

IPWorks Manual Health Check

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2017, 2018. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
1.1	Prerequisites	1
1.1.1	Documents	1
1.1.2	Conditions	1
1.2	Related Information	1
2	Health Check Procedure	2
2.1	Checking Alarms	2
2.2	Checking UUID for Alarms	2
2.3	Checking LDE Dump Files	2
2.4	Checking Core Middleware Services	3
2.5	Checking CPU Load	3
2.6	Checking Disk Use	3
2.7	Checking Memory Use	4
2.8	Checking Internal Communication	4
2.9	Checking Controller Status	5
2.10	Checking Virtual IP Status	6
2.11	Checking Latest Available Backup	7
2.12	Checking IPWork Counters	8
2.13	Checking Nodes Restart	9
2.14	Checking IPWorks Application Logs	9
2.14.1	Checking DNS Logs	10
2.14.2	Checking ASDNS Logs	10
2.14.3	Checking SS Logs	10
2.14.4	Checking ENUM Logs	11
2.14.5	Checking ENUM-FE Logs	11
2.14.6	Checking Radius AAA Logs	11
2.14.7	Checking EPC AAA Logs	12
2.14.8	Checking DHCPv4 Logs	12
2.15	Checking MySQL Nodes Status	12
2.16	Checking Number of MySQL Tables	13
2.17	Checking Software Release Version	14
2.18	Checking License	14
2.19	Checking LDAP Connections	15
2.20	Checking SOAP Listening Status	15
2.21	Checking Backup Files	16



2.21.1	Checking the Backup Files	16
2.21.2	SS Backup Files	17
2.21.3	DNS Backup Files	17
2.21.4	MySQL NDB Cluster Backup Files	17
2.21.5	ENUM Backup Files	18
2.21.6	ENUM-FE Backup Files	18
2.21.7	Radius AAA Backup Files	18
2.21.8	EPC AAA Backup Files	18
2.21.9	DHCPv4 Backup Files	19
2.22	Checking AAA Service Port Listening Status	19
2.22.1	Checking Radius AAA Service Port Listening Status	19
2.22.2	Checking EPC AAA Service Port Listening Status	20
2.23	Checking DHCPv4 Service Port Listening Status	21
3	Problem Reporting	22
	Reference List	23



1 Introduction

This document describes how to perform the health check procedure on the IPWorks. The health check procedures are recommended to be performed before and after a system update/upgrade, a normal backup, or during periodic maintenance.

If you want to perform the auto health check via ECLI, refer to the document [IPWorks Auto Health Check](#).

1.1 Prerequisites

This section states the prerequisites for performing the health check procedure.

1.1.1 Documents

Before starting this procedure, ensure that the following information or documents are available:

- For how to use Ericsson Command-Line Interface (ECLI), refer to [Ericsson Command-Line Interface User Guide](#).
- The current IPWorks version in the system.
- The network plan and the System Controller (SC) address of the cluster.

1.1.2 Conditions

By default all actions are performed on the SC, unless otherwise specified.

1.2 Related Information

For the trademark information, typographic conventions, definition, and explanation of acronyms and terminology, see the following documents:

- [Glossary of Terms and Acronyms](#)
- [Trademark Information](#)
- [Typographic Conventions](#)



2 Health Check Procedure

2.1 Checking Alarms

To check active alarms reported by the system:

1. Log on to ECLI.

```
#ssh <user>@<OAM IP Address> -p <port> -t -s cli
```

Note: The <user> can be root or IPWadministrator depending if Local Authorization is enabled or not.

2. Verify that no active alarms are shown.

```
>show ManagedElement=<Node Name>,SystemFunctions=1,Fm=1,total  
Active
```

The output must be zero. The string <node_name> is specific for the ME.

3. If active alarms are present, check them.

```
>show ManagedElement=<Node Name>,SystemFunctions  
=1,Fm=1 -m FmAlarm  
show ManagedElement=<Node Name>,SystemFunctions=1,Fm=1 -m FmAlarm | filter
```

For specific information on alarms, refer to [IPWorks Alarm List](#).

4. Log out.

```
#exit
```

2.2 Checking UUID for Alarms

To check UUID on SC or PL:

```
# cat /sys/devices/virtual/dmi/id/product_uuid
```

2.3 Checking LDE Dump Files

1. For core dumps at Linux Distribution Extensions (LDE) level, check that the directory /cluster/dumps is empty.
2. If the directory is not empty, gather the information and report it to the next level of support.



2.4 Checking Core Middleware Services

Check that the state of the following system items at Core Middleware (Core MW) level is Status OK:

```
#cmw-status node app csiass comp node sg si siass su | grep
PresenceState | grep -v UNINSTANTIATED
```

The output must be empty.

