

Cacti Installation Manual

DOCUMENT VERSION HISTORY

VERSION	DATE	DESCRIPTION	AUTHOR/EDITOR
0.90	1/17/2024	1 st . version	Autumn.Shi, Harry.Chen HongQing, Lei.Liu Double.Lin
0.94	10/2/2024	Add Netflow configuration	Spencer

Contents

1	Platform Installation	2
1.1	VM Spec	2
1.2	Install OS	2
2	Cacti Installation	8
2.1	Install Apache (Web Server)	8
2.2	Install MariaDB (DB Server)	9
2.3	Install Cacti.....	11
2.4	Configure Cacti DB	12
2.5	Configure Cacti.....	13
2.6	Install & Configure Spine	14
2.7	Generate self-signed CA, 10 years, Disable tls1.x	17
2.8	Enable http compression	18
2.9	Disable firewall	20
2.10	(Optional) Enable firewall port: http https snmp	20
2.11	Install & Configure NTP.....	20
3	Cacti Configuration	22
3.1	Pre-Installation Check.....	22
3.2	Configure Cacti.....	31
3.3	Install Plug-in	35
3.4	Enable thold as a service	36
3.5	Enable 1 minute data collection and keep 1 month & 1Year.....	37
3.6	Import Monitor Template – Win Service & TCP Port & Linux process.....	40
3.7	Improve data collection performance	44
3.8	(Optional) Install Chinese language pack.....	44
4	Add Cacti into Monitor	46
4.1	Configure SNMP.....	46
4.2	Configure Cacti Service to monitor	47
4.3	Add Cacti device	48
5	Enable syslogs plugin	49
6	Enable flowview plugin.....	55
6.1	Create a dedicated disk partition 200GB for flowview DB.....	55
6.2	Create a dedicated DB for flowview	57
6.3	Flowview install & configure.....	58
6.4	Configure flowview generator simulator	65
6.5	Configure listeners.....	67
6.6	Configure filters	68
6.7	Configure listeners	69
6.8	Configure filters	70
6.9	Statistical Report.....	71
6.10	Check DB size & Row numbers.....	71
6.11	Sample flow export configuration on Cisco SW & Fortigate.....	72

1 Platform Installation

1.1 VM Spec

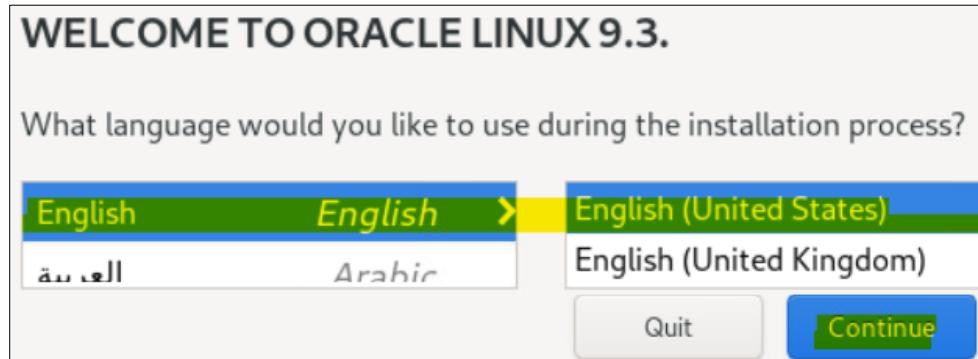
#CPU 8 core, RAM 8G, HD 100G.

Power Status		Powered On	Capacity and Usage
Guest OS		Oracle Linux 7 (64-bit) Oracle Linux 9.3 (64-bit) is realistic	CPU
VMware Tools	Running, version:12357 (Guest Managed)	39 MHz used	8 CPUs allocated
DNS Name (1)	TWTPSVHQ014.tpvaoc.com	Memory	8 GB allocated
IP Addresses (1)	172.17.32.14	Storage	100GB is real. 111.16 GB allocated
Encryption	Not encrypted	12.94 GB used	

1.2 Install OS

#Linux ISO: Oracle Linux 9.3 is fully supported by this manual.

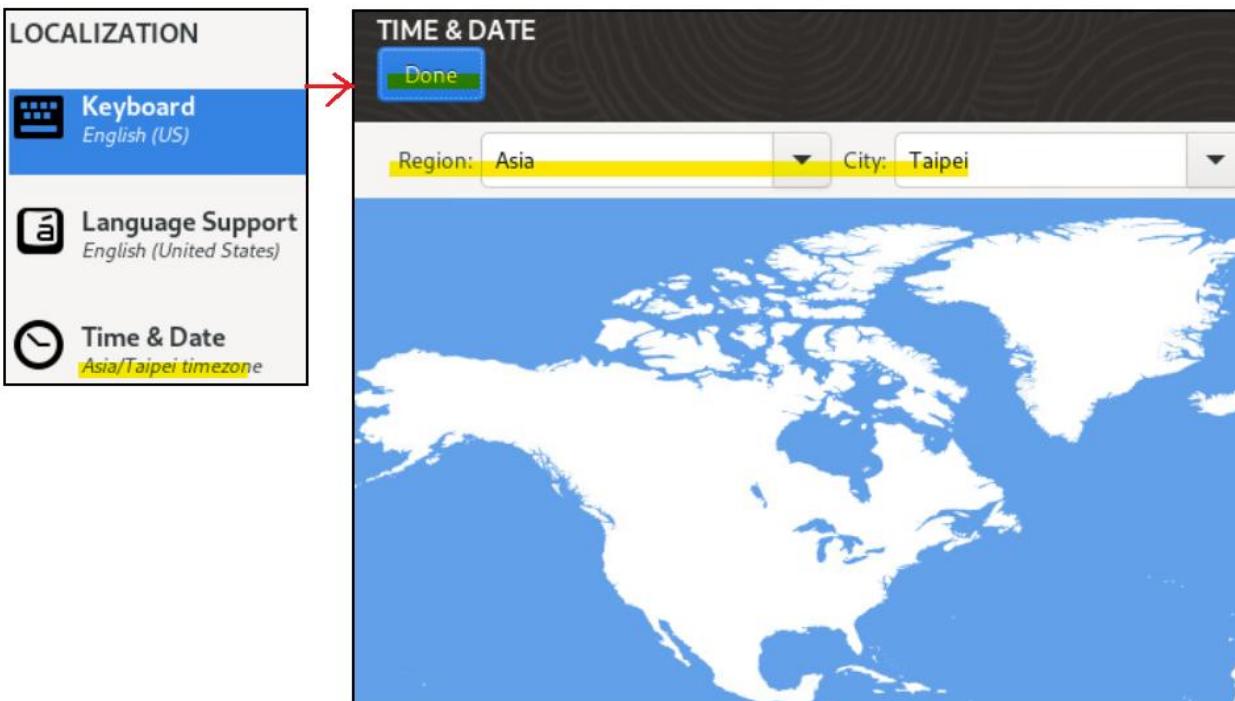
OracleLinux-R9-U3-x86_64-boot.iso (minimal version, 930MB)

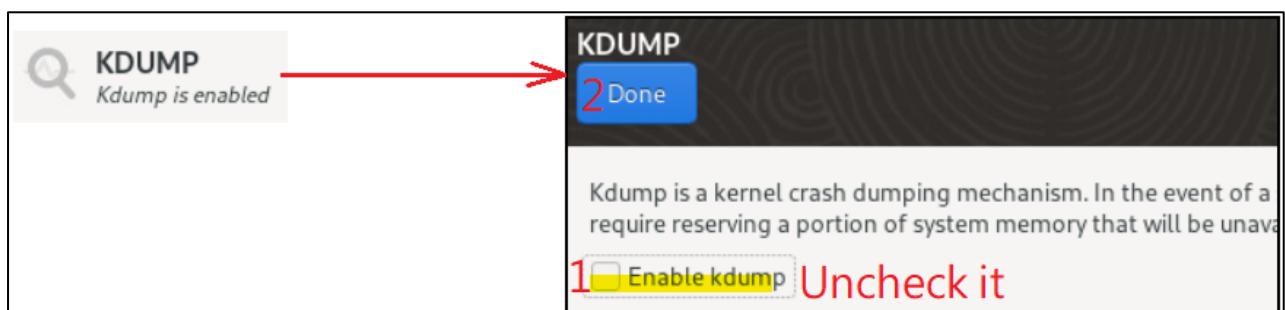
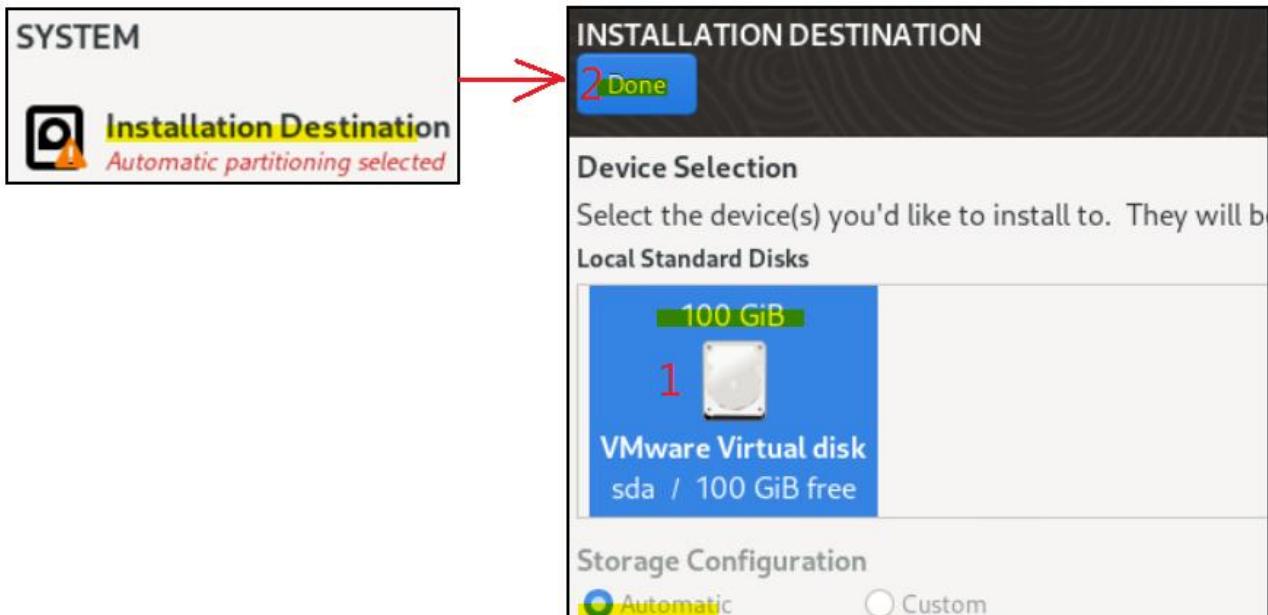


INSTALLATION SUMMARY

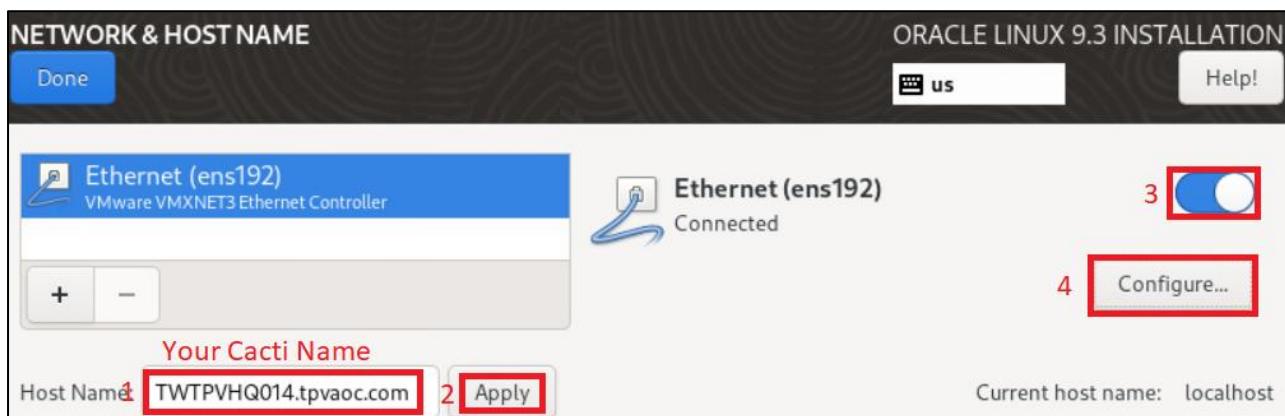
LOCALIZATION	SOFTWARE	SYSTEM
Keyboard English (US)	Installation Source <i>Error setting up base repository</i>	Installation Destination <i>Automatic partitioning selected</i>
Language Support English (United States)	Software Selection <i>Installation source not set up</i>	KDUMP <i>Kdump is enabled</i>
Time & Date Americas/New York timezone		Network & Host Name <i>Unknown</i>
USER SETTINGS		
Root Password <i>Root account is disabled</i>		Security Profile <i>No profile selected</i>
User Creation <i>No user will be created</i>		

Select your time zone





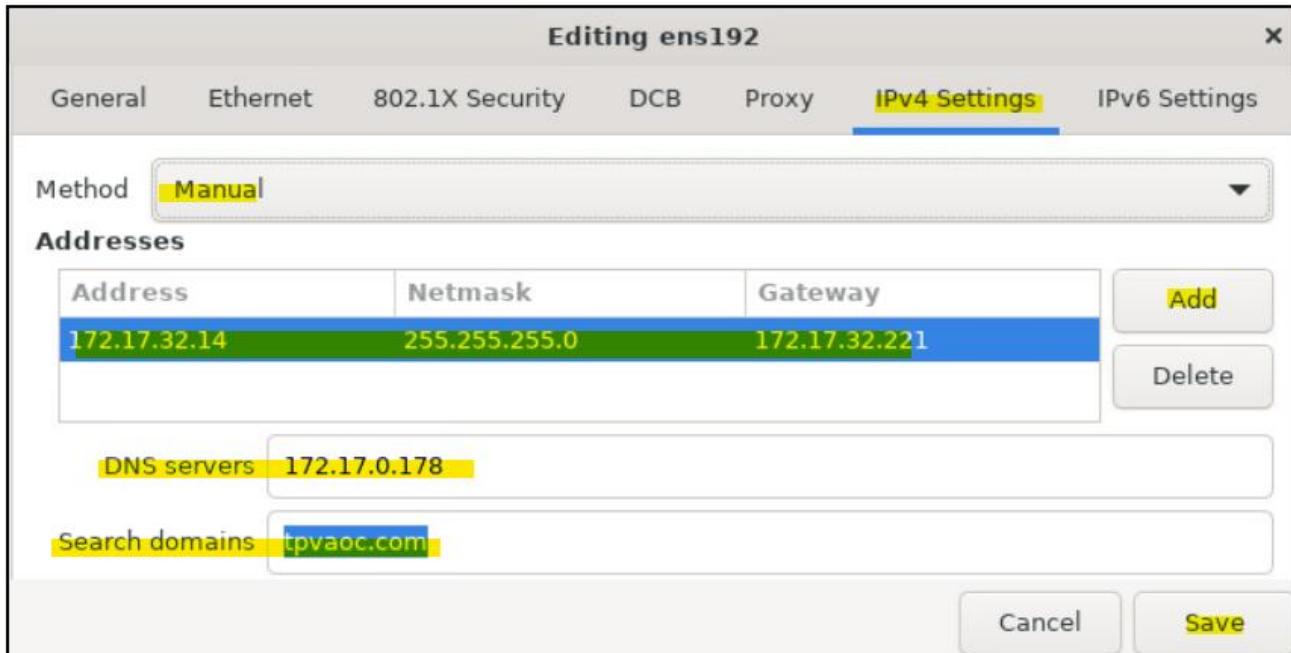
1.Type Host Name =>2.Apply =>3 Check =>4 Click Configure



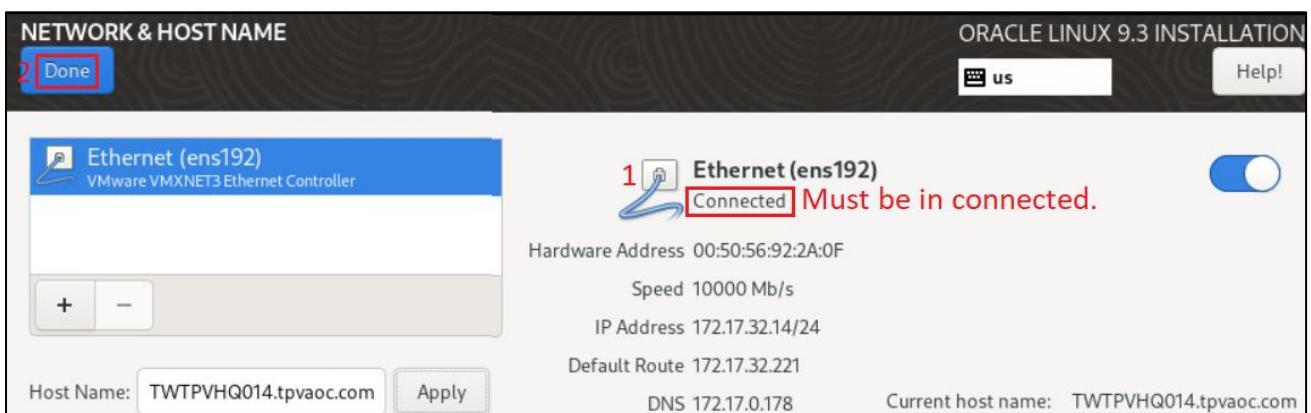
Click IPV6 setting => Select Method “Disabled”



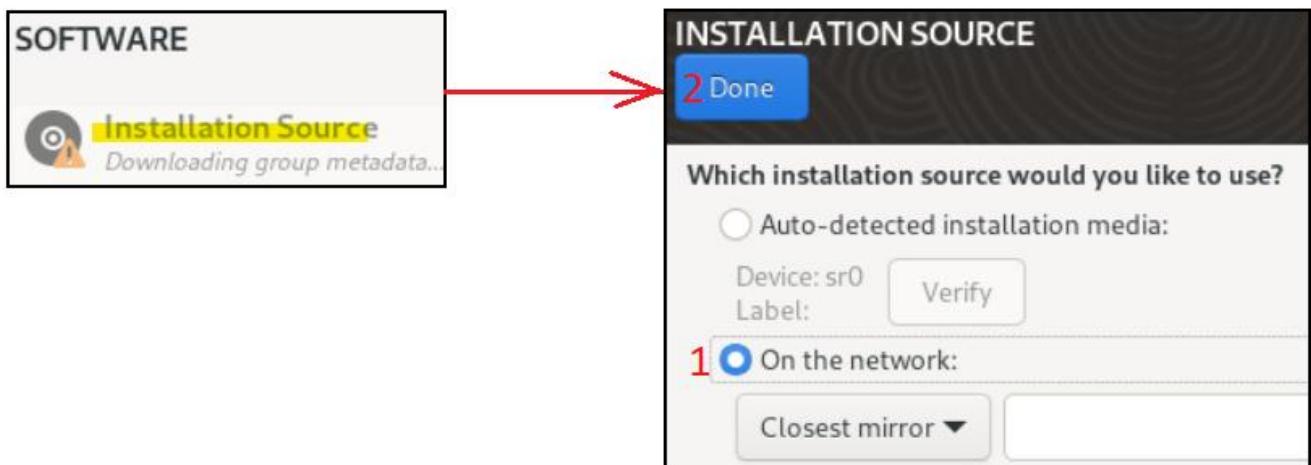
Click IPv4 Settings => Manual => Type Address IP, DNS IP, Search Domain tpvaoc.com => Click Save.



