NetGuardians

RiskTech 100 2018

Gartner 2015 Cool Vendor

NG|Screener Administration

Ljupce Nikolov

September 2018

Summary

- Appliance Administration
- Appliance Services
- Management Center
- NG|Storage Administration
- Troubleshooting

Appliance Administration

Network Configuration

- Needs to be done at install
  - VM deployment
  - Install on hardware
- Use of DHCP configuration for labs
  - Not common on client side → use of static IPs
- Need of command line network configuration knowledge

Appliance Administration

Network Configuration

- Need of root privileges

- Network configuration files
  - Interfaces configuration
    - `/etc/sysconfig/network-scripts/ifcfg-*`
  - Hostname and Default Gateway
    - `/etc/sysconfig/network`
  - DNS
    - `/etc/resolv.conf`

Appliance Administration

Interface Configuration

- `vim /etc/sysconfig/network-scripts/ifcfg-{NAME_OF_INTERFACE}`

- Important parameters (minimum set)
  - `IPADDR=<STATIC_IP>`
  - `NETMASK=<NETMASK>`
  - `ONBOOT=yes (To bring interface up on boot)`
  - `BOOTPROTO=[none|dhcp] (dhcp only for testing)`
  - `DEVICE=<INTERFACE_NAME>`

Appliance Administration

Hostname and Gateway configuration

- `vim /etc/sysconfig/network`
- Important parameters
  - `HOSTNAME=<MACHINE_HOSTNAME>`
  - `GATEWAY=<IP_OF_DEFAULT_GATEWAY>`

Appliance Administration

DNS Configuration

- `vim /etc/resolv.conf`

- Important parameters
  - `search <SEARCH_DOMAIN> (optional)`
  - `nameserver <IP_OF_DNS> (write dns in order of querying)`

Appliance Administration

Network Checks

- To apply settings, restart network service
  - `systemctl restart network`
- Check if service restarted
  - `systemctl status network`
- Network checks (from appliance)
  - `ping <IP_OF_DEFAULT_GATEWAY>`
  - `ping <IP_OF_DNS>`
  - `ping <FQN_OF_ACCESSIBLE_SERVER> (if possible)`
- If firewall opened, appliance should be accessible from the network

Appliance Administration

Sanity Check

- Sanity checks script available
- In `/usr/local/ng-screener/tools/sanity/`
  - `software-check.py` → Check of software processes and parameters for ng-screener to be able to run properly
  - `system-check.py` → Linux system check to be prepared for ng-screener install
  - `sanity-check.py` → Combine both software and system checks
- Python scripts
  - Should be called with `python script_name.py`

```
Centos Version Check: OK
RAM Check: WRONG - Less than 8GB memory
Swap Check: OK
Check Partitions (/, /var/log, /data and /storage): OK
Check Databases Users OK
Check limits: OK
Check mariadb.ngc Service is running OK
Check licensing: OK
Check Java Version: OK
Check mysql2 is installed: OK
Check installed MariaDb packages: OK
Check if user ng-screener exists: OK
Check if /log-collector directory exists: OK
Check if ngStorage is installed: OK
Check if ng-storage.service is running: OK
Check ngStorage status: OK
Check LimitMEMLOCK property: OK
Check ES_JAVA_OPTS property: OK
Check if ng-zookeeper.service is running: OK
Check if ng-messaging.service is running: OK
Check if ng-mesos-master.service is running: OK
Check if ng-mesos-slave.service is running: OK
Check if ng-thrift-server.service is running: OK
Check if ng-history-server.service is running: OK
Check if ng-screener.service is running: OK
Check heap size properly set in /etc/ng-screener/daemon/ng-screener.env: OK
Check database exists: OK
Check user admin exists: OK
Check if ng-screener-ui.service is running: OK
Check heap size properly set in /etc/ng-screener/ui/ng-screener-ui.env: OK
Check if case-manager.ngc is running: OK
Check if /etc/init.d/management.ngc is running: OK
Check indices count: OK
```

Appliance Administration

Ngadmin tool

- Administration tool for NG|Screener Daemon
- Simply type `ngadmin` in command line
  - Tenant information has to be provided (using `--tenant=TENANT_NAME` option)
- Possible actions
  - Import/Export controls
  - Remove data from NG|Storage
  - Launch processing of data to NG|Storage
  - Reload reference data caches
  - Import/Export Dashboards
  - Update license
  - …

Appliance Administration

Ngadmin tool

- Help on commands
  - use -h option

```
[root@NG-SCREENER translators]# ngadmin licensing_updateLicense -h
licensing_updateLicense
Update license
Parameter  Required  Description
f          true      The license to update
s          false     Skip checking if the file is valid for update (default: false)
```

