Dell EMC NetWorker Troubleshooting Tool (NTT)

February 2020

H17924.2

User Guide

Abstract

This user guide describes the capabilities of the NetWorker Troubleshooting Tool. It outlines NTT validation procedures and provides information about using the NetWorker Troubleshooting Tool.

Dell EMC Solutions

Copyright

 February 2020 White Paper H17924.2.

Contents

Revisions

Table 1. Revision table

Date	Version	Description
February 2020	1.5.0	• Added NTT on remote host • Version changes
November 2019	1.4.0	• Added new functionality on RMT • Version changes
August 2019	1.3.0	• Additional enhancements on SIGT • Version changes

Executive summary

Dell EMC NetWorker is a backup solution that works predominantly in a computer network environment. Data from the production server is backed up to a backup server over the network. Any problems in the network may disrupt the backup job. The NetWorker Troubleshooting Tool (NTT) is designed to help NetWorker users identify any potential network problems that could adversely affect their NetWorker backup procedures. This document describes various NTT use cases and capabilities and contains instructions for downloading and installing NTT through the user interface.

Audience

This guide is designed for use by:

- NetWorker customers
- NetWorker technical support team
- NetWorker deployment team

NetWorker Troubleshooting Tool (NTT)

NTT can be used in an existing or new NetWorker environment. NTT is packaged with eight tools: NVT, NSRPCHK, NSRGET, NSRDDRCHK, vProxy Health check, SIGT, RMT, and Remote NTT. The following sections describe these tools in detail:

1. Running the NVT—NetWorker Validation Tool – Runs on a live network and provides information about network connectivity between the NetWorker server and its clients.
2. NSRPCHK—NetWorker Proactive Check Tool – Probes the NetWorker Server database for information that is helpful for troubleshooting.
3. NSRGET—Collects and packages NetWorker logs, configuration parameters, and environment data.
4. vProxy Health Check—Provides an automated, efficient, and easily understood first-step, basic self-diagnostic tool for the NetWorker VMware Proxy (NVP) appliance.

5. NSRDDRCHK—NetWorker Cross Check Tool – Allows you to perform cross checks between the NetWorker media database (MMDB) and the Domain mtree contents.
6. SIGT—System Information Gathering Tool – Allows you to log in to a remote host and collect system details.
7. RMT—Resource Monitoring Tool – Collects utilization statistics of system and NetWorker related modules.
8. Remote NTT—The Remote NTT tool is available on the Windows platform and can be used to run NSRPCHK on remote Linux host(s) only.

NVT validations

These validations are initiated by NVT:

1. Host availability on the network
2. DNS resolution
3. Network Time Protocol (NTP) access

Host Availability check

You can install NTT on a NetWorker server, client or storage node. When you initiate validation after entering required information in NTT, the tool generates a 'ping' request from the host on which the tool is installed to all other hosts provided as input. You can select the normal 'ping' or an extended 'ping'. With the extended option, you can provide the MTU size while pinging to each host. The MTU size indicates how many bytes of data can be set up in an IP frame. The default MTU size is 1,500 Bytes, while the jumbo frame size is 9,000 Bytes.

At the end of validation, you can see how many 'ping' requests were successful. The test displays a "success" status if 80% of 'ping' requests receive a reply from the remote hosts.

To make sure NetWorker services are running, NTT uses the `nsrrpcinfo` utility to examine each remote host and provide a status update at the end of validation.

DNS resolution

Host information provided in the NTT UI is validated against the DNS servers provided as input. Because NetWorker requires a host name to IP address resolution (Forward lookup) and IP address to host name resolution (Reverse lookup), the tool validates both resolutions using the `nslookup` command and provides test results in the validation summary.

Network Time Protocol Access

From the host on which NVT is running, NVT initiates the `w32tm` command to access the NTP Server provided as input. The validation summary will contain the NTP server access result: Success or Failure.

Installation Guidelines

Prerequisites

You can install NTT on a 32-bit or 64-bit Windows/Linux Operating System.

Note: The computer system should support English as the default language.

Download Location

You can download the NTT installer from the NetWorker Support Page, by searching for NTT, or from the following direct links:

- NTT 1.5.0 for Linux
- NTT 1.5.0 for Windows

Installation overview

NTT comes as a zip file that you must download to a local host. The .zip file contains the .exe (NTTv1.5.0_Windows.exe for Windows) or .rpm (NTTv1.5.0_Linux.rpm for Linux) file, a user guide, and a checksum file. Steps for installing NTT for each Operating System are provided below.

Which NetWorker tools will be installed?

The following table contains supported operating system, platform and supported Networker version for Dell EMC NetWorker Tools.

Table 2. Supported NetWorker Tools by operating system and version

Operating System	Platform	NetWorker Tools	NTT Version	NetWorker Release Version
CentOS-7 and above	Linux	NVT, NSRPCHK, NSRGET, vProxy HC, NSRDDRCHK, SIGT[1] , and RMT[2]	1.1.0, 1.2.0, 1.3.0, 1.4.0 and 1.5.0	8.x, 9.x,18.x and 19.x
Red Hat (RHEL)–7 and above	Linux	NVT, NSRPCHK, NSRGET, vProxy HC, NSRDDRCHK, SIGT[1] , and RMT[2]	1.1.0, 1.2.0, 1.3.0, 1.4.0 and 1.5.0	
SuSE - 11 and above	Linux	NVT, NSRPCHK, NSRGET, vProxy HC, NSRDDRCHK, SIGT[1] , and RMT[2]	1.1.0, 1.2.0, 1.3.0, 1.4.0 and 1.5.0	
Oracle -7 and above	Linux	NVT, NSRPCHK, NSRGET, vProxy HC, NSRDDRCHK, SIGT[1] , and RMT[2]	1.1.0, 1.2.0, 1.3.0, 1.4.0 and 1.5.0	
Windows 7 and above	Windows	NVT, NSRPCHK, NSRGET, vProxy HC, NSRDDRCHK, SIGT[1] , RMT[2], and Remote NTT[3]	1.1.0, 1.2.0, 1.3.0, 1.4.0 and 1.5.0	

[1] SIGT is supported only on versions 1.3.0, 1.4.0 and 1.5.0.
[2] RMT is supported only on versions 1.4.0 and 1.5.0.
[3] Remote NTT is supported only on version 1.5.0 and can only be launched from a Windows host. The target remote host must be a Linux host.

Installing NTT on MS Windows

This section explains step-by-step instructions for installing NetWorker Troubleshooting Tool Setup.

1. Download the .zip file, unzip the file, and run NTTv1.5.0_Windows.exe. You may be prompted by User Account Control. Select **Yes** to run the file. The NetWorker Troubleshooting Tool Setup opens.
2. The system prompts, “Do you want to allow this app from an unknown publisher to make changes to your device?” Click **Yes** to proceed with the installation.
3. Review the License Agreement and Click **I Agree** to proceed. If you do not want to proceed with the installation, click **Cancel** to stop the installation.

Note: Review the license terms before installing NTT.

---

4. Choose the name of the folder in which to install NTT (the default is recommended) and click **Install**.

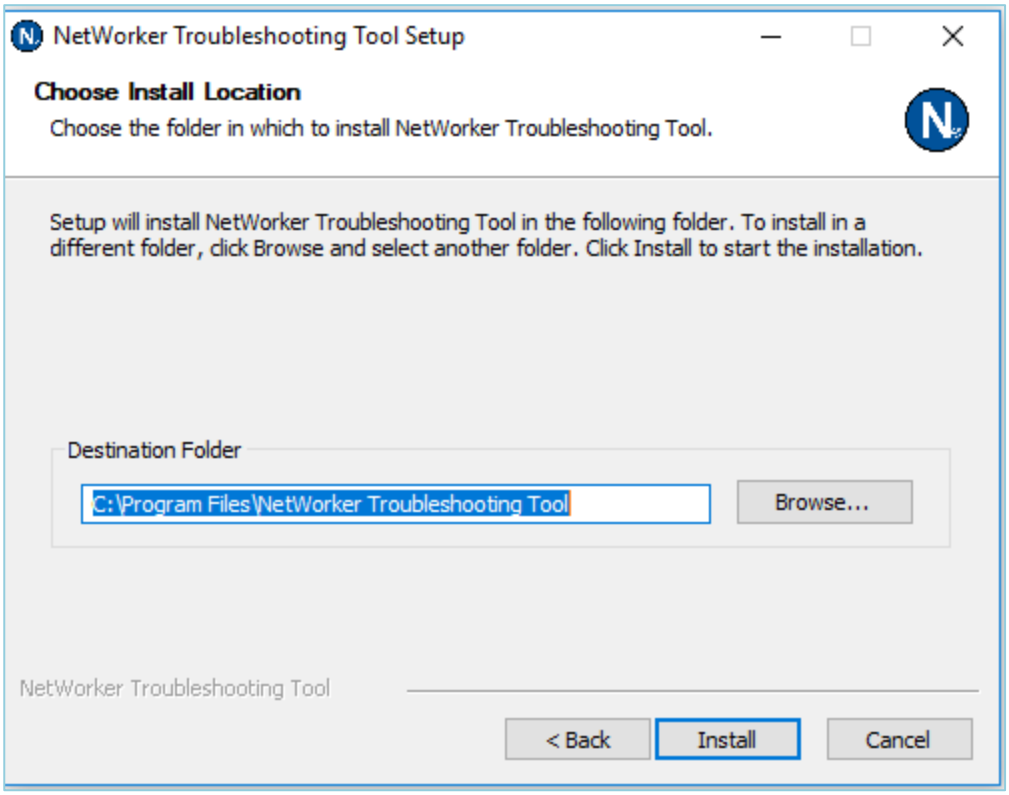

Figure 1. Choose Install Location

5. Click **Finish** to close setup. NTT is now successfully installed.
6. To launch NTT, navigate to **Start Menu→ NetWorker Troubleshooting Tool**.

Installing NTT on Linux

Prerequisites for Linux

Complete these steps before you install NTT on a Linux machine:

1. Start the Linux GUI if necessary and use the GUI to launch the NTT-like GNOME for CentOS, Redhat, SuSE, or Oracle.
2. Set the GUI resolution to '1280x1024'. For CentOS, update the content as highlighted below- File: /etc/systemd/system/vncserver@:1.service

Content

```
[Unit]
Description=Remote desktop service (VNC)
After=syslog.target network.target
[Service]
Type=forking
ExecStartPre=/bin/sh -c '/usr/bin/vncserver -kill
%i > /dev/null 2>&1 || :'
ExecStart=/sbin/runuser -l root -c
"/usr/bin/vncserver %i -geometry 1280x1024"
PIDFile=/root/.vnc/%H%i.pid
ExecStop=/bin/sh -c '/usr/bin/vncserver -kill %i >
/dev/null 2>&1 || :'
[Install]
WantedBy=multi-user.target
```

~

Finding the installed version of NTT

You can check to see if there is a previously installed NTT Tool version from your Linux Machine.

1. Run the command below to retrieve the existing application ID on your Linux machine.

```
rpm -qa ntt\*
```

The NTT installed path in Linux currently defaults to **/opt/NetWorker Troubleshooting Tool/**

Uninstalling NTT (optional)

1. Run the command below to uninstall any older NTT version that might be installed on your Linux machine.

```
rpm -e <application id>
rpm -e ntt-nvt-1.5.0-1.x86_64 (Other Linux machines)
```

Checking dependencies

1. Run the command below to check for dependencies on your Linux machine. Make sure that dependencies are installed before you install NTT.

```
rpm – "qpR" <RPM file name>
For example: rpm -qpR NTTv1.5.0_Linux.rpm
Zypper install NTTv1.5.0_Linux.rpm (SuSE)
```

Installing dependencies (optional)

1. Run the command below to install the dependencies on NTT installation for your Linux machine.

```
sudo yum install <dependency name>
```

Where <dependency name> can be any of these values:

- libnotify
- libappindicator
- libXScrnSaver
- nss

2. Run the commands shown in the figure below on your Linux machine. (Run this command for the first-time installation of NTT only.)

```
For Example:
yum install nss(for Redhat/Oracle/CentOS)
zypper install nss(for SuSE)
```

Note: If you are installing NTT on the Linux platform, you must install the 'nss' package, version 2.2 or later.

Installing NTT on Linux

1. Run the command below to install the NTT program on your Linux machine.

```
rpm –ivh <RPM file name>
For example: rpm –ivh NTTv1.5.0_Linux.rpm
Zypper install NTTv1.5.0_Linux.rpm (SuSE)
```

2. After installation, the NTT will be shown under **Applications → Accessories → NetWorker Troubleshooting Tool**
3. To view the validation results in Excel format, install **libreoffice calc**

Example: Installing NTT on Linux

Here is an example of an installation command to install NTT on a Linux machine:

```
rpm –ivh <RPM file name>
```

For example: `rpm –ivh NTTv1.5.0_Linux.rpm` as shown below.

```
File  Edit  View  Search  Terminal  Help
[root@NVT-POC-vishns2-Centos7ui-03 networker-ui]# rpm -qa ntt\*
ntt-nvt-1.1.0-1.x86_64
[root@NVT-POC-vishns2-Centos7ui-03 networker-ui]# rpm -e ntt-nvt-1.1.0-1.x86_64
[root@NVT-POC-vishns2-Centos7ui-03 networker-ui]# rpm -ivh installers/NTTv1.1.0_Linux.rpm
Preparing...                          ################################# [100%]
Updating / installing...
   1:ntt-nvt-1.1.0-1                  ################################# [100%]
[root@NVT-POC-vishns2-Centos7ui-03 networker-ui]#
```

Figure 2. Installation Command

Installing NTT on SuSE Linux

The following section explains how to install NTT on SuSE Linux.

1. Install the libnotify or libappindicator libraries using the `zypper install libnotify` command, or using the following command for SuSE 12:

   ```
   zypper install
   http://dl.fedoraproject.org/pub/epel/7/x86_64/Packages/l/lib
   appindicator-12.10.0-11.el7.x86_64.rpm
   ```

2. Install NTT with the following command:

   `zypper install NTTv1.5.0_Linux.rpm` or

   `rpm -ivh NTTv1.5.0_Linux.rpm`

   Alternatively, use this command to install NTT on SUSE when there is a 'libXScrnSaver' dependency in SUSE m/c and you are unable to install NTT in the same dependency:

   ```
   sudo zypper install NTT< version>.rpm
   ```

Note: These installation steps are for a host running SuSE SLES 12 SP3 ISO.

Example: Installing NTT on SuSE Linux

Here is an example of an installation command to install NTT on a SuSE Linux machine:

```
zypper install NTTv1.5.0_Linux.rpm or rpm –ivh NTTv1.5.0_Linux.rpm
```

Alternatively, you can use this command for installing NTT on SuSE if there is a 'libXScrnSaver' dependency in SuSE m/c and you cannot install the same dependency:

```
sudo zypper install NTT< version>. rpm
```

Note: The installation steps are for a host running SuSE SLES 12 SP3 ISO.

```
mabel# rpm -ivh NTTv1.2.2_Linux.rpm
error: Failed dependencies:
        libXScrnSaver is needed by ntt-nvt-1.2.2-1.x86_64
mabel#
```

Figure 3. Dependency Issue

```
mabel# ls
NTTv1.2.2_Linux.rpm  NTTv1.2.34_Linux.rpm
mabel# rpm -ivh NTTv1.2.34_Linux.rpm
error: Failed dependencies:
        libXScrnSaver is needed by ntt-nvt-1.2.34-1.x86_64
mabel# zypper install NTTv1.2.34_Linux.rpm
Loading repository data...
Reading installed packages...
Resolving package dependencies...

Problem: nothing provides libXScrnSaver needed by ntt-nvt-1.2.34-1.x86_64
 Solution 1: do not install ntt-nvt-1.2.34-1.x86_64
 Solution 2: break ntt-nvt-1.2.34-1.x86_64 by ignoring some of its dependencies

Choose from above solutions by number or cancel [1/2/c] (c): 2
Resolving dependencies...
Resolving package dependencies...

The following NEW package is going to be installed:
  ntt-nvt

1 new package to install.
Overall download size: 111.3 MiB. Already cached: 0 B  After the operation, additional 393.4 MiB will be used.
Continue? [y/n/? shows all options] (y): y
Retrieving package ntt-nvt-1.2.34-1.x86_64                                                    (1/1), 111.3 MiB (393.4 MiB unpacked)
Checking for file conflicts: ..........................................................................................................[done]
(1/1) Installing: ntt-nvt-1.2.34-1 ....................................................................................................[done]
mabel#
```

Figure 4. Alternate installation command for NTT in SUSE-Linux

Installing NTT on Oracle Linux 7

To install the dependencies for Linux 7 testing follow these steps:

1. Install the libnotify library with the command `yum install libnotify`
2. Add a repository url inside cd /etc/yum.repos.d, by entering this command:

   ```
   wget
   http://yum.oracle.com/repo/OracleLinux/OL7/latest/x86_64
   ```

3. Install libindicator, libdbusmenu and libdbusmenu-gtk2, which are internal dependencies of **libappindicator**:

   a. To install libindicator, type this command:

   ```
   yum install
   https://dl.fedoraproject.org/pub/epel/7/x86_64/Packages/l/li
   bindicator-12.10.1-5.el7.x86_64.rpm
   ```

   b. To install libdbusmenu, type this command:

   ```
   yum install
   https://dl.fedoraproject.org/pub/epel/7/x86_64/Packages/l/li
   bdbusmenu-16.04.0-2.el7.x86_64.rpm
   ```

   c. To install libdbusmenu-gtk2, type this command:

   ```
   yum install
   https://dl.fedoraproject.org/pub/epel/7/x86_64/Packages/l/li
   bdbusmenu-gtk2-16.04.02.el7.x86_64.rpm
   ```

d. To install libappindicator, type this command:

```
yum install
http://dl.fedoraproject.org/pub/epel/7/x86_64/Packages/l/lib
appindicator-12.10.0-11.el7.x86_64.rpm
```

e. Install libXScreenSaver, type this command:

```
yum install
https://yum.oracle.com/repo/OracleLinux/OL7/latest/x86_64/ge
tPackage/libXScrnSaver-1.5.0-6.1.el7.x86_64.rpm
```

f. Install NTT by running `yum install NTTv1.5.0_Linux.rpm` or `rpm -ivh NTTv1.5.0_Linux.rpm`.

