Description

The purpose of this document is to provide a reference for the backup and restore feature for NDLP. This is tested on NDLP (VM) version 9.2.x platform.

Detailed information can be found in the kb article:
Operationally Functional Manager

• Manager 1: Fully Functional (Dashboard) – Note the number of incidents count for each categories
Manager 1: All Incidents populated

<table>
<thead>
<tr>
<th>Total Incidents: 228</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group by...</td>
</tr>
<tr>
<td>Source Code Leaksages 90</td>
</tr>
<tr>
<td>Board Meeting Minutes Leaksages 48</td>
</tr>
<tr>
<td>Engineering Drawings Leaksages 46</td>
</tr>
<tr>
<td>Unprotected Credit Card Number Violations 16</td>
</tr>
<tr>
<td>Manager and Acquisition Leaksages 14</td>
</tr>
<tr>
<td>Financial Reports Leaksages 6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Filter by...</th>
<th>Clear All</th>
<th>Apply</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Previous 24 hours</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Actions</th>
<th>Deselect All</th>
<th>Assign to Case</th>
<th>Tune Rule</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recipients</th>
<th>Subject</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>JaneStev <a href="mailto:janeStev@raylasey.com">janeStev@raylasey.com</a></td>
<td>topic code</td>
<td>Sat Jun 09 02:52:01 SGT 2012</td>
</tr>
<tr>
<td>Terence <a href="mailto:Terence@technopol.com">Terence@technopol.com</a></td>
<td>Main Services running</td>
<td>Sat Jun 09 02:51:48 SGT 2012</td>
</tr>
<tr>
<td>DaleCasa <a href="mailto:daleCasa@technopol.com">daleCasa@technopol.com</a></td>
<td>main execution app from the org</td>
<td>Sat Jun 09 02:51:45 SGT 2012</td>
</tr>
<tr>
<td>LeroyTan <a href="mailto:LeroyTan@technopol.com">LeroyTan@technopol.com</a></td>
<td>Main source code used</td>
<td>Sat Jun 09 02:50:51 SGT 2012</td>
</tr>
<tr>
<td>LindaSer <a href="mailto:LindaSer@technopol.com">LindaSer@technopol.com</a></td>
<td>Our company's org chart</td>
<td>Sat Jun 09 02:47:53 SGT 2012</td>
</tr>
<tr>
<td>ThomasEd <a href="mailto:ThomasEd@goostamine.com">ThomasEd@goostamine.com</a></td>
<td>Our main computing engine</td>
<td>Sat Jun 09 02:47:41 SGT 2012</td>
</tr>
<tr>
<td>&quot;Giiberte&quot; <a href="mailto:Giiberte@Kingstone.com">Giiberte@Kingstone.com</a></td>
<td>Our development plans with iPhone</td>
<td>Sat Jun 09 02:44:42 SGT 2012</td>
</tr>
<tr>
<td>&quot;Giiberte&quot; <a href="mailto:Giiberte@Kingstone.com">Giiberte@Kingstone.com</a></td>
<td>Key code</td>
<td>Sat Jun 09 02:43:32 SGT 2012</td>
</tr>
<tr>
<td>&quot;Giiberte&quot; <a href="mailto:Giiberte@Kingstone.com">Giiberte@Kingstone.com</a></td>
<td>Look at our process</td>
<td>Sat Jun 09 02:42:51 SGT 2012</td>
</tr>
<tr>
<td>MSWord &quot;Giiberte&quot; <a href="mailto:Giiberte@Kingstone.com">Giiberte@Kingstone.com</a></td>
<td>Our Financial Disclosure Statement</td>
<td>Sat Jun 09 02:41:29 SGT 2012</td>
</tr>
<tr>
<td>Excel &quot;Giiberte&quot; <a href="mailto:Giiberte@Kingstone.com">Giiberte@Kingstone.com</a></td>
<td>CHECK IT OUT</td>
<td>Sat Jun 09 02:38:30 SGT 2012</td>
</tr>
<tr>
<td>C++ Source &quot;Giiberte&quot; <a href="mailto:Giiberte@Kingstone.com">Giiberte@Kingstone.com</a></td>
<td>This is the header used for transmission</td>
<td>Sat Jun 09 02:36:28 SGT 2012</td>
</tr>
<tr>
<td>C++ Source &quot;Giiberte&quot; <a href="mailto:Giiberte@Kingstone.com">Giiberte@Kingstone.com</a></td>
<td>Lack of control for source code release</td>
<td>Sat Jun 09 02:36:26 SGT 2012</td>
</tr>
<tr>
<td>&quot;Giiberte&quot; <a href="mailto:Giiberte@Kingstone.com">Giiberte@Kingstone.com</a></td>
<td>Key modulator</td>
<td>Sat Jun 09 02:36:23 SGT 2012</td>
</tr>
<tr>
<td>&quot;Giiberte&quot; <a href="mailto:Giiberte@Kingstone.com">Giiberte@Kingstone.com</a></td>
<td>Source code command</td>
<td>Sat Jun 09 02:36:20 SGT 2012</td>
</tr>
<tr>
<td>&quot;Giiberte&quot; <a href="mailto:Giiberte@Kingstone.com">Giiberte@Kingstone.com</a></td>
<td>KEY SOURCE CODE</td>
<td>Sat Jun 09 02:37:24 SGT 2012</td>
</tr>
</tbody>
</table>
Incidents linked to the Managed device (Monitor) can be accessed.
Operationally Functional Manager

