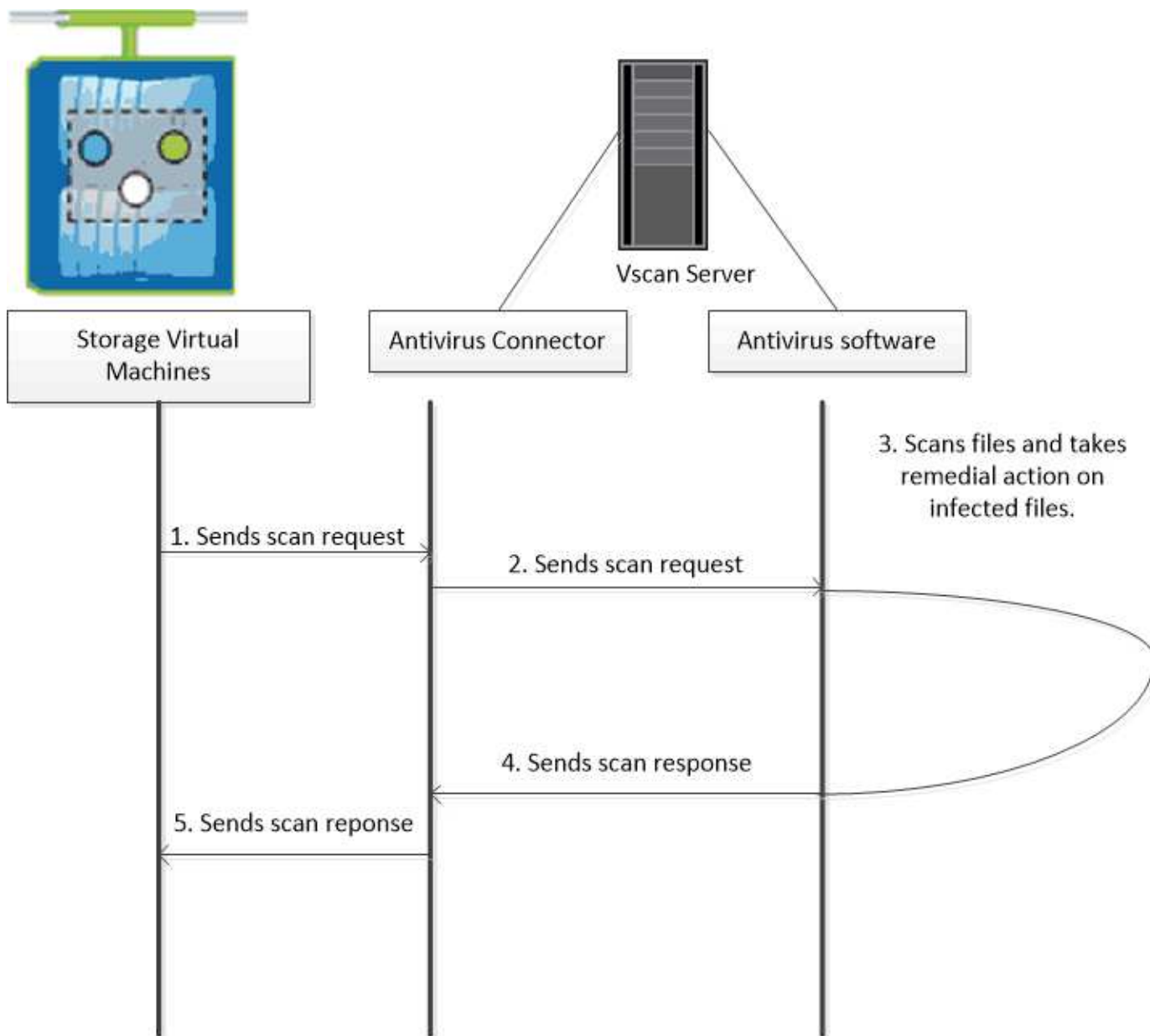
NFS 不支持实时扫描。

- 您可以使用 `_on-Demand scanning` 立即或按计划检查文件中的病毒。我们建议按需扫描只在非高峰时段运行、以避免现有AV基础架构过载、而现有AV基础架构的规模通常适合实时扫描。外部服务器会更新已检查文件的扫描状态、以便通过SMB减少文件访问延迟。如果进行了文件修改或软件版本更新、则会从外部服务器请求新的文件扫描。