Running the NVT Tool

The Network Validation Tool for Networker (NVT) initiates a series of tests on a network. It checks connectivity among various computer systems where Networker will be installed or is already running.

The tool can automatically extract all host details from the NetWorker server's resource database for testing if NTT is installed on the NetWorker Server. To test the environment before installing NetWorker, details for hosts to be tested cannot be auto-discovered; you must enter them manually.

Because NetWorker is a time-dependant and network-reliant application suite, NTP and DNS servers are required for some tests.

Validation performs an array of tests against the provided list of hosts, generating a table summarizing the test results for each host. Use the validation summary results table to detect and resolve environmental problems in your NetWorker data zone.

Run the NTT tool in administrative mode. By default, the tool has been built in administrative mode, but if you do not have administrative privileges, you will need to **Run as Administrator** specifically. To do so, navigate to **Start-> All Programs-> NetWorker Troubleshooting Tool** and then right-click **Run as Administrator.**

Enter data

Provide data to NVT by entering data manually, or by importing a JSON file that was saved earlier from the NVT Validation tab. The JSON file contains hostnames and IP addresses required for validation using NTT. The **Export** button on the Validation page enables you to save this data and create a JSON file.

1. If you are using an existing JSON file, click **Browse**, locate the JSON file, and then click **Open**. The JSON file is uploaded into NVT. Click **NEXT** to continue.
2. If you don't have an existing JSON file, skip this option and click **NEXT** as shown in the following figure.

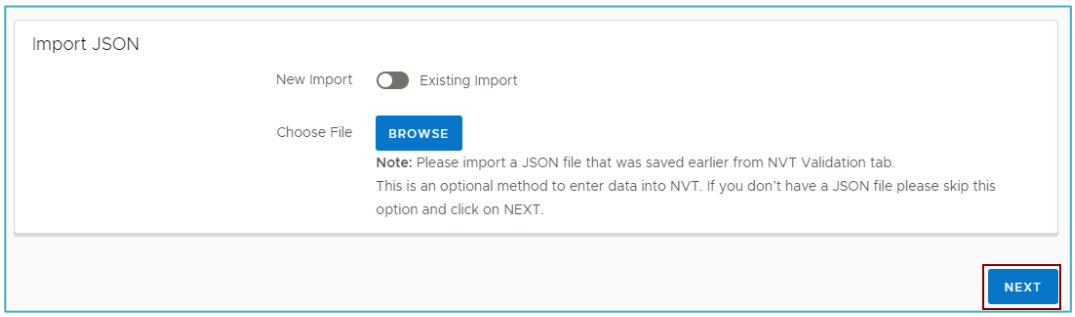

Figure 5. Import JSON

3. If a previously imported JSON file is not found, use **New Import** as shown in the following figure.

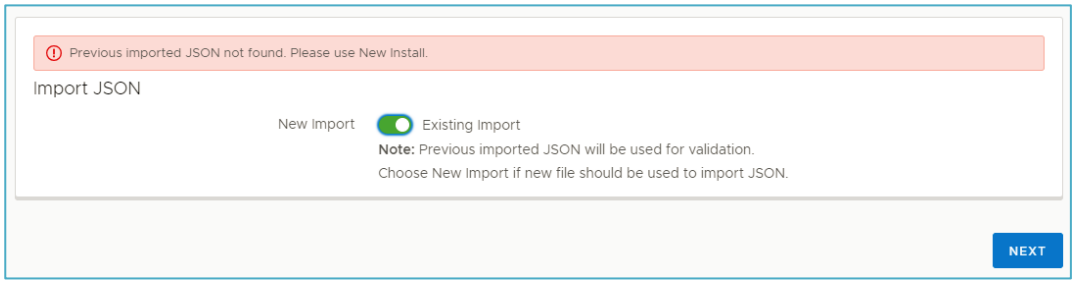

Figure 6. Choose New Import

4. Complete the Site Information, Network Services, and Compute IP Address pages, which guide you through the steps to enter data into NVT:
   a. If you did not use a JSON file, enter all data manually.
   b. If you used a JSON file, edit data or enter missing data, if necessary.
   c. The JSON file populates most, but not all, the fields in the following pages.

Site Information

1. Enter site information in this screen. From the NVT Tool Main Menu, click **Site Information**, as shown in the following figure.

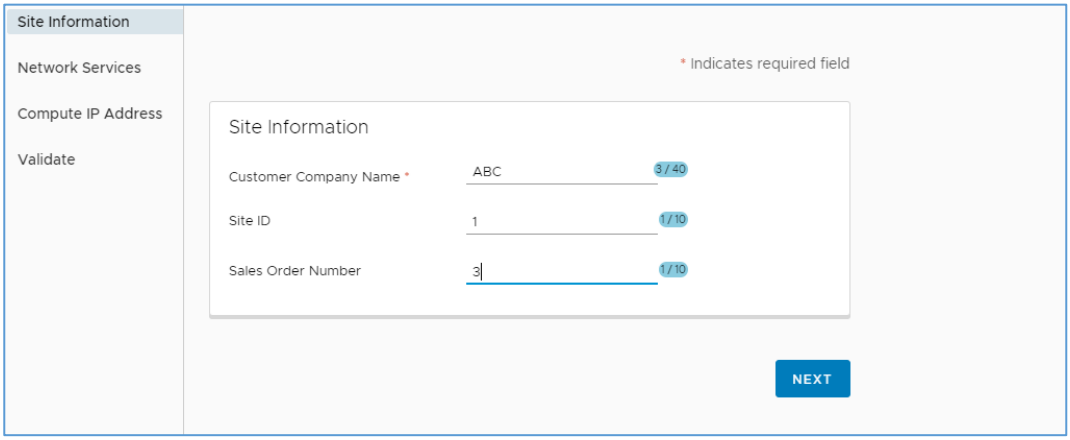

Figure 7. Site Information

2. Enter the customer details that are described in the following table, and then click **Next**.

Table 3. Site information

Field	Description
Customer Company Name	Enter the name of the customer's company.
Site ID	Enter the site ID of the NTT installation.
Sales Order Number	Enter a sales order number, if applicable.

Network Services

1. To identify network services, from the NVT Tool Main Menu, click **Network Services**, as shown in the following figure.

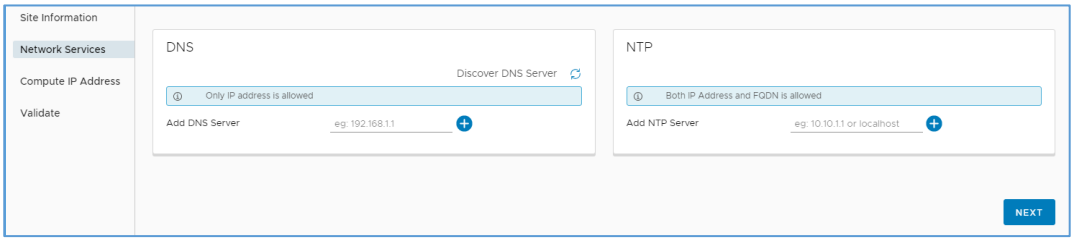

Figure 8. Network Services

2. Enter the DNS and NTP Server details that are described in the following table. Click the plus or minus icons to add or delete DNS and NTP server information.

Table 4. Network services fields

Field	Description
DNS	Enter the IP address of the DNS server. The NetWorker software installed IP address and associated hostname must be registered in the DNS server. NVT sends `nslookup`-equivalent calls to the specified DNS server to verify the NTT IP address and hostname resolution.
NTP	Enter the FQDN or IP address of the NTP Server. The host running NTT must reach the NTP server for time synchronization. NVT sends `w32tm`-equivalent calls to the specified NTP server to verify server accessibility.

NTT validates DNS entries against each DNS server IP address that is provided on this page. NTT attempts to reach the IP address/hostname or FQDN of the NTP Servers and provides status after validation.

3. You can discover the DNS server from the NVT running host as shown in the following figure.

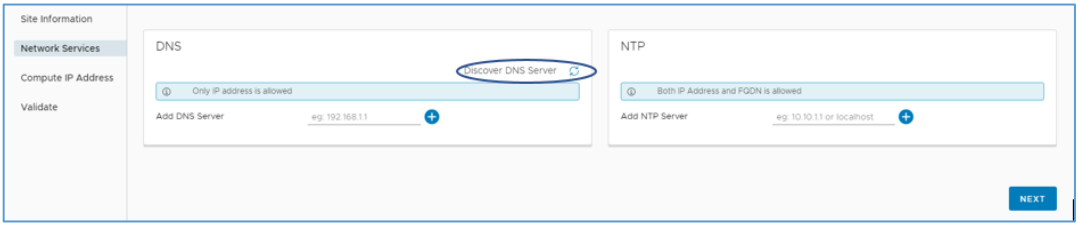

Figure 9. Discover DNS Server

Compute IP Address

1. From the NVT Tool Main Menu, click **Compute IP Address**.
2. Select the existing installation type to retrieve the data automatically from NetWorker DB. Alternatively, you can update the Host FQDN, Host Alias, OS, IP Address, Subnet Mask, Gateway and Host Role fields manually.

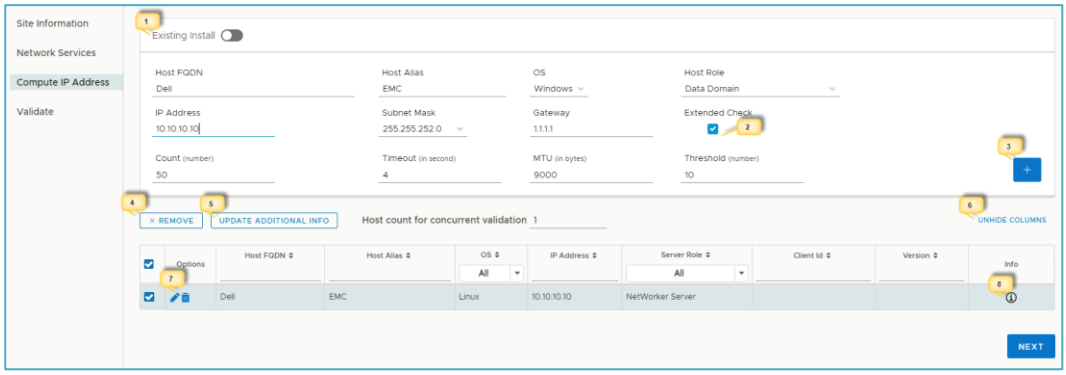

Figure 10. Compute IP Address

The marked points in the above figure listed below:

Table 5. Compute IP Address

Field	Description
Existing Install	Retrieve data automatically (see Figure 11).
Extended Check	This option lets you provide the number of ping requests and a different MTU size during validation, if desired. (See Extended Check Information).
Add (Plus Symbol)	After you have entered the compute IP address, click **Add** (Plus symbol) to retrieve the data. (See Figure 14).
Remove Button	Selected host(s) will be removed from validation.
Update Additional Info	Updates information for multiple nodes. (See Figure 17).
Hide/Unhide columns	Hide/Unhide “**Gateway**” and “**Subnet Mask**” fields.
Edit/Delete	Edit or delete options. (See Figure 18).
Extended Check Info	Enables the Extended Check Info option. (See Figure 19).

3. You can select **Existing Install** to retrieve data automatically, as shown in the following figure.

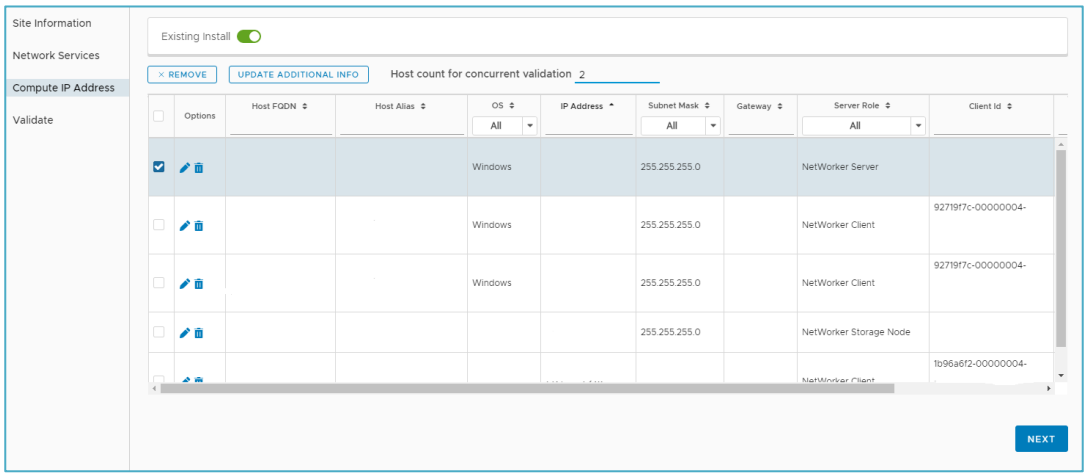

Figure 11. Select existing installation type

Use case 1: Using the NVT tool to validate an existing NetWorker environment

In this use case, an NTT user wants to check the network connectivity and DNS resolution of a set of hosts on which NetWorker is already running. This will be useful before upgrading NetWorker software, or for troubleshooting any backup failures that occur due to network-related issues.

Launch NTT

1. After successful installation, launch NTT from the Windows Start Menu → NetWorker Troubleshooting Tool
2. In the Linux environment, launch NTT from Applications → Accessories → NetWorker Troubleshooting Tool

Select a tool

The NetWorker Troubleshooting Tool home page allows you to select any of the NTT packaged tools including NVT, NSRPCHK, NSRGET, NSRDDRCHK, vProxy Health check, or SIGT.

1. To select a tool, click on the button next to the tool name and click **Next**.

Note: You can only select one tool at a time.

Figure 12. Home Page

Use case 2: Using the NVT tool to perform validation before a new NetWorker Installation

1. To check network connectivity and DNS resolution for a set of hosts before NetWorker is installed, manually enter the host name and IP address details of the hosts in the Compute IP Address page of NTT, as shown below.

   You can save this data from the Validate page using the **Export** option and reload it using the Import page.

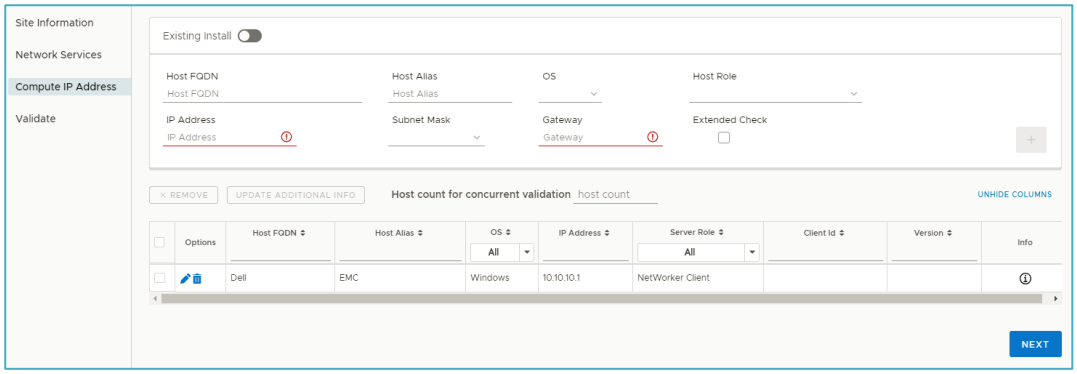

Figure 13. Validation before new NetWorker installation

2. Complete the fields that are described in the following table.

Table 6. Compute IP Address

Component	Description
Host FDQN	A hostname assigned to a host computer.
Host Alias	Host alias name that correspond to existing host records.
OS	Choose Windows or Linux from the drop-down menu.
Host Role	Based on host role, NTT initiates various tests such as ‘nsrrpcinfo’ or ‘telent’ to reach the remote host. This is in addition to the ‘ping’ tests. Select any one of the following host roles from the drop-down menu: ▪ NetWorker Server ▪ NetWorker Storage Node ▪ NetWorker Client ▪ Data Domain ▪ Hypervisor ▪ VMware Proxy (NVP) ▪ VMware Backup Appliance (VBA) ▪ Cloud Boost
IP Address	Enter the IP address of a remote host (NetWorker Server, client, etc.)
Subnet Mask	Select one of the Subnet masks from the dropdown menu. For example, a common subnet mask for an IP address is 255.255.255.0.
Gateway	Enter the default gateway IP address of the remote host.
Extended Check	Extended option allows you to provide additional options such as the number of ping requests or a specific MTU size.

Component	Description
Count (number)	Enter the count number, for example, 50.
Timeout (in second)	Specify the timeout, for example, 4.
MTU (in bytes)	Provide MTU in bytes, for example, 9000.
Threshold(number)	Provide threshold number, for example, 10.

