VOSS

# Dashboard and Arbitrator Maintenance and Upgrade Guide

Jul 01, 2021

## Legal Information

Please take careful note of the following legal notices:

-
- VOSS, VisionOSS and VOSS-4-UC are trademarks of VisionOSS Limited.
- No part of this document may be reproduced or transmitted in any form without the prior written permission of VOSS.
- VOSS does not guarantee that this document is technically correct, complete, or that the product is free from minor flaws. VOSS endeavors to ensure that the information contained in this document is correct, whilst every effort is made to ensure the accuracy of such information, VOSS accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.
- This document is used entirely at the users own risk. VOSS cannot be held responsible or liable for any damage to property, loss of income, and or business disruption arising from the use of this document.
- The product capabilities described in this document and the actual capabilities of the product provided by VOSS are subject to change without notice.
- VOSS reserves the right to publish corrections to this document whenever VOSS deems it necessary.
- All vendor/product names mentioned in this document are registered trademarks and belong to their respective owners. VOSS does not own, nor is related to, these products and vendors. These terms have been included to showcase the potential of the VOSS solution and to simplify the deployment of these products with VOSS should you select to utilize them.

## Security Information

This product may contain cryptographic features that may be subject to state and local country laws that govern the import, export, transfer and use of such features. The provision of this software does not imply that third-party authorization to import, export, distribute or use encryption in your particular region has been obtained. By using this product, you agree to comply with all applicable laws and regulations within your region of operation. If you require further assistance, please contact your dedicated VOSS support person.

# Contents

# 1. Troubleshooting the Dashboard

## 1.1. Add Mongo as a Datasource on Dashboard server

In some deployments when going to add VOSS-4-UC as a data source, in the drop down list Mongo will be missing.

To rectify this:

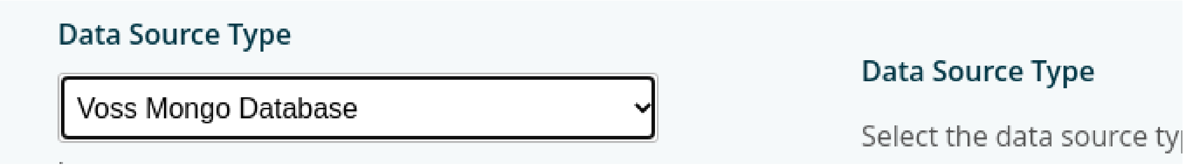
1. Log in to CLI as root
2. Run the following

```
cp -v /etc/lxt/voss4uc/Lxt/lxt-datasource-types/voss-mongo.lxt-datasource-type /
↪var/www/api/Lxt/lxt-datasource-types/
```

3. Restart apache

```
sv restart apache
```

4. Now go back to the gui and check datasources, ensure you see Mongo Datasource in the list.



Data Source Type

Voss Mongo Database

Data Source Type

Select the data source ty

## 1.2. Arbstats dashboard Recovery

1. Log in to CLI as root
2. Run the following command

```
/usr/share/bin/runsv_kill.sh zoom_check
```

## 1.3. Broken Arbitrator stats fix

Usually if it isn't working when you run **ps axfw**, you will see this process stuck:

```
/var/www/api/zoom/zoom_check.php
/var/www/api/zoom/configs/LXT_Stats_AnalytiX.json
```

1. Log in to CLI as root
2. Run:

```
rm -f /var/www/api/lxt_api_staging/datasource/
↪NCF09REOSJTKVN0T1556654742966FPPHHMCNC1W7DP.lxt-datasource
rm -f /var/www/api/datasource/NCF09REOSJTKVN0T1556654742966FPPHHMCNC1W7DP.lxt-
↪datasource

/usr/share/bin/runsv_kill.sh zoom_check
```

So, we are just removing the data source if it is there and then killing the stuck zoom process

You can manually try to run it with:

```
/var/www/api/zoom/zoom_check.php
/var/www/api/zoom/configs/LXT_Stats_AnalytiX.json
```

That will kick off the arbitrator stats collection manually.

## 1.4. The system Index file is corrupted

System Impact – **Critical**

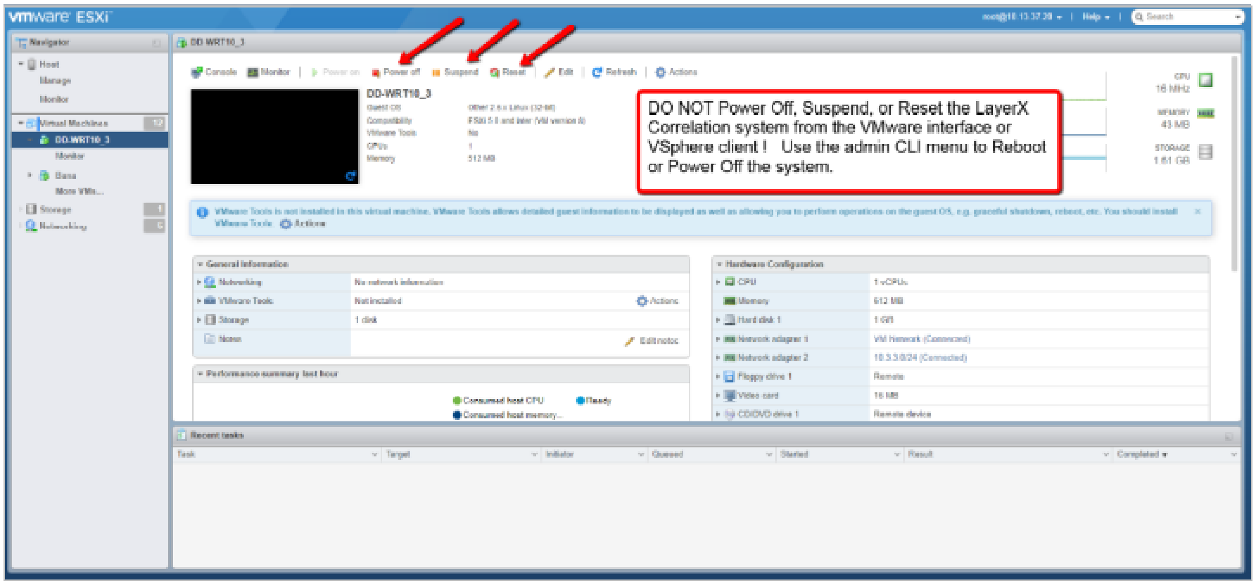
### 1.4.1. About the system Index file

The Index file in the Dashboard/Reporting server is the main text file that contains all logs forwarded from Correlation servers and logs sent directly to the system listeners (Netflow). It is the main archive of raw log data, and rotates as it archives from a "hot bucket" to a "cold bucket" The current Index that is being written in the system is the "hot bucket", while archived Indexes are "cold" and no longer actively being appended. The Index file that is affected in the problem description is the current "hot" or active Index file.

### 1.4.2. How the Index becomes corrupted

The Index becomes corrupted when either the Virtual Machine is improperly shut down in the VMWare management interface, or the VMWare host has an issue that removes CPU or disk resources from the system while it is writing to the file.

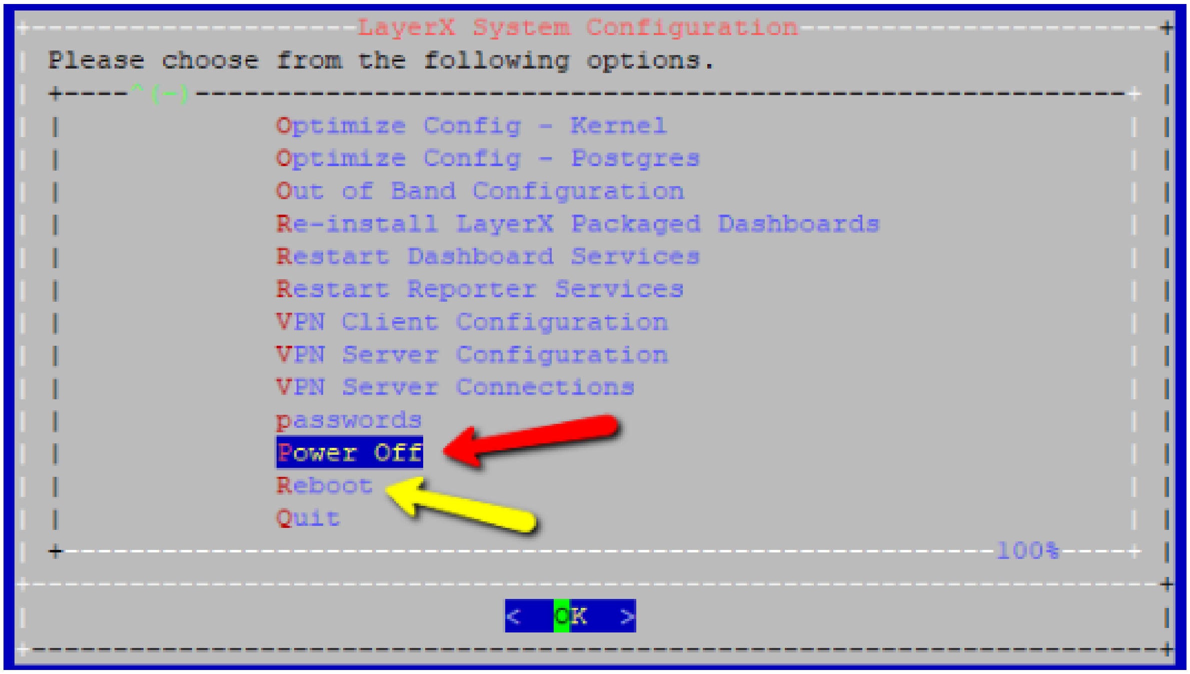
Do NOT Power Off, Suspend, or Reset the VOSS Correlation system from the VMWare management interface!



DO NOT Power Off, Suspend, or Reset the LayerX Correlation system from the VMware interface or VSphere client ! Use the admin CLI menu to Reboot or Power Off the system.

### 1.4.3. How to properly reboot or power off the system

1. To properly power off or reboot the Dashboard/Reporting system, ssh to the system and login as the “admin” user to access the admin CLI menu.
2. From the Main Menu, use the arrow keys to navigate down to the **Power Off** and **Reboot** menu options. These operations will properly stop the system services and close the Index file so that it does not become corrupted when rebooting or shutting down the system.



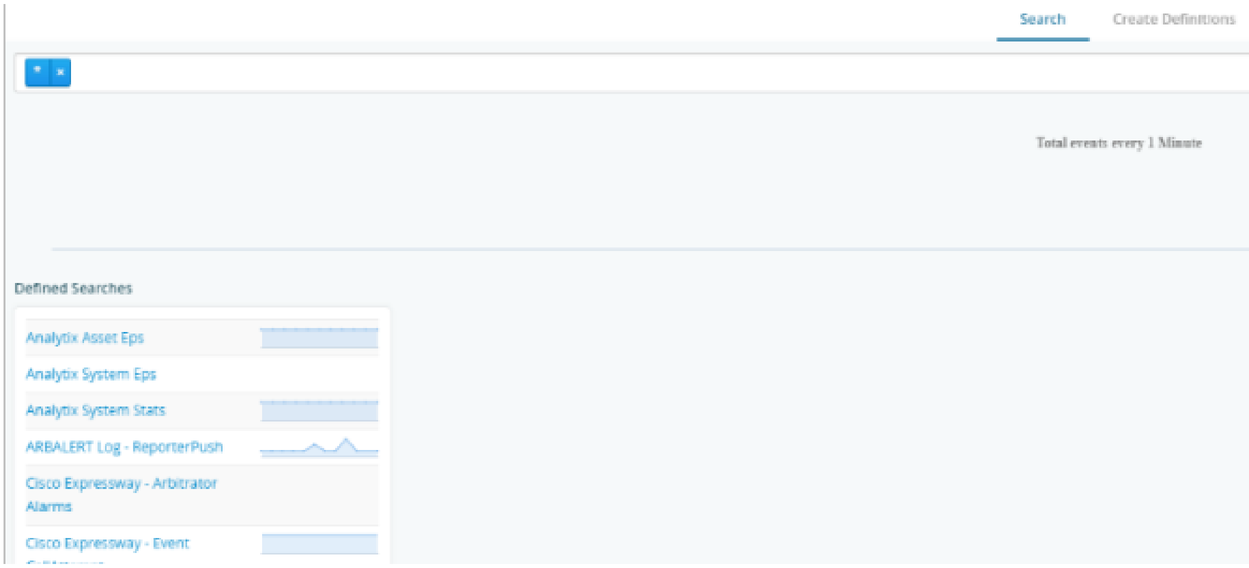
```
+--------------------LayerX System Configuration---------------------+
| Please choose from the following options.                           |
| +----^(-)---------------------------------------------------------+ |
| |              Optimize Config - Kernel                           | |
| |              Optimize Config - Postgres                         | |
| |              Out of Band Configuration                          | |
| |              Re-install LayerX Packaged Dashboards              | |
| |              Restart Dashboard Services                         | |
| |              Restart Reporter Services                          | |
| |              VPN Client Configuration                           | |
| |              VPN Server Configuration                           | |
| |              VPN Server Connections                             | |
| |              passwords                                          | |
| |              Power Off                                          | |
| |              Reboot                                             | |
| |              Quit                                               | |
| +-------------------------------------------------------100%------+ |
+---------------------------------------------------------------------+
|                             <  OK  >                                |
+---------------------------------------------------------------------+
```

### 1.4.4. Symptoms of a corrupted Index

If the index is corrupted no new data can be written into the system. From the Dashboard Server GUI use the Search interface to look at the Index . When the index is corrupted the Search interface will return no data and look blank since the corrupted index cannot be read or accessed.

Side effects of a corrupted Index are no Search definitions will match data during the time frame that the Index is corrupted. This means there will be gaps in Dashboard data for widgets that utilize those Search definitions.