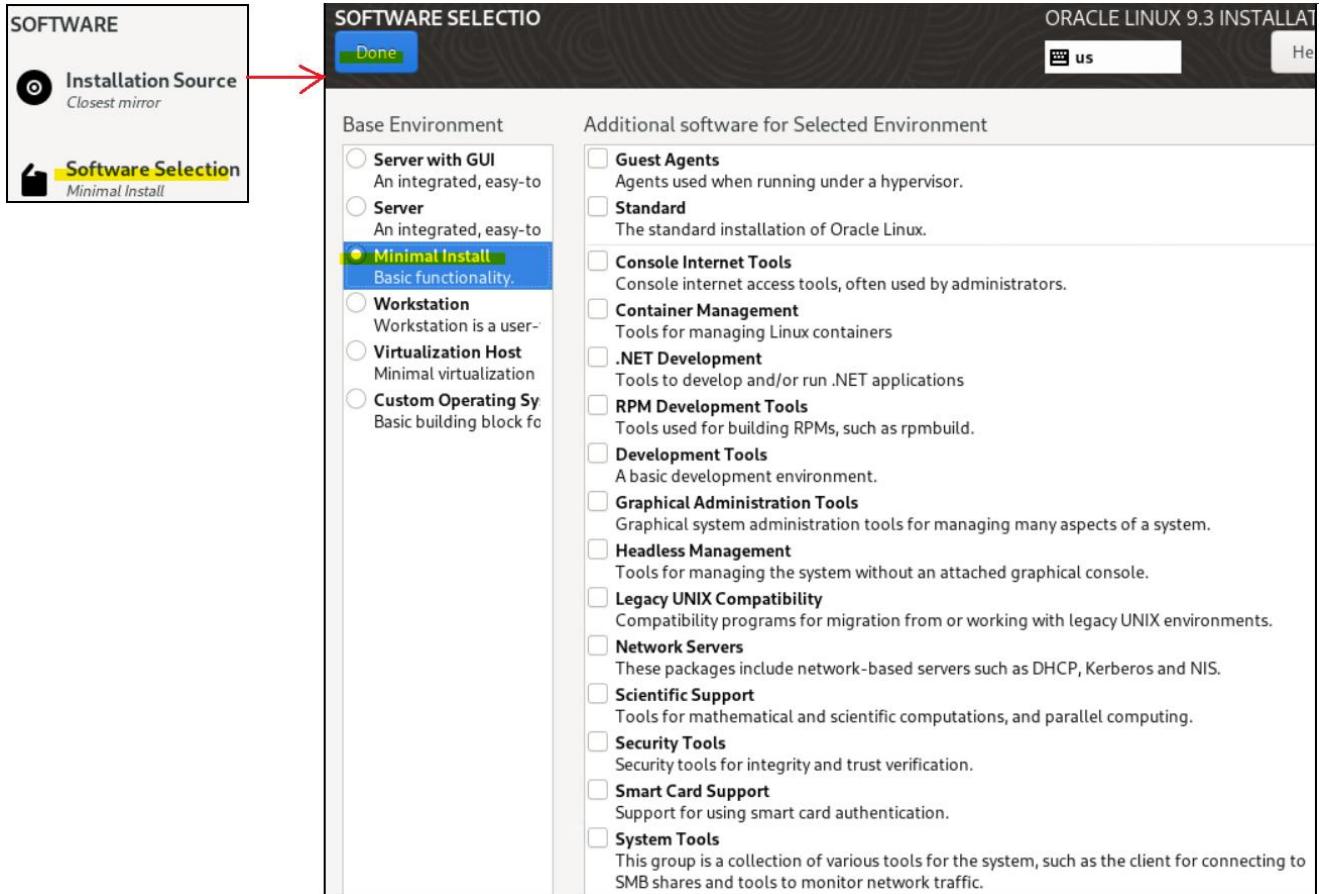
Verify network is “Connected” => Click Done.



Click Software => Installation Source => Click “On the network” => Done



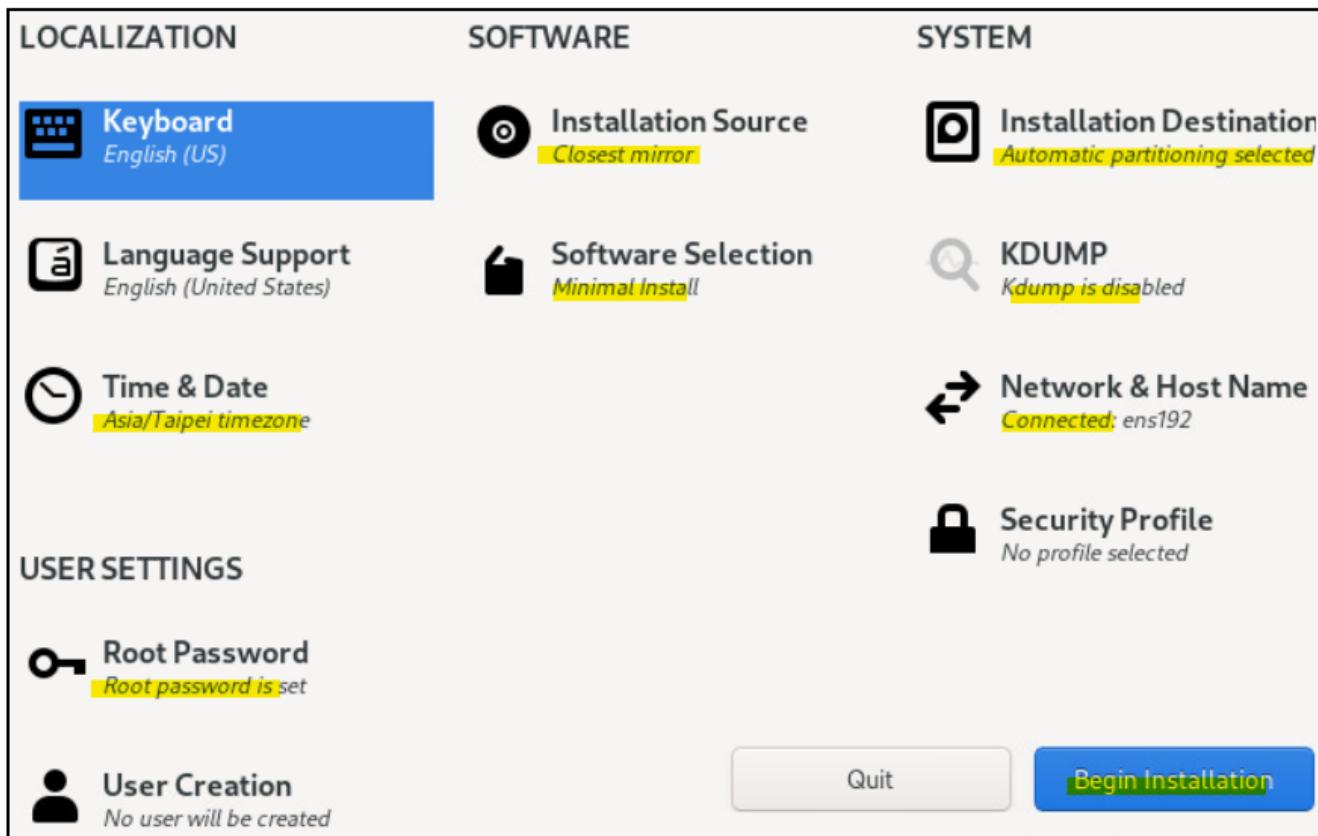
Click “SW selection” => Just select “Minimal Install”



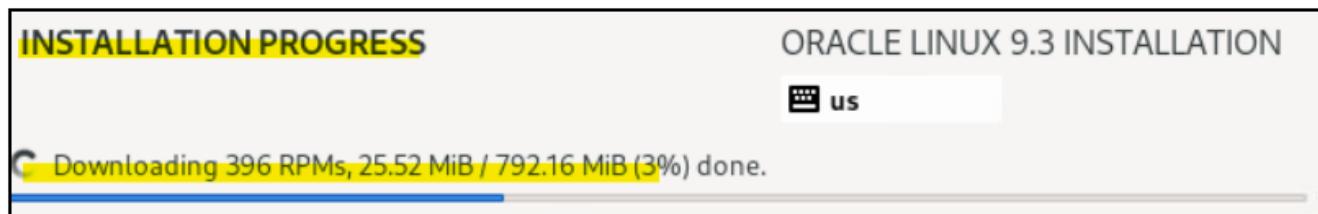
Set root Password => Unlock root account => Allow SSH



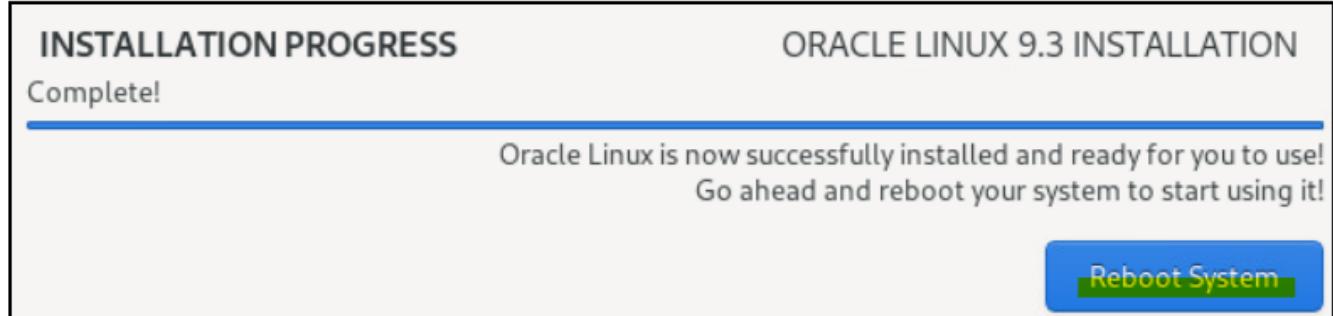
Confirmed 7 yellow marked is matched to your situation



Start installation



Reboot



#update patch to newest

yum -y update

```
[root@TWTPSVHQ014 ~]# yum -y update
Oracle Linux 9 BaseOS Latest (x86_64)           5.7 MB/s | 18 MB    00:03
Oracle Linux 9 Application Stream Packages (x86_64)
Oracle Linux 9 UEK Release 7 (x86_64)
Last metadata expiration check: 0:00:06 ago on Tue 09 Jan 2024 12:57:45 AM CST.
Dependencies resolved.
Nothing to do.
Complete!
```

2 Cacti Installation

2.1 Install Apache (Web Server)

```
#Enable Epel repo to enable PHP 7.2 package download
```

```
yum install -y http://rpms.remirepo.net/enterprise/remi-release-7.rpm
```

```
yum install -y yum-utils
```

```
yum-config-manager --enable remi-php72
```

```
[root@TWTPVHQ014 ~]# yum install -y http://rpms.remirepo.net/enterprise/remi-release-7.rpm
Last metadata expiration check: 0:37:08 ago on Mon 08 Jan 2024 09:20:24 PM CST.
remi-release-7.rpm
Dependencies resolved.
=====
 Package           Architecture   Version      Repository    Size
=====
 Installing:
  remi-release     noarch        7.9-6.el7.remi @commandline 28 k
 Installing dependencies:
  oracle-epel-release-el9 x86_64       1.0-1.el9      ol9_baseos_latest 14 k
  yum-utils        noarch        4.3.0-11.0.1.el9_3 ol9_baseos_latest 53 k
 Transaction Summary
=====
 0 packages up-to-date.
 0 packages downgraded.
 0 packages upgraded from 0.
 0 packages newly installed.
 0 packages to remove.
 0 packages not upgraded due to dependency problems.
```

```
[root@TWTPVHQ014 ~]# yum install -y yum-utils
Oracle Linux 9 EPEL Packages for Development (x86_64)
Safe Remi's RPM repository for Enterprise Linux 7 - x86_64
Last metadata expiration check: 0:00:03 ago on Mon 08 Jan 2024 09:59:36 PM CST.
Package yum-utils-4.3.0-11.0.1.el9_3.noarch is already installed.
Dependencies resolved.
Nothing to do.
```

```
[root@TWTPVHQ014 ~]# yum-config-manager --enable remi-php72
[root@TWTPVHQ014 ~]# 
```

```
#Linux OS patch update to newest
```

```
yum -y update
```

```
[root@TWTPVHQ014 ~]# yum -y update
Remi's PHP 7.2 RPM repository for Enterprise Linux 7 - x86_64
Last metadata expiration check: 0:00:01 ago on Mon 08 Jan 2024 10:04:51 PM CST.
Dependencies resolved.
=====
 Package           Architecture   Version      Repository    Size
=====
 Upgrading:
  python3-hwdata   noarch        2.3.7-13.el9   ol9_developer_EPEL 63 k
  python3-pyOpenSSL noarch        21.0.0-1.el9   ol9_developer_EPEL 118 k
 Transaction Summary
=====
 0 packages up-to-date.
 0 packages downgraded.
 0 packages upgraded from 0.
 0 packages newly installed.
 0 packages to remove.
 0 packages not upgraded due to dependency problems.
```

```
# Install Apache
```

```
yum install -y httpd
```

```
systemctl enable httpd
```

```
systemctl start httpd
```

```
[root@TWTPVHQ014 ~]# yum install -y httpd
Last metadata expiration check: 0:03:59 ago on Mon 08 Jan 2024 10:04:51 PM CST.
Dependencies resolved.
=====
Package           Architecture   Version      Repository    Size
=====
Installing:
httpd            x86_64        2.4.57-5.0.1.el9   ol9_appstream 65 k
Installing dependencies:
apr              x86_64        1.7.0-12.el9_3     ol9_appstream 131 k
apr-util          x86_64        1.6.1-23.el9     ol9_appstream 99 k
apr-util-bdb      x86_64        1.6.1-23.el9     ol9_appstream 12 k
httpd-core        x86_64        2.4.57-5.0.1.el9   ol9_appstream 1.8 M
httpd-filesystem  noarch       2.4.57-5.0.1.el9   ol9_appstream 12 k
httpd-tools       x86_64        2.4.57-5.0.1.el9   ol9_appstream 94 k
mailcap           noarch       2.1.49-5.el9     ol9_baseos_latest 38 k
oracle-logos-httpd  noarch       90.2-1.0.4.el9   ol9_baseos_latest 37 k
Installing weak dependencies:
apr-util-openssl x86_64        1.6.1-23.el9     ol9_appstream 14 k
mod_http2         x86_64        1.15.19-5.el9    ol9_appstream 157 k
mod_lua            x86_64        2.4.57-5.0.1.el9   ol9_appstream 59 k
```

```
[root@TWTPSVHQ014 ~]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[root@TWTPSVHQ014 ~]# systemctl start httpd
```

2.2 Install MariaDB (DB Server)

```
dnf install -y mariadb-server
systemctl enable mariadb
systemctl start mariadb
```

```
[root@TWTPVHQ014 ~]# dnf install -y mariadb-server
Last metadata expiration check: 1:40:15 ago on Mon 08 Jan 2024 10:04:51 PM CST.
Dependencies resolved.
=====
Package           Architecture   Version      Repository    Size
=====
Installing:
mariadb-server   x86_64        3:10.5.22-1.el9_2   ol9_appstream 9.7 M
Installing dependencies:
checkpolicy       x86_64        3.5-1.el9       ol9_appstream 355 k
mariadb-gssapi-server x86_64        3:10.5.22-1.el9_2   ol9_appstream 15 k
mariadb-server-utils x86_64        3:10.5.22-1.el9_2   ol9_appstream 234 k
Transaction Summary
=====
Install 18 Packages
```

```
[root@TWTPVHQ014 ~]# systemctl enable mariadb
Created symlink /etc/systemd/system/mysql.service → /usr/lib/systemd/system/mariadb.service.
Created symlink /etc/systemd/system/mysqld.service → /usr/lib/systemd/system/mariadb.service.
Created symlink /etc/systemd/system/multi-user.target.wants/mariadb.service → /usr/lib/systemd/system/mariadb.service.
[root@TWTPVHQ014 ~]# systemctl start mariadb
```

IMPORTANT: Secure your MySQL installation before doing any more changes
`/usr/bin/mysql_secure_installation`

```
[root@TWTPVHQ014 ~]# /usr/bin/mysql_secure_installation
Enter current password for root (enter for none):  
Type ENTER
OK, successfully used password, moving on...      because NO PW of
Switch to unix_socket authentication [Y/n] Y      fresh installation.
Enabled successfully!
Reloading privilege tables..
... Success!
You already have your root account protected, so you can safely answer 'n'.
Change the root password? [Y/n] y
New password: Type new PW
Re-enter new password:
Password updated successfully!
```

```
Disallow root login remotely? [Y/n] Y
... Success!
Remove test database and access to it? [Y/n] Y
- Dropping test database...
... Success!
Reload privilege tables now? [Y/n] Y
... Success!
All done! If you've completed all of the above
installation should now be secure.
```

The following MySQL/MariaDB recommendations may vary depending on your system setup. In any case, Cacti will prompt you with more accurate recommendations during the installation



Copy to /etc/my.cnf.d/

/etc/my.cnf.d/			
Name	Size	Changed	
..		1/9/2024 1:15:00 AM	
auth_gssapi.cnf	1 KB	10/19/2023 1:05:50 AM	
client.cnf	1 KB	5/9/2022 12:33:23 AM	
enable_encryptio...	1 KB	8/11/2023 3:22:13 AM	
mariadb-server.c...	2 KB	10/19/2023 12:57:35 ...	
mysql-clients.cnf	1 KB	8/11/2023 3:22:13 AM	
server.cnf	1 KB	1/1/2024 5:29:20 PM	
spider.cnf	1 KB	8/11/2023 3:22:12 AM	

Content of nano /etc/my.cnf.d/server.cnf as below

```
[mysqld]
character-set-server=utf8mb4
collation-server=utf8mb4_unicode_ci
innodb_file_format = Barracuda
max_allowed_packet = 16777777
```

```
join_buffer_size = 32M
innodb_file_per_table = ON
innodb_large_prefix = 1
innodb_buffer_pool_size = 250M
#innodb_additional_mem_pool_size = 90M
innodb_flush_log_at_trx_commit = 2
#log-error = /var/log/mariadb/mysql-error.log
log-queries-not-using-indexes = 1
slow-query-log = 0
#slow-query-log-file = /var/log/mariadb/mysql-slow.log
max_heap_table_size = 124M
tmp_table_size = 124M
innodb_buffer_pool_size = 2000M
innodb_doublewrite = ON
innodb_flush_log_at_timeout = 3
innodb_read_io_threads = 32
innodb_write_io_threads = 16
innodb_io_capacity = 5000
innodb_io_capacity_max = 10000
```

```
systemctl restart mariadb
```

```
[root@TWTPSVHQ014 ~]# systemctl restart mariadb
[root@TWTPSVHQ014 ~]#
```