Appliance Administration

Ngadmin tool

- `data_launchInitialProcessing`
  - Start loading Initial data to NG|Storage
    - Related to NG|Storage window
    - Done usually once by implementation consultant at first install
  - Meta data in NG|Screener to know where it should start (what has already been processed)
    - Table `PROCESSING_LOG_FILE` in MariaDB

```
[root@NG-SCREENER translators]# ngadmin data_launchInitialProcessing -h
data_launchInitialProcessing
start the initial procesing
Parameter  Required  Description
wait       false     Wait for end of job
```

Appliance Administration

Side note on MariaDB

- Used to store application data
  - Also stores NG|Case Manager DB
- Persistant data (needs to be backup)
- Accessible by:
  - `mysql`
  - `connect ngscreener;`
  - `SHOW TABLES;` (To show tables in DB)

- Example of data stored:
  - Roles on NG|Screener UI
  - Control definitions
  - Realtime Analysis policies

Ngadmin tool

- `data_removeEntries`
  - Delete data from NG|Storage
    - Data still present in log-collector
    - Reloaded when executing `data_launchInitialProcessing`
  - If data not present in log-collector, `data_removeEntries` will not delete data

```
[root@NG-SCREENER translators]# ngadmin data_removeEntries -h
data_removeEntries
Remove data from NgStorage
Parameter  Required  Description
f          false     The date pattern to select data to clean. Format dd-mm-yyyy
force      false     Skip confirmation
o          false     The hostPattern pattern to select data to clean. Default value: *
s          false     The service pattern to select data to clean. Default value: *
t          false     The date pattern to select data to clean. Format dd-mm-yyyy
```

Appliance Administration

Ngadmin tool

- `data_sanitize`
  - Sanitize data by synchronizing NG|Storage and data in log-collector
    - Remove from NG|Storage data not present in log-collector

```
[root@NG-SCREENER translators]# ngadmin data_sanitize -h
data_sanitize
Remove data not present in log collector from NG|Storage
Parameter  Required  Description
f          false     The date pattern to select data to clean. Format dd-mm-yyyy
t          false     The date pattern to select data to clean. Format dd-mm-yyyy
```

Appliance Administration

Ngadmin tool

- `data_removeEntries` vs `data_sanitize`

- `data_removeEntries`
  - Will remove data in NG|Storage if data still available in log-collector
    - Clean way to delete data from both NG|Storage and log-collector
      1. Delete from NG|Storage using data_removeEntries
      2. Afterwards, delete data from log-collector

- `data_sanitize`
  - Will take log-collector as reference to synchronize data in NG|Storage
    - Used to clean NG|Storage when the procedure above has not been followed

Appliance Administration

Ngadmin tool

- `util_encodePassword`
  - Encode password to not be readable inside configuration files
  - Use == before value inside configuration file to specify that password is encoded
    - Polling configurations
    - security.conf file (LDAP configuration)

```
[root@NG-SCREENER translators]# ngadmin util_encodePassword -h
util_encodePassword
Encode the password
Parameter  Required  Description
args       true
```

Appliance Administration

Important configuration files

- Could be modified in command line
- Or using Management Center

Appliance Administration

Important configuration files

- `/etc/ng-screener/common/ngStorage.conf`
- Configure data loading in NG|Storage
- Important parameters
  - `ngStorageWindowInDays=365`
    - By default ngStorage will have 365 days of data, need to be modified to set different window
    - `ngadmin data_launchInitialProcessing` to load missing data
  - `ngStorageExcludedServices=service@host`
    - Comma separated list of services to be excluded
    - `data_removeEntries -s service` to clean already loaded data
- Restart of Daemon and UI
- Warning: Only increase NG|Storage window if storage capacity is sufficient
  - ~8 times size in log-collector

Appliance Administration

Important configuration files

- `/etc/ng-screener/daemon/modules/control.conf`
- Configure parameters for control execution
- Important parameters
  - `globalControlTimeout` → Timeout for query execution in milliseconds
  - Option relative to concurrent executions, missed executions, templates, …
- Restart of Daemon

Appliance Administration

Important configuration files

- `/etc/ng-screener/daemon/modules/realtimeAnalysis.conf`
- Configure notification for threshold policies on number of events (Realtime Analysis cf. NG|screener UI admin training)
- Important parameters
  - `Tenant Information` → Always even when only one tenant
  - `config[x].AnalysisCheckInterval` → Interval of checking against threshold
  - `config[x].EmailSubject`
  - `config[x].EmailBody`
  - SMTP configuration parameters
- Restart of Daemon

