关于 NetApp 防病毒保护

ONTAP 9

NetApp
April 24, 2024

目录

关于 NetApp 防病毒保护 1
关于 NetApp 病毒扫描 1
病毒扫描工作流 2
防病毒架构 3
Vscan合作伙伴解决方案 5

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。

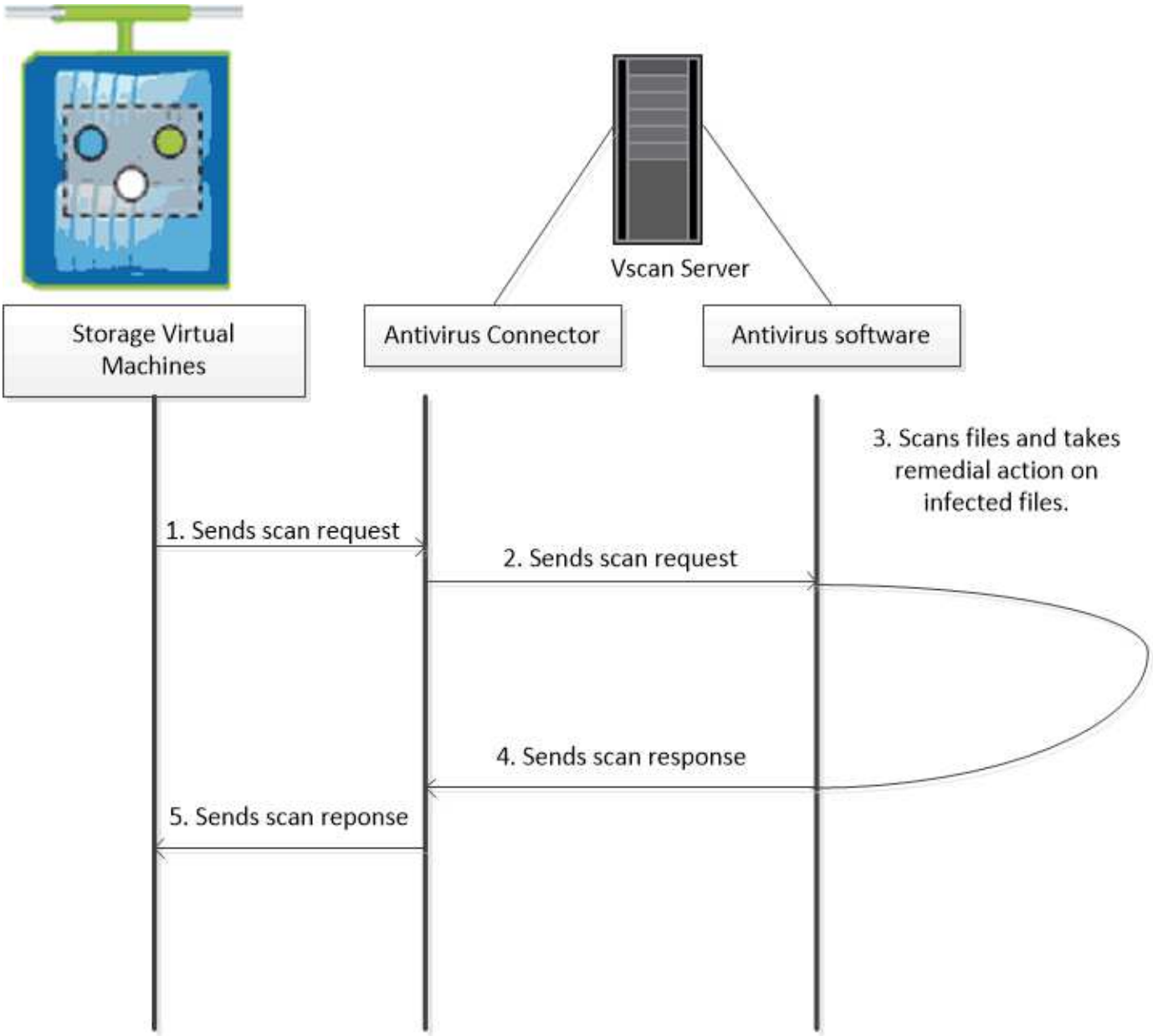
  NFS 不支持实时扫描。

- 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。

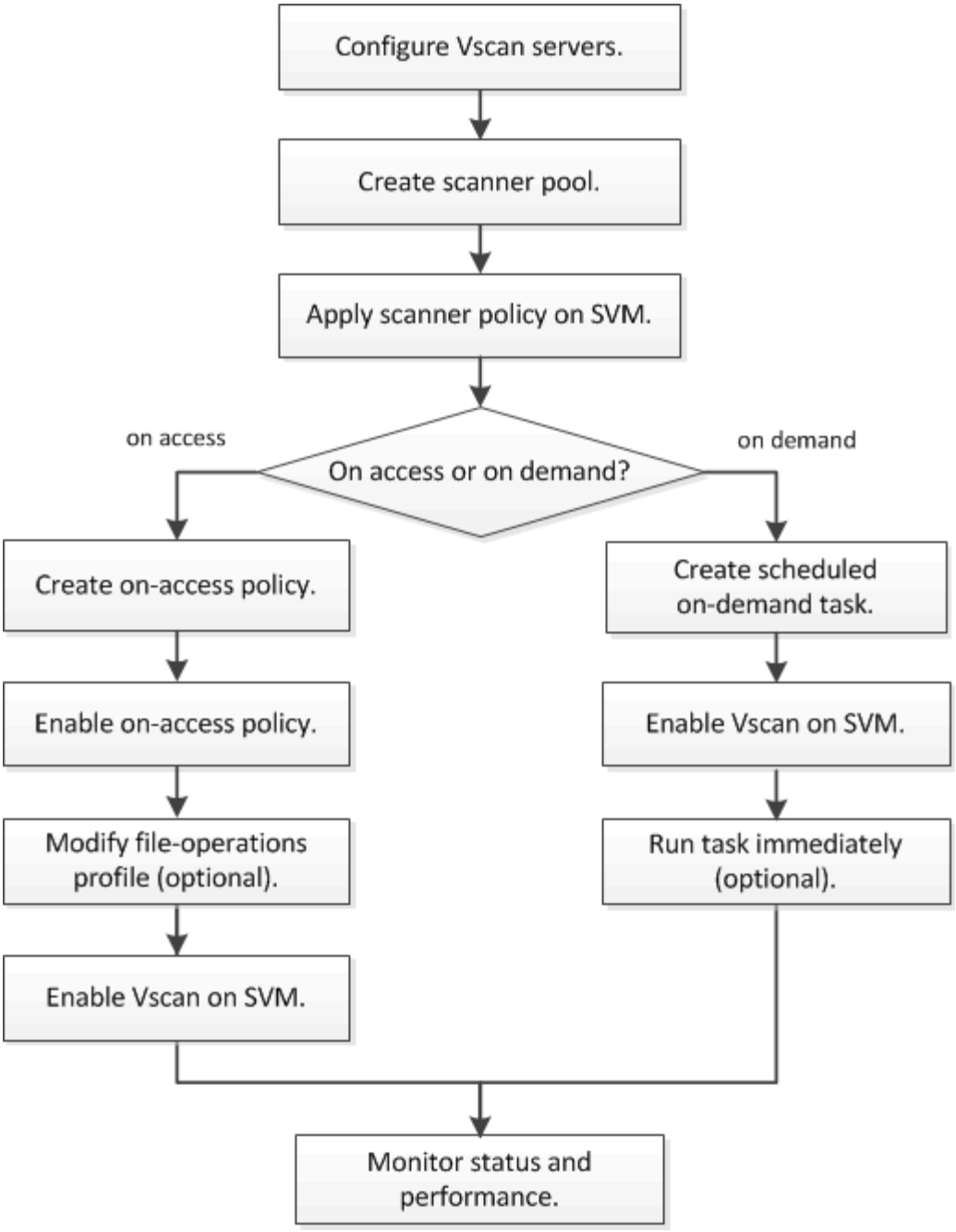
ONTAP 防病毒连接器由 NetApp 提供并安装在外部服务器上，用于处理存储系统与防病毒软件之间的通信。



病毒扫描工作流

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没有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"	• "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"	• "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	• "SentinelOne Singlity Cloud Data Security" • "SentinelOne支持" 此链接需要用户登录。您可以从Sentinel One申请访问权限。	深刻的直觉