

VDCF - Virtual Datacenter Cloud Framework for the Solaris™ Operating System

Monitoring

Version 5.0
2 December 2025

Copyright © 2005-2025 JomaSoft GmbH
All rights reserved.

Table of Contents

1 Introduction.....	4
1.1 Overview.....	4
1.2 Hardware Monitoring.....	4
1.2.1 Alarming.....	4
1.2.2 Requirements.....	4
1.3 Resource Monitoring.....	5
1.3.1 Requirements.....	5
1.4 Operating System (OS) Monitoring.....	6
1.5 VDCF Dashboard web application.....	8
2 Installation.....	9
2.1 Prerequisites.....	9
2.2 Installation.....	9
3 Configuration.....	10
3.1 Granting User Access.....	10
3.2 Customizing Monitoring eMail.....	10
3.2.1 Alarming.....	10
3.3 Customizing Hardware Monitoring.....	11
3.3.1 Check Interval.....	11
3.3.2 Alarming.....	12
3.4 Customizing Resource Monitoring.....	13
3.4.1 Usage interval.....	13
3.4.2 Usage delivery.....	13
3.4.3 Collector and aggregator interval.....	13
3.5 Customizing OS Monitoring.....	14
3.5.1 Check Interval.....	14
3.5.2 Enable/disable components.....	15
3.5.3 Warning Threshold.....	16
3.5.4 Alarming.....	17
3.5.5 OS Security Compliance benchmarks.....	18
3.5.6 OS Security hardening profiles.....	18
3.6 Customizing VDCF Dashboard web application.....	19
3.6.1 Initial setup.....	19
3.6.2 VDCF user for the web application.....	19
3.6.3 Firewall Rules.....	19
4 Usage.....	20
4.1 Hardware Monitoring.....	20
4.1.1 Check Node manually.....	20
4.1.2 System Locator LED.....	20
4.1.3 Display Hardware state.....	21
4.1.4 Clear hardware state history.....	23
4.2 Server Power Usage.....	24
4.2.1 Configuration of different datacenter locations.....	24
4.2.2 Power Usage 'History'.....	24
4.3 Resource Monitoring.....	25
4.3.1 Enable resource monitoring.....	25
4.3.2 Usage Collector.....	25
4.3.3 Usage Aggregator.....	25
4.3.4 Disable resource monitoring.....	26
4.3.5 Update Node data manually.....	26
4.3.6 Show resource consumption data.....	27
4.4 OS Monitoring.....	29
4.4.1 Enabling / Disabling.....	29
4.4.2 Check Node manually.....	29
4.4.3 Individual warning threshold for filesystems, datasets, swap, ram and cpu.....	30
4.4.4 Individual 'Target Path Count' for a node.....	31
4.4.5 Limit failed cronjob reporting.....	31
4.4.6 Display Filesystem usage.....	32
4.4.7 Display Dataset usage.....	33
4.4.8 Display SWAP usage.....	34
4.4.9 Display SMF services.....	35
4.4.10 Display Disk Path Count.....	36
4.4.11 Display physical network interface states.....	37
4.4.12 Display RAM/CPU usage.....	37
4.4.13 Display NTP client states.....	37



4.4.14 VDCF Monitoring Report.....	38
4.5 OS Security.....	39
4.5.1 Run Security Compliance Assessments.....	39
4.5.2 Display Compliance Reports.....	40
4.5.3 OS Hardening.....	41
4.6 VDCF Dashboard web application.....	42
4.6.1 Enabling / Disabling.....	42
4.6.2 Logfiles.....	42
4.6.3 Web application screenshots.....	43

1 Introduction

This documentation describes the Monitoring features of the Virtual Datacenter Cloud Framework (VDCF) for the Solaris Operating System and explains how to use this features.

See these documents for more information about the related VDCF products:

<i>VDCF – Administration Guide</i>	for information about VDCF usage
<i>VDCF – High Availability</i>	for information about VDCF HA (Automated Failover for Zones and LDOMs)

1.1 Overview

VDCF Monitoring is a VDCF extension available to VDCF Standard and Enterprise customers.

This extension consists of four separate components:

- Hardware Monitoring (hwmon) to detect hardware failures
- Resource Monitoring (rcmon) to collect and display resource usage of global and local Solaris zones
- Operating System Monitoring (osmon) to enable alerts when filesystems, datasets, swap, SMF services, core files, network interfaces, virtual memory, disk paths, faults, ntp, cronjobs, RAM or CPU reach critical resource usage or state
- VDCF Dashboard web application

While VDCF Resource Monitoring collects and displays resource usage, VDCF Resource Management is used to configure resource limits.

1.2 Hardware Monitoring

The VDCF Hardware Monitoring connects periodically to the system controller of all Nodes defined in the VDCF repository and checks for hardware, OS state and power usage.

1.2.1 Alarming

If the VDCF Hardware Monitoring detects hardware failures the user may be informed in two ways:

- sending e-Mails
- executing a script to integrate other software products

1.2.2 Requirements

As the Hardware Monitor is based on information from the system controller it's required to configure a 'console' for each Node within VDCF.

1.3 Resource Monitoring

Resource Monitoring may be enabled (and disabled) individually for each Node. A usage collector service is then started on the Node. This service is recording the resource usage (CPU and memory) of the Node and all installed vServers. Periodically each Node is pushing the recorded data onto the VDCF Management Server.

A cron job called 'Usage Data Collector' on the Management Server is importing the collected data periodically into the VDCF database.

A second cron job 'Usage Data Aggregator' is used to generate aggregated resource information. The aggregated data can be displayed on a daily, weekly, monthly or yearly base.

A third cron job is started / stopped together with the 'Usage Data Collector' cron job. This cron job is evaluating the current average resource usage of Nodes and vServers in the last 24 hours. This information may be used later by the HA monitor Node evacuation feature.

1.3.1 Requirements

The VDCF Resource Monitoring implementation is based on Solaris 10 8/07 (Update 4) features. To use this feature the target Nodes must run Solaris 10 8/07 or later. It is supported to use an older Solaris 10 Release (Update1,2,3) with Kernel Patch 120011-14 (sparc) or 120012-14 (i386) or later.

1.4 Operating System (OS) Monitoring

Using the OS Monitoring you can monitor the filesystem usage of vServers. This Monitoring can be enabled/disabled globally on the VDCF management server. By enabling the OS Monitor a cron job for User root is added.

If the filesystem usage exceeds the defined WARNING threshold an alert eMail is sent or a RECOVERED eMail if the filesystem goes below the threshold.

New since VDCF Monitoring 2.4

OS Monitoring has been extended with dataset (zpool) and SMF monitoring.

If the dataset usage exceeds the defined WARNING threshold or a SMF service has a critical state (maintenance/degraded) an alert eMail is sent. A RECOVERED eMail is sent if the dataset usage goes below the threshold or the SMF service is back online. OS Monitoring does also send an alarm, if the zpool has a critical state (degraded or failed).

New since VDCF Monitoring 2.5

Individual warn thresholds may be defined for filesystems and datasets.

New since VDCF Monitoring 2.6

OS Monitoring has been extended with SWAP monitoring.

If the SWAP usage exceeds the defined WARNING threshold an alert eMail is sent or a RECOVERED eMail if the SWAP usage goes below the threshold.

New since VDCF Monitoring 3.0

OS Monitoring has been extended with disk path count monitoring for MPxIO SAN storage LUNs.

If the 'Current Path Count' doesn't match the 'Target Path Count' an alert eMail is sent.

When the path count gets normal again a recovered eMail is sent.

Additionally this Release introduces Security Compliance Assessments, where Nodes and vServer are checked against predefined Security Benchmarks. Solaris 11.3 is required for this feature.

