**LIST MATCHING DOCUMENTATION**

Updated: Apr 15, 2016

**Scripts**

hostInfoReports.ksh: generates 4 different reports that contain all the nodes’ information

* hostInfoReport.txt: contains all info including name, date, os, kernel, model, cpu, zonetype and other physical attributes.
* hardwareReport.txt: contains name, date, os, kernel, model, cpu, zonetype.
* softwareReport.txt: contains Uptime version, NetBackup version, and rsync version.
* zonelistReport.txt: contains name, date, zonelist.

listMatching.ksh: takes in list of nodes from each tool (BoKS, NetBackup, etc.) to generate a MasterTable (1).

listMatchingReports.ksh: generates 6 different reports:

* Yes\_NA\_Report.txt: A text file that contains the number of 'YES's and 'N/A's/total for each source with percentages, respectively.
* Extra\_Hosts\_Report.txt: A text file that contains all the lists of extra hosts that don’t supposed to be in the source but end up appearing in the MasterTable.
* Expired\_Exceptions\_Report.txt: A text file that contains all the expired exceptions as of the date the script runs.
* Exceptions\_By\_Date\_Report.txt: A text file that contains all the exceptions sorted by date.
* Exceptions\_By\_Hostname\_Report.txt: A text file that contains all the exceptions sorted by host name.
* Missing\_Hosts\_Report.txt: A text file that contains all the missing hosts that aren't in any sources but are in the ExceptionFile (2)

convert2HTML.ksh: using information from the Master (3) with no header and the MasterTable itself to convert MasterTable into MasterTable.html and other inventory reports into their respective html files.

extractnodes-for-listMatching.ksh: extract registered nodes out of a central administrative tool (NetBackup, BoKS, etc.) from each applicable node.

Example output: netbackup- psx02backup.list

extractnodes\_syscheck-for-listMatching.ksh: similar to extractnodes-for-listMatching.ksh but only for Syscheck.

Example output: syscheck-psa03mgmt.list

catSources.ksh: concatenates all lists of produced by the extractnodes-for-listmatching.ksh from a respective tool into a final list of registered nodes for that tool. Also generates a list of exclusions.

Example output: NETBACKUP.list

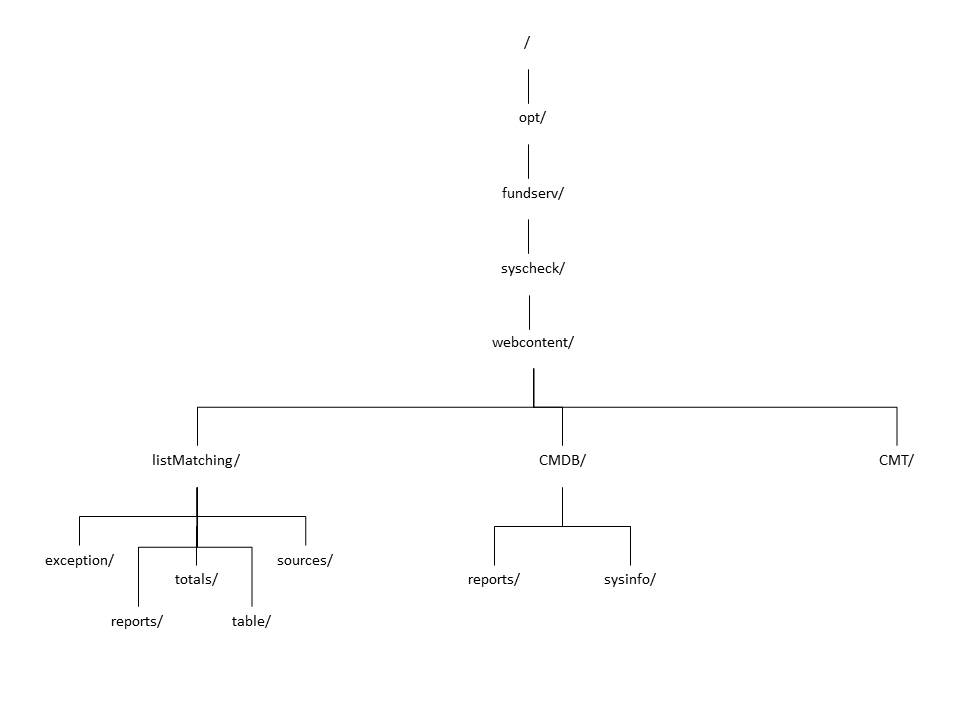
vx.ksh: generates vxdisk\_list\_info.txt (4).

IPinfo.ksh: generates hostname-IPinfo.txt (5).

collectIPinfo.ksh: collect all hostname-IPinfo.txt from all-data folder in syscheck (psa03mgmt) and concatenate them into a networkReport.txt (6).