3. After you enter the compute IP address, click **Add (Plus symbol)** to retrieve the data as shown below.

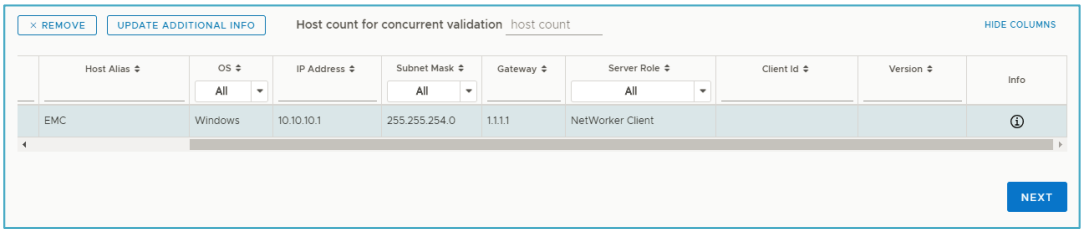

Figure 14. Retrieved Data

4. Complete the fields as described in the following table.

Table 7. Retrieve Data

Component	Description
Remove	Selected host(s) will be removed from validation.
Update Additional Info	Selected host(s) will be updated.
Host count for concurrent validation	Enter the host count for concurrent validation. This is to control the CPU usage of the local host from which NTT initiates validation.
Hide & Unhide Columns	Hide and unhide “Gateway” and “Subnet Mask fields” to make it easier to view and analyze your data.

5. When you click **Next** from Figure 14, the Validation Confirmation Screen is displayed, as shown in the following figure. The validation confirmation workflow allows you to select the number of hosts to initiate validation concurrently. If you run NTT – NVT on too many hosts concurrently, performance may be impacted. If there are many systems in the data zone, to avoid any performance impact, you can change number of hosts for concurrent validation. You can modify the number of hosts for concurrent validation by clicking the **Modify** button and changing the number of hosts in the Compute IP Address screen. Otherwise, Click **Next** to proceed with the validation confirmation workflow.

   Then continue to the Validate function.

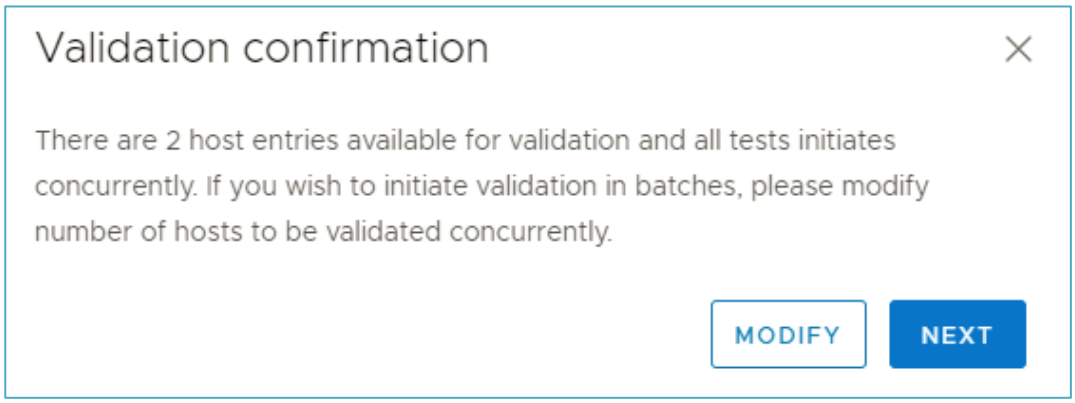

Figure 15. Validation Confirmation

Enabling Extended check

When you click **Update Additional Info** from the Retrieved Data screen and enable **Extended check**, the Extended check info screen appears as shown below.

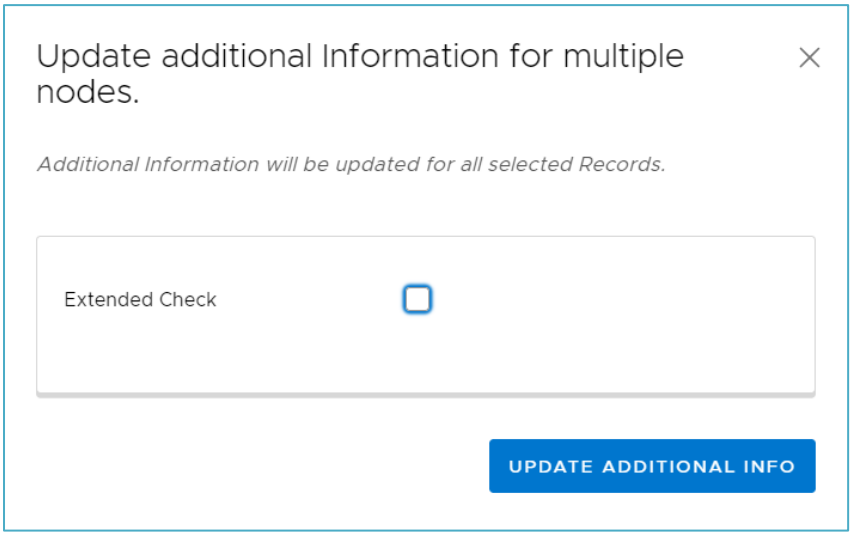

Figure 16. Extended check

1. Enable **Extended Check** by clicking the box. The selected host(s) will be updated as shown below.

Update Additional Information

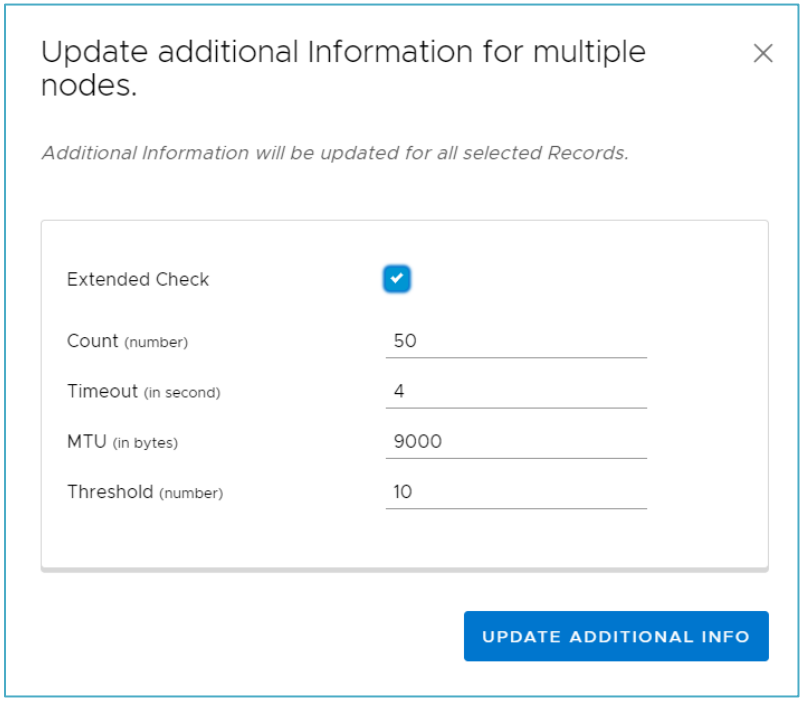

Figure 17. Update additional Information for multiple nodes

The Extended check info option lets you provide additional information during validation. See Figure 10. You can change the number of ping requests and enter a different MTU size.

Editing the compute IP address

1. Click the **Edit** button to edit the Compute IP Address page as shown below

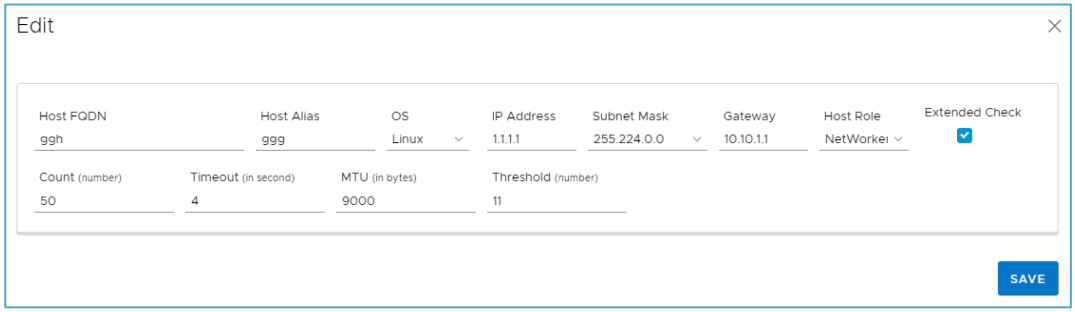

Figure 18. Editing the Compute IP Address page

2. Click **Delete** , to delete the compute IP address.

Extended Check Information

Using the Extended check info option , you can view the figure below.

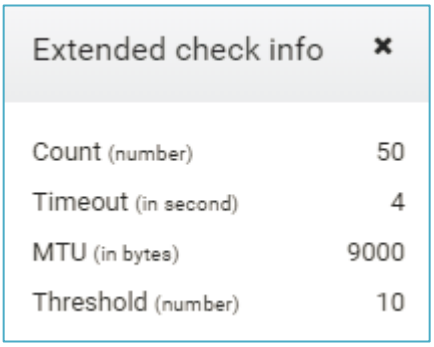

Figure 19. Extended Check info

Validate

Several host entries may be available for validation and all tests will initiate concurrently.

1. Once all fields are complete, from the NVT Tool Main Menu, click **Validate**, as shown in the following figure.

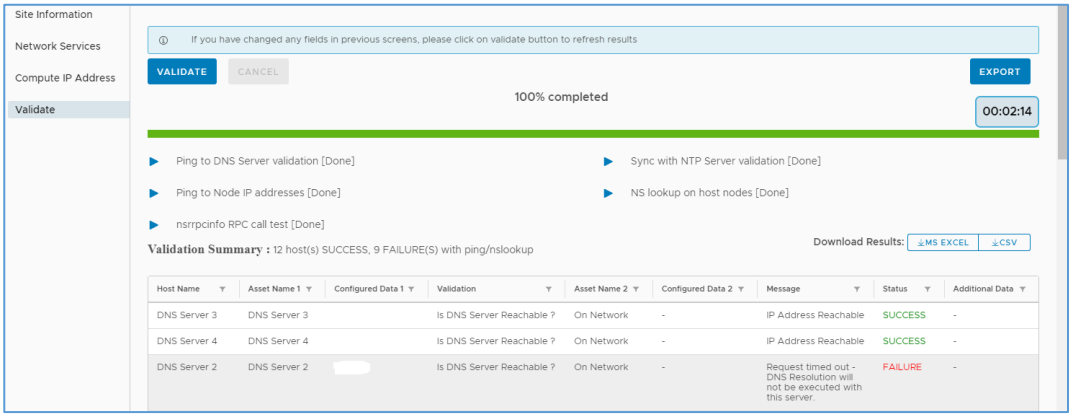

Figure 20. Validate

2. Click a button from the Validate screen:

- **VALIDATE**—Runs the validation. The progress bar displays the percentage of the process that is complete and an estimate of the time remaining.

Note: If you change any fields, click **VALIDATE** to refresh the results.

- **CANCEL**—Cancels the validation process.
- **DOWNLOAD RESULTS—**After validation is complete, generates a report in MS Excel or CSV format.
- **EXPORT**—Saves a JSON file that you can use when you open NTT again.

3. After validation is complete, you can export the configuration details and data from NTT to a .CSV or Excel file: for example, `NTT-Config-v1.0.8_2018-09-25_122137`

NSRPCHK

The NetWorker Server Proactive Check tool (NSRPCHK) is a diagnostic binary check with the following objectives:

- Report brief NetWorker configuration information (the NSRDB).
- Search for the most common NetWorker server problems in Media DB, Client file index, and the daemon log area.
- Automate the time-intensive review of Dell EMC Networker logs.
- Report possible Operating System tuning configuration issues.

The tool is non-invasive (it reads NetWorker server resources). Customers, remote workers, and the Field Support community can run this tool on a daily basis while working on a NetWorker server to help resolve any service requests.

The NSRPCHK tool discovers common error codes quickly and reports them to the end user.

Figure 21. NetWorker Proactive Check Tool

1. To initiate the NetWorker Server Proactive Check tool, select **NSRPCHK** from the NTT home page and click **Next**. The tool requires NetWorker Server to be running on the host.
2. Click **Run NSRPCHK**. In a few minutes the test is complete, and the results are displayed in the UI.

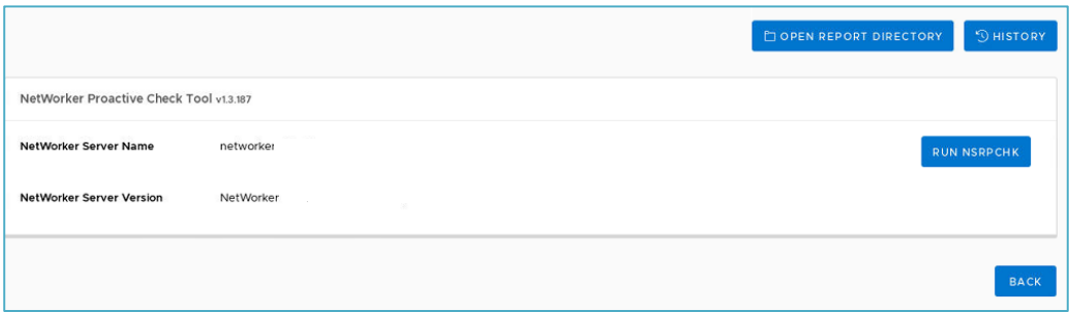

Figure 22. Run NSRPCHK

3. Click **Open Report Directory** to locate previous test results. Share the test result files, as shown in the following figure, with NetWorker Technical Support personnel for use in troubleshooting any NetWorker issues.

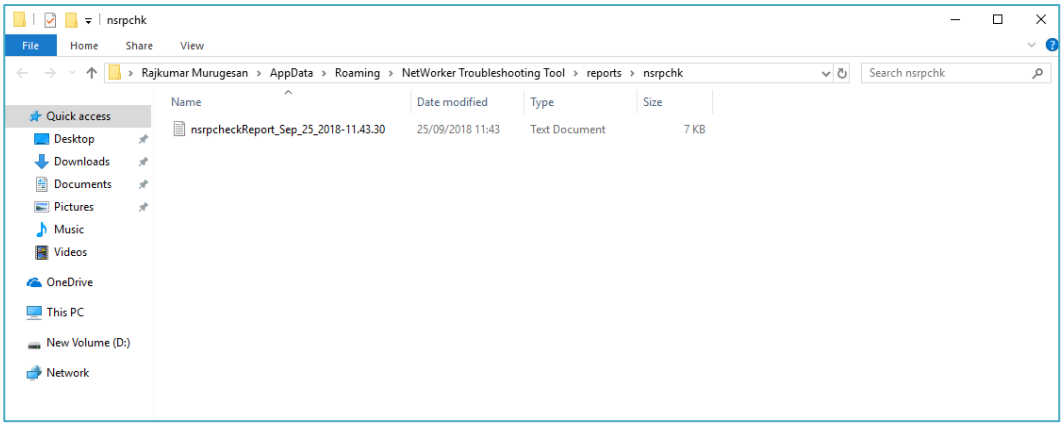

Figure 23. NSRPCHK Report

History: Displaying older NSRPCK reports

1. From the Run NSRPCHK Check Tool screen shown in Figure 22, click **History** to display historical reports.
2. Select a report from the drop-down menu at the top of the screen, as shown below. The last 10 NSRPCHK test results are displayed in the drop-down menu. If you want to display older records, click the **Open Report Directory** Button from the Networker Proactive Check Tool screen shown in Figure 21.

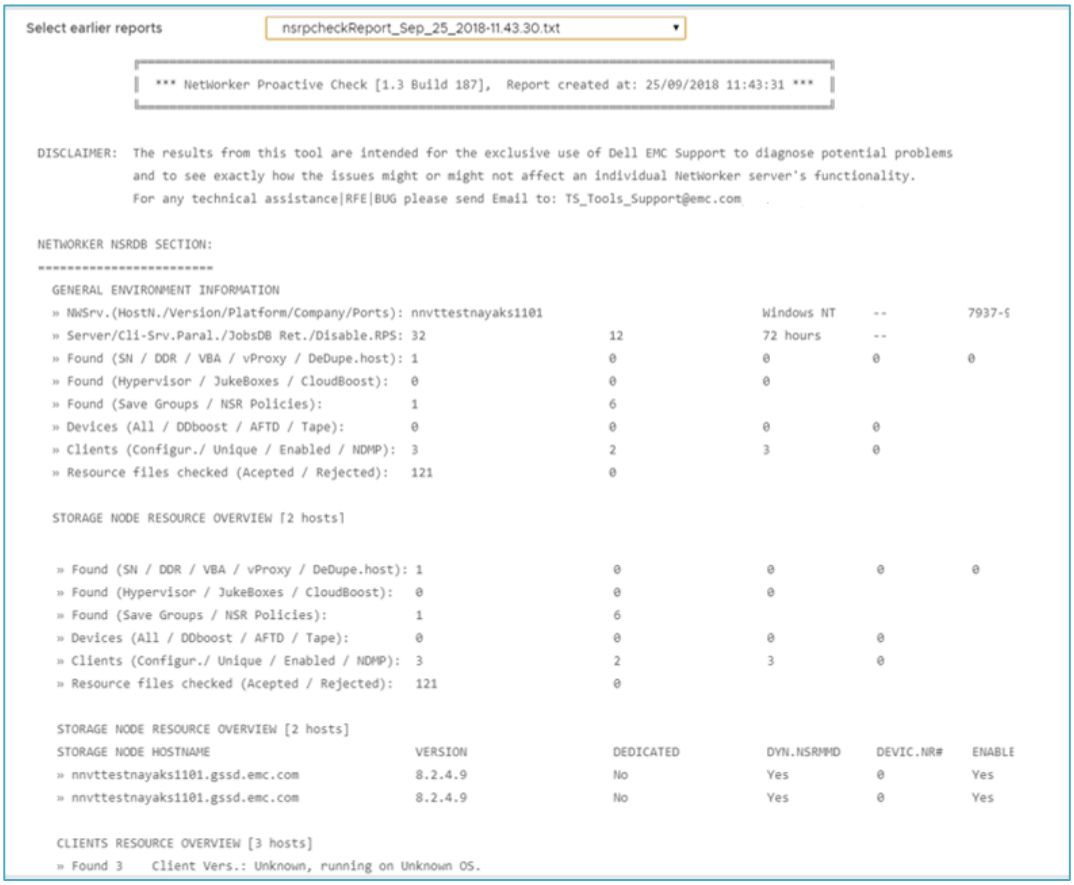

Figure 24. Select earlier reports

NSRGET

The NSRGET Tool collects and packages Networker logs, configuration, and environment data. This utility provides a series of NetWorker and host-specific data collection commands and bundles them for Dell EMC Support. It includes Dell EMC Standard, EMC Reports and EMC Grab Utilities to collect the standard data required for Dell EMC eLab analysis.

