Lenovo

NDMP Configuration Express Guide

ONTAP® 9

Second Edition (March 2021)

Contents

Chapter 1. Deciding whether to use the NDMP Configuration Express Guide

This guide describes how to quickly configure an ONTAP 9 cluster to use the Network Data Management Protocol (NDMP) to back up data directly to tape using a third-party backup application.

You should use this guide if you want to configure NDMP in the following context:

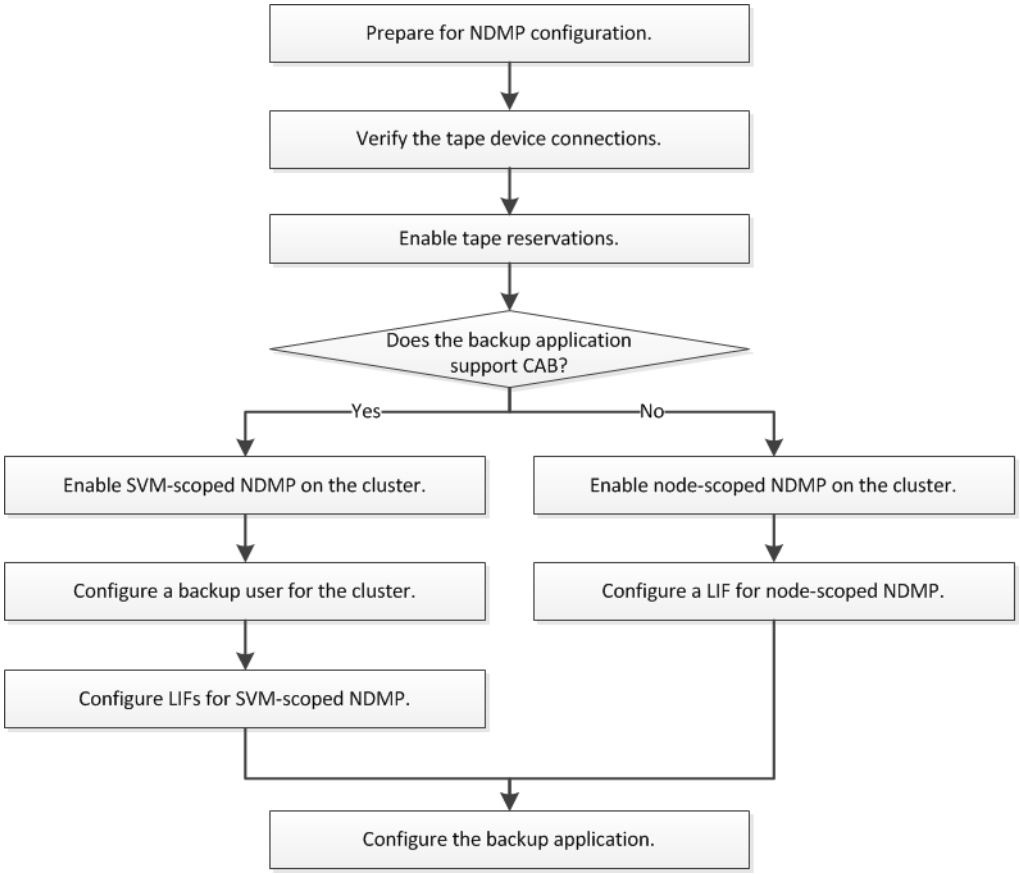
- The cluster is running ONTAP 9.
- You have a third-party backup application (also called a Data Management Application or DMA).
- You are a cluster administrator.
- You want to perform backup operations either at the cluster level (using the admin storage virtual machine (SVM)) or node level.
- Tape devices and an optional media server are installed.
- Tape devices are connected to the cluster through a Fibre Channel (FC) switch and not directly attached.
- At least one tape device has a logical unit number (LUN) of 0.
- You are using FlexVol volumes and not Infinite Volumes.
- You want to use best practices, not explore every available option.
- You do not want to read a lot of conceptual background.

