# Running an Audit from Start to Finish

This appendix outlines the major steps needed to run a Net Audit on NATkit 3.1.x. The following steps should be read and understood before scheduling a Net Audit on NATkit.

## Registering the Audit on DAVE/Running the Audit End-to-End on NATkit Using CLI

### Procedure

**Step 1** Go to the Definitive Accounts VEhicle web page.

**Step 2** Select the service type (e.g. ANS- Enterprise)

**Step 3** Select the desired Account.

**Step 4** Under Network Performance, click on **Net Audits**.

**Step 5** Click on **Schedule A Net Audit**.

**Step 6** Select the Audit type and press **Next**.

**Step 7** Select the NATkit you want to use for the audit.

**Step 8** Check the check box and press **Next**. The message 'Your request was submitted successfully' should appear.

**Note** The checkbox below the NATkit selection should be checked only if you want to select the devices and generate the templates on the NATkit box itself. In this case you will receive only the audit key in a zip file.

If you wish to do the device selection and template generate on DAVE, please leave the checkbox unchecked and proceed to the next section of this document.This process will reserve an audit ID for this request in the backend and create an audit key.

You will receive two emails at the completion of this process. One email will contain the instructions on how to proceed further with the audit scheduling on NATkit. The second email will contain the URL of the ZIP file that needs to be copied into the NATkit box to register the audit.

**Step 9** Click on the URL located in the second email to view a window with an <audit_id>.tar.gz file inside it.

**Step 10** Open a FTP session to the NATkit machine and copy the above .gz file in the NATkit in the following location in ASCII mode.

**/opt/CSCONsa/bin/NSA/commandline**

**Step 11** Run the following command.

**cd /opt/CSCONsa/bin/NSA/supportutils**

**Step 12** For **Audit Registration**, run the following script:

**./register_audit /opt/CSCONsa/bin/NSA/commandline/<audit_id>.tar.gz**

The following are example messages:

```
Enter company name: Cisco Systems
Enter name of data collector: ggarg
Enter email id for alerts: ggarg@cisco.com
Enter comments: test audit
Whether entered data correct(y/n)? y
Successfully Audit Registration Completed.
```

This will register the audit id with the netaudit database. If an audit has been registered prior to this audit, it will prompt the user accordingly.

**Step 13** For **Device Selection**, run the following script:

**./select_devices**

(takes no arguments)

This exports the auditable devices into auditable_devices.csv file in /opt/CSCONsa/bin/NSA/commandline folder for the user to select. If the discovery/inventory has not been run since the NATkit has been installed, this will give an error.

- Auditable Devices: For each audit type, the auditable sys object ids can be found at Nettools web page.

The Ops engineer should manually verify this file for any devices that he/she would like to exclude. No new/missing devices should be added into this file, however devices can be removed if they are not required in the audit.

This is equivalent to the device selection GUI on NATkit or DAVE.

**Step 14** To import the auditable devices from the .csv file listed into the netaudit database, run the following script:

**./complete_selection**

(takes no arguments)

This script imports the auditable devices from the above csv file into the netaudit database.

**Step 15** For **Access Verification**, run the following script:

**./verify_device_access**

(takes no arguments)

This script runs the ping, SNMP and telnet access verification on all the devices in the natkit database in Routers table.

**Step 16** For **Template Generation**, run the following script:

**./generate_audit_templates YYYYMMDD.hhmm**

(takes the start time in the above format as an argument).

The start time is local NATkit server time in the same time zone as the NATkit (not GMT time as on DAVE).

This script generates the XML file and ptask files and puts them into /opt/CSCONsa/bin/NSA/commandline folder.

**Note** For LAN V4 audits, the trunk/cdp ports needed, are automatically populated into the ptask files.A status file, generated while detecting these ports, can be found at: '/opt/CSCOpx/htdocs/NSA/COMPANIES/<cust-id>/out/audits/lanv4ports-<audit-id>.status'

**Step 17** For **Audit Scheduling**, run the following script:

**./schedule_audit**

(takes no arguments)

This script parses the XML templates and schedules the audit collection. The SNMP Poller also starts polling based on the ptask files.

**Step 18** To use **View Audit Status**, run the following script:

**./view_collection_status**

(takes no arguments)

This script writes the audit collection status into the <audit_id>_Collection_Status.txt file in /opt/CSCOpx/htdocs/NSA/COMPANIES/natkit_id/out folder.

**Step 19** To write the detailed node status into the <audit_id>_Node_Status.txt file in the/opt/CSCOpx/htdocs/NSA/COMPANIES/natkit_id/out folder, run the following script:

**./view_node_status**

(takes no arguments)

**Step 20** To **Stop** the audit, run the following script

**./stop_audit**

(takes no arguments)

This script stops the running audit. It will also cancel any audit scheduled in future.