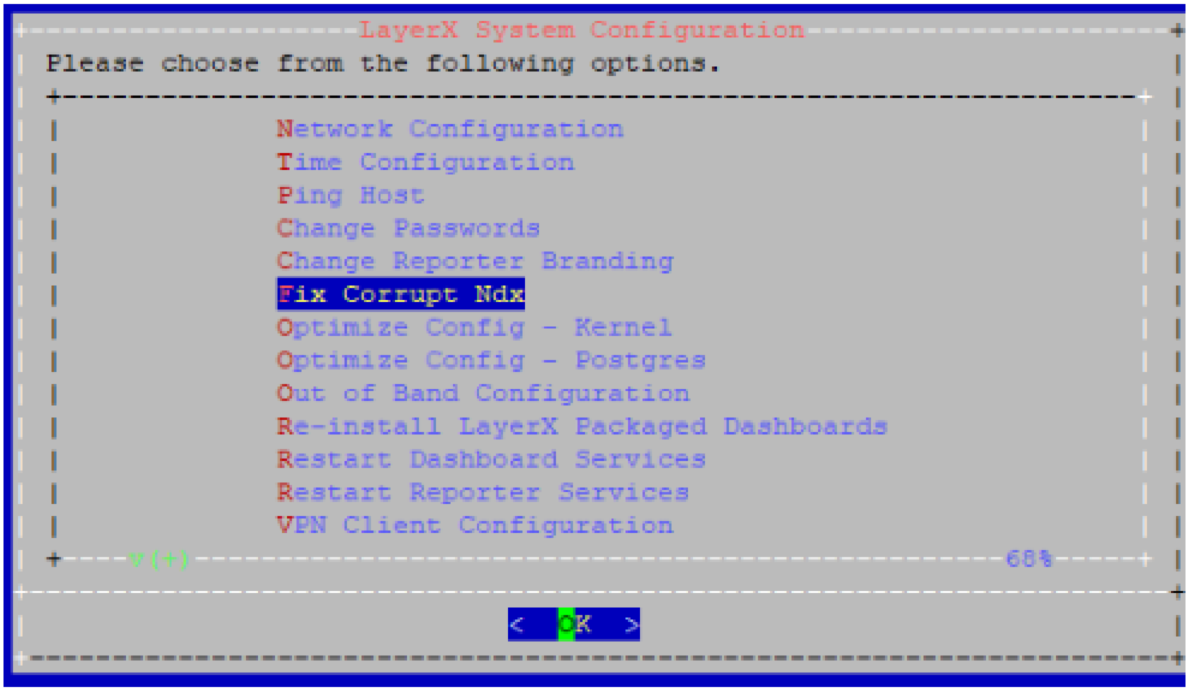
Example of a blank Search screen as a result of a corrupted index:



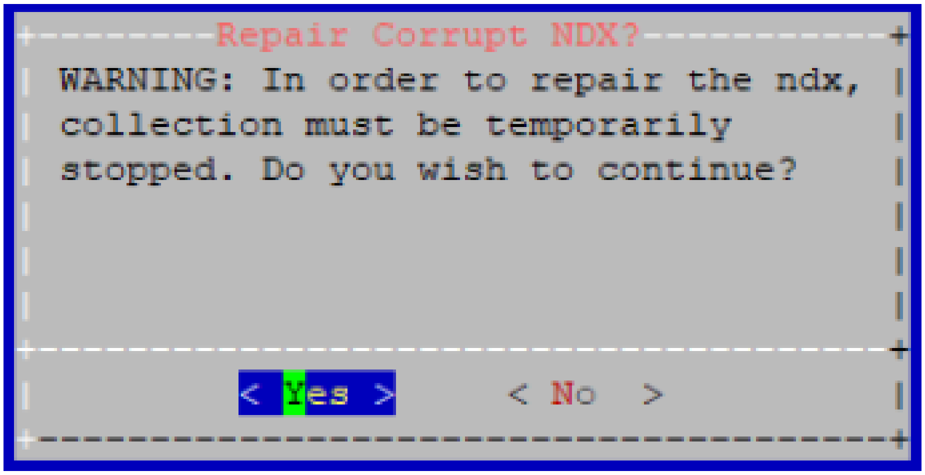
Analytix Asset Eps
Analytix System Eps
Analytix System Stats
ARBALERT Log - ReporterPush
Cisco Expressway - Arbitrator Alarms
Cisco Expressway - Event

### 1.4.5. How to repair a corrupted Index file and restore operation

1. To properly repair the Index in the Dashboard/Reporting system, ssh to the system and login as the “admin” user to access the admin CLI menu.
2. Use the arrow keys to navigate to the **Fix Corrupt Ndx** menu option. Confirm the prompt to proceed.



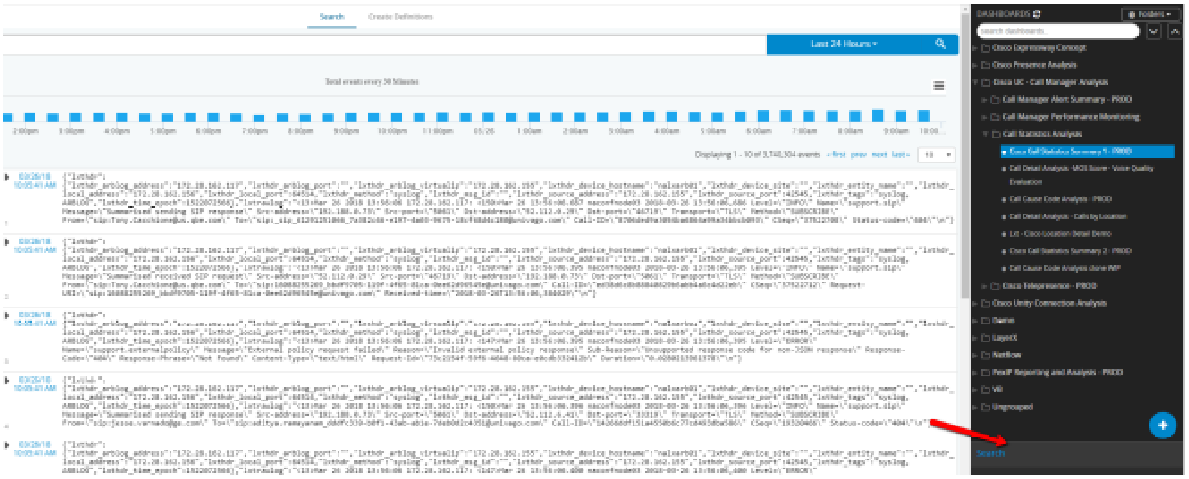
```
LayerX System Configuration
Please choose from the following options.

        Network Configuration
        Time Configuration
        Ping Host
        Change Passwords
        Change Reporter Branding
        Fix Corrupt Ndx
        Optimize Config - Kernel
        Optimize Config - Postgres
        Out of Band Configuration
        Re-install LayerX Packaged Dashboards
        Restart Dashboard Services
        Restart Reporter Services
        VPN Client Configuration
  v(+)                                        68%

                    <  OK  >
```



```
Repair Corrupt NDX?
WARNING: In order to repair the ndx,
collection must be temporarily
stopped. Do you wish to continue?

      < Yes >      < No  >
```

The system will indicate that services are stopping and the index repair is proceeding. Upon completion it will return to the admin menu.

3. Use the Search interface in the GUI to validate that new logs are being written into the new Index “hot” bucket. The blue graph at the top of the Search interface is an indicator of log events being written into the Index in that time frame.


Search
Create Definitions
Last 24 Hours
Total events every 30 Minutes
2:00pm
3:00pm
4:00pm
5:00pm
6:00pm
7:00pm
8:00pm
9:00pm
10:00pm
11:00pm
03/26
1:00am
2:00am
3:00am
4:00am
5:00am
6:00am
7:00am
8:00am
9:00am
10:00
Displaying 1 - 10 of 3,740,304 events
« first prev next last »
10
DASHBOARDS
Folders
search dashboards...
Cisco Expressway Concept
Cisco Presence Analysis
Cisco UC - Call Manager Analysis
Call Manager Alert Summary - PROD
Call Manager Performance Monitoring
Call Statistics Analysis
Cisco Call Statistics Summary 1 - PROD
Call Detail Analysis- MOS Score - Voice Quality Evaluation
Call Cause Code Analysis - PROD
Call Detail Analysis - Calls by Location
LX - Cisco Location Detail Demo
Cisco Call Statistics Summary 2 - PROD
Call Cause Code Analysis clone IMP
Cisco Telepresence - PROD
Cisco Unity Connection Analysis
Demo
LayerX
Netflow
PexIP Reporting and Analysis - PROD
VB
Ungrouped
Search

## 1.5. Drop Tables to free up Disk

1. Find the tables with the biggest in size

```
/usr/share/bin/dbTableSizes.v2.sh
```

2. This will display largest tables at the top. Take note of the name and the date in the table name. When you are ready to drop some tables, run the following command:

```
/usr/share/bin/dropTables.sh <Table name> <Table date - YYYY_MM>
```

   This command simply prints the psql commands and the table names. It does not actually do any deletes yet. Confirm the list is what you want. If not adjust search and date accordingly.

3. Final command to commit delete is same command with `| psql ReporterServices`.

## 1.6. Retrieve Dashboards

There isn't a way from the UI but you can see the files on the backend.

1. Run

```
cd /var/www/api/dashboards
```

   Here you will find a list of userids.

2. Run the following script to get the id of the user. Change "admin" to the userid of the person u want to see.

```
/usr/share/amfphp/services/lxt/bin/getLdapUser.php admin

a05818[...]
```

3. Then you can **cd** into

```
/var/www/api/dashboards/a05818[...]
```

You are now in the user dashboard directory.

4. Then you can run this to see all the dashboard names and guids. The guid is the same as the filename.

```
jq '{name:.name,guid:.guid}' *
```

This will print out something like this:

```
{
  "name": "Voss Customer Overview",
  "guid": "UFY1XV[...]"
}
```

5. Then copy the dashboards:

```
cp UFY1XV[...].lxtdashboard <destination>
```

## 1.7. Sync dashboards using CLI

If there are multiple users and dashboards sometimes this can have a detrimental effect on the dashboard server and cause Error 500 within the GUI when trying to sync dashboards to users.

A workaround is to identify the dashboards required and set up a script to sync them in the CLI

1. Create a PHP script at root in the CLI or copy ones from the files section and edit

```
#!/usr/bin/php
<?php

require_once("/usr/share/amfphp/services/Lxt/Lxt.php");
\Lxt\Lxt::registerAutoloader();
use \Lxt\Api\Model\LxtFieldConstants as LxtFieldConstants;
$model = new \Lxt\Api\Model\LxtDashboardGroupModel();
if ($argc > 1)
{
    $dusername = $argv[1];
}
else
{
    printf("Please provide destination user id\n");
    exit(1);
}
$directory = "/var/www/api/dashboard_groups";
$userid = trim(`/usr/share/amfphp/services/lxt/bin/getLdapUser.php admin`);
$dest_userid = trim(`/usr/share/amfphp/services/lxt/bin/getLdapUser.php
↪$dusername`);
if (empty($dest_userid))
{
    printf("Unable to find userid: $dusername\n");
    exit(1);
}
$dg = array("A5A4R6YE74BRW08J1600705040082MI1SXXGPC7XDSU");   (Edit this line␣
↪with the folder id that contains the dashboards to sync)
```

(continues on next page)

(continued from previous page)

```
$allgroups = array();
foreach ($dg as $guid)
{
    $newgroup = new \stdclass();
    $newgroup->name = "";
    $newgroup->guid = $guid;
    $allgroups[] = $newgroup;
}
foreach ($dg as $guid)
{
    $groups = array();
    $groups = $model->getChildDashboardGroups($userid, $directory, $guid);
    foreach ($groups as $group)
    {
        $newgroup = new \stdclass();
        $newgroup->name = $group->name;
        $newgroup->guid = $group->guid;
        $allgroups[] = $newgroup;
    }
}
$model->syncGroups( $userid, $dest_userid, $directory, $allgroups, true, $error);
$model = null;
?>
```

2. To run the script in CLI

```
./scriptname_sync.php (username of the user to receive the dashboards)
```

## 1.8. Test mail from Dashboard

1. Log in to CLI
2. Run

```
echo "Subject: sendmail test" | sendmail -v Recipent email address
```

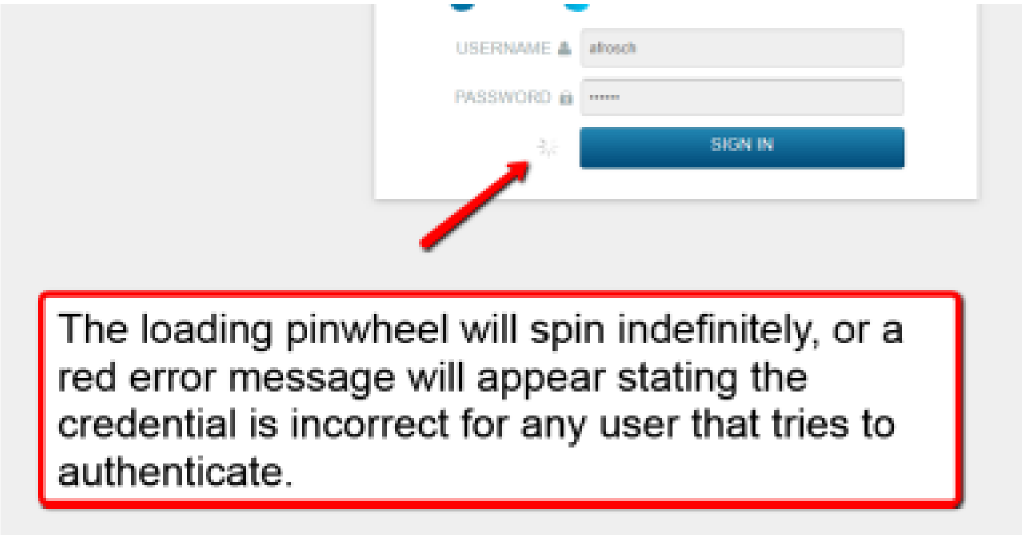
## 1.9. The local OpenLDAP service has stopped

System Impact – Minor

### 1.9.1. Symptoms of a down OpenLDAP service

Local administrative users are created and stored in the instance of OpenLDAP on the Dashboard/Reporting server. If the service is ever stopped, local users cannot authenticate to access the GUI. Users synchronized from a SAML or AD repository are also affected and will not be able to access the GUI.

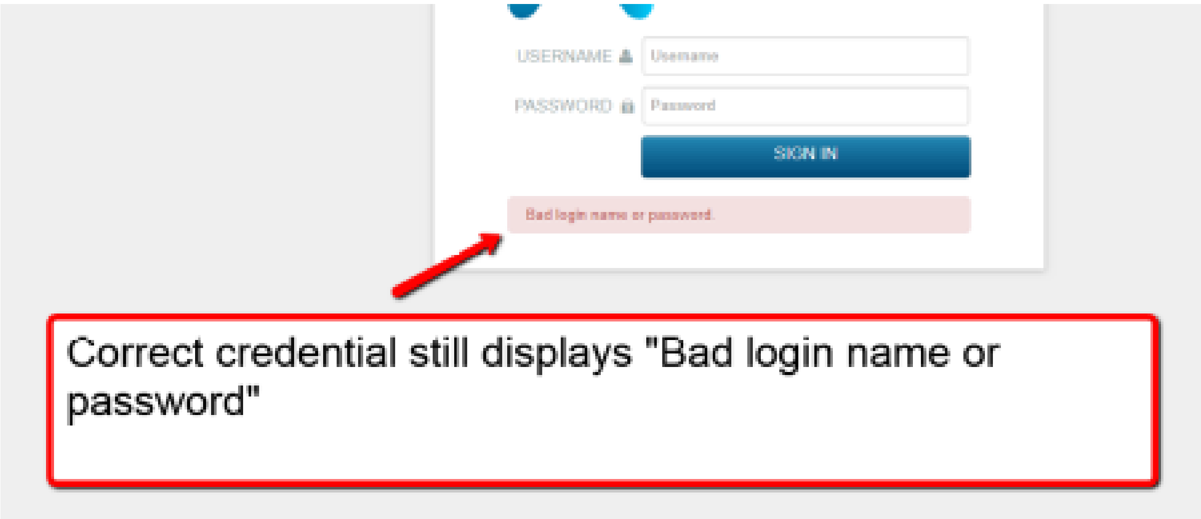
The OpenLDAP service state does not affect normal system processing, so logging and alerting functions will continue.