Compliance reports are generated as html files and can be viewed with the VDCF Dashboard web application.

Additionally the node and vserver commands got a new function for hardening the OS to fix non-compliant systems. See Chapter 4.5.3 for details.

New since VDCF Monitoring 3.1

Node and OS filesystems Monitoring has been added. Using `osmon -c show` you have a complete Monitoring Report where you see all critical objects. When enabling the report cronjob you can produce a daily eMail report (`osmon -c enable report`).

New since VDCF Monitoring 3.3

`osmon` automatically clears SMF services with state 'maintenance'. The SMF services which should be auto cleared must be predefined:

```
-bash-3.2$ vdcfadm -c show_config | grep OSMON_SMF_AUTOCLEAR
      OSMON_SMF_AUTOCLEAR svc:/system/filesystem/minimal:default
```

`filesystem/minimal` is the default, because it may fail from time to time at boot because of busy filesystems.

New since VDCF Monitoring 3.4

Alarming of new core files has been added.

Physical network interface states are now checked and can be viewed using `osmon -c show_net`

SWAP Monitoring was enhanced. In old versions only the SWAP on disk was monitored. With this release the use of Virtual Memory is monitored additionally.

New since VDCF Monitoring 3.6

Resource usage is stored in the VDCF repository using the `rcmon` tool since several years. Now alarming was added to detect and report high resource usage over a defined period. The default limit is 80% and the default duration period is 15 minutes. The limit can be configured individually for each server where required.

zpool autoclear

Suspended zpools are automatically cleared by the `osmon update` job. This optional features improves application and server availability and is very helpful for short storage outages at night.

New since VDCF Monitoring 4.0

Alarming of new `fmadm` faults has been added.

New since VDCF Monitoring 5.0

Alarming of failed cronjobs has been added. Additionally `ntp` clients without connection to `ntp` server are reported.

1.5 VDCF Dashboard web application

New since VDCF Monitoring 3.0

Using the new 'VDCF dashboard' web application you can access the Compliance reports by some clicks in your browser. Furthermore VDCF dashboard gives access to your VDCF Repository objects: Node, CDom, Gdom, vServers and Dataset lists are available.

New since VDCF Monitoring 5.0

Additional pages for an overview of your Hardware and OS Monitoring issues are available. And a page for filesystems with high usage (70%) was added.

2 Installation

2.1 Prerequisites

The JSvdcf-monitor package requires the following VDCF packages to be installed on the VDCF Management Server:

- JSvdcf-base 10.0.0 or later

2.2 Installation

a) sparc platform

```
cd <download-dir>  
pkgadd -d ./JSvdcf-monitor_<version>_sparc.pkg
```

b) i386 platform

```
cd <download-dir>  
pkgadd -d ./JSvdcf-monitor_<version>_i386.pkg
```

3 Configuration

3.1 Granting User Access

The VDCF Monitoring package introduces two new RBAC Profiles:

- "VDCF hwmonitor Module" for the Hardware and Resource Monitoring,
- "VDCF osmonitor Module" for the OS Monitoring feature.

Assign these RBAC profiles to your admin users.

3.2 Customizing Monitoring eMail

3.2.1 Alarming

The Hardware Monitoring and OS Monitoring are able to send e-Mails, if a Hardware fault is detected or a OS Monitor threshold is reached.

To enable this feature you have to set the following variables in VDCF's customize.cfg:

```
export HWMON_EVENT=true
export OSMON_EVENT=true
export MONITOR_EVENT_EMAIL_LIST="user1@company.ch user2@company.ch"
export MONITOR_EVENT_EMAIL_FROM="root@system.domain.ch"
```

For the OS Monitor you can add additional eMail addresses per node using

```
nodecfg -c modify name=mynode email=team1@customer.com,team2@customer.com
```

3.3 Customizing Hardware Monitoring

3.3.1 Check Interval

By default the Hardware Monitoring cronjob is executed once an hour to check the state of all Nodes.

You may display the current setting with this command:

```
$ hwmon -c status

                                Central Monitor Component Status
                                HW Monitor: enabled

                                Central Monitor Component Timespec
                                Crontab timespec for HW Monitor: '15 * * * *'

                                VDCF Configuration Variables
                                HWMON_EVENT true
                                MONITOR_EVENT_EMAIL_FROM support@jomasoft.ch
                                MONITOR_EVENT_EMAIL_LIST support@jomasoft.ch
                                MONITOR_EVENT_SCRIPT /opt/jomasoft/vdcf/testing/monitor
```

To change this setting configure the cron timespec in `customize.cfg` using this variable:

```
export MONITOR_HW_INTERVAL="15 * * * *"
```

If the Hardware Monitor was already enabled before, you have to re-enable the cron job using these commands:

```
$ hwmon -c disable
HW Monitor: disabled

$ hwmon -c enable
HW Monitor: enabled
```

3.3.2 Alarming

The following state changes are reported by default

```
MONITOR_EVENT_STATE_OF_INTEREST=OK|FAULTED|N/A
```

If you want to be informed of power changes you can add this var to the customize.cfg file

```
export MONITOR_EVENT_STATE_OF_INTEREST=OK|FAULTED|N/A|PWR-OFF|PWR-ON|OS-RUN
```

Additionally to send eMails it is supported to configure a script, which is called at every event. This feature allows you to forward events to your event management or ticketing system.

```
export MONITOR_EVENT_SCRIPT=/opt/company/bin/my_vdcf_hwmon_script
```

The 'MONITOR_EVENT_SCRIPT' will be executed if a monitor event occurs. The script may use the following 5 input arguments:

```
<node> <new_state> <date> <time> <logfile name>
```

<node>	Node name where the event occurred
<new_state>	Hardware and OS state after the event occurred e.g. OK:OS-RUN FAULTED:ON-OBP N/A:N/A
<date/time>	Date and time when the event was recorded
<logfile name>	Logfile on the management server where detailed information is stored

3.4 Customizing Resource Monitoring

You may customize some aspects of the resource monitoring by overwriting this VDCF variables using the customize.cfg.

3.4.1 Usage interval

With this variable you may set the interval used to get zone usage information on the Compute Node in seconds. Using the default value of 60 produces a usage record every minute.

```
export MONITOR_ZONE_USAGE_INTERVAL=60
```

3.4.2 Usage delivery

The number of samples accumulated before delivery to the VDCF Management Server happens. The actual time between delivery of zone usage information is computed by `MONITOR_ZONE_USAGE_INTERVAL * MONITOR_ZONE_USAGE_DELIVERY`.

```
export MONITOR_ZONE_USAGE_DELIVERY=60
```

3.4.3 Collector and aggregator interval

You may display the current cron timespec setting with this command:

```
$ rcmon -c status verbose
                                Central Monitor Component Status
                                Usage Data Collector: enabled
                                Usage Data Aggregation: enabled

                                Central Monitor Component Timespec
                                Crontab timespec for Usage Data Collector: '5,25,45 * * * *'
                                Crontab timespec for Usage Data Aggregation: '0 6 * * *'
                                Crontab timespec for Usage Data 24h average: '0 23 * * *'
```

To change this settings configure the cron timespec in customize.cfg using these variables:

```
export MONITOR_USAGE_TX_INTERVAL="5,25,45 * * * *"
export MONITOR_AGGR_INTERVAL="0 6 * * *"
export CURRENT_RES_USAGE_UPDATE_INTERVAL="0 23 * * *"
```

If resource monitoring was already enabled before, you have to re-enable the cron jobs using these commands. (The 24h average cron job is controlled together with the collector cron job):

```
$ rcmon -c disable aggregator
$ rcmon -c enable aggregator

$ rcmon -c disable collector
$ rcmon -c enable collector
```

3.5 Customizing OS Monitoring

3.5.1 Check Interval

By default the OS Monitoring cronjob is executed once an hour to check the usage and states of filesystems, datasets, swap usage, SMF services, disks paths, network interface states, faults, ntp and cpu/ram usage.