Appliance Administration

Service Config files

- `/etc/ng-screener/daemon/serviceConfig/`
- Link between syslog-ng and NG|Screener daemon
- One file per service and type of data collection
  - T24 Protocol two different, one for flat file import and another one for polling
- To check when service do not appear in NG|Screener UI
- Important parameters
  - `syslogService_x = <directory name in log-collector>`
    - Can add an entry if needed (have syslogService_1, syslogService_2, etc…)
  - `indexPattern = <BDM index pattern to be used for the service>`
  - `indexGranularity=<day | month | year>`
- Restart of Daemon and UI

Appliance Administration

Syslog-ng Rules

- `/etc/syslog-ng-rules/`
- Syslog-ng rules files
- `/etc/syslog-ng-rules/syslog-ng.conf`
  - Global configuration file, should not be modified
- Rules for handling syslog entries for specific service
  - .root for all services should be present
- Restart of syslog-ng.ngc

Appliance Administration

NG|Storage Configuration file

- `/etc/ng-screener/ngstorage/ngStorage.yml`

- Modification to be done when:
  - NG|Storage to be run as a cluster*
  - Performance tuning of NG|Storage

- Need a restart of `ng-storage` service

* For information about installation on cluster, refer to Cluster Installation chapter in NG|Install guide

Appliance Administration

NG|Processing Configuration files

- `/usr/local/ng-screener/ngprocessing/ngspark/conf/spark-defaults.conf`
  - Spark memory configuration
  - Mesos connectivity
  - ElasticSearch Connectivity
  - …
- `/usr/local/ng-screener/ngprocessing/ngmesos/etc/mesos-slave/resources/mem`
  - Memory that will be allocated to mesos slave for job execution
  - Given in MB
- `/usr/local/ng-screener/ngprocessing/ngmesos/etc/mesos-slave/resources/cpus`
  - Number of CPUs that could be used by mesos slave service
- Side note: Number of parallel executions will depend on `spark.executor.memory`, `spark.executor.cores` as well as previous mesos slave config
  - Example: if `spark.executor.memory=2G`, `spark.executor.cores=2` and we have mesos mem → 6000 and cpus → 6
    - 3 parallel execution will be possible

Appliance Administration

Multi Tenancy Configuration

- NG|Screener (starting with V7.1) is always multi-tenant
  - DEFAULT tenant on a single tenant configuration
  - Will make changes on Data collection and Reference Data
    - Need to specify the tenant (see related slides)

- If new tenant has to be defined
  - Scripts available to define new tenants

Appliance Administration

New Tenant creation

- Execute `createTenant.py` script in `/usr/local/ng-screener/tools/multi-tenancy/`
  - `python createTenant.py -t MYTENANT-u superadmin -p netguardians -url https://demolocal1.netguardians.ch/auth/`
    - -t: name of tenant
    - -u: name of the super admin user
    - -p: password of the super admin user
    - -url: URL for accessing NG|Auth for the tenant (different host each time)
  - Restart needed of `ng-screener` and `ng-screener-ui` (and `case-manager`*)

- `/etc/httpd/conf.d/netguardians.conf` has to be modified as well
  - `ServerAlias NEW_TENANT_DNS_NAME`
  - `RequestHeader set X-NG-TENANTID “MYTENANT" "expr=%{HTTP_HOST} == NEW_TENANT_DNS_NAME’”`
  - Restart of httpd service: `systemctl restart httpd.ngc`

- Add an entry in `/etc/hosts`
  - `IP_OF_MACHINE NEW_TENANT_DNS_NAME`
  - Example: `192.168.56.11 demolocal1.netguardians.ch`