2.3 Install Cacti

```
yum install -y cacti
```

```
[root@TWTPSVHQ014 ~]# yum install -y cacti
Last metadata expiration check: 3:00:31 ago on Wed 10 Jan 2024 06:32:36 PM CST.
Dependencies resolved.
=====
Package           Architecture      Version       Repository      Size
=====
Installing:
cacti             noarch          1.2.25-1.el9   ol9_developer_EPEL 37 M
```

```

Installed:
  cacti-1.2.25-1.el9.noarch
  dejavu-sans-mono-fonts-2.37-18.el9.noarch
  freetype-2.10.4-9.el9.x86_64
  gd-2.3.2-3.el9.x86_64
  harfbuzz-2.7.4-8.el9.x86_64
  libX11-1.7.0-8.el9.x86_64
  libXau-1.0.9-8.el9.x86_64
  libXft-2.3.3-8.el9.x86_64
  libXrender-0.9.10-16.el9.x86_64
  libicu-67.1-9.el9.x86_64
  libpng-2:1.6.37-12.el9.x86_64
  libtiff-4.4.0-10.el9.x86_64
  libxcb-1.13.1-9.el9.x86_64
  net-snmp-1:5.9.1-11.0.3.el9_3.1.x86_64
  net-snmp-libs-1:5.9.1-11.0.3.el9_3.1.x86_64
  nginx-filesystem-1:1.20.1-14.0.1.el9_2.1.noarch
  pango-1.48.7-3.el9.x86_64
  php-cli-8.0.30-1.el9_2.x86_64
  php-fpm-8.0.30-1.el9_2.x86_64
  php-gmp-8.0.30-1.el9_2.x86_64
  php-ldap-8.0.30-1.el9_2.x86_64
  php-mysqlnd-8.0.30-1.el9_2.x86_64
  php-process-8.0.30-1.el9_2.x86_64
  php-xml-8.0.30-1.el9_2.x86_64
  rrdtool-1.7.2-21.el9.x86_64
  cairo-1.17.4-7.el9.x86_64
  fontconfig-2.14.0-2.el9_1.x86_64
  fribidi-1.0.10-6.el9.2.x86_64
  graphite2-1.3.14-9.el9.x86_64
  jbigkit-libs-2.1-23.el9.x86_64
  libX11-common-1.7.0-8.el9.noarch
  libXext-1.3.4-8.el9.x86_64
  libXpm-3.5.13-8.el9_1.x86_64
  libdatrie-0.2.13-4.el9.x86_64
  libjpeg-turbo-2.0.90-6.el9_1.x86_64
  libthai-0.1.28-8.el9.x86_64
  libwebp-1.2.0-8.el9_3.x86_64
  lm_sensors-libs-3.6.0-10.el9.x86_64
  net-snmp-agent-libs-1:5.9.1-11.0.3.el9_3.1.x86_64
  net-snmp-utils-1:5.9.1-11.0.3.el9_3.1.x86_64
  oniguruma-6.9.6-1.el9.5.x86_64
  perl-Term-ReadLine-1.17-480.el9.noarch
  php-common-8.0.30-1.el9_2.x86_64
  php-gd-8.0.30-1.el9_2.x86_64
  php-intl-8.0.30-1.el9_2.x86_64
  php-mbstring-8.0.30-1.el9_2.x86_64
  php-pdo-8.0.30-1.el9_2.x86_64
  php-snmp-8.0.30-1.el9_2.x86_64
  pixman-0.40.0-6.el9_3.x86_64
  xml-common-0.6.3-58.el9.noarch

```

2.4 Configure Cacti DB

```

mysql -u root -p c@Ct1Vser
create database if not exists cacti;
use cacti;
source /usr/share/doc/cacti/cacti.sql
quit

```

```

[root@TWTPSVHQ014 ~]# mysql -uroot -pc@Ct1Vser
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 5
Server version: 10.5.22-MariaDB-log MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database if not exists cacti;
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]> use cacti;
Database changed
MariaDB [cacti]> source /usr/share/doc/cacti/cacti.sql
Query OK, 0 rows affected (0.001 sec)

```

```

# Grant Cacti username access to Cacti database.
mysql -uroot -pc@Ct1Vser
CREATE USER 'cactiuser'@'localhost' IDENTIFIED BY 'c@Ct1Vser';
GRANT ALL PRIVILEGES ON cacti.* TO 'cactiuser'@'localhost';

```

```

GRANT SELECT ON mysql.time_zone_name TO 'cactiuser'@'localhost';
FLUSH PRIVILEGES;
exit

```

```

[root@TWTPSVHQ014 ~]# mysql -uroot -pc@Ct1Vser
Welcome to the MariaDB monitor. Commands end with ; or \g.
MariaDB [(none)]> GRANT ALL PRIVILEGES ON cacti.* TO 'cactiuser'@'localhost';
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> GRANT SELECT ON mysql.time_zone_name TO 'cactiuser'@'localhost';
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)

```

2.5 Configure Cacti

#Install some tools

```
dnf install -y net-tools nano wget git hping3
```

```

[root@TWTPSVHQ014 ~]# dnf install -y net-tools nano wget git
Last metadata expiration check: 3:40:34 ago on Wed 10 Jan 2024 06:32:36 PM CST.
Dependencies resolved.
=====
Package           Architecture   Version      Repository    Size
=====
Installing:
git              x86_64        2.39.3-1.el9_2      ol9_appstream  78 k
nano             x86_64        5.6.1-5.el9       ol9_baseos_latest 790 k
net-tools         x86_64        2.0-0.62.20160912git.el9 ol9_baseos_latest 344 k
wget             x86_64        1.21.1-7.el9      ol9_appstream  861 k
=====
Transferring dependencies...
=====
Installed:
emacs-filesystem-1:27.2-9.el9.noarch      git-2.39.3-1.el9_2.x86_64      git-core-2.39.3-1.el9_2.x86_64
git-core-doc-2.39.3-1.el9_2.noarch        nano-5.6.1-5.el9.x86_64        net-tools-2.0-0.62.20160912git.el9.x86_64
perl-Error-1:0.17029-7.el9.noarch        perl-File-Find-1.37-480.el9.noarch  perl-Git-2.39.3-1.el9_2.noarch
perl-TermReadKey-2.38-11.el9.x86_64       perl-lib-0.65-480.el9.x86_64      wget-1.21.1-7.el9.x86_64

```

#Edit /etc/php.ini to replace with your time zone

```
nano /etc/php.ini
```

```
date.timezone = Asis/Taipei      #replace with your time zone.
```

```

[Date]
; Defines the default timezone used by the date functions
; http://php.net/date.timezone
;date.timezone =
date.timezone = Asis/Taipei

[ line 910/1665 (54%), col 2/2

```

Edit the config.php file, replace PW

```
nano /usr/share/cacti/include/config.php
```

```

$database_type      = 'mysql';
$database_default  = 'cacti';
$database_hostname = 'localhost';
$database_username = 'cactiuser';
$database_password = 'c@Ct1Vser';
$database_port      = '3306';

```

```
# Create your cron task file  
nano /etc/cron.d/cacti # remove #
```

```
GNU nano 5.6.1 /etc/cron.d/cacti  
*/5 * * * * apache /usr/bin/php /usr/share/cacti/poller.php > /dev/null 2>&1
```

2.6 Install & Configure Spine

```
# Install the necessary packages to compile and install spine  
dnf --enablerepo=ol9_codeready_builder install mariadb-devel  
dnf --enablerepo=ol9_codeready_builder install help2man  
yum install -y net-snmp-devel  
yum install -y autoconf automake libtool dos2unix openssl-devel
```

```
[root@TWTPSVHQ014 ~]# dnf --enablerepo=ol9_codeready_builder install mariadb-devel  
Oracle Linux 9 CodeReady Builder (x86_64) - (Unsupported) 3.3 MB/s | 6.8 MB 00:02  
Last metadata expiration check: 0:00:04 ago on Wed 10 Jan 2024 10:48:36 PM CST.
```

```
Installed:  
libpkgconf-1.7.3-10.el9.x86_64 mariadb-connector-c-devel-3.2.6-1.el9_0.x86_64  
mariadb-connector-c-doc-3.2.6-1.el9_0.noarch mariadb-devel-3:10.5.22-1.el9_2.x86_64  
openssl-devel-1:3.0.7-24.0.1.el9.x86_64 pkgconf-1.7.3-10.el9.x86_64  
pkgconf-m4-1.7.3-10.el9.noarch pkgconf-pkg-config-1.7.3-10.el9.x86_64  
zlib-devel-1.2.11-40.el9.x86_64
```

```
[root@TWTPSVHQ014 ~]# dnf --enablerepo=ol9_codeready_builder install help2man  
Last metadata expiration check: 0:03:41 ago on Wed 10 Jan 2024 10:48:36 PM CST.
```

```
Installed:  
help2man-1.48.2-3.el9.noarch
```

```
[root@TWTPSVHQ014 ~]# yum install -y net-snmp-devel  
Last metadata expiration check: 0:30:07 ago on Wed 10 Jan 2024 10:25:12 PM CST.  
Dependencies resolved.  
=====  
 Package Architecture Version Repository Size  
=====  
 Installing:  
 net-snmp-devel x86_64 1:5.9.1-11.0.3.el9_3.1 ol9_appstream 553 k
```

```

Installed:
annobin-12.12-1.el9.x86_64           cpp-11.4.1-2.1.0.1.el9.x86_64
dtrace-2.0.0-1.13.1.el9.x86_64       dwz-0.14-3.el9.x86_64
efi-srpm-macros-6-2.0.1.el9.noarch  elfutils-devel-0.189-3.el9.x86_64
elfutils-libelf-devel-0.189-3.el9.x86_64 fonts-srpm-macros-1:2.0.5-7.el9.1.noarch
fuse3-3.10.2-6.el9.x86_64           fuse3-libs-3.10.2-6.el9.x86_64
gcc-11.4.1-2.1.0.1.el9.x86_64       gcc-plugin-annobin-11.4.1-2.1.0.1.el9.x86_64
ghc-srpm-macros-1.5.0-6.el9.noarch  glibc-devel-2.34-83.0.1.el9_3.7.x86_64
glibc-headers-2.34-83.0.1.el9_3.7.x86_64 go-srpm-macros-3.2.0-2.el9.noarch
kernel-headers-5.14.0-362.13.1.el9_3.x86_6 kernel-srpm-macros-1.0-13.0.1.el9.noarch
libmpc-1.2.1-4.el9.x86_64           libpfm-4.13.0-4.el9.x86_64
libcrypt-devel-4.4.18-3.el9.x86_64   libzstd-devel-1.5.1-2.el9.x86_64
llvm-libs-16.0.6-4.el9.x86_64       lm_sensors-devel-3.6.0-10.el9.x86_64
lua-srpm-macros-1-6.el9.noarch     make-1:4.3-7.el9.x86_64
net-snmp-devel-1:5.9.1-11.0.3.el9_3.x86_6 ocaml-srpm-macros-6-6.el9.noarch
openblas-srpm-macros-2-11.el9.noarch perl-AutoSplit-5.74-480.el9.noarch
perl-Benchmark-1.23-480.el9.noarch  perl-CPAN-Meta-2.150010-460.el9.noarch
perl-CPAN-Meta-Requirements-2.140-461.el9. perl-CPAN-Meta-YAML-0.018-461.el9.noarch
perl-Devel-PPPort-3.62-4.el9.x86_64    perl-Encode-Locale-1.05-21.el9.noarch
perl-ExtUtils-Command-2:7.60-3.el9.noarch perl-ExtUtils-Constant-0.25-480.el9.noarch
perl-ExtUtils-Install-2.20-4.el9.noarch  perl-ExtUtils-MakeMaker-2:7.60-3.el9.noarch
perl-ExtUtils-Manifest-1:1.73-4.el9.noarch perl-ExtUtils-ParseXS-1:3.40-460.el9.noarch
perl-File-Compare-1.100.600-480.el9.noarch perl-I18N-Langinfo-0.19-480.el9.x86_64
perl-JSON-PP-1:4.06-4.el9.noarch       perl-Test-Harness-1:3.42-461.el9.noarch
perl-Time-HiRes-4:1.9764-462.el9.x86_64 perl-devel-4:5.32.1-480.el9.x86_64
perl-doc-5.32.1-480.el9.noarch       perl-locale-1.09-480.el9.noarch
perl-srpm-macros-1-41.el9.noarch    perl-version-7:0.99.28-4.el9.x86_64
popt-devel-1.18-8.el9.x86_64        pyproject-srpm-macros-1.9.0-1.el9.noarch
python-srpm-macros-3.9-52.el9.noarch qt5-srpm-macros-5.15.9-1.el9.noarch

```

```

[root@TWTSPVHQ014 ~]# yum install -y autoconf automake libtool dos2unix openssl-devel
Last metadata expiration check: 0:36:30 ago on Wed 10 Jan 2024 10:25:12 PM CST.
Package openssl-devel-1:3.0.7-24.0.1.el9.x86_64 is already installed.

```

```

Installed:
autoconf-2.69-38.el9.noarch          automake-1.16.2-8.el9.noarch          dos2unix-7.4.2-4.el9.x86_64
libtool-2.4.6-45.el9.x86_64          m4-1.4.19-1.el9.x86_64              perl-Thread-Queue-3.14-460.el9.noarch
perl-threads-1:2.25-460.el9.x86_64  perl-threads-shared-1.61-460.el9.x86_64

```

```

# Download spine source code from Cacti Web Site
cd /tmp
wget https://www.cacti.net/downloads/spine/cacti-spine-1.2.25.tar.gz
tar -zvxf cacti-spine-1.2.25.tar.gz
cd cacti-spine-1.2.25

```

```

# Run the configure script and compile spine.
sh
./bootstrap
./configure
make
make install
chown root:root /usr/local/spine/bin/spine
chmod +s /usr/local/spine/bin/spine

```

```
[root@TWTPSVHQ014 tmp]# cd cacti-spine-1.2.25
[root@TWTPSVHQ014 cacti-spine-1.2.25]# sh
sh-5.1# ./bootstrap
INFO: Starting Spine build process
INFO: Removing cache directories
INFO: Ensuring UNIX format for *.ac
```

```
sh-5.1# ./configure
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking for gcc... gcc
```

```
sh-5.1# make
gcc -DHAVE_CONFIG_H -I. -I./config -I/usr/include/net-snmp -I/usr/include/net-snmp
o -MD -MP -MF .deps/sql.Tpo -c -o sql.o sql.c
mv -f .deps/sql.Tpo .deps/sql.Po
```

```
sh-5.1# make install
make[1]: Entering directory '/tmp/cacti-spine-1.2.25'
/usr/bin/mkdir -p '/usr/local/spine/bin'
 /bin/sh ./libtool --mode=install /usr/bin/install -c spine '/usr/local/spine/bin/spine'
libtool: install: /usr/bin/install -c spine /usr/local/spine/bin/spine
/usr/bin/mkdir -p '/usr/local/spine/etc'
/usr/bin/install -c -m 644 spine.conf.dist '/usr/local/spine/etc'
/usr/bin/mkdir -p '/usr/local/spine/share/man/man1'
/usr/bin/install -c -m 644 spine.1 '/usr/local/spine/share/man/man1'
make[1]: Leaving directory '/tmp/cacti-spine-1.2.25'
sh-5.1# chown root:root /usr/local/spine/bin/spine
sh-5.1# chmod +s /usr/local/spine/bin/spine
sh-5.1# chown root:root /usr/local/spine/bin/spine
```

```
# Edit spine.conf
cp /usr/local/spine/etc/spine.conf.dist /usr/local/spine/etc/spine.conf
nano /usr/local/spine/etc/spine.conf
```

DB_Host	localhost
DB_Database	cacti
DB_User	cactiuser
DB_Pass	c@Ct1Vser
DB_Port	3306

```
# Enable cacti as a service
cp /usr/share/cacti/service/cactid.service /usr/lib/systemd/system/
nano /usr/lib/systemd/system/cactid.service
touch /etc/sysconfig/cactid
nano /etc/cron.d/cacti
systemctl enable cactid
systemctl daemon-reload
systemctl start cactid
systemctl status cactid
```

2.7 Generate self-signed CA, 10 years, Disable tls1.x

```
mkdir /etc/ca
```

```
openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -keyout /etc/ca/cacti.key -out /etc/ca/cacti.crt  
ls -lh /etc/ca
```

```
Country Name (2 letter code) [XX]:TW
State or Province Name (full name) []:Taipei Replace with your own information.
Locality Name (eg, city) [Default City]:New Taipei City
Organization Name (eg, company) [Default Company Ltd]:TPV Technology Ltd.
Organizational Unit Name (eg, section) []:IT Your Cacti IP address.
Common Name (eg, your name or your server's hostname) []:172.17.32.14
Email Address []:Double.lin@tpv-tech.com
```

```
[root@TWTPVHQ014 ~]# ls -lh /etc/ca  
total 8.0K  
-rw-r--r--. 1 root root 1.5K Jan  8 22:21 cacti.crt  
-rw-----. 1 root root 1.7K Jan  8 22:19 cacti.key
```

```
#Install mod_ssl, net-tools, nano, wget & git tools
```

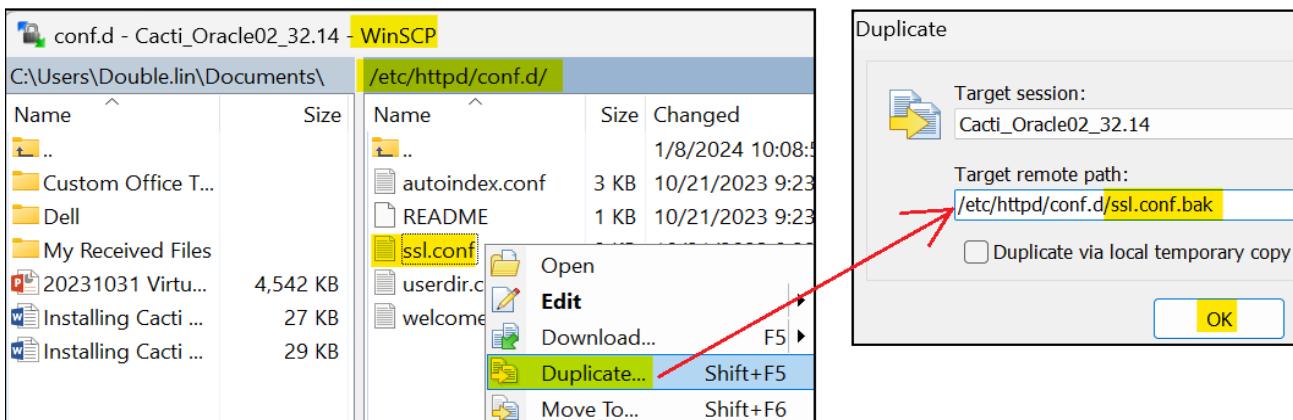
```
yum install -y mod_ssl net-tools nano wget git
```

```
[root@TWPVHQ014 ~]# yum install -y mod_ssl net-tools nano wget git
Last metadata expiration check: 0:32:03 ago on Mon 08 Jan 2024 10:04:51 PM CST.
Dependencies resolved.
=====
Package           Architecture   Version      Repository    Size
=====
Installing:
git              x86_64        2.39.3-1.el9_2   ol9_appstream 78 k
mod_ssl          x86_64        1:2.4.57-5.0.1.el9  ol9_appstream 118 k
nano             x86_64        5.6.1-5.el9     ol9_baseos_latest 790 k
net-tools         x86_64        2.0-0.62.20160912git.el9  ol9_baseos_latest 344 k
wget             x86_64        1.21.1-7.el9    ol9_appstream 861 k
```

```
# Configure ssl.conf after backup
```

```
cp /etc/httpd/conf.d/ssl.conf /etc/httpd/conf.d/ssl.conf.bak
```

(Option) Duplicate /etc/httpd/conf.d/ssl.conf via WinSCP



new add lines to disable TLS v1.x & CA path, add (#) on the 2 original .crt &.key path

```
SSLProtocol all -SSLv3 -TLSv1 -TLSv1.1
```

SSLCertificateFile /etc/ca/cacti.crt

```
SSLCertificateKeyFile /etc/ca/cacti.key  
#SSLCertificateFile /etc/pki/tls/certs/localhost.crt  
#SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

```
📝 /etc/httpd/conf.d/ssl.conf - Cacti_Oracle02_32.14 - Editor - WinSCP  
Listen 443 https  
  
