配置实时扫描

ONTAP 9

NetApp
April 24, 2024

目录

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。

> 不会对具有的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	`vserver vscan on-access-policy create`
修改实时策略	`vserver vscan on-access-policy modify`
启用实时策略	`vserver vscan on-access-policy enable`
禁用实时策略	`vserver vscan on-access-policy disable`
删除实时策略	`vserver vscan on-access-policy delete`
查看实时策略的摘要和详细信息	`vserver vscan on-access-policy show`
添加到要排除的路径列表	`vserver vscan on-access-policy paths-to-exclude add`
从要排除的路径列表中删除	`vserver vscan on-access-policy paths-to-exclude remove`
查看要排除的路径列表	`vserver vscan on-access-policy paths-to-exclude show`
添加到要排除的文件扩展名列表	`vserver vscan on-access-policy file-ext-to-exclude add`
从要排除的文件扩展名列表中删除	`vserver vscan on-access-policy file-ext-to-exclude remove`

查看要排除的文件扩展名列表	`vserver vscan on-access-policy file-ext-to-exclude show`
添加到要包含的文件扩展名列表中	`vserver vscan on-access-policy file-ext-to-include add`
从要包含的文件扩展名列表中删除	`vserver vscan on-access-policy file-ext-to-include remove`
查看要包括的文件扩展名列表	`vserver vscan on-access-policy file-ext-to-include show`

有关这些命令的详细信息，请参见手册页。