You may display the current setting with this command:

```
$ osmon -c status

                                Central Monitor Component Status
                                OS Monitor: enabled
                                OS Monitor Report: enabled

                                Central Monitor Component Timespec
                                Crontab timespec for OS Monitor: '30 * * * *'
                                Crontab timespec for OS Monitor Report: '0 8 * * 1-5'

                                VDCF Configuration Variables
                                OSMON_EVENT true
                                MONITOR_EVENT_EMAIL_FROM support@jomasoft.ch
                                MONITOR_EVENT_EMAIL_LIST support@jomasoft.ch
                                OSMON_FS_WARNING 80
                                OSMON_DATASET_WARNING 80
                                OSMON_SWAP_WARNING 60
                                OSMON_REPORT_FLAGS -R -s -H -e
```

To change this setting configure the cron timespecs in customize.cfg using this variables:

```
export OSMON_FS_INTERVAL="30 * * * *"
export OSMON_REPORT_INTERVAL="0 8 * * 1-5"
```

If the OS Monitor was already enabled before, you have to re-enable the cron job using these commands:

```
$ osmon -c disable
OS Monitor: disabled

$ osmon -c enable
OS Monitor: enabled

$ osmon -c disable report
OS Monitor Report: disabled

$ osmon -c enable report
OS Monitor Report: enabled
```

3.5.2 Enable/disable components

By default all components are monitored. (`export OSMON_DEFAULT_UPDATE_STATE=all`)

You can enable only a few individual components of them using

```
export  
OSMON_DEFAULT_UPDATE_STATE=dataset, fs, swap, smf, cores, disk, net, res, faults, ntp, cron
```

After changing this variable you have to disable/enable the osmon cronjob using
`osmon -c disable` and `osmon -c enable`.

The feature zpool autoclear is disabled by default. You enable this features to automatically clear
SUSPENDED zpool using

```
export OSMON_ZPOOL_AUTOCLEAR=TRUE
```

Cronjob monitoring is disabled by default, because there are typically a lot of failed jobs. Start with
individual execution using `osmon -c update node=mynode cron`.

If failed jobs are cleaned up you can enable using

```
export OSMON_CRON_ENABLED=TRUE
```

3.5.3 Warning Threshold

The default warning threshold for filesystems and datasets is set to 80 (%).

To change this value add or modify the “OSMON_FS_WARNING” or “OSMON_DATASET_WARNING” variable in customize.cfg

```
export OSMON_FS_WARNING=70
export OSMON_DATASET_WARNING=70
```

The default warning threshold for swap usage is set to 60 (%).

To change this value add or modify the “OSMON_SWAP_WARNING” variable in customize.cfg

```
export OSMON_SWAP_WARNING=70
```

For the CPU/RAM resource usage alarming the default warning threshold is set to 80 (%).
The default duration period is 15 minutes. Both settings can be changed by adding the variables in customize.cfg

```
export OSMON_CPU_LIMIT=70
export OSMON_RAM_LIMIT=90

export OSMON_CPU_DURATION=10
export OSMON_RAM_DURATION=20
```

The reported faults can be configured using MSG-IDs or 'ALL'.
By default Kernel Panics and slow disk I/O are reported

```
export OSMON_FAULTS=SUNOS-8000-KL,DISK-8000-VP,DISK-8000-WA
```

Individual warning threshold may be set for filesystems, datasets, swap and cpu/ram. See Chapter 4.4.3 for details

3.5.4 Alarming

The OS Monitor will send WARNING e-Mails if

- filesystems reach the defined threshold
(default from OSMON_FS_WARNING or individual filesystem configuration)
- datasets reach the defined threshold
(default from OSMON_DATASET_WARNING or individual dataset configuration)
- swap usage reach the defined threshold
(default from OSMON_SWAP_WARNING or individual node configuration)
- zpool datasets reach a critical state (faulted, degraded or suspended)
(default from OSMON_ZPOOL_STATE_OF_INTEREST)

To receive eMails when a mirror operation starts and ends you can optionally add "RESILVERING" to the OSMON_ZPOOL_STATE_OF_INTEREST

- Solaris SMF services or Linux services reach a critical state (degraded or maintenance)
- MPxIO or iSCSI disks fail to reach the defined Target Path Count
- new cores files are created
- used physical network interfaces go DOWN
- RAM or CPU usage reach the defined threshold during the defined period
- fmadm faults are detected (which matches OSMON_FAULTS MSG-ID's)
- ntp clients are not in sync with the ntp servers
- failed cronjobs are found (if OSMON_CRON_ENABLED=TRUE)

3.5.5 OS Security Compliance benchmarks

Solaris 11.3 includes 3 predefined standard benchmarks 'baseline', 'recommended' and 'pci-dss'. VDCF delivers additional tailorings named 'default' and 'cdom' both based on the 'baseline' benchmark. These tailorings are stored in this configuration directory:

```
$ ls -l /var/opt/jomasoft/vdcf/conf/compliance/*.tailor
-rw-r--r--  1 root    root          1314 Sep 11 15:31 cdom.tailor
-rw-r--r--  1 root    root          1321 Sep 11 15:31 default.tailor
```

Customers can define additional benchmarks by copying and modifying the tailor files. For system individual benchmarks the files can be named <vserver>.tailor or <node>.tailor.

3.5.6 OS Security hardening profiles

Use the 'node -c harden help' command to get a list of available hardening rules and the available hardening profiles. You can create your own hardening profiles matching your security guidelines.

The hardening profiles must be stored in:

```
$ ls -l /var/opt/jomasoft/vdcf/conf/compliance/*.hardening
-rw-r--r--  1 root    other          578 Oct 23 14:22 baseline.hardening
```

3.6 Customizing VDCF Dashboard web application

3.6.1 Initial setup

VDCF dashboard is a python based web application. Integrated into your Apache http server. To setup the Apache Server config you have to run this command once:

```
# /opt/jomasoft/vdcf/mods/setup/setup_gui [ -p <apache https port> ]  
Creating self-signed Test Certificate ...  
Configuring apache web server ...  
Apache restarted successfully. VDCF dashboard is ready on this URL:  
https://yourserver:443
```

The web application requires user authentication. Users are authenticated against their local Solaris User Account. For security reasons the web application is running SSL-enabled.

The setup script configures Apache with a self-signed test server certificate! Please replace it by a valid server certificate. The certificate is configured in this apache file:

```
# grep SSLCertificate /etc/apache2/2.*conf.d/vdcf_django_httpd_2*.conf  
SSLCertificateFile /var/opt/jomasoft/vdcf/conf/apache-cert/dashboard.crt  
SSLCertificateKeyFile /var/opt/jomasoft/vdcf/conf/apache-cert/dashboard.key
```

3.6.2 VDCF user for the web application

The web application is using the read-only vdcf user `vdcfgui` to access the VDCF repository.

Using the VDCF `vpool` command you can define what data you want to show to `vdcfgui` user and i.e. display in the VDCF dashboard.