If the output is not empty, use the following command to collect the information and report it to the next level of support.

```
#cmw-status node app csiass comp node sg si siass su pm
```

2.5 Checking CPU Load

1. On the SC, enter the following:

```
#for VAR in /etc/cluster/nodes/all/*/hostname; do echo
$(<$VAR); ssh $(<$VAR) "mpstat -P ALL"; done;
```

```
SC-1
Linux 3.12.55-52.42-default (SC-1)      08/29/16      _x86_64_      (2 CPU)
03:46:00  CPU      %usr    %nice    %sys %iowait    %irq    %soft    %steal    %guest    %gnice   %idle
03:46:00  all       2.18    0.13    2.41    0.37    0.00    0.28    0.06    0.00    0.00    94.56
03:46:00    0       2.18    0.13    2.42    0.31    0.00    0.26    0.00    0.00    0.00    94.69
03:46:00    1       2.18    0.13    2.40    0.43    0.00    0.30    0.12    0.00    0.00    94.44
SC-2
Linux 3.12.55-52.42-default (SC-2)      08/29/16      _x86_64_      (2 CPU)
03:46:01  CPU      %usr    %nice    %sys %iowait    %irq    %soft    %steal    %guest    %gnice   %idle
03:46:01  all       1.00    0.05    1.48    0.22    0.00    0.16    0.07    0.00    0.00    97.03
03:46:01    0       0.99    0.05    1.54    0.16    0.00    0.15    0.14    0.00    0.00    96.97
03:46:01    1       1.00    0.05    1.43    0.28    0.00    0.16    0.00    0.00    0.00    97.09
PL-3
Linux 3.12.55-52.42-default (PL-3)      08/29/16      _x86_64_      (2 CPU)
03:46:01  CPU      %usr    %nice    %sys %iowait    %irq    %soft    %steal    %guest    %gnice   %idle
03:46:01  all       2.77    0.00    4.79    0.07    0.00    0.47    0.01    0.00    0.00    91.89
03:46:01    0       2.81    0.00    4.85    0.07    0.00    0.44    0.01    0.00    0.00    91.82
03:46:01    1       2.74    0.00    4.74    0.07    0.00    0.50    0.00    0.00    0.00    91.95
PL-4
Linux 3.12.55-52.42-default (PL-4)      08/29/16      _x86_64_      (2 CPU)
03:46:01  CPU      %usr    %nice    %sys %iowait    %irq    %soft    %steal    %guest    %gnice   %idle
03:46:01  all       2.57    0.00    4.43    0.03    0.00    0.38    0.01    0.00    0.00    92.57
03:46:01    0       2.60    0.00    4.51    0.03    0.00    0.35    0.02    0.00    0.00    92.48
03:46:01    1       2.54    0.00    4.36    0.03    0.00    0.41    0.00    0.00    0.00    92.66
```

2. Verify that the %idle column shows values higher than 20%.

2.6 Checking Disk Use

1. On both SCs, enter the command:

```
#df -h -x tmpfs -x devtmpfs
```



Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/vda2	20G	2.4G	17G	13%	/
/dev/vda4	9.8G	634M	8.6G	7%	/var/log
/dev/vda1	3.9G	136M	3.5G	4%	/boot
/dev/mapper/lde--cluster--vg-lde--cluster--lv	50G	3.6G	44G	8%	/.cluster
169.254.100.101:/.cluster	50G	3.6G	44G	8%	/cluster
/dev/vda5	99G	2.6G	91G	3%	/local/ipworks
com_fuse_module	50G	3.6G	44G	8%	/var/filem/nbi_root

2. Verify that the used disk space does not exceed 80%, otherwise, clean up this partition.

2.7 Checking Memory Use

1. On every SC and PL, enter the following, enter the following:

```
# /opt/ipworks/common/scripts/ipworks_memory_health_check
```

```
SC-1
3.02633
SC-2
3.09388
PL-3
17.2859
PL-4
30.867
```

2. Verify that the free memory represents more than 10% of the total memory in all nodes.

2.8 Checking Internal Communication

All the links must be up. On the SC, enter the following:

```
#for VAR in /etc/cluster/nodes/all/*/hostname; do echo $(<$VAR);
ssh $(<$VAR) /sbin/tipc-config -n -l; done;
```

```
SC-1
Neighbors:
<1.1.2>: up
<1.1.3>: up
<1.1.4>: up
Links:
broadcast-link: up
1.1.1:eth0-1.1.2:eth0: up
1.1.1:eth0-1.1.3:eth0: up
1.1.1:eth0-1.1.4:eth0: up
SC-2
Neighbors:
<1.1.1>: up
<1.1.3>: up
<1.1.4>: up
```




```

Links:
broadcast-link: up
1.1.2:eth0-1.1.1:eth0: up
1.1.2:eth0-1.1.3:eth0: up
1.1.2:eth0-1.1.4:eth0: up
PL-3
Neighbors:
<1.1.1>: up
<1.1.2>: up
<1.1.4>: up
Links:
broadcast-link: up
1.1.3:eth0-1.1.1:eth0: up
1.1.3:eth0-1.1.2:eth0: up
1.1.3:eth0-1.1.4:eth0: up
PL-4
Neighbors:
<1.1.1>: up
<1.1.2>: up
<1.1.3>: up
Links:
broadcast-link: up
1.1.4:eth0-1.1.1:eth0: up
1.1.4:eth0-1.1.2:eth0: up
1.1.4:eth0-1.1.3:eth0: up