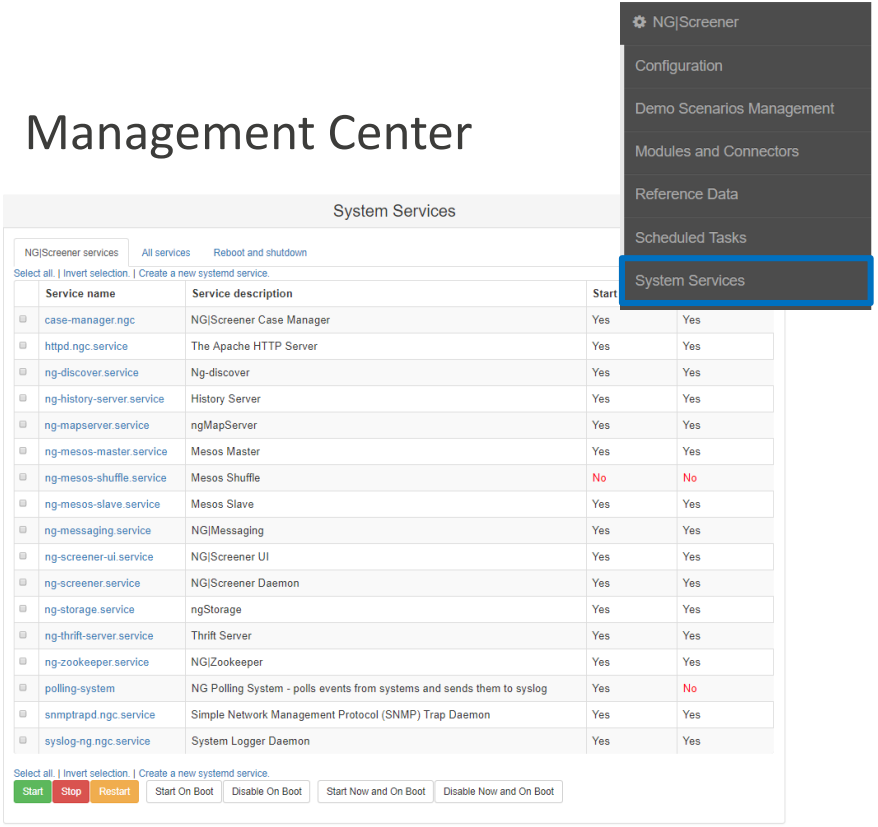
*case manager new tenant creation is not automated at the moment, but will be in next minor release

Appliance Services

Command Line

- Using `systemctl` command
- `systemctl start service_name`
- `systemctl status service_name`
- `systemctl stop service_name`

Management Center



General Services

syslog-ng.ngc Syslog server, central point for data collection and routing

httpd.ngc Http proxy for all web applications

mariadb.ngc Maria DB, use to store meta data for NG|Screener solution and Case Manager DB

Which component (RPM) provides which services?

- ngDaemonDistrib
  - ng-screener
- ngBrowser
  - ng-screener-ui
- ngStorage
  - ng-storage
  - ng-platform
- ngSyslogNg
  - syslog-ng.ngc
- ngMessaging
  - ng-messaging
  - ng-kafka-manager
  - ng-zookeeper
- ngScoringApi
  - ng-scoring-api
- ngScoringApiUi
  - ng-scoring-api-ui
- NgProcessing
  - ng-history-server
  - ng-mesos-master
  - ng-mesos-slave
  - ng-mesos-shuffle
  - ng-thrift-server
- ngCaseManager
  - case-manager
- ngMapServer
  - ng-mapserver
- NgPollingSystem
  - polling-system
- NgManagementCenter
  - Management
- NgAuth
  - ng-screener-auth

Ng-platform service

- Pseudo service for easily restarting platform services without caring about order

- Platform is not all products
  - Storage
  - Messaging
  - Daemon
  - Processing
  - UI

- Normal to not have status running

NgProcessing Services

ng-mesos-master Receive execution requests from the daemon. Will be the one executing the python code.

ng-mesos-slave Present on the master and on each node having ngstorage. Will be doing partial processing of the parent process from the master.

ng-mesos-shuffle Responsible to split the master job to multiple sub-jobs to be dispatched on slaves.

ng-history-server Web UI for tracking completed and running spark applications.

ng-thrift-server Provides JDBC access to SparkSQL (used to fill jasper reports).

NgMessaging Services

ng-messaging Kafka server itself.

ng-kafka-manager Web UI to manage Kafka topics.

ng-zookeeper keep the state of the "zoo". Small service that handle configuration and topology of the Kafka and Mesos cluster (who is master, where are the slaves)

Health Checks

- Check disk usage
  - Partition usage: `df -h`
  - Directories size: `du -h --max-depth=1 /storage`

- CPU and memory usage
  - `top`
  - `ps aux`

Connectors Installation and Update

- Can be done either in command line or using management center

- By command line (as root)
  - Install: `rpm -ivh connector-xyz.rpm`
    - Check if return code = 0 (`command echo $?`)
    - Check if listed in installed rpms (`rpm -qa | grep connector-xyz`)
  - Uninstall: `rpm -e connector-xyz`
  - Update
    - Uninstall old version then install new