3.6.3 Firewall Rules

If your system environment contains firewalls you may have to add a firewall rule to access the webserver on the VDCF management Server:

VDCF Management Server	Direction	Browser Client	Comment
WebServer (port 443)	←		Web server port depends on your apache configuration, default is 443 (see chapter 3.6)

4 Usage

4.1 Hardware Monitoring

Enabling / Disabling

The hardware monitoring feature can be enabled/disabled globally.

```
$ hwmon -c enable  
$ hwmon -c disable
```

Use the status command to display the current state of hardware monitoring:

```
$ hwmon -c status  
  
Central Monitor Component Status  
HW Monitor: enabled  
  
Central Monitor Component Timespec  
Crontab timespec for HW Monitor: '15 * * * *'  
  
VDCF Configuration Variables  
HWMON_EVENT true  
MONITOR_EVENT_EMAIL_FROM support@jomasoft.ch  
MONITOR_EVENT_EMAIL_LIST support@jomasoft.ch  
MONITOR_EVENT_SCRIPT /opt/jomasoft/vdcf/testing/monitor
```

It's also possible to disable or enable specific Nodes from being monitored:

```
$ hwmon -c disable node=s0003  
HW Monitor disabled for Node s0003
```

4.1.1 Check Node manually

If the hwmon is enabled a cron job is checking periodically the state of all Nodes. To check a Node manually you may issue this command:

```
$ hwmon -c update all | node=<node name>
```

4.1.2 System Locator LED

The hardware monitoring feature let you also control the system locator LED.

Displays the current state of the Locator LED as either on or off:

```
$ hwmon -c show_locator node=<node name>  
Locator led is OFF
```

Turns the locator LED on:

```
$ hwmon -c set_locator node=<node name>
```

Turns the locator LED off:

```
$ hwmon -c clear_locator node=<node name>
```



4.1.3 Display Hardware state

Using the show operation an overview about all Nodes is displayed.

```
$ hwmon -c show
```

```
Current Hardware State
Node Model Console Soft State HW State Last Change Last Update Mon..
s0003 SUNW,Sun-Fire-T1000 ALOMCMT PWR-OFF OK 2013-04-22 2013-04-22 ON
s0024 ORCL,SPARC-T4-1 ILOM OS-RUN OK 2012-06-04 2013-04-23 ON
```

Using the Node attribute and/or verbose flag the state history and details from the system controller is shown.

```
$ hwmon -c show node=s0003
```

```
Current Hardware State
Node Model Console Soft State HW State Last Change Last Update Mon..
s0003 SUNW,Sun-Fire-T1000 ALOMCMT PWR-OFF OK 2013-04-22 2013-04-22 ON
```

```
State Change History
Node Soft State HW State Event Date
s0003 OS-RUN OK 2010-08-18 09:15:01
s0003 PWR-OFF OK 2010-05-25 17:15:02
```

```
$ hwmon -c show node=s0003 verbose
```

```
Current Hardware State
Node Model Console Soft State HW State Last Change Last Update Mon..
s0003 SUNW,Sun-Fire-T1000 ALOMCMT PWR-OFF OK 2013-04-22 2013-04-22 ON
```

```
State Change History
Node Soft State HW State Event Date
s0003 OS-RUN OK 2010-08-18 09:15:01
s0003 PWR-OFF OK 2010-05-25 17:15:02
```

```
System Locator Status
Locator led is OFF
```

```
System Specific Status Informations
```

```
==== Environmental Status =====
```

```
-----
System Temperatures (Temperatures in Celsius):
-----
```

Sensor	Status	Temp	LowHard	LowSoft	LowWarn	HighWarn	HighSoft	HighHard
MB/T_AMB	OK	24	-10	-5	0	45	50	55
MB/CMP0/T_CORE	OK	40	-10	-5	0	85	90	95
MB/CMP0/T_BCORE	OK	39	-10	-5	0	85	90	95
MB/IOB/T_CORE	OK	37	-10	-5	0	95	100	105

```
-----
System Indicator Status:
-----
```

```
SYS/LOCATE SYS/SERVICE SYS/ACT
OFF OFF ON
```


Fans (Speeds Revolution Per Minute):

Sensor	Status	Speed	Warn	Low
FT0/F0	OK	9166	2240	1920
FT0/F1	OK	8776	2240	1920
FT0/F2	OK	8967	2240	1920
FT0/F3	OK	8967	2240	1920

Voltage sensors (in Volts):

Sensor	Status	Voltage	LowSoft	LowWarn	HighWarn	HighSoft
MB/V_VCORE	OK	1.32	1.20	1.24	1.36	1.39
MB/V_VMEM	OK	1.78	1.69	1.72	1.87	1.90
MB/V_VTT	OK	0.87	0.84	0.86	0.93	0.95
MB/V_+1V2	OK	1.18	1.09	1.11	1.28	1.30
MB/V_+1V5	OK	1.48	1.36	1.39	1.60	1.63
MB/V_+2V5	OK	2.50	2.27	2.32	2.67	2.72
MB/V_+3V3	OK	3.29	3.06	3.10	3.49	3.53
MB/V_+5V	OK	4.99	4.55	4.65	5.35	5.45
MB/V_+12V	OK	12.18	10.92	11.16	12.84	13.08
MB/V_+3V3STBY	OK	3.31	3.13	3.16	3.53	3.59

System Load (in amps):

Sensor	Status	Load	Warn	Shutdown
MB/I_VCORE	OK	23.360	80.000	88.000
MB/I_VMEM	OK	6.420	60.000	66.000

Current sensors:

Sensor	Status
MB/BAT/V_BAT	OK

Power Supplies:

Supply	Status	Underspeed	Overtemp	Overvoltage	Undervoltage	Overcurrent
PS0	OK	OFF	OFF	OFF	OFF	OFF

Last POST run: WED AUG 18 05:52:20 2010
POST status: Passed all devices

No failures found in System

4.1.4 Clear hardware state history

A history record is generated for every hardware state change discovered by the periodical (or manually initiated) system check.

To clear all history records of a Node:

```
$ hwmon -c clear_history node=<node name>
```

4.2 Server Power Usage

New since VDCF Monitoring 2.6

The actual Usage (Watts) is collected during the health check of the hardware (by default once an hour).

Use this command to show the current power usage of all nodes and a summary for each datacenter location:

```
$ hwmon -c show_power
```

By default there is no datacenter location configured for a server. If you need the power usage summarized by the datacenter location, you must enable the datacenter location feature first:

4.2.1 Configuration of different datacenter locations

The 'DataCenter' is optional and can be enabled by creating the file `/var/opt/jomasoft/vdcf/conf/datacenter.cfg`

In this file you list all your physical datacenter locations. For example:

```
$ cat /var/opt/jomasoft/vdcf/conf/datacenter.cfg
#NODE DataCenters
#DCName,default -> Default Datacenter
#DCName -> additional DataCenter
#DCName allowed characters and number, no special characters
ZUERICH,default
NEWYORK
SINGAPORE
```

The datacenter attribute is displayed using `nodecfg -c show`, but only if you add 'DATACENTER' to the `NODECFG_SHOW_ATTR` variable in `customize.cfg`.

To modify the datacenter attribute, use the following command:

```
-bash-3.2$ nodecfg -c modify name=<node name> datacenter=<datacenter>
```

4.2.2 Power Usage 'History'

The power changes are logged to a separate VDCF logfile `/var/opt/jomasoft/vdcf/log/hwmon_power.log` where you can see the history of each node.

This log can be disabled by setting the variable 'HWMON_POWER_LOG' to 'FALSE'.