**Step 21** If the download doesn't begin or an on demand download is required at a later stage, run the following script to execute the Download Audit Data (on demand download) command:

**./download_audit_data_now <audit_id>**

The download process is scheduled to start an hour after the audit completes and it will download both telnet and SNMP data to the CCO.

The audit tar file after packaging is kept in /opt/CSCOpx/htdocs/NSA/COMPANIES/<natkit_id> folder with file name "transport-event-NDC-<natkit_id>.tar".

**Note** All of the scripts above will display information about their usage (parameter help) by adding **--help** after the script as follows: **./script_name --help**

# Generate Templates from DAVE/Run Audit Through NATkit CLI

## Procedure

**Step 1** Go to the Definitive Accounts VEhicle web page.

**Step 2** Select the service type (e.g. ANS- Enterprise)

**Step 3** Select the desired Account.

**Step 4** Under Network Performance, click on **Net Audits**.

**Step 5** Click on **Schedule A Net Audit**.

**Step 6** Select the Audit type and press **Next**.

**Step 7** Select the NATkit you want to use for the audit and press **Next**.

**Note** The checkbox below the NATkit selection should not be checked in this case. It should be checked only if you want to select the devices and generate the templates on the NATkit box itself. Please refer to earlier section of the document in that case.

**Step 8** On the Net Audit: Schedule screen, select the audit schedule time and devices to be included in the audit. The audit schedule time can also be changed later on the NATkit box. Click on **Confirm Request**.

The start time is the time when audit should start on NATkit, in GMT (not in NATkit server's time zone). The templates generated from DAVE would need to be changed (updated) for start time to convert the time in templates (in GMT) to NATkit server time. The schedule script doesn't convert the time and would interpret the GMT time as local time and would start the audit according to that time. So update-timestamp should be run to change the time into NATkit local time zone (refer to step 15).

You may also wish to verify the dialup information for the NATkit box at this stage.

**Step 9** Once all prerequisites are met and the audit type, start time and device list have been verified, click **Submit** to submit your request for template generation.

The message 'Your request was submitted successfully' should appear.

This process will reserve an audit ID for this request in the backend and create the collection templates.

**Note** You will receive two emails at the completion of this process. One email will contain the instructions on how to proceed further with the audit scheduling on NATkit. The second email will contain the URL of the ZIP file that needs to be copied into the NATkit box to register the audit

**Step 10** Click on the URL found in the scond email to view a window with an <audit_id>.tar.gz file inside it.

**Step 11** Open a FTP session to the NATkit machine and put the above .gz file in the NATkit in the following location in ASCII mode.

**/opt/CSCONsa/bin/NSA/commandline**

**Step 12** Run the following command.

**cd /opt/CSCONsa/bin/NSA/supportutils**

**Step 13** For **Audit Registration**, run the following script:

**./register_audit/opt/CSCONsa/bin/NSA/commandline/<audit_id>.tar.gz**

The following are example messages:

```
Enter company name: Cisco Systems
Enter name of data collector: ggarg
Enter email id for alerts: ggarg@cisco.com
Enter comments: test audit
Whether entered data correct(y/n)? y
Successfully Audit Registration Completed.
```

This will register the audit id with the netaudit database. If an audit has been registered prior to this audit, it will prompt the user accordingly.

**Step 14** For **Device Access Verification**, run the following script:

**./rcmd verify_device_access/opt/CSCONsa/bin/NSA/commandline/A<audit_id>.xml**

**Note** LAN Switch Version 4 audit requires polling for only CDP and VLAN trunking ports.To poll these ports from the devices and put them into the interface specific ptask files (task name ending with 08), run the following CLI:

**./lanv4_add_ports**

You should see the following change in the interface specific ptask files.

- Before running the CLI:
DEVICE=172.18.1.1 TABLE_GROUP=6K_CatOS_Interface_Poll TABLE_INDEX=

- After running the CLI:
DEVICE=172.18.1.1 TABLE_GROUP=6K_CatOS_Interface_Poll TABLE_INDEX=4,5,6,23,24,41

**Step 15** To use **Audit Scheduling**, run the following script:

**./schedule_audit**

(takes no arguments)

This script will update the start time in the XML and ptask files.

This script looks into the /opt/CSCONsa/bin/NSA/commandline folder for the XML file and ptask files. It parses the XML templates and schedules the audit collection. The SNMP Poller also starts polling based on the ptask files.

**Note** If the NATkit timezone differs from GMT, run following script to make the start time of the audit as the time present in the XML template generated from DAVE (in GMT).

**./update_timestamp YYYYMMDD.hhmm**

(it takes the start time in the above format as an argument).

**Be sure to run the above script prior to Audit Scheduling.**

**Step 16** To **View Audit Status**, run the following script:

**./view_collection_status**

(takes no arguments)

This script writes the audit collection status into the <audit_id>_Collection_Status.txt file in the /opt/CSCOpx/htdocs/NSA/COMPANIES/natkit_id/out folder.