1. To start the NSRGET Tool, select **NSRGET** from the NetWorker Troubleshooting Tool home page and click **Next**.
2. On the NSRGET Tool home screen shown below, select the required options for NSRGET and click the **Run NSRGET** button.

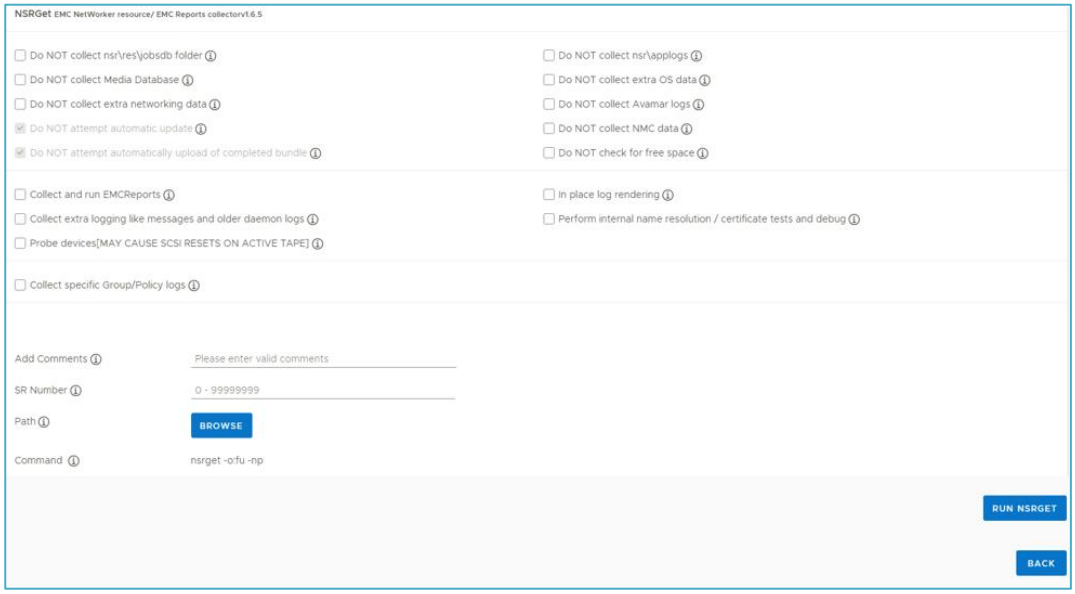

Figure 25. NSRGET

3. Check any applicable boxes next to the fields as described in the following table.

Table 8. NSRGET checkboxes

Field	Description
Do Not collect nsr/res/jobsdb folder	Disable Job Database collection.
Do Not collect mmdb in XDR format	Disable Media Database collection.
Do Not collect extra networking data	Disable networking data collection. **Note:** Some tests may take extra time to complete if name resolution or connectivity is an issue.
Do Not attempt automatic update	Do not attempt to update NSRGet before execution.
Do Not attempt automatically upload of completed bundle	Auto upload: You can use FTP2EMC to upload to support after completion if desired, or simply attach bundle to SR.
Do not collect nsr\applogs	Display Database Module log collection (e.g. NMM, NMDA)

Field	Description
Do Not collect extra OS data	Disable extra OS data collection. Include outputs from tasklist, vssadmin, diskshadow, scquery and gpresult commands as well as registry CurrentControlSet and Policy Keys.
Do Not collect Avamar logs	Disable Avamar module data collection
Do Not collect NMC data	Disable NMC application log and configuration collection.
Do Not check for free space	Override failsafe warning of 10 GB on target drive, 10 GB on target drive. 10 GB free space is recommended to store NSRGET output file. Default path is c:\Dell\util
Collect and run EMCReports	Run EMCReports as part of collection
Collect extra logging like messages and older daemon logs	Collects all daemon logs and other larger logs. Collects all historical daemon. raws. NetWorker messages log file, as well as all savegroup/policy logs, unless specific ones specified below.
Probe devices [MAY CAUSE SCSI RESETS ON ACTIVE TYPE]	Comprehensive device checks may interface with active tape. Runs comprehensive and intrusive tape device testing Active reads or writes may fail on locally attached tape
In place log rendering	Render all logs before collection. This may require additional time and bundle space depending on log size and count.
Perform internal name resolution/certificate tests and debug	This runs a series of extra tests which may take time in a very deep nsr file system or on systems which have networking issues. It includes nsradmin roadmen tests for certificates, nodes and usergroups, as well as nsrclientfix and nsr filesystem permissions collection
Collect specific Group/Policy logs	Collect specific workflow logs

4. Complete the remaining fields as described in the following table.

Table 9. NSRGET fields

Field	Description
Add Comments	Add comments to be included with bundle
SR Number	Enter SR number to ensure data is routed properly, for example `0-99999999`
Path	Browse the path. If needed, change NSRGet bundle output path; default is `c:\Dell\util`
Command	Displays the syntax to run the NSRGet command as specified by the selected options.

5. Click the **Run NSRGet** button. The following screen is displayed.

```
##############################################################################
#   NSRGet 1.6.5 - EMC NetWorker resource / EMCReports collector (Windows)   #
#      Last update: May 2019 - Latest version: ftp://nwc:nwc@ftp.emc.com     #
#      Please submit all requests or problems via EMC NetWorker Support      #
##############################################################################

16:34:23 - Running NSRGet 1.6.5 [-o:funmjzgvoa    -np -s:20190610] @ 2019-06-10_16-34-23
16:34:23 - Prompts disabled - ensure all information supplied
16:34:23 - Options identified as funmjzgvoa
16:34:25 - U option detected: Autoupdate check suppressed
16:34:25 - F Option detected: Autoupload disabled
16:34:25 - Z option detected in funmjzgvoa: Skipping space check
16:34:25 - Finding NetWorker install path...
16:34:26 - NetWorker binary path found in PATH variable
16:34:26 - Setting NSRGet paths...
16:34:26 - Script launched from C:\Program Files\NetWorker Troubleshooting Tool\nsrutilities\nsrget.bat
16:34:26 - Arguments specified: funmjzgvoa
16:34:26 - Proceeding with Service Request: [20190610]
16:34:26 - Collecting basic host information
16:34:43 - Platform detected as Windows 10 R1 Enterprise for x64
16:34:44 - Found .nsrget files - copying to C:\dell\util
16:34:44 - E option not detected in funmjzgvoa: Skipping EMCReports
16:34:45 - NetWorker Server version 8.2.4.9.Build.1416 - server
16:34:45 - Collecting binary versions
16:34:52 - Processing Resource Database
16:34:52 - Collecting Resource Database
16:35:00 - Collecting NSR Local Agent Database
```

Figure 26. NSRGET Output Screen

6. After completion of NSRGET, the output file will be saved in the default location `C:\Dell\util\nsrget` or in a folder that you select by clicking the **Browse** option from the NSRGET home screen.

vProxy Health Check

The vProxy Health Check Utility provides an automated, efficient, and human-readable way to perform first-step/basic self-diagnostics for the NetWorker VMware Proxy (NVP) appliance. This utility helps you find and fix problems related to the status of NVP such as account status, registration, resource usage, connectivity, installation and service state. You can share the results with the NetWorker Technical support team for further investigation.

1. To start the vProxy Health Check utility, select **vProxy Health Check** from the NTT home page and click **Next**.

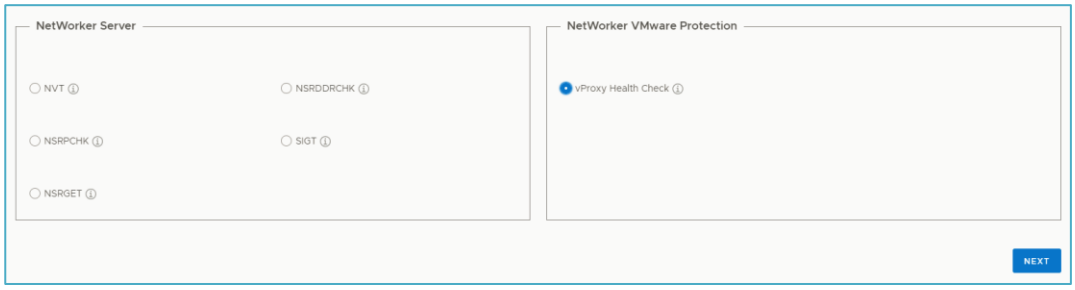

Figure 27. vProxy Health Check

vProxy HC discovered page

A vProxy HC feature discovers the NetWorker server and all vProxy hostnames configured in the NetWorker Server. After discovery, NTT displays the NetWorker server name and all discovered vProxy hostnames.

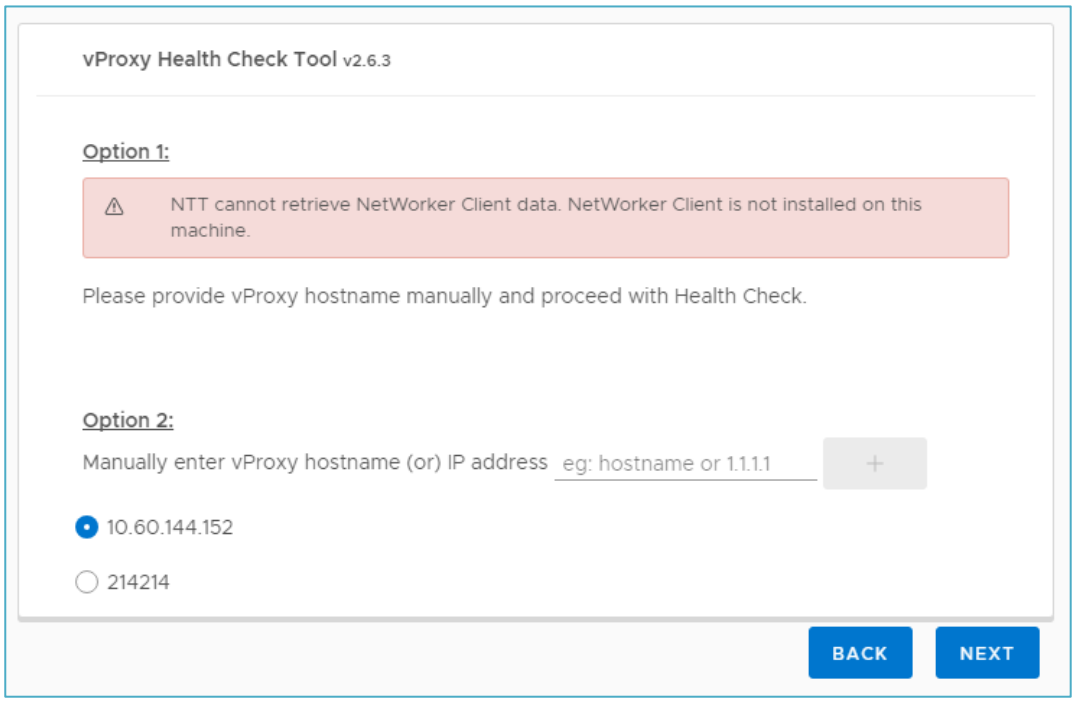

Figure 28. vProxy HC discovered page

When there is any change in the environment, or if you want to rediscover the NetWorker server or any vProxy hosts, close and re-open the NTT application.

If you leave the NTT console open for a long time, there may be changes in the environment such as the addition or removal of a vProxy host. If you run the test again, it will yield an inconsistent result. As shown in the figure above, in this instance NTT cannot retrieve Networker Client data. The NetWorker Client is not installed on this machine. In this instance, you can manually enter the vProxy hostname or IP address and click **Next** to proceed.

The vProxy HC login page appears, as shown below.

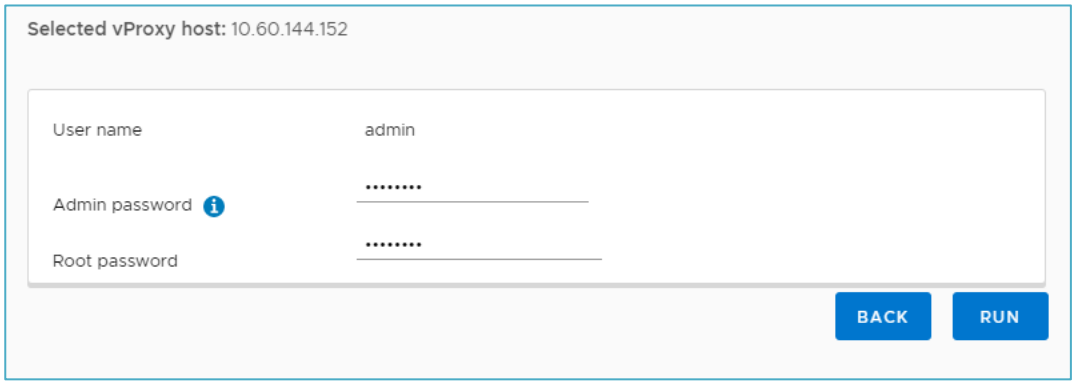

Figure 29. vProxy HC login page

Complete the fields as described in the following table.

Table 10. Selected vProxy host

Field	Description
Username	Provide a username that uniquely identifies someone on a system, for example `Default user name- admin`
Admin Password	Admin password is required for vProxy version 3.0 and above.
Password	Enter the correct password to verify the identity of a user. In the Root password field, enter root account password or the default password. The default password is `changeme`

Note: NVP HC is supported for all Networker tools and utilities. VMware health check vProxy machines support versions 2, 3 and above.

Click **Run** to generate the HC report.

ProxyHC process states

The ProxyHC process states screen shows the vProxy Health check progress through the Authenticate, Copy, Grant permission, Execute, and Collect Report stages.

Figure 30. Stages in generating the HC report

1. Click **Open Log Directory** to open the log directory. Logs are saved in the local system and can be used to troubleshoot errors.
2. Click **Cancel**, to cancel the ProxyHC report.
3. If Proxy HC runs successfully, the vProxy Health Check report screen is displayed, as shown below.

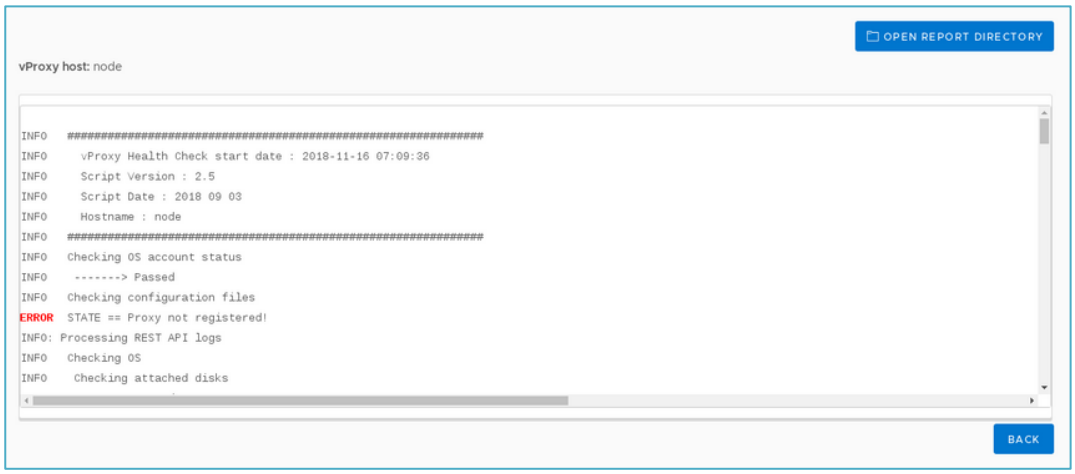

Figure 31. vProxy HC result page

4. Click **Open Report Directory** to open the folder containing the report file.
5. If any error occurs during the ProxyHC process, a message is displayed in a red box as shown below.