# Disable TLS v1.x & modify CA path  
SSLProtocol all -SSLv3 -TLSv1 -TLSv1.1  
SSLCertificateFile /etc/ca/cacti.crt  
SSLCertificateKeyFile /etc/ca/cacti.key  
  
#SSLCertificateFile /etc/pki/tls/certs/localhost.crt  
# ECC keys, when in use, can also be configured in parallel  
#SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

#Edit /etc/httpd/conf.d/cacti.conf after backup by cp or winscp

nano /etc/httpd/conf.d/cacti.conf

```
<Directory /usr/share/cacti/>  
    <IfModule mod_authz_core.c>  
        # httpd 2.4  
        #Require host localhost  
        Require all granted  
    </IfModule>  
    <IfModule !mod_authz_core.c>  
        # httpd 2.2  
        #Order deny,allow  
        #Deny from all  
        #Allow from localhost  
        Order allow,deny  
        Allow from all  
    </IfModule>
```

systemctl restart httpd

```
[root@TWTPSVHQ014 ~]# systemctl restart httpd  
[root@TWTPSVHQ014 ~]#
```

2.8 Enable http compression

```
cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.bak  
nano /etc/httpd/conf/httpd.conf
```

```
# Enable GZIP compression  
LoadModule deflate_module modules/mod_deflate.so  
#  
# add the MIME (Multipurpose Internet Mail Extensions) types which  
# you want the server to compress  
<IfModule mod_deflate.c>  
    AddOutputFilterByType DEFLATE application/javascript  
    AddOutputFilterByType DEFLATE application/rss+xml
```

```

AddOutputFilterByType DEFLATE application/vnd.ms-fontobject
AddOutputFilterByType DEFLATE application/x-font
AddOutputFilterByType DEFLATE application/x-font-opentype
AddOutputFilterByType DEFLATE application/x-font-otf
AddOutputFilterByType DEFLATE application/x-font-truetype
AddOutputFilterByType DEFLATE application/x-font-ttf
AddOutputFilterByType DEFLATE application/x-javascript
AddOutputFilterByType DEFLATE application/xhtml+xml
AddOutputFilterByType DEFLATE application/xml
AddOutputFilterByType DEFLATE application/json
AddOutputFilterByType DEFLATE font/opentype
AddOutputFilterByType DEFLATE font/otf
AddOutputFilterByType DEFLATE font/ttf
AddOutputFilterByType DEFLATE image/svg+xml
AddOutputFilterByType DEFLATE image/x-icon
AddOutputFilterByType DEFLATE text/css
AddOutputFilterByType DEFLATE text/html
AddOutputFilterByType DEFLATE text/javascript
AddOutputFilterByType DEFLATE text/plain
AddOutputFilterByType DEFLATE text/xml

```

</IfModule>

```

GNU nano 5.6.1      /etc/httpd/conf/httpd.conf
ServerRoot "/etc/httpd"

# Enable GZIP compression
LoadModule deflate_module modules/mod_deflate.so

#
# add the MIME (Multipurpose Internet Mail Extensions) types
# you want the server to compress
<IfModule mod_deflate.c>
    AddOutputFilterByType DEFLATE application/javascript
    AddOutputFilterByType DEFLATE application/rss+xml
    AddOutputFilterByType DEFLATE application/vnd.ms-fontobj
    AddOutputFilterByType DEFLATE application/x-font
    AddOutputFilterByType DEFLATE application/x-font-opentype
    AddOutputFilterByType DEFLATE application/x-font-otf
    AddOutputFilterByType DEFLATE application/x-font-truetype
    AddOutputFilterByType DEFLATE application/x-font-ttf
    AddOutputFilterByType DEFLATE application/x-javascript
    AddOutputFilterByType DEFLATE application/xhtml+xml
    AddOutputFilterByType DEFLATE application/xml
    AddOutputFilterByType DEFLATE application/json
    AddOutputFilterByType DEFLATE font/opentype
    AddOutputFilterByType DEFLATE font/otf
    AddOutputFilterByType DEFLATE font/ttf
    AddOutputFilterByType DEFLATE image/svg+xml

```

systemctl restart httpd

PS. Gzip compression can be check later after Cacti is completed setup by Press F12 =>Network =>All => Select a php => Header => Response Headers =>content-encoding =>gzip

2.9 Disable firewall

```
systemctl stop firewalld
```

```
systemctl disable firewalld
```

```
systemctl status firewalld
```

```
[root@twtpsvhq014 ~]# systemctl stop firewalld
[root@twtpsvhq014 ~]# systemctl disable firewalld
[root@twtpsvhq014 ~]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; preset: enabled)
   Active: inactive (dead)
     Docs: man:firewalld(1)
```

2.10 (Optional) Enable firewall port: http https snmp

```
firewall-cmd --zone=public --add-service=http --add-service=https --add-service=snmp
```

```
firewall-cmd --runtime-to-permanent
```

```
[root@TWTPSVHQ014 ~]# firewall-cmd --zone=public --add-service=http --add-service=https --add-service=snmp
success
[root@TWTPSVHQ014 ~]# firewall-cmd --runtime-to-permanent
success
```

2.11 Install & Configure NTP

```
#Check NTP daemon is running & source IP
```

```
systemctl status chronyd
```

```
[root@TWTPSVHQ014 ~]# systemctl status chronyd
● chronyd.service - NTP client/server
  Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled; preset: enable
  Active: active (running) since Wed 2024-01-10 23:40:26 CST; 4 days ago
    Docs: man:chronyd(8)
          man:chrony.conf(5)
   Main PID: 904 (chronyd)
     Tasks: 1 (limit: 50492)
    Memory: 4.4M
      CPU: 1.310s
     CGroup: /system.slice/chronyd.service
             └─904 /usr/sbin/chronyd -F 2

Jan 10 23:40:25 TWTPSVHQ014.tpvaoc.com systemd[1]: Starting NTP client/server...
Jan 10 23:40:25 TWTPSVHQ014.tpvaoc.com chronyd[904]: chronyd version 4.3 starting (+C
Jan 10 23:40:26 TWTPSVHQ014.tpvaoc.com chronyd[904]: Frequency -15.308 +/- 0.173 ppm
Jan 10 23:40:26 TWTPSVHQ014.tpvaoc.com chronyd[904]: Using right/UTC timezone to obtain
Jan 10 23:40:26 TWTPSVHQ014.tpvaoc.com chronyd[904]: Loaded seccomp filter (level 2)
Jan 10 23:40:26 TWTPSVHQ014.tpvaoc.com systemd[1]: Started NTP client/server.
Jan 10 23:40:34 TWTPSVHQ014.tpvaoc.com chronyd[904]: Selected source 210.243.152.152
Jan 10 23:40:34 TWTPSVHQ014.tpvaoc.com chronyd[904]: System clock TAI offset set to 3
```

cp /etc/chrony.conf /etc/chrony.conf.bak

nano /etc/chrony.conf

```
#pool 2.pool.ntp.org iburst
pool 172.16.0.179 iburst
pool 172.16.0.178 iburst
```

```
GNU nano 5.6.1                                     /etc/chrony.conf
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (https://www.pool.ntp.org/join.html).
#pool 2.pool.ntp.org iburst
pool 172.16.0.179 iburst Replace with your local DC IPs
pool 172.16.0.178 iburst
```

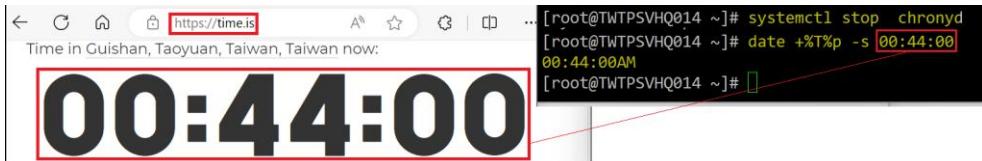
systemctl restart chronyd

```
[root@TWTPSVHQ014 ~]# systemctl restart chronyd
[root@TWTPSVHQ014 ~]#
```

systemctl status chronyd (verify selected source IP is switch to local DC now)

```
[root@TWTPSVHQ018 ~]# systemctl status chronyd
● chronyd.service - NTP client/server
  Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled; preset: enabled)
  Active: active (running) since Thu 2024-02-15 11:19:59 CST; 10s ago
Feb 15 11:19:59 TWTPSVHQ018.tpvaoc.com systemd[1]: Starting NTP client/server...
Feb 15 11:19:59 TWTPSVHQ018.tpvaoc.com chronyd[3640]: chronyd version 4.3 starting (+CMDMON +NT
Feb 15 11:19:59 TWTPSVHQ018.tpvaoc.com chronyd[3640]: Frequency -8.853 +/- 1.482 ppm read from
Feb 15 11:19:59 TWTPSVHQ018.tpvaoc.com chronyd[3640]: Using right/UTC timezone to obtain leap s
Feb 15 11:19:59 TWTPSVHQ018.tpvaoc.com chronyd[3640]: Loaded seccomp filter (level 2)
Feb 15 11:19:59 TWTPSVHQ018.tpvaoc.com systemd[1]: Started NTP client/server.
Feb 15 11:20:03 TWTPSVHQ018.tpvaoc.com chronyd[3640]: Selected source 172.16.0.178 <-Your DC IP
Feb 15 11:20:03 TWTPSVHQ018.tpvaoc.com chronyd[3640]: System clock TAI offset set to 37 seconds
```

(Optional-Troubleshooting) Reboot now if Selected source IP still not change to your local DC



3 Cacti Configuration

3.1 Pre-Installation Check

Default credential is **admin/admin**, change PW to **Tpv@TP2024**

<https://172.17.32.14/cacti>

Cacti Server v1.2.25 - Installation Wizard

Pre-installation Checks

Location checks

PHP - Recommendations (web)

PHP Recommendations (/etc/php.ini)				
Name	Current	Recommended	Status	Description
version	8.0.30	>= 5.4.0	Passed	PHP 5.4.0 is the minimum version
memory_limit	128M	>= 400M	Restart Required	A minimum of 400M memory limit
max_execution_time	30	>= 60	Warning	A minimum of 60 m execution time
date.timezone	Asis/Taipei	>=	Passed	A valid timezone that matches MySQL and the system

PHP - Recommendations (cli)

PHP Recommendations (/etc/php.ini)				
Name	Current	Recommended	Status	Description
version	8.0.30	>= 5.4.0	Passed	PHP 5.4.0 is the minimum version
memory_limit	128M	>= 400M	Restart Required	A minimum of 400M memory limit
max_execution_time	0	>= 60	Passed	A minimum of 60 m execution time
date.timezone	Asis/Taipei	>=	Passed	A valid timezone that matches MySQL and the system

↑Follow up yellow marker to modify /etc/php.ini

cp /etc/php.ini /etc/php.ini.bak

nano /etc/php.ini

systemctl restart php-fpm

```
GNU nano 5.6.1          /etc/php.ini      Modified
; Maximum amount of memory a script may consume
; http://php.net/memory-limit
memory_limit = 400M
; Maximum execution time of each script, in seconds
; http://php.net/max-execution-time
; Note: This directive is hardcoded to 0 for the CLI SAPI
max_execution_time = 60

[root@TWTPSVHQ014 ~]# systemctl restart php-fpm
[root@TWTPSVHQ014 ~]# 
```

Cacti Server v1.2.25 - Installation Wizard

MySQL - TimeZone Support

!

ERROR: Your MySQL TimeZone database is not populated. Please populate this database before proceeding.

↑ fix MySql Time zone DB issue

mysql_tzinfo_to_sql /usr/share/zoneinfo | mysql -uroot -pc@Ct1Vser mysql

```
[root@TWTPSVHQ014 ~]# mysql_tzinfo_to_sql /usr/share/zoneinfo | mysql -uroot -pc@Ct1Vser mysql
[root@TWTPSVHQ014 ~]# 
```

MySQL - Settings			
These MySQL performance tuning settings will help your Cacti system perform better without issues for a longer time.			
Recommended MySQL System Variable Settings			
MariaDB Tuning (/etc/my.cnf.d/server.cnf) - [Documentation] Note: Many changes below require a database restart	Variable	Current Value	Recommended Value
Comments			
sort_buffer_size	2 M	<= -6.99 M	When performing joins, if they are below this size, they will be kept in memory and never written to a temporary file. As this is a per connection memory allocation, care must be taken not to increase it too high. The sum of the join_buffer_size + sort_buffer_size + read_buffer_size + read_rnd_buffer_size + thread_stack + binlog_cache_size + Core MySQL/MariaDB memory should be below 80%. If the recommendation is negative, you must decrease this and or the sort_buffer_size until the recommendation fits within the allowable memory.
innodb_doublewrite	ON	= OFF	When using MariaDB 10.2.4 and above, this setting should be off if atomic writes are enabled. Therefore, please enable atomic writes instead of the double write buffer as it will increase performance.

↑ fix MySql settings issue

cp /etc/my.cnf.d/server.cnf /etc/my.cnf.d/server.cnf.bak

nano /

sort_buffer_size = 10M

join_buffer_size = 15M

innodb_doublewrite = OFF

max_connections = 600

```
GNU nano 5.6.1                               /etc/my.cnf.d/server.cnf
[[mysqld]]
sort_buffer_size = 10M
join_buffer_size = 15M
innodb_doublewrite = OFF
```

systemctl restart mariadb

Refresh cacti web page to check status are all GREEN thumb UP => Click Next

Cacti Server v1.2.25 - Installation Wizard

Pre-installation Checks

Location checks	✓
PHP - Recommendations (web)	✓
PHP - Recommendations (cli)	✓
PHP - Module Support (Required)	✓
PHP - Module Support (Optional)	✓
MySQL - TimeZone Support	✓
MySQL - Settings	✓

Previous | Next

Cacti Server v1.2.25 - Installation Wizard

Installation Type

Please select the type of installation

Installation options:

- **New Primary Server** - Choose this for the Primary site.
- **New Remote Poller** - Remote Pollers are used to access networks that are not readily accessible to the Primary site.

New Primary Server

The following information has been determined from Cacti's configuration file. If it is not correct, please edit "include/config.php" before continuing.

Local Database Connection Information

```
Database: cacti
Database User: cactiuser
Database Hostname: localhost
Port: 3306
Server Operating System Type: unix
```

Previous Next

Cacti Server v1.2.25 - Installation Wizard

Directory Permission Checks

Please ensure the directory permissions below are correct before proceeding. During the install, these directories need to be owned by the Web Server user. These permission changes are required to allow the Installer to install Device Template packages which include XML and script files that will be placed in these directories. If you choose not to install the packages, there is an 'install_package.php' cli script that can be used from the command line after the install is complete.

After the install is complete, you can make some of these directories read only to increase security.

NOTE: If you are installing packages, once the packages are installed, you should change the scripts directory back to read only as this presents some exposure to the web site.

Potential permission issues

Please make sure that your webserver has read/write access to the cacti folders that show errors below. If SELinux is enabled on your server, you can either permanently disable this, or temporarily disable it and then add the appropriate permissions using the SELinux command-line tools.

An example of how to set folder permissions is shown here, though you may need to adjust this depending on your operating system, user accounts and desired permissions.

EXAMPLE: `chown -R apache.apache /usr/share/cacti/log/`

NOTE: Once installation has completed the CSRF path, should be set to read-only.

Required Writable at Install Time Only

Required Writable after Install Complete

/tmp/	Writable
/usr/share/cacti/log/	Not Writable
/usr/share/cacti/cache/boost/	Writable
/usr/share/cacti/cache/mibcache/	Writable
/usr/share/cacti/cache/realtime/	Writable
/usr/share/cacti/cache/spikekill/	Writable

Previous Next

↑ fix writable permission issue of /usr/share/cacti/log/ by Disable SELinux temporarily
setenforce 0

```
[root@TWTPSVHQ014 ~]# setenforce 0
[root@TWTPSVHQ014 ~]#
```

#disable selinux permanently from enforcing to disabled
cp /etc/sysconfig/selinux /etc/sysconfig/selinux.bak
nano /etc/sysconfig/selinux
SELINUX=disabled

```
GNU nano 5.6.1
/etc/sysconfig/selinux
#   grubby --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#   grubby --update-kernel ALL --remove-args selinux
#
SELINUX=disabled
```

Refresh Cacti web page =>Click Next

The screenshot shows the 'Cacti Server v1.2.25 - Installation Wizard' interface. The title bar says 'Cacti Server v1.2.25 - Installation Wizard'. The main content area is titled 'Directory Permission Checks'. It contains instructions about ensuring directory permissions are correct before proceeding, mentioning XML and script files that will be placed in these directories. It also notes that after the install, some directories can be made read-only for security. A note states: 'If you are installing packages, once the packages are installed, you should change the scripts directory back to read only as this presents some exposure to the web site.' Below this, there are three sections with thumbs-up icons: 'Potential permission issues', 'Required Writable at Install Time Only', and 'Required Writable after Install Complete'. At the bottom, there are 'Previous' and 'Next' buttons.

↓Change spine path later => Select RRDTool 1.8 (default is 1.7.2)

Critical Binary Locations and Versions

Make sure all of these values are correct before continuing.

PHP Binary Path ?	/usr/bin/php	
RRDtool Binary Path ?	/usr/bin/rrdtool	
snmpwalk Binary Path ?	/usr/bin/snmpwalk	
snmpget Binary Path ?	/usr/bin/snmpget	
snmpbulkwalk Binary Path ?	/usr/bin/snmpbulkwalk	
snmpgetnext Binary Path ?	/usr/bin/snmpgetnext	
snmptrap Binary Path ?	/usr/bin/snmptrap	
Sendmail Path ?	/usr/sbin/sendmail	
Spine Binary File Location ?	/usr/local/spine/bin/spine	
Spine Config File Path ?	Enter a valid file path Change path later	
Cacti Log Path ?	/usr/share/cacti/log/cacti.log	
Poller Standard Error Log Path ?	/usr/share/cacti/log/cacti_stder.log	
RRDtool Version ?	RRDtool 1.8+ Select 1.8	

[Previous](#)[Next](#)

Input Validation Whitelist Protection

Cacti Data Input methods that call a script can be exploited in ways that a non-administrator can perform damage to either files owned by the poller account, and in cases where someone runs the Cacti poller as root, can compromise the operating system allowing attackers to exploit your infrastructure.

Therefore, several versions ago, Cacti was enhanced to provide Whitelist capabilities on the these types of Data Input Methods. Though this does secure Cacti more thoroughly, it does increase the amount of work required by the Cacti administrator to import and manage Templates and Packages.

The way that the Whitelisting works is that when you first import a Data Input Method, or you re-import a Data Input Method, and the script and or arguments change in any way, the Data Input Method, and all the corresponding Data Sources will be immediately disabled until the administrator validates that the Data Input Method is valid.

To make identifying Data Input Methods in this state, we have provided a validation script in Cacti's CLI directory that can be run with the following options:

- **php -q input_whitelist.php --audit** - This script option will search for any Data Input Methods that are currently banned and provide details as to why.
- **php -q input_whitelist.php --update** - This script option un-ban the Data Input Methods that are currently banned.
- **php -q input_whitelist.php --push** - This script option will re-enable any disabled Data Sources.

It is strongly suggested that you update your config.php to enable this feature by uncommenting the **\$input_whitelist** variable and then running the three CLI script options above after the web based install has completed.

Check the Checkbox below to acknowledge that you have read and understand this security concern

I have read this statement

[Previous](#)[Next](#)

Disable “Scan mode”

Cacti Server v1.2.25 - Installation Wizard

Default Profile

Please select the default Data Source Profile to be used for polling sources. This is the maximum amount of time between scanning devices for information so the lower the polling interval, the more work is placed on the Cacti Server host. Also, select the intended, or configured Cron interval that you wish to use for Data Collection.