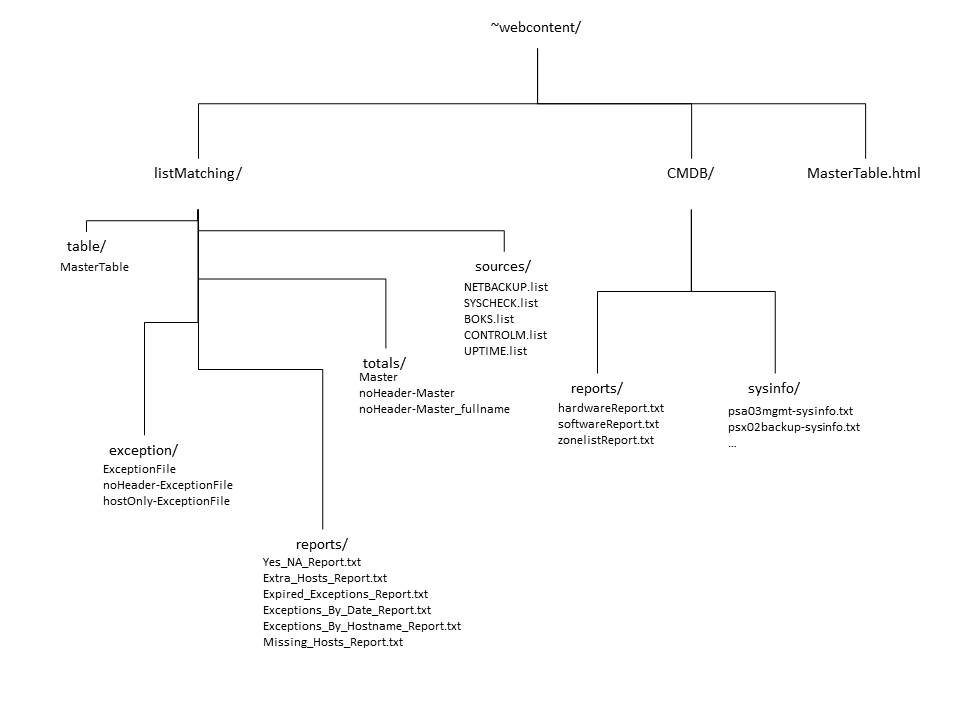
collectVXinfo.ksh: collect all vxdisk\_list\_info.txt from all-data folder in syscheck (psa03mgmt) and concatenate them into a VXReport.txt (7).

**Folder Structure**

****

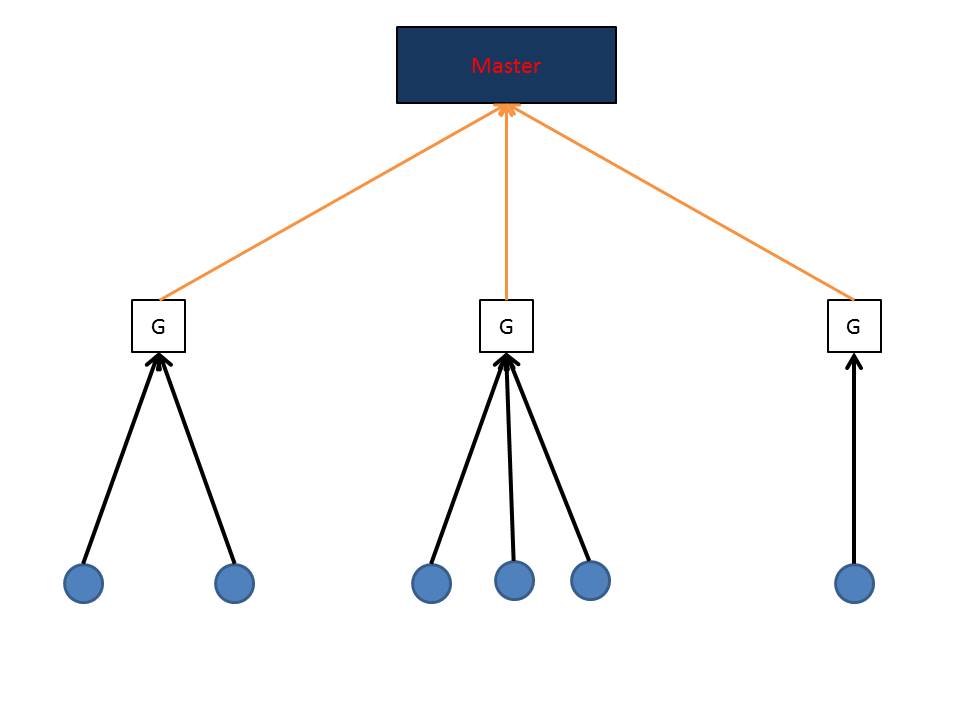
**Location of files**

\*Since nothing is currently in CMT/, we’ll leave it out for now (Mar 6)