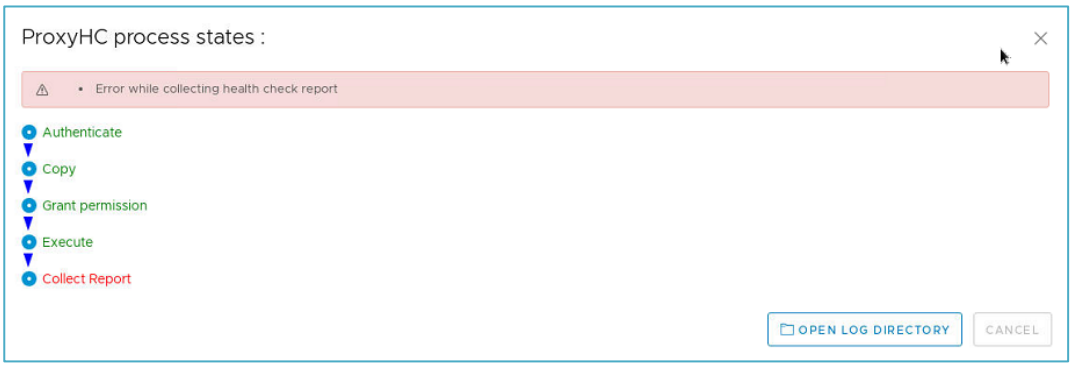

Figure 32. Error in vProxy HC Process

NSRDDRCHK

The NetWorker Cross Check tool (NSRDDRCHK) lets you perform cross checks between the NetWorker Media Management Data Base (MMDB) and the Domain mtree contents. The NSRDDRCHK tool is supported by the following platforms.

- Linux (CentOS, RHEL, SLES), 64-bit
- Windows (2008, 2012, 2016), 64-bit

The NSRDDRCHK tool generates outputs from the NetWorker `mminfo` command and from the Data Domain `sfsdump` command. It then builds a list containing the Save Set IDs (SSIDs) recorded in the NetWorker Media Management Data Base. The list contains the names of the files and directories located on the NetWorker related mtrees on the Data Domain Restorers (DDRs). NSRDDRCHK compares the outputs line by line and provides a report containing the unique records.

This tool enables Data Domain and NetWorker customers to identify and confirm any mismatches between backup savesets managed by NetWorker and those stored in the Data Domain NetWorker LSU. This lets you determine if there are any problems related to unmanaged savesets, leftover/orphans savesets, Data Domain capacity issues, etc.

Note: If NetWorker Client is not installed on this machine, NTT cannot retrieve NetWorker Client data.

---

1. To start the NSRDDRCHK tool, from the NetWorker Server home page, click on the button next to the tool name and click **Next**.

Figure 33. NTT Home Page

2. The NSRDDR Check Tool screen appears, as shown below.

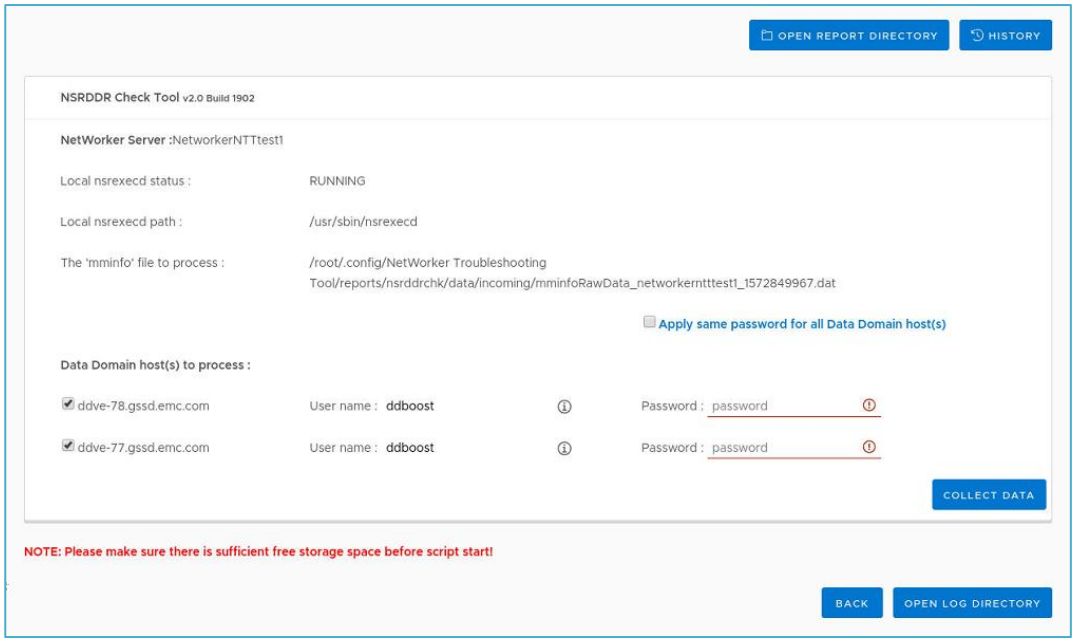

Figure 34. NSRDDR Check Tool screen

3. In **Data Domain host(s) to process**, select the DDR hosts to be processed and enter the passwords associated with the displayed user names.

   If you check **Apply same password for all Data Domain host(s)** and enter a password, it applies that same password for all DDR hosts.

   Note: Make sure there is enough free storage space before you click **Collect Data**.

4. Click **Collect Data** to begin collecting data from the remote Data Domain system. Collection progress is displayed as shown below.

Figure 35. NSRDDRCHK Collect Data

Successful NSRDDRCHK collection results

After a successful login to Data Domain, NSRDDRCHK initiates the required data collection. At the end of the data collection, NSRDDRCHK provides an option to start analyzing the collected data.

1. Once you see the successful data collection completion message, you can open the log directory, as shown below.

Figure 36. NSRDDRCHK Successful Collect Data Result

Accessing previous NSRDDRCHK reports

1. From the NSRDDR Check Tool screen (Figure 34), click **Open Report Directory** to display previous reports in a folder as shown below:

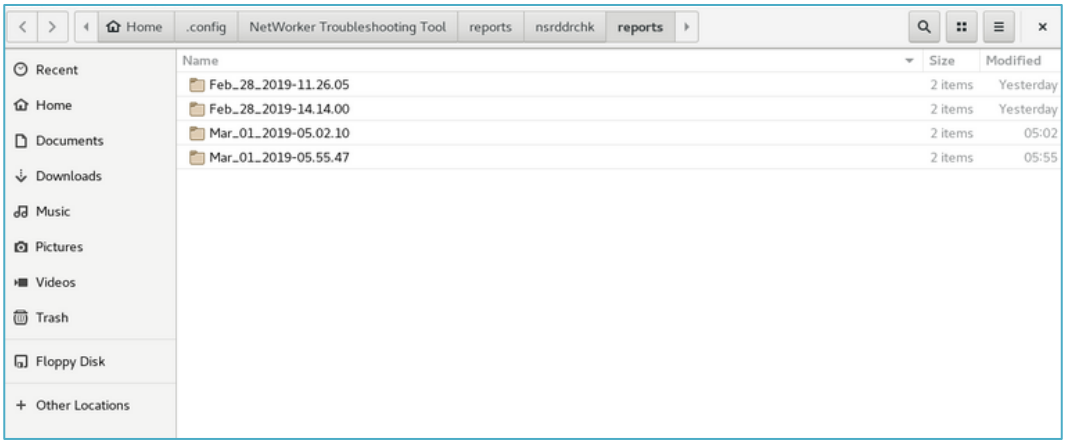

Figure 37. Report Directory window

2. From the NSRDDR Check Tool screen (Figure 34), click **History** to display a list of earlier NSRDDRCHK reports as shown below. Select a historical report from the list and it will be displayed in a separate window.

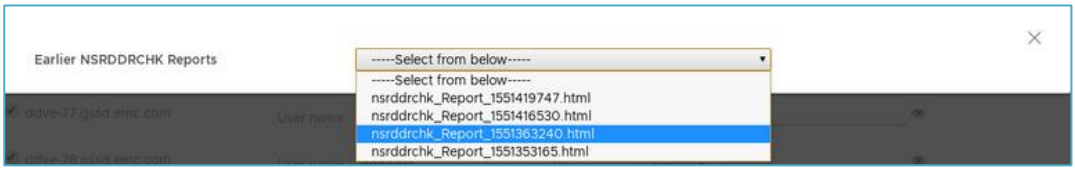

Figure 38. Earlier NSRDDRCHK Reports

Unsuccessful NSRDDRCHK collection results

1. If the data was not successfully collected, an error message is displayed, as shown below. Configure the parameters for analysis by checking the box(es) next to the parameter(s) listed, complete any required fields as described in the table below.

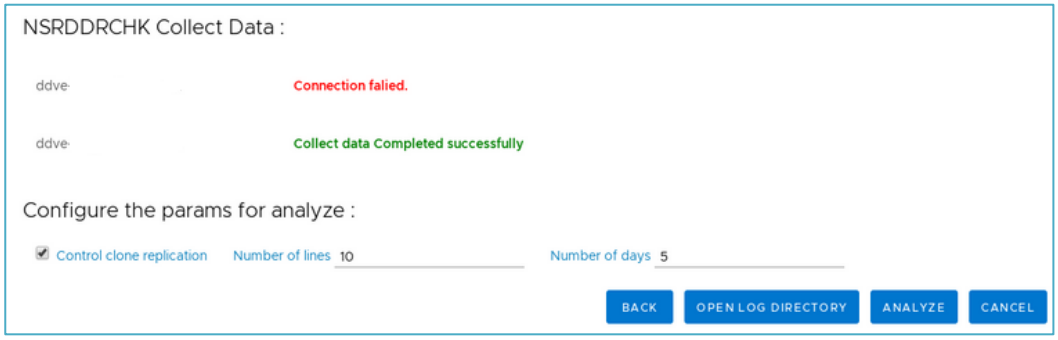

Figure 39. Unsuccessful NSRDDCHK results and analysis parameters

Table 11. Configure parameters for analysis

Field	Description
Control Clone replication	Enable ‘control clone replication’
Number of Lines	Enter the value between 10 to 1000. Default is 10
Number of days	Provide an approximation of the number of days

2. Click **Analyze** to generate the NSRDDRCHK analysis report in a separate window as shown below.

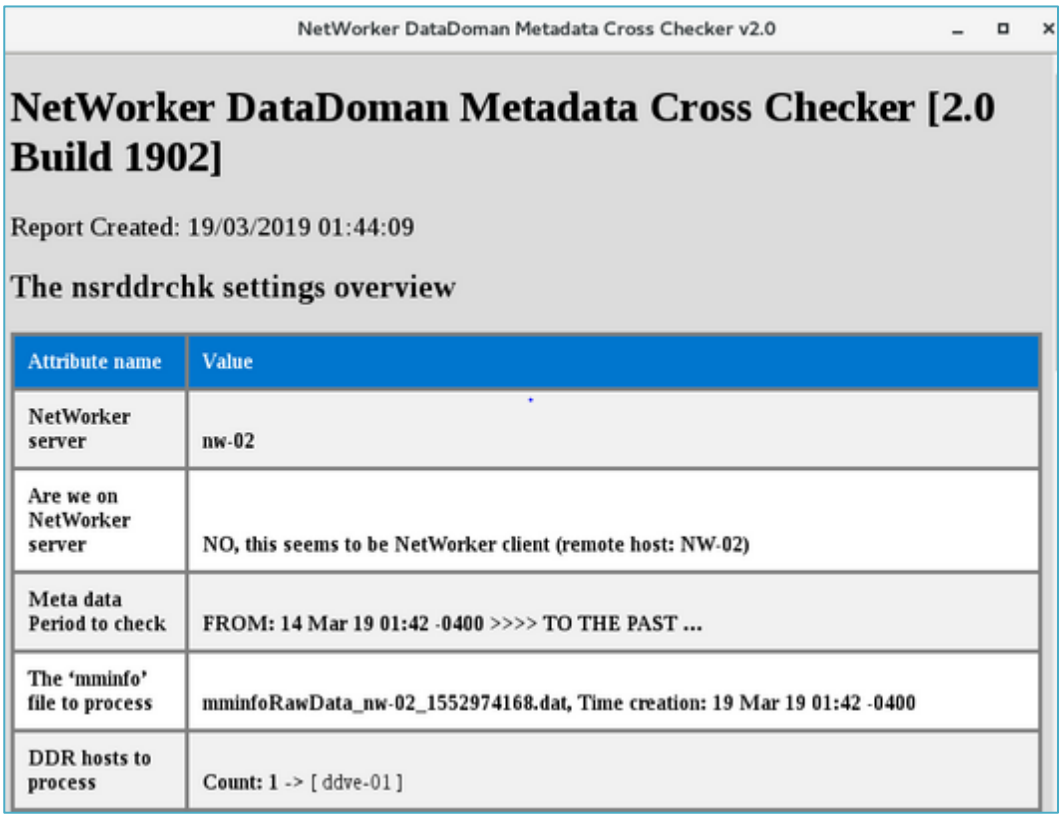

Figure 40. NSRDDRCHK analysis report

Open Log Directory

Logs are saved in the local system. These logs can be used for troubleshooting in case of errors. To open the log directory, click the **Open Log Directory** button from any of the preceding screens.

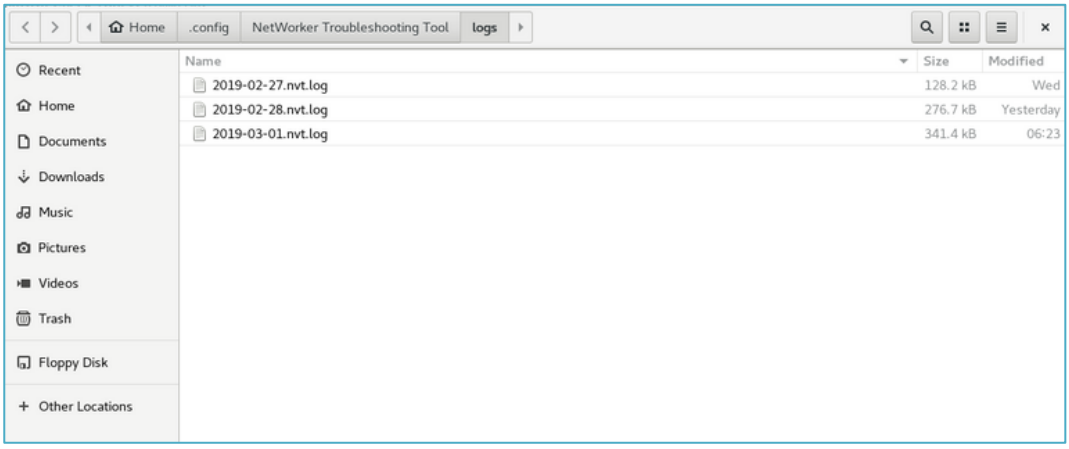

Figure 41. Log Directory Window

SIGT

System Information Gathering Tool (SIGT) lets you log in to a remote host and collect system details. SIGT can query a remote host to collect information about installed software and platform-related information. The tool internally uses WMI calls for Windows, and Linux native commands for Linux hosts, to collect the system information.

Prerequisites

The tool works for following platforms.

Table 12. Prerequisites

Source	Destination	Prerequisite
Windows	Windows	WMI on current host
Linux	Windows	Not Supported
Windows	Linux	ssh enabled (default)
Linux	Linux	ssh enabled (default)

Note: Remote connections in WMI are affected by the Windows Firewall and DCOM settings.

1. To use the SIGT tool, check the button next to SIGT from the NTT home screen, as shown below, and click **Next**.

Figure 42. SIGT Selection Page

2. The System Information Gathering Tool screen appears, as shown below:

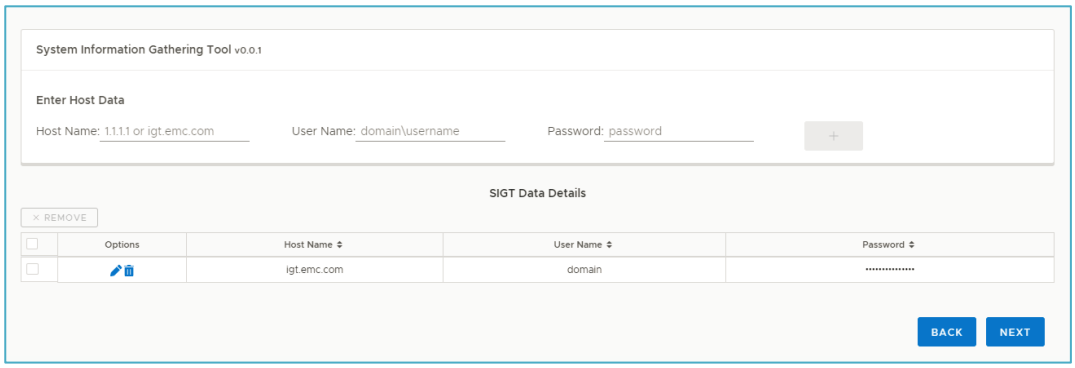

Figure 43. SIGT Data Details

3. Enter the host data details as described in the following table and click **Next**.

Table 13. Host Data Information

Field	Description
Host Name	Enter the hostname or IP address. For example, igt.emc.com as hostname and IP address as 1.1.1.1
User Name	Provide an administrative username that uniquely identifies someone on a system
Password	Enter the correct password to verify the identity of a user.

4. In the System Information Gathering Tool screen (Figure 43), if you click **REMOVE**, all host(s) will be removed.
5. **Options:** You can click the pencil icon to edit the SIGT data details. The Edit screen appears as shown below. Change the details as needed and click **Save** to save them.