Default Profile	5 Minute Collection ▾
Cron Interval	Every 5 Minutes ▾

Default Automation Network

Cacti can automatically scan the network once installation has completed. This will utilise the network range below to work out the range of IPs that can be scanned. A predefined set of options are defined for scanning which include using both 'public' and 'private' communities.

If your devices require a different set of options to be used first, you may define them below and they will be utilized before the defaults

All options may be adjusted post installation

Default Options

Scan Mode	
Network Range	192.168.1.0/24
Additional Defaults	

Previous **Next**

Default all Template are selected. => Next

Template Setup

Please select the Device Templates that you wish to use after the Install. If your Operating System is Windows, you need to ensure that you select the 'Windows Device' Template. If your Operating System is Linux/UNIX, make sure you select the 'Local Linux Machine' Device Template.

Templates

Name	Description	Author	Homepage	<input checked="" type="checkbox"/>
ACME.xml.gz	ACME Device Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>
AKCP_Device.xml.gz	AKCP Device Device Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>
APC_InfraStruXure_InRow_CRAC.xml.gz	APC InfraStruXure InRow CRAC Device Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>
APC_InfraStruXure_PDU.xml.gz	APC InfraStruXure PDU Device Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>
Apache_Webserver.xml.gz	Apache Webserver Device Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>
Aruba_Instant_AP_Cluster.xml.gz	Aruba Instant AP Cluster Device Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>
BayTech_PDU.xml.gz	BayTech PDU Device Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>
Cacti_Stats.xml.gz	Cacti Stats Device Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>
Cisco_Router.xml.gz	Cisco Router Device Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>
Citrix_NetScaler_VPX.xml.gz	Citrix NetScaler VPX Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>
ESXi_Device.xml.gz	ESXi Device Device Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>
Fortigate.xml.gz	Fortigate Device Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>
Generic_SNMP_Device.xml.gz	Generic SNMP Device Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>
Local_Linux_Machine.xml.gz	Local Linux Machine Device Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>
MikroTik_Device.xml.gz	MikroTik Device Device Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>
MikroTik_Switch_SWOS.xml.gz	MikroTik Switch (SWOS) Device Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>
Motorola_SB6141.xml.gz	Motorola SB6141 Device Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>
NetSNMP_Device.xml.gz	Net-SNMP Device Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>
PING_Advanced_Ping.xml.gz	PING - Advanced Ping Graph Template Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>
SNMP_Printer.xml.gz	SNMP Printer Device Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>
SNMP_UPS.xml.gz	SNMP UPS Device Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>
Synology_NAS.xml.gz	Synology NAS Device Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>
Windows_Device.xml.gz	Windows Device Package	The Cacti Group	cacti.net	<input checked="" type="checkbox"/>

Device Templates allow you to monitor and graph a vast assortment of data within Cacti. After you select the desired Device Templates, press 'Next' and the installation will complete. Please be patient on this step, as the importation of the Device Templates can take a few minutes.

[Previous](#)[Next](#)

Cacti Server v1.2.25 - Installation Wizard

Server Collation

Your server collation appears to be UTF8 compliant

Database Collation

Your database default collation appears to be UTF8 compliant

Table Setup

All your tables appear to be UTF8 and Dynamic row format compliant

[Previous](#) [Next](#)

Check "Confirmed Installation" => Install

Cacti Server v1.2.25 - Installation Wizard

Confirm Installation

Your Cacti Server is almost ready. Please check that you are happy to proceed.

NOTE: Press 'Confirm Installation' then click 'Install' to complete the installation process after selecting your Device Templates.

Confirm Installation

[Previous](#) [Install](#)

Cacti Server v1.2.25 - Installation Wizard

Installing Cacti Server v1.2.25

Your Cacti Server is now installing

Refresh in [Progress](#) Last updated: 01:50:47

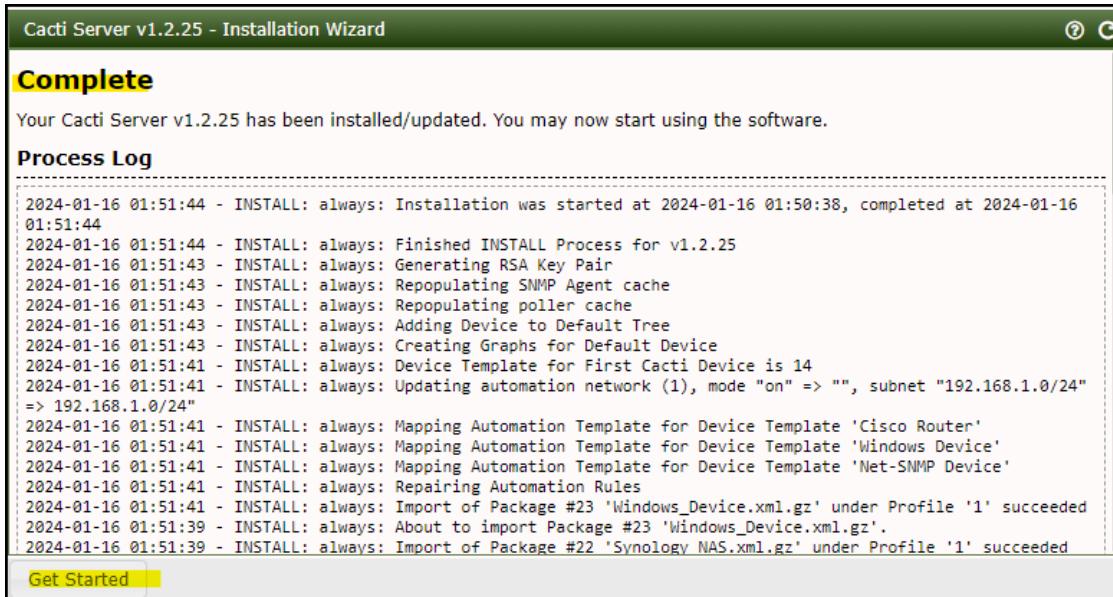
47 %

```
2024-01-16 01:50:47 - INSTALL: always: About to import Package #7 'BayTech_PDU.xml.gz'.
2024-01-16 01:50:47 - INSTALL: always: Import of Package #6 'Aruba_Instant_AP_Cluster.xml.gz' under Profile '1' succeeded
2024-01-16 01:50:46 - INSTALL: always: About to import Package #6 'Aruba_Instant_AP_Cluster.xml.gz'.
2024-01-16 01:50:46 - INSTALL: always: Import of Package #5 'APC_InfraStruXure_PDU.xml.gz' under Profile '1' succeeded
2024-01-16 01:50:44 - INSTALL: always: About to import Package #5 'APC_InfraStruXure_PDU.xml.gz'.
2024-01-16 01:50:44 - INSTALL: always: Import of Package #4 'APC_InfraStruXure_InRow_CRAC.xml.gz' under Profile '1' succeeded
2024-01-16 01:50:42 - INSTALL: always: About to import Package #4 'APC_InfraStruXure_InRow_CRAC.xml.gz'.
2024-01-16 01:50:42 - INSTALL: always: Import of Package #3 'Apache_Webserver.xml.gz' under Profile '1' succeeded
```

Cacti Server v1.2.25 - Installation Wizard

```
2024-01-16 01:50:47 - INSTALL: always: About to import Package #7 'BayTech_PDU.xml.gz'.
2024-01-16 01:50:47 - INSTALL: always: Import of Package #6 'Aruba_Instant_AP_Cluster.xml.gz' under Profile '1' succeeded
2024-01-16 01:50:46 - INSTALL: always: About to import Package #6 'Aruba_Instant_AP_Cluster.xml.gz'.
2024-01-16 01:50:46 - INSTALL: always: Import of Package #5 'APC_InfraStruXure_PDU.xml.gz' under Profile '1' succeeded
2024-01-16 01:50:44 - INSTALL: always: About to import Package #5 'APC_InfraStruXure_PDU.xml.gz'.
2024-01-16 01:50:44 - INSTALL: always: Import of Package #4 'APC_InfraStruXure_InRow_CRAC.xml.gz' under Profile '1' succeeded
2024-01-16 01:50:42 - INSTALL: always: About to import Package #4 'APC_InfraStruXure_InRow_CRAC.xml.gz'.
2024-01-16 01:50:42 - INSTALL: always: Import of Package #3 'Apache_Webserver.xml.gz' under Profile '1' succeeded
2024-01-16 01:50:41 - INSTALL: always: About to import Package #3 'Apache_Webserver.xml.gz'.
2024-01-16 01:50:41 - INSTALL: always: Import of Package #2 'AKCP_Device.xml.gz' under Profile '1' succeeded
2024-01-16 01:50:40 - INSTALL: always: About to import Package #2 'AKCP_Device.xml.gz'.
2024-01-16 01:50:40 - INSTALL: always: Import of Package #1 'ACME.xml.gz' under Profile '1' succeeded
2024-01-16 01:50:39 - INSTALL: always: About to import Package #1 'ACME.xml.gz'.
2024-01-16 01:50:39 - INSTALL: always: Found 23 templates to install
2024-01-16 01:50:39 - INSTALL: always: No tables where found or selected for conversion
2024-01-16 01:50:39 - INSTALL: always: Starting INSTALL Process for v1.2.25
2024-01-16 01:50:38 - INSTALL: always: Setting PHP Option memory_limit = -1
2024-01-16 01:50:38 - INSTALL: always: Setting PHP Option max_execution_time = 0
2024-01-16 01:50:38 - INSTALL: Checking arguments
2024-01-16 01:50:38 - INSTALL: always: Spawning background process: /usr/bin/php '/usr/share/cacti/install/background.php' 1705369838.1457
```

[Get Started](#)



Done.

The screenshot shows the Cacti web interface at <https://172.17.32.14/cacti/>. The left sidebar contains links for Main Console, Create, Management, Data Collection, Templates, Automation, Presets, Import/Export, Configuration, Utilities, and Troubleshooting. The main content area displays a message: "You are now logged into **Cacti**. You can follow these basic steps to get started." followed by a bulleted list: "Create devices for network", "Create graphs for your new devices", and "View your new graphs".

3.2 Configure Cacti

#Define spine execute path to /usr/local/spine/etc/spine.conf & Enable RRD File Auto Clean

On Device Default.

General	Paths	Device Defaults	Poller	Data	Visual	Authentication	Performance	Spikes
Cacti Settings (Device Defaults)								
General Defaults								
Template ?	None		Default is ACME					
Site ?	Core							
Poller ?	Main Poller							
Device Threads ?	8 Threads		Default is 1 Thread					
Re-index Method for Data Queries ?	Uptime							
Default Interface Speed ?	1 Gbps Ethernet							
SNMP Defaults								
Version ?	Version 2							
Community ?	TpvTech1							
Port Number ?	161							
Timeout ?	600		Default is 500ms					
Retries ?	3							
Availability/Reachability								
Downed Device Detection ?	Ping		Default is SNMP Uptime					
Ping Type ?	ICMP Ping							
Ping Port ?	23							
Ping Timeout Value ?	600		Default is 400ms					
Ping Retry Count ?	3		Default is 1 Retry					
Up/Down Settings								
Failure Count ?	1		Default is 2					
Recovery Count ?	2		Default is 3					
<input type="button" value="Save"/>								

Polling

General	Paths	Device Defaults	Poller	Authentication	Pe
Cacti Settings (Poller)					
General					
Data Collection Enabled ?	<input type="button" value=""/>				
SNMP Agent Support Enabled ?	<input type="button" value=""/>				
Poller Type ?	spine ▾				
Poller Sync Interval ?	Every 2 Hours ▾				
Poller Interval ?	Every 5 Minutes				
Cron/Daemon Interval ?	Every 5 Minutes				
Balance Process Load ?	<input type="button" value=""/>				
Debug Output Width ?	<input type="button" value=""/>				
Disable increasing OID Check ?	<input type="button" value=""/>				
Remote Agent Timeout ?	5 Seconds ▾				
SNMP Bulkwalk Fetch Size ?	10 ▾				
SNMP Get OID Limit ?	10				
Refresh Poller Table Per Cycle ?	<input type="button" value=""/>				
Disable Resource Cache Replication ?	<input type="button" value=""/>				
Additional Data Collector Settings					
Invalid Data Logging ?	None ▾				
Number of PHP Script Servers ?	Default is 8 1 server				
Script and Script Server Timeout Value ?	25				
Periodic All Device Re-Index					
Re-Index All Device Schedule ?	Disabled ▾				
Background Timeout and Concurrent Process Settings					
Report Generation Timeout ?	5 Minutes ▾				
Data Source Statistics Timeout ?	5 Minutes ▾				
RRDfile Check Timeout ?	5 Minutes ▾				
Poller Commands Timeout ?	5 Minutes ▾				
Poller Command Concurrent Processes ?	Default is 8 Processes 1 Process				
Maintenance Background Generation Timeout ?	5 Minutes ▾				
Spikekill Background Generation Timeout ?	1 Hour ▾				
Data Collector Defaults					
Data Collector Processes ?	Both default 8				
Threads per Process ?	Both default are 1 Process 2				
<input type="button" value="Save"/>					

Mail/Reporting/DNS

Performance	Spikes	Mail/Reporting/DNS
Cacti Settings (Mail/Reporting/DNS)		
URL Linking		
Server Base URL ?	https://172.17.32.14/cacti/	
Emailing Options		
Notify Primary Admin of Issues ?	<input type="button" value=""/>	
Test Email ?	Double.lin@tpv-tech.com	
Mail Services ?	SMTP ▾	
Ping Mail Server ?	Yes ▾	
From Email Address ?	Cacti.GIOS@tpv-tech.com	
From Name ?	Cacti.GIOS	
Word Wrap ?	120	
SMTP Options		
SMTP Hostname ?	172.16.15.205	
SMTP Port ?	25	
SMTP Username ?		
SMTP Password ?	***** *****	
SMTP Security ?	None ▾	
SMTP Timeout ?	10	
Reporting Presets		
Default Graph Image Format ?	Inline PNG Image ▾	
Maximum E-Mail Size ?	10 Megabytes ▾	
Poller Logging Level for Cacti	LOW - Statistics and	
Reporting		
Enable Lotus Notes (R) tweak ?	<input type="button" value=""/>	
DNS Options		
Primary DNS IP Address ?	172.16.0.179	
Secondary DNS IP Address ?	172.16.0.278	
DNS Timeout ?	500	
<input type="button" value="Save"/>		

Change Data collectors to your hostname & Time zone

3.3 Install Plug-in

#Install Plug-in, configuration will be in next step.

```
cd /usr/share/cacti/site/plugins
sudo git clone https://github.com/Cacti/plugin_thold.git
sudo mv plugin_thold thold
```

```
[root@TWTPSVHQ014 ~]# cd /usr/share/cacti/plugins
[root@TWTPSVHQ014 plugins]# git clone https://github.com/Cacti/plugin_thold.git
Cloning into 'plugin_thold'...
remote: Enumerating objects: 7557, done.
remote: Counting objects: 100% (2106/2106), done.
remote: Compressing objects: 100% (425/425), done.
remote: Total 7557 (delta 1715), reused 2066 (delta 1677), pack-reused 5451
Receiving objects: 100% (7557/7557), 7.87 MiB | 9.14 MiB/s, done.
Resolving deltas: 100% (5844/5844), done.
[root@TWTPSVHQ014 plugins]# mv plugin_thold thold
```

goto configuration=>Plugins=>Install “Thold” =>Enable “Thold”

All 1 Plugins						
Actions	Plugin Name	Plugin Description	Status	Author	Requires	Version
1	Thold	Thresholds	Active	The Cacti Group		1.8

#Repeat above to install other plug-ins

```
git clone https://github.com/Cacti/plugin_maint
mv plugin_maint maint
git clone https://github.com/Cacti/plugin_monitor
mv plugin_monitor monitor
git clone https://github.com/Cacti/plugin_weathermap
mv plugin_weathermap weathermap
git clone https://github.com/Cacti/plugin_syslog
mv plugin_syslog syslog
git clone https://github.com/Cacti/plugin_wmi
mv plugin_wmi wmi
git clone https://github.com/Cacti/plugin_webseer
mv plugin_webseer webseer
git clone https://github.com/Cacti/plugin_flowview
```

```
mv plugin_flowview flowview  
goto configuration=>Plugins=>Install "Thold" =>Enable plug-ins
```

All 8 Plugins				
Actions	Plugin Name	Plugin Description	Status	Author
	Monitor	Device Monitoring	Active	The Cacti Group
	Flowview	FlowView	Active	The Cacti Group
	Maint	Maintenance Scheduler	Active	The Cacti Group
	Webseer	Service Monitor	Active	The Cacti Group
	Syslog	Syslog Monitoring	Not Installed	The Cacti Group
	Thold	Thresholds	Active	The Cacti Group
	Weathermap	Weathermap Plugin	Active	Howard Jones and The Cacti Group
	Wmi	WMI Information Collector	Active	The Cacti Group

Disable Cacti alert mail when add a New Device into monitor

Main Console

Configuration

Settings

Users

User Groups

User Domains

Plugins

Alerting/Thold

Monitor

Reports

Cacti Settings (Monitor)

Reboot Notifications

Send Reboot Notifications ?

Send one Email to all addresses ?

Include Threshold Alert Lists ?

3.4 Enable thold as a service

```
cp /usr/share/cacti/plugins/thold/service/systemd/thold_daemon.service /etc/systemd/system  
nano /etc/systemd/system/ thold_daemon.service
```

```

/etc/systemd/system/thold_daemon.service - Cacti_Oracle02_32.14 - Editor - WinSCP
[Unit]
Description=Cacti Threshold Daemon Service
Required=mariadb.service
After=network.target auditd.service mariadb.service

[Service]
User=apache
Group=apache
Type=forking
ExecStart=/usr/bin/php /usr/share/cacti/plugins/thold/thold_daemon.php
KillMode=process
Restart=on-failure

[Install]
WantedBy=multi-user.target

```

chmod +x /usr/share/cacti/plugins/thold/thold_daemon.php

systemctl daemon-reload

```

# chmod +x /usr/share/cacti/plugins/thold/thold_daemon.php
# systemctl daemon-reload

```

systemctl start thold_daemon

systemctl status thold_daemon

```

● thold_daemon.service - Cacti Threshold Daemon Service
  Loaded: loaded (/etc/systemd/system/thold_daemon.service; enabled; preset: disabled)
  Active: active (running) since Tue 2024-10-01 10:58:23 CST; 3min 8s ago
    Process: 1550 ExecStart=/usr/bin/php /usr/share/cacti/plugins/thold/thold_daemon.php (code=exited, status=0/SUCCESS)
   Main PID: 1600 (php)
      Tasks: 2 (limit: 153761)
     Memory: 47.4M
        CPU: 1.238s
       CGroup: /system.slice/thold_daemon.service
               └─1600 /usr/bin/php /usr/share/cacti/plugins/thold/thold_daemon.php
                   ├─1605 /usr/bin/php /usr/share/cacti/plugins/thold/thold_process.php --thread=1

Oct 01 10:58:22 twtpsvhq014.tpvao.com systemd[1]: Starting Cacti Threshold Daemon Service...
Oct 01 10:58:22 twtpsvhq014.tpvao.com php[1550]: Starting Thold Daemon ... [OK]
Oct 01 10:58:23 twtpsvhq014.tpvao.com systemd[1]: Started Cacti Threshold Daemon Service.

```

3.5 Enable 1 minute data collection and keep 1 month & 1Year

Data Source Profile RRAs (Read Only)					
	Name	Data Retention	Graph Timespan	Steps	Rows
SNMP	Daily (1 Minute Average)	1 Month, 24 Hours	1 Day	1	44640
CDEFs	Yearly (5 Minute Average)	12 Months, 5 Days	1 Year	5	105120
VDEFs					

- 日圖: 用於故障排排& 效能優化. 1min 採樣, 保留 1 個月.
- 年圖: 用於歷史數據回顧. 5mins 採樣, 保留 1 年. 使用場景如: D:碟過去一年使用率的增長趨勢, 過去一年這條 Internet 線路的頻寬使用狀況. 以做為設備增購參考.
- 提高準確度: 會較現況年圖增加 288 倍 (1440min/5min), 因為現況年圖是 24 小時(1440 mins)

取樣,新版 5 分鐘.