****

**Collect and propagate procedures**

* **Collect files**

****

(ROOT) [1:00 AM/PM] common-bin/collectdata.ksh

(SYSCHECK) [1:30 AM/PM] local-bin/collectdata-local.ksh

Note:

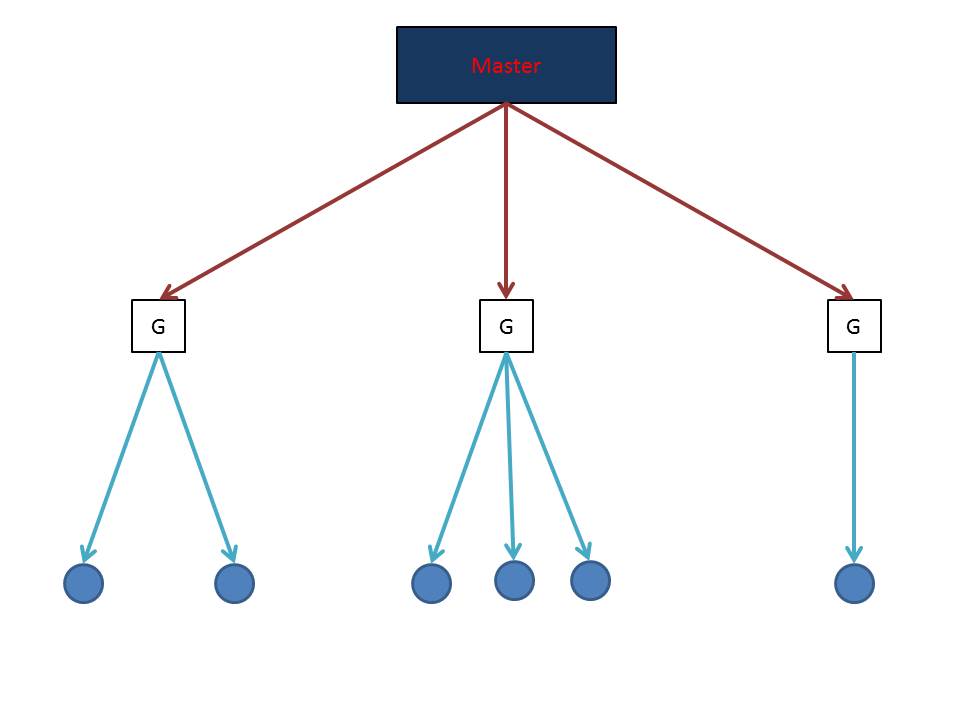
folder being collected: common-data

will collect all “**common-data**” folders from all global zones and put it into “**all-data**” folder in Master.

will use all\_dev, all\_mgt, all\_prod, all\_uat lists as targets to collect data from. All these lists are currently stored in /opt/fundserv/syscheck/local-etc.

*‘hostname’*-all.zones will be generated by collectdata.ksh and collectdata-local.ksh for global hosts.

* **Propagate files**



(SYSCHECK) [3:45 AM/PM] local-bin/rsyncwrapper-local.ksh

(ROOT) [4:00 AM/PM] common-bin/rsyncwrapper.ksh

Note:

folder being propagated: common-bin

will use all\_dev, all\_mgt, all\_prod, all\_uat lists as targets to propagate. All these lists are currently stored in /opt/fundserv/syscheck/local-etc.

*‘hostname’*-all.zones generated by collectdata.ksh and collectdata-local.ksh will be used as target hosts for propagation in global hosts.

**Procedures**

1. Collect all sources’ lists (besides Syscheck) of nodes (extractnodes-for-listMatching.ksh and catSources.ksh)
2. Collect list of nodes from Syscheck (extractnodes\_syscheck-for-listMatching.ksh)
3. Generate a Master and a MasterTable (listMatching.ksh)
4. Generate 6 general reports (listMatchingReports.ksh)
5. Generate host-related reports (hostInfoReports.ksh)
6. Convert mentioned reports and MasterTable into html format (convert2HTML.ksh)
7. Generate networkReport.txt (collectIPinfo.ksh)
8. Generate VXReport.txt (collectVXinfo.ksh)