USERNAME afrosch

PASSWORD ••••••

The loading pinwheel will spin indefinitely, or a red error message will appear stating the credential is incorrect for any user that tries to authenticate.



USERNAME Username

PASSWORD Password

Bad login name or password.

Correct credential still displays "Bad login name or password"

### 1.9.2. How to restore local system authentication for the GUI

The system will need to be restarted from the admin CLI menu to resolve the OpenLDAP issue. Reference the “Corrupted Index” section at the top of this document for system reboot procedures.

## 1.10. The main service (Reporter) is DOWN

System Impact – **Critical**

### 1.10.1. Symptoms of a down Reporter service

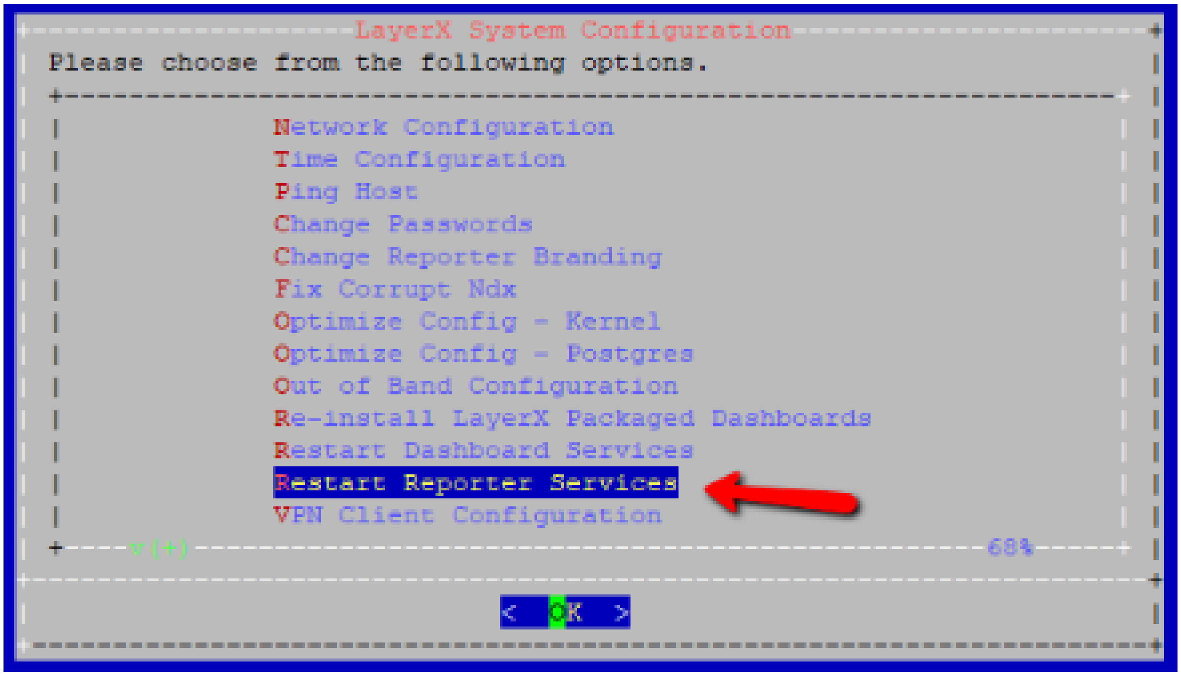
When the Reporter service is down, no new logs or events can be written to the Index. The Search interface will look responsive since the Index is not corrupted. Use the log time stamp to validate that new logs are not being written into the Index.

### 1.10.2. Other side effects of a stopped Reporter process

- Data for Dashboards gathered from Search definitions using logs will have gaps for the time frame that the Reporter service is down
- NetFlow data sent directly to the Dashboard/Reporting server will not be gathered in the time frame that the Reporter service is down.

### 1.10.3. How to restart the Reporter service

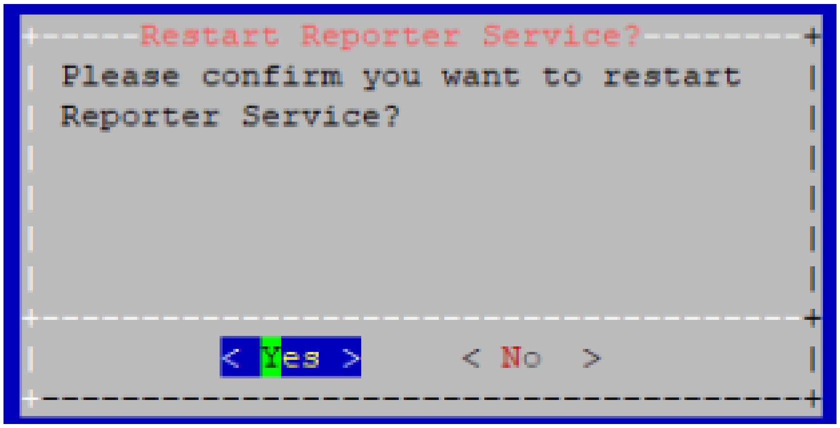
1. To restart the Reporter process in the Dashboard/Reporting system, ssh to the system and login as the “admin” user to access the admin CLI menu. From the Main Menu select use the arrow keys to navigate to the **Restart Reporter Services** menu.



LayerX System Configuration

Please choose from the following options.

2. Select that option to restart the Reporter service. Confirm the operation. Upon completion of the operation the system will prompt the user to hit <Enter> to return to the menu.

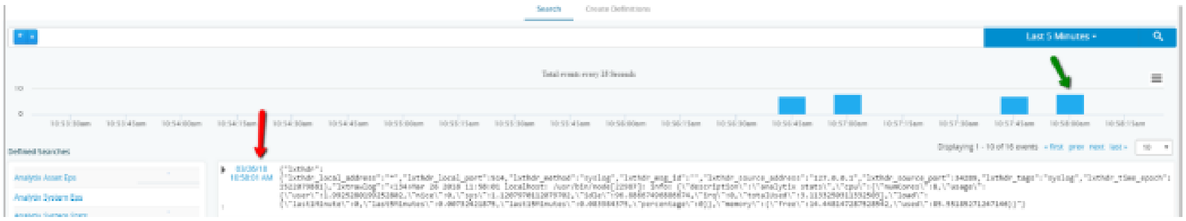


Restart Reporter Service?

Please confirm you want to restart Reporter Service?

We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

3. Use the Search interface in the GUI to validate that new logs are being written into the Index by looking at the log time stamp. The blue graph at the top of the Search interface is an indicator of log events being written into the Index in that time frame.



# 2. Troubleshooting the Arbitrator

## 2.1. Change Policy IRP in Bulk

1. Run the following:

```
psql sca

select "IRP_ID", "IRP_NAME" from "INCIDENT_RESPONSE_PROCEEDURES";

IRP_ID | IRP_NAME
-------+----------------------
6      | Push to Spark
1      | Default IRP
5      | Push to Zenoss Cloud
```

2. Take the `IRP_ID` number next to the Responce Procedure and replace it where `##` is on the next command

```
update "CORRELATION_RULEBASE" set "IRP_ID" = ## WHERE "THREAT_SCORE" = 31;
```

   Example

```
sca=# update "CORRELATION_RULEBASE" set "IRP_ID" = 1 WHERE "THREAT_SCORE" = 31;
```

3. Exit psql and do

```
lxtsv restart arbitrator
```

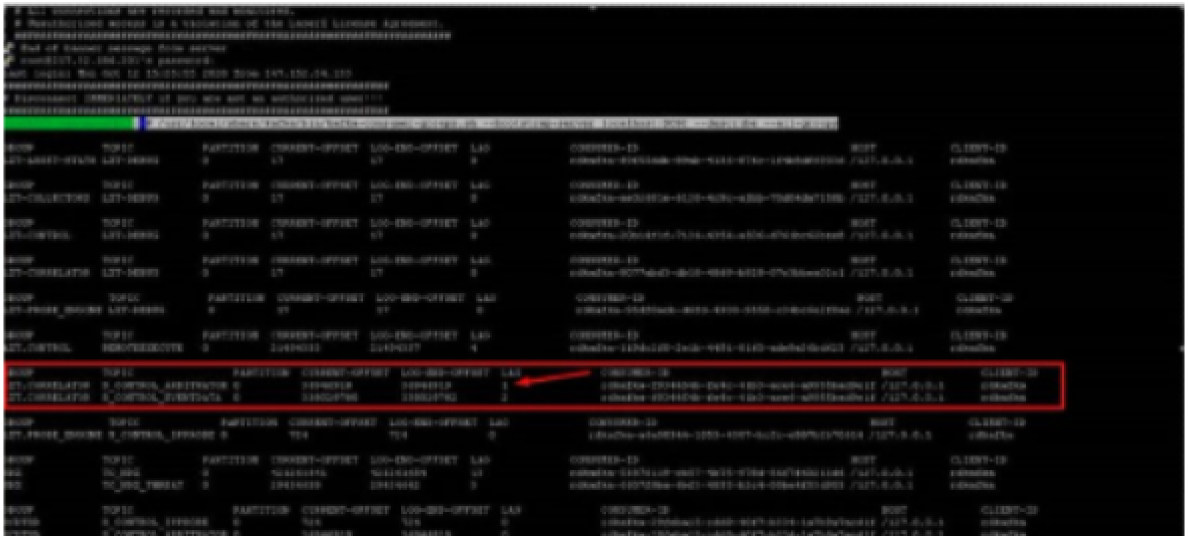
## 2.2. Check Lag on Central Arbitrator

If you are set with multiple arbitrators pushing alerts to a central arbitrator there may be an occasion where alerts do not show in a timely manner on the central arbitrator or the dashboard.

1. Log in to the GUI on the central arbitrator, go to the Config area.
2. Check that this arbitrator only has the catch all policy. If more policies are present then remove them.
3. Log in to the same arbitrator via CLI as root.
4. Run the following command:

```
/usr/local/share/kafka/bin/kafka-consumer-groups.sh --bootstrap-server␣
↪localhost:9092 --describe --all-groups
```

5. This will return the below…



Look at the highlighted box and ensure the lag is less than 2000, run the command a couple more times to check if the number raises and falls.

6. If we see the number only climbing, we need to take action.

Run:

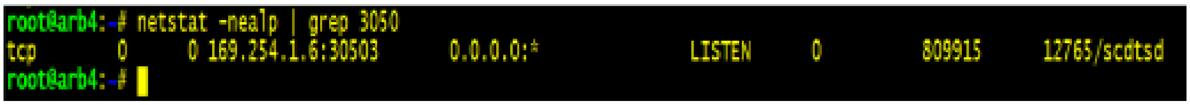
```
monit stop lxt-correlator

/bin/kafka_consumer -g LXT.correlator S_CONTROL_ARBITRATOR >/dev/null

/bin/kafka_consumer -g LXT.correlator S_CONTROL_EVENTDATA>/dev/null

monit start lxt-correlator
```

## 2.3. Check VPN Tunnel Between Arbitrators

1. To test the status go into the Arbitrator as root and run:

```
netstat -nealp | grep 3050
```

This will return the below for the tunnel

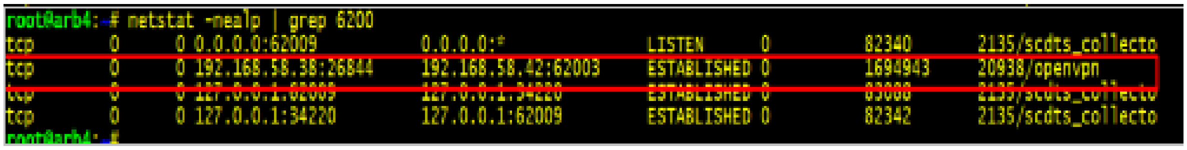


```
root@arb4:~# netstat -nealp | grep 3050
tcp        0      0 169.254.1.6:30503       0.0.0.0:*               LISTEN      0          809915      12765/scdtsd
root@arb4:~# 
```

2. Then run

```
netstat -nealp | grep 6200
```

This will return the below for the TLS connection



```
root@arb4:~# netstat -nealp | grep 6200
tcp        0      0 0.0.0.0:62009           0.0.0.0:*               LISTEN      0          82340      2135/scdts_collecto
tcp        0      0 192.168.58.38:26844     192.168.58.42:62003     ESTABLISHED 0          1694943    20938/openvpn
tcp        0      0 127.0.0.1:62009         127.0.0.1:34220         ESTABLISHED 0          [illegible]      2135/scdts_collecto
tcp        0      0 127.0.0.1:34220         127.0.0.1:62009         ESTABLISHED 0          82342      2135/scdts_collecto
root@arb4:~#
```

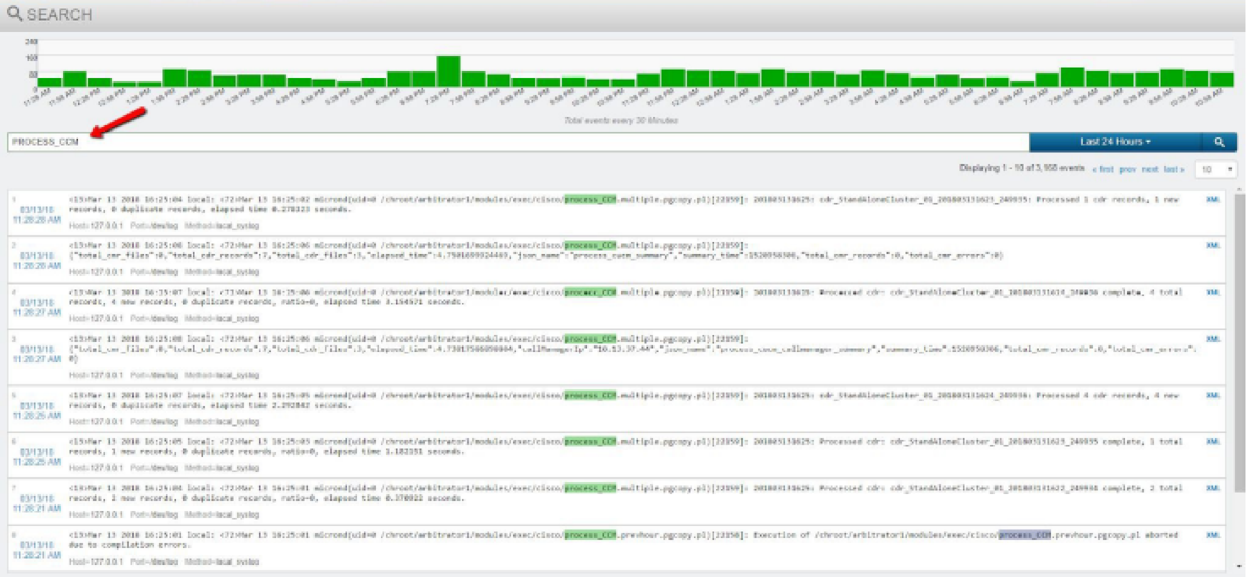
# 2.4. Cisco CDR processing appears to have stopped

System Impact – **Minor**

## 2.4.1. Symptoms that CDR ingestion appears to have stopped

The system will write a log in the Index as it processes CDR files. The log can be found in the Search interface using a keyword search for `PROCESS_CCM`. Look at the time stamp of the last CDR processing log as an indicator of when a CDR record was last processed in the system.