Preset=>Data Profile =>Click ‘+’ =>

Main Console	Data Source Profile [new]	
Create	Name ?	UDF_1 min & keep 1Mon-1Year
Management	Polling Interval ?	Every Minute
Data Collection	Heartbeat ?	2 Minutes
Templates	X-Files Factor ?	0.5
Automation	Consolidation Functions ?	AVERAGE, MIN, MAX, LAST
Presets	Default ?	
Data Profiles	RRDfile Size (in Bytes) ?	0 KBytes per Data Sources and 284 Bytes for the Header
SNMP	Cancel Create	
CDEFs		
VDEFs		
Colors		
GPRINTs		

Click ‘+’

Data Source Profile RRAs (press save to update timespan)				
Name	Data Retention	Graph Timespan	Steps	Rows

Create “Daily (1 Minute Average) =>44640 => 1 Day => Create

RRA [edit:]	
Name ?	Daily (1 Minute Average)
Aggregation Level ?	Each Insert is New Row
Rows ?	44640
Default Timespan ?	1 Day
Data Retention ?	1 Month, 24 Hours
RRA Size (in Bytes) ?	1,428 KBytes per Data Source
Cancel Create	

Click ‘+’

Data Source Profile RRAs (press save to update timespan)				
Name	Data Retention	Graph Timespan	Steps	Rows
Daily (1 Minute Average)	1 Month, 24 Hours	1 Day	1	44640

Create “Yearly (5 Minute Average)” =>5 minutes =>105120 rows=>1 year =>Create

RRA [edit:]

Name ?	Yearly (5 Minute Average)
Aggregation Level ?	5 Minutes ▾
Rows ?	105120
Default Timespan ?	1 Year ▾
Data Retention ?	12 Months, 5 Days
RRA Size (in Bytes) ?	3,364 KBytes per Data Source

Cancel **Create**

Click Save =>Done

Data Source Profile [edit: UDF_1 min & keep 1Mon-1Year]

Name ?	UDF_1 min & keep 1Mon-1Year
Polling Interval ?	Every Minute ▾
Heartbeat ?	2 Minutes ▾
X-Files Factor ?	0.5
Consolidation Functions ?	AVERAGE, MIN, MAX, LAST ▾
Default ?	
RRDfile Size (in Bytes) ?	4,793 KBytes per Data Sources and 284 Bytes for the Header

Data Source Profile RRAs (press save to update timespar) +

Name	Data Retention	Graph Timespan	Steps	Rows
Daily (1 Minute Average)	1 Month, 24 Hours	1 Day	1	44640
Yearly (5 Minute Average)	12 Months, 5 Days	1 Year	5	105120

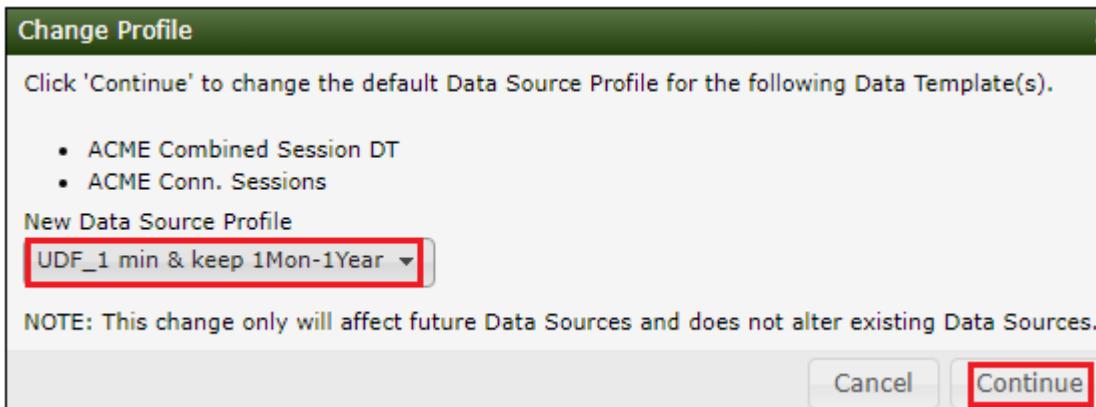
Return **Save**

Replace all Template 'data sources' with new profile

Template => Data Source => Data Template "750" => select ALL data sources => "Change Profile" => Go

Templates		Data Templates										
Device Graph	Data Source	All 336 Data Templates										
		Data Template Name		ID	Deletable	Data Sources Using		Input Method	Profile Name	Status		
		ACME Combined Session DT		2	Yes	0		Get SNMP Data	1 Minute Collection	Active		
		ACME Conn. Sessions		6	Yes	0		Get SNMP Data	1 Minute Collection	Active		
		ACME CPS		7	Yes	0		Get SNMP Data	1 Minute Collection	Active		
		ACME CPU Usage (5 min.)		9	Yes	0		Get SNMP Data	1 Minute Collection	Active		
		All 336 Data Templates							Change Profile	Go		

Select "UDF_1 min & Keep 1mon-1Year"=>Continue



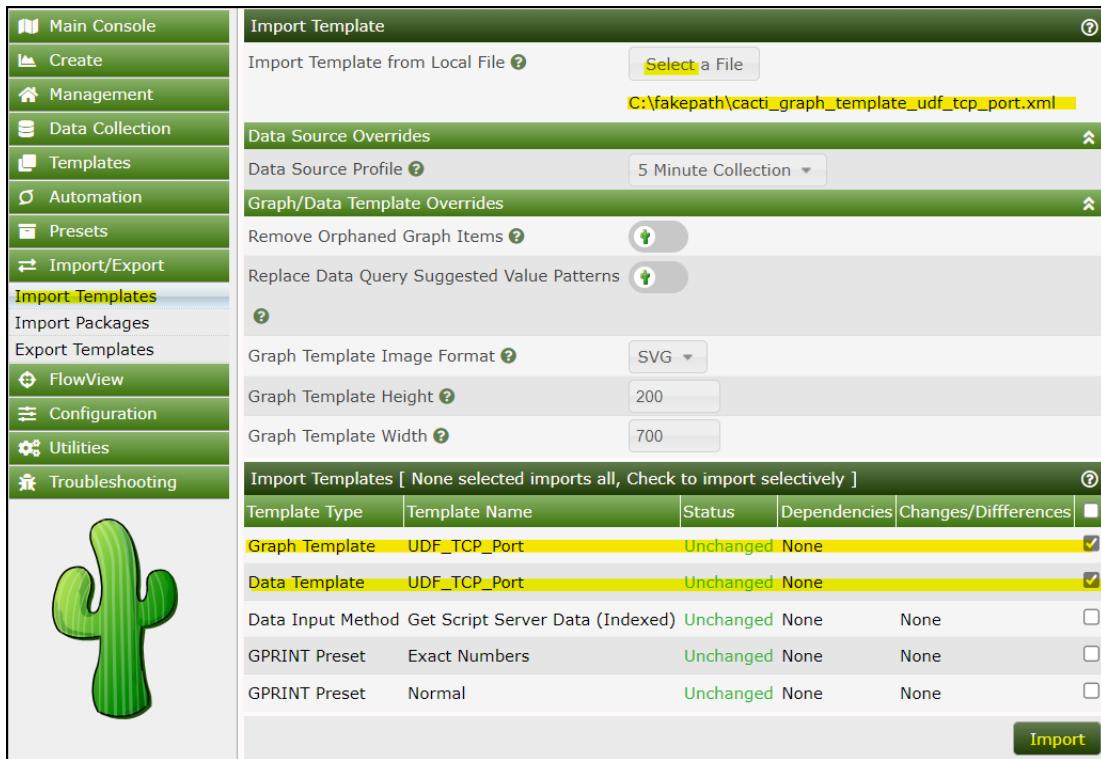
Done.

All 336 Data Templates							
Data Template Name	ID	Deletable	Data Sources Using	Input Method	Profile Name	Status	
ACME Combined Session DT	2	Yes	0	Get SNMP Data	UDF_1 min & keep 1Mon-1Year	Active	
ACME Conn. Sessions	6	Yes	0	Get SNMP Data	UDF_1 min & keep 1Mon-1Year	Active	
ACME CPS	7	Yes	0	Get SNMP Data	UDF_1 min & keep 1Mon-1Year	Active	
ACME CPU Usage (5 min.)	9	Yes	0	Get SNMP Data	UDF_1 min & keep 1Mon-1Year	Active	

3.6 Import Monitor Template - Win Service & TCP Port & Linux process

cacti_graph_template_udf_tcp_port.xml
cacti_graph_template_udf_winservices.xml

Template Type	Template Name	Status	Dependencies	Changes/Differences
Graph Template	UDF_WinServices	New	None	<input checked="" type="checkbox"/>
Data Template	UDF_WinServices	New	None	<input checked="" type="checkbox"/>
Data Input Method	Get Script Server Data (Indexed)	Unchanged	None	<input type="checkbox"/>
GPRINT Preset	Exact Numbers	Unchanged	None	<input type="checkbox"/>
GPRINT Preset	Normal	Unchanged	None	<input type="checkbox"/>



/usr/share/cacti/resource/script_server/tcp.xml
 /usr/share/cacti/resource/script_server/win_services.xml

D:\...\Source\Template\	/usr/share/cacti/resource/script_server/					
Name		Name	Size	Changed	Rights	Owner
..		..		1/10/2024 9:33:36 PM	rwxr-xr-x	apache
ucd_net_processes		win_services.xml	2 KB	12/3/2013 5:42:04 PM	rw-r--r--	root
cacti_graph_template_udf_tcp		tcp.xml	2 KB	12/13/2013 2:55:14 PM	rw-r--r--	root
cacti_graph_template_udf_win		webseer.xml	2 KB	1/16/2024 9:50:52 AM	rw-r--r--	apache
TCP&WinService.txt		netsnmp_lmsensors_...	2 KB	1/16/2024 9:51:26 AM	rw-r--r--	apache
tcp.php		netsnmp_lmsensors_...	2 KB	1/16/2024 9:51:26 AM	rw-r--r--	apache
tcp.xml		netsnmp_lmsensors_...	2 KB	1/16/2024 9:51:26 AM	rw-r--r--	apache
ucd_net_processes.zip		mikrotik_wireless_reg...	4 KB	1/16/2024 9:51:16 AM	rw-r--r--	apache
win_services.php		mikrotik_trees.xml	2 KB	1/16/2024 9:51:16 AM	rw-r--r--	apache
win_services.xml		mikrotik_qusers.xml	3 KB	1/16/2024 9:51:16 AM	rw-r--r--	apache

/usr/share/cacti/scripts/tcp.php
 /usr/share/cacti/scripts/win_services.php

D:\...\Source\Template\	/usr/share/cacti/scripts/					
Name		Name	Size	Changed	Rights	Owner
..		..		1/10/2024 9:33:36 PM	rwxr-xr-x	root
ucd_net_processes		win_services.php	5 KB	12/13/2013 2:52:51 PM	rw-r--r--	root
cacti_graph_template_udf_tcp		tcp.php	2 KB	12/13/2013 2:56:17 PM	rw-r--r--	root
cacti_graph_template_udf_win		webhits.pl	1 KB	9/5/2023 7:55:54 AM	rw-r--r--	apache
TCP&WinService.txt		weatherbug.pl	1 KB	9/5/2023 7:55:54 AM	rw-r--r--	apache
tcp.php		unix_users.pl	1 KB	1/16/2024 9:51:16 AM	rw-r--r--	apache
tcp.xml		unix_tcp_connections.pl	1 KB	9/5/2023 7:55:54 AM	rw-r--r--	apache
ucd_net_processes.zip		unix_processes.pl	1 KB	1/16/2024 9:51:16 AM	rw-r--r--	apache
win_services.php		ss_webseer.php	5 KB	1/16/2024 9:50:52 AM	rwxr-xr-x	apache
win_services.xml		ss_sql.php	3 KB	9/5/2023 7:55:55 AM	rw-r--r--	apache

Import Template

Import Template from Local File [?](#) Select a File C:\fakepath\cacti_data_query_ucdnet_-_get_monitored_processes.xml

Data Source Overrides

Data Source Profile [?](#) 5 Minute Collection

Graph/Data Template Overrides

Remove Orphaned Graph Items [?](#)

Replace Data Query Suggested Value Patterns [?](#)

Graph Template Image Format [?](#) SVG

Graph Template Height [?](#) 200

Graph Template Width [?](#) 700

Import Files [If Files are missing, locate and install before using]

File Name	Status
/usr/share/cacti/resource/snmp_queries/net-snmp_linux_processes.xml	Not Found

Import Templates [None selected imports all, Check to import selectively]

Template Type	Template Name	Status	Dependencies	Changes/Differences
Data Query	ucd/net - Get monitored processes	New	None	<input checked="" type="checkbox"/>
Graph Template	ucd/net - Process Status	New	None	<input checked="" type="checkbox"/>
Data Template	ucd/net - Process Status	New	None	<input checked="" type="checkbox"/>

Differences
Data Input Method Get SNMP Data (Indexed) Updated None Table: data_input_fields, Column: allow_nulls, New Value: on, Old Value:

GPRINT Preset Normal Unchanged None None

Import

Import Template

Import Template from Local File [?](#) Select a File C:\fakepath\cacti_data_template_ucdnet_-_process_status.xml

Data Source Overrides

Data Source Profile [?](#) 5 Minute Collection

Graph/Data Template Overrides

Remove Orphaned Graph Items [?](#)

Replace Data Query Suggested Value Patterns [?](#)

Graph Template Image Format [?](#) SVG

Graph Template Height [?](#) 200

Graph Template Width [?](#) 700

Import Templates [None selected imports all, Check to import selectively]

Template Type	Template Name	Status	Dependencies	Changes/Differences
Data Template	ucd/net - Process Status	Unchanged	None	<input type="checkbox"/>

Differences
Data Input Method Get SNMP Data (Indexed) Updated None Table: data_input_fields, Column: allow_nulls, New Value: on, Old Value:

Import

Copy `net-snmp_linux_processes.xml` to `/usr/share/cacti/resource/snmp_queries` directory

snmp_queries - Cacti_Oracle9_32.14 - WinSCP					
D:\...\resource\snmp_queries\		/usr/share/cacti/resource/snmp_queries/			
Name		Name	Size	Changed	Rights
..		..		1/10/2024 9:33:36 PM	rwxr-xr-x
<code>net-snmp_linux_processes.xml</code>		<code>host_disk.xml</code>	2 KB	9/5/2023 7:55:54 AM	rw-r--r--
		<code>index.php</code>	2 KB	9/5/2023 7:55:55 AM	rw-r--r--
		<code>net-snmp_linux_processes.xml</code>	2 KB	11/30/2023 5:20:16 PM	rw-r--r--
					root

```
# Change owner from root to apache:apache
chown apache:apache /usr/share/cacti/resource/script_server/tcp.xml
chown apache:apache /usr/share/cacti/resource/script_server/win_services.xml
chown apache:apache /usr/share/cacti/scripts/tcp.php
chown apache:apache /usr/share/cacti/scripts/win_services.php
chown apache:apache /usr/share/cacti/resource/snmp_queries/net-snmp_linux_processes.xml
```

```
# chown apache:apache /usr/share/cacti/resource/script_server/tcp.xml
# chown apache:apache /usr/share/cacti/resource/script_server/win_services.xml
# chown apache:apache /usr/share/cacti/scripts/tcp.php
# chown apache:apache /usr/share/cacti/scripts/win_services.php
# chown apache:apache /usr/share/cacti/resource/snmp_queries/net-snmp_linux_processes.xml
```

##Append linux process that required to be monitor

nano /etc/snmp/snmpd.conf

```
#### Process monitor
proc apache2 10 1
proc httpd 10 1
proc mariabd 10 1
proc nano 10 1
proc snmpd 10 1
proc sshd 10 1
proc vmtoolsd 10 1
```

```

GNU nano 5.6.1                               /etc/snmp/snmpd.conf
## <<<<<< End of config >>>>>>>

##### Process monitor
proc apache2 10 1
proc httpd 10 1
proc mariabd 10 1
proc nano 10 1
proc snmpd 10 1
proc sshd 10 1
proc vmtoolsd 10 1

```

3.7 Improve data collection performance

Configuration => Setting => Poller => Data Collector Default => increase 2 values to 16 & 20 as below.

Data Collector Defaults	
Data Collector Processes	16 <= Before is 8
Threads per Process	20 <= Before is 10

Benchmark:

1. Data collected duration improved from 22seconds to 13 seconds based on GIOS 530 monitored items.
Result is graphs are stable without any broken.
2. Methodology is increase poller threshold from default 80 to 320 (4 times).

3.8 (Optional) Install Chinese language pack

```
sudo yum install langpacks-zh_CN
```

```
[root@twtpsvhq014 ~]# yum install langpacks-zh_CN
Last metadata expiration check: 3:59:45 ago on Sun 28 Jul 2024 06:27:33 PM CST.
Dependencies resolved.
=====
Package                                     Architecture      Version
=====
Installing:
langpacks-zh_CN                           noarch          3.0-16.el9
Installing dependencies:
google-noto-cjk-fonts-common               noarch          20230817-2.el9
google-noto-sans-cjk-ttc-fonts              noarch          20230817-2.el9
langpacks-core-font-zh_CN                  noarch          3.0-16.el9
langpacks-core-zh_CN                        noarch          3.0-16.el9
Installing weak dependencies:
glibc-langpack-zh                          x86_64          2.34-83.0.1.el9_3.7
google-noto-serif-cjk-ttc-fonts             noarch          20230817-2.el9
=====
Transaction Summary
=====
Install 7 Packages

Total download size: 199 M
Installed size: 313 M
```



4 Add Cacti into Monitor

4.1 Configure SNMP

```
cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.bak

nano /etc/snmp/snmpd.conf
#####
# SNMP configuration #
#####
# Agent address
agentaddress udp:161
agentaddress udp6:161

## Access control
# sec.name source community
com2sec AllowAll 127.0.0.1 TpvTech1

#group <group_name> <security_mode> <security_name>
group AllGroup v2c AllowAll

# Define 'AllView', which includes everything under .1
# view.name incl/excl subtree.mask(Optional)
view AllView included .1

# group.name context model level prefix read write notify
access AllGroup "" any noauth exact AllView none none

## System contact information
#syslocation <location set>
#syscontact <contact_info>
syslocation Cacti.GIOS@Taipei
syscontact Double.lin@tpv-tech.com
## <<<<<<< End of config >>>>>>>
```

```

GNU nano 5.6.1                               /etc/snmp/snmpd.conf
#####
# SNMP configuration #
#####
# Agent address
agentaddress udp:161
agentaddress udp6:161

## Access control
# sec.name source community
com2sec AllowAll 127.0.0.1 TpvTech1

#group <group_name> <security_mode> <security_name>
group AllGroup v2c AllowAll

# Define 'AllView', which includes everything under .1
# view.name incl/excl subtree.mask(optional)
view AllView included .1

# group.name context model level prefix read write notify
access AllGroup "" any noauth exact AllView none none

## System contact information
#syslocation <location set>
#syscontact <contact_info>
syslocation Cacti.GIOS@Taipei
syscontact Double.lin@tpv-tech.com
## <<<<<< End of config >>>>>>
```

systemctl enable snmpd

systemctl restart snmpd

systemctl status snmpd

```

[root@TWTPSVHQ014 plugins]# systemctl enable snmpd
[root@TWTPSVHQ014 plugins]# systemctl restart snmpd
[root@TWTPSVHQ014 plugins]# systemctl status snmpd
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/usr/lib/systemd/system/snmpd.service; enabled; preset: disabled)
   Active: active (running) since Tue 2024-01-16 15:56:47 CST; 9s ago
     Main PID: 13189 (snmpd)
        Tasks: 1 (limit: 50492)
       Memory: 4.6M
          CPU: 136ms
        CGroup: /system.slice/snmpd.service
                  └─13189 /usr/sbin/snmpd -LS0-6d -f

Jan 16 15:56:47 TWTPSVHQ014.tpvaoc.com systemd[1]: Starting Simple Network Management Protocol...
Jan 16 15:56:47 TWTPSVHQ014.tpvaoc.com snmpd[13189]: NET-SNMP version 5.9.1
Jan 16 15:56:47 TWTPSVHQ014.tpvaoc.com systemd[1]: Started Simple Network Management Protocol...
```

4.2 Configure Cacti Service to monitor

##Append Linux process that required to be monitor

```

nano /etc/snmp/snmpd.conf
#### Process monitor
proc apache2 10 1
proc httpd 10 1
proc mariabd 10 1
proc nano 10 1
```

```
proc snmpd 10 1  
proc sshd 10 1  
proc vmtoolsd 10 1
```

```
GNU nano 5.6.1 /etc/snmp/snmpd.conf  
## <<<<<< End of config >>>>>>  
  
##### Process monitor  
proc apache2 10 1  
proc httpd 10 1  
proc mariabd 10 1  
proc nano 10 1  
proc snmpd 10 1  
proc sshd 10 1  
proc vmtoolsd 10 1
```

4.3 Add Cacti device

The screenshot shows the Cacti web interface for managing a device. The top navigation bar includes links for 'Create New Device', 'Create Graphs for this Device', 'Re-Index Device', 'Enable Device Debug', 'Repopulate Poller Cache', 'View Poller Cache', 'Data Source List', and 'Graph List'. The main content area is divided into two tabs: 'General Device Options' and 'Device Monitoring Settings'.