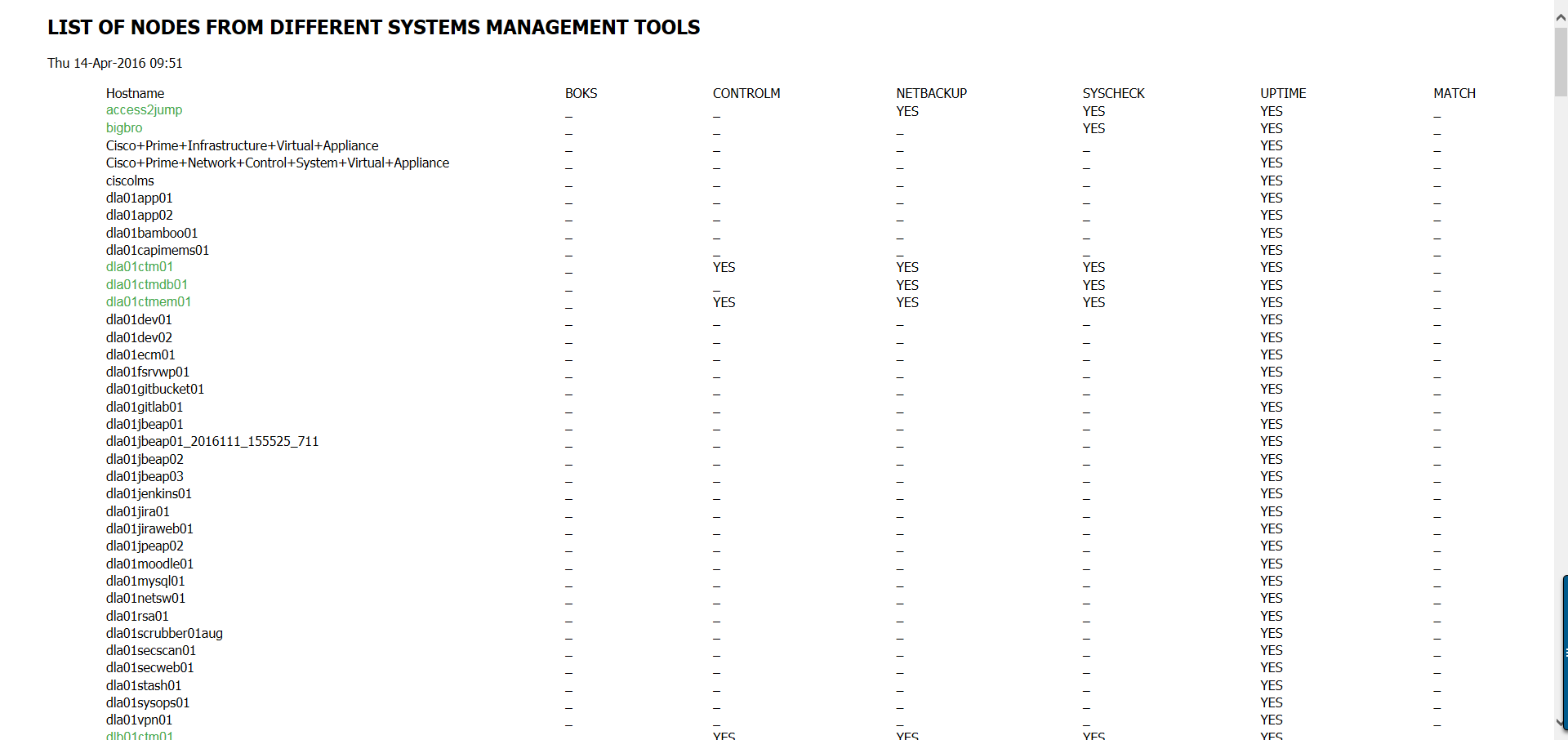
**Terminology**

1. MasterTable: a table that contains all the nodes and which nodes exist in which tool (Uptime, BoKS, NetBackup, Syscheck, Control-M)

path on syscheck:

/opt/fundserv/syscheck/webcontent/listMatching/table/MasterTable

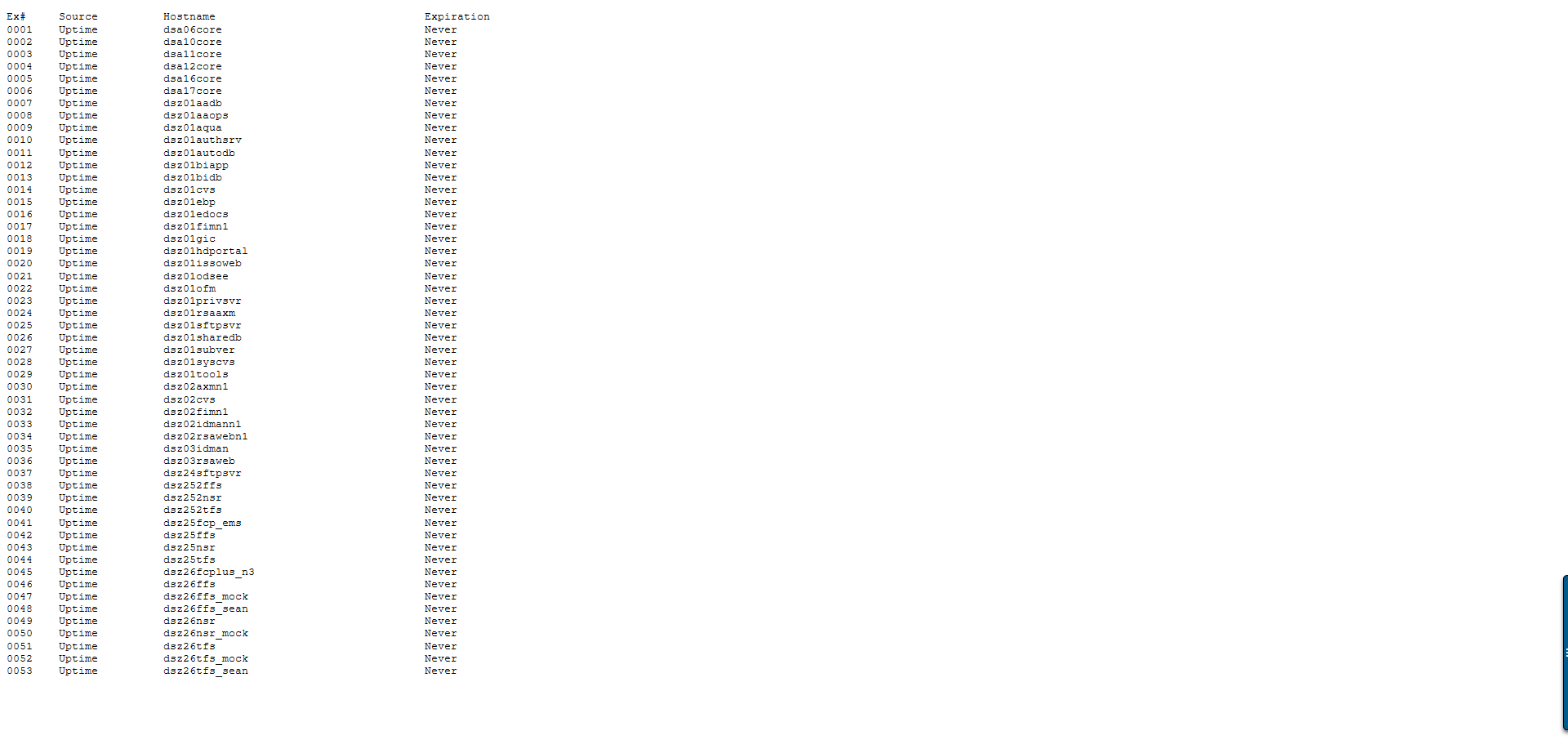
link: <http://opsportal/listMatching/MasterTable.html>



1. ExceptionFile: a table that contains all the exceptions and their respective exception ids, tools (BoKS, NetBackup, etc.), nodes’ names, and expiration status.

path on syscheck: /opt/fundserv/syscheck/webcontent/listMatching/exception/ExceptionFile

link: <http://opsportal/listMatching/exception/ExceptionFile>



1. Master: the first column of MasterTable that contains all the nodes registered in all the tools.

path on syscheck:

/opt/fundserv/syscheck/webcontent/listMatching/totals/Master

link: <http://opsportal/listMatching/totals/Master>

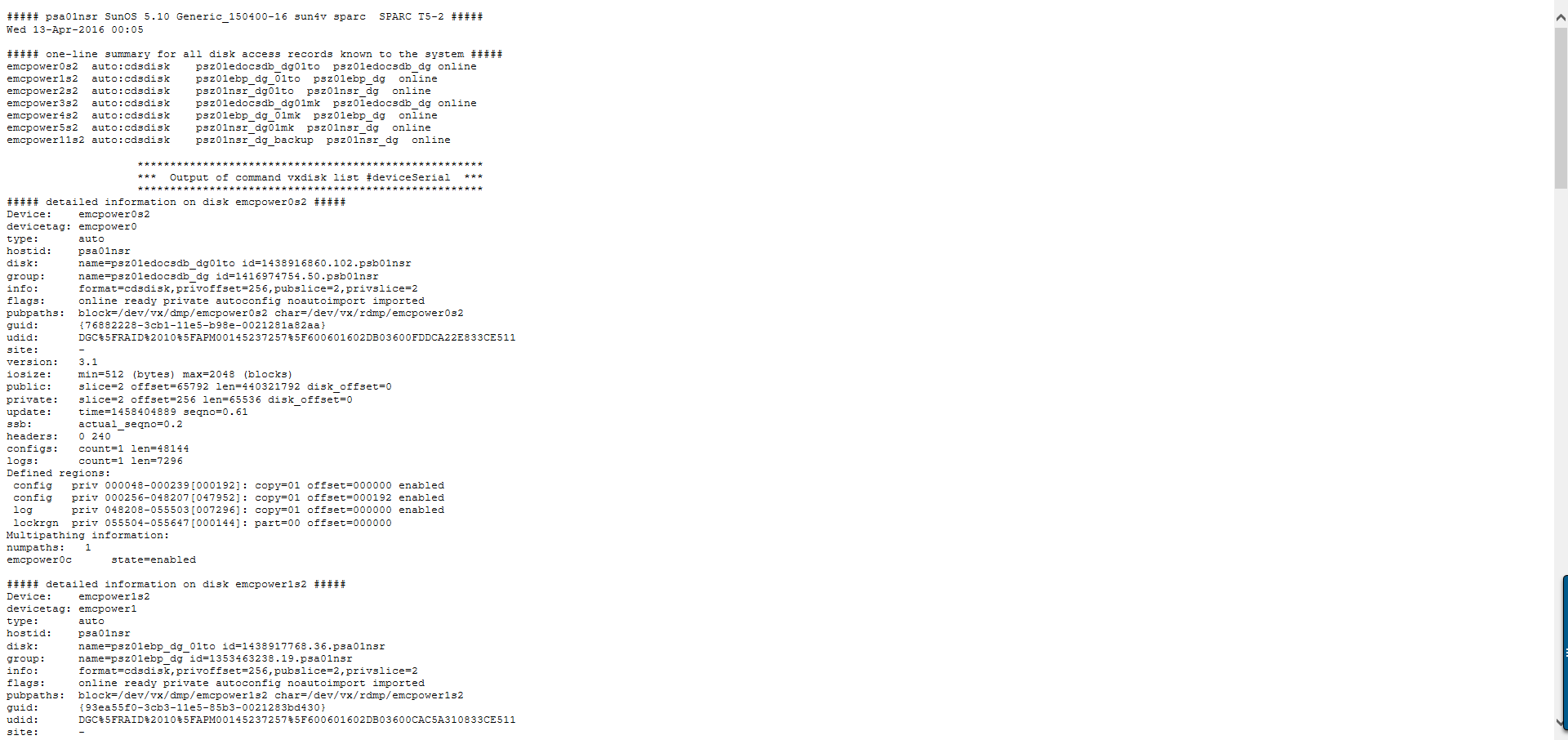


1. vxdisk\_list\_info.txt: a file that contains all the output of vxdisk list command (if exists).

path on syscheck:

/opt/fundserv/syscheck/all-data/*YMD*/*hostname*/CMDB/vxdisk\_list\_info.txt

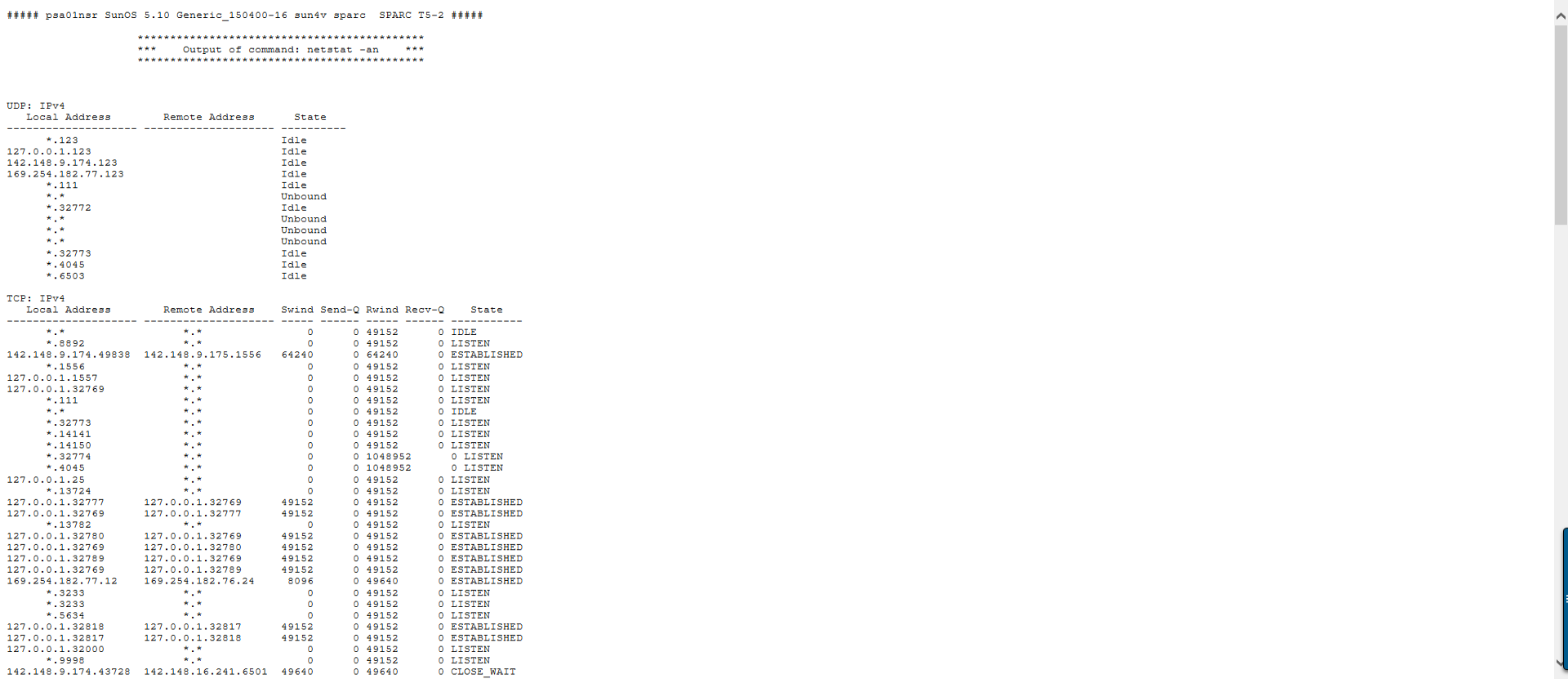
link: [http://opsportal/all-data/*YMD*/*hostname*/CMDB/vxdisk\_list\_info.txt](http://opsportal/all-data/YMD/hostname/CMDB/vxdisk_list_info.txt)



