Lenovo

Antivirus Configuration

ONTAP

First edition (February 2022)

Contents

Chapter 1. Antivirus configuration overview

This content describes how to use Lenovo virus scanning, called *Vscan*, to protect data from being compromised by viruses or other malicious code. It shows you how to use on-access scanning to check for viruses when clients access files over CIFS, and how to use on-demand scanning to check for viruses immediately or on a schedule.

You should use this content if you want to work with Vscan in the following ways:

- You want to use the ONTAP command-line interface (CLI), not ThinkSystem Storage Manager or an automated scripting tool.

  Vscan is not supported by ThinkSystem Storage Manager.

Chapter 2. About Lenovo antivirus protection

2.1. About Lenovo virus scanning

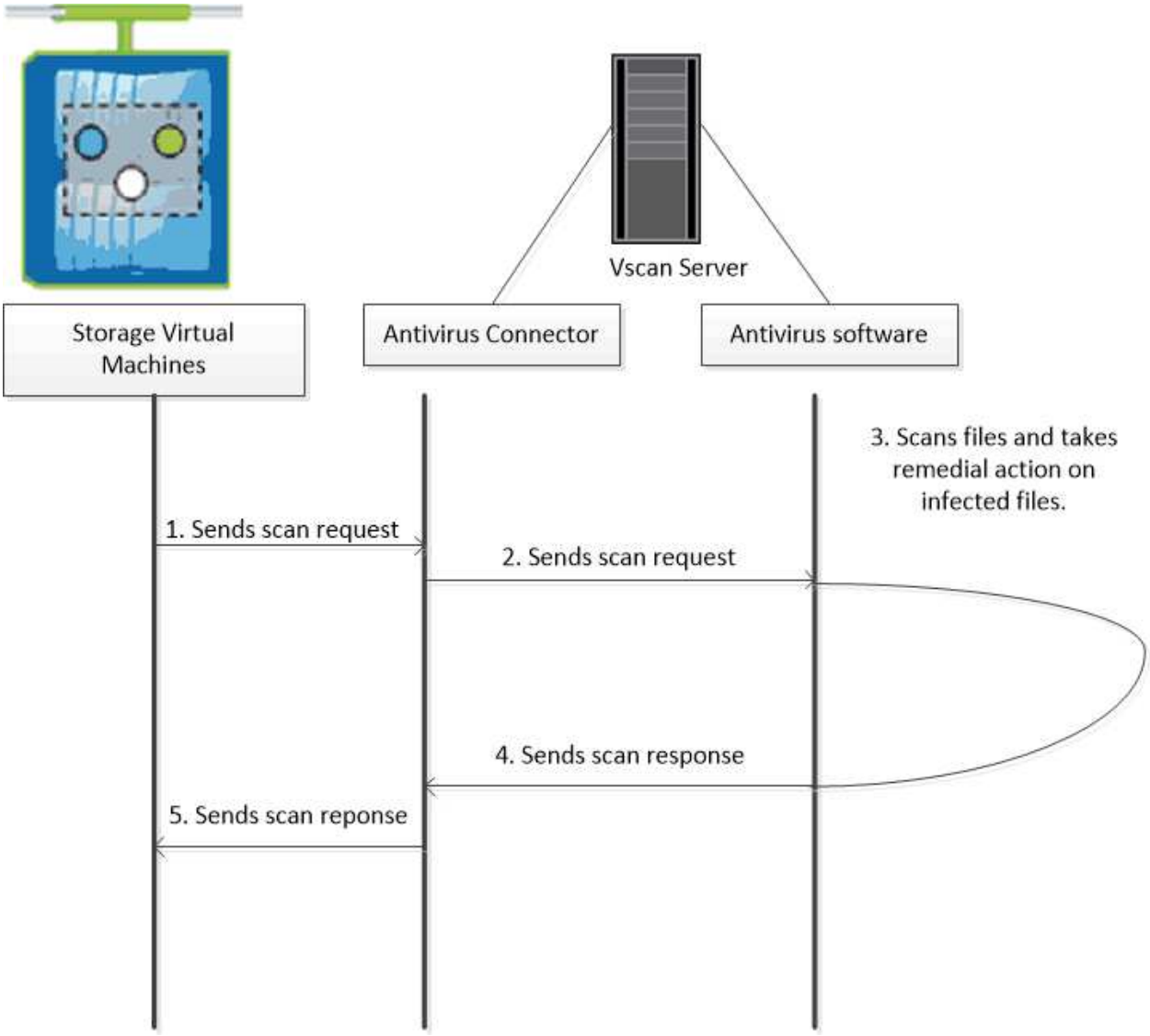
You can use integrated antivirus functionality on Lenovo DM storage systems to protect data from being compromised by viruses or other malicious code. Lenovo virus scanning, called *Vscan*, combines best-in-class third-party antivirus software with ONTAP features that give you the flexibility you need to control which files get scanned and when.