您可以对 SVM 命名空间中的任何路径使用按需扫描，即使是仅通过 NFS 导出的卷也是如此。

通常、您会在SVM上同时启用实时和按需扫描模式。在任一模式下、防病毒软件都会根据您的软件设置对受感染的文件采取补救措施。

ONTAP 防病毒连接器由 NetApp 提供并安装在外部服务器上，用于处理存储系统与防病毒软件之间的通信。

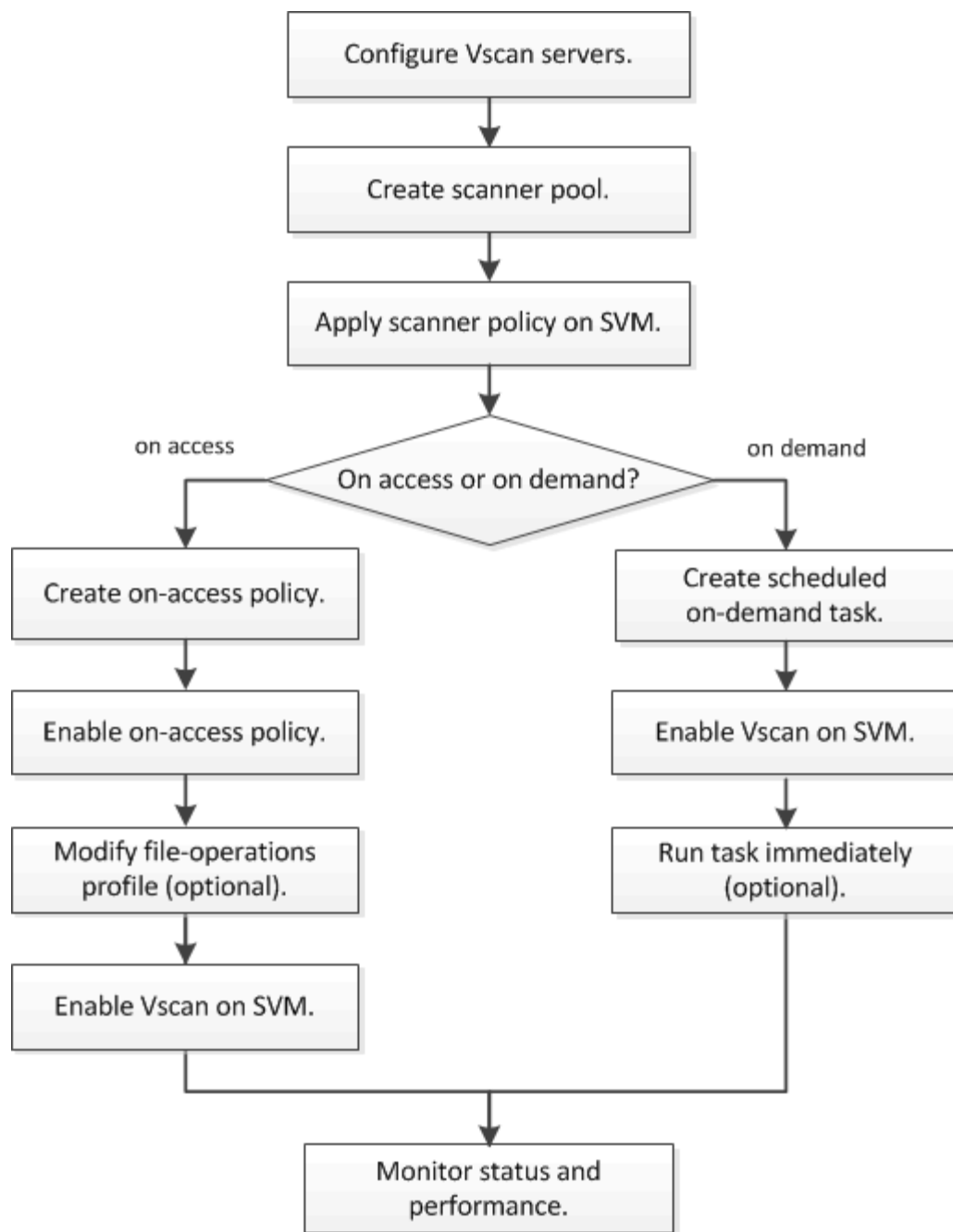


病毒扫描 workflow

您必须先创建扫描程序池并应用扫描程序策略，然后才能启用扫描。通常、您会在SVM上同时启用实时和按需扫描模式。



您必须已完成 CIFS 配置。



后续步骤

- [在单个集群上创建扫描程序池](#)
- [在单个集群上应用扫描程序策略](#)
- [创建实时策略](#)

防病毒架构

NetApp防病毒架构由Vscan服务器软件和相关设置组成。

Vscan服务器软件

您必须在Vscan服务器上安装此软件。

- * ONTAP 防病毒连接器 *

这是NetApp提供的软件、用于处理SVM与防病毒软件之间的扫描请求和响应通信。它可以在虚拟机上运行、但为了获得最佳性能、请使用物理机。您可以从NetApp 支持站点 下载此软件(需要登录)。

- * 防病毒软件 *

这是合作伙伴提供的软件、用于扫描文件中的病毒或其他恶意代码。您可以指定在配置软件时对受感染文件采取的补救措施。

Vscan软件设置

您必须在Vscan服务器上配置这些软件设置。

- * 扫描程序池 *

此设置用于定义可连接到SVM的Vscan服务器和有权限的用户。它还定义了扫描请求超时期限，之后，如果有备用 Vscan 服务器，则会将扫描请求发送到该服务器。



您应将Vscan服务器上防病毒软件的超时期限设置为比扫描程序池扫描请求超时期限少五秒。这样可以避免因软件超时期限大于扫描请求超时期限而导致文件访问延迟或被完全拒绝的情况。

- * 特权用户 *

此设置是Vscan服务器用于连接到SVM的域用户帐户。该帐户必须位于扫描程序池中的有权限用户列表中。

- * 扫描程序策略 *

此设置确定扫描程序池是否处于活动状态。扫描程序策略是系统定义的、因此您无法创建自定义扫描程序策略。只有以下三种策略可用：

- Primary 指定扫描程序池处于活动状态。
- Secondary 指定扫描程序池仅在主扫描程序池中无Vscan服务器连接时处于活动状态。
- Idle 指定扫描程序池处于非活动状态。

- * 实时策略 *

此设置定义实时扫描的范围。您可以指定要扫描的最大文件大小、要包括在扫描中的文件扩展名和路径以及要从扫描中排除的文件扩展名和路径。

默认情况下，仅扫描读写卷。您可以指定允许扫描只读卷或将扫描限制为使用执行访问打开的文件的筛选器：

- scan-ro-volume 启用只读卷扫描。
- scan-execute-access 限制对通过执行访问打开的文件的扫描。



“执行访问”不同于“执行权限。” 仅当可执行文件是使用“execute intent”打开时、给定客户端才会对该文件具有“execute access”。

您可以设置 `scan-mandatory` 选项设置为off、用于指定在没有可用于病毒扫描的Vscan服务器时允许文件访问。在实时模式下、您可以从以下两个互斥选项中进行选择：

- 必填：使用此选项、Vscan会尝试向服务器传送扫描请求、直到超时期限到期为止。如果服务器未接受扫描请求、则客户端访问请求将被拒绝。
- Non-Mandatory:使用此选项时，无论Vscan服务器是否可用于病毒扫描，Vscan始终允许客户端访问。

• * 按需任务 *

此设置定义按需扫描的范围。您可以指定要扫描的最大文件大小、要包括在扫描中的文件扩展名和路径以及要从扫描中排除的文件扩展名和路径。默认情况下会扫描子目录中的文件。

您可以使用 `cron` 计划指定任务运行的时间。您可以使用 `vserver vscan on-demand-task run` 命令以立即运行任务。

• * Vscan 文件操作配置文件（仅限实时扫描） *

◦ `vscan-fileop-profile` 的参数 `vserver cifs share create` 命令用于定义触发病毒扫描的SMB文件操作。默认情况下、参数设置为 `standard`，这是NetApp最佳实践。在创建或修改SMB共享时、您可以根据需要调整此参数：

- `no-scan` 指定从不为共享触发病毒扫描。
- `standard` 指定病毒扫描由打开、关闭和重命名操作触发。
- `strict` 指定病毒扫描由打开、读取、关闭和重命名操作触发。
- `strict` 如果多个客户端同时访问一个文件、则配置文件可增强安全性。如果一个客户端在向某个文件写入病毒后将其关闭、而同一文件在另一个客户端上保持打开状态、`strict` 确保在关闭文件之前、对第二个客户端执行读取操作会触发扫描。