```

2.9 Checking Controller Status

To check or verify the controller status:

1. Log on to the SC.

```
# ssh <username>@<OAM IP Address>
```

2. Retrieve the Distributed Replicated Block Device (DRBD) state:

```
# drbdsetup status drbd0 --verbose --statistics
```

Example output:

```

drbd0 node-id:0 role:Secondary suspended:no
write-ordering:flush
volume:0 minor:0 disk:UpToDate
SC-2 node-id:1 connection:Connected role:Primary congested:no
volume:0 replication:Established peer-disk:UpToDate resync-suspended:no

```

Check the output result:

- Make sure that the SC is connected. That is, the value of the connection state field (connection) is connected.



- Make sure that the disk state is normal. That is, the value of the disk field is UpToDate.
 - Determine if the SC is primary or secondary by checking the role field:
 - On the primary SC: role:Primary
 - On the secondary SC: role:Secondary
3. Execute below command on both SC-1 and SC-2.

```
# drbdadm get-gi drbd0 | awk '{print substr($1,18,16)}'
```

The output **MUST** be 0000000000000000, otherwise the status is abnormal.

2.10 Checking Virtual IP Status

To check virtual IP status:

1. Run script on SC1.

```
SC-1:~ #/opt/ipworks/common/scripts/ipworks_evip_health_check
```

2. Check the result.

If the result is STATUS OK, the output is shown as the example below:

```
Connection closed by foreign host.
Connection closed by foreign host.
Connection closed by foreign host.
STATUS OK
```

If the result is STATUS NOT OK, proceed to check Abstract Load Balancer (ALB) Status.

- a. Connect to the eVIP CLI:

```
# telnet `/opt/vip/bin/getactivecontrol` 25190
```

- b. See the configured Abstract Load Balancer (ALB), and check that every listed ALB has status ACTIVE:

```
> show albs
```

```
0 : 'ipw_sig_sp' : ACTIVE
1 : 'ipw_data_sp' : ACTIVE
```

```
OK
```



- c. Use `show agents` for each listed ALB, check the agents status, and verify that all eVIP links or agents are ACTIVE, ACTIVE UP, and ACTIVE RDY.

```
> show agents ipw_sig_sp |grep -v '\[0\]'
```

```
> show agents ipw_data_sp |grep -v '\[0\]'
```

Take `show agents ipw_sig_sp` for example:

```
+-----[ ALB ipw_sig_sp (ACTIVE) ]-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| pagent (4)                                     | lbesel_pn (28)
|[4] fe80::ff:fe01:21 : ACTIVE                  |[4] fe80::ff:fe01:21 : ACTIVE
|[3] fe80::ff:fe01:1f : ACTIVE                  |[3] fe80::ff:fe01:1f : ACTIVE
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ersipc (0)                                     | repdb (28)
|[4] fe80::ff:fe01:21 : ACTIVE                  |[4] fe80::ff:fe01:21 : ACTIVE
|[3] fe80::ff:fe01:1f : ACTIVE                  |[3] fe80::ff:fe01:1f : ACTIVE
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| lbeagent (44)                                 | lbesel_lbe (12)
|[4] fe80::1:f4ff:fe01:4 : ACTIVE               |[4] fe80::1:f4ff:fe01:4 : ACTIVE
|[3] fe80::1:f4ff:fe01:3 : ACTIVE               |[3] fe80::1:f4ff:fe01:3 : ACTIVE
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| feeagent (46)                                 | sesel_fe (12)
|[4] fe80::1:f6ff:fe01:19 : ACTIVE UP           |[4] fe80::1:f6ff:fe01:19 : ACTIVE
|[3] fe80::1:f6ff:fe01:17 : ACTIVE UP           |[3] fe80::1:f6ff:fe01:17 : ACTIVE
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| seagent (12)                                 | lbesel_se (34)
|[4] fe80::1:f5ff:fe01:e : ACTIVE RDY           |[4] fe80::1:f5ff:fe01:e : ACTIVE
|[3] fe80::1:f5ff:fe01:d : ACTIVE RDY           |[3] fe80::1:f5ff:fe01:d : ACTIVE
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| sesel_se (10)                                 |
|[4] fe80::1:f5ff:fe01:e : ACTIVE                |
|[3] fe80::1:f5ff:fe01:d : ACTIVE                |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ikeagent (0)                                 | ipsecuagent (6)
|                                                |[4] fe80::ff:fe01:22 : ACTIVE R
|                                                |[3] fe80::ff:fe01:20 : ACTIVE R
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
eRSIP state: ACTIVE                                cIPSEC state: ACTIVE
```

- d. Exit the eVIP CLI:

```
# exit
```

2.11 Checking Latest Available Backup

1. Log on to ECLI.

```
#ssh <user>@<OAM IP Address> -p <port> -t -s cli
```

Note: The <user> can be root or IPWadministrator depending if Local Authorization is enabled or not.