Sample Output of Logfile:

```
$ tail -f /var/opt/jomasoft/vdcf/log/hwmon_power.log
16:09:2016 17:41:24 LOG PowerUsage change discovered for node: s0024 old usage: 317 Watts new usage: 314 Watts
16:09:2016 17:41:25 LOG PowerUsage change discovered for node: s0009 old usage: 213 Watts new usage: 0 Watts
16:09:2016 17:41:27 LOG PowerUsage change discovered for node: s0013 old usage: 62 Watts new usage: 65 Watts
```

4.3 Resource Monitoring

4.3.1 Enable resource monitoring

The recording of resource usage information may be activated individually for each Node. By enabling a Node a `usage_collect` service is started on the Node. After the defined interval (`MONITOR_ZONE_USAGE_INTERVAL`) a usage record is saved locally on the Node. After a defined number of records (`MONITOR_ZONE_USAGE_DELIVERY`) are saved the `usage_collect` service transfers the data to the VDCF management server.

To enable usage collection on Nodes use this command:

```
$ rcmon -c enable      node=<node name> | node all
```

To display the status of resource monitoring for all Nodes use this command:

```
$ rcmon -c status node

                Central Monitor Component Status
                Usage Data Collector: enabled
                Usage Data 24h average: enabled
                Usage Data Aggregation: enabled

                Node Monitor Component Status
                Usage Data Collection on s0002: enabled
                Usage Data Collection on s0003: enabled
```

4.3.2 Usage Collector

The usage data transferred from the Nodes is imported periodically into the VDCF repository using the 'Usage Data Collector' cron job.

You enable this collector using:

```
$ rcmon -c enable collector
```

When enabling the collector a further cron job is enabled: The 'Usage Data 24h average' cron job is a summary function to calculate the average resource usage of all Nodes and vServers in the last 24 hours. To display that average data use the `rcmon -c summary` command.

4.3.3 Usage Aggregator

To avoid using up too much space on the VDCF management server VDCF offers a 'Usage Data Aggregation'. This cron job aggregates old data.

```
$ rcmon -c enable aggregator
```

Usage records older than a week are aggregated to a record per hour.

Usage records older than a month are aggregated to a record per day.

4.3.4 Disable resource monitoring

Same procedure as for enabling the resource monitoring components

Disable collection on Nodes:

```
$ rcmon -c disable node=<node name> | node all
```

Disable Usage Data Collector:

```
$ rcmon -c disable collector
```

Disable Usage Data Aggregation:

```
$ rcmon -c disable aggregator
```

4.3.5 Update Node data manually

You may request an update of the database with the newest usage data available.

This command restarts the usage collector service on the Node and transfers back the current usage data file to the VDCF management server. Followed by an import into the VDCF repository.

```
$ rcmon -c update node=<node name> | node all
```



4.3.6 Show resource consumption data

To show the collected usage information for a vServer or a Node use the show operation.

```
rcmon -c show          cpu | memory | memory_extended
                      hourly | daily | monthly | yearly
                      server=<server name>
                      [ verbose ]

                      [ gz_total | gzt ]
```

```
rcmon -c show          cpu | memory | memory_extended
                      from=<'time-spec'>
                      server=<server name>
                      [ to=<'time-spec'> ]
                      [ aggr=<aggr-spec> ]
                      [ verbose ]
                      [ gz_total | gzt ]
```

For explanation of the command flags and output, please see manpage 'rcmon -H show' for detailed information. Some examples:

The following command lists the available CPU usage information of the last hour with no further aggregation:

```
$ rcmon -c show server=s0180 cpu hourly
```

```
----- Pool -----   --- CpuShr ---   --- CpuSys ---   --- CpuUsr ---
--- CpuAll --   -- CpuSAll --
DateTime          ID/Type  Max   Cur   All   Min /Avg /Max   Min /Avg /Max   Min /Avg /Max
Min /Avg /Max   Min /Avg /Max   Name
2010-08-26 18:48:18 30/priv 15   2     8.3% - 100% -   -   0.0% -   -   0.0% -
-   0.0% -   -   0.0% -   s0180
2010-08-26 18:49:19 30/priv 15   2     8.3% - 100% -   -   0.0% -   -   0.0% -
-   0.0% -   -   0.0% -   s0180
...
```

This command lists a Nodes memory consumption during the last month. It includes summed up resource values of the global and the non global zones:

```
$ rcmon -c show server=s0003 memory monthly gzt
```

```
----- RamTot -----   ---- RamKern ----   ---- RamFree ----   ---- RamUse ----
---- RamUtil ----   ---- VmUse ----   ---- VmUtil ----
DateTime          Min / Avg / Max   Min / Avg / Max   Min / Avg / Max   Min / Avg / Max
Min / Avg / Max   Min / Avg / Max   Name
2010-07-26 23:59:07 -   1920M -   -   1625M -   -   427M -   -   455M -
-   24% -   -   367M -   -   18% -   s0003
2010-07-27 23:59:36 -   1920M -   -   1628M -   -   423M -   -   456M -
-   24% -   -   367M -   -   18% -   s0003
...
```



The following command lists the used memory resources of a vServer of the last 5 hours:

```
$ rcmon -c show server=s0180 memory from="-5 hours" aggr=hour
```

----- VmUtil -----		---- RamKern ----			---- RamUse -----			---- RamUtil ----			----- VmUse -----		
DateTime	Min / Avg / Max	Min	Avg	Max	Min	Avg	Max	Min	Avg	Max	Min	Avg	Max
2010-08-26 14:59:51	2.0% 2.0% 2.0%	1614M	1614M	1615M	-	48M	-	-	12%	-	-	42M	-
		Name s0180											
2010-08-26 15:59:37	2.0% 2.0% 2.0%	1614M	1615M	1615M	-	48M	-	-	12%	-	-	42M	-
		Name s0180											
2010-08-26 16:59:23	2.0% 2.0% 2.0%	1615M	1615M	1616M	48M	48M	48M	12%	12%	12%	-	42M	-
		Name s0180											
2010-08-26 17:59:39	2.0% 2.0% 2.3%	1615M	1616M	1618M	48M	49M	55M	12%	12%	14%	42M	43M	49M
		Name s0180											
2010-08-26 18:59:25	- 2.0% -	1617M	1617M	1618M	49M	49M	49M	12%	12%	12%	-	42M	-
		Name s0180											
2010-08-26 19:47:04	- 2.0% -	1617M	1618M	1618M	-	49M	-	-	12%	-	-	42M	-
		Name s0180											

Use this summary operation to display the average resource usage data of the last 24 hours. Results may be ordered by ram, cpu or server name in ascending or descending order. Default ordering is ram descending:

```
$ rcmon -c summary sortkey=cpu
```

24h resource usage average ordered by cpu/desc:

Node	Total RAM	Free RAM	Total CPU	Free CPU	LastUpdate	Comment
s0003	768	40 (5.2%)	800	795 (99.4%)	2011-10-11 23:00:28	Sol 11
s0006	2048	135 (6.6%)	658	612 (93.0%)	2011-12-06 23:00:20	Sol 10
s0009	1024	615 (60.1%)	193	188 (97.4%)	2011-12-06 23:00:17	Bank01

vServer	Used RAM	Used CPU	CPU Pool	LastUpdate	Comment
v0104	25	1	0	2011-11-30 23:00:33	Exkl IP im AccessNet
v0100	50	1	0	2011-12-04 23:00:19	ZFS vServer
v0101	50	1	0	2011-12-06 23:00:20	on Diskset
v0103	50	1	0	2011-12-06 23:00:21	Virtual Server v0103
v0105	50	1	0	2011-12-06 23:00:23	ufs to zfs
v0106	50	1	0	2011-12-06 23:00:26	VDCF Zone

The data shown for free ram and free cpu are reduced by a percentage reserved for the global zone (Node). This reserved percentage of the total ram/cpu can be configured using these framework variables:

```
# - Minimum RAM required/reserved for NODE in %
export RESOURCE_NODE_RAM_MIN=10
# - Minimum CPU required/reserved for NODE in %
export RESOURCE_NODE_CPU_MIN=0
```

The data of the summary operation is also used by the Node evacuation feature. The configured percentage is used to prevent overloading a Node with too many vServers.