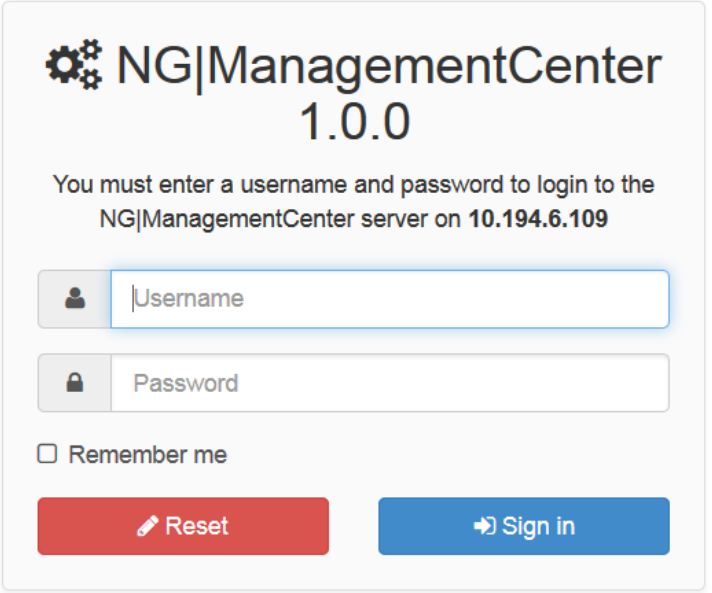
NetGuardians

Management Center

swiss made software

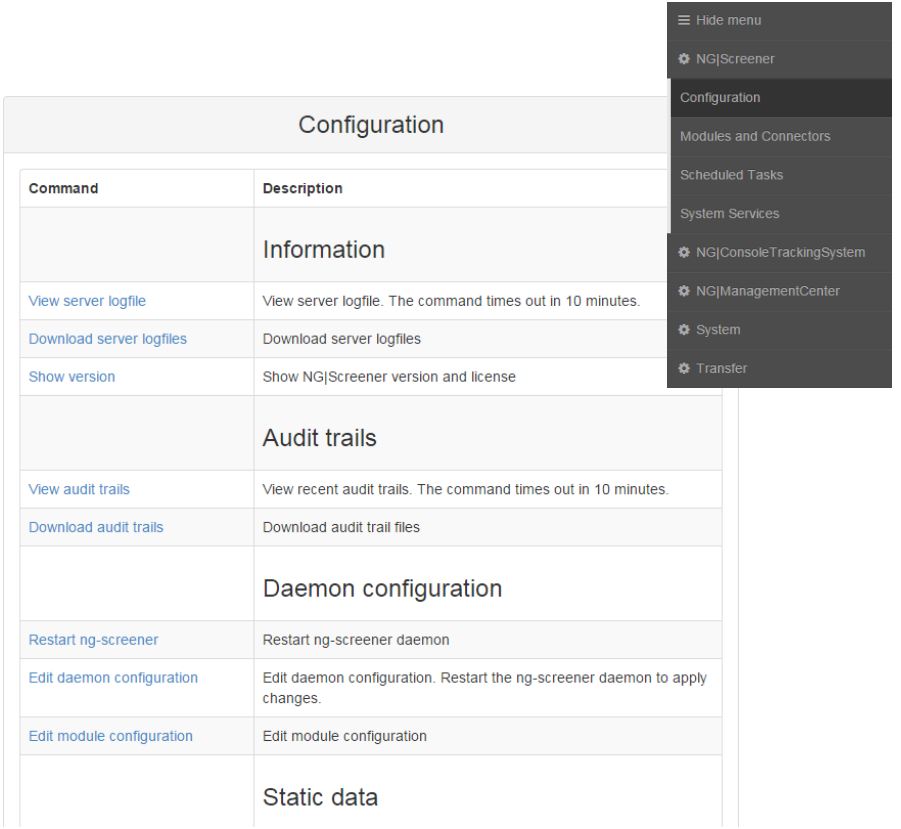
Accessing Management Center

- Web Interface for management
- https://NG_SCREENER_IP/mc/
- Default credentials
  - User: admin
  - Password: netguardians



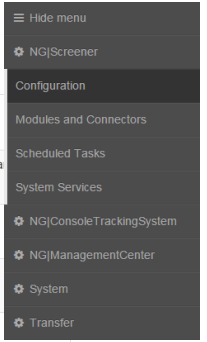
MC – NG|Screener Configuration

- Information:
  NG|Screener logs and status
- Audit trails:
  Collected audit trails
- Daemon configuration:
  NG|Screener restart and advanced tweaking