2.1.1. How virus scanning works

Storage systems offload scanning operations to external servers hosting antivirus software from third-party vendors. The ONTAP Antivirus Connector, provided by Lenovo and installed on the external server, handles communication between the storage system and the antivirus software.

- You can use *on-access scanning* to check for viruses when clients open, read, rename, or close files over CIFS. File operation is suspended until the external server reports the scan status of the file. If the file has already been scanned, ONTAP allows the file operation. Otherwise, it requests a scan from the server.
- You can use *on-demand scanning* to check files for viruses immediately or on a schedule. You might want to run scans only in off-peak hours, for example. The external server updates the scan status of the checked files, so that file-access latency for those files (assuming they have not been modified) is typically reduced when they are next accessed over CIFS. You can use on-demand scanning for any path in the SVM namespace, even for volumes that are exported only through NFS.

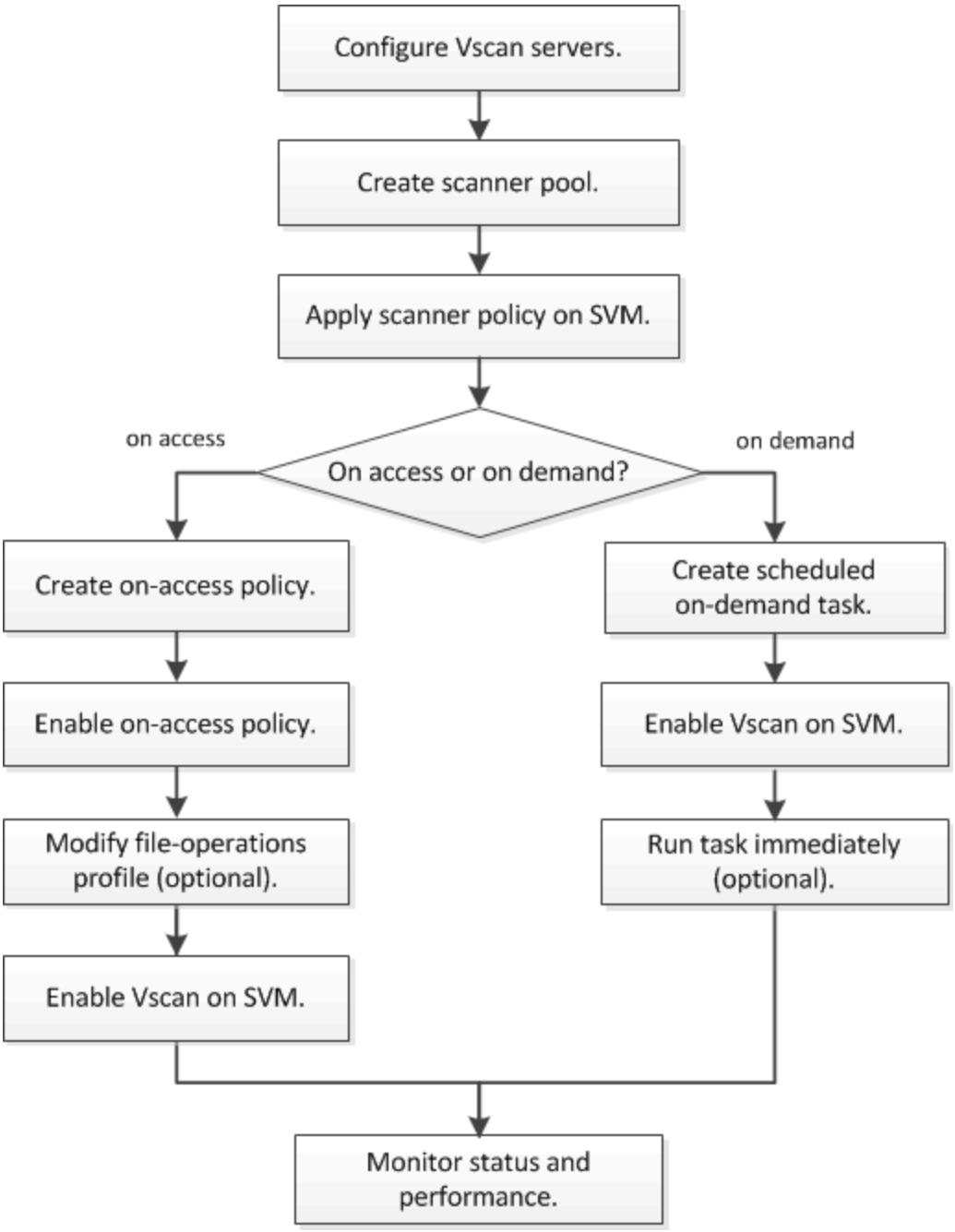
You typically enable both scanning modes on an SVM. In either mode, the antivirus software takes remedial action on infected files based on your settings in the software.