4.4 OS Monitoring

The OS Monitor is used to monitor the following components

- vServer and Node filesystems
 - SMF services
 - Dataset for Node and vServer (including local zfs rpoools)
 - Node SWAP usage
 - MPxIO SAN disk path count
 - Network interface states
 - CPU/RAM usage
 - fmadm faults
 - ntp clients
 - failed cronjobs
- Security Compliance (manually triggered only)

4.4.1 Enabling / Disabling

The OS Monitoring feature can be enabled/disabled globally.

```
$ osmon -c enable
```

```
$ osmon -c disable
```

Use the status command to display the current state of the OS monitoring:

```
$ osmon -c status
```

4.4.2 Check Node manually

If the osmon is enabled a cron job is checking periodically the state and usage of all OS Monitor objects.

To update monitoring values in the database manually you may issue this command:

```
$ osmon -c update all | node=<node name>
```

4.4.3 Individual warning threshold for filesystems, datasets, swap, ram and cpu

You can set an individual threshold for a specific filesystem, dataset or node swap.

To update the threshold for a filesystem, issue the following command:

```
$ osmon -c modify_fs server=<server name> mountpoint=<mountpoint> warnover=<percent>
```

To update the threshold for a dataset, issue the following command:

```
$ osmon -c modify_dataset server=<server name> dataset=<dataset> warnover=<percent>
```

To update the threshold for the swap usage (disk), issue the following command:

```
$ osmon -c modify_swap node=<node name> warnover=<percent>
```

To update the threshold for the swap usage (virtualmemory), issue the following command:

```
$ osmon -c modify_swap node=<node name> warnover=<percent> virtualmem
```

To update the threshold for the cpu usage, issue the following command:

```
$ osmon -c modify_cpu server=<server> name> warnover=<percent>
```

To update the threshold for the ram usage, issue the following command:

```
$ osmon -c modify_ram server=<server> name> warnover=<percent>
```

To remove an individual threshold use the 'remove_warn' flag:

```
$ osmon -c modify_fs server=<server name> mountpoint=<mountpoint> remove_warn
```

```
$ osmon -c modify_dataset server=<server name> dataset=<dataset> remove_warn
```

Special handling for swap usage:

Default is to remove threshold for swap disk usage.

Use 'virtualmem' flag to remove threshold for swap virtualmemory usage or 'all' flag for both

```
$ osmon -c modify_swap node=<node name> remove_warn  
$ osmon -c modify_swap node=<node name> remove_warn virtualmem  
$ osmon -c modify_swap node=<node name> remove_warn all
```

4.4.4 Individual 'Target Path Count' for a node

By default, the 'Target Path Count' is based on the total configured path (listed by mpathadm) or from the variable DISK_DEFAULT_PATH_COUNT.

You can set an individual 'Target Path Count' for a specific or all LUNs assigned to a node.

To update the 'Target Path Count' for one LUN assigned to a node, issue the following command:

```
$ osmon -c modify_disk node=<node name> targetcount=<target path count> guides=<guid list>
```

To update the 'Target Path Count' for all LUNs assigned to a node, issue the following command:

```
$ osmon -c modify_disk node=<node name> targetcount=<target path count> all
```

4.4.5 Limit failed cronjob reporting

If enabled (OSMON_CRON_ENABLED=TRUE) all failed cronjobs are reported. In development environments cronjobs may fail, but don't need to be reported.

Nodes (including vservers) can be ignored using

```
export OSMON_CRON_IGNORE_NODE=node1,node2
```

To avoid reporting cronjobs for individual vservers

```
export OSMON_CRON_IGNORE_VSERVER=vserver1,vserver2
```

To ignore individual jobs on all servers

```
export OSMON_CRON_IGNORE_CMD=console_check,opscenterharvester
```

The cronjobs of the current day are checked and reported. If you would like to check multiple days back you can use this variable (maximum 7 days)

```
export OSMON_CRON_DAYS=4
```

4.4.6 Display Filesystem usage

The filesystem usage is displayed on the vserver and node show detail command and a list of all critical filesystems can be displayed using the 'osmon -c show_fs' command.

```
$ osmon -c show_fs
```

Filesystems with usage over warn threshold

Node	vServer	Dataset	Mountpoint	zRoot	Type	Size/GB	Used	warn-over
g0051	v0151	v0151_root	/zones/v0151	yes	zfs	<undefined>	100%	(80%)
g0080	v0160	v0160_root	/zones/v0160	yes	zfs	4.0	92%	(80%)
g0086		g0086_root	/var	no	zfs	<undefined>	85%	(80%)
g0059	v0134	v0134_root	/tmp	no	tmpfs	1.0	81%	(80%)

Use the summary flag to display additionally a usage summary of the most utilized filesystems or the root flag to only show root filesystems:

```
$ osmon -c show_fs summary
```

Used	Count
100%	1
90%-99%	1

Filesystems with usage over warn threshold

Node	vServer	Dataset	Mountpoint	zRoot	Type	Size/MB	Used	warn-over
g0051	v0151	v0151_root	/zones/v0151	yes	zfs	<undefined>	100%	80% (default)
g0080	v0160	v0160_root	/zones/v0160	yes	zfs	4096	92%	80% (default)

To view filesystems with another usage than defined in 'OSMON_FS_WARNING' you can give a value directly on the command line by the option 'over'.

4.4.7 Display Dataset usage

A list of all critical datasets can be displayed using the 'osmon -c show_dataset' command.

```
$ osmon -c show_dataset
```

```
Datasets with critical state found
```

Server	Type	Dataset	Dataset-Type	State	Size/MB	Used	warn-over
g0081	Node	rpool	Node rpool	DEGRADED	n/a	50%	80% (default)

```
Datasets with usage over warn threshold
```

Server	Type	Dataset	Dataset-Type	State	Size/MB	Used	warn-over
v0145	vServer	v0145_root	ZPOOL	ONLINE	5120	91%	80% (default)
s0030	Node	s0030_vbox	ZPOOL	ONLINE	51200	88%	80% (default)

Use the summary flag to display additionally a usage summary of the most utilized datasets or the root flag to only show Node rootpools:

```
$ osmon -c show_dataset summary root
```

```
State Count
DEGRADED 1
```

```
Used Count
50%-59% 1
```

```
Datasets with critical state found
```

Server	Type	Dataset	Dataset-Type	State	Size/MB	Used	warn-over
g0081	Node	rpool	Node rpool	DEGRADED	n/a	50%	80% (default)

```
rpool Datasets with usage over warn threshold
```

Server	Type	Dataset	Dataset-Type	State	Size/MB	Used	warn-over
g0085	Node	rpool	Node rpool	ONLINE	n/a	58%	50%

To view datasets with another usage than defined in 'OSMON_DATASET_WARNING' you can give a value directly on the command line by the option 'over'.

4.4.8 Display SWAP usage

A list of critical swap usage can be displayed using the 'osmon -c show_swap' command.

```
$ osmon -c show_swap
```

```
Node swap with usage over warn threshold
```

Node	Size/GB	Used	warn-over
g0081	1.0	60%	(60%)

Use the summary flag to display additionally a usage summary of the most utilized swap areas:

```
$ osmon -c show_swap summary
```

```
Node swap with usage over 60%
```

Used	Count
70%-79%	1
60%-69%	2

Node	Size/GB	Used	warn-over
g0081	1.0	70%	(60%)
g0069	1.0	62%	(60%)
g0091	1.0	61%	(60%)

To view the swap usage with another usage than defined in 'OSMON_SWAP_WARNING' you can give a value directly on the command line by the option 'over'.