If these assumptions are not correct for your situation, you should see the *Clustered Data ONTAP Data Protection Tape Backup and Recovery Guide*.

Data protection using tape backup

Chapter 2. NDMP configuration workflow

Setting up tape backup over NDMP involves preparing for NDMP configuration, verifying the tape device connections, enabling tape reservations, configuring NDMP at the SVM or node level, enabling NDMP on the cluster, configuring a backup user, configuring LIFs, and configuring the backup application.



Preparing for NDMP configuration

Before you configure tape backup access over Network Data Management Protocol (NDMP), you must verify that the planned configuration is supported, verify that your tape drives are listed as qualified drives on each node, verify that all nodes have intercluster LIFs, and identify whether the backup application supports the Cluster Aware Backup (CAB) extension.

Step 1. Verify that the planned configuration is supported by checking Lenovo Storage Interoperability Center (LSIC).

https://datacentersupport.lenovo.com/lsic

You should verify that the following components are compatible:

- The version of ONTAP 9 that is running on the cluster.
- The backup application vendor and application version: for example, Symantec NetBackup 7.6 or CommVault Simpana 10 SP8.

- The tape devices details, such as the manufacturer, model, and interface of the tape drives: for example, IBM Ultrium-TD4 FC or HP Ultrium-5 SAS.
- The platforms of the nodes in the cluster: for example, FAS3260 or FAS6280.

Step 2. Verify that your tape drives are listed as qualified drives in each node's built-in tape configuration file:

a. On the command line-interface, view the built-in tape configuration file by using the **storage tape show-supported-status** command.

Example

```
cluster1::> storage tape show-supported-status

Node: cluster1-1
                                  Is
Tape Drives                       Supported  Support Status
--------------------------------  ---------  --------------------------------
Certance Ultrium 2                true       Dynamically Qualified
Certance Ultrium 3                true       Dynamically Qualified
Digital DLT2000                   true       Qualified
....
```

b. Compare your tape drives to the list of qualified drives in the output.

Note: The names of the tape devices in the output might vary slightly from the names on the device label or in Lenovo Storage Interoperability Center (LSIC). For example, Digital DLT2000 can also be known as DLT2k. You can ignore these minor naming differences.

c. If a device is not listed as qualified in the output even though the device is qualified according to Lenovo Storage Interoperability Center (LSIC), download and install an updated configuration file for the device using the instructions on the Lenovo Data Center Support site.

Lenovo Downloads: Tape Device Configuration Files

A qualified device might not be listed in the built-in tape configuration file if the tape device was qualified after the node was shipped.

Step 3. Verify that every node in the cluster has an intercluster LIF:

a. View the intercluster LIFs on the nodes by using the **network interface show -role intercluster** command.

Example

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1    e0a     true
```

b. If an intercluster LIF does not exist on any node, create an intercluster LIF by using the **network interface create** command.

Example

```
cluster1::> network interface create -vserver cluster1 -lif IC2 -role intercluster
-home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask 255.255.255.0
-status-admin up -failover-policy local-only -firewall-policy intercluster

cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current       Current Is
```

```
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1    e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2    e0b     true
```

Network Management Guide

Step 4. Identify whether the backup application supports Cluster Aware Backup (CAB) by using the documentation provided with the backup application.

CAB support is a key factor in determining the type of backup you can perform.

Verifying tape device connections

You must ensure that all drives and media changers are visible in Data ONTAP as devices.

Step 1. View information about all drives and media changers by using the **storage tape show** command.

Example

```
cluster1::> storage tape show

Node: cluster1-01
Device ID                Device Type     Description                     Status
-----------------------  --------------  ------------------------------  --------
sw4:10.11                tape drive      HP LTO-3                        normal
0b.125L1                 media changer   HP MSL G3 Series                normal
0d.4                     tape drive      IBM LTO 5 ULT3580               normal
0d.4L1                   media changer   IBM 3573-TL                     normal
...
```

Step 2. If a tape drive is not displayed, troubleshoot the problem.

Step 3. If a media changer is not displayed, view information about media changers by using the **storage tape show-media-changer** command, and then troubleshoot the problem.

Example