2.2. Virus scanning workflow

You must create a scanner pool and apply a scanner policy before you can enable scanning. You typically enable both on-access and on-demand scanning on an SVM.

You must have completed the CIFS configuration.



2.3. Antivirus architecture

The Lenovo antivirus architecture consists of a Vscan server and a set of ONTAP configurables.

2.3.1. Vscan server components

You must install the following components on the Vscan server.

- **ONTAP Antivirus Connector**

The ONTAP Antivirus Connector provided by Lenovo handles communication between ONTAP and the Vscan server.

- **Antivirus software**

  ONTAP-compliant third-party antivirus software scans files for viruses or other malicious code. You specify the remedial actions to be taken on infected files when you configure the software.

2.3.2. ONTAP configurables

You must configure the following items on the Lenovo DM storage system.

- **Scanner pool**

  A scanner pool defines the Vscan servers and privileged users that can connect to SVMs. It also defines a scan request timeout period, after which the scan request is sent to an alternative Vscan server if one is available.

  It is a best practice to set the timeout period in the antivirus software on the Vscan server to five seconds less than the scanner-pool request timeout period, to avoid situations in which file access is delayed or denied altogether because the timeout period on the software is greater than the timeout period for the scan request.

- **Privileged user**

  A privileged user is a domain user account that a Vscan server uses to connect to the SVM. The account must be included in the list of privileged users defined in the scanner pool.

- **Scanner policy**

  A scanner policy determines whether a scanner pool is active. A scanner policy can have one of the following values:

  - `Primary` specifies that the scanner pool is active.
  - `Secondary` specifies that the scanner pool is active only if none of the Vscan servers in the primary scanner pool is connected.
  - `Idle` specifies that the scanner pool is inactive. Scanner policies are system-defined. You cannot create a custom scanner policy.

- **On-access policy**

  An on-access policy defines the scope of an on-access scan. You can specify the maximum size of the files to be scanned, the extensions of the files to be included in the scan, and the extensions and paths of the files to be excluded from the scan.

  By default, only read-write volumes are scanned. You can specify filters that enable scanning of read-only volumes or that restrict scanning to files opened with execute access:

- `scan-ro-volume` enables scanning of read-only volumes.
- `scan-execute-access` restricts scanning to files opened with execute access.

"Execute access" is not identical with "execute permission". A given client will have "execute access" on an executable file only if the file was opened with "execute intent".

You can set the `scan-mandatory` option to off to specify that file access is allowed when no Vscan servers are available for virus scanning.

- **On-demand task**

  An on-demand task defines the scope of an on-demand scan. You can specify the maximum size of the files to be scanned, the extensions and paths of the files to be included in the scan, and the extensions and paths of the files to be excluded from the scan. Files in subdirectories are scanned by default.

  You use a cron schedule to specify when the task runs. You can use the `vserver vscan on-demand-task run` command to run the task immediately.

- **Vscan file-operations profile (on-access scanning only)**

  The `-vscan-fileop-profile` parameter for the `vserver cifs share create` command defines which operations on a SMB share can trigger virus scanning. By default, the parameter is set to `standard`, which is the Lenovo best practice.

  You can adjust this parameter as necessary when you create or modify a SMB share:

  - `no-scan` specifies that virus scans are never triggered for the share.
  - `standard` specifies that virus scans can be triggered by open, close, and rename operations.
  - `strict` specifies that virus scans can be triggered by open, read, close, and rename operations.

    The `strict` profile provides enhanced security for situations in which multiple clients access a file simultaneously. If one client closes a file after writing a virus to it, and the same file remains open on a second client, `strict` ensures that a read operation on the second client triggers a scan before the file is closed.

    You should be careful to restrict the `strict` profile to shares containing files that you anticipate will be accessed simultaneously. Because the profile generates more scan requests than the others, it may affect performance adversely.

  - `writes-only` specifies that virus scans can be triggered only when a file that has been modified is closed.

If a client application performs a rename operation, the file is closed with the new name and is not scanned. If such operations pose a security concern in your environment, you should use the `standard` or `strict` profile.

Because `writes-only` generates fewer scan requests than the other profiles (except `no-scan`), it typically improves performance.