4.4.9 Display SMF services

A list of all critical SMF services can be displayed using the 'osmon -c show_smf' command.

```
$ osmon -c show_smf
```

```
SMF with state: degraded,maintenance
Server Type      SMF-Name (FMRI)                State
s0013 Node       svc:/system/sysobj:default     maintenance
v0149 vServer      svc:/site/vdcf_postinstall:default maintenance
```

Use the summary flag to additionally display a summary of the critical SMF services:

```
$ osmon -c show_smf summary
```

```
SMF-State  Count
maintenance 2
```

```
SMF with state: degraded,maintenance
Server Type      SMF-Name (FMRI)                State
s0013 Node       svc:/system/sysobj:default     maintenance
v0149 vServer      svc:/site/vdcf_postinstall:default maintenance
```

To view SMF services other than 'degraded,maintenance' you can define states on the command line by the option 'state'.

```
$ osmon -c show_smf state=uninitialized
```

```
SMF with state: uninitialized
Server Type      SMF-Name (FMRI)                State
v0142 vServer      svc:/application/font/stfsloader:default uninitialized
v0142 vServer      svc:/application/print/rfc1179:default uninitialized
```

It is also possible to search services of interest by the option 'search'.

```
$ osmon -c show_smf search=sendmail
```

```
Server Type      SMF-Name (FMRI)                State
s0013 Node       svc:/network/sendmail-client:default disabled
s0013 Node       svc:/network/smtp:sendmail     disabled
v0149 vServer      svc:/network/sendmail-client:default online
v0149 vServer      svc:/network/smtp:sendmail     online
```



4.4.10 Display Disk Path Count

A list of all disks without enough paths online can be displayed using the 'osmon -c show_disk' command.

```
$ osmon -c show_disk
```

```
Disk Path Count with critical state
Node GUID Current Path Count Target Path Count
s0024 6001438012599B620001100010C70000 1 2
s0024 6001438012599B6200011000291E0000 1 2
s0024 6001438012599B620001100029220000 1 2
s0024 6001438012599B62000110001F4E0000 1 2
```

Use the summary flag to additionally display a summary of the current path count:

```
$ osmon -c show_disk summary
```

```
CurrentPathCount Count
                1    4
```

```
Disk Path Count with critical state
Node GUID Current Path Count Target Path Count
s0024 6001438012599B620001100010C70000 1 2
s0024 6001438012599B6200011000291E0000 1 2
s0024 6001438012599B620001100029220000 1 2
s0024 6001438012599B62000110001F4E0000 1 2
```

You can list the current path count for each node the disk is assigned by using the following command:

```
$ diskadm -c show name=6001438012599B620001100029220000
```

```
Dataset-Name Use-Type Dev-Type GUID Size/GB Tier Location
- FREE MPXIO 600143..29220000 15.0 n/a HPEVA
```

Nodes connected to this disk:

```
Node Model cPool Location Path Count Comment
s0003 ORCL, SPARC-S7-2 sol11 RZ 4 S7-2 Server
s0024 ORCL, SPARC-T4-1 sol11 RZ 1 T4-1 Server
```

4.4.11 Display physical network interface states

A list of all critical network interfaces can be displayed using the 'osmon -c show_net' command.

```
-bash-5.2$ osmon -c show_net

Interface with critical state
  Node  LinkName      Interface  Usage      State
  s0003  i40e1         i40e1     ACCESS     DOWN
```

4.4.12 Display RAM/CPU usage

High cpu and ram usage can be listed using show_ram and show_cpu.

The flag 'hourly' lists the usage in the past hour and 'daily' lists the usage in the past 24 hours.

```
-bash-5.2$ osmon -c show_ram node=g0069 hourly

WARNING Node    g0069      : RAM Limit 80 % reached during 55 minutes between
                2023-08-21 13:35:48 and 2023-08-21 14:29:53
                : RAM Peak was 86 % at 2023-08-21 13:55:50
```

4.4.13 Display NTP client states

A list of all critical ntp clients can be displayed as follows

```
-bash-5.2$ osmon -c show_ntp

NTP with critical state
  Node  NTP State
  g0058 NOT_IN_SYNC
```

4.4.14 VDCF Monitoring Report

New since VDCF Monitoring 3.1

The `osmon -c show` provides a full report about all critical objects.

```
-bash-4.4$ osmon -c show hwmon
```

```
-----  
VDCF Monitoring Report from g0069  
Date: 25.03.2019 07:57:28  
-----
```

OS-Monitor

Filesystems with usage over warn threshold

Node	vServer	Dataset	Mountpoint	zRoot	Type	Size/GB	Used	warn-over
g0056	v0124	v0124_root	/export/home/admin	no	zfs	0.1	85%	(80%)
g0056	v0145	v0145_root	/export/home/admin	no	zfs	0.1	81%	(80%)

SMF with state: degraded,maintenance

Server	Type	SMF-Name (FMRI)	State
v0121	vServer	svc:/system/webconsole:console	maintenance
v0170	vServer	svc:/application/puppet:master	maintenance

```
-----  
HW-Monitor (with State FAULTED or N/A)
```

Current Hardware State

Node	Model	Console	Soft State	HW State	Last Change
s0009	SUNW,SPARC-T5220	ILOM	PWR-OFF	FAULTED	2019-01-05 14:00:56

```
-----  
The OS Monitoring daily report cronjob can be enabled/disabled.
```

```
$ osmon -c enable report
```

```
$ osmon -c disable report
```

Use the `status` command to display the current state of the OS monitoring components:

```
$ osmon -c status
```

4.5 OS Security

4.5.1 Run Security Compliance Assessments

Security Compliance Assessments can be run against Nodes and vServer running on Solaris 11.3 or later.

The benchmark to be used can be defined individually per system. For systems without a defined benchmark the VDCF 'default' benchmark is used. You can configure your default Benchmark by adding the COMPLIANCE_DEFAULT_BENCHMARK variable to customize.cfg.

```
$ vserver -c modify name=myserver benchmark=baseline
$ nodecfg -c modify name=server1 benchmark=cdom
```

See Chapter 3.5.5 to see where to define your own benchmarks.

The assessments may be running for several minutes, therefore they are not executed by 'osmon -c update' operation. Use the assess operation to initiate a Security Compliance Assessment:

```
$ osmon -c assess node=g0062 all_vserver

Assessing Node and all vServers on Node g0062
Executing compliance assess with Benchmark Solaris Baseline on g0062 ...
Executing compliance assess with Benchmark default on v0123 ...
Executing compliance assess with Benchmark default on v0143 ...

Compliance Report for Node g0062 from 2017-09-11T16:33:55
Score:          89.855064
Total Rules: 140  Passed: 134
                  Failed: 6   (Error: 0 / High: 1 / Med: 5 / Low: 0 / Info: 0)

Compliance Report for vServer v0123 from 2017-09-11T16:35:39
Score:          77.938248
Total Rules: 144  Passed: 140
                  Failed: 4   (Error: 0 / High: 0 / Med: 4 / Low: 0 / Info: 0)

Compliance Report for vServer v0143 from 2017-09-11T16:37:19
Score:          77.938248
Total Rules: 144  Passed: 140
                  Failed: 4   (Error: 0 / High: 0 / Med: 4 / Low: 0 / Info: 0)

Detailed Text Report can be found in /var/opt/jomasoft/vdcf/compliance_reports
WARN: Assess of Node and all vServers on Node g0062 was not successful
```