```
cluster1::> storage tape show-media-changer

Media Changer: sw4:10.11L1
  Description: PX70-TL
         WWNN: 2:00a:000e11:10b919
         WWPN: 2:00b:000e11:10b919
Serial Number: 00FRU7800000_LL1

       Errors: -

Paths:
Node                      Initiator  Alias    Device State              Status
------------------------  ---------  -------  ------------------------  --------
cluster1-01               2b         mc0      in-use                    normal
...
```

Enabling tape reservations

You must ensure that tape drives are reserved for use by backup applications for NDMP backup operations.

About this task

The reservation settings vary in different backup applications, and these settings must match the backup application and the nodes or servers using the same drives. See the vendor documentation of the backup application for the correct reservation settings.

Step 1. Enable reservations by using the **options -option-name tape.reservations -option-value persistent** command.

Example

The following command enables reservations with the persistent value:

```
cluster1::> options -option-name tape.reservations -option-value persistent
2 entries were modified.
```

Step 2. Verify that reservations are enabled on all nodes by using the **options tape.reservations** command, and then review the output.

Example

```
cluster1::> options tape.reservations

cluster1-1
    tape.reservations                 persistent

cluster1-2
    tape.reservations                 persistent
2 entries were displayed.
```

Configuring NDMP at the SVM level or the node level

If the backup application supports Cluster Aware Backup (CAB), you can configure NDMP as SVM-scoped at the cluster (admin SVM) level, which enables you to back up all volumes hosted across different nodes of the cluster. Otherwise, you can configure node-scoped NDMP, which enables you to back up all the volumes hosted on that node.

Configuring SVM-scoped NDMP

If the DMA supports the Cluster Aware Backup (CAB) extension, you can back up all the volumes hosted across different nodes in a cluster by enabling SVM-scoped NDMP, configuring a backup user account, and configuring LIFs for data and control connection.

Before you begin

The CAB extension must be supported by the DMA.

Enabling SVM-scoped NDMP on the cluster

You can configure SVM-scoped NDMP on the cluster by enabling SVM-scoped NDMP mode and NDMP service on the cluster (admin SVM).

About this task

Turning off node-scoped NDMP mode enables SVM-scoped NDMP mode on the cluster.

Step 1. Enable SVM-scoped NDMP mode by using the **system services ndmp** command with the node-scope-mode parameter.

Example

```
cluster1::> system services ndmp node-scope-mode off
```

```
NDMP node-scope-mode is disabled.
```

Step 2. Enable NDMP service on the admin SVM by using the **vserver services ndmp on** command.

Example

```
cluster1::> vserver services ndmp on -vserver cluster1
```
The authentication type is set to challenge by default and plaintext authentication is disabled.

Note: For secure communication, you should keep plaintext authentication disabled.

Step 3. Verify that NDMP service is enabled by using the **vserver services ndmp show** command.

Example

```
cluster1::> vserver services ndmp show

Vserver       Enabled   Authentication type
------------- --------- -------------------
cluster1      true      challenge
vs1            false     challenge
```

Configuring a backup user for the cluster

To authenticate NDMP from the backup application, you must create a local backup user, or an NIS or LDAP user for the cluster with the admin or backup role, and generate an NDMP password for the backup user.

Before you begin

If you are using an NIS or LDAP user, the user must be created on the respective server. You cannot use an Active Directory user.

Step 1. Create a backup user with the admin or backup role by using the **security login create** command. You can specify a local backup user name or an NIS or LDAP user name for the -user-or-group-name parameter.

Example

The following command creates the backup user backup_admin1 with the backup role:
```
cluster1::> security login create -user-or-group-name backup_admin1 -application ssh
-authmethod password -role backup