Keep in mind, though, that if you use this profile for a share, the scanner must be configured to delete or quarantine an unrepairable infected file, so that it cannot be accessed by clients later. If, for example, a client closes a file after writing a virus to it, and the file is not repaired, deleted, or quarantined, any client that accesses the file *without* writing to it will be infected.

Chapter 3. Vscan server installation and configuration

You must set up one or more Vscan servers to ensure that files on your system are scanned for viruses. Follow the instructions provided by your vendor to install and configure the antivirus software on the server. Follow the instructions in the readme file provided by Lenovo to install and configure the ONTAP Antivirus Connector.

For disaster recovery and MetroCluster configurations, you must set up separate Vscan servers for the local and partner clusters.

3.1. Antivirus software requirements

- For information about antivirus software requirements, see the vendor documentation.

3.2. ONTAP Antivirus Connector requirements

- You can download the ONTAP Antivirus Connector from the Software Download page on Lenovo Data Center Support.
- For information about the recommended windows versions for ONTAP Antivirus Connector, see the Lenovo Interoperability Matrix.

  datacentersupport.lenovo.com/lsic

  You can install different versions of Windows servers for different Vscan servers in a cluster.

- .NET 3.0 or later must be installed on the Windows server.
- SMB 2.0 must be enabled on the Windows server.

Chapter 4. Configure scanner pools

4.1. Configure scanner pools overview

A scanner pool defines the Vscan servers and privileged users that can connect to SVMs. A scanner policy determines whether a scanner pool is active.

If you use an export policy on a CIFS server, you must add each Vscan server to the export policy.

4.2. Create a scanner pool on a single cluster

A scanner pool defines the Vscan servers and privileged users that can connect to SVMs. You can create a scanner pool for an individual SVM or for all of the SVMs in a cluster.

What you'll need

- SVMs and Vscan servers must be in the same domain or in trusted domains.
- For scanner pools defined for an individual SVM, you must have configured the ONTAP Antivirus Connector with the SVM management LIF or the SVM data LIF.
- For scanner pools defined for all of the SVMs in a cluster, you must have configured the ONTAP Antivirus Connector with the cluster management LIF.

About this task

The list of privileged users must include the domain user account the Vscan server uses to connect to the SVM.

Steps

1. Create a scanner pool:

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

   - Specify a data SVM for a pool defined for an individual SVM, and specify a cluster admin SVM for a pool defined for all of the SVMs in a cluster.
   - Specify an IP address or FQDN for each Vscan server host name.
   - Specify the domain and user name for each privileged user. For a complete list of options, see the man page for the command.

   The following command creates a scanner pool named `SP` on the SVM `vs1`:

```
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. Verify that the scanner pool was created: `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner-pool scanner_pool`

   For a complete list of options, see the man page for the command.

   The following command displays the details for the scanner pool `SP`:

```
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
```

   You can also use the `vserver vscan scanner-pool show` command to view all of the scanner pools on an SVM. For complete command syntax, see the man page for the command.

4.3. Create scanner pools in MetroCluster configurations

You must create primary and secondary scanner pools on each cluster in a MetroCluster configuration, corresponding to the primary and secondary SVMs on the cluster.

What you'll need

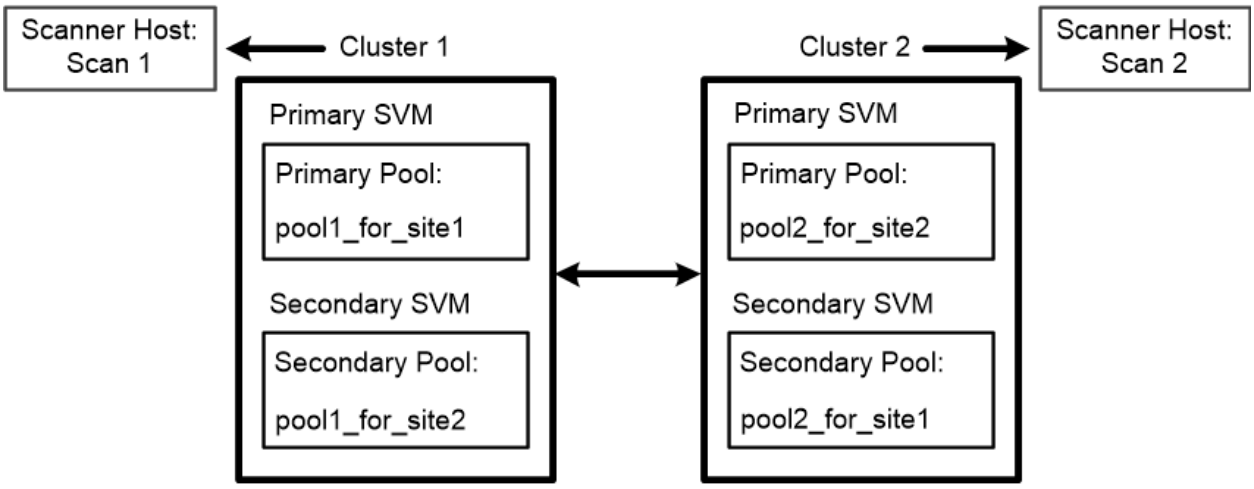
- SVMs and Vscan servers must be in the same domain or in trusted domains.
- For scanner pools defined for an individual SVM, you must have configured the ONTAP Antivirus Connector with the SVM management LIF or the SVM data LIF.
- For scanner pools defined for all of the SVMs in a cluster, you must have configured the ONTAP Antivirus Connector with the cluster management LIF.

About this task

MetroCluster configurations protect data by implementing two physically separate mirrored clusters. Each cluster synchronously replicates the data and SVM configuration of the other. A primary SVM on the local cluster serves data when the cluster is online. A secondary SVM on the local cluster serves data when the remote cluster is offline.

This means that you must create primary and secondary scanner pools on each cluster in a

MetroCluster configuration, corresponding to the primary and secondary SVMs on the cluster. The secondary pool becomes active when the cluster begins serving data from the secondary SVM. The following illustration shows a typical MetroCluster configuration.



The list of privileged users must include the domain user account the Vscan server uses to connect to the SVM.

Steps

1. Create a scanner pool:

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

   - Specify a data SVM for a pool defined for an individual SVM, and specify a cluster admin SVM for a pool defined for all the SVMs in a cluster.
   - Specify an IP address or FQDN for each Vscan server host name.
   - Specify the domain and user name for each privileged user.

   You must create all scanner pools from the cluster containing the primary SVM.

   For a complete list of options, see the man page for the command.

   The following commands create primary and secondary scanner pools on each cluster in a MetroCluster configuration:

```
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. Verify that the scanner pools were created: `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner-pool scanner_pool`

   For a complete list of options, see the man page for the command.

   The following command displays the details for the scanner pool `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
```

   You can also use the `vserver vscan scanner-pool show` command to view all of the scanner pools on an SVM. For complete command syntax, see the man page for the command.

4.4. Apply a scanner policy on a single cluster

A scanner policy determines whether a scanner pool is active. You must make a scanner pool active before the Vscan servers that are defined in the scanner pool can connect to an SVM.

About this task

- You can apply only one scanner policy to a scanner pool.
- If you created a scanner pool for all of the SVMs in a cluster, you must apply a scanner policy on each SVM individually.

- For disaster recovery and MetroCluster configurations, you must apply a scanner policy to the scanner pools for the local cluster and partner cluster.

  In the policy that you create for the local cluster, you must specify the local cluster in the `cluster` parameter. In the policy that you create for the partner cluster, you must specify the partner cluster in the `cluster` parameter. The partner cluster can then take over virus scanning operations in case of a disaster.

Steps

1. Apply a scanner policy:

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

   A scanner policy can have one of the following values:

   - `Primary` specifies that the scanner pool is active.
   - `Secondary` specifies that the scanner pool is active only if none of the Vscan servers in the primary scanner pool are connected.
   - `Idle` specifies that the scanner pool is inactive.

   The following example shows that the scanner pool named `SP` on the SVM `vs1` is active:

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

2. Verify that the scanner pool is active:

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

   For a complete list of options, see the man page for the command.

   The following command displays the details for the scanner pool `SP`:

   ```
   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
   ```

You can use the `vserver vscan scanner-pool show-active` command to view the active scanner pools on an SVM. For the complete command syntax, see the man page for the command.

4.5. Apply scanner policies in MetroCluster configurations

A scanner policy determines whether a scanner pool is active. You must apply a scanner policy to the primary and secondary scanner pools on each cluster in a MetroCluster configuration.

About this task

- You can apply only one scanner policy to a scanner pool.
- If you created a scanner pool for all of the SVMs in a cluster, you must apply a scanner policy on each SVM individually.

Steps

1. Apply a scanner policy:

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

   A scanner policy can have one of the following values:

   - `Primary` specifies that the scanner pool is active.
   - `Secondary` specifies that the scanner pool is active only if none of the Vscan servers in the primary scanner pool is connected.
   - `Idle` specifies that the scanner pool is inactive.

   You must apply all scanner policies from the cluster containing the primary SVM.

   The following commands apply scanner policies to the primary and secondary scanner pools on each cluster in a MetroCluster configuration:

   ```
   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 secondary -cluster cluster2

   cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
   -scanner-pool pool2_for_site2 -scanner-policy primary -cluster cluster2
   ```

2. Verify that the scanner pool is active:

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

   For a complete list of options, see the man page for the command.

   The following command displays the details for the scanner pool `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
```

   You can use the `vserver vscan scanner-pool show-active` command to view the active scanner pools on an SVM. For complete command syntax, see the man page for the command.

