Nutanix

How to Send Logs to a Remote Syslog Server

Summary:

This article briefly describes how to configure a Nutanix cluster to send logs to an rsyslog server.

Description:

This article briefly describes configuring a Nutanix cluster to send logs to an rsyslog server.

Solution:

1. Connect to a Controller VM (CVM) in the cluster using SSH.
2. Enter the **ncli** command to log into the nCLI prompt.

   ```
   nutanix@cvm$ ncli
   <ncli>
   ```

   Note: "<ncli>" is the nCLI prompt.

3. The remote syslog server is enabled by default. Disable it while you configure the settings.

   ```
   <ncli> rsyslog-config set-status enable=false
   ```

4. Add an rsyslog server using the following command, which adds it to the cluster.

   ```
   <ncli> rsyslog-config add-server name=<remote_server_name> ip-
   address=<remote_server_address> port=<rsyslog port> network-protocol=udp relp-
   enabled=false
   ```

5. Choose a module to forward log information from and specify the level of information to collect.

   ```
   <ncli> rsyslog-config add-module server-name=<remote_server_name> module-
   name=<module_name> level=<log_level>
   ```

   Replace <module_name> with one of the following:

   - ACROPOLIS - The acropolis services are responsible for task scheduling, execution, stat collection, publishing, etc. For more information, see Acropolis Services in the

Nutanix Bible.

- AUDIT - Seeds the "consolidated_audit.log" which is used to track ergon tasks that result in changes to the cluster and UVMs.
- CASSANDRA - Stores and manages all of the cluster metadata
- CEREBRO - Responsible for replication and DR capabilities
- CURATOR - Responsible for managing and distributing tasks throughout the cluster
- GENESIS - Responsible for any services interactions (start/stop/etc.) as well as the initial configuration
- PRISM - Management gateway for components and administrators to configure the cluster, monitor the cluster and track logins (successful and unsuccessful).
- STARGATE - Responsible for all data management and I/O operations
- APLOS - API requests
- SYSLOG_MODULE - SSH logins and much information about local root account usage (starting processes, for example)
- ZOOKEEPER - Stores all of the cluster configuration

For more information about the modules above, see Cluster Components in the Prism Web Console Guide or the Nutanix Bible.

Enable module logs at the ERROR level unless you require more information. Replace <log_level> with one of the following:

- EMERGENCY
- ALERT
- CRITICAL
- ERROR
- WARNING
- NOTICE
- INFO
- DEBUG

For example, if you set the level to INFO, it also covers the levels above it (i.e. EMERGENCY, ALERT, CRITICAL, ERROR, WARNING and NOTICE). If you select INFO for a module, you do not have to select any of the levels above it for the same module.

Note: CVMs send system audit logs to the syslog server by default, even when no modules are configured for the server. Below is an example of these audit logs:

```
2021-09-09T08:56:01.353708-05:00 ntnx-xxx-cvm audispd[5307]: node=ntnx-xxx-cvm
type=PROCTITLE msg=audit(1631195761.351:193118):
proctitle=2F7573722F62696E2F707974686F6E322E37002D42002F686F6D652F6E7574616E69782F736
57276696365616269 6C6974792F62696E2F7573696E672D67666C616773002F686F6D652F
6E7574616E69782F7365727669636561626 96C6974792F62696E2F63726F6E5F736572766963656162696
C6974792E7079

2021-09-09T08:56:01.353827-05:00 ntnx-xxx-cvm audispd[5307]: node=ntnx-xxx-cvm
type=SYSCALL msg=audit(1631195761.351:193119):
arch=c000003e syscall=90 success=yes exit=0 a0=16fbbe0 a1=1ed a2=1 a3=0 items=1
```

```
ppid=5498 pid=5503 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000
egid=1000 sgid=1000 fsgid=1000 tty=(none) ses=13210 comm="python2.7"
exe="/usr/bin/python2.7" subj=nutanix_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="audit_time_perm_mod_export_delete"

2021-09-09T08:56:01.353939-05:00 ntnx-xxx-cvm audispd[5307]: node=ntnx-xxx-cvm
type=PATH msg=audit(1631195761.351:193119):
item=0 name="/home/nutanix/.python-eggs/psutil-5.7.0-py2.7-linux-x86_64.egg-
tmp/psutil/tmpe8m0Gx.$extract" inode=1705569 dev=09:02 mode=0100600 ouid=1000
ogid=1000 rdev=00:00 obj=nutanix_u:object_r:user_home_t:s0 objtype=NORMAL
cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
```

To prevent flooding of the rsyslog server with these audit logs, they need to be filtered on the server level. One possible solution is to filter logs based on the keyword "audispd".

6. Enable the rsyslog server:

```
<ncli> rsyslog-config set-status enable=true
```

Logs should start forwarding to the remote syslog server.
To test functionality of sending messages from the Nutanix Cluster to an external rsyslog server, use the native Linux logger command.
For TCP network protocol:

```
logger -T -P <port number> -n <rsyslog ip> -s "This is a Test"
```

For UDP Network protocol:

```
logger -d -P <port number> -n <rsyslog ip> -s "This is a Test"
```

The above commands should print the test message in */var/log* directory of the rsyslog server.

7. To show the current rsyslog server setting and modules added, run the following commands:

```
<ncli> rsyslog-config ls
<ncli> rsyslog-config ls-modules server-name=<rsyslog_name>
```

Source: *https://portal.nutanix.com/page/documents/kbs/details?targetId=kA00e0000009CEECA2*

If you need further assistance, kindly contact our support at ***support@cytechint.com*** *for prompt assistance and guidance.*

Revision #3
Created 16 January 2025 08:56:45 by Richmond Abella
Updated 17 January 2025 09:52:37 by Richmond Abella