General Device Options:

- Description: Cacti_SiteName
- Hostname: 127.0.0.1
- Location: None
- Poller Association: Main Poller
- Device Site Association: Core
- Device Template: Cacti Stats
- Number of Collection Threads: 8 Threads
- Disable Device: Enabled (green switch)

Device Monitoring Settings:

- Monitor Device: Enabled (green switch)
- Device Criticality: Medium
- Ping Warning Threshold: 0
- Ping Alert Threshold: 0
- Re-Baseline Warning: Do not Change
- Re-Baseline Alert: Do not Change
- Down Device Message: (empty input field)

Device Up/Down Notification Settings					
Threshold Up/Down Email Notification ?	Global List ▾				
Host Failure Count ?	Use Cacti Setting ▾				
SNMP Options					
SNMP Version ?	Version 2 ▾				
SNMP Community String ?	TpvTech1				
SNMP Port ?	161				
SNMP Timeout ?	600				
Maximum OIDs Per Get Request ?	10 OID's ▾				
Bulk Walk Maximum Repetitions ?	5 Repetitions ▾				
Availability/Reachability Options					
Downed Device Detection ?	Ping ▾				
Ping Method ?	ICMP Ping ▾				
Ping Timeout Value ?	600				
Ping Retry Count ?	3				
Associated Graph Templates					
Graph Template Name		Status			
1) Cacti Stats - Boost Average Row Size		Is Being Graphed (Edit)			
2) Cacti Stats - Boost Memory		Is Being Graphed (Edit)			
3) Cacti Stats - Boost Records		Is Being Graphed (Edit)			
4) Cacti Stats - Boost Runtime		Is Being Graphed (Edit)			
5) Cacti Stats - Boost Table Size		Is Being Graphed (Edit)			
6) Cacti Stats - Boost Timing Detail		Is Being Graphed (Edit)			
7) Cacti Stats - Boost Updates		Is Being Graphed (Edit)			
22) Cacti Stats - User Types		Is Being Graphed (Edit)			
23) Host MIB - Logged in Users		Is Being Graphed (Edit)			
24) Host MIB - Processes		Is Being Graphed (Edit)			
25) UDF_TCP_Port		Is Being Graphed (Edit)			
Associated Data Queries					
Data Query Name	Re-Index Method				Status
1) Cacti Stats - Data Collector Stats	None	Uptime	Index Count	Verify All	Success [2 Items, 1 Rows]
2) Cacti Stats - Graph Exports	None	Uptime	Index Count	Verify All	Success [0 Items, 0 Rows]
3) Cacti Stats - WebSeer Service Checks	None	Uptime	Index Count	Verify All	Success [0 Items, 0 Rows]
4) SNMP - Get Mounted Partitions	None	Uptime	Index Count	Verify All	Success [39 Items, 13 Rows]
5) SNMP - Get Processor Information	None	Uptime	Index Count	Verify All	Success [9 Items, 9 Rows]
6) SNMP - Interface Statistics	None	Uptime	Index Count	Verify All	Success [23 Items, 2 Rows]
7) ucd/net - Get monitored processes	None	Uptime	Index Count	Verify All	Success [14 Items, 7 Rows]

5 Enable syslogs plugin

Goal: Function will receive Cacti mail notification in 1~2 minutes, since Server generate error logs

Cacti Syslog Alert '100_system Error'

Hostname	Date	Severity	Level	Message
TWTPNBJR71	2024-05-09 00:06:58	Warning	err	100 TPVAOC:giadmin-tp02 system Error event test, 11:52PM 5/8

```
#create a dedicated DB for syslog
```

```
nano /etc/my.cnf.d/server.cnf
```

```
sql_mode=NO_ENGINE_SUBSTITUTION,NO_AUTO_CREATE_USER
```

```
GNU nano 5.6.1 /etc/my.cnf.d/server.cnf
[mysqld]
sort_buffer_size = 10M
max_connections = 900
sql_mode=NO_ENGINE_SUBSTITUTION,NO_AUTO_CREATE_USER
```

```
mysql -u root -p
```

```
show global variables like 'sql_mode';
```

```
[root@TWTPSVHQ018 ~]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 5577614
Server version: 10.5.22-MariaDB MariaDB Server
Type 'help;' or '\h' for help. Type '\c' to clear the current input.
MariaDB [(none)]> show global variables like 'sql_mode';
+-----+-----+
| Variable_name | Value
+-----+-----+
| sql_mode      | STRICT_TRANS_TABLES,ERROR_FOR_DIVISION_BY_ZERO,NO
1 row in set (0.001 sec)
```

```
create database syslog;
```

```
GRANT ALL ON syslog.* TO 'cactiuser'@'localhost';
```

```
flush privileges;
```

```
exit;
```

```
MariaDB [(none)]> create database syslog;
Query OK, 1 row affected (0.000 sec)
MariaDB [(none)]> GRANT ALL ON syslog.* TO 'cactiuser'@'localhost';
Query OK, 0 rows affected (0.021 sec)
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.001 sec)
MariaDB [(none)]> exit
Bye
```

```
#Configure rsyslog by
```

```
nano /etc/rsyslog.d/cacti.conf
```

```
##cacti.conf is a new file, copy and paste below lines
```

```
$ModLoad imudp
```

```
$UDPServerRun 514
```

```
$ModLoad ommysql
```

```
$template cacti_syslog,"INSERT INTO syslog_incoming(facility_id, priority_id, program, logtime>
```

```
values (%syslogfacility%, %syslogpriority%, '%programname%', '%timegenerated:::date-mysql%',>
```

```
*.* >localhost,my_database,my_user,my_password;cacti_syslog
```

```
GNU nano 5.6.1 /etc/rsyslog.d/cacti.conf
$ModLoad imudp
$UDPServerRun 514
$ModLoad ommysql

$template cacti_syslog,"INSERT INTO syslog_incoming(facility_id,
values (%syslogfacility%, %syslogpriority%, '%programname%',

*.* >localhost,my_database,my_user,my_password;cacti_syslog
```

```
#Install rsyslog-mysql package
```

```
yum -y install rsyslog-mysql
```

```
[root@TWTPSVHQ018 ~]# yum -y install rsyslog-mysql
Last metadata expiration check: 2:45:02 ago on Mon 06 May 2024 10:44:55 AM CST.
Dependencies resolved.
=====
Package           Arch      Version       Repository      Size
=====
Installing:
  rsyslog-mysql    x86_64    8.2310.0-4.el9   ol9_appstream  20 k
Upgrading:
  rsyslog          x86_64    8.2310.0-4.el9   ol9_appstream  831 k
  rsyslog-logrotate x86_64    8.2310.0-4.el9   ol9_appstream  11 k
  selinux-policy    noarch    38.1.35-2.0.1.el9_4 ol9_baseos_latest 58 k
  selinux-policy-targeted noarch    38.1.35-2.0.1.el9_4 ol9_baseos_latest 7.8 M
Transaction Summary
=====
Install  1 Package
Upgrade  4 Packages
```

```
systemctl restart rsyslog
```

```
[root@TWTPSVHQ018 ~]# systemctl restart rsyslog
[root@TWTPSVHQ018 ~]#
```

```
#configure syslog & DB connection
```

```
cd /usr/share/cacti/plugins/syslog
```

```
cp config.php.dist config.php
```

```
nano config.php
```

```
$use_cacti_db = false;
$syslogdb_password = 'c@CtiVser';
```

```

GNU nano 5.6.1          /usr/share/cacti/plugins/syslog/config.php

/* revert if you dont use the Cacti database */
$use_cacti_db = false;

if (!$use_cacti_db) {
    $syslogdb_type      = 'mysql';
    $syslogdb_default   = 'syslog';
    $syslogdb_hostname  = 'localhost';
    $syslogdb_username  = 'cactiuser';
    $syslogdb_password  = 'c@CtiVser';
    $syslogdb_port       = 3306;

```

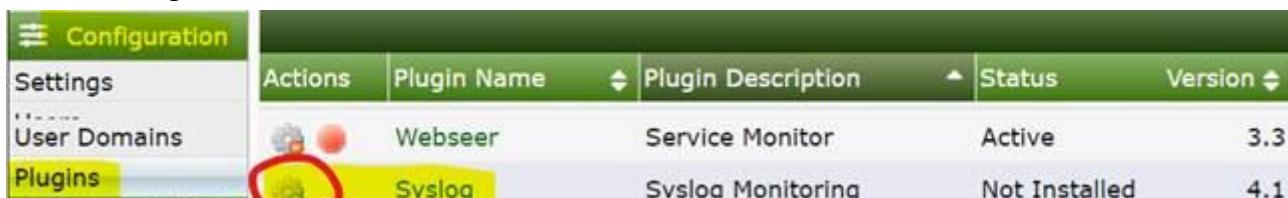
```

#Enable syslog as a service
cp /etc/rsyslog.d/cacti.conf.dist /etc/rsyslog.d/cacti.conf
cp /usr/share/cacti/plugins/syslog/config.php.dist /usr/share/cacti/plugins/syslog/config.php
cd /usr/share/cacti/plugins/syslog
cp config.php.dist /etc/rsyslog.d/cacti.conf
nano /etc/rsyslog.d/cacti.conf
rm nano /etc/rsyslog.d/cacti.conf
nano /etc/rsyslog.d/cacti.conf
yum -y install rsyslog-mysql
systemctl restart rsyslog
cp config.php.dist config.php
nano config.php

```

#Enable plug-in

Configuration => Plugins => Click red circle “Gear” to install



Actions	Plugin Name	Plugin Description	Status	Version
	Webseer	Service Monitor	Active	3.3
	Syslog	Syslog Monitoring	Not Installed	4.1

1 day for retention => Install

Syslog Install Advisor<

You have several options to choose from when installing Syslog. The first is the Database Partitioning to prevent the size of the tables from becoming excessive thus slowing query performance.

You can also set the MySQL storage engine. If you have not tuned your system for InnoDB, then you may want to change that to MyISAM.

You can also select the retention duration. Please keep in mind that if you have several large log files, it may be better to keep the size smaller.

Syslog Install Settings

Database Storage Engine ?	InnoDB Storage
Database Architecture ?	Partitioned Table
Retention Policy ?	1 Day
Partitions per Day ?	1 Per Day

Click green point to activate => change to red & status in Active.

Plugin Management			
Actions	Plugin Name	Plugin Description	Status
	Syslog	Syslog Monitoring	Active

#Enable Win Server to export logs by follow attachment.

#On win server, generate testing event logs

```
eventcreate /t error /id 100 /l system /d "system Error event test, 11:12PM 5/8"
eventcreate /t warning /id 200 /l system /d "system warning event test, 11:12PM 5/8"
eventcreate /t error /id 300 /l application /d "application Error event test, 11:12PM 5/8"
eventcreate /t warning /id 400 /l application /d "application warning event test, 11:12PM 5/8"
```

```
C:\Windows\System32>eventcreate /t error /id 100 /l system /d "system Error event test, 11:52PM 5/8"
SUCCESS: An event of type 'error' was created with 'system' as the log.
C:\Windows\System32>eventcreate /t warning /id 200 /l system /d "system warning event test, 11:52PM 5/8"
SUCCESS: An event of type 'warning' was created with 'system' as the log.
C:\Windows\System32>eventcreate /t error /id 300 /l application /d "application Error event test, 11:52PM 5/8"
SUCCESS: An event of type 'error' was created in the 'application' log with 'EventCreate' as the source.
C:\Windows\System32>eventcreate /t warning /id 400 /l application /d "application warning event test, 11:52PM 5/8"
SUCCESS: An event of type 'warning' was created in the 'application' log with 'EventCreate' as the source.
```

#Check result: Syslog => System Logs

Console	Graphs	Reporting	Logs	Monitor	Topx	Syslog	MXToolBox
Syslog							
System Logs		Alert Logs					
Syslog Message Filter [Start: '2024-05-08 00:07:08' to End: '2024-05-09 00:07:08', Unprocessed Messages: 1]							
Timespan	Custom	From	2024-05-08 00:07:08	To	2024-05-09 00:07:08	1 Day	Go
Search	Enter a regular expression	Devices	1 Devices Selected	Messages	Default	Trim	75 Chars
Program	All Programs	Facility	All Facilities	Priority	All Priorities	Record Type	All Records
All 8 Messages							
Actions	Date	Device	Program	Message			
+	2024-05-09 00:06:58	TWTPNBJR71	eventcreate	300 TPVAOC\giadmin-tp02 application Error event test, 11:52PM 5/8			
+	2024-05-09 00:06:58	TWTPNBJR71	system	200 TPVAOC\giadmin-tp02 system warning event test, 11:52PM 5/8			
+	2024-05-09 00:06:58	TWTPNBJR71	system	100 TPVAOC\giadmin-tp02 system Error event test, 11:52PM 5/8			
+	2024-05-09 00:06:58	TWTPNBJR71	eventcreate	400 TPVAOC\giadmin-tp02 application warning event test, 11:52PM 5/8			

#Create alert

Main Console	Syslog Alert Filters						
Create	Search	Enter a search term	Enabled	All	Rows	Default	
Management	All 4 Alerts						
Data Collection	Alert Name	Severity	Method	Threshold Count	Enabled	Match Type	Search String
Templates	100_system_Error	Warning	Individual	N/A	Yes	Contains	system Error event test
Automation	200_system_warning	Warning	Individual	N/A	Yes	Contains	system warning event test
Presets	300_application_Error	Warning	Individual	N/A	Yes	Contains	application Error event test
Import/Export	400_application_warning	Warning	Individual	N/A	Yes	Contains	application warning event test
Syslog Settings	All 4 Alerts						
Alert Rules							
Removal Rules							
Report Rules							

#Check alerts mail

All Unread By Date Newest ↓

Cacti.GIOS Event Alert - 100_system_Error 12:07 AM Cacti Syslog Alert '100_system'

Cacti.GIOS Event Alert - 200_system_warning 12:07 AM Cacti Syslog Alert '200_system'

Cacti.GIOS Event Alert - 400_application_warn... 12:07 AM

Cacti.GIOS <cacti.gios@tpv-tech.com> Double Lin 林林弘

Event Alert - 100_system_Error

Cacti Syslog Alert '100_system_Error'

Hostname	Date	Severity	Level	Message
TWTPNBJR71	2024-05-09 00:06:58	Warning	err	100 TPVAOC\giadmin-tp02 system Error event test, 11:52PM 5/8

#On Cacti, use tcpdump to check if received event logs from Win Svr.

tcpdump -i ens192 host 172.17.36.19 and port 514

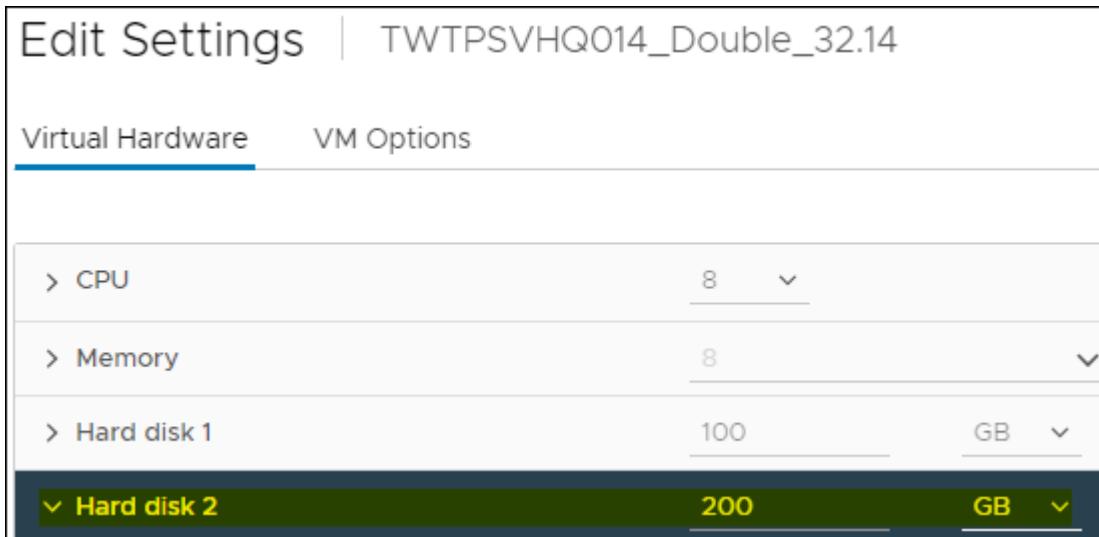
```
[root@TWTPSVHQ018 ~]# tcpdump -i ens192 host 172.17.36.19 and port 514
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens192, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:04:19.310678 IP SGTANB277.tpvaoc.com.61500 > TWTPSVHQ018.syslog: SYSLOG daemon.error, length: 107
23:04:19.310712 IP SGTANB277.tpvaoc.com.61500 > TWTPSVHQ018.syslog: SYSLOG daemon.warning, length: 111
23:04:19.310716 IP SGTANB277.tpvaoc.com.61500 > TWTPSVHQ018.syslog: SYSLOG local7.error, length: 118
23:04:19.310877 IP SGTANB277.tpvaoc.com.61500 > TWTPSVHQ018.syslog: SYSLOG local7.warning, length: 122
23:07:11.678786 IP SGTANB277.tpvaoc.com.61500 > TWTPSVHQ018.syslog: SYSLOG local7.warning, length: 444
```

6 Enable flowview plugin

Goal: Function will receive Cacti mail notification in 1~2 minutes, since Server generate error logs