4.6. Commands for managing scanner pools

You can modify and delete scanner pools, and manage privileged users and Vscan servers for a scanner pool. You can view summary and details for a scanner pool.

If you want to…	Enter the following command…
Modify a scanner pool	`vserver vscan scanner-pool modify`
Delete a scanner pool	`vserver vscan scanner-pool delete`
Add privileged users to a scanner pool	`vserver vscan scanner-pool privileged-users add`
Delete privileged users from a scanner pool	`vserver vscan scanner-pool privileged-users remove`
Add Vscan servers to a scanner pool	`vserver vscan scanner-pool servers add`
Delete Vscan servers from a scanner pool	`vserver vscan scanner-pool servers remove`

If you want to…	Enter the following command…
View summary and details for a scanner pool	`vserver vscan scanner-pool show`
View privileged users for a scanner pool	`vserver vscan scanner-pool privileged-users show`
View Vscan servers for all scanner pools	`vserver vscan scanner-pool servers show`

For more information about these commands, see the man pages.

Chapter 5. Configure on-access scanning

5.1. Create an on-access policy

An on-access policy defines the scope of an on-access scan. You can specify the maximum size of the files to be scanned, the extensions of the files to be included in the scan, and the extensions and paths of the files to be excluded from the scan. You can create an on-access policy for an individual SVM or for all the SVMs in a cluster.

About this task

By default, ONTAP creates an on-access policy named “default_CIFS” and enables it for all the SVMs in a cluster.

You can set the `scan-mandatory` option to off to specify that file access is allowed when no Vscan servers are available for virus scanning. Keep in mind that any file that qualifies for scan exclusion based on the `paths-to-exclude`, `file-ext-to-exclude`, or `max-file-size` parameters is not considered for scanning even if the `scan-mandatory` option is set to `on`.

For potential issues related to the `scan-mandatory` option, see Potential connectivity issues involving the scan-mandatory option.

By default, only read-write volumes are scanned. You can specify filters that enable scanning of read-only volumes or that restrict scanning to files opened with execute access.

Steps

1. Create an on-access policy:

```
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
```

   - Specify a data SVM for a policy defined for an individual SVM, a cluster admin SVM for a policy defined for all the SVMs in a cluster.
   - The `-file-ext-to-exclude` setting overrides the `-file-ext-to-include` setting.
   - Set `-scan-files-with-no-ext` to true to scan files without extensions. The following command creates an on-access policy named `Policy1` on the SVM `vs1`:

```
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. Verify that the on-access policy has been created: `vserver vscan on-access-policy show -vserver data_SVM|cluster_admin_SVM -policy-name policy_name`

   For a complete list of options, see the man page for the command.

   The following command displays the details for the policy `Policy1`:

```
cluster1::> vserver vscan on-access-policy show -vserver 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
```

5.2. Enable an on-access policy

You must enable an on-access policy on an SVM before its files can be scanned. If you created an on-access policy for all the SVMs in a cluster, you must enable the policy on each SVM individually. You can enable only one on-access policy on an SVM at a time.

Steps

1. Enable an on-access policy:

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

   The following command enables an on-access policy named `Policy1` on the SVM `vs1`:

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

2. Verify that the on-access policy is enabled: `vserver vscan on-access-policy show -vserver data_SVM -policy-name policy_name`

   For a complete list of options, see the man page for the command.

   The following command displays the details for the on-access policy `Policy1` :