1. hostname-IPinfo.txt: a file that contains the output of command netstat –an and ifconfig –a (if exist).

path on syscheck:

/opt/fundserv/syscheck/all-data/*YMD*/*hostname*/CMDB/hostname-IPinfo.txt

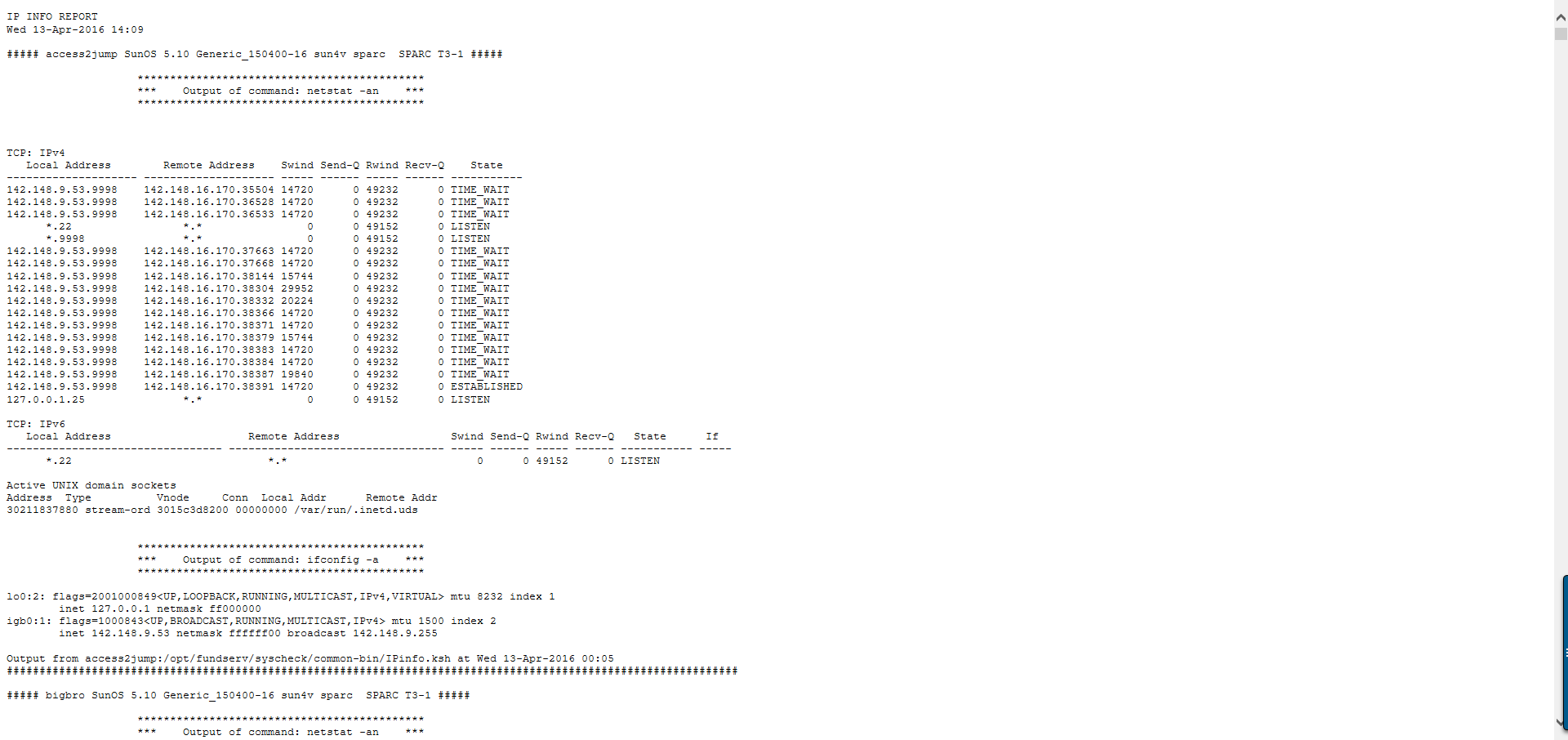
link: [http://opsportal/all-data/*YMD*/*hostname*/CMDB/*hostname*-IPinfo.txt](http://opsportal/all-data/YMD/hostname/CMDB/hostname-IPinfo.txt)