CDR files should be received and processed every 5 minutes maximum, but that can depend on the configured interval on the CUCM for sending CDR records. The system will constantly check for new CDR files to ingest into the system.

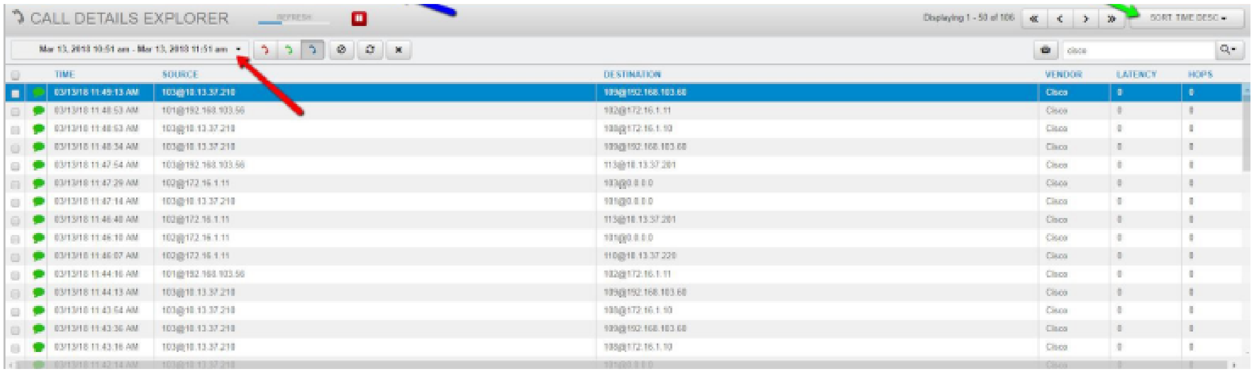


SEARCH
Total events every 30 Minutes
PROCESS_CCM
Last 24 Hours ▾
Displaying 1 - 10 of 3,168 events
« first prev next last »
10
XML

```
1  03/13/18 11:28:28 AM
<15>Mar 13 2018 16:25:04 local: <72>Mar 13 16:25:02 mIcrond[uid=0 /chroot/arbitrator1/modules/exec/cisco/process_CCM.multiple.pgcopy.pl][22859]: 201803131625: cdr_StandAloneCluster_01_201803131623_240935: Processed 1 cdr records, 1 new records, 0 duplicate records, elapsed time 0.278323 seconds.
Host=127.0.0.1   Port=/dev/log   Method=local_syslog

2  03/13/18 11:28:28 AM
<15>Mar 13 2018 16:25:08 local: <72>Mar 13 16:25:06 mIcrond[uid=0 /chroot/arbitrator1/modules/exec/cisco/process_CCM.multiple.pgcopy.pl][22859]:
{"total_cmr_files":0,"total_cdr_records":7,"total_cdr_files":3,"elapsed_time":4.7501699924469,"json_name":"process_ccm_summary","summary_time":1520958300,"total_cmr_records":0,"total_cmr_errors":0}
Host=127.0.0.1   Port=/dev/log   Method=local_syslog

4  03/13/18 11:28:27 AM
<15>Mar 13 2018 16:25:07 local: <72>Mar 13 16:25:06 mIcrond[uid=0 /chroot/arbitrator1/modules/exec/cisco/process_CCM.multiple.pgcopy.pl][22859]: 201803131625: Processed cdr: cdr_StandAloneCluster_01_201803131624_240936 complete, 4 total records, 4 new records, 0 duplicate records, ratio=0, elapsed time 3.154571 seconds.
Host=127.0.0.1   Port=/dev/log   Method=local_syslog

3  03/13/18 11:28:27 AM
<15>Mar 13 2018 16:25:08 local: <72>Mar 13 16:25:06 mIcrond[uid=0 /chroot/arbitrator1/modules/exec/cisco/process_CCM.multiple.pgcopy.pl][22859]:
{"total_cmr_files":0,"total_cdr_records":7,"total_cdr_files":3,"elapsed_time":4.7301750050004,"callManagerIp":"10.53.37.44","json_name":"process_ccm_callmanager_summary","summary_time":1520958300,"total_cmr_records":0,"total_cmr_errors":
0}
Host=127.0.0.1   Port=/dev/log   Method=local_syslog

5  03/13/18 11:28:26 AM
<15>Mar 13 2018 16:25:07 local: <72>Mar 13 16:25:05 mIcrond[uid=0 /chroot/arbitrator1/modules/exec/cisco/process_CCM.multiple.pgcopy.pl][22859]: 201803131625: cdr_StandAloneCluster_01_201803131624_240936: Processed 4 cdr records, 4 new records, 0 duplicate records, elapsed time 2.292842 seconds.
Host=127.0.0.1   Port=/dev/log   Method=local_syslog

6  03/13/18 11:28:25 AM
<15>Mar 13 2018 16:25:05 local: <72>Mar 13 16:25:03 mIcrond[uid=0 /chroot/arbitrator1/modules/exec/cisco/process_CCM.multiple.pgcopy.pl][22859]: 201803131625: Processed cdr: cdr_StandAloneCluster_01_201803131623_240935 complete, 1 total records, 1 new records, 0 duplicate records, ratio=0, elapsed time 1.182151 seconds.
Host=127.0.0.1   Port=/dev/log   Method=local_syslog

7  03/13/18 11:28:21 AM
<15>Mar 13 2018 16:25:04 local: <72>Mar 13 16:25:01 mIcrond[uid=0 /chroot/arbitrator1/modules/exec/cisco/process_CCM.multiple.pgcopy.pl][22859]: 201803131625: Processed cdr: cdr_StandAloneCluster_01_201803131622_240934 complete, 2 total records, 2 new records, 0 duplicate records, ratio=0, elapsed time 0.370822 seconds.
Host=127.0.0.1   Port=/dev/log   Method=local_syslog

8  03/13/18 11:28:21 AM
<15>Mar 13 2018 16:25:01 local: <72>Mar 13 16:25:01 mIcrond[uid=0 /chroot/arbitrator1/modules/exec/cisco/process_CCM.prevhour.pgcopy.pl][22858]: Execution of /chroot/arbitrator1/modules/exec/cisco/process_CCM.prevhour.pgcopy.pl aborted due to compilation errors.
Host=127.0.0.1   Port=/dev/log   Method=local_syslog
```

A secondary symptom of CDR processing issues, or no receipt of CDR files would be no new call records in the Call Details interface.

Sort the **Calls by Time**: Descending to see the most recent calls first. Choose a 1 hour time frame and look for the most recent call time stamp to validate the last call record received and processed.



Mar 13, 2018 10:51 am - Mar 13, 2018 11:51 am

cisco

| TIME | SOURCE | DESTINATION | VENDOR | LATENCY | HOPS |
|---|---|---|---|---|---|
| 03/13/18 11:49:13 AM | 103@10.13.37.210 | 109@192.168.103.60 | Cisco | 0 | 0 |
| 03/13/18 11:48:53 AM | 101@192.168.103.56 | 102@172.16.1.11 | Cisco | 0 | 0 |
| 03/13/18 11:48:53 AM | 103@10.13.37.210 | 108@172.16.1.10 | Cisco | 0 | 0 |
| 03/13/18 11:48:34 AM | 103@10.13.37.210 | 109@192.168.103.60 | Cisco | 0 | 0 |
| 03/13/18 11:47:54 AM | 103@192.168.103.56 | 113@10.13.37.201 | Cisco | 0 | 0 |
| 03/13/18 11:47:29 AM | 102@172.16.1.11 | 103@0.0.0.0 | Cisco | 0 | 0 |
| 03/13/18 11:47:14 AM | 103@10.13.37.210 | 101@0.0.0.0 | Cisco | 0 | 0 |
| 03/13/18 11:46:48 AM | 102@172.16.1.11 | 113@10.13.37.201 | Cisco | 0 | 0 |
| 03/13/18 11:46:18 AM | 102@172.16.1.11 | 101@0.0.0.0 | Cisco | 0 | 0 |
| 03/13/18 11:46:07 AM | 102@172.16.1.11 | 110@10.13.37.220 | Cisco | 0 | 0 |
| 03/13/18 11:44:16 AM | 101@192.168.103.56 | 102@172.16.1.11 | Cisco | 0 | 0 |
| 03/13/18 11:44:13 AM | 103@10.13.37.210 | 109@192.168.103.60 | Cisco | 0 | 0 |
| 03/13/18 11:43:54 AM | 103@10.13.37.210 | 108@172.16.1.10 | Cisco | 0 | 0 |
| 03/13/18 11:43:36 AM | 103@10.13.37.210 | 109@192.168.103.60 | Cisco | 0 | 0 |
| 03/13/18 11:43:16 AM | 103@10.13.37.210 | 108@172.16.1.10 | Cisco | 0 | 0 |
| 03/13/18 11:42:14 AM | 103@10.13.37.210 | 101@0.0.0.0 | Cisco | 0 | 0 |

Process_CCM Log Example:

Below is an example of the log in the index indicating that CDR files have been received and processed. Use the keyword `PROCESS_CCM` in the **Search** interface to find this log.

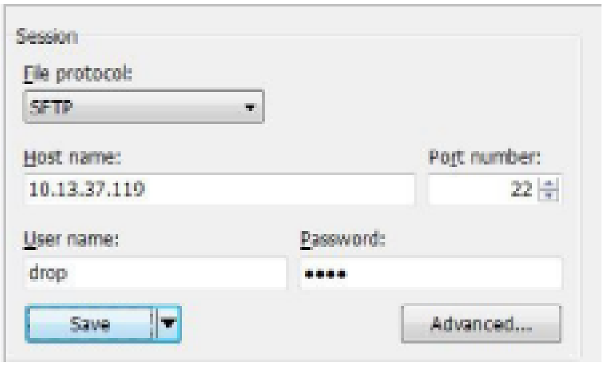
```
Mar 13 2018 16:25:04 local: Mar 13 16:25:02 microND(uid=0
/chroot/arbitrator1/modules/exec/cisco/process_CCM.multiple.pgcopy.pl)[22159]:
201803131625: cdr_StandAloneCluster_01_201803131623_249935: Processed
1 cdr records, 1 new records, 0 duplicate records, elapsed time
0.278323 seconds.
```

Cisco CDR files are sent from the Cisco CUCM Publisher to the Correlation server using sftp on port 22. Validate that the Correlation server sftp function is available for connections for the file transfer.

### 2.4.2. How to validate the SFTP service is up and ready to accept CDR

Use an SFTP client like *WinSCP* or *Filezilla* to connect to the Correlation server using sftp on port 22. Use the username “drop” and its password for the connection. The drop user credential is used in the CUCM Billing server configuration on the Publisher. Reference the CUCM billing server configuration for the drop user password.

When connected to the SFTP service the default directory will be `/pub`.



File protocol: SFTP

Host name: 10.13.37.110

Port number: 22

User name: drop

Password: ••••

If the SFTP service is not responsive, reboot the Correlation server from the admin CLI menu using the procedure in the *Corrupted Index* section of this document.

### 2.4.3. What else should I troubleshoot in this scenario?

Try connections to the SFTP server from a system in the same subnet if possible just to remove any potential network connectivity issues for the test. Test the SFTP connection from a system in the same subnet as the CUCM Publisher.

If SFTP service is available on the Correlation server, the system can receive CDR files. The issue will then be either network connectivity or an issue on the CUCM Publisher.

If Cisco has an issue sending CDR files to billing server destinations it will generate a syslog alert in the Correlation system (if the rule to catch it is in the system). The alert log will indicate details about the CDR transfer issue and destination of the files.

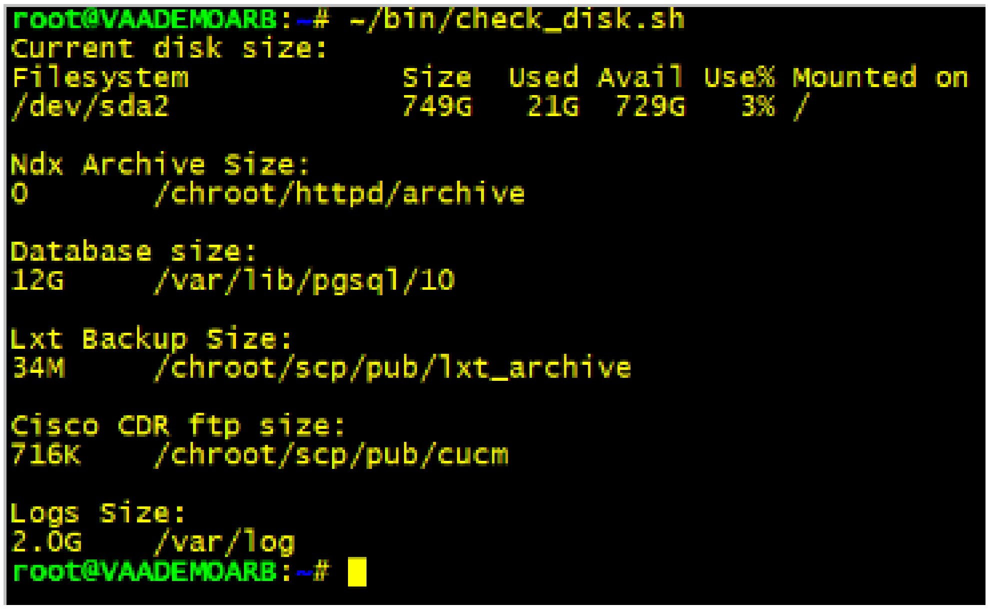
## 2.5. Clear Disk Space

To clear disk space being used by archive

1. To identify if the archive is using massive amounts of disk space, log in to cli as root.
2. Then enter the following command and press <Enter>

```
~/bin/check_disk.sh
```

3. This will return the screen below



```
root@VAADEMOARB:~# ~/bin/check_disk.sh
Current disk size:
Filesystem              Size  Used Avail Use% Mounted on
/dev/sda2               749G   21G  729G   3% /

Ndx Archive Size:
0       /chroot/httpd/archive

Database size:
12G     /var/lib/pgsql/10

Lxt Backup Size:
34M     /chroot/scp/pub/lxt_archive

Cisco CDR ftp size:
716K    /chroot/scp/pub/cucm

Logs Size:
2.0G    /var/log
root@VAADEMOARB:~#
```

If the `Ndx Archive Size` is huge we need to clear it down.