- Added a specific comments for the incidents:
Operationally Functional Manager

- Cases that were created under this Manager
Operationally Functional Manager

- Details of case can be opened and accessed.
• Policies, template and concepts created under this manager
• Discover scan created under this manager
Operationally Functional Manager

- Filter scans and system Administration under this manager
Operationally Functional Manager (1.3)

- Filter scans and system Administration under this manager. (connection to ePO and unified Policy)
• Information under the “Device” ➔ configure section: Syslog and time zone, and Company’s Name as example
Set up a Secondary Manager (Same version as the primary one)

- Fresh image for the secondary manager. Note: You need to set your own IP, DNS server, Gateway and so on.
Backup Process

Backup
2 things to back up

1) Backup the configurations to the secondary manager from the backup GUI (SSH Keys and the Public keys) – one time effort

Backup the files through config

Files is backed up in Manager 2
Unpack the tar file created during backup

```
# tar -xzvf <filename>.tar
```
Stop all the NDLP required Services (In the following order)

# service stingray stop
# service jboss stop
# service mysql stop
2 things to back up

2) Backup the Database (MYSQL) – (You can create a cron job to perform this task daily)

**Execute on Manager 1:**

```
# scp -rp /data/mysql root@manager2:/data/archivedir/data/
```

This automatically replace the original database of manager 2 to manager 1

Copying process will begin

Database is backed up in Manager 2
Restore
Check your diski-space

Make sure that you have at least 80 GB of space available for restoration

`# df -h`
Check your NDLP versions

It is important that you ensure the Primary and Secondary NDLP are of the same version.

# more /data/archivedir/data/stingray/gui/backup/version.txt
# cat /data/stingray/etc/version
Check the platform

Check the platform that you are running (you need it later). (In this case it is vm)

```bash
# mysql -e "select platform_type from unified_config.stingray_misc_config\G"
```

![MySQL output](image)
3 Steps in restoration

Step 1) Replace the installed keystore and public and private keys. This will allow authentication of users and the tunnel between NDLP devices.

```bash
# mv /data/archivedir/usr/share/ssl/mcafeeinternalks /usr/share/ssl/

NOTE: You might not require the following commands if there are no public and private keys in the backup archive. If the ssh_tunnel_keys directory does not exist in your extracted data directory, go to the next step.

# mv /data/archivedir/root/ssh_tunnel_keys/iManager_RSA_Key.pub /root/ssh_tunnel_keys/
# mv /data/archivedir/root/ssh_tunnel_keys/iManager_RSA_Key /root/ssh_tunnel_keys
```
3 Steps in restoration

Step 2) **Restore MySQL Database**

- Remove the process ID file of the existing installation.
  
  ```
  # rm –rf /data/mysql/* .pid
  ```

- Remove data directory that might interfere with the MySQL process.
  
  ```
  # rm –rf /data/mysql/datarm
  ```

- Change the permission on MySQL directory
  
  ```
  # chown –R mysql:mysql /data/mysql/
  ```
3 Steps in restoration

Step 2) **Restore MySQL Database**

• Start MySQL Service

  `# service mysql start`

• Check if the service is running

  `# service mysql status`
Step 3) Drop the installed Stingray configuration

```bash
# mysql --execute="DROP DATABASE IF EXISTS unified_config"
# mysql --execute="DROP DATABASE IF EXISTS stingray"
# mysql --execute="CREATE DATABASE IF NOT EXISTS stingray"
# mysql --execute="DROP DATABASE etl_star"
# mysql --execute="USE search_results; DROP TABLE search_results_realtime_host"
# mysql --execute="USE search_results; DROP TABLE search_results_realtime_incident"
# mysql --execute="USE search_results; DROP TABLE search_results_realtime_object"
```
3 Steps in restoration

Step 3) **Drop the installed Stingray configuration**  
Create a new Stingray configuration.

```bash
#/data/stingray/bin/stingray_config_install <platform_type>
```
3 Steps in restoration

Complete your restoration – reboot (Make sure that you do not have the primary manager online. The managed device cannot have 2 manager running). It takes a few minute before the system comes back up.

#reboot
Restored State
Secondary Manager functioning

- Manager 2: Fully Functional (Dashboard) – However, all status (action) on the incidents are not recovered. (E.g. Pending, investigated…)
Secondary Manager functioning

- Manager 2: Incident page
Secondary Manager functioning

- Manager 2: No problem accessing the Managed device (Monitor) from secondary manager
Secondary Manager functioning

• Manager 2: However, the action (such as comments) done for that incidents is not recovered
Secondary Manager functioning

- Manager 2: Cases information still available
Secondary Manager functioning

- Manager 2: Content of the case can still be accessed
Secondary Manager functioning

- Manager 2: Policy, concept and template still there.
Secondary Manager functioning (1.3)

• Manager 2: Policy, concept and template still there.
Secondary Manager functioning

- Manager 2: Discover scan configurations still there
Secondary Manager functioning

- Manager 2: Capture filters is the same and system status is running
Secondary Manager functioning (1.3)

- Search Results is still available
Secondary Manager functioning (1.3)

- All the link (even in ePO) is still available
Secondary Manager functioning

- While some information like “Company Name” remains, others like syslog information, and time zone is not recovered. It is important that you configure these information before performing restoration.