MC – NG|Screener Configuration

- Reference data:
  Reference data file editing
- Polling:
  Status of polling and definition of polling targets
- Custom scripts:
  Process automation script definition (cf. Automation training)
- **Maintenance:**
  Backup creation and other maintenance activities



	Reference Data
Edit cache configuration	**Edit cache configuration**. Reload Reference Data module or restart daemon to apply cha To delete a cache configuration, edit it and delete all content from the file.
Add cache configuration	Add cache configuration with sample parameters. Then edit the cache configuration to adapt to your need.
List cache entries	List entries of cache. Number of entries displayed are limited to accelerate the loading process.
	Polling
Show polling status	Show polling status
Edit polling target	**Edit polling target**. Restart the ng-screener daemon to apply changes. To delete a target, edit it and delete all content from the file.
Add polling target	Add polling target. Restart the ng-screener daemon to apply changes.
	Custom scripts
Edit custom script	**Edit custom script**. To delete a script, edit it and delete all content from the file.
Add custom script	Add custom script
	Maintenance
Backup	Creates a backup file
Reset search index	Recreate full-text search index database. While recreating the database, text searches performed on NG|Browser will return only partial results. This operation can take a long time.

NetGuardians

NG|Storage Administration

swiss made software

Overview

- NG|Storage provides a REST API
- Can be queried using `curl` command
  - Only from localhost
- A web UI is provided to perform some administration tasks
  - NG|Storage Admin

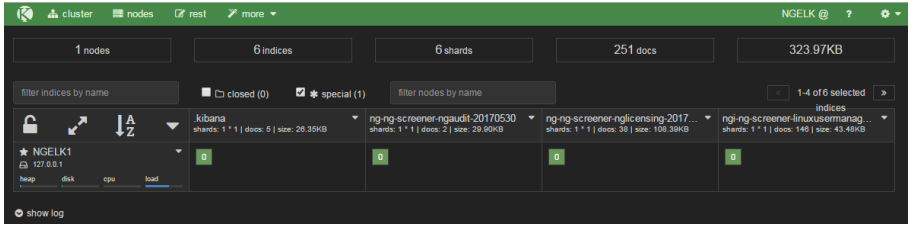
Health Check – Command line

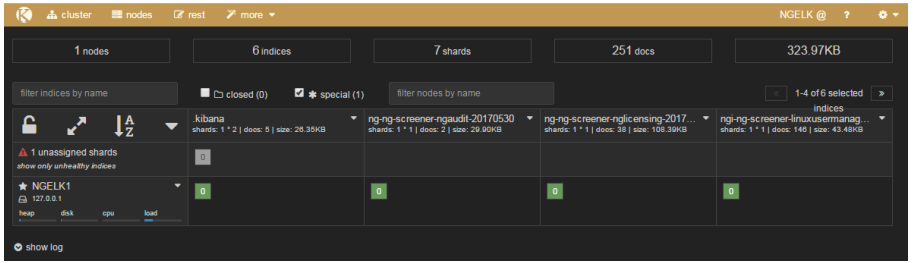
- curl command can be used to check health of cluster
  - `curl -XGET 'http://localhost:9200/_cluster/health?pretty=true'`

```
{
        "cluster_name" : "NGELK",
        "status" : "green",
        "timed_out" : false,
        "number_of_nodes" : 1,
        "number_of_data_nodes" : 1,
        "active_primary_shards" : 6,
        "active_shards" : 6,
        "relocating_shards" : 0,
        "initializing_shards" : 0,
        "unassigned_shards" : 0,
        "delayed_unassigned_shards" : 0,
        "number_of_pending_tasks" : 0,
        "number_of_in_flight_fetch" : 0,
        "task_max_waiting_in_queue_millis" : 0,
        "active_shards_percent_as_number" : 100.0
}
```

Health Check – Web UI

- KOPF can be used to check health of cluster as well
- Accessible through NG|Screener UI only to admin users
- The color of top menu = status of cluster





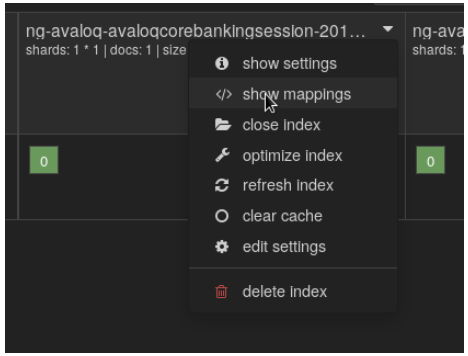
Query NG|Storage with curl

- Query data for administrative purpose can be done either with
  - NG|Discover (cf. NG|Discover training)
  - curl in command line (REST API)