您应小心限制 `strict` 配置文件到包含您预计将同时访问的文件的共享。由于此配置文件生成的扫描请求较多、因此可能会影响性能。

- `writes-only` 指定仅在关闭修改后的文件时才触发病毒扫描。

自此 `writes-only` 生成的扫描请求更少、通常可提高性能。

如果使用此配置文件、则必须将扫描程序配置为删除或隔离不可修复的受感染文件、以便无法访问这些文件。例如、如果客户端在向某个文件写入病毒后关闭该文件、并且该文件未被修复、删除或被隔离、则访问该文件的任何客户端都是如此 `without` 写入数据将受到感染。



如果客户端应用程序执行重命名操作，则文件将使用新名称关闭，不会进行扫描。如果此类操作在您的环境中造成安全问题、则应使用 `standard` 或 `strict` 配置文件。

Vscan合作伙伴解决方案

NetApp与Trellix、Symantec、Trend Micro和Sentinel One合作、提供基于ONTAP Vscan技术构建的行业领先的反恶意软件和防病毒解决方案。这些解决方案可帮助您扫描文件中的恶意软件并修复任何受影响的文件。

如下表所示、NetApp互操作性表维护了Trellix、Symantec和Trend Micro的互操作性详细信息。有关Trellix和Symantec的互操作性详细信息、请参见合作伙伴网站。Sentinel One和其他新合作伙伴的互操作性详细信息将由合作伙伴在其网站上维护。

合作伙伴	解决方案文档	互操作性详细信息
Trellix (前身为McAfee)	"Trellix产品文档"	<ul style="list-style-type: none">• "NetApp 互操作性表工具"• "支持的端点安全存储保护平台(trellix.com)"
Symantec	"Symantec Protection Engine 9.0.0"	<ul style="list-style-type: none">• "NetApp 互操作性表工具"• "合作伙伴设备支持表—已通过网络连接存储(NAS) 9.x.x.x.x.x.x.z的Symantec保护引擎(Protection Engine、身份验证引擎)认证"• "获得网络连接存储(NAS) 8.x版Symantec保护引擎(SPE)认证的合作伙伴设备支持列表(broadcom.com)"
Trend Micro	"《Trend Micro Serverect for Storage 6.0入门指南》"	"NetApp 互操作性表工具"
Sentinel One	<ul style="list-style-type: none">• "SentinelOne Singlity Cloud Data Security"• "SentinelOne支持" <p>此链接需要用户登录。您可以从Sentinel One申请访问权限。</p>	深刻的直觉

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	<ol style="list-style-type: none">a. 将"Role"设置为"data"b. 将"data protocol (数据协议)"设置为"CIFS (CIFS)"c. 将"Firewall policy"设置为"data"d. 将"service policy"设置为"default-data-files"
管理LIF	<ol style="list-style-type: none">a. 将"Role"设置为"data"b. 将"data protocol (数据协议)"设置为"none (无)"c. 将"Firewall policy"设置为"mgmt"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)。

配置扫描程序池

配置扫描程序池概述

扫描程序池用于定义可连接到 SVM 的 Vscan 服务器和有权限的用户。扫描程序策略用于确定扫描程序池是否处于活动状态。



如果在SMB服务器上使用导出策略、则必须将每个Vscan服务器添加到此导出策略中。

在单个集群上创建扫描程序池

扫描程序池用于定义可连接到 SVM 的 Vscan 服务器和有权限的用户。您可以为单个SVM或集群中的所有SVM创建扫描程序池。

您需要的内容

- SVM 和 Vscan 服务器必须位于同一域或受信任域中。
- 对于为单个SVM定义的扫描程序池、您必须已为ONTAP防病毒连接器配置SVM管理LIF或SVM数据LIF。
- 对于为集群中的所有SVM定义的扫描程序池、您必须已使用集群管理LIF配置ONTAP防病毒连接器。
- 有权限的用户列表必须包含 Vscan 服务器用于连接到 SVM 的域用户帐户。
- 配置扫描程序池后、请检查与服务器的连接状态。

步骤

1. 创建扫描程序池：

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

- 为为为单个 SVM 定义的池指定数据 SVM ，并为为为集群中的所有 SVM 定义的池指定集群管理员 SVM 。
- 为每个 Vscan 服务器主机名指定 IP 地址或 FQDN 。
- 为每个有权限的用户指定域和用户名。 有关完整的选项列表，请参见命令手册页。

以下命令将创建名为的扫描程序池 SP 在上 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. 验证是否已创建扫描程序池：

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

有关完整的选项列表，请参见命令手册页。

以下命令将显示的详细信息 SP 扫描程序池：

```
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
```

您也可以使用 `vserver vscan scanner-pool show` 命令以查看SVM上的所有扫描程序池。有关完整的命令语法，请参见命令手册页。

在 MetroCluster 配置中创建扫描程序池

您必须在 MetroCluster 配置中的每个集群上创建主和二级扫描程序池，这些池对应于集群上的主和二级 SVM。

您需要的内容

- SVM 和 Vscan 服务器必须位于同一域或受信任域中。
- 对于为单个SVM定义的扫描程序池、您必须已为ONTAP防病毒连接器配置SVM管理LIF或SVM数据LIF。
- 对于为集群中的所有SVM定义的扫描程序池、您必须已使用集群管理LIF配置ONTAP防病毒连接器。
- 有权限的用户列表必须包含 Vscan 服务器用于连接到 SVM 的域用户帐户。
- 配置扫描程序池后、请检查与服务器的连接状态。

关于此任务

MetroCluster 配置通过实施两个物理上独立的镜像集群来保护数据。每个集群会同步复制另一个集群的数据和 SVM 配置。当集群联机时，本地集群上的主 SVM 将提供数据。当远程集群脱机时，本地集群上的二级 SVM 将提供数据。

这意味着您必须在MetroCluster配置中的每个集群上创建主扫描程序池和二级扫描程序池、当集群开始从二级SVM提供数据时、二级池将变为活动状态。对于灾难恢复(Disaster Recovery、DR)、此配置与MetroCluster类似。