Change your directory

```
cd /chroot/httpd/archive
```

**Important:** Do not run the next command unless you are in this directory.

4. Now run

```
rm -rf *
```

5. Once this has finished run:

```
sv restart arbitrator_ndx
```

6. Once the service has restarted you can now run

```
~/bin/check_disk.sh
```

again to confirm that the space has now been freed up.

## 2.6. Drop Tables to free up Disk

1. Find the tables with the biggest in size

```
/root/bin/`dbTableSizes.v2.sh
```

This will list the tables and size

2. Drop tables

```
/root/bin/dropTables.sh <Table name pattern - can be partial> <Table date - YYYY_MM>
```

For example to delete RTMT data for `2020_03`

```
/root/bin/dropTable.sh "RTMT" 2020_03
```

This command simply prints the psql commands and the table names. It does not actually do any deletes yet. Confirm the list is what you want. If not adjust search and date accordingly.

3. Final command to commit delete is same command with `| psql sca`

## 2.7. Manually Pull Phones into Arbitrator

1. Log in as root to CLI
2. Change directory to

```
/chroot/arbitrator1/modules/exec/cisco/cucmrisphone
```

3. Then run the pre-canned script

```
./collectrisphones.sh <ip of cucm> <axl username> <axl password>
```

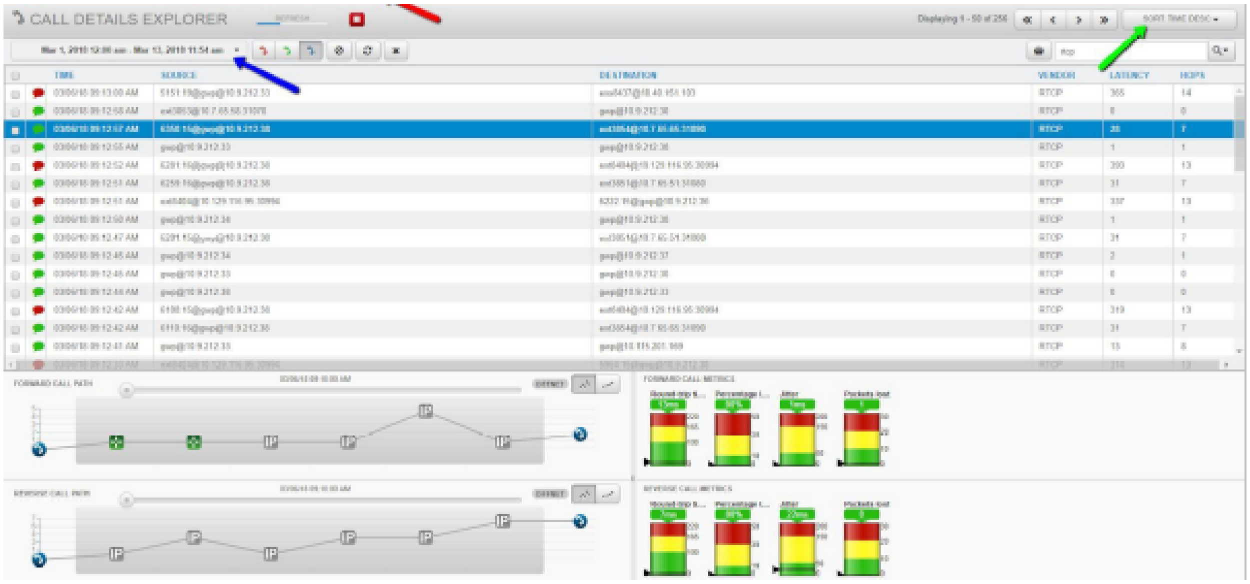
## 2.8. RTCP call data appears to have stopped

System Impact – **Minor**

### 2.8.1. Symptoms that RTCP ingestion appears to have stopped

No new RTCP call records in the Call Details interface.

In the **Call Details** interface, sort the Calls by `Time: Descending` to see the most recent calls first. Choose a 1 hour time frame and look for the most recent call time stamp to validate the last call record received and processed.



The SCDTSD service mentioned earlier in the document controls the ingestion of the RTCP data, so if SCDTSD has an issue it will impact RTCP data as well. Validate the integrity of the SCDTSD service.

### 2.8.2. What else should I troubleshoot in this scenario?

RTCP is sent from every phone in every network region to the Correlation server on the default port 5005. Validate that the RTCP destination configuration has not changed on the UC application.

## 2.9. Set Alarm Expiry Timers

```
update "INCIDENT_RESPONSE_MAPPING" set "TIMER" = 86400;
```

updates alarm expiry from the default to 24 hours

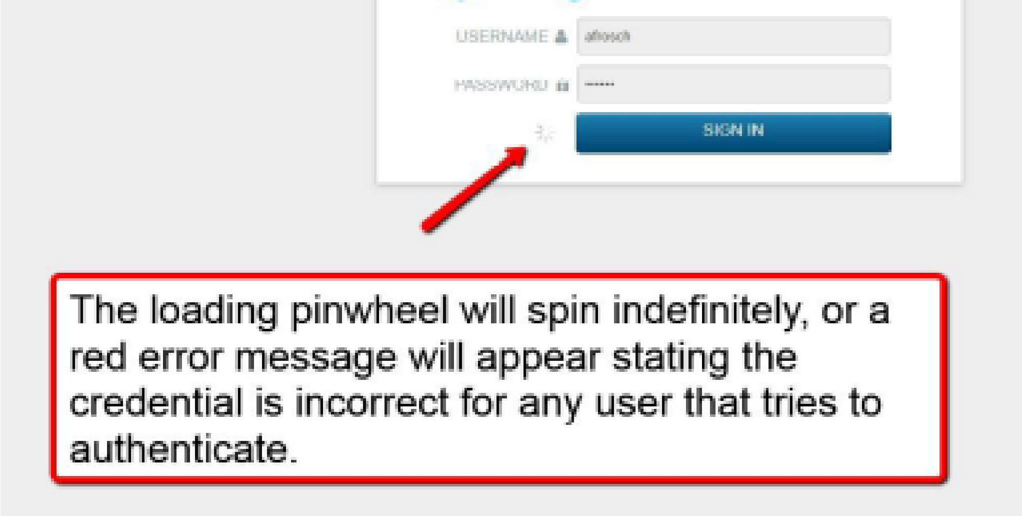
## 2.10. The local OpenLDAP service has stopped

System Impact – **Minor**

### 2.10.1. Symptoms of a down openldap service

Local administrative users are created and stored in the instance of OpenLDAP on the Correlation server. If the service is ever stopped, local users cannot authenticate to access the GUI. Users synchronized from a SAML or AD repository are also affected and will not be able to access the GUI.

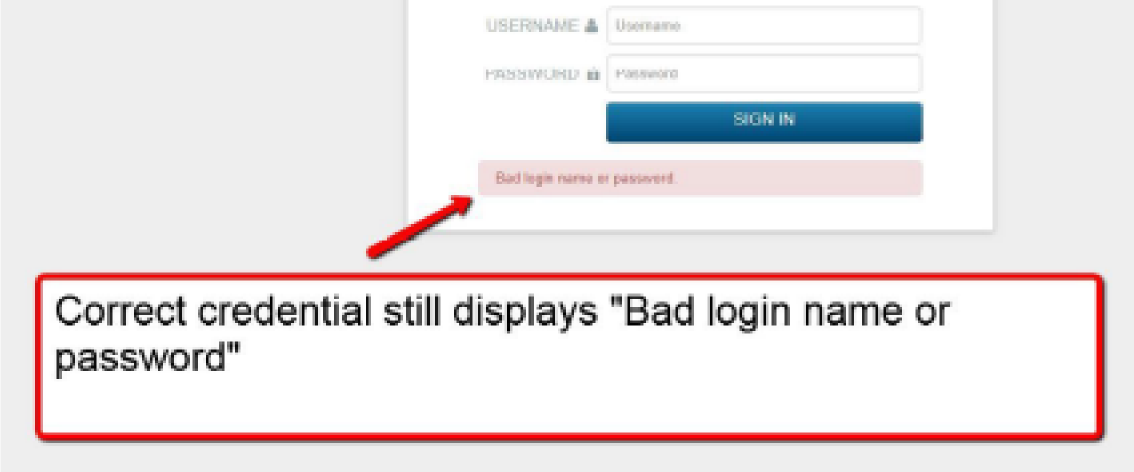
The OpenLDAP service state does not affect normal system processing, so logging and alerting functions will continue.



USERNAME: afrosch

PASSWORD: ······

The loading pinwheel will spin indefinitely, or a red error message will appear stating the credential is incorrect for any user that tries to authenticate.



Bad login name or password.

Correct credential still displays "Bad login name or password"

### 2.10.2. How to restore local system authentication for the GUI

The system will need to be restarted from the admin CLI menu to resolve the OpenLDAP issue.

## 2.11. The main Arbitrator Service is DOWN

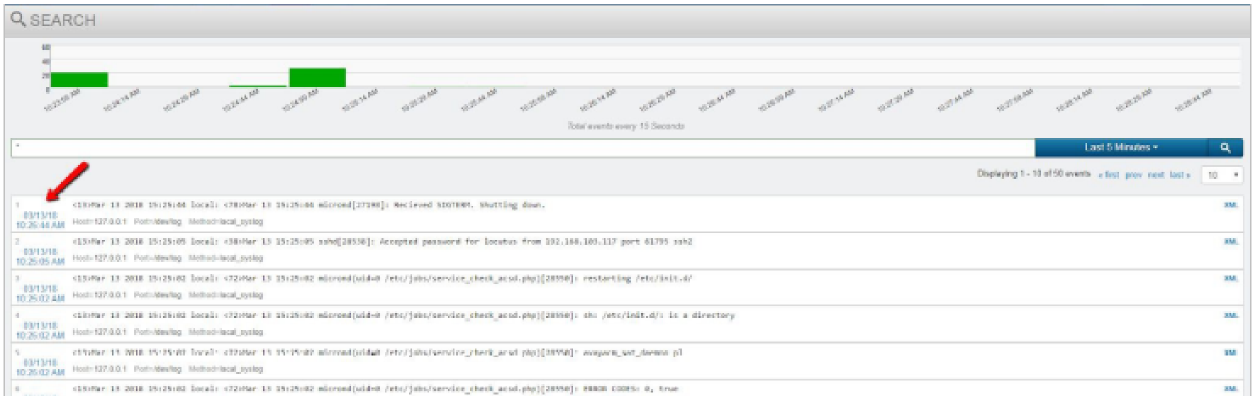
System Impact – **Critical**

### 2.11.1. About the Arbitrator service

The main correlation engine service on the system is called Arbitrator. It controls all of the alerting, probe, and automated response procedure operations. It also is the mechanism that actually writes to the Index file “hot” bucket.

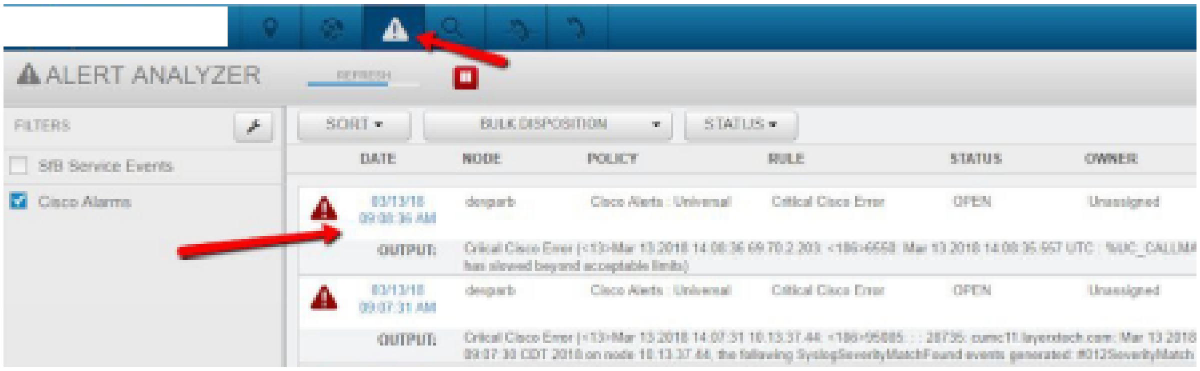
### 2.11.2. Symptoms of a down Arbitrator service

When the Arbitrator service is down, no new logs or events can be written to the Index. The Search interface will look responsive since the Index is not corrupted. Use the log time stamp to validate that new logs are not being written into the Index.


SEARCH
Total events every 15 Seconds
Last 5 Minutes
Displaying 1 - 10 of 50 events « first prev next last »
10
XML

```
1 03/13/18 10:25:44 AM
<13>Mar 13 2018 15:25:44 local: <78>Mar 13 15:25:44 microd[27198]: Recieved SIGTERM. Shutting down.
Host=127.0.0.1 Port=/dev/log Method=local_syslog
2 03/13/18 10:25:05 AM
<15>Mar 13 2018 15:25:05 local: <38>Mar 13 15:25:05 sshd[28538]: Accepted password for locutus from 192.168.103.117 port 61795 ssh2
Host=127.0.0.1 Port=/dev/log Method=local_syslog
3 03/13/18 10:25:02 AM
<15>Mar 13 2018 15:25:02 local: <72>Mar 13 15:25:02 microd(uid=0 /etc/jobs/service_check_acsd.php)[28550]: restarting /etc/init.d/
Host=127.0.0.1 Port=/dev/log Method=local_syslog
4 03/13/18 10:25:02 AM
<15>Mar 13 2018 15:25:02 local: <72>Mar 13 15:25:02 microd(uid=0 /etc/jobs/service_check_acsd.php)[28550]: sh: /etc/init.d/: is a directory
Host=127.0.0.1 Port=/dev/log Method=local_syslog
5 03/13/18 10:25:02 AM
<15>Mar 13 2018 15:25:02 local: <72>Mar 13 15:25:02 microd(uid=0 /etc/jobs/service_check_acsd.php)[28550]: avayarm_sat_daemon pl
Host=127.0.0.1 Port=/dev/log Method=local_syslog
6
<15>Mar 13 2018 15:25:02 local: <72>Mar 13 15:25:02 microd(uid=0 /etc/jobs/service_check_acsd.php)[28550]: ERROR CODES: 0, true
```

Use the Alert Analyzer interface to validate that no new alerts have been created. Look at the time stamp of the latest alert in the system to further validate if the Arbitrator process has stopped.