2. Get the name of the latest created backup.

```
> show ManagedElement=<Node Name>,SystemFunctions=1,BrM=1,BrmB
ackupManager=SYSTEM_DATA,BrmBackupLabelStore=SYSTEM_DATA,last
CreatedBackup
```



```
lastCreatedBackup="<latest Backup name>" <read-only>
```

3. Get the date of the latest created backup.

```
>show -v ManagedElement=<Node Name>,SystemFunctions=1,BrM=1,B  
rmBackupManager=SYSTEM_DATA,BrMBackup=<latest Backup name> |  
filter creationTime
```

4. Log out.

```
>exit
```

5. Check that the latest backup is not older than 48 hours. This figure is just a recommendation, it depends on the periodicity of the scheduled backup in the system.

2.12 Checking IPWork Counters

1. To verify that the PmJob instances are active for the different IPWorks activated modules, execute the following command checking the ones that start with IPWorks:

```
#cmw-pmjob-list
```

Note:

- Other counters can be also active in the node.
- Currently, independently of the module's activated, all IPWorks counters are active in the system by default.

2. Check that the IPWorks counters are stored under:

```
#ssh <user>@<OAM IP Address> -p <port> -t -s cli
```

```
>show ManagedElement=<Node Name>,SystemFunctions=1,FileM=1,Logi  
calFs=1,FileGroup=PerformanceManagementReportFiles
```

The counters are accessible also under `/var/filem/nbi_root/PerformanceManagementReportFiles` from one of the Service Controllers (SCs).

Note:

- The `<user>` can be `root` or `IPWadministrator` depending if Local Authorization is enabled or not.
- Because of a current bug already reported, Local Authorization cannot be enabled in the node to access these files.

3. Go to the file location of IPWroks coutners and decompress the files using `gunzip` if there are compression files.



```
#cd /var/filem/nbi_root/PerformanceManagementReportFiles
```

- If there is no compression files there, go to Step 4 directly.
- If CompressionType is configured as GZIP, the counters files will be compressed. Firstly decompress the files.

Here is an example for DnsASDNSDefaultJob, in which compressionType is configured as GZIP.

```
>ManagedElement=IPWorkNode1,SystemFunctions=1,Pm=
1,PmJob=DnsASDNSDefaultJob
(PmJob=DnsASDNSDefaultJob)>show
PmJob=DnsASDNSDefaultJob
  compressionType=GZIP
  currentJobState=ACTIVE
  granularityPeriod=ONE_MIN
  reportingPeriod=ONE_MIN
  MeasurementReader=mr_1
(PmJob=DnsASDNSDefaultJob)>
```

Decompress the latest files using gunzip from the location in the SC.

```
#gunzip A20160603.2035+0200-2040+0200_1.xml.gz
```

Note: Although it complains about lack of permission, the operation is successful.

4. Look for IPWorks counters reflecting an undesired behavior.

The file specified here is just an example.

```
grep -i "userunknown unabletocomply rejected notallowed invalid
toobusy dontmatch unsupported missing" A20160603.2030+0200-20
40+0200_1.xml
```

2.13 Checking Nodes Restart

1. Enter the following:

```
#for VAR in /etc/cluster/nodes/all/*/hostname; do echo
$(<$VAR); ssh $(<$VAR) who -b; done;
```

2. Check that the date corresponds to the latest backup restore, or the latest planned cluster, or node reboot.

2.14 Checking IPWorks Application Logs

This section describes how to check server logs.



2.14.1 Checking DNS Logs

To check the DNS logs:

1. Log on to the PL which DNS starts on.

```
#ssh <username>@<OAM IP Address>
```

2. Display the errors logs.

```
#cat /cluster/storage/no-backup/ipworks/logs/<PL  
hostname>/ipworks_dns.log* | grep -i error
```

The expected result is that there is no major error information related to server start or traffic.

2.14.2 Checking ASDNS Logs

To check the ASDNS logs:

1. Log on to the PL which ASDNS starts on.

```
#ssh <username>@<OAM IP Address>
```

2. Display the error logs.

```
#cat /cluster/storage/no-backup/ipworks/logs/<PL  
hostname>/ipworks_asdnsmon.log* | grep -i error
```

The expected result is that there is no major error information related to server start or traffic.