Please enter a password for user 'backup_admin1':
Please enter it again:
```

Step 2. Generate a password for the admin SVM by using the **vserver services ndmp generate password** command.
The generated password must be used to authenticate the NDMP connection by the backup application.

Example

```
cluster1::> vserver services ndmp generate-password -vserver cluster1 -user backup_admin1

 Vserver: cluster1
    User: backup_admin1
Password: qG5CqQHYxw7tE57g
```

Configuring LIFs

You must identify the LIFs that will be used for establishing a data connection between the data and tape resources, and for control connection between the admin SVM and the backup application. After identifying

the LIFs, you must verify that firewall and failover policies are set for the LIFs, and specify the preferred interface role.

Step 1. Identify the intercluster, cluster-management, and node-management LIFs by using the **network interface show** command with the -role parameter.

Example

The following command displays the intercluster LIFs:

```
cluster1::> network interface show -role intercluster

            Logical          Status     Network            Current       Current Is
Vserver     Interface        Admin/Oper Address/Mask       Node          Port    Home
----------- ----------       ---------- ------------------ ------------- ------- ----
cluster1    IC1              up/up      192.0.2.65/24      cluster1-1    e0a     true
cluster1    IC2              up/up      192.0.2.68/24      cluster1-2    e0b     true
```

The following command displays the cluster-management LIF:

```
cluster1::> network interface show -role cluster-mgmt

            Logical          Status     Network            Current       Current Is
Vserver     Interface        Admin/Oper Address/Mask       Node          Port    Home
----------- ----------       ---------- ------------------ ------------- ------- ----
cluster1    cluster_mgmt     up/up      192.0.2.60/24      cluster1-2    e0M     true
```

The following command displays the node-management LIFs:

```
cluster1::> network interface show -role node-mgmt

            Logical          Status     Network            Current       Current Is
Vserver     Interface        Admin/Oper Address/Mask       Node          Port    Home
----------- ----------       ---------- ------------------ ------------  ------  ------
cluster1    cluster1-1_mgmt1 up/up      192.0.2.69/24      cluster1-1    e0M     true
            cluster1-2_mgmt1 up/up      192.0.2.70/24      cluster1-2    e0M     true
```

Step 2. Ensure that the firewall policy is enabled for NDMP on the intercluster, cluster-management (cluster-mgmt), and node-management (node-mgmt) LIFs:

a. Verify that the firewall policy is enabled for NDMP by using the **system services firewall policy show** command.

Example

The following command displays the firewall policy for the cluster-management LIF:

```
cluster1::> system services firewall policy show -policy cluster

Vserver     Policy        Service    Allowed
-------     ------------  ---------- ------------------
cluster     cluster       dns        0.0.0.0/0
                          http       0.0.0.0/0
                          https      0.0.0.0/0
                          ndmp       0.0.0.0/0
                          ndmps      0.0.0.0/0
                          ntp        0.0.0.0/0
                          rsh        0.0.0.0/0
                          snmp       0.0.0.0/0
                          ssh        0.0.0.0/0
                          telnet     0.0.0.0/0
10 entries were displayed.
```

The following command displays the firewall policy for the intercluster LIF:

```
cluster1::> system services firewall policy show -policy intercluster
```

```
Vserver     Policy        Service    Allowed
-------     ------------ ---------- --------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         ndmp        0.0.0.0/0, ::/0
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

The following command displays the firewall policy for the node-management LIF:

```
cluster1::> system services firewall policy show -policy mgmt

Vserver     Policy        Service    Allowed
-------     ------------ ---------- --------------------
cluster1-1  mgmt          dns        0.0.0.0/0, ::/0
                         http       0.0.0.0/0, ::/0
                         https      0.0.0.0/0, ::/0
                         ndmp        0.0.0.0/0, ::/0
                         ndmps      0.0.0.0/0, ::/0
                         ntp        0.0.0.0/0, ::/0
                         rsh        -
                         snmp       0.0.0.0/0, ::/0
                         ssh        0.0.0.0/0, ::/0
                         telnet     -
10 entries were displayed.
```

b. If the firewall policy is not enabled, enable the firewall policy by using the **system services firewall policy modify** command with the -service parameter.