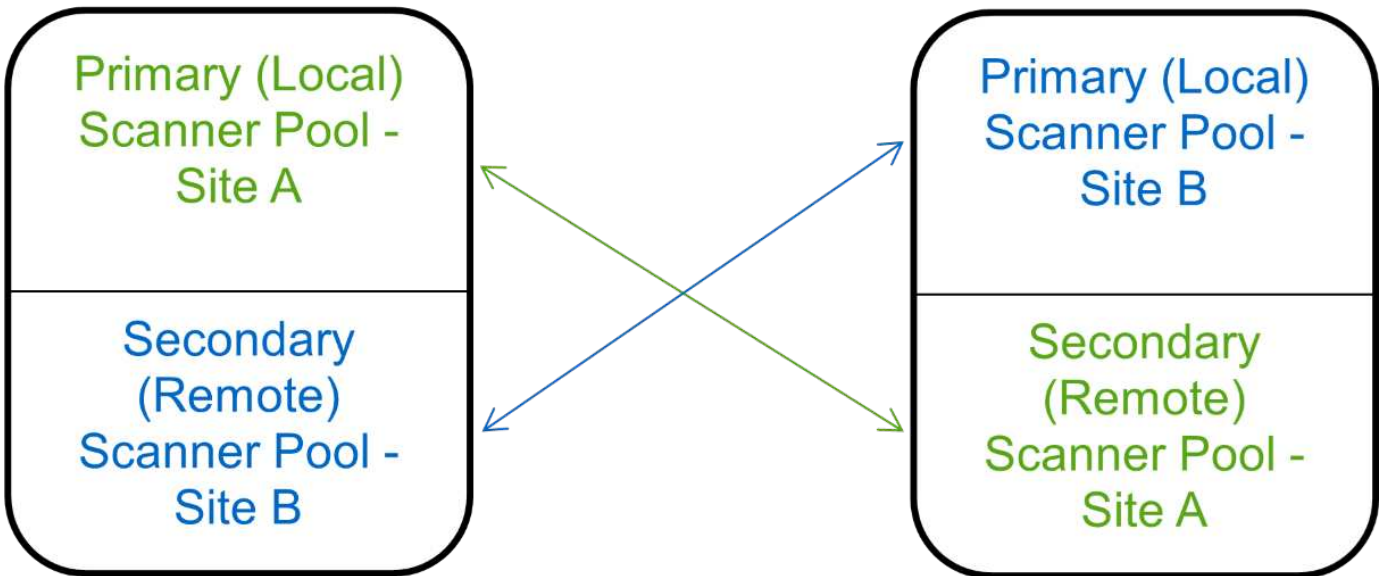
此图显示了典型的MetroCluster/DR配置。



Site A



Site B



步骤

1. 创建扫描程序池：

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

- 为为为单个 SVM 定义的池指定数据 SVM ，并为为为集群中的所有 SVM 定义的池指定集群管理员 SVM 。
- 为每个 Vscan 服务器主机名指定 IP 地址或 FQDN 。
- 为每个有权限的用户指定域和用户名。



您必须从包含主 SVM 的集群创建所有扫描程序池。

有关完整的选项列表，请参见命令手册页。

以下命令会在 MetroCluster 配置中的每个集群上创建主扫描程序池和二级扫描程序池：

```

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. 验证是否已创建扫描程序池:

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

有关完整的选项列表，请参见命令手册页。

以下命令显示扫描程序池的详细信息 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

```

您也可以使用 `vserver vscan scanner-pool show` 命令以查看SVM上的所有扫描程序池。有关完整的命令语法，请参见命令手册页。

在单个集群上应用扫描程序策略

扫描程序策略用于确定扫描程序池是否处于活动状态。您必须先激活扫描程序池、然后它

定义的Vscan服务器才能连接到SVM。

关于此任务

- 一个扫描程序池只能应用一个扫描程序策略。
- 如果为集群中的所有SVM创建了扫描程序池、则必须分别对每个SVM应用扫描程序策略。

步骤

1. 应用扫描程序策略：

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

扫描程序策略可以具有以下值之一：

- Primary 指定扫描程序池处于活动状态。
- Secondary 指定只有在主扫描程序池中沒有Vscan服务器连接时扫描程序池才处于活动状态。
- Idle 指定扫描程序池处于非活动状态。

以下示例显示名为的扫描程序池 SP 在上 vs1 SVM处于活动状态：

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

2. 验证扫描程序池是否处于活动状态：

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

有关完整的选项列表，请参见命令手册页。

以下命令将显示的详细信息 SP 扫描程序池：

```
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
```

您可以使用 `vserver vscan scanner-pool show-active` 命令以查看SVM上的活动扫描程序池。有关完整的命令语法，请参见命令的手册页。

在 MetroCluster 配置中应用扫描程序策略

扫描程序策略用于确定扫描程序池是否处于活动状态。必须将扫描程序策略应用于 MetroCluster 配置中每个集群上的主扫描程序池和二级扫描程序池。

关于此任务

- 一个扫描程序池只能应用一个扫描程序策略。
- 如果为集群中的所有SVM创建了扫描程序池、则必须分别对每个SVM应用扫描程序策略。
- 对于灾难恢复和MetroCluster配置、您必须将扫描程序策略应用于本地集群和远程集群中的每个扫描程序池。
- 在为本地集群创建的策略中、必须在中指定本地集群 `cluster` 参数。在为远程集群创建的策略中、必须在中指定远程集群 `cluster` 参数。然后、远程集群可以在发生灾难时接管病毒扫描操作。

步骤

1. 应用扫描程序策略：

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

扫描程序策略可以具有以下值之一：

- `Primary` 指定扫描程序池处于活动状态。
- `Secondary` 指定只有在主扫描程序池中沒有Vscan服务器连接时扫描程序池才处于活动状态。
- `Idle` 指定扫描程序池处于非活动状态。



您必须应用包含主 SVM 的集群中的所有扫描程序策略。

以下命令会将扫描程序策略应用于 MetroCluster 配置中每个集群上的主扫描程序池和二级扫描程序池：

```
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. 验证扫描程序池是否处于活动状态：

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

有关完整的选项列表，请参见命令手册页。

以下命令显示扫描程序池的详细信息 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
```

您可以使用 `vserver vscan scanner-pool show-active` 命令以查看SVM上的活动扫描程序池。有关完整的命令语法，请参见命令手册页。

用于管理扫描程序池的命令

您可以修改和删除扫描程序池，以及管理扫描程序池的有权限用户和 Vscan 服务器。您还可以查看有关扫描程序池的摘要信息。

如果您 ...	输入以下命令 ...
修改扫描程序池	<code>vserver vscan scanner-pool modify</code>
删除扫描程序池	<code>vserver vscan scanner-pool delete</code>
将有权限的用户添加到扫描程序池	<code>vserver vscan scanner-pool privileged-users add</code>
从扫描程序池中删除有权限的用户	<code>vserver vscan scanner-pool privileged-users remove</code>
将 Vscan 服务器添加到扫描程序池	<code>vserver vscan scanner-pool servers add</code>
从扫描程序池中删除 Vscan 服务器	<code>vserver vscan scanner-pool servers remove</code>
查看扫描程序池的摘要和详细信息	<code>vserver vscan scanner-pool show</code>
查看扫描程序池的有权限用户	<code>vserver vscan scanner-pool privileged-users show</code>
查看所有扫描程序池的 Vscan 服务器	<code>vserver vscan scanner-pool servers show</code>