□ S/B Service Events

☑ Cisco Alarms

| DATE | NODE | POLICY | RULE | STATUS | OWNER |
|---|---|---|---|---|---|
| 03/13/18 09:08:36 AM | devgarb | Cisco Alerts : Universal | Critical Cisco Error | OPEN | Unassigned |
| OUTPUT: | Critical Cisco Error (<13>Mar 13 2018 14:08:36 69.70.2.203: <186>6558: Mar 13 2018 14:08:35.957 UTC : %UC_CALLMA<br>has slowed beyond acceptable limits) | | | | |
| 03/13/18 09:07:31 AM | devgarb | Cisco Alerts : Universal | Critical Cisco Error | OPEN | Unassigned |
| OUTPUT: | Critical Cisco Error (<13>Mar 13 2018 14:07:31 10.13.37.44: <186>95885: : : 28735: cumc11.layerxtech.com: Mar 13 2018<br>09:07:30 CDT 2018 on node 10.13.37.44, the following SyslogSeverityMatchFound events generated: #012SeverityMatch | | | | |

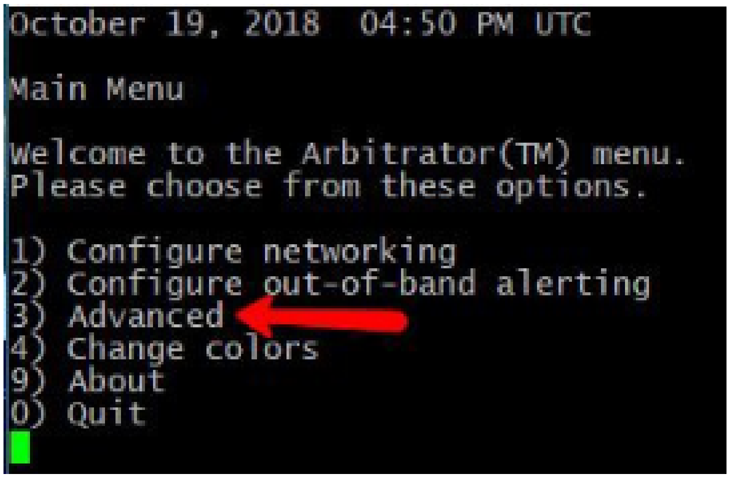
### 2.11.3. Other side effects of a stopped Arbitrator process

- Cisco CDR files will not be processed - no new calls in the Call Details interface
- Avaya RTCP stream data will not be processed - no new calls in the Call Details interface.

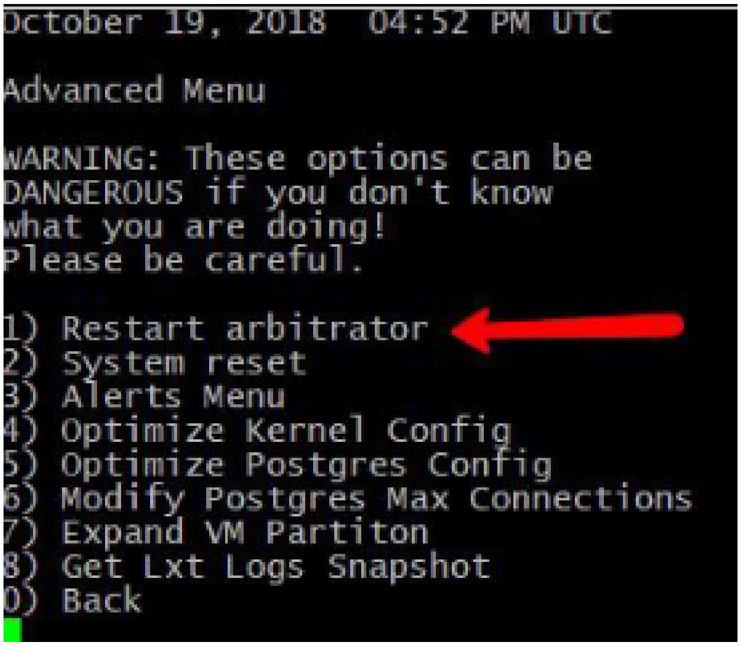
We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

## 2.12. How to restart the Arbitrator service

To restart the Arbitrator process in the Correlation system, ssh to the system and login as the “admin” user to access the admin CLI menu. From the Admin Menu select the **Advanced ARB Options** menu to navigate to the Main sub menu. From there select option 3 **Advanced**, and then option 1 **Restart arbitrator** to restart the Arbitrator process. This is not a reboot of the system, it is only a restart of the main Arbitrator process. For those that may not know, Arbitrator is the legacy name of the Correlation system. In can still be seen referenced in some documentation and the admin CLI menu until the resources are updated.



```
October 19, 2018  04:50 PM UTC

Main Menu

Welcome to the Arbitrator(TM) menu.
Please choose from these options.

1) Configure networking
2) Configure out-of-band alerting
3) Advanced
4) Change colors
9) About
0) Quit
```



```
October 19, 2018  04:52 PM UTC

Advanced Menu

WARNING: These options can be
DANGEROUS if you don't know
what you are doing!
Please be careful.

1) Restart arbitrator
2) System reset
3) Alerts Menu
4) Optimize Kernel Config
5) Optimize Postgres Config
6) Modify Postgres Max Connections
7) Expand VM Partiton
8) Get Lxt Logs Snapshot
0) Back
```

Press <ENTER> to exit the operation when prompted and return to the menu.

Use the Search interface in the GUI to validate that new logs are being written into the Index by looking at the log time stamp. The green graph at the top of the Search interface is an indicator of log events being written into the Index in that time frame.

# 2.13. The system Index file is corrupted

System Impact – **Critical**

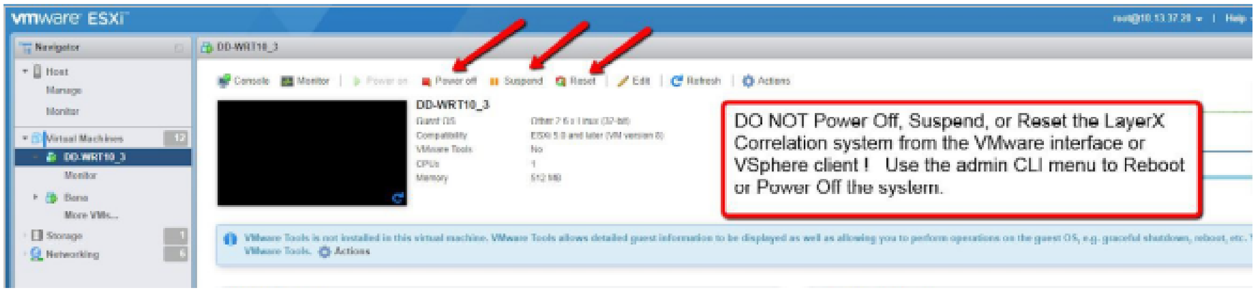
## 2.13.1. About the system Index file

The Index file in the correlation server is the main text file that all logs, traps, probe return data, and system logs are written to and then processed by the Correlation engine. It is the main archive of raw log data, and rotates as it archives from a "hot bucket" to a "cold bucket" The current Index that is being written in the system is the "hot bucket", while archived Indexes are "cold" and no longer actively being appended. The Index file that is affected in the problem description is the current "hot" or active Index file.

## 2.13.2. How the Index becomes corrupted

The Index becomes corrupted when either the Virtual Machine is improperly shut down in the VMWare management interface, or the VMWare host has an issue that removes CPU or disk resources from the system while it is writing to the file.

**Important:** Do NOT Power Off, Suspend, or Reset the Correlation system from the VMWare management interface!

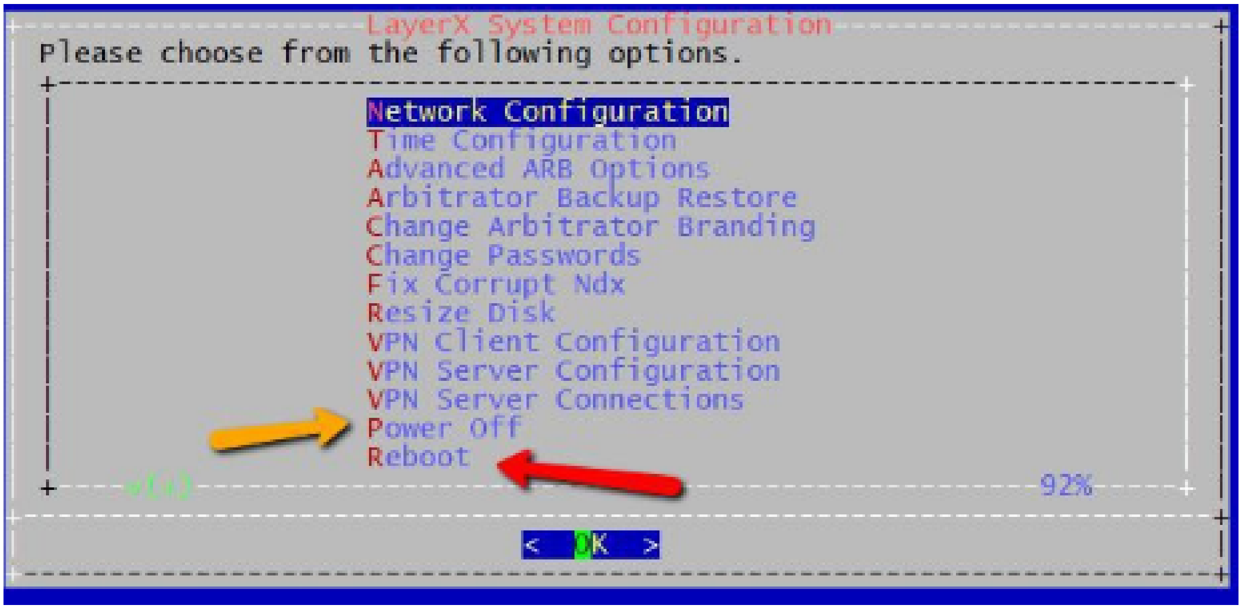


DO NOT Power Off, Suspend, or Reset the LayerX Correlation system from the VMware interface or VSphere client ! Use the admin CLI menu to Reboot or Power Off the system.

VMware Tools is not installed in this virtual machine. VMware Tools allows detailed guest information to be displayed as well as allowing you to perform operations on the guest OS, e.g. graceful shutdown, reboot, etc. VMware Tools. Actions

## 2.13.3. How to properly reboot or power off the system

To properly power off or reboot the Correlation system, ssh to the system and login as the "admin" user to access the admin CLI menu. From the Main Menu use the arrow keys to navigate to the 'Reboot' option to reboot the system or 'Power Off' to power off the system. These operations will properly stop the system services and close the Index file so that it does not become corrupted.



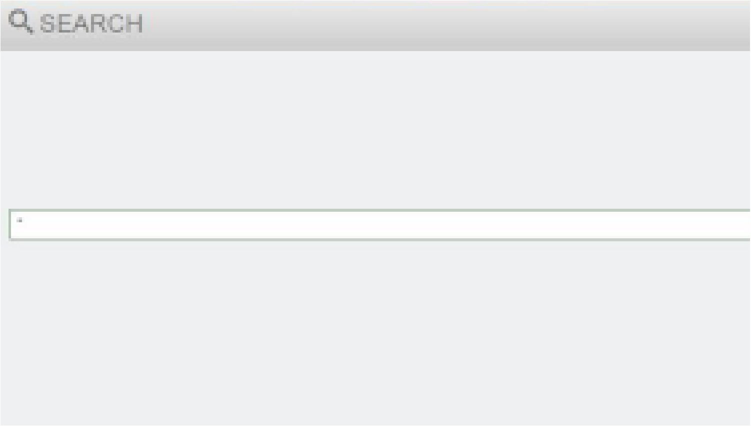
Please choose from the following options.

## 2.13.4. Symptoms of a corrupted Index

If the index is corrupted no new data can be written into the system. From the Correlation server GUI use the Search interface to look at the Index . When the index is corrupted the Search interface will return no data and look blank since the corrupted index cannot be read or accessed.

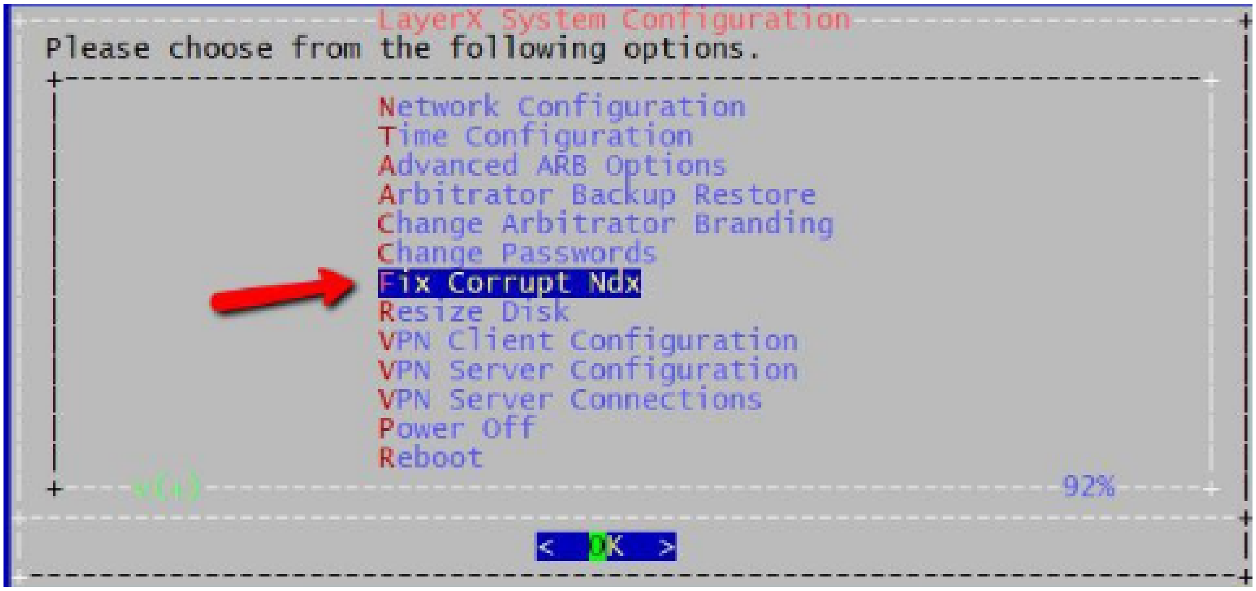
Side effects of a corrupted Index are no new alerts can be generated since no data can be written into the system and processed by the Correlation engine.

Example of a blank Search screen as a result of a corrupted index.