Example

The following command enables firewall policy for the intercluster LIF:

```
cluster1::> system services firewall policy modify
 -vserver cluster1 -policy intercluster -service ndmp 0.0.0.0/0
```

Step 3. Ensure that the failover policy is set appropriately for all the LIFs:

a. Verify that the failover policy for the cluster-management LIF is set to broadcast-domain-wide , and the policy for the intercluster and node-management LIFs is set to local-only by using the **network interface show -failover** command.

Example

The following command displays the failover policy for the cluster-management, intercluster, and node-management LIFs:

```
cluster1::> network interface show -failover

           Logical             Home               Failover              Failover
Vserver    Interface           Node:Port          Policy                Group
---------- -----------------  -----------------  --------------------  ---------
cluster    cluster1_clus1     cluster1-1:e0a     local-only            cluster
                                                        Failover Targets:
                                                       .......

cluster1   cluster_mgmt        cluster1-1:e0m     broadcast-domain-wide Default
                                                        Failover Targets:
                                                        .......
           IC1                 cluster1-1:e0a     local-only            Default
                                                        Failover Targets:
           IC2                 cluster1-1:e0b     local-only            Default
```

```
                                                    Failover Targets:
                                                    .......
cluster1-1  cluster1-1_mgmt1    cluster1-1:e0m      local-only          Default
                                                    Failover Targets:
                                                    ......
cluster1-2  cluster1-2_mgmt1    cluster1-2:e0m      local-only          Default
                                                    Failover Targets:
                                                    ......
```

b. If the failover policies are not set appropriately, modify the failover policy by using the **network interface modify** command with the -failover-policy parameter.

Example

```
cluster1::> network interface modify -vserver cluster1 -lif IC1 -failover-policy local-only
```

Step 4. Specify the LIFs that are required for data connection by using the **vserver services ndmp modify** command with the preferred-interface-role parameter.

Example

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

Step 5. Verify that the preferred interface role is set for the cluster by using the **vserver services ndmp show** command.

Example

```
cluster1::> vserver services ndmp show -vserver cluster1

                            Vserver: cluster1
                       NDMP Version: 4
                       .......
                       .......
          Preferred Interface Role: intercluster, cluster-mgmt, node-mgmt
```

Configuring node-scoped NDMP

You can back up volumes hosted on a node by enabling node-scoped NDMP, setting up the password for the root user, and configuring a LIF for data and control connection.

Enabling node-scoped NDMP on the cluster

You can configure node-scoped NDMP by enabling node-scoped NDMP on the cluster and NDMP service on all nodes of the cluster. You must also configure the root user for NDMP when enabling the NDMP service.

Step 1. Enable node-scoped NDMP mode by using the **system services ndmp** command with the node-scope-mode parameter.

Example

```
cluster1::> system services ndmp node-scope-mode on
NDMP node-scope-mode is enabled.
```

Step 2. Enable NDMP service on all nodes in the cluster by using the **system services ndmp on** command.
Using the wildcard “*” enables NDMP service on all nodes at the same time.
You must specify a password for authentication of the NDMP connection by the backup application.

Example

```
cluster1::> system services ndmp on -node *

Please enter password:
Confirm password:
2 entries were modified.
```

Step 3. Disable the -clear-text option for secure communication of the NDMP password by using the **system services ndmp modify** command.
Using the wildcard "*" disables the -clear-text option on all nodes at the same time.

Example

```
cluster1::> system services ndmp modify -node * -clear-text false
2 entries were modified.
```

Step 4. Verify that NDMP service is enabled and the -clear-text option is disabled by using the **system services ndmp show** command.