- Example using curl
  - ```
    curl -XPOST 'http://localhost:9200/ngt-*/_search?pretty=true'
    -d '
        { "from" : 0,
          "size" : 1,
          "query": { "prefix": { "business_reference" : "FT" } }
        }'
    ```
    ```

NG|Storage Admin UI

- NG|Storage Admin offers easy way to perform common tasks
  - Show mappings of index
  - refresh index
    - Usually automatically refreshed every 30 seconds
  - Edit some settings of index (number of replicas for example)
  - Delete index



- Warning: NG|Screener keeps metadata regarding loading in NG|Storage → Deleting index directly from NG|Storage Admin will not delete metadata
  - Use `ngadmin` command `data_removeEntries` for clean remove

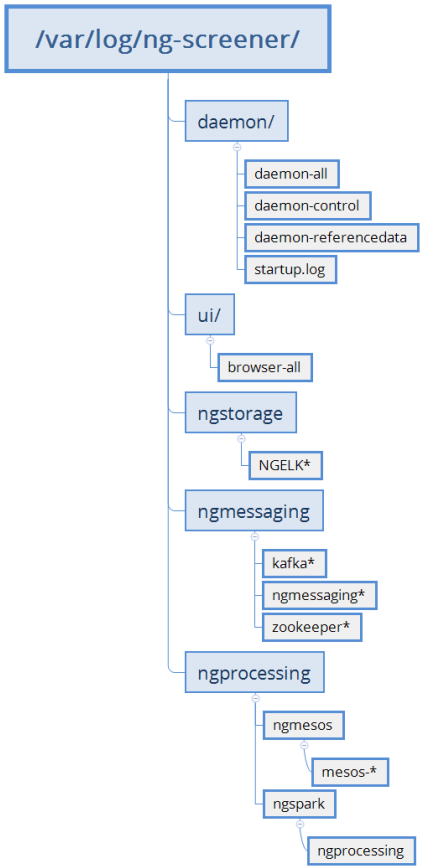
NetGuardians

Troubleshooting

swiss made software

Application Log Files

- NG|Screener Daemon
  - `/var/log/ng-screener/daemon/`
- NG|Screener UI
  - `/var/log/ng-screener/ui/`
- NG|Storage
  - `/var/log/ng-screener/ngstorage/`
- NG|Messaging
  - `/var/log/ng-screener/ngmessaging/`
- NG/Processing
  - `/var/log/ng-screener/ngprocessing/`



Application Log Files – Most common cases

- When UI issues:
  - `/var/log/ng-screener/ui/browser-all.log`
- Data feeding and general processing:
  - `/var/log/ng-screener/daemon/daemon-all.log`
  - `/var/log/ng-screener/ngstorage/NGELK.log`
  - `/var/log/ng-screener/ngmessaging/kafka-server.log`
- Control execution:
  - `/var/log/ng-screener/daemon/daemon-all.log`
  - `/var/log/ng-screener/ngprocessing/ngmesos/mesos-master.ERROR`
  - `/var/log/ng-screener/ngprocessing/ngspark/ngprocessing.log`

Other solution Log Files

- Polling System
  - `/var/log/ng-screener/polling-system/`
- NG|Case manager
  - `/var/log/ng-screener/case-manager.log`

Useful Tools

- Check if a port is open
  - `telnet <IPADDR> <PORT>`
  - If could connect, port is closed

- Check messages exchange
  - tcpdump
    - `tcpdump -i eth0 -vvv -s 65535 -w /home/admin/MyCaptureFile.pcap host 1.2.3.4` (write to file for analysis with wireshark)
    - `tcpdump -i eth0 -s0 -n -X -vvv port 389` (decode ldap packets)
    - `man tcpdump` for more informations

- Check connection to Database and execute queries
  - jisql tool
  - Available in `/usr/local/ng-screener/tools/jisql.zip`

Useful Tools

- Jisql example
  - Unzip in `/home/admin/`
  - Move inside directory
  - Example command to connect to Oracle DB
    - ```
      java -classpath lib/jisql.jar:lib/jopt-simple-3.2.jar:lib/javacsv.jar:/usr/local/ng-screener/lib/ojdbc6-11.2.0.3.jar com.xigole.util.sql.Jisql -formatter csv -user system -password netguardians -driver oracle.jdbc.driver.OracleDriver -c \; -cstring jdbc:oracle:thin:@//10.194.6.92:1521/ORCL
      ```