**Step 17** To write the detailed node status into the <audit_id>_Node_Status.txt file in the /opt/CSCOpx/htdocs/NSA/COMPANIES/natkit_id/out folder, run the following script:

**./view_node_status**

(takes no arguments)

This script writes the detailed node status into the <audit_id>_Node_Status.txt file in /opt/CSCOpx/htdocs/NSA/COMPANIES/natkit_id/out folder.

**Step 18** To **Stop** the audit, run the following script:

**./stop_audit**

(takes no arguments)

This script stops the running audit. It will also cancel any audit scheduled in future.

**Step 19** If the download doesn't begin or an on demand download is required at a later stage, run the following script to execute the Download Audit Data (on demand download) command:

**./download_audit_data_now <audit_id>**

The download process is scheduled to start an hour after the audit completes and it will download both telnet and SNMP data to the CCO.

The audit tar file after packaging is kept in /opt/CSCOpx/htdocs/NSA/COMPANIES/<natkit_id> folder with file name "transport-event-NDC-<natkit_id>.tar".

**Note** All of the scripts above will display information about their usage (parameter help) by adding **--help** after the script as follows: **./script_name --help**

# Register the Audit on DAVE and Run Audit on NATkit GUI

## Procedure

**Step 1** Go to the Definitive Accounts VEhicle web page.

**Step 2** Select the service type (e.g. ANS- Enterprise)

**Step 3** Select the desired Account.

**Step 4** Under Network Performance, click on **Net Audits**.

**Step 5** Click on **Schedule A Net Audit**.

**Step 6** Select the Audit type and press **Next**.

**Step 7** Select the NATkit you want to use for the audit.

**Step 8** Check the check box and press **Next**.

**Note** The checkbox below the NATkit selection should be checked only if you want to select the devices and generate the templates on the natkit box itself. In this case you will receive only the audit key in a zip file.

The message ‘Your request was submitted successfully’ should appear.

This process will reserve an audit ID for this request in the backend and create an audit key.

You will receive two emails at the completion of this process. One email will contain the instructions on how to proceed further with the audit scheduling on NATkit. The second email will contain the URL of the ZIP file that needs to be copied into the NATkit box to register the audit

**Step 9** Click on the URI in the email and you should see a window with an <audit_id>.tar.gz file inside it.

**Step 10** Open a FTP session to the NATkit machine and copy the above .gz file in the NATkit in the following location in ASCII mode.

**/opt/CSCONsa/bin/NSA/commandline**

**Step 11** Run the following command.

**cd /opt/CSCONsa/bin/NSA/supportutils**

**Step 12** For **Audit Registration**, run the following script:

**./register_audit /opt/CSCONsa/bin/NSA/commandline/<audit_id>.tar.gz**

Example messages:

```
Enter company name: Cisco Systems
Enter name of data collector: ggarg (email id of the data collector,
max 8 characters)
Enter email id for alerts: ggarg@cisco.com
Enter comments: test audit
Whether entered data correct(y/n)? y
```

This will register the audit id with the netaudit database. If an audit has been registered prior to this audit, it will prompt the user accordingly.

**Step 13** Logon to the NATkit GUI via http://natkit-host:1741

**Step 14** Click on **Network Analysis Toolkit** and select Net Audit

**Step 15** Verify the audit settings on Net Audit Settings GUI.

**Step 16** Click on device selection and select the devices you would like to include in the audit. All the devices are taken from the NATkit routers table. If you don't see any devices in the left panel of the screen, rerun the discovery/inventory and/or import from a seed file.

**Step 17** Click on **Access Verification** and verify the telnet, ping and SNMP access for all the devices included in the audit.

**Step 18** Click on **Start/Stop Data Collection** link in the same Net Audit folder and start/schedule the data collection.

The start/schedule time is local NATkit server time in the same time zone as the NATkit (not GMT time as on DAVE). GUI accessed through any client machine will show and schedule the audit according to NATkit server time.

For LanV4 audits, the trunk/cdp ports needed, are automatically populated into the ptask files.

A status file, generated while detecting these ports, can be found as '/opt/CSCOpx/htdocs/NSA/COMPANIES/<cust-id>/out/audits/lanv4ports-<audit-id>.status'.

**Step 19** To Stop the audit, select **Start/Stop Data Collection** and click **Stop Collection**. This GUI can be used to cancel any audit scheduled in future.

**Step 20** Download Audit Data (on demand download).

**Step 21** The download process is scheduled to start an hour after the audit completes and it will download both telnet and SNMP data to the CCO.

**Step 22** In case the download doesn't happen because of some reason or an on demand download is required at a later stage, execute the following command.

**./download_audit_data_now <audit_id>**

The audit tar file after packaging is kept in the /opt/CSCOpx/htdocs/NSA/COMPANIES/<natkit_id> folder under the file name "transport-event-NDC-<natkit_id>.tar".