Example

```
cluster1::> system services ndmp show
Node                  Enabled   Clear text  User Id
--------------------- --------- ----------- ---------
cluster1-1            true      false       root
cluster1-2            true      false       root
2 entries were displayed.
```

Configuring a LIF

You must identify a LIF that will be used for establishing a data connection and control connection between the node and the backup application. After identifying the LIF, you must verify that firewall and failover policies are set for the LIF.

Step 1. Identify the intercluster LIF hosted on the nodes by using the **network interface show** command with the -role parameter.

Example

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1    e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2    e0b     true
```

Step 2. Ensure that the firewall policy is enabled for NDMP on the intercluster LIFs:

a. Verify that the firewall policy is enabled for NDMP by using the **system services firewall policy show** command.

Example

The following command displays the firewall policy for the intercluster LIF:

```
cluster1::> system services firewall policy show -policy intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
```

```
                                ndmp        0.0.0.0/0, ::/0
                                ndmps       -
                                ntp         -
                                rsh         -
                                ssh         -
                                telnet      -
9 entries were displayed.
```

b. If the firewall policy is not enabled, enable the firewall policy by using the **system services firewall policy modify** command with the -service parameter.

Example

The following command enables firewall policy for the intercluster LIF:

```
cluster1::> system services firewall policy modify
 -vserver cluster1 -policy intercluster -service ndmp 0.0.0.0/0
```

Step 3. Ensure that the failover policy is set appropriately for the intercluster LIFs:

a. Verify that the failover policy for the intercluster LIFs is set to local-only by using the **network interface show -failover** command.

Example

```
cluster1::> network interface show -failover
             Logical           Home                Failover     Failover
Vserver      Interface         Node:Port           Policy       Group
---------    ---------------   -----------------   ------------ --------
cluster1     IC1               cluster1-1:e0a      local-only   Default
                                                               Failover Targets:
                                                               .......
             IC2               cluster1-2:e0b      local-only   Default
                                                               Failover Targets:
                                                               .......
cluster1-1   cluster1-1_mgmt1 cluster1-1:e0m     local-only    Default
                                                               Failover Targets:
                                                               .......
```

b. If the failover policy is not set appropriately, modify the failover policy by using the **network interface modify** command with the -failover-policy parameter.

Example

```
cluster1::> network interface modify -vserver cluster1 -lif IC1 -failover-policy local-only
```

Configuring the backup application

After the cluster is configured for NDMP access, you must gather information from the cluster configuration and then configure the rest of the backup process in the backup application.

Step 1. Gather the following information that you configured earlier in Data ONTAP:

- The user name and password that the backup application requires to create the NDMP connection
- The IP addresses of the intercluster LIFs that the backup application requires to connect to the cluster

Step 2. In Data ONTAP, display the aliases that Data ONTAP assigned to each device by using the **storage tape alias show** command.
The aliases are often useful in configuring the backup application.

Example

```
cluster1::> storage tape show -alias

  Device ID: 2a.0
Device Type: tape drive
Description: Hewlett-Packard LTO-5

Node                        Alias     Mapping
--------------------------- --------- ------------------------------
stsw-3220-4a-4b-02          st2        SN[HU19497WVR]
...
```

Step 3. In the backup application, configure the rest of the backup process by using the backup application's documentation.

After you finish

If a data mobility event occurs, such as a volume move or LIF migration, you must be prepared to reinitialize any interrupted backup operations.

Chapter 3. Where to find additional information

Additional documentation is available to further configure tape backup, restore from tape, and configure other types of data protection.

Documentation about tape backup and restore

- Data protection using tape backup

  Describes how to back up and recover data using tape backup and recovery features in clusters, using NDMP, SMTape, and dump technologies.

Documentation on other types of data protection

- Data Protection Power Guide

  Describes how to plan and manage disaster recovery and disk-to-disk backup of clustered systems.

Appendix A. 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.

Appendix B. 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.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

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.

Trademarks