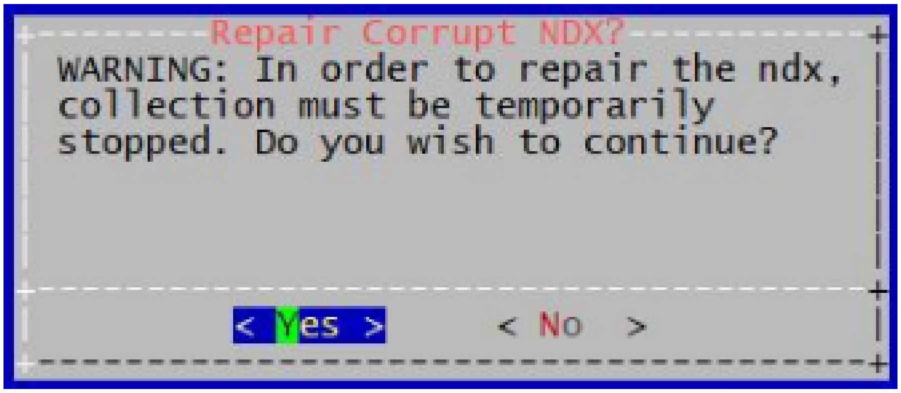
## 2.13.5. How to repair a corrupted Index file and restore operation

To properly repair the Index in the Correlation system, ssh to the system and login as the “admin” user to access the admin CLI menu. From the Main Menu navigate using the arrow keys to select option **Fix Corrupt Ndx** to fix the corrupted Index.



```
Please choose from the following options.
```

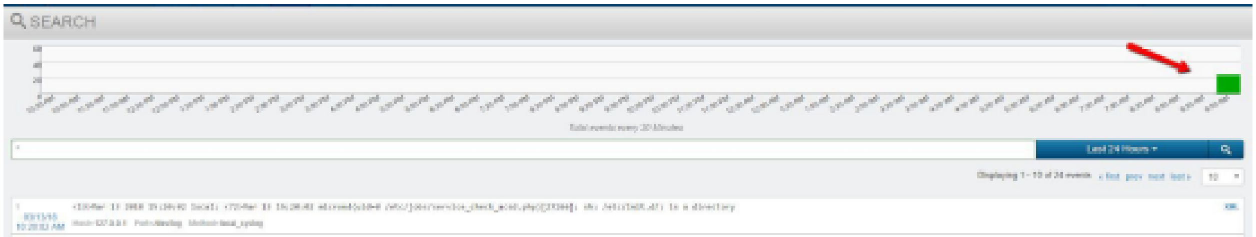
When running the “fix” Index operation there will be a WARNING prompt before proceeding.



```
WARNING: In order to repair the ndx,
collection must be temporarily
stopped. Do you wish to continue?
```

Select <YES> and Press <ENTER> to execute the operation. Press <ENTER> when prompted upon completion to return to the menu.

Use the Search interface in the GUI to validate that new logs are being written into the new Index “hot” bucket. The green graph at the top of the Search interface is an indicator of log events being written into the Index in that time frame.



## 2.14. Threat Scores

```
info = 0
minor = 11
major = 31
critical = 60
```

## 2.15. To disable policies in Bulk

```
psql sca -c 'update "CORRELATION_RULEBASE" set "STATUS" = 0 WHERE "THREAT_SCORE" =11;'
```

disables all Minor alarms

```
psql sca -c 'update "CORRELATION_RULEBASE" set "STATUS" = 0 WHERE "THREAT_SCORE" =0;'
```

disables all Informational alarms

## 2.16. Truncate System Logs

If you run

```
/root/bin/dbTablesizes.v2.sh
```

and the SYSTEM_LOG is over 10GB in size you will need to truncate the log:

1. Log in as root
2. Then from the command line

   ```
   psql sca -c 'truncate "SYSTEM_LOG"'
   ```

   This will then truncate the log.

# 3. Upgrade

## 3.1. Pre Checks

1. Check the current version of the software by running the command **about** and viewing the version.
2. Check GUI Access.
3. Check available storage of the disk of the server.

## 3.2. Backup dashboards before upgrades

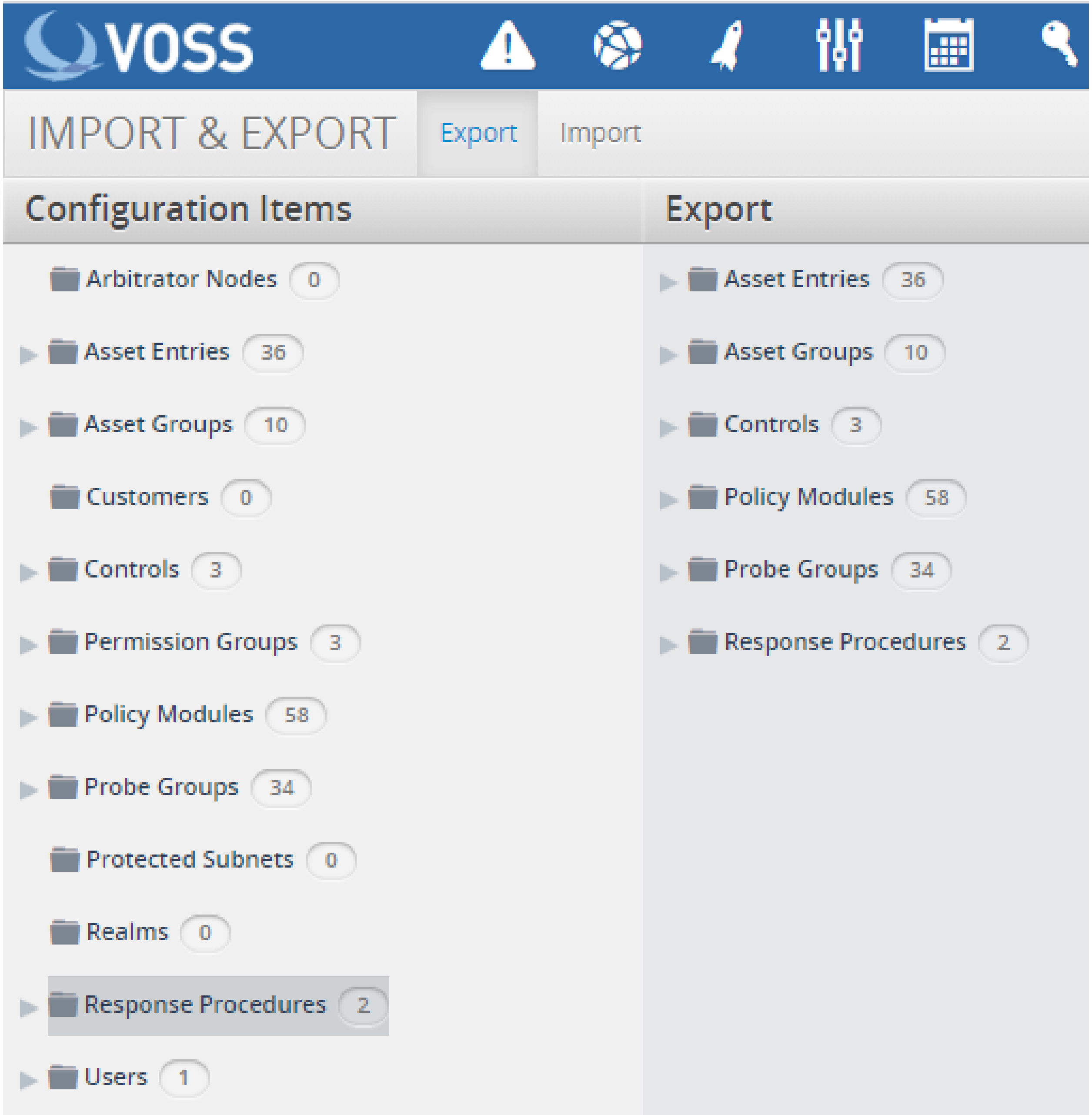
1. Log in as admin.
2. Click on the **admin** top right.
3. Click Import/Export Wizard.
4. Click the Export Tab.
5. Select all the dashboards.
6. Click the Export .lxtr blue button on the top right.
7. click the **Download** button and save to a safe place.

## 3.3. Run a backup

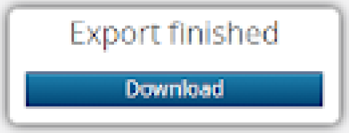
On Arbitrator:

1. Navigate to settings
2. Choose **IMPORT & EXPORT**
3. Drag from the **Configuration items** pane to the **Export** pane:
    - Asset Entries
    - Asset Groups
    - Controls
    - Policy Modules
    - Probe groups

- Response procedures



4. Click **Export**



5. Click **Download**. Store the file in a safe place.

## 3.4. Upgrade timings

- Arbitrator = Approx 20 Mins
- Dashboard Server = 20-60mins depending on resources

## 3.5. Upgrade MOP

### 3.5.1. VOSS Engineers upgrade via `root`

1. Using *Winscp* log in to the server using the root account
2. Copy the patch file

   (Example patch file for the arbitrator `layerX-arbitrator-sp19-sp20.lxsp`) in to the root directory
3. Log in to server using *Putty* via the root account.
4. Run the command **install-service-pack <filename>**

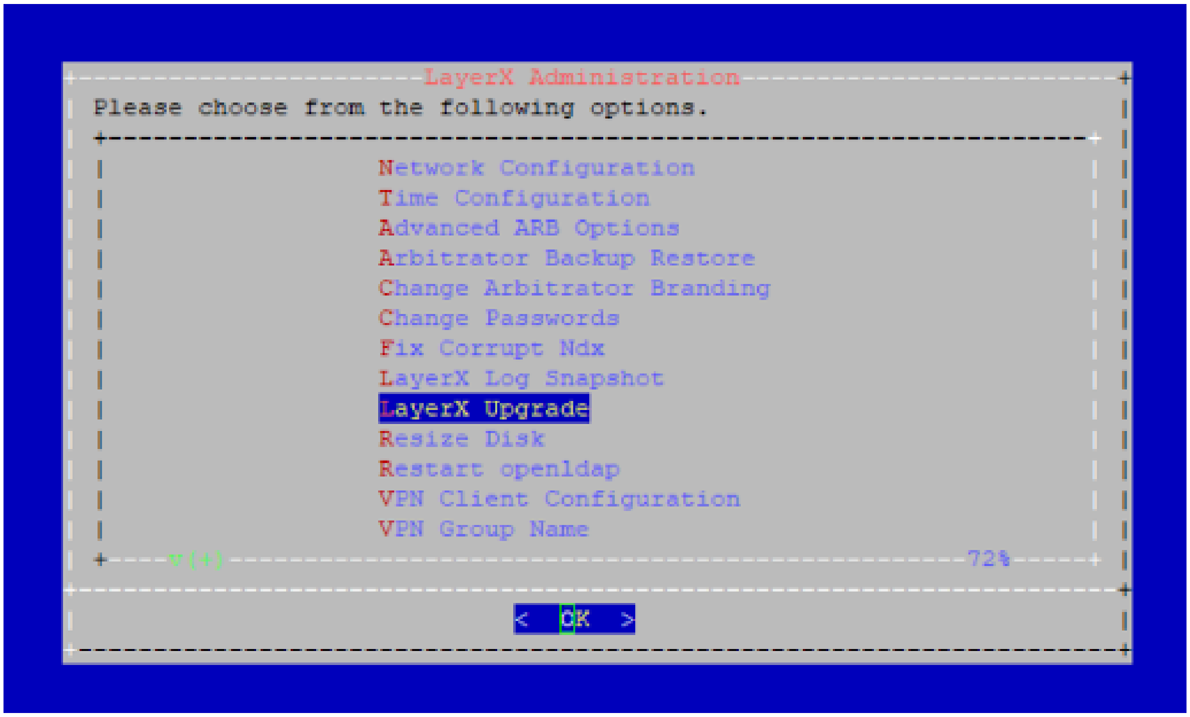
   Example: **install-service-pack layerX-arbitrator-sp19-sp20.lxsp**
5. Once the install has taken place reboot the server by running the command **reboot**.

### 3.5.2. Customer Upgrade via Admin

Upgrade check, download and install:

- The server will need access to the internet on port 443

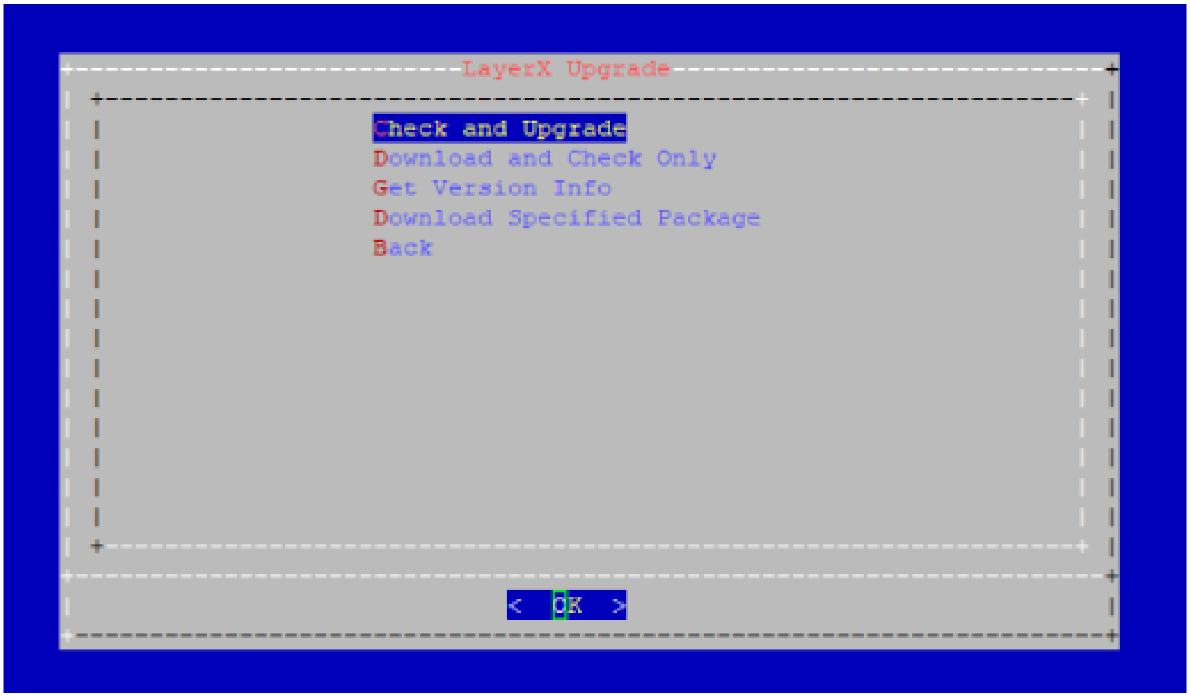
1. Log on to the server using *Putty* and the admin user credentials
2. Navigate down to **Layerx Upgrade**
3. Click/enter **OK**



LayerX Administration

Please choose from the following options.