1. networkReport.txt: a list of all hostname-IPinfo.txt collected by the collectIPinfo.ksh

path on syscheck:

/opt/fundserv/syscheck/webcontent/CMDB/reports/networkReport.txt

link: <http://opsportal/CMDB/reports/networkReport.txt>

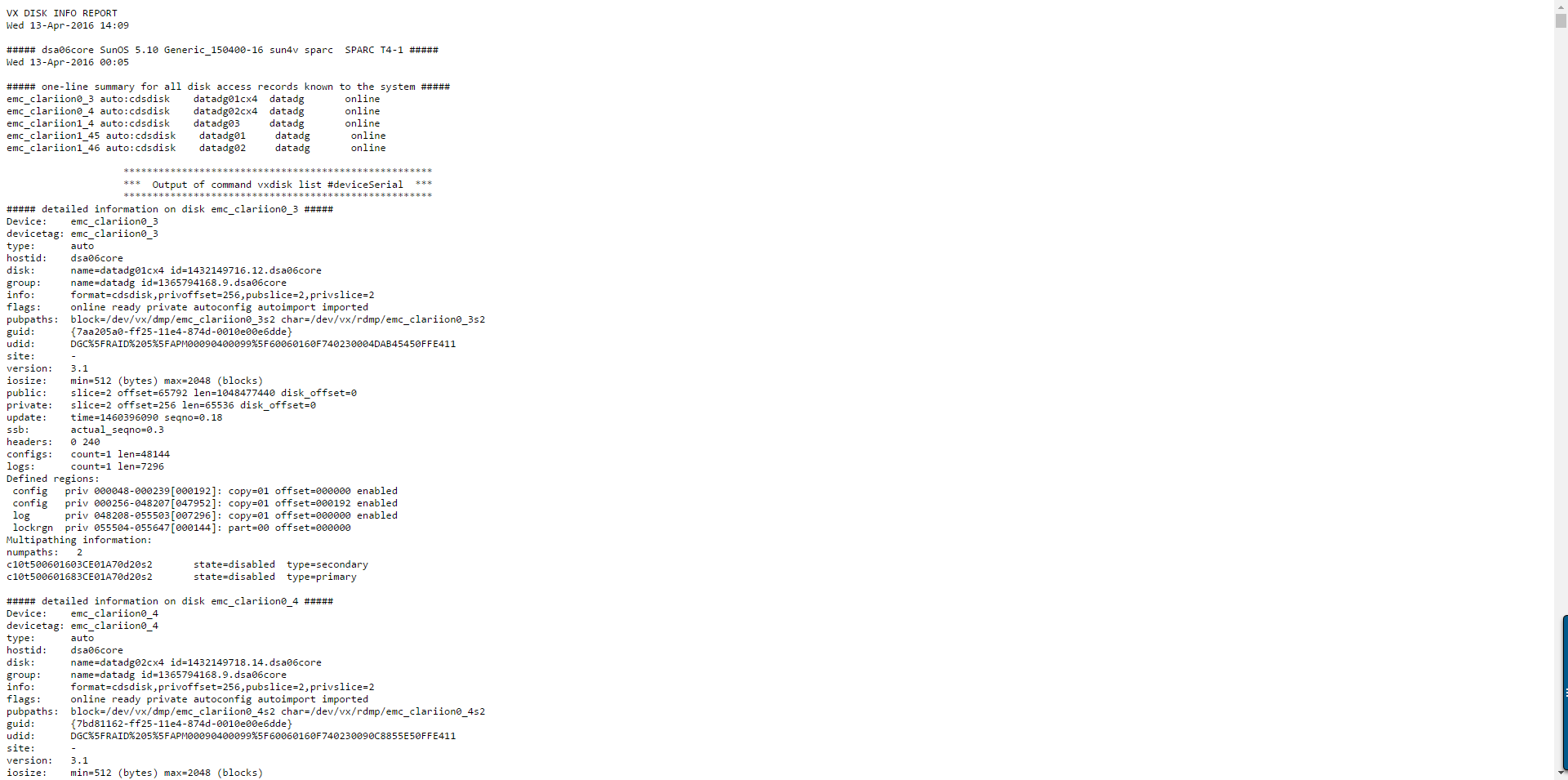


1. VXReport.txt: a list of all vxdisk\_list\_info.txt collected by the collectVXinfo.ksh

path on syscheck:

/opt/fundserv/syscheck/webcontent/CMDB/reports/networkReport.txt

link: <http://opsportal/CMDB/reports/VXReport.txt>



**Notes:**

PIKT wasn’t included in this list of tools since their it doesn’t have any central server to extract nodes from.