```
cluster1::> vserver vscan on-access-policy show -vserver 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
```

5.3. Modify the Vscan file-operations profile for a CIFS share

The Vscan file-operations profile for a CIFS share defines which operations on the share can trigger scanning. By default, the parameter is set to `standard`. You can adjust the parameter as necessary when you create or modify a CIFS share.

About this task

For more information on the available values for a Vscan file-operations profile, see "Vscan file-operations profile".

Vscan file-operations profile (on-access scanning only)

Virus scanning is not performed on a CIFS share for which the `continuously-available` parameter is set to `Yes`.

Step

1. Modify the value of the Vscan file-operations profile for a CIFS share: `vserver cifs share modify -vserver data_SVM -share-name share -path share_path -vscan-fileop-profile no-scan|standard|strict|writes-only`

   For a complete list of options, see the man page for the command.

   The following command changes the Vscan file operations profile for a CIFS share to `strict`:

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

5.4. Commands for managing on-access policies

You can modify, disable, or delete an on-access policy. You can view a

summary and details for the policy.

If you want to…	Enter the following command…
Modify an on-access policy	`vserver vscan on-access-policy modify`
Disable an on-access policy	`vserver vscan on-access-policy disable`
Delete an on-access policy	`vserver vscan on-access-policy delete`
View summary and details for an on-access policy	`vserver vscan on-access-policy show`
Add to the list of paths to exclude	`vscan on-access-policy paths-to-exclude add`
Delete from the list of paths to exclude	`vscan on-access-policy paths-to-exclude remove`
View the list of paths to exclude	`vscan on-access-policy paths-to-exclude show`
Add to the list of file extensions to exclude	`vscan on-access-policy file-ext-to-exclude add`
Delete from the list of file extensions to exclude	`vscan on-access-policy file-ext-to-exclude remove`
View the list of file extensions to exclude	`vscan on-access-policy file-ext-to-exclude show`
Add to the list of file extensions to include	`vscan on-access-policy file-ext-to-include add`
Delete from the list of file extensions to include	`vscan on-access-policy file-ext-to-include remove`
View the list of file extensions to include	`vscan on-access-policy file-ext-to-include show`

For more information about these commands, see the man pages.

Chapter 6. Configure on-demand scanning

6.1. Configure on-demand scanning overview

You can use on-demand scanning to check files for viruses immediately or on a schedule. You might want to run scans only in off-peak hours, for example, or you might want to scan very large files that were excluded from an on-access scan.

You can use a cron schedule to specify when the task runs:

- You can assign a schedule when you create a task.
- You can create a task without assigning a schedule, and use the `vserver vscan on-demand-task schedule` command to assign a schedule.
- You can use the `vserver vscan on-demand-task run` command to run a task immediately, whether or not you have assigned a schedule.

Only one task can be scheduled at a time on an SVM.

On-demand scanning does not support scanning of symbolic links or stream files.

6.2. Create an on-demand task

An on-demand task defines the scope of an on-demand scan. You can specify the maximum size of the files to be scanned, the extensions and paths of the files to be included in the scan, and the extensions and paths of the files to be excluded from the scan. Files in subdirectories are scanned by default.

Steps

1. Create an on-demand task:

```
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_of_files_to_exclude -file-ext-to
-exclude extensions_of_files_to_exclude -file-ext-to-include
extensions_of_files_to_include -scan-files-with-no-ext true|false -directory
-recursion true|false
```

   - The `-file-ext-to-exclude` setting overrides the `-file-ext-to-include` setting.
   - Set `-scan-files-with-no-ext` to true to scan files without extensions. For a complete list of options, see the man page for the command.

   The following command creates an on-access task named `Task1` on the SVM `vs1`:

```
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.
```

You can use the `job show` command to view the status of the job. You can use the `job pause` and `job resume` commands to pause and restart the job, or the `job stop` command to end the job.

2. Verify that the on-demand task has been created: `vserver vscan on-demand-task show -vserver data_SVM -task-name task_name`

   For a complete list of options, see the man page for the command.

   The following command displays the details for the task `Task1`:

```
cluster1::> vserver vscan on-demand-task show -vserver 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: -
```

After you finish

You must enable scanning on the SVM before the task is scheduled to run.

6.3. Schedule an on-demand task

If you have created an on-demand task without assigning a schedule, or if you want to assign a different schedule to a task, you can use the `vserver vscan on-demand-task schedule` command to assign a schedule to the task.

About this task

The schedule assigned with the `vserver vscan on-demand-task schedule` command overrides a

schedule already assigned with the `vserver vscan on-demand-task create` command.

Steps

1. Schedule an on-demand task:

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

   The following command schedules an on-access task named `Task2` on the SVM `vs2`:

   ```
   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.
   ```

   > You can use the `job show` command to view the status of the job. You can use the `job pause` and `job resume` commands to pause and restart the job, or the `job stop` command to end the job.

2. Verify that the on-demand task has been scheduled: `vserver vscan on-demand-task show -vserver data_SVM -task-name task_name`

   For a complete list of options, see the man page for the command.

   The following command displays the details for the task `Task 2` :

   ```
   cluster1::> vserver vscan on-demand-task show -vserver 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
   ```

After you finish

You must enable scanning on the SVM before the task is scheduled to run.

6.4. Run an on-demand task immediately

You can run an on-demand task immediately, whether or not you have assigned a schedule.

What you'll need

You must have enabled scanning on the SVM.

Step

1. Run an on-demand task immediately:

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

   The following command runs an on-access task named `Task1` on the SVM `vs1`:

   ```
   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.
   ```

   You can use the `job show` command to view the status of the job. You can use the `job pause` and `job resume` commands to pause and restart the job, or the `job stop` command to end the job.

6.5. Commands for managing on-demand tasks

You can modify, delete, or unschedule an on-demand task. You can view a summary and details for the task, and manage reports for the task.

If you want to…	Enter the following command…
Modify an on-demand task	`vserver vscan on-demand-task modify`
Delete an on-demand task	`vserver vscan on-demand-task delete`
Unschedule an on-demand task	`vserver vscan on-demand-task unschedule`
View summary and details for an on-demand task	`vserver vscan on-demand-task show`
View on-demand reports	`vserver vscan on-demand-task report show`
Delete on-demand reports	`vserver vscan on-demand-task report delete`

For more information about these commands, see the man pages.

Chapter 7. Enable virus scanning on an SVM

You must enable virus scanning on an SVM before an on-access or on-demand scan can run. The Vscan configuration must exist.

Steps

1. Enable virus scanning on an SVM:

   `vserver vscan enable -vserver data_SVM`

   You can use the `vserver vscan disable` command to disable virus scanning if necessary.

   The following command enables virus scanning on the SVM `vs1`:

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

2. Verify that virus scanning is enabled on the SVM:

   `vserver vscan show -vserver data_SVM`

   For a complete list of options, see the man page for the command.

   The following command displays the Vscan status of the SVM `vs1`:

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

                            Vserver: vs1
                       Vscan Status: on
   ```