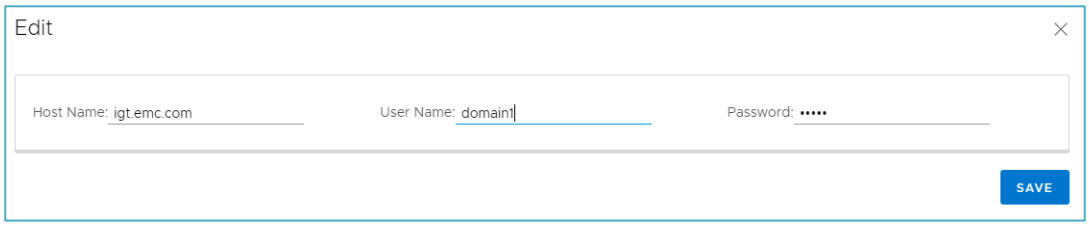

Figure 44. Edit Window

6. In the System Information Gathering screen under **Options**, you can click the trash can icon to remove individual host information.
7. When you click **Next** from the System Information Gathering screen, the retrieved Host Scan Information is displayed, as shown below.

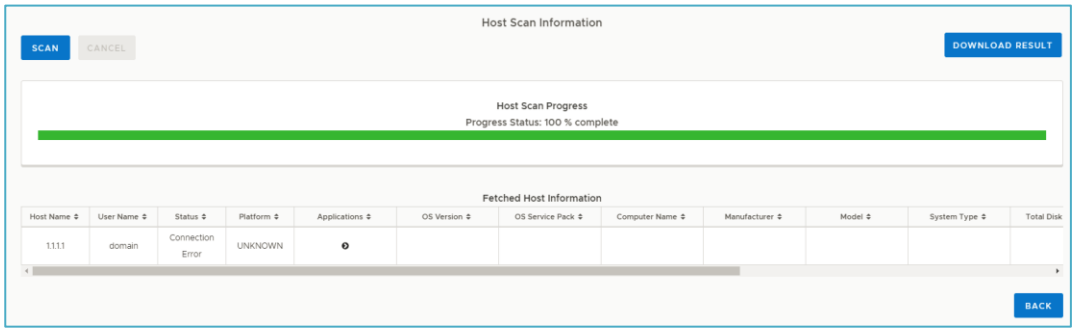

Figure 45. Host Scan Progress

The green status bar shows the progress of the information being retrieved.

- **SCAN**—Starts the Host Scan Progress.
- **CANCEL**—Cancels the Host Scan progress.
- **BACK**—Returns to the previously viewed page.
- **DOWNLOAD RESULTS**—Generates a report of the Host Scan results in Excel format.

RMT

The Resource Monitoring Tool (RMT) collects utilization statistics of system and NetWorker related modules.

Description

RMT assists with NetWorker performance problem troubleshooting by capturing requested environment details about the machine on which it is running. The tool captures details about machine resource utilization such as CPU, Memory, I/O, and network operation. RMT captures the NetWorker process memory and CPU utilization, as well as NetWorker daemon response time.

Prerequisites

On a Linux machine, the RMT tool script requires "iostat" and "sar" utilities for capturing the I/O information. If these utilities are not available, RMT will not capture the I/O details.

The script captures the "pstack" output for NetWorker critical daemons for the Linux machine. If the pstack process is not available, RMT will not capture the process stack but it will still collect details about other processes.

Ensure that you have enough disk space to run the script. The disk space requirement depends on how many days the script is continuously running, and on the interval time that is specified to capture the resource details.

If you are capturing the resource details for a longer duration, make sure that the large interval is selected in the NTT – RMT GUI. The script will immediately begin capturing as many details as possible and may fill the available disk space before it is able to finish.

Detailed overview of RMT tool

You can use the RMT tool to capture information about any process. The tool will parse the collected details for these processes and generate a ".tsv" file which you can export into a MS Excel file to create graphs.

Note: The RMT tool captures overall system CPU and memory as well as per-process CPU and memory for all processes.

The NTT - RMT GUI features an “interval” parameter in which you must provide the appropriate interval value for capturing the results. For example, if you specify a 60 second interval, RMT will capture all required details once every sixty seconds.

The RMT tool captures following useful information:

- Environment details on the machine where it is running, including CPU speed, number of CPUs, CPU arch, OS details, ulimit details, memory information, and system bus info.
- The memory and CPU utilization details reported are for the processes that are selected from the UI.

Note: For Windows, the RMT tool creates a Perf counter automatically and captures CPU and memory utilization details for the processes listed in NTT – RMT GUI and for the overall system.

- Overall system CPU and memory utilization

- Disk I/O statistics using the iostat command
- IOPS details for all the configured disks

Note: IOPS are captured based on the interval specified in the NTT – RMT GUI

- TCP LISTEN, WAIT, ESTABLISHED etc. for all TCP connections
- Summary statistics for each network protocol such as TCP, IP for inte4 and inte6.
- Overall number of "NetWorker" sessions running on NW server.
- If the machine on which the tool is running is the NetWorker server, then the RMT tool captures the daemon response time for networker key daemons such as nsrexecd, nsrd, nsrjobd, nsrindex and nsrmmdbd.

  If the response time for any of the critical daemon is >60 seconds, the tool captures the "pstack" details for that daemon during that time. See Prerequisites for pstack requirements.
- All *.tsv files provide resource utilization details that you can export directly to MS Excel file for plotting graphs.

Current limitations of RMT tool

The following limitations exist for the RMT tool at the time of publication:

- If there is no "pstack" command, then script will not capture the pstack output for daemons.
- Network utilization is currently captured only for Linux.
- The tool runs on Windows 2008 and newer versions,

Starting the RMT tool

1. To start the RMT Tool, select **RMT** from the NetWorker Troubleshooting Tool home page and click **Next,** as shown below.

Figure 46. NetWorker Troubleshooting Tool Home Page

RMT Data Collection

RMT performs two functions:

- Process Performance Monitoring, which monitors process performance
- Daemon Response (nsrwatch), which checks daemon latency

RMT for Windows

1. On the RMT Tool home screen shown below, select the required options for process performance monitoring.

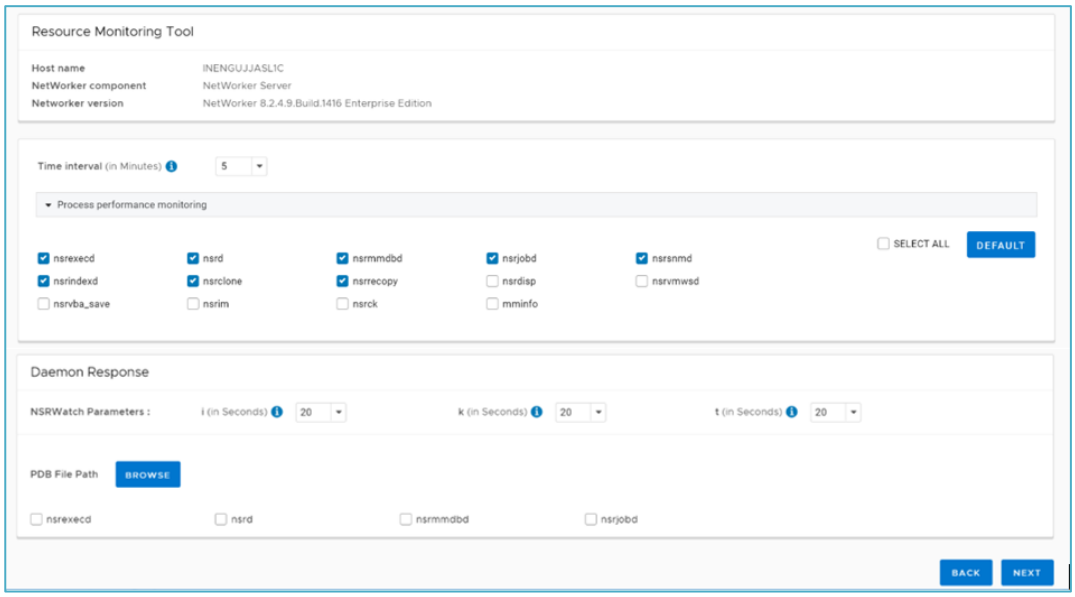

Figure 47. RMT Home Screen

The process performance monitoring details are described in the following table:

Table 14. RMT performance monitoring details

Field	Description
Host Name	Default hostname is auto populated. For example, NetWorker NTT test1
NetWorker Component	Default Networker Component is displayed like Networker Server, Networker Client etc.
NetWorker Version	If NetWorker Version is available, it will be displayed
Time Interval (in Minutes)	Choose a numeric value between 5 and 60 from the drop-down menu
Process performance monitoring	DEFAULT: only default process performance parameters are monitored. SELECT ALL: all performance monitoring parameters can be selected or deselected at once, or individually.
Daemon Process, NSRWatch parameters	Select one of the daemon processes (Nsrwatch i, Nsrwatch k, or Nsrwatch t). Then select an interval (10, 20, or 30 seconds) from the drop-down menu

Field	Description
PDB File Path	On a Windows machine, if you have a PDB file and need to select the required NSR modules manually, you will be prompted to provide the PDB file path. Browse and provide the path where the PDB files are located on your machine.

Note: On a Windows machine, the networker related PDB file (not Operating system file) is mandatory for running nsrwatch.

2. After you enter the performance monitoring and daemon details and click **START** from the RMT home screen, the following screen appears.

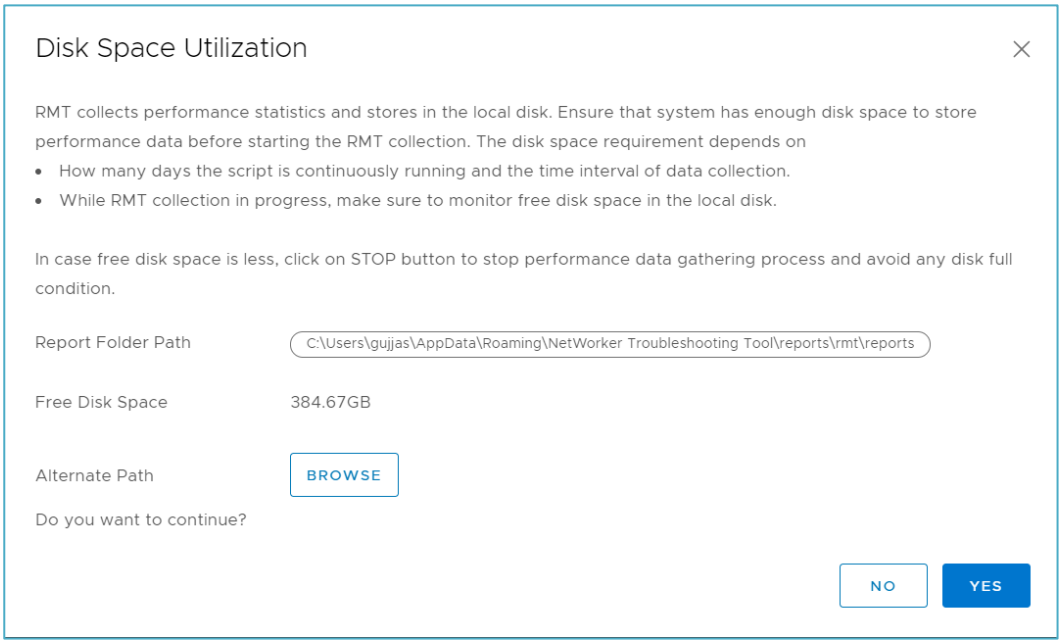

Figure 48. Disk Space Utilization Pop-up window

3. Read through disk space utilization and click **Yes**, as shown in the following figure, to continue using the tool for data collections.

   In Figure 47, daemon response details are not selected. Therefore, the errors occur during the RMT machine details collection process and a message is displayed in red as shown below.

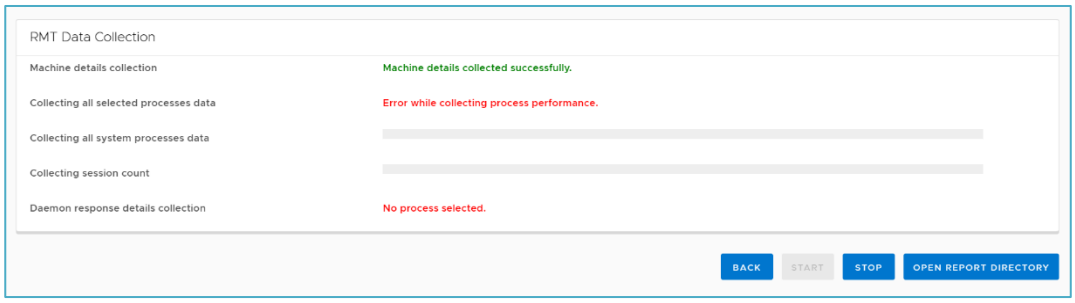

Figure 49. RMT Data Collection Error Message

4. After you enter the performance monitoring and daemon details and click **START** from the RMT home screen, the following screen appears.

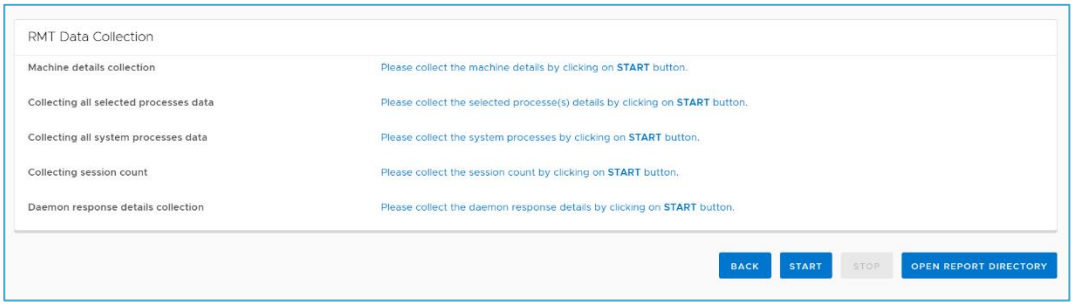

Figure 50. RMT Data Collection Successful message

Back—Click **Back** to return to the RMT Home Screen.

Start—Click **Start** to collect the machine(m/c) details

Stop—Click **Stop** to stop the collection of machine details when the collection is in progress.

5. **Open Report Directory**—Click **Open Report Directory** to open the folder containing the report files. This is an active feature which allows you to view and report details while data collection is in process.
6. If for any reason you click **STOP** during the collection process, the following screen is displayed:

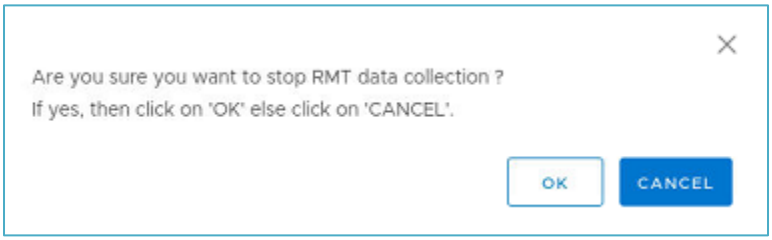

Figure 51. STOP RMT Data Collection

7. Click **OK** to stop the RMT data collection. If you want to continue with RMT data collection, click **Cancel**
8. Click **Open Report Directory** to locate previous test results/reports in a folder as shown below.

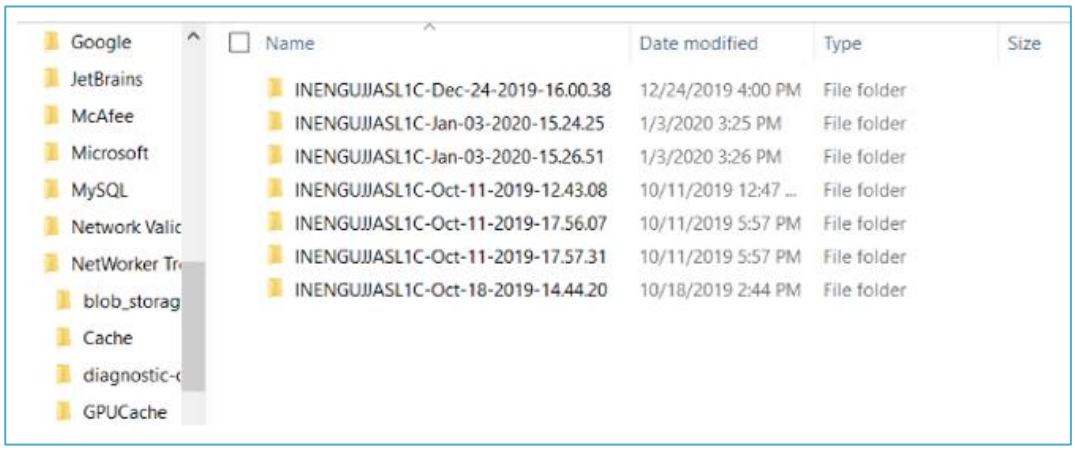

Figure 52. Open Report Directory

RMT for Linux

The process performance monitoring and daemon response details are shown in the following figure:

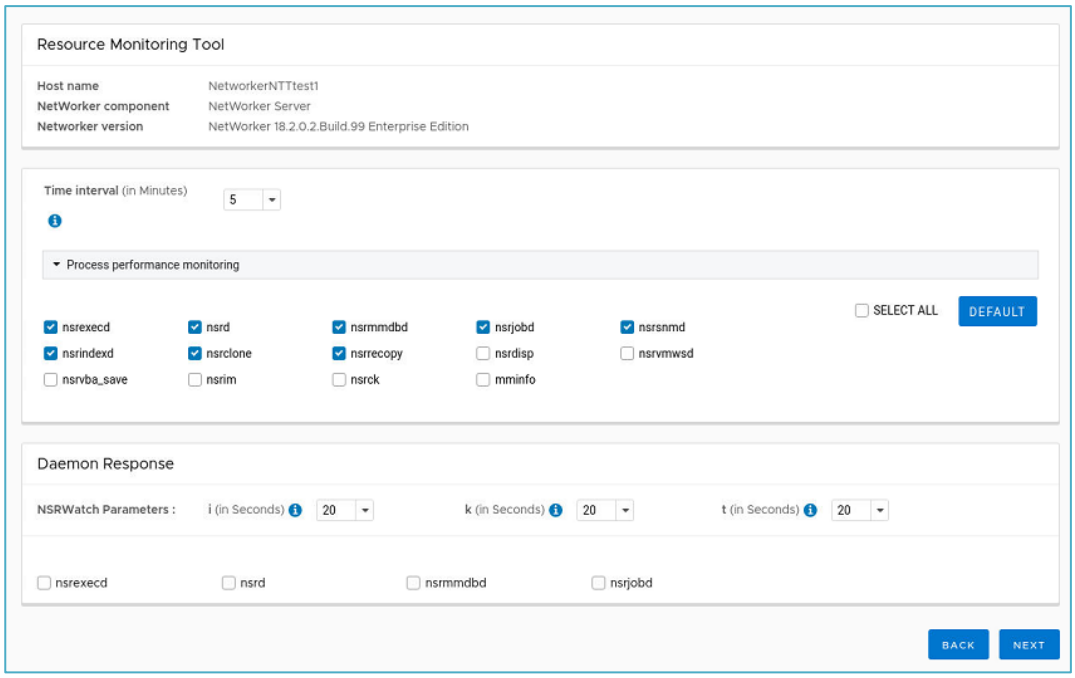

Figure 53. RMT Home Screen

1. After you enter the performance monitoring details and click **Next** from the RMT home screen, the following screen appears, confirming the host scan details you intend to collect.