For convenience the assess operation is also available in the node and vserver commands:

```
$ node -c assess name=g0062 vserver
$ vserver -c assess name=v0123 benchmark=recommended
```

4.5.2 Display Compliance Reports

A Compliance Report overview can be displayed by 'osmon -c show_compliance':

```
$ osmon -c show_compliance
```

Server	Type	Benchmark	Score	Time	Passed	Failed	Error ...
v0123	vServer	default	77.938248	2017-09-11	140	4	0
v0143	vServer	default	77.938248	2017-09-11	140	4	0
s0024	Node	cdom	87.619041	2017-09-11	140	3	0
g0062	Node	baseline	89.855064	2017-09-11	134	6	0
s0004	Node	baseline	92.323235	2022-06-03	138	5	1
s0003	Node	cdom	95.238091	2017-09-11	142	1	0

Result of each rule can be listed for individual servers.

```
$ osmon -c show_compliance server=s0004
```

Rule	Description	Result
OSC-54005	Package integrity is verified	pass
OSC-53005	The OS version is current	informational
OSC-53015	Required CVE fixes are installed	pass
OSC-53505	Package signature checking is globally activated	pass
OSC-16005	All local filesystems are ZFS	pass
.....		

A detailed report in HTML can be found in the compliance html report directory:
`/var/opt/jomasoft/vdcf/compliance_reports/html`

These reports can be displayed with your preferred browser using the VDCF Dashboard.
See Chapter 4.6 for details.

4.5.3 OS Hardening

This feature is only available on Solaris 11.

To resolve the security findings discovered by the assess operation you may use the hardening operations on the node and vserver commands. These commands do apply OS hardening using a dedicated hardening profile:

```
$ node -c harden profile=<hardening profile>
```

```
$ vserver -c harden profile=<hardening profile>
```

Use the 'node -c harden help' or 'vserver -c harden help' to get a list of all available hardening profiles. You may define your own hardening profiles (see Chapter 3.5.6)

```
-bash-4.4$ node -c harden name=g0098 profile=baseline
```

```
Hardening started ...
OSC-12510: Service svc:/network/nfs/fedfs-client:default is in disabled state - DONE
OSC-15510: Service svc:/network/finger is disabled or not installed - DONE
OSC-17510: Service svc:/network/ftp:default is in disabled state - DONE
OSC-55010: The r-protocols services are disabled in PAM - DONE
OSC-63005: Service svc:/network/rpc/gss is enabled if and only if Kerberos is
configured - DONE
Hardening of 5 items on Node g0098 was successful
```

Since VDCF Monitoring 3.6 and later you can execute hardening based on the last compliance report, without creating a hardening profile manually.

```
-bash-5.2$ vserver -c harden name=dev49 compliance
```

```
Hardening profile created: /var/opt/jomasoft/vdcf/conf/compliance/dev49_2023-09-
27.hardening
Hardening started ...
OSC-12510: Service svc:/network/nfs/fedfs-client:default is in disabled state - DONE
OSC-63005: Service svc:/network/rpc/gss is enabled if and only if Kerberos is
configured - DONE
OSC-85000: The maximum number of waiting TCP connections is set to at least 1024 -
DONE (Changed from 128 to 1024)
OSC-99011: Service svc:/system/rad:remote is in enabled state - DONE
Hardening of 4 items on vServer dev49 on Node g0049 was successful
```

4.6 VDCF Dashboard web application

Starting with Version 3.0 the VDCF Monitoring includes a web application to display some information stored in the VDCF Repository and to access compliance reports generated by the 'osmon -c assess' command.

4.6.1 Enabling / Disabling

The web application is running as a apache daemon process and therefore it can be controlled by the normal apache restart commands. The web application is deployed in a separate virtual host.

It's enabled by default (after running the setup_gui tool, see Chapter 3.6).

To disable the web application just remove this file from the apache conf.d directory:
/etc/apache2/2.*/*conf.d/vdcf_django_httpd_2*.conf
and restart Apache.

4.6.2 Logfiles

Web application logfiles are located in the normal VDCF log directory:

```
$ ls -l /var/opt/jomasoft/vdcf/log/vdcfgui_*
-rw-r--r-- 1 root root 304 Sep 19 15:44 vdcfgui_access.log
-rw-r--r-- 1 vdcfgui webservd 92 Sep 19 15:43 vdcfgui_django.log
-rw-r--r-- 1 root root 465 Sep 19 15:17 vdcfgui_error.log
```

4.6.3 Web application screenshots

Start your preferred browser and navigate to the dashboard url: `https://<yourserver>:<your port>` (depends on your apache configuration).

To authenticate you have to use your local unix account credentials.
Users without a Solaris account can't use the VDCF Dashboard.



VDCF Dashboard 

Login (use your Solaris credentials)

Username:

Password:

Login

VDCF Dashboard - python 3.11

After authentication you get redirected to the home page of the application:



VDCF Dashboard 

logout

System Reports	Monitoring	Security Compliance
Control Domains	OS Monitoring	Compliance report
Guest Domains	HW Monitoring	
Nodes		
vServer (Zones)		
Datasets		
Filesystems		

VDCF Dashboard v5 - python 3.11

From here you can select the different reports. For example the compliance overview:

Server	Type	Benchmark	Score	Timestamp	# Passed	# Failed	# Error	# High	# Medium	# Low	# Info	# OS	Patch-Level
v0141	vServer	baseline										11	4.24.0.1.75.2 (U4.SRU24)
v0143	vServer	pci-dss	63.85527	2018-01-19T10.53.38	157	35	0	3	31	0	1	11	3.36.0.23.0 (U3.SRU36)
v0148	vServer	default	71.638359	2020-08-21T13.37.37	136	12	1	1	10	0	0	11	4.27.0.1.82.1 (U4.SRU27)
v0162	vServer	baseline	74.974121	2019-05-25T12.19.49	132	8	0	1	7	0	0	11	4.17.0.1.3.0 (U4.SRU17)
v0124	vServer	default	78.04351	2020-08-21T13.46.16	139	9	1	3	5	0	0	11	4.27.0.1.82.1 (U4.SRU27)

And finally display a compliance report for a specific system:

ORACLE Solaris Compliance Report

Oracle Solaris Security Policy

Oracle Solaris Compliance baseline and recommended settings for general purpose operating systems installations.

Evaluation Characteristics

Target machine	v0148
Benchmark Title	Oracle Solaris Security Policy
Benchmark Version	1.13387
Benchmark Description	Oracle Solaris Compliance baseline and recommended settings for general purpose operating systems installations.

CPE Platforms

- cpe:/o:oracle:solaris:11

Addresses

Or navigate to the OS Monitoring page to see all open issues

VDCF Dashboard

Home - CDoms - GDoms - Nodes - vServers - Datasets - Filesystems - HW Monitoring - Compliance Reports - logout

OS Monitoring - open issues

Show entries Search:

Server	Component	State	Name	Type	Size/GB	Used %	WarnOver %	Free/GB
g0058	SMF	maintenance	svc:/network/http:apache24	-	-	-	-	-
g0058	VIRTUALMEMORY	-	-	-	8.52	30	25	-
g0058	NTP	NOT_IN_SYNC	-	-	-	-	-	-
s0012	DISK	PathCountLowerThanTarget	2 LUNs	-	-	-	-	-
v0118	FS	-	/export/home/admin	zfs	0.49	95	80	0.02
v0118	FS	-	/export/home	zfs	10.0	83	60	1.15
v0118	DATASET	ONLINE	v0118_data	ZPOOL	29.8	26	20	-

Showing 1 to 7 of 7 entries Previous **1** Next