2.14.3 Checking SS Logs

To check the SS logs:

1. Log on to the SC which Storage Server starts on.

```
#ssh <username>@<OAM IP Address>
```

2. Display the errors logs.

```
#cat /cluster/storage/no-backup/ipworks/logs/<SC  
hostname>/ipworks_ss_SC*.log* | grep -i error
```

The expected result is that there is no major error information related to server start or traffic.



2.14.4 Checking ENUM Logs

To check the ENUM logs:

1. Log on to the PL which ENUM starts on.

```
# ssh <username>@<PL which ENUM starts on IP Address>
```

2. Display the error logs.

```
#cat /cluster/storage/no-backup/ipworks/logs/<PL
hostname>/ipwenum.log* | grep -i error
```

The expected result is that there is no major error information related to server start or traffic.

2.14.5 Checking ENUM-FE Logs

To check the ENUM-FE logs:

1. Log on to the PL which ENUM-FE starts on.

```
#ssh <username>@<OAM IP Address>
```

2. Display the error logs.

```
#cat /cluster/storage/no-backup/ipworks/logs/<PL
hostname>/ipworks_enumfe_wrapper.log* | grep error
```

```
#cat /cluster/storage/no-backup/ipworks/logs/<PL
hostname>/ipworks_fesync.log* | grep error
```

The expected result is that there is no major error information related to server start or traffic.

2.14.6 Checking Radius AAA Logs

To check the Radius AAA logs:

1. Log on to the active SC.

```
#ssh <username>@<OAM IP Address>
```

2. Display the error logs.

```
#cat /cluster/storage/no-backup/ipworks/logs/<PL
hostname>/aaa_radius_stack.log* | grep -I error
```

```
#cat /cluster/storage/no-backup/ipworks/logs/<PL
hostname>/aaa_radius_backend.log* | grep -i error
```



The expected result is that there is no major error information related to server start or traffic.

2.14.7 Checking EPC AAA Logs

To check the EPC AAA logs:

1. Log on to the active SC.

```
#ssh <username>@<OAM IP Address>
```

2. Display the error logs.

```
#cat /cluster/storage/no-backup/ipworks/logs/<PL  
hostname>/aaa_diameter_server.log* | grep -i error
```

The expected result is that there is no major error information related to server start or traffic.

2.14.8 Checking DHCPv4 Logs

To check the dhcpv4 logs:

1. Log on to the active SC.

```
#ssh <username>@<OAM IP Address>
```

2. Display the error logs.

```
#cat /cluster/storage/no-backup/ipworks/logs/<PL  
hostname>/ipworks_dhcpv4.log* | grep -i error
```

The expected result is that there is no major error information related to server start or traffic.

2.15 Checking MySQL Nodes Status

Use the following command to check all the MySQL nodes state on SCs. The expected result is that at least the nodes (id: 1, 2, 27, 28) are started and one of the nodes (id: 3 or 4) is started.

For example:

```
# /etc/init.d/ipworks.mysql show-status
```

```
Connected to Management Server at: localhost:1186  
Cluster Configuration  
-----  
[ndbd(NDB)]      2 node(s)
```




```

id=27 @169.254.100.1 (mysql-5.6.31 ndb-7.4.12, Nodegroup: 0, *)
id=28 @169.254.100.2 (mysql-5.6.31 ndb-7.4.12, Nodegroup: 0)

[ndb_mgmd(MGM)] 2 node(s)
id=1 @169.254.100.1 (mysql-5.6.31 ndb-7.4.12)
id=2 @169.254.100.2 (mysql-5.6.31 ndb-7.4.12)

[mysqld(API)] 24 node(s)
id=3 @169.254.100.1 (mysql-5.6.31 ndb-7.4.12)

id=4 (not connected, accepting connect from SC-2)
id=5 @169.254.100.3 (mysql-5.6.31 ndb-7.4.12)
id=6 @169.254.100.4 (mysql-5.6.31 ndb-7.4.12)
id=7 @169.254.100.4 (mysql-5.6.31 ndb-7.4.12)
id=8 @169.254.100.3 (mysql-5.6.31 ndb-7.4.12)
id=9 (not connected, accepting connect from any host)
id=10 (not connected, accepting connect from any host)
id=11 (not connected, accepting connect from any host)
id=12 (not connected, accepting connect from any host)
id=13 (not connected, accepting connect from any host)
id=14 (not connected, accepting connect from any host)
id=15 (not connected, accepting connect from any host)
id=16 (not connected, accepting connect from any host)
id=17 (not connected, accepting connect from any host)
id=18 (not connected, accepting connect from any host)
id=19 (not connected, accepting connect from any host)
id=20 (not connected, accepting connect from any host)
id=21 (not connected, accepting connect from any host)
id=22 (not connected, accepting connect from any host)
id=23 (not connected, accepting connect from any host)
id=24 (not connected, accepting connect from any host)
id=25 (not connected, accepting connect from any host)
id=26 (not connected, accepting connect from any host)

```

The example shows that the nodes (id: 27, 28, 1, 2, 3, 4, 5, 6, 7, 8) are started.