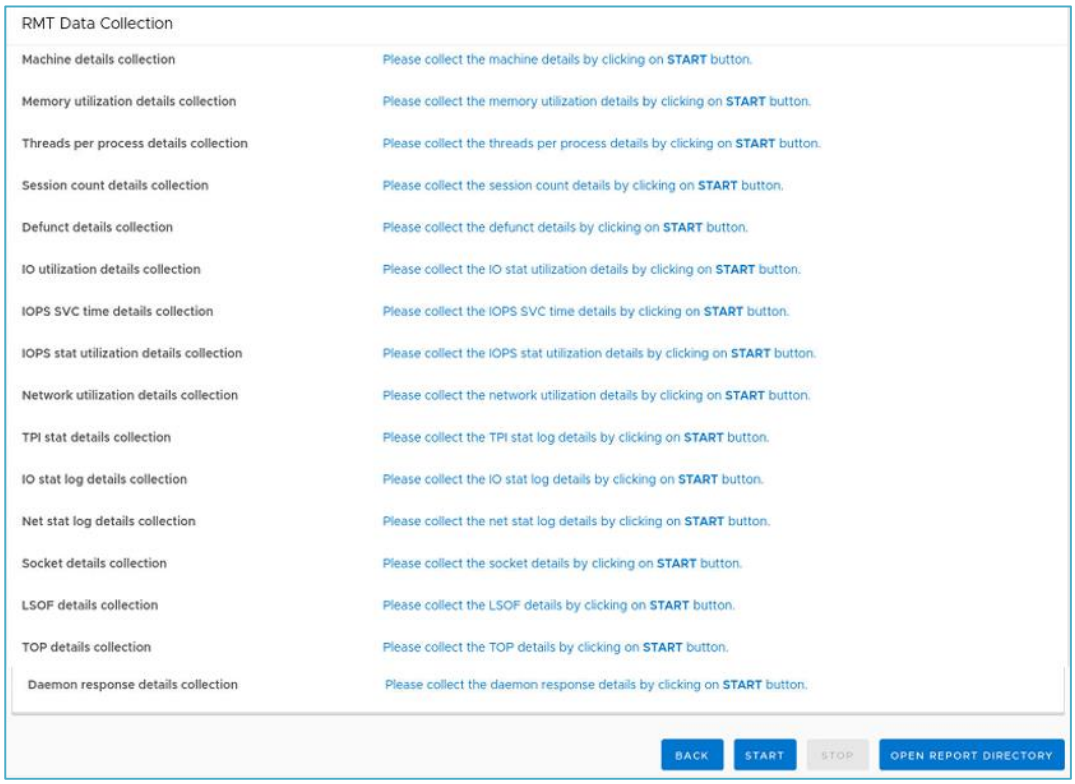

Figure 54. RMT Data Collection: Host scan information confirmation screen

2. Click **START**. The following screen appears.

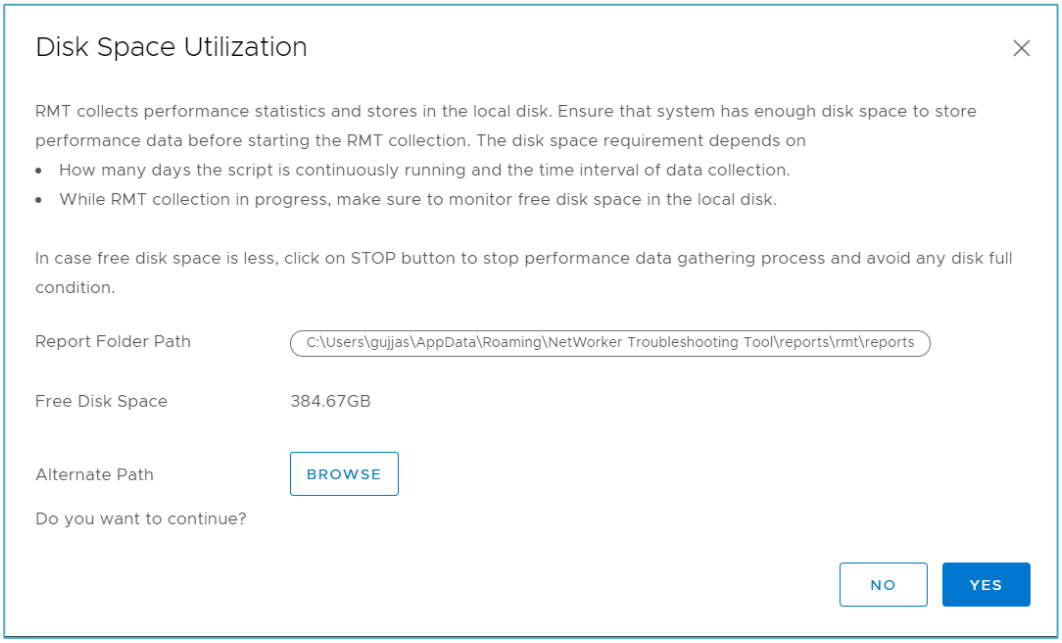

Figure 55. Disk Space Utilization Pop-up window

3. Review the disk space utilization information and click **Yes** to begin collecting the machine (m/c) details as shown in the following figure.

Figure 56. RMT machine details collection status window

4. The blue status bars indicate the progress of the machine details collection process.
5. If for any reason you click **STOP** during the collection process, the following screen is displayed:

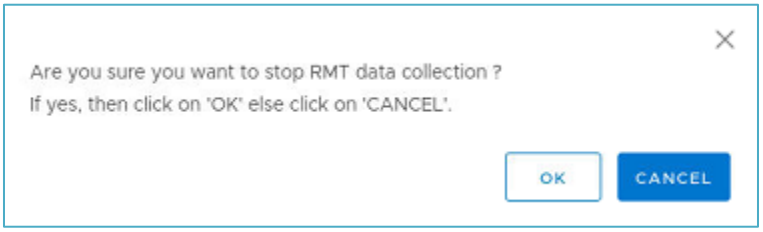

Figure 57. STOP RMT Data Collection

6. Click **OK** to stop the RMT data collection. If you want to continue with RMT data collection, click **Cancel**

If any errors occur during the RMT machine details collection process, a message is displayed in red as shown below.

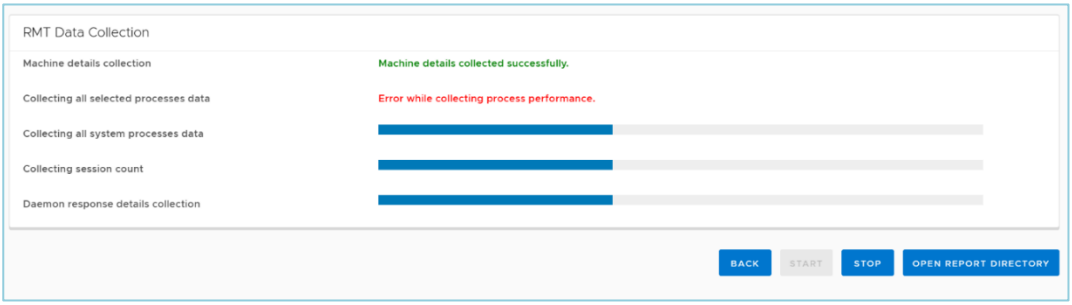

Figure 58. RMT Data Collection Error Message

The other remaining data collection processes continue despite the one that has stopped with an error message. Successfully completed details collection results are shown below.

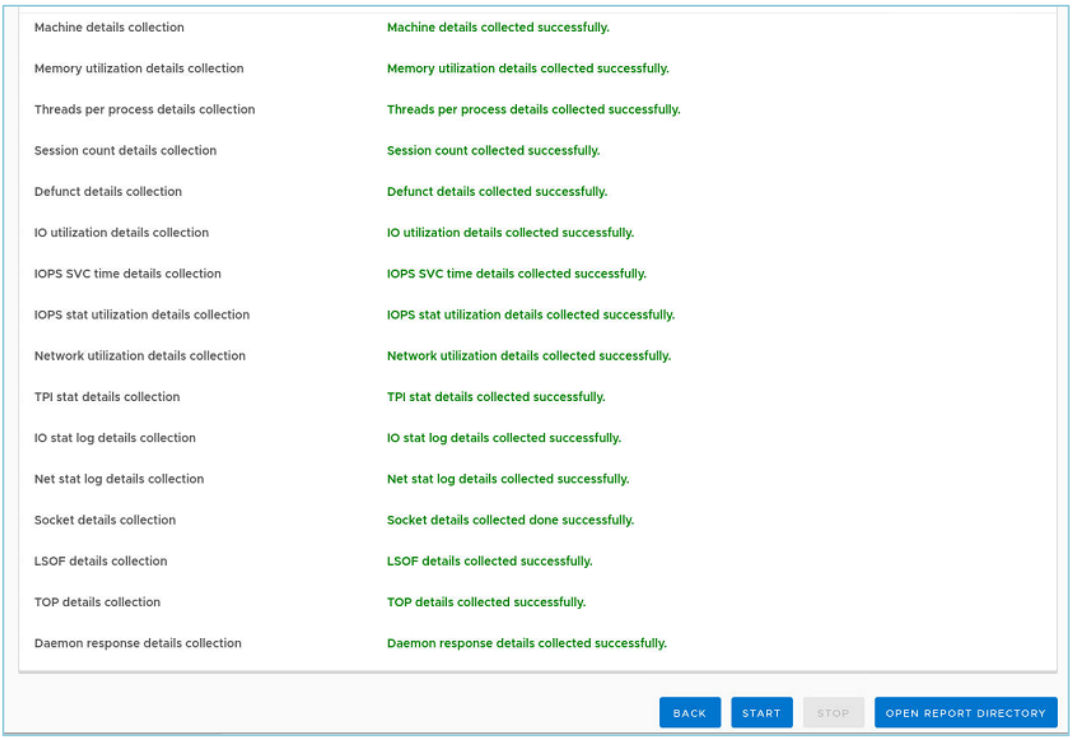

Figure 59. RMT Data Collection Successful message

7. Click **Open Report Directory** to locate previous test results/reports in a folder as shown below.

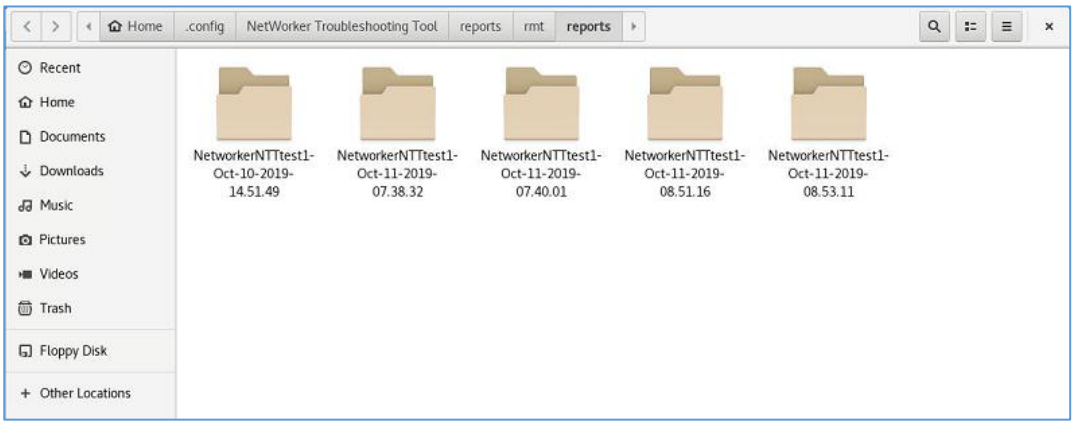

Figure 60. Open Report Directory

The following screen shows an example of the report.

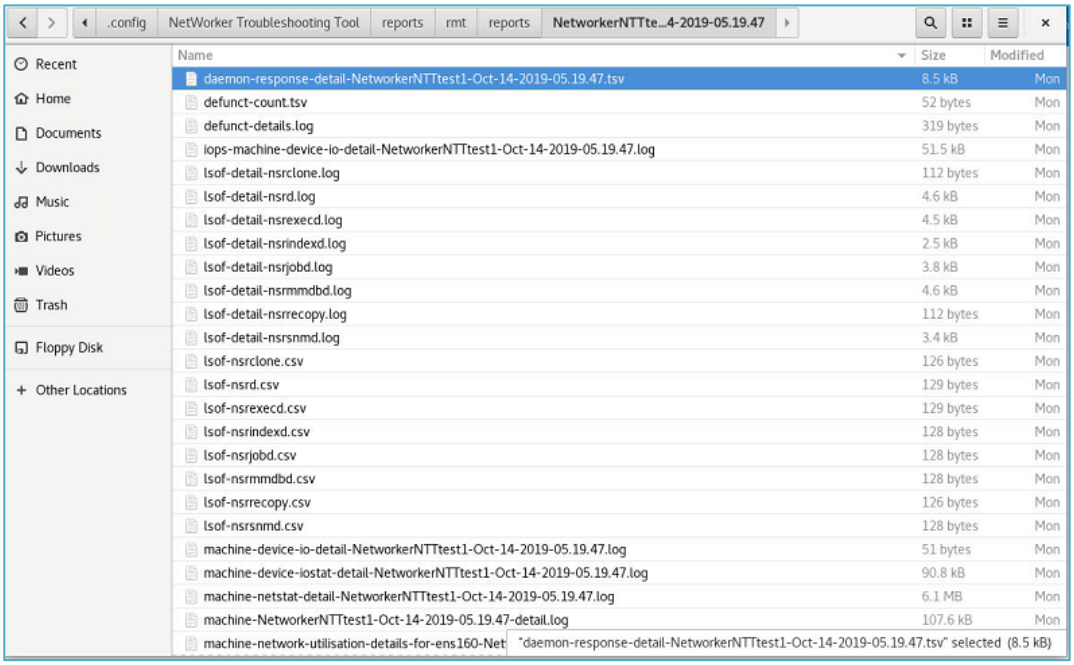

Figure 61. Example of the RMT data collection report

Run NTT on remote host

The Remote NTT tool is available on Windows platform and can be used to run NSRPCHK on remote Linux host(s) only.

Starting the Remote NTT tool

1. To start the Remote NTT tool, select **Remote NTT** from the NetWorker Troubleshooting Tool home page and click **Next,** as shown below.

Figure 62. NetWorker Troubleshooting Tool Home Page

In the following figure, Remote NTT is grayed out and cannot be enabled because NTT is running on a Linux host. Currently the Remote NTT feature can only be invoked from a Windows host.