有关这些命令的详细信息，请参见手册页。

配置实时扫描

创建实时策略

实时策略用于定义实时扫描的范围。您可以为单个 SVM 或集群中的所有 SVM 创建实时策略。如果您为集群中的所有 SVM 创建了实时策略，则必须分别在每个 SVM 上启用该策略。

关于此任务

- 您可以指定要扫描的最大文件大小、要包括在扫描中的文件扩展名和路径以及要从扫描中排除的文件扩展名和路径。
- 您可以设置 `scan-mandatory` 选项设置为off、用于指定在没有可用于病毒扫描的Vscan服务器时允许文件访问。
- 默认情况下、ONTAP会创建一个名为"default_CIFS"的实时策略、并为集群中的所有SVM启用该策略。
- 符合基于的扫描排除条件的任何文件 `paths-to-exclude`, `file-ext-to-exclude` 或 `max-file-size` 扫描时不考虑参数、即使是 `scan-mandatory` 选项设置为on。(选中此项 [故障排除](#) 部分、了解与相关的连接问题 `scan-mandatory` 选项。)
- 默认情况下，仅扫描读写卷。您可以指定允许扫描只读卷或将扫描限制为使用执行访问打开的文件的筛选

器。

- 如果持续可用参数设置为是、则不会对SMB共享执行病毒扫描。
- 请参见 ["防病毒架构"](#) 第节、了解有关_Vscan文件操作配置文件_的详细信息。
- 每个SVM最多可以创建十(10)个实时策略。但是、一次只能启用一个实时策略。
 - 在实时策略中、最多可以从病毒扫描中排除一百(100)个路径和文件扩展名。
- 一些文件排除建议：
 - 请考虑从病毒扫描中排除大型文件(可以指定文件大小)、因为它们可能会导致CIFS用户的响应速度较慢或扫描请求超时。要排除的默认文件大小为2 GB。
 - 请考虑排除文件扩展名、例如 .vhd 和 .tmp 因为具有这些扩展名的文件可能不适合扫描。
 - 请考虑排除一些文件路径、例如隔离目录或仅存储虚拟硬盘驱动器或数据库的路径。
 - 验证是否在同一策略中指定了所有排除项、因为一次只能启用一个策略。NetApp强烈建议使用在防病毒引擎中指定的一组相同排除项。
- 需要使用实时策略 [按需扫描](#)。要避免对进行实时扫描、您应设置 -scan-files-with-no-ext 设置为false、然后 -file-ext-to-exclude 至*以排除所有扩展名。

步骤

1. 创建实时策略：

```
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
```

- 为为为单个 SVM 定义的策略指定数据 SVM ，为为集群中的所有 SVM 定义的策略指定集群管理员 SVM 。
- 。 -file-ext-to-exclude 设置将覆盖 -file-ext-to-include 设置。
- 设置 -scan-files-with-no-ext 设置为true可扫描不带扩展名的文件。以下命令将创建一个名为的实时策略 Policy1 在上 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. 验证是否已创建实时策略：vserver vscan on-access-policy show -instance data_SVM|cluster_admin_SVM -policy-name name

有关完整的选项列表，请参见命令手册页。

以下命令将显示的详细信息 Policy1 策略：


```
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
```

启用实时策略

实时策略用于定义实时扫描的范围。必须先在 SVM 上启用实时策略，然后才能扫描其文件。

如果您为集群中的所有 SVM 创建了实时策略，则必须分别在每个 SVM 上启用该策略。一次只能在 SVM 上启用一个实时策略。

步骤

1. 启用实时策略：

```
vserver vscan on-access-policy enable -vserver data_SVM -policy-name
policy_name
```

以下命令将启用名为的实时策略 Policy1 在上 vs1 SVM：

```
cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy
-name Policy1
```

2. 验证是否已启用实时策略：

```
vserver vscan on-access-policy show -instance data_SVM -policy-name
policy_name
```

有关完整的选项列表，请参见命令手册页。

以下命令将显示的详细信息 Policy1 实时策略：

```
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
```

修改 SMB 共享的 Vscan 文件操作配置文件

SMB共享的_Vscan文件操作配置文件_用于定义共享上可触发扫描的操作。默认情况下、参数设置为 standard。创建或修改 SMB 共享时，您可以根据需要调整参数。

请参见 ["防病毒架构"](#) 第节、了解有关_Vscan文件操作配置文件_的详细信息。



不会对具有SMB共享执行病毒扫描 continuously-available 参数设置为 Yes。

步骤

1. 修改SMB共享的Vscan文件操作配置文件的值：

```
vserver cifs share modify -vserver data_SVM -share-name share -path share_path
-vscan-fileop-profile no-scan|standard|strict|writes-only
```

有关完整的选项列表，请参见命令手册页。

以下命令将SMB共享的Vscan文件操作配置文件更改为 strict：

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

用于管理实时策略的命令

您可以修改，禁用或删除实时策略。您可以查看策略的摘要和详细信息。

如果您要 ...

输入以下命令 ...

创建实时策略	<code>vserver vscan on-access-policy create</code>
修改实时策略	<code>vserver vscan on-access-policy modify</code>
启用实时策略	<code>vserver vscan on-access-policy enable</code>
禁用实时策略	<code>vserver vscan on-access-policy disable</code>
删除实时策略	<code>vserver vscan on-access-policy delete</code>
查看实时策略的摘要和详细信息	<code>vserver vscan on-access-policy show</code>
添加到要排除的路径列表	<code>vserver vscan on-access-policy paths-to-exclude add</code>
从要排除的路径列表中删除	<code>vserver vscan on-access-policy paths-to-exclude remove</code>
查看要排除的路径列表	<code>vserver vscan on-access-policy paths-to-exclude show</code>
添加到要排除的文件扩展名列表	<code>vserver vscan on-access-policy file-ext-to-exclude add</code>
从要排除的文件扩展名列表中删除	<code>vserver vscan on-access-policy file-ext-to-exclude remove</code>
查看要排除的文件扩展名列表	<code>vserver vscan on-access-policy file-ext-to-exclude show</code>
添加到要包含的文件扩展名列表中	<code>vserver vscan on-access-policy file-ext-to-include add</code>
从要包含的文件扩展名列表中删除	<code>vserver vscan on-access-policy file-ext-to-include remove</code>
查看要包括的文件扩展名列表	<code>vserver vscan on-access-policy file-ext-to-include show</code>