4. Select the **Check and Upgrade** option.



LayerX Upgrade

The server will go to the file repository and download the image to the local server.

```
Current system info:  arbitrator-sp20, expecting layerX-arbitrator-sp20-sp21.lxsp
Could not find expected lxsp file locally, so attempting download from
https://www.layerxtech.com/downloads/arbitratorhawaii/updates/layerX-arbitrator-sp20-
↪sp21.lxsp
--2020-12-10 10:08:54--
```

(continues on next page)

(continued from previous page)

```
 https://www.layerxtech.com/downloads/arbitratorhawaii/updates/layerX-arbitrator-sp20-
↪sp21.lxsp
Resolving www.layerxtech.com... 50.87.196.167
Connecting to www.layerxtech.com|50.87.196.167|:443... connected.
WARNING: cannot verify www.layerxtech.com's certificate, issued by
'CN=Let\'s Encrypt Authority X3,O=Let\'s Encrypt,C=US':
  Unable to locally verify the issuer's authority.
HTTP request sent, awaiting response... 200 OK
Length: 119664932 (114M)
Saving to: 'layerX-arbitrator-sp20-sp21.lxsp'

layerX-arbitrator-sp20-sp21.lxsp
 100%[================================================>]
114.12M  10.7MB/s    in 12s

2020-12-10 10:09:09 (9.33 MB/s) - 'layerX-arbitrator-sp20-sp21.lxsp' saved
[119664932/119664932]

wget --no-check-certificate -O layerX-arbitrator-sp20-sp21.lxsp.md5sum
https://www.layerxtech.com/downloads/php/md5.php?
 filename=/home3/layerxte/www/downloads/arbitratorhawaii/updates/layerX-arbitrator-
↪sp20-sp21.lxsp
--2020-12-10 10:09:09--
https://www.layerxtech.com/downloads/php/md5.php?
 filename=/home3/layerxte/www/downloads/arbitratorhawaii/updates/layerX-arbitrator-
↪sp20-sp21.lxsp
Resolving www.layerxtech.com... 50.87.196.167
Connecting to www.layerxtech.com|50.87.196.167|:443... connected.
WARNING: cannot verify www.layerxtech.com's certificate, issued by
'CN=Let\'s Encrypt Authority X3,O=Let\'s Encrypt,C=US':
  Unable to locally verify the issuer's authority.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'layerX-arbitrator-sp20-sp21.lxsp.md5sum'

layerX-arbitrator-sp20-sp21.lxsp.md5sum
[ <=>                                      ]      97  --.-KB/s
   in 0s

2020-12-10 10:09:12 (7.70 MB/s) -
'layerX-arbitrator-sp20-sp21.lxsp.md5sum' saved [97]

Download completed.  md5sum values match.
-rw-r--r-- 1 drop drop 119664932 Dec  7 23:31
/chroot/scp/pub/lxt_upgrade/layerX-arbitrator-sp20-sp21.lxsp

SUCCESS:  Download and check specified.  Not performing install.
Press any key to return to the menu.

Press any key to continue the upgrade
```

Note: the location where the upgrade files get placed ready for the upgrade is location here:

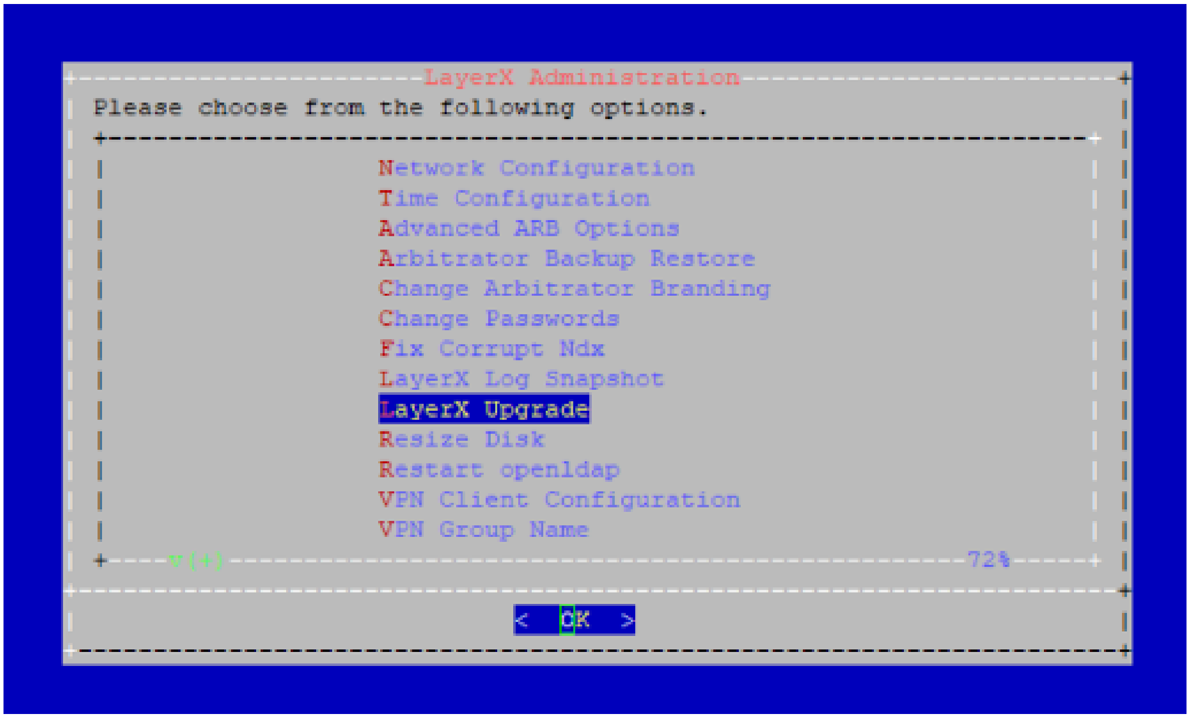
downloads file to:

`/chroot/scp/pub/lxt_upgrade/`

### 3.5.3. Manual download of a upgrade image:

- The server will need access to the internet on port 443

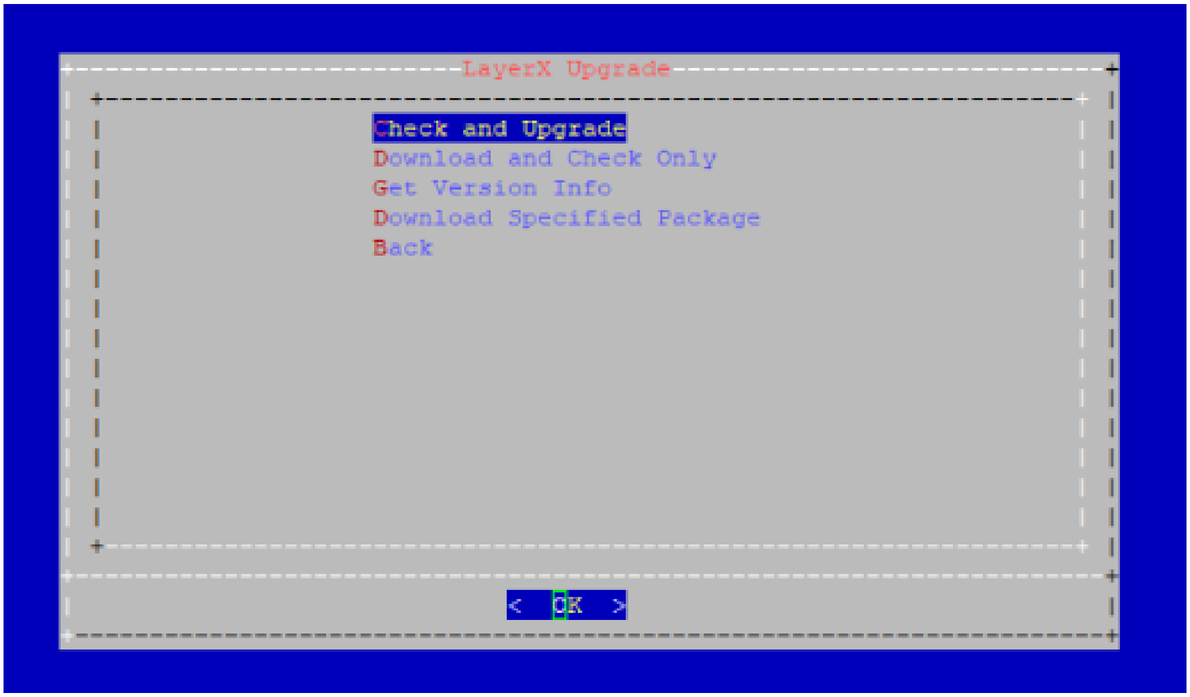
1. Log on to the server using *Putty* and the admin user credentials
2. Navigate down to **LayerX Upgrade**
3. Click/enter **OK**



LayerX Administration

Please choose from the following options.

4. Select the **Download Specified Package**



**Download Specified package** - Enter the following information changing the `<upgrade filename>` with the actual file name:

```
https://www.layerxtech.com/downloads/arbitratorhawaii/updates/<upgrade filename>
```

E.g. `layerX-arbitrator-sp19-sp20.lxsp`

The file will continue to install

```
Please enter the path to download and install:
https://www.layerxtech.com/downloads/arbitratorhawaii/updates/layerX-arbitrator-
↪sp19-sp20.lxsp
Fetching
https://www.layerxtech.com/downloads/arbitratorhawaii/updates/layerX-arbitrator-
↪sp19-sp20.lxsp
--2020-12-10 10:38:18--
 https://www.layerxtech.com/downloads/arbitratorhawaii/updates/layerX-arbitrator-
↪sp19-sp20.lxsp
Resolving www.layerxtech.com... 50.87.196.167
Connecting to www.layerxtech.com|50.87.196.167|:443... connected.
WARNING: cannot verify www.layerxtech.com's certificate, issued by
'CN=Let\'s Encrypt Authority X3,O=Let\'s Encrypt,C=US':
  Unable to locally verify the issuer's authority.
HTTP request sent, awaiting response... 200 OK
Length: 206254372 (197M)
Saving to: 'layerX-arbitrator-sp19-sp20.lxsp'

layerX-arbitrator-s 100%[===================>] 196.70M  11.1MB/s    in 20s

2020-12-10 10:38:38 (9.99 MB/s) - 'layerX-arbitrator-sp19-sp20.lxsp' saved
[206254372/206254372]

Download completed
Continuing with install
```

(continues on next page)

(continued from previous page)

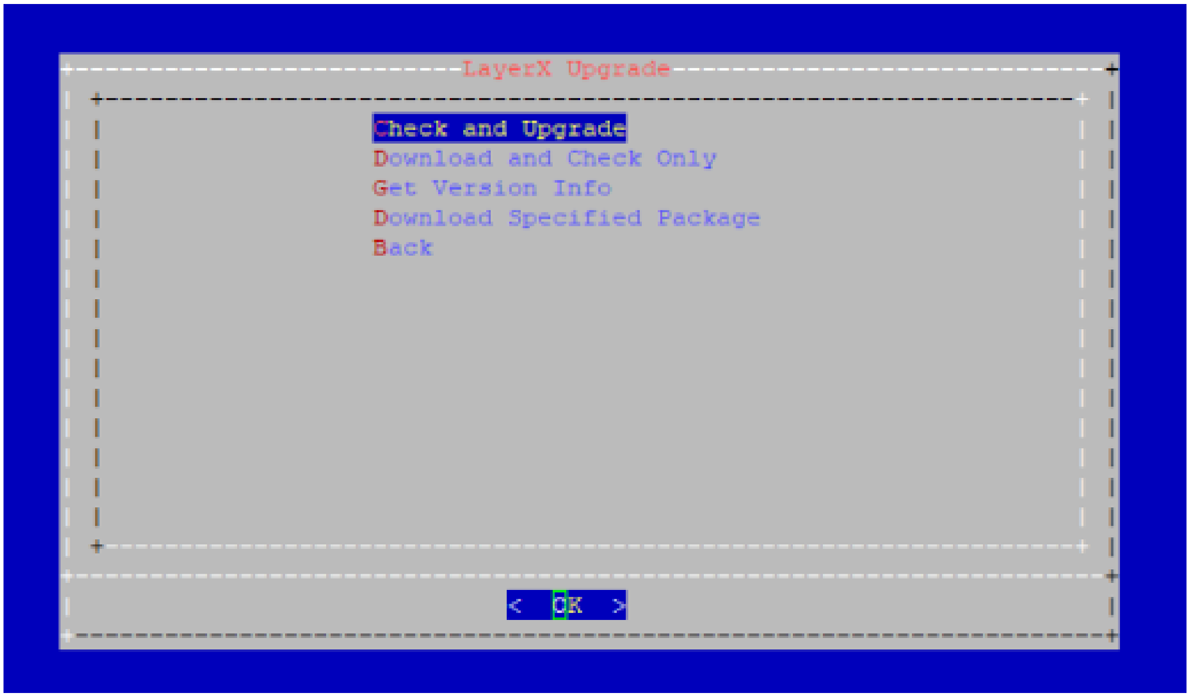
```
Thu Dec 10 10:38:43 GMT 2020: Validating service pack file.
Thu Dec 10 10:38:43 GMT 2020: Extracting service pack file.
Thu Dec 10 10:38:45 GMT 2020: Validating service pack phase 1.
Verified OK
Thu Dec 10 10:38:45 GMT 2020: Validating service pack phase 2.
Thu Dec 10 10:38:46 GMT 2020: Service pack validation complete.
Thu Dec 10 10:38:46 GMT 2020: Starting installation processes.
You cannot upgrade release sp20 => sp20.
The required release for this service pack is sp19 or sp19.1 or sp19.2 or
sp19.3 or sp19.4 or sp19.5 or sp19.6 or sp19.7 or sp19.8 or sp19.9 or
sp19.10.
Press any key to return to the menu.

Press the enter key to return to the menu
```

Note: the location where the upgrade files get placed ready for the upgrade is location here:

downloads file to:

```
/chroot/scp/pub/lxt_upgrade/
```

5. On the menu select the **Get Version Number**



## 3.6. Post Checks

Check the patch version by running the command **about**.

```
root@arbitrator:~# about

                    About
===============================================
```

(continues on next page)

(continued from previous page)

```
      Hostname: arbitrator
       Version:  sp20
         Theme:  voss
         Flavor  arbitrator
       License:  9H3EJ-H3A4A-7X79K-9PQ7Q-4RATT
 Days Licensed:  143
Days Remaining:  41
   Product Key:
 7a426f46634971795a446e3379777a4e6e66452f4c4c7a[...]
       Website:  http://www.layerxtech.com/
        Kernel:  Linux 4.14.17-lxt-3 x86_64 GNU/Linux
```

# 4. Add Certificates

1. SCP the new `server.crt` and `server.key` tiles to the `etc/apache2/` directory on the system, ovewriting the old certificate files.

   Recommended: back up the current certificate files prior to overwriting them.

2. SSH to the system as `root` and restart the apache service using the **sv restart apache** command.
3. Clear browser cache.
4. Apache will now use the new signed certificate.