  - Best to put this line in shell script, to be found easily
      ```

Useful Tools

- Check LDAP settings
  - ldapsearch tool
    - `ldapsearch -x -D "ngscreener@corp.netguardians.ch" -W -H ldap://10.194.6.51 -b "dc=corp,dc=netguardians,dc=ch“`

    - `-x: Simple Authentication Mode`
    - `-D: user to bind to LDAP`
    - `-W: Ask for password`
    - `-H: LDAP Host (using default port 389)`
    - `-b: Base DN`

Useful Tools

- Check Data collection with Kafkacat
  - `/usr/local/ng-screener/tools/kafkacat -C -b 127.0.0.1 -t ng-syslogEvents -z snappy`
  - Enables to have a look directly at the flow of events coming into the solution
  - In addition to checking event coming into the log-collector, this will be second check of data collection mechanism

Useful GUI

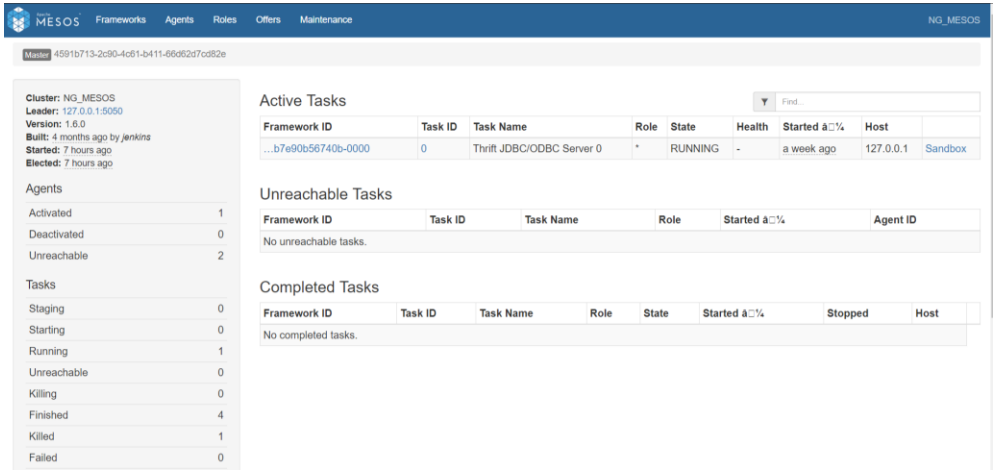
- Mesos Console
  - Monitor Control execution
  - See available resources

Active Tasks

Framework ID	Task ID	Task Name	Role	State	Health	Started	Host	
…66d62d7cd82e-0004	0	control_93_2068 0	*	STAGING	-		127.0.0.1	Sandbox
…b7e90b56740b-0000	0	Thrift JDBC/ODBC Server 0	*	RUNNING	-	a week ago	127.0.0.1	Sandbox

Resources

	CPUs	GPUs	Mem	Disk
Total	7	0	6.8 GB	43.8 GB
Allocated	1	0	512 MB	0 B
Offered	0	0	0 B	0 B
Idle	6	0	6.3 GB	43.8 GB



Troubleshooting Method

- Most Important thing
  - Follow the flow of data
  - Always look at the logs
    - At startup
    - During execution of specific action
  - Try understanding the logs
    - Sometimes useful information is provided (bad credentials, file does not exist, …)
      - See if it is related to your issue or not (Do not focalize on first error in logs)
    - Google can be used, sometimes error is not NG|Screener specific
      - For example when doing polling configurations, common errors will be DB specific errors and not NG|Screener errors

Support Contact Prerequisites

- When contacting support, please provide
  - Logs related to issues (cf. log files)
  - Clear description of the problem
  - Actions that lead to issue

Final note

- Refer to NG|Screener Administration Guide for further information and details.

THANK YOU!

Contact us

+41 24 425 97 60

info@netguardians.ch

www.netguardians.ch

Linkedin.com/company/netguardians

Facebook.com/NetGuardians

@netguardians

https://www.youtube.com/netguardians

NetGuardians Headquarters

Y-Parc, Av. des Sciences 13
1400 Yverdon-les-Bains
Switzerland

T +41 24 425 97 60
F +41 24 425 97 65

NetGuardians Africa

KMA Centre , 7th floor,
Mara Road Upper Hill,
Nairobi, Kenya

T +254 204 93 11 96

NetGuardians Asia

143 Cecil Street
#09-01 GB Building
069542 Singapore

T +65 6224 0987

NetGuardians
Eastern Europe

Koszykowa 61, 00-667
Warsaw, Poland

NetGuardians Germany

Rhein-Main Gebiet
Germany

T +49 172 3799003