有关这些命令的详细信息，请参见手册页。

配置按需扫描

配置按需扫描概述

您可以使用按需扫描立即或按计划检查文件中的病毒。

例如，您可能希望仅在非高峰时段运行扫描，或者您可能希望扫描从实时扫描中排除的非常大的文件。您可以使用cron计划指定任务运行的时间。

关于本主题

- 您可以在创建任务时分配计划。
- 一次只能在一个 SVM 上计划一个任务。
- 按需扫描不支持扫描符号链接或流文件。



按需扫描不支持扫描符号链接或流文件。



要创建按需任务、必须至少启用一个实时策略。它可以是默认策略、也可以是用户创建的实时策略。

创建按需任务

按需任务定义按需病毒扫描的范围。您可以指定要扫描的文件的最大大小，要包含在扫描中的文件的扩展名和路径，以及要从扫描中排除的文件的扩展名和路径。默认情况下会扫描子目录中的文件。

关于此任务

- 每个SVM最多可以有十(10)个按需任务、但只能有一个处于活动状态。
- 按需任务会创建一个报告、其中包含与扫描相关的统计信息。可通过命令或下载任务在定义的位置创建的报告文件来访问此报告。

开始之前

- 您必须拥有 [已创建实时策略](#)。此策略可以是默认策略、也可以是用户创建的策略。如果没有实时策略、则无法启用扫描。

步骤

1. 创建按需任务：

```
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 设置将覆盖 -file-ext-to-include 设置。

° 设置 -scan-files-with-no-ext 设置为true可扫描不带扩展名的文件。

有关完整的选项列表、请参见 ["命令参考"](#)。

以下命令将创建一个名为的按需任务 Task1 在`VS1`虚拟机上:

```
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.
```

+



您可以使用 `job show` 命令以查看作业状态。您可以使用 `job pause` 和 `job resume` 用于暂停和重新启动作业的命令、或 `job stop` 命令以结束作业。

2. 验证是否已创建按需任务:

```
vserver vscan on-demand-task show -instance data_SVM -task-name task_name
```

有关完整的选项列表, 请参见命令手册页。

以下命令将显示的详细信息 Task1 任务:

```
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: -
```

完成后

在计划运行任务之前, 必须在 SVM 上启用扫描。

计划按需任务

您可以在不分配计划的情况下创建任务、然后使用 `vserver vscan on-demand-task schedule` 命令以分配计划；或者在创建任务时添加计划。

关于此任务

分配给的计划 `vserver vscan on-demand-task schedule` 命令会覆盖已使用分配的计划 `vserver vscan on-demand-task create` 命令：

步骤

1. 计划按需任务：

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

以下命令会计划一个名为的实时任务 Task2 在上 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.
```

要查看作业状态、请使用 `job show` 命令：。 `job pause` 和 `job resume` 命令、分别暂停和重新启动作业； `job stop` 命令将终止作业。

2. 验证是否已计划按需任务：

```
vserver vscan on-demand-task show -instance data_SVM -task-name task_name
```

有关完整的选项列表，请参见命令手册页。

以下命令将显示的详细信息 Task 2 任务：

```
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
```