2.16 Checking Number of MySQL Tables

If all the MySQL NDB nodes are started, use the following command to check number of the IPWorks relevant tables on the SC:

For example:

```

# /usr/local/mysql/bin/mysql -P 3307 -h ipw_sql --protocol=tcp
-e "SELECT count(*) FROM information_schema.TABLES where
table_schema='ipworks' or table_schema='ipw_prov_aaa' or
table_schema='ipw_enum';"

```



```
+-----+
| count(*) |
+-----+
|      336 |
+-----+
```

The expected result is that the number of tables is 336.

2.17 Checking Software Release Version

The operator can check the software version by ECLI or the command **cmw-repository-list**.

The expected result is that the correct software and version are installed on the machine. For details, refer to [View Software Information](#).

Note: On System Controller (SC), the command **cmw-repository-list** shows versions of all the installed software, including the installed software on Payload (PL).

On PL, the command only shows the versions of the installed software on the PL.

2.18 Checking License

To check or verify the license information of IPWorks servers:

1. Start an ECLI session on the active SC.

```
# ssh <username>@<OAM IP Address> -p 22 -t -s cli
```

2. Navigate to the Lm Managed Object (MO), for example:

```
> ManagedElement=<Node Name>,SystemFunctions=1,Lm=1
```

3. View the license information, for example:

```
(Lm=1)>show-table -m FeatureKey -p keyId,name,productType,validFrom,expiration
```

```
=====
| keyId          | name          | productType | validFrom | expiration |
=====
| FAT1023219/1   | FAT1023219/1 | IPWorks     | 2015-6-2  | 2016-8-21  |
=====
| FAT1023219/5   | FAT1023219/5 | IPWorks     | 2015-6-2  | 2016-8-21  |
=====
```

```
(Lm=1)>show-table -m CapacityKey -p keyId,name,productType,validFrom,expiration
```



```
=====
| keyId          | name          | productType | validFrom | expiration |
|=====|=====|=====|=====|=====|
| FAT1023219/4   | FAT1023219/4 | IPWorks     | 2015-6-2  | 2016-8-21  |
|=====|=====|=====|=====|=====|
| FAT1023219/2   | FAT1023219/2 | IPWorks     | 2015-6-2  | 2016-8-21  |
|=====|=====|=====|=====|=====|
```

The expected result is that the all the ordered licenses are not expired.

For more information about the `Lm` MO, refer to the class `Lm` in Managed Object Model (MOM).

2.19 Checking LDAP Connections

To check LDAP connections between IPWorks and CUDB when ENUM-FE or ERH-FE is activated, do the following:

1. Log on to the PL which ENUM starts on.

```
# ssh <username>@<OAM IP Address>
```

```
# ssh PL-X
```

2. Show LDAP connections between IPWorks and CUDB.

```
# netstat -apn | grep 389 | grep ESTABLISHED
```

The expected result is as below:

```
tcp          0      0 10.170.19.188:33024 80.0.5.141:389    ESTABLISHED 8863/ipwenum
```

Note: Either ENUM-FE or ERH-FE is activated, 16 connections are ESTABLISHED. If both of them are activated, 32 connections are ESTABLISHED.

2.20 Checking SOAP Listening Status

To check SOAP listening is OK when ENUM-FE is activated, do the following:

1. Log on to the PL which fesync starts on.

```
# ssh <username>@<OAM IP Address>
```

See Section 3.12.5 to get which PL fesync starts on.

2. Show SOAP connections between IPWorks and CUDB.

```
# netstat -apn | grep 808
```

The expected result is as below:



```
tcp      0      0 0.0.0.0:8080      0.0.0.0:*        LISTEN   8312/java
```

2.21 Checking Backup Files

To check backup files, the following sections work for all IPWorks modules to check backup files.

Prerequisites:

- Backup must be created, refer to [Create Backup](#).

2.21.1 Checking the Backup Files

To check the backup files, do the following:

1. Log on to a System Controller by using SSH.

```
# ssh <username>@<OAM IP Address>
```

2. List the content of backup archive.

- For system backup,

```
# cd /cluster/brf/backup
```

```
# ls -lrt
```

- For user backup,

```
# cd /cluster/ipwbrf/backup/
```

```
# ls -lrt
```

In the command output, all backup files are listed. For backup files of different IPWorks modules, see the following subsections.

The expected results:

- All backup files are listed.
- Created time is correct.