Figure 63. Remote NTT grayed out on Linux host

Connecting to Remote Machine

2. When you click **Next** from Figure 63, the following screen is displayed.

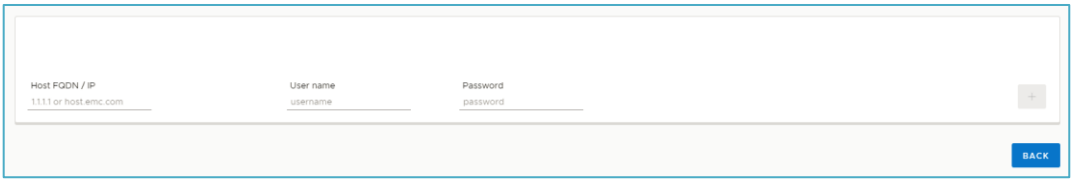

Figure 64. Remote NTT screen

3. Click the plus icon to collect information as shown below.

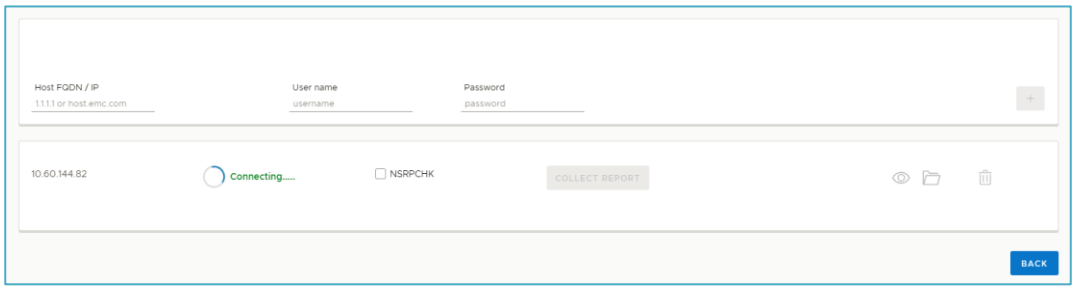

Figure 65. Connecting Remote NTT

4. Enter the Remote NTT details that are described in the following table:

Table 15. Run NTT on Remote Host

Field	Description
Host FQDN/ IP	Enter the FQDN or IP address of the Remote Host. Hostname is required.
User name	Provide a username that uniquely identifies someone on a system, for example, `1.1.1.1` or `host.emc.com`
Password	Enter the correct password to verify the identity of a user. In the password field, enter remote host password. The default password is `changeme`

5. If Remote NTT data connection runs unsuccessfully or if you get an error while copying Utilities/Agent to the remote host, the following screen is displayed.

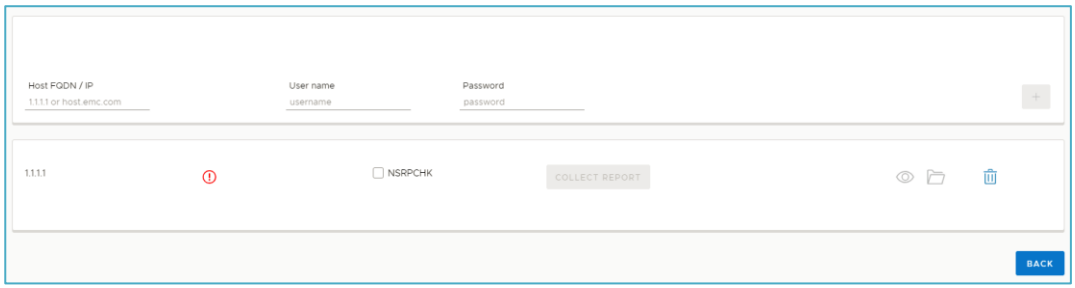

Figure 66. NTT Data connection unsuccessful

6. Click **BACK** to return to the Remote NTT screen and re-enter the credentials. You cannot continue with this process until you successfully enter acceptable credentials.

Running the NSRPCHK tool on a remote machine

If the Remote NTT connects successfully, the following screen is displayed, as shown below.

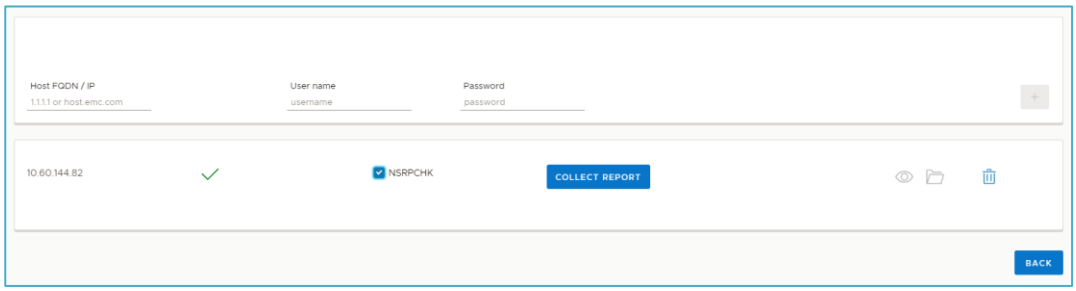

Figure 67. Enabling NSRPCHK

1. Click **Collect Report** to run the NSRPCHK tool on the remote Linux server. The following screen is displayed.

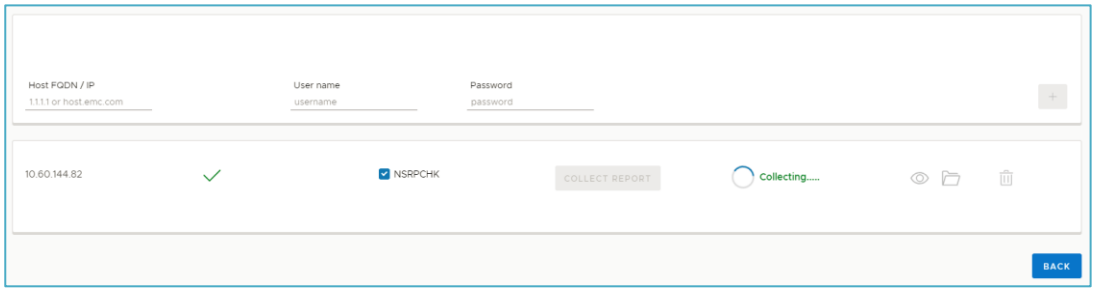

Figure 68. Collecting Report

Collecting the report to local machine

If the NSRPCHK report is collected successfully, the following screen is displayed:

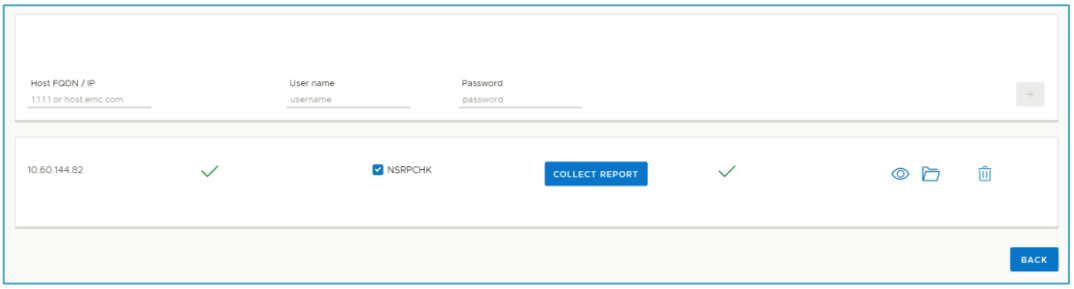

Figure 69. Successfully collected report

1. Click the icons that are described in the following table.

Table 16. Collected Report

Icons	Description
	Click here to view the remote host's latest report(s).
	Click here to open the local folder where reports are stored.

Icons	Description
	Click here to remove the remote host information from NTT.

 Click this icon to view the remote host's latest report(s) as shown below. This is an active feature which allows you to view and report details while data collection is in progress.

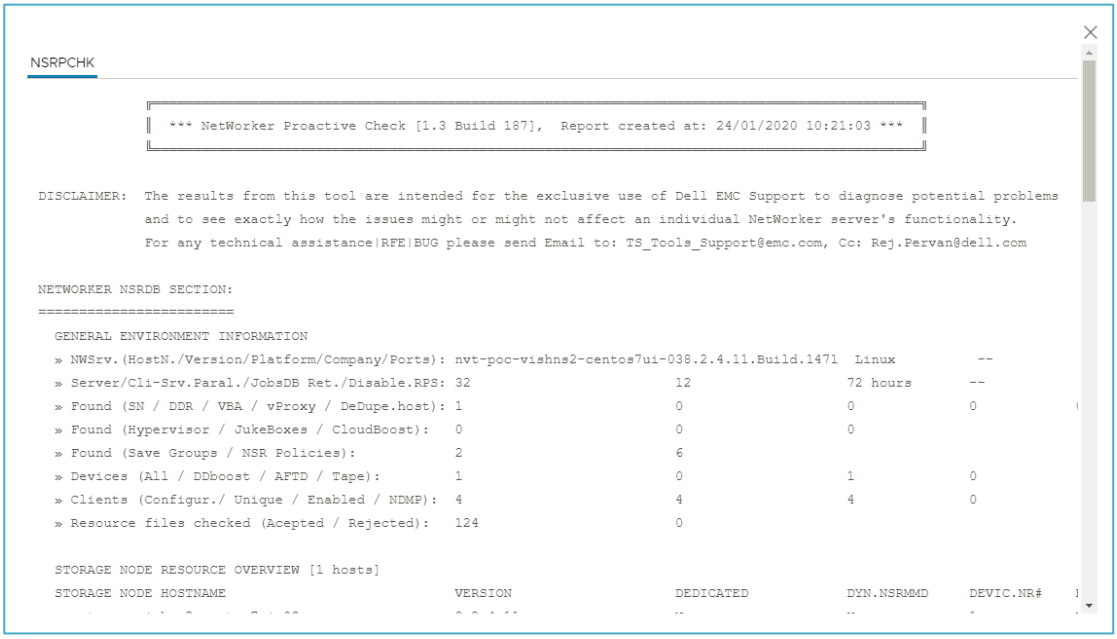

Figure 70. View Report

 Click this icon to open the local folder where reports are stored, as shown below.

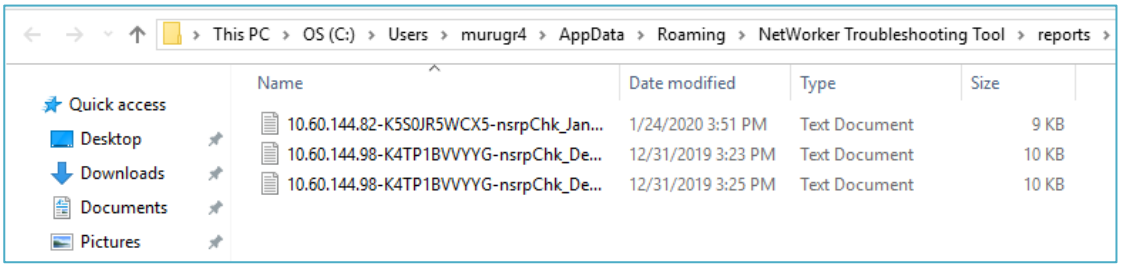

Figure 71. Open Local Folder

 Click this icon to remove the remote host information from NTT.

If any error occurs during the NSRPCHK process, an error message is displayed as shown below.

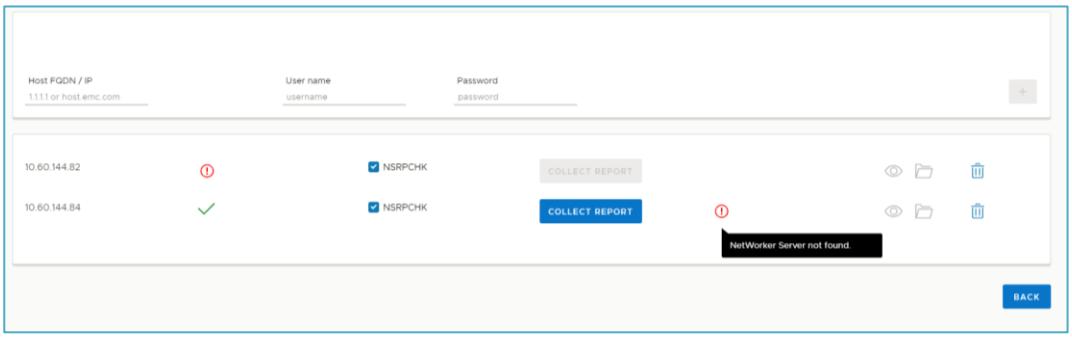

Figure 72. Error in NSRPCHK Report collection

Note: This error occurred because, for NSRPCHK, a networker server is mandatory.

Contact Us

1. To Contact Dell EMC technical support for the NetWorker Troubleshooting Tool, from the Home page, click **Contact Us** as shown in the following screen.

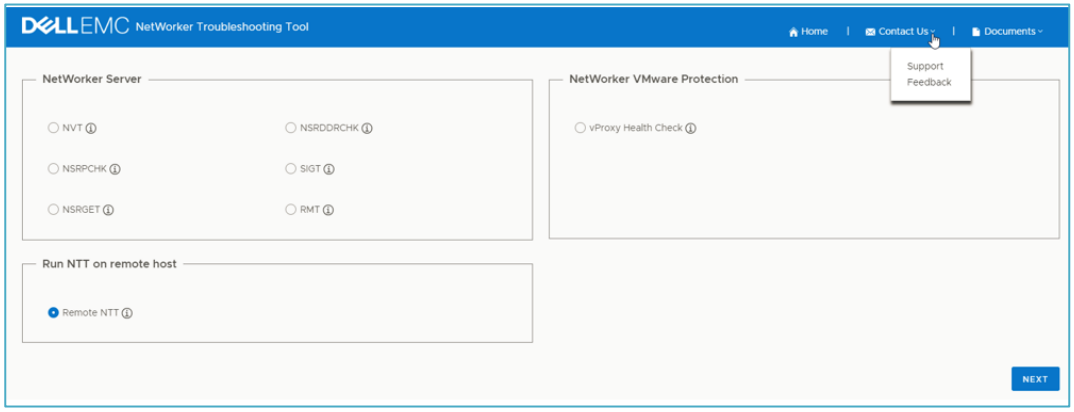

Figure 73. Contact Us

2. Click **Support** from the dropdown menu. The following screen is displayed.

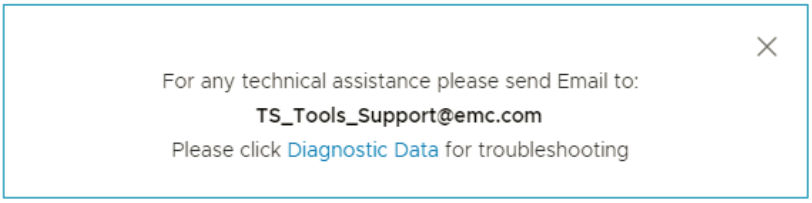

Figure 74. Support

3. For technical assistance, send an email to: TS_Tools_Support@emc.com with diagnostic data.
4. To collect required files for troubleshooting, click **Diagnostic Data** under **Contact Us** on the Masthead Navigation. Send these files to the support team.
5. Click **Feedback**, the following screen is displayed.

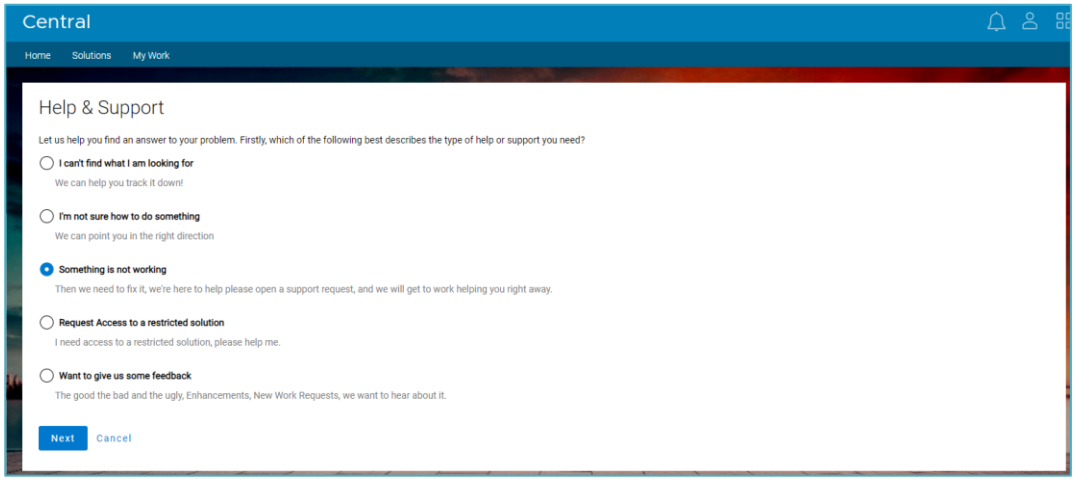

Figure 75. Central Help & Support page

6. Open a support ticket from Central Help & Support Request Support.

Frequently Asked Questions (FAQs)

1. **Does NTT support in CentOS6/RHEL 6?**

   No. NTT requires a higher version of CGLIB (native library) which is available on CentOS 7 and above.

2. **NSRGET is not working in NTT 1.1.0 running on a newly installed CentOS Linux host?**

   The KSH package is required to run NSRGET. In the newly installed CentOS host, KSH was not installed by default.

   Install KSH package in a host which has connectivity to the internet.

3. **Unknown Error during Ping execution and DNS resolution reported?**

   Customer tried to use the NetWorker Troubleshooting Tool (NTT) v1.0.4. on a Windows 2012 R2 Standard (German) Networker server.

   Change the default language to English.

4. **How do I increase the maximum number of open files under CentOS Linux? Or How do I open more file descriptors under Linux?**

   The "`ulimit`" command provides control over the resources available to the shell and processes that it started, on systems that allow such control.

   For more details visit this website: https://www.cyberciti.biz/faq/linux-increase-the-maximum-number-of-open-files/

5. **What is a PDB file and what is it used for?**

   A Program DataBase (PDB) file is used for storing debugging information about a program. It is typically created from source files during compilation. PDB files have a .pdb extension, typically.

   When a program is debugged, the debugger loads debugging information from the .pdb file and uses it to find symbols or determine the current execution state of program source code by comparing crash data to the specific parts of the source code.

6. **Can I run only the RMT of NW Daemons without running the nsrwatch and vice versa?**

   You can collect single process details by deselecting all the other nsrwatch /daemon processes.