Chapter 8. Reset the status of scanned files

Occasionally, you might want to reset the scan status of successfully scanned files on an SVM by using the `vserver vscan reset` command to discard the cached information for the files. You might want to use this command to restart the virus scanning processing in case of a misconfigured scan, for example.

About this task

After you run the `vserver vscan reset` command, all eligible files will be scanned the next time they are accessed.

This command can affect performance adversely, depending on the number and size of the files to be rescanned.

Step

1. Reset the status of scanned files:

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

   The following command resets the status of scanned files on the SVM `vs1`:

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

Chapter 9. View Vscan event log information

You can use the `vserver vscan show-events` command to view event log information about infected files, updates to Vscan servers, and the like. You can view event information for the cluster or for given nodes, SVMs, or Vscan servers.

What you'll need

Advanced privileges are required for this task.

Steps

1. Change to advanced privilege level:

   ```
   set -privilege advanced
   ```

2. View Vscan event log information:

   ```
   vserver vscan show-events
   ```

   For a complete list of options, see the man page for the command.

   The following command displays event log information for the cluster `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.
   ```

Chapter 10. Troubleshoot connectivity issues

10.1. Potential connectivity issues involving the scan-mandatory option

You can use the `vserver vscan connection-status show` commands to view information about Vscan server connections that you might find helpful in troubleshooting connectivity issues.

By default, the `scan-mandatory` option for on-access scanning denies file access when a Vscan server connection is not available for scanning. Although this option offers important safety features, it can lead to problems in a few situations.

- Before enabling client access, you must ensure that at least one Vscan server is connected to an SVM on each node that has a LIF. If you need to connect servers to SVMs after enabling client access, you must turn off the `scan-mandatory` option on the SVM to ensure that file access is not denied because a Vscan server connection is not available. You can turn the option back on after the server has been connected.
- If a target LIF hosts all the Vscan server connections for an SVM, the connection between the server and the SVM will be lost if the LIF is migrated. To ensure that file access is not denied because a Vscan server connection is not available, you must turn off the `scan-mandatory` option before migrating the LIF. You can turn the option back on after the LIF has been migrated.

Each SVM should have at least two Vscan servers assigned to it. It is a best practice to connect Vscan servers to the storage system over a different network from the one used for client access.

10.2. Commands for viewing Vscan server connection status

You can use the `vserver vscan connection-status show` commands to view summary and detailed information about Vscan server connection status.

If you want to…	Enter the following command…
View a summary of Vscan server connections	`vserver vscan connection-status show`
View details for Vscan server connections	`vserver vscan connection-status show-all`
View details for connected Vscan servers	`vserver vscan connection-status show-connected`
View details for available Vscan servers that are not connected	`vserver vscan connection-status show-not-connected`

For more information about these commands, see the man pages.

Chapter 11. Appendix

11.1. Contacting support

You can contact Support to obtain help for your issue.

You can receive hardware service through a Lenovo Authorized Service Provider. To locate a service provider authorized by Lenovo to provide warranty service, go to https://datacentersupport.lenovo.com/serviceprovider and use filter searching for different countries. For Lenovo support telephone numbers, see https://datacentersupport.lenovo.com/supportphonelist for your region support details.

11.2. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document is not an offer and does not provide a license under any patents or patent applications. You can send inquiries in writing to the following:

```
Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing
```

LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information

contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

11.3. Trademarks