完成后

在计划运行任务之前，必须在 SVM 上启用扫描。

立即运行按需任务

无论是否分配了计划，您都可以立即运行按需任务。

开始之前

您必须已在 SVM 上启用扫描。

步骤

1. 立即运行按需任务：

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

以下命令将运行名为的实时任务 Task1 在上 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.
```



您可以使用 `job show` 命令以查看作业状态。您可以使用 `job pause` 和 `job resume` 用于暂停和重新启动作业的命令、或 `job stop` 命令以结束作业。

用于管理按需任务的命令

您可以修改，删除或取消计划按需任务。您可以查看任务的摘要和详细信息，并管理任务的报告。

如果您要 ...	输入以下命令 ...
创建按需任务	<code>vserver vscan on-demand-task create</code>
修改按需任务	<code>vserver vscan on-demand-task modify</code>
删除按需任务	<code>vserver vscan on-demand-task delete</code>
运行按需任务	<code>vserver vscan on-demand-task run</code>
计划按需任务	<code>vserver vscan on-demand-task schedule</code>
取消计划按需任务	<code>vserver vscan on-demand-task unschedule</code>
查看按需任务的摘要和详细信息	<code>vserver vscan on-demand-task show</code>
查看按需报告	<code>vserver vscan on-demand-task report show</code>
删除按需报告	<code>vserver vscan on-demand-task report delete</code>

有关这些命令的详细信息，请参见手册页。

在ONTAP中配置机下防病毒功能的最佳实践

在ONTAP中配置机下功能时、请考虑以下建议。

- 限制有权限的用户执行病毒扫描操作。不应鼓励普通用户使用有权限的用户凭据。可以通过关闭Active Directory上有权限的用户的登录权限来实现此限制。
- 有权限的用户不必属于在域中拥有大量权限的任何用户组、例如管理员组或备份操作员组。有权限的用户只能通过存储系统进行验证、以便可以创建Vscan服务器连接并访问文件以进行病毒扫描。
- 运行Vscan服务器的计算机仅用于病毒扫描。为了阻止常规使用、请禁用这些计算机上的Windows终端服务和其他远程访问配置、并仅向管理员授予在这些计算机上安装新软件的权限。
- 将Vscan服务器专用于病毒扫描、不要将其用于备份等其他操作。您可能决定将Vscan服务器作为虚拟机(VM)运行。如果将Vscan服务器作为VM运行、请确保分配给该VM的资源不会共享、并且有足够的资源来执行病毒扫描。
- 为Vscan服务器提供足够的CPU、内存和磁盘容量、以避免资源分配过度。大多数Vscan服务器都设计为使用多个CPU核心服务器、并在CPU之间分布负载。

- NetApp建议使用具有专用VLAN的专用网络从SVM连接到Vscan服务器、以使扫描流量不受其他客户端网络流量的影响。创建一个单独的网络接口卡(Network Interface Card、NIC)、专用于Vscan服务器上的防病毒VLAN和SVM上的数据LIF。此步骤可简化出现网络问题时的管理和故障排除。防病毒流量应使用专用网络进行隔离。应将防病毒服务器配置为通过以下方式之一与域控制器(DC)和ONTAP进行通信：
 - DC应通过用于隔离流量的专用网络与防病毒服务器通信。
 - DC和防病毒服务器应通过不同的网络(而不是前面提到的专用网络)进行通信、这与CIFS客户端网络不同。
 - 要为防病毒通信启用Kerberos身份验证、请为专用LIF创建一个DNS条目、并在DC上创建一个与为专用LIF创建的DNS条目对应的服务主体名称。将LIF添加到防病毒连接器时、请使用此名称。DNS应该能够为连接到防病毒连接器的每个专用LIF返回一个唯一的名称。



如果Vscan流量的LIF配置在与客户端流量的LIF不同的端口上、则在发生端口故障时、Vscan LIF可能会故障转移到其他节点。此更改会使Vscan服务器无法从新节点访问、并且此节点上的文件操作的扫描通知将失败。验证Vscan服务器是否可通过节点上的至少一个LIF访问、以便它可以处理对该节点执行文件操作的扫描请求。

- 至少使用1GbE网络连接NetApp存储系统和Vscan服务器。
- 对于具有多个Vscan服务器的环境、请连接具有类似高性能网络连接的所有服务器。连接Vscan服务器可实现负载共享、从而提高性能。
- 对于远程站点和分支机构、NetApp建议使用本地Vscan服务器、而不是远程Vscan服务器、因为前者是实现高延迟的理想选择。如果考虑到成本因素、请使用笔记本电脑或PC进行中等程度的病毒防护。您可以通过共享卷或qtrees并从远程站点中的任何系统扫描它们来计划定期执行完整文件系统扫描。
- 使用多个Vscan服务器扫描SVM上的数据、以实现负载平衡和冗余。CIFS工作负载的数量以及生成的防病毒流量因SVM而异。监控存储控制器上的CIFS和病毒扫描延迟。监控结果随时间的变化趋势。如果由于Vscan服务器上的CPU或应用程序队列超过趋势阈值而导致CIFS延迟和病毒扫描延迟增加、则CIFS客户端可能会出现长时间等待。添加其他Vscan服务器以分布负载。
- 安装最新版本的ONTAP防病毒连接器。
- 使防病毒引擎和定义保持最新。请咨询合作伙伴、了解有关更新频率的建议。
- 在多租户环境中、可以与多个SVM共享一个扫描程序池(Vscan服务器池)、但前提是Vscan服务器和SVM属于同一个域或受信任域。
- 受感染文件的防病毒软件策略应设置为"delete"或"隔离区"、这是大多数防病毒供应商设置的默认值。如果"vscaand-fileop-profile"设置为"write_only"、并且发现受感染的文件、则该文件将保留在共享中、并且可以打开、因为打开文件不会触发扫描。只有在关闭文件后、才会触发防病毒扫描。
- 。 scan-engine timeout 值应小于 scanner-pool request-timeout 价值。如果设置为较高的值、则访问文件可能会延迟、并且最终可能会超时。要避免这种情况、请配置 scan-engine timeout 比低5秒 scanner-pool request-timeout 价值。有关如何更改的说明、请参阅扫描引擎供应商的文档 scan-engine timeout 设置。。 scanner-pool timeout 可以在高级模式中使用以下命令并为提供适当的值来更改 request-timeout 参数： `vserver vscan scanner-pool modify`。
- 对于为实时扫描工作负载调整规模并需要使用按需扫描的环境、NetApp建议将按需扫描作业计划在非高峰时间进行、以避免现有防病毒基础架构产生额外负载。

要了解有关合作伙伴专用最佳实践的更多信息、请访问 ["Vscan合作伙伴解决方案"](#)。

在 SVM 上启用病毒扫描

必须先在 SVM 上启用病毒扫描，然后才能运行实时或按需扫描。

步骤

1. 在 SVM 上启用病毒扫描：

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



您可以使用 `vserver vscan disable` 命令以禁用病毒扫描(如果需要)。

以下命令将在上启用病毒扫描 vs1 SVM：

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

2. 验证是否已在 SVM 上启用病毒扫描：

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

有关完整的选项列表，请参见命令手册页。

以下命令将显示的Vscan状态 vs1 SVM：

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

```
Vserver: vs1
Vscan Status: on
```

重置已扫描文件的状态

有时、您可能需要使用重置SVM上已成功扫描文件的扫描状态 `vserver vscan reset` 命令以丢弃文件的缓存信息。例如，如果扫描配置不当，您可能需要使用此命令重新启动病毒扫描处理。

关于此任务

运行之后 `vserver vscan reset` 命令时、所有符合条件的文件都会在下次访问时进行扫描。



此命令可能会对性能产生不利影响，具体取决于要重新扫描的文件的数量和大小。

您将需要什么

此任务需要高级权限。

步骤

1. 更改为高级权限级别：

```
set -privilege advanced
```

2. 重置已扫描文件的状态：

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

以下命令将在上重置已扫描文件的状态 vs1 SVM：

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

查看 Vscan 事件日志信息

您可以使用 `vserver vscan show-events` 命令以查看有关受感染文件、Vscan服务器更新等的事件日志信息。您可以查看集群或给定节点，SVM 或 Vscan 服务器的事件信息。

开始之前

要查看Vscan事件日志、需要高级权限。

步骤

1. 更改为高级权限级别：