Note: Use command `tar -tvf <File name>` to check the backed-up files.

For example:

```
/cluster/ipwbrf/backup/ndb_testUserDataBackup_2076 tar
-tvf ndb_testUserDataBackup_2076.tar.gz
```



2.21.2 SS Backup Files

The following SS-related files are included in the backup file which is created in Section 2.21.1 on page 16:

```
/cluster/home/ipworks/etc/root_cert.cfg  
/cluster/home/ipworks/etc/ipworks_ss_lm.conf  
/cluster/home/ipworks/etc/ipworks_ss.conf
```

Example 1 SS Backup Files

2.21.3 DNS Backup Files

The following DNS-related files are included in the backup file which is created in Section 2.21.1 on page 16:

```
/cluster/home/ipworks/etc/ipworks_asdnsmonsm.conf  
/cluster/home/ipworks/etc/ipworks_dnssm.conf  
/cluster/home/ipworks/etc/<hostname>/ipworks_dns.conf  
/cluster/home/ipworks/etc/<hostname>/ipworks_asdnsmon.conf
```

Example 2 DNS Backup Files

2.21.4 MySQL NDB Cluster Backup Files

The following MySQL NDB Cluster related files are included in the backup file which is created in Section 2.21.1 on page 16:

```
/cluster/home/ipworks/etc/mysql/confd/ipworks_mgm.conf  
/cluster/home/ipworks/etc/mysql/confd/ipworks_datanode_my.conf  
/cluster/home/ipworks/etc/mysql/confd/ipworks_sqlnode.conf
```

Example 3 MySQL NDB Cluster Configuration Files

If the backup file contains the MySQL data, use command `tar -tvf file_name.tar.gz` to check the backed-up files under `/cluster/ipwbrf/backup/<BACKUP NAME>`. The MySQL dump files are listed as follows:

`ipworks_dump.gz`

`ipw_prov_aaa_dump.gz`

`ipw_enum_dump.gz`

`ipw_dhcp_dump.gz`

`mysql_user_dump.sql`



2.21.5 ENUM Backup Files

The following ENUM-related files are included in the backup file which is created in Section 2.21.1 on page 16:

```
/cluster/home/ipworks/etc/enum/ipworks_enum.conf  
/cluster/home/ipworks/etc/enum/ldap_cluster.conf  
/cluster/home/ipworks/etc/ldapschema/ldap_dictionary.xml  
/cluster/storage/system/config/ss7caf-ana90137/etc/cp.cnf  
/cluster/storage/system/config/ss7caf-ana90137/etc/ecm.xml  
/cluster/storage/system/config/ss7caf-ana90137/etc/oam.cnf  
/cluster/storage/system/config/ss7caf-ana90137/etc/signmgr.cnf  
/cluster/storage/system/config/ss7caf-ana90137/etc/ss7license.lic
```

Example 4 ENUM Backup Files

2.21.6 ENUM-FE Backup Files

The following ENUM-FE related files are included in the backup file:

```
/cluster/home/ipworks/etc/enumfe/axis2.xml
```

Example 5 ENUM-FE Backup Files

2.21.7 Radius AAA Backup Files

The following Radius AAA-related directory (including all the sub folder and files) are included in the backup file which is created in Section 2.21.1 on page 16:

```
/cluster/home/ipworks/etc/PL-3/aaa_radius/  
/cluster/home/ipworks/etc/PL-4/aaa_radius/  
/cluster/home/ipworks/etc/aaa_radius/
```

Example 6 Radius AAA Backup Files

2.21.8 EPC AAA Backup Files

The following EPC AAA-related directory (including all the sub folder and files) are included in the backup file which is created in Section 2.21.1 on page 16:

```
/cluster/home/ipworks/etc/PL-4/aaa_diameter/  
/cluster/home/ipworks/etc/PL-3/aaa_diameter/  
/cluster/home/ipworks/etc/aaa_diameter/
```

Example 7 EPC AAA Backup Files



2.21.9 DHCPv4 Backup Files

The following DHCPv4-related directory (including all the sub folder and files) are included in the backup file which is created in Section 2.21.1 on page 16:

```
/cluster/home/ipworks/etc/ipworks_dhcpv4sm.conf
/cluster/home/ipworks/etc/<PL hostname>/ipworks_dhcpv4.conf
/cluster/home/ipworks/etc/<PL hostname>/dhcp/dhcpd.conf
/cluster/home/ipworks/etc/<PL hostname>/dhcp/dhcpkey.conf
/cluster/home/ipworks/etc/<PL hostname>/dhcp/dhcpv4
Option82format.conf
```

Example 8 DHCP Backup Files

2.22 Checking AAA Service Port Listening Status

2.22.1 Checking Radius AAA Service Port Listening Status

To check whether service port is listened correctly, do the following:

1. Log on to a System Controller by using SSH.

```
# ssh <username>@<OAM IP Address>
```

2. Check whether Radius AAA process is up.

```
# ipw-ctr status all
```

aaa_radius_stack, aaa_radius_backend, and aaasm must be running on all Payloads.

The expected result is as below:

```
on PL-3:
aaa_diameter is running.
aaa_radius_stack is running.
aaa_radius_backend is running.
aaasm is running.
```

```
on PL-4:
aaa_diameter is running.
aaa_radius_stack is running.
aaa_radius_backend is running.
aaasm is running.
```

3. Log on to PL-3 and check whether port 1812, 1813, 3799 and 3800 are listened correctly.

```
# ssh PL-3
```



```
# netstat -anp | grep 1812

udp 0 0 0.0.0.0:1812 0.0.0.0:* 30730/a3radiusd

#netstat -anp | grep 1813

udp 0 0 0.0.0.0:1813 0.0.0.0:* 30730/a3radiusd

# netstat -anp | grep 3799

udp 0 0 0.0.0.0:3799 0.0.0.0:* 30730/a3radiusd

# netstat -anp | grep 3800

udp 0 0 0.0.0.0:3800 0.0.0.0:* 30730/a3radiusd
```

4. Repeat Step 3 on PL-4.

Note: For PL-4, 3800 port should be 3801 according to the formula $380x=3799+(4-2)$ defined in IPWorks IPTables Service Configuration.

5. If the result is not shown as expected, refer to section Radius AAA Server in IPWorks Troubleshooting Guideline.

2.22.2 Checking EPC AAA Service Port Listening Status

To check whether service port is listened correctly, do the following:

1. Log on to a System Controller by using SSH.

```
# ssh <username>@<OAM IP Address>
```

2. Check whether EPC AAA process is up.

```
# ipw-ctr status all
```

aaa_diameter and aaasm must be running on all Payloads.

The expected result is as below:

on PL-3:

```
aaa_diameter is running.
aaa_radius_stack is running.
aaa_radius_backend is running.
aaasm is running.
```

on PL-4:

```
aaa_diameter is running.
aaa_radius_stack is running.
aaa_radius_backend is running.
aaasm is running.
```




3. Log on to PL-3 and check whether port 20001 is listened correctly.

```
# ssh PL-3
```

```
# netstat -anp | grep 20001
```

The expected result is as below:

```
tcp    0  0 169.254.100.3:20001 0.0.0.0:*  LISTEN  8508/beam.smp
```

4. Log on to PL-3 and check whether port 3868 is listened correctly.

```
# ssh PL-3
```

```
# netstat -anp | grep 3868
```

The expected result is as below:

```
tcp    0  0 192.168.20.193:3868 0.0.0.0:*  LISTEN  12745/DiaS
```

5. Repeat Step 4 on PL-4.
6. If the result is not shown as expected, refer to section Radius AAA Server in [IPWorks Troubleshooting Guideline](#).

2.23 Checking DHCPv4 Service Port Listening Status

To check whether service port is listened correctly, do the following:

1. Log on to a System Controller by using SSH.

```
# ssh <username>@<OAM IP Address>
```

2. Check whether DHCPv4 process is up.

```
# ipw-ctr status all
```

dhcp and dhcpsm must be running on all Payloads.

The expected result is as below:

```
on SC-1 :
ss is running as active role.
sqlnodemgr is running as active role.
```

```
on SC-2 :
ss is running as standby role.
sqlnodemgr is running as standby role.
```

```
on PL-3:
dhcp is running.
```



```
dhcpcsm is running.
```

```
on PL-4:
```

```
dhcp is running.
```

```
dhcpcsm is running.
```

3. Log on to PL-3 and check whether port 67 is listened correctly.

```
# ssh PL-3
```

```
# netstat -anp | grep 67
```

The expected result is as below:

```
udp 0 0 10.170.15.65:67 0.0.0.0:* 16417/dhcpd
```

4. Repeat Step 3 on PL-4.
5. If the result is not shown as expected, refer to section DHCPv4 Server in IPWorks Troubleshooting Guideline.

3 Problem Reporting

For details, refer to IPWorks Troubleshooting Guideline for any abnormal situation. If the problem still exists, consult the next level support.

Before reporting the problem, it is important to collect the related data according to Data Collection Guideline for IPWorks.



Reference List

Ericsson Documents

- [1] Ericsson Command-Line Interface User Guide
- [2] IPWorks Troubleshooting Guideline
- [3] Data Collection Guideline for IPWorks
- [4] Command Line Interface User Guide for IPWorks SS
- [5] IPWorks Measurement List
- [6] Performance Management Report File Format
- [7] IPWorks Configuration Management
- [8] License Management
- [9] Backup and Restore
- [10] IPWorks Alarm List
- [11] IPWorks Auto Health Check