```
set -privilege advanced
```

2. 查看 Vscan 事件日志信息：

```
vserver vscan show-events
```

有关完整的选项列表，请参见命令手册页。

以下命令显示集群的事件日志信息 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.

监控连接问题并对其进行故障排除

与 **scan-mandatory** 选项相关的潜在连接问题

您可以使用 `vserver vscan connection-status show` 用于查看有关Vscan服务器连接的信息的命令、您可能会发现这些信息有助于对连接问题进行故障排除。

默认情况下、`scan-mandatory` 当Vscan服务器连接不可用于扫描时、实时扫描选项会拒绝文件访问。虽然此选项提供了重要的安全功能，但在某些情况下可能会导致问题。

- 在启用客户端访问之前，您必须确保至少有一个 Vscan 服务器连接到每个具有 LIF 的节点上的 SVM。如果在启用客户端访问后需要将服务器连接到SVM、则必须关闭 `scan-mandatory` 选项、以确保文件访问不会因Vscan服务器连接不可用而被拒绝。连接服务器后，您可以重新打开此选项。
- 如果目标 LIF 托管 SVM 的所有 Vscan 服务器连接，则迁移 LIF 后，服务器与 SVM 之间的连接将丢失。要确保不会因Vscan服务器连接不可用而拒绝文件访问、必须关闭 `scan-mandatory` 选项。迁移 LIF 后，您可以重新启用此选项。

每个 SVM 应至少分配两个 Vscan 服务器。最佳做法是，通过与客户端访问不同的网络将 Vscan 服务器连接到存储系统。

用于查看 **Vscan** 服务器连接状态的命令

您可以使用 `vserver vscan connection-status show` 用于查看有关Vscan服务器连接状态的摘要和详细信息的命令。

如果您要 ...	输入以下命令 ...
查看 Vscan 服务器连接的摘要	<code>vserver vscan connection-status show</code>
查看 Vscan 服务器连接的详细信息	<code>vserver vscan connection-status show-all</code>

如果您要 ...	输入以下命令 ...
查看已连接 Vscan 服务器的详细信息	<code>vserver vscan connection-status show-connected</code>
查看未连接的可用 Vscan 服务器的详细信息	<code>vserver vscan connection-status show-not-connected</code>

有关这些命令的详细信息，请参见 ["ONTAP 手册页"](#)。

对病毒扫描进行故障排除

对于常见的病毒扫描问题、可能的原因和解决方法是存在的。病毒扫描也称为Vscan。

问题描述	如何解决
Vscan服务器无法连接到 集群模式ONTAP存储系统。	检查扫描程序池配置是否指定Vscan服务器IP地址。同时检查扫描程序池列表中允许的有权限用户是否处于活动状态。要检查扫描程序池、请运行 <code>vserver vscan scanner-pool show</code> 命令。如果Vscan服务器仍无法连接、则网络中可能存在问题描述。
客户端存在高延迟。	现在可能是向扫描程序池添加更多Vscan服务器的时候了。
触发的扫描次数过多。	修改的值 <code>vscan-fileop-profile</code> 用于限制因病毒扫描而监控的文件操作数的参数。
未扫描某些文件。	检查实时策略。这些文件的路径可能已添加到路径排除列表中、或者其大小超过为排除项配置的值。要检查实时策略、请运行 <code>vserver vscan on-access-policy show</code> 命令。
文件访问被拒绝。	检查是否在策略配置中指定了 <code>_scan-MANUALIANDI_SETTING</code> 设置。如果未连接Vscan服务器、则此设置将拒绝数据访问。根据需要修改设置。

监控状态和性能活动

您可以监控Vscan模块的关键方面、例如Vscan服务器连接状态、 Vscan服务器的运行状况以及已扫描的文件数。此信息将有所帮助 您可以诊断与Vscan服务器相关的问题。

查看Vscan服务器连接信息

您可以查看Vscan服务器的连接状态、以管理已在使用的连接 以及可供使用的连接。各种命令可显示信息 关于Vscan服务器的连接状态。

命令...	显示的信息...
<code>vserver vscan connection-status show</code>	连接状态摘要
<code>vserver vscan connection-status show-all</code>	有关连接状态的详细信息
<code>vserver vscan connection-status show-not-connected</code>	可用但未连接的连接的状态
<code>vserver vscan connection-status show-connected</code>	有关已连接Vscan服务器的信息

有关这些命令的详细信息，请参见 ["手册页"](#)。

查看Vscan服务器统计信息

您可以查看Vscan服务器专用的统计信息、以监控性能并诊断与相关的问题 病毒扫描。您必须先收集数据样本、然后才能使用 `statistics show` 命令 显示Vscan服务器统计信息。要完成数据样本、请完成以下步骤：

步骤

1. 运行 `statistics start` 命令和 `optional statistics` 停止命令。

查看有关Vscan服务器请求和持续时间的统计信息

您可以使用ONTAP `offbox_vscan` 每个SVM上的计数器、用于监控Vscan速率 每秒分派和接收的服务器请求以及所有Vscan的服务器时间 服务器。要查看这些统计信息、请完成以下步骤：

步骤

1. 运行统计信息`show object offbox_vscan -instance SVM` 命令 以下计数器：

计数器...	显示的信息...
<code>scan_request_dispatched_rate</code>	每秒从ONTAP发送到Vscan服务器的病毒扫描请求数
<code>scan_noti_received_rate</code>	ONTAP每秒从Vscan服务器收到的病毒扫描请求数
<code>dispatch_latency</code>	ONTAP中用于确定可用Vscan服务器并将请求发送到该Vscan服务器的延迟
<code>scan_latency</code>	从ONTAP到Vscan服务器的往返延迟、包括扫描运行时间

从ONTAP机下vscan计数器生成的统计信息示例

```
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
-----
```

查看单个Vscan服务器请求和持续时间的统计信息

您可以使用ONTAP offbox_vscan_server 每个SVM、每个机下Vscan服务器上的计数器、并按节点监控已分派Vscan服务器请求的速率以及上的服务器延迟 每个Vscan服务器单独。要收集此信息、请完成以下步骤：

步骤

- 1. 运行 statistics show -object offbox_vscan -instance SVM:servername:nodename 命令和以下计数器：

计数器...	显示的信息...
scan_request_dispatched_rate	从ONTAP发送的病毒扫描请求数
scan_latency	从ONTAP到Vscan服务器的往返延迟、包括扫描运行时间 每秒Vscan服务器数

ONTAP offbox_vscan_server计数器生成的统计信息示例

```
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
-----
```

查看Vscan服务器利用率的统计信息

您也可以使用ONTAP `offbox_vscan_server` 用于收集Vscan服务器端利用率的计数器 统计信息。这些统计信息会按每个SVM、每个机下Vscan服务器和每个节点进行跟踪。他们 包括Vscan服务器上的CPU利用率、Vscan服务器上扫描操作的队列深度 (当前和最大)、已用内存和已用网络。 这些统计信息由防病毒连接器转发到ONTAP中的统计信息计数器。他们 基于每20秒轮询一次的数据、为确保准确性、必须收集多次； 否则、统计信息中显示的值仅反映上次轮询。CPU利用率和队列为 尤其需要进行监控和分析。平均队列的值较高表示Vscan服务器存在瓶颈。 收集每个SVM上的Vscan服务器、每个机下Vscan服务器和每个节点的利用率统计信息 请完成以下步骤：

步骤

1. 收集Vscan服务器的利用率统计信息

运行 `statistics show -object offbox_vscan_server -instance SVM:servername:nodename` 命令 `offbox_vscan_server` 计数器：

计数器...	显示的信息...
<code>scanner_stats_pct_cpu_used</code>	Vscan服务器上的CPU利用率
<code>scanner_stats_pct_input_queue_avg</code>	Vscan服务器上扫描请求的平均队列
<code>scanner_stats_pct_input_queue_hiwatermark</code>	Vscan服务器上扫描请求的峰值队列
<code>scanner_stats_pct_mem_used</code>	Vscan服务器上使用的内存
<code>scanner_stats_pct_network_used</code>	Vscan服务器上使用的网络

Vscan服务器利用率统计信息示例

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  
-----
```

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。