6.1 Create a dedicated disk partition 200GB for flowview DB

#on vCenter, add a new 200GB partition to Cacti VM



#list current disk partition

lsblk

#sdb is new disk name & size is 200G

NAME	MAJ:MIN	RM	SIZE	RO	TYPE	MOUNTPOINTS
sda	8:0	0	100G	0	disk	
└─sda1	8:1	0	1G	0	part	/boot
└─sda2	8:2	0	99G	0	part	
└─ol_twtpsvhq014-root	252:0	0	66.5G	0	lvm	/
└─ol_twtpsvhq014-home	252:1	0	32.5G	0	lvm	/home
sdb	8:16	0	200G	0	disk	
sr0	11:0	1	1024M	0	rom	

#Create new partition with name "flowview" on new disk-sdb

fdisk /dev/sdb

```
[root@twtpsvhq014 ~]# fdisk /dev/sdb

Welcome to fdisk (util-linux 2.37.4).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0x1ef5fd41.
```

Type n => create a new partition
 Type p => create a primary partition
 Type 1 => 1st partition number
 Type Enter twice => to use default value of beginning and end sector number
 Type w => save settings.

```
Command (m for help): n
Partition type
  p  primary (0 primary, 0 extended, 4 free)
  e  extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-419430399, default 2048):Enter
Last sector, +/-sectors or +/-size{K,M,G,T,P} (2048-419430399, default 419430399):Enter

Created a new partition 1 of type 'Linux' and of size 200 GiB.

Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.
```

mkfs.xfs /dev/sdb1

```
[root@twtpsvhq014 ~]# mkfs.xfs /dev/sdb1
meta-data=/dev/sdb1              isize=512    agcount=4, agsize=13107136 blks
                                =          sectsz=512   attr=2, projid32bit=1
                                =          crc=1      finobt=1, sparse=1, rmapbt=0
                                =          reflink=1 bigtime=1 inobtcount=1 nnext64=0
data     =               bsize=4096   blocks=52428544, imaxpct=25
        =          sunit=0      swidth=0 blks
naming   =version 2             bsize=4096   ascii-ci=0, ftype=1
log      =internal log          bsize=4096   blocks=25599, version=2
        =          sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                 extsz=4096   blocks=0, rtextents=0
Discarding blocks...Done.
```

#create a mount point “flowview” for sdb1

```
mkdir /flowview
mount /dev/sdb1 /flowview
```

```
[root@twtpsvhq014 ~]# mkdir /mnt/flowview
[root@twtpsvhq014 ~]# mount /dev/sdb1 /mnt/flowview
```

#verify new partition created and mounted

lsblk -f

NAME	FSTYPE	FSVER	LABEL	UUID	FSAVAIL	FSUSE%	MOUNTPOINTS
sda							
└─sda1	xfs			8882e73a-aaf5-48ce-a5ae-782eae871c42	713.3M	26%	/boot
└─sda2	LVM2_member	LVM2 001		9ekFty-fXEq-o0ey-T6Je-oCPC-Gbl2-yI4ea1			
└─ol_twtpsvhq014-root	xfs			5a1215a8-e143-4e81-853c-3f51413515ba	62.5G	6%	/
└─ol_twtpsvhq014-home	xfs			30744b32-5f1f-4485-bae4-f749a81832c2	32.2G	1%	/home
sdb							
└─sdb1	xfs			fb93812f-9845-4296-92fa-9e445a19ac9f	198.5G	1%	/flowview
sr0							

copy flowview's UUID: fb93812f-9845-4296-92fa-9e445a19ac9f

```
#Auto mount flowview partition during server booting, adding new 1 line as below
```

```
nano /etc/fstab
```

```
UUID=fb93812f-9845-4296-92fa-9e445a19ac9f /flowview xfs defaults 0 0
```

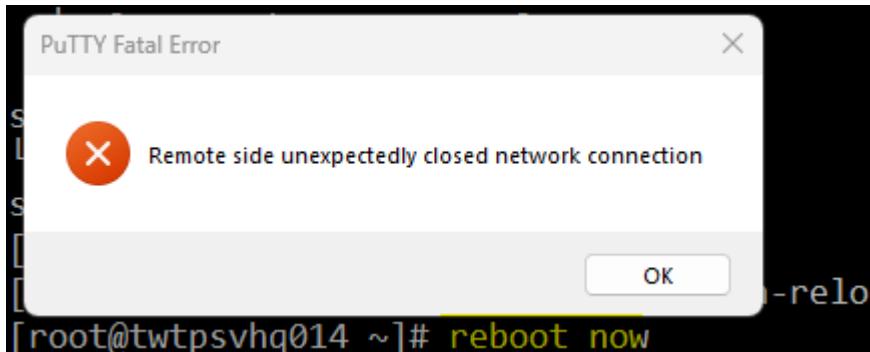
```
GNU nano 5.6.1 /etc/fstab

#
# /etc/fstab
# Created by anaconda on Mon Jan  8 16:40:20 2024
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
/dev/mapper/ol_twtpsvhq014-root / xfs defaults 0 0
UUID=8882e73a-aaf5-48ce-a5ae-782eae871c42 /boot xfs defaults 0 0
/dev/mapper/ol_twtpsvhq014-home /home xfs defaults 0 0
UUID=fb93812f-9845-4296-92fa-9e445a19ac9f /flowview xfs defaults 0 0
```

```
systemctl daemon-reload
```

```
[root@twtpsvhq014 ~]# systemctl daemon-reload
```

```
reboot now
```



```
#verify flowview mounted successful.
```

```
lsblk -f
```

NAME	FSTYPE	FSVER	LABEL	UUID	FSAVAIL	FSUSE%	MOUNTPOINTS
sda							
└─sda1	xfs			8882e73a-aaf5-48ce-a5ae-782eae871c42	713.3M	26%	/boot
└─sda2	LVM2_member	LVM2 001		9ekFty-fXEq-o0ey-T6Je-oCPc-Gbl2-yI4ea1	62.5G	6%	/
└─ol_twtpsvhq014-root	xfs			5a1215a8-e143-4e81-853c-3f51413515ba	32.2G	1%	/home
└─sdb				30744b32-5f1f-4485-bae4-f749a81832c2			
└─sdb1	xfs			fb93812f-9845-4296-92fa-9e445a19ac9f	198.5G	1%	/flowview
sr0							

6.2 Create a dedicated DB for flowview

```
mysql -uroot
```

```
create database flowview;
```

```
GRANT ALL ON flowview.* TO 'cactiuser'@'localhost';
```

```
flush privileges;
```

```
exit;
```

```

MariaDB [(none)]> create database flowview;
Query OK, 1 row affected (0.002 sec)

MariaDB [(none)]>
MariaDB [(none)]> GRANT ALL ON flowview.* TO 'cactiuser'@'localhost';
Query OK, 0 rows affected (0.017 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.003 sec)

```

verify DB is NO table

mysqlshow -uroot flowview

```

[root@TWTPSVHQ015 ~]# mysqlshow -uroot flowview
Database: flowview
+-----+
| Tables |
+-----+

```

#verify flowview db folder created

ls -lh /var/lib/mysql/flowview/

```

[root@twtpsvhq014 ~]# ls -lh /var/lib/mysql/flowview/
total 4.0K
-rw-rw----. 1 mysql mysql 67 Aug 12 13:18 db.opt

```

#move flowview folders to new partition-flowview

systemctl stop httpd

systemctl stop mariadb

mv /var/lib/mysql/flowview /flowview/

ln -s /flowview/flowview /var/lib/mysql/flowview

systemctl start mariadb

systemctl start httpd

```

[root@twtpsvhq014 ~]# systemctl stop mariadb
[root@twtpsvhq014 ~]# mv /var/lib/mysql/flowview /flowview/
[root@twtpsvhq014 ~]# sudo ln -s /flowview/flowview /var/lib/mysql/flowview
[root@twtpsvhq014 ~]# systemctl start mariadb

```

#verify symbol link created

ls -lh /flowview/

ls -lh /var/lib/mysql/flowview/

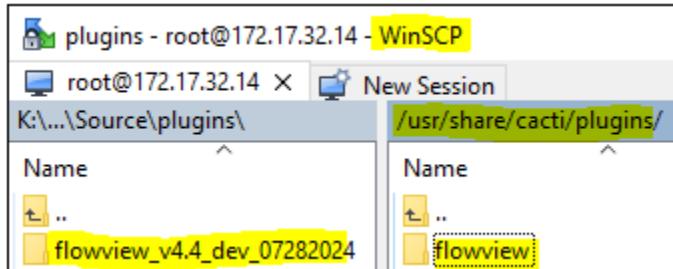
```

[root@twtpsvhq014 ~]# ls -lh /flowview/
total 0
drwx-----. 2 mysql mysql 20 Aug 12 13:18 flowview
[root@twtpsvhq014 ~]# ls -lh /var/lib/mysql/flowview/
total 4.0K
-rw-rw----. 1 mysql mysql 67 Aug 12 13:18 db.opt

```

6.3 Flowview install & configure

WinSCP Flowview develop version v4.4_07282024 & rename



```
cd /usr/share/cacti/plugins/flowview/
cp config.php.dist config.php
nano config.php
    change from truth  to false
    use same credential with cacti (change PW)
```

```
GNU nano 5.6.1                                     config.php
/* revert if you dont use the Cacti database */
$flowview_use_cacti_db = false;

if (!$flowview_use_cacti_db) {
    $flowviewdb_type      = 'mysql';
    $flowviewdb_default   = 'flowview';
    $flowviewdb_hostname  = 'localhost';
    $flowviewdb_username  = 'cactiuser';
    $flowviewdb_password  = 'c@Ct1Vser';
```

```
cp ./service/flow-capture.service /etc/systemd/system
#Modify flowview service 3 paths to /usr/share/.....
nano /etc/systemd/system/flow-capture.service
```

```
GNU nano 5.6.1                                     /etc/systemd/system/flow-capture.service          Modified
Description=Flow Capture Service for Cacti
After=network.target mariadb.service

[Service]
User=apache
Group=apache
TimeoutStartSec=0
Type=simple
KillMode=process
WorkingDirectory=/tmp
ExecStart=/usr/bin/php -q /usr/share/cacti/plugins/flowview/service/flow-capture --systemd
ExecStop=/usr/bin/php -q /usr/share/cacti/plugins/flowview/service/flow-capture stop
ExecReload=/usr/bin/php -q /usr/share/cacti/plugins/flowview/service/flow-capture reload
Restart=always
RestartSec=2
```

#On Cacti console, Install flowview plugin

Plugin Management				
Search	Enter a search term		Status	All
All 11 Plugins				
Actions	Plugin Name	Plugin Description	Status	
	Monitor	Device Monitoring	Active	
	Flowview	FlowView	Installed	

#//verify tables created

mysqlshow -uroot flowview

```
[root@TWTPSVHQ015 flowview]# mysqlshow -uroot flowview
Database: flowview
+-----+-----+
|       Tables      |
+-----+
| parallel_database_query
| parallel_database_query_shard
| parallel_database_query_shard_cache
| plugin_flowview_arin_information
| plugin_flowview_device_streams
| plugin_flowview_device_templates
| plugin_flowview_devices
| plugin_flowview_dnscache
| plugin_flowview_irr_as_block
| plugin_flowview_irr_as_set
| plugin_flowview_irr_aut_num
| plugin_flowview_irr_domain
| plugin_flowview_irr_filter_set
| plugin_flowview_irr_inet_rtr
| plugin_flowview_irr_inetnum
| plugin_flowview_irr_irt
| plugin_flowview_irr_mntner
| plugin_flowview_irr_organisation
| plugin_flowview_irr_peering_set
| plugin_flowview_irr_person
| plugin_flowview_irr_poem
| plugin_flowview_irr_poetic_form
| plugin_flowview_irr_role
| plugin_flowview_irr_route
| plugin_flowview_irr_route_set
| plugin_flowview_irr_rtr_set
| plugin_flowview_ports
| plugin_flowview_queries
| plugin_flowview_schedules
+-----+
```

```
systemctl start flow-capture
```

```
systemctl enable flow-capture
```

```
systemctl status flow-capture
```

```
[root@TWTPSVHQ015 flowview]# systemctl enable flow-capture
Created symlink /etc/systemd/system/multi-user.target.wants/flow-capture.service → /etc/systemd/system/flow-capture.service.
```

```

● flow-capture.service - Flow Capture Service for Cacti
   Loaded: loaded (/etc/systemd/system/flow-capture.service; enabled; preset: disabled)
   Active: active (running) since Mon 2024-07-22 11:06:20 CST; 19s ago
     Main PID: 10145 (php)
        Tasks: 1 (limit: 50492)
       Memory: 16.8M
          CPU: 282ms
        CGroup: /system.slice/flow-capture.service
                   └─10145 /usr/bin/php -q /usr/share/cacti/plugins/flowview/service/flow-capture --systemd

Jul 22 11:06:20 TWTPSVHQ015.tpvaoc.com systemd[1]: Started Flow Capture Service for Cacti.
Jul 22 11:06:20 TWTPSVHQ015.tpvaoc.com php[10145]: NOTE: Starting Flow Collection
Jul 22 11:06:20 TWTPSVHQ015.tpvaoc.com php[10145]: NOTE: No Flow Capture Listeners configured

```

Reduce data retention to **1 week** (default is 1 month) & **16 Threads** (default is 4) on flowview Web Console, and below yellow marked.

Main Console	Mail/Reporting/DNS	Alerting/Thold	Monitor	Reports	Misc	Syslog	Flowview
Create	Cacti Settings (Flowview)						
Management	Name Resolution						
Data Collection	Hostname Resolution ?						
Templates	Use Local Server ▾						
Automation	Local Domain Name ? mydomain.net						
Presets	Local IP Range ? 172.16.0.0/16						
Import/Export	Use Arin to find Domains and AS Numbers ?						
FlowView	Whois Provider Host ? whois.radb.net						
Syslog Settings	Whois Binary Path ? /usr/bin/whois						
Configuration	Graph Drilldown Settings						
Settings	Default Search Filter for Graph Drilldowns ? ▾						
Users	Data Retention and Report Generation						
User Groups	Format File to Use ? Standard Formating (default.)						
User Domains	Data Retention Policy ? 1 Week ▾						
Plugins	Database Partitioning Scheme ? Hourly ▾						
Utilities	Storage Engine for Raw Tables ? Aria (Fast, Crash Safe) ▾						
Troubleshooting	Parallel Queries						
	Max Concurrent Threads ? 16 Threads ▾						
	Maximum Run Time ? 5 Minutes ▾						
	Cached Data Time to Live ? 6 Hours ▾						
	MaxScale Sharding ?						
	Leverage MaxScale to Distribute Query Shards ?						
	MaxScale Read-Write Split Port ? 3307						

Active flowview plugin

Actions	Plugin Name	Plugin Description	Status
	Monitor	Device Monitoring	Active
	Flowview	FlowView	Active

#Check logs & Solve error logs

Error: CMDPHP ERROR: A DB Row Failed!, Error: Table 'flowview.reports_que'

#CREATE TABLE `reports_queued`

mysql -uroot flowview -e "

```
CREATE TABLE IF NOT EXISTS `reports_queued` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `name` varchar(64) NOT NULL DEFAULT '',
  `source` varchar(20) NOT NULL DEFAULT '',
  `source_id` int(10) unsigned NOT NULL DEFAULT 0,
  `status` varchar(10) NOT NULL DEFAULT 'pending',
  `scheduled_time` timestamp NOT NULL DEFAULT '0000-00-00',
  `start_time` timestamp NOT NULL DEFAULT '0000-00-00',
  `run_command` varchar(512) NOT NULL DEFAULT '',
  `run_timeout` int(10) NOT NULL DEFAULT '60',
  `notification` blob NOT NULL,
  `request_type` int(10) unsigned NOT NULL DEFAULT 0,
  `requested_by` varchar(20) NOT NULL DEFAULT '',
  `requested_id` int(11) NOT NULL DEFAULT -1,
  PRIMARY KEY (`id`),
  KEY `source` (`source`),
  KEY `source_id` (`source_id`)
) ENGINE=InnoDB
ROW_FORMAT=DYNAMIC
COMMENT='Holds Scheduled Reports';
"
```

CMDPHP ERROR: A DB Row Failed!, Error: Table 'flowview.reports_log' doesn't exist

mysql -uroot flowview -e "

```
CREATE TABLE IF NOT EXISTS `reports_log` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `name` varchar(64) NOT NULL DEFAULT '',
  `source` varchar(20) NOT NULL DEFAULT '',
  `source_id` int(10) unsigned NOT NULL DEFAULT 0,
  `report_output_type` varchar(5) NOT NULL DEFAULT '',
  `report_raw_data` longblob,
  `report_raw_output` longblob,
  `report_txt_output` longblob,
  `report_html_output` longblob,
  `notification` blob NOT NULL,
  `send_type` int(10) unsigned NOT NULL DEFAULT 0,
```

```

`send_time` timestamp NOT NULL DEFAULT current_timestamp(),
`run_time` double NOT NULL DEFAULT 0,
`sent_by` varchar(20) NOT NULL DEFAULT '',
`sent_id` int(11) NOT NULL DEFAULT -1,
PRIMARY KEY (`id`),
KEY `source` (`source`),
KEY `source_id` (`source_id`)
) ENGINE=InnoDB
COMMENT='Holds All Cacti Report Output';
"
```

DBCALL ERROR: SQL Save on table 'reports_queued': Column 'request_type' does not exist, unable to save!

#Check columes's name of this table.

```
mysql -uroot -e "SHOW COLUMNS FROM flowview.reports_queued;"
```

Field	Type	Null	Key	Default	Extra
id	int(10) unsigned	NO	PRI	NULL	auto_increment
name	varchar(64)	NO			
source	varchar(20)	NO	MUL		
source_id	int(10) unsigned	NO	MUL	0	
status	varchar(10)	NO		pending	
scheduled_time	timestamp	NO		0000-00-00 00:00:00	
start_time	timestamp	NO		0000-00-00 00:00:00	
run_command	varchar(512)	NO			
run_timeout	int(10)	NO		60	
notification	blob	NO		NULL	
requeste_type	int(10) unsigned	NO		0	
requested_by	varchar(20)	NO			
requested_id	int(11)	NO		-1	

Result is filename is incorrect, “e” is typo.

#On table “reports_queued”, replace column’s name from “requeste_type” to “request_type”

```
mysql -uroot flowview -e "ALTER TABLE flowview.reports_queued CHANGE COLUMN requeste_type request_type
int(10) unsigned NOT NULL DEFAULT 0;"
```

Field	Type	Null	Key	Default	Extra
id	int(10) unsigned	NO	PRI	NULL	auto_increment
name	varchar(64)	NO			
source	varchar(20)	NO	MUL		
source_id	int(10) unsigned	NO	MUL	0	
status	varchar(10)	NO		pending	
scheduled_time	timestamp	NO		0000-00-00 00:00:00	
start_time	timestamp	NO		0000-00-00 00:00:00	
run_command	varchar(512)	NO			
run_timeout	int(10)	NO		60	
notification	blob	NO		NULL	
request_type	int(10) unsigned	NO		0	
requested_by	varchar(20)	NO			
requested_id	int(11)	NO		-1	

6.4 Configure flowview generator simulator

Download and Configure NetFlow Generator to create test flow source traffic on UDP port 9099, version 9

NetFlow Generator

NetFlow Generator free tool

Configuration

Orion server

IP address or hostname: 172.17.32.14 <=Cacti IP

Port: 9099 <=Listen port

Node simulation

IP addresses:

Single or CIDR Range

IP address or CIDR: 172.16.15.99 <=Desktop IP which run this flow generator

SNMP interfaces

Number of interfaces: 8

Traffic level

Average flows per second: 10 <=Reduce to 10 to lower traffic.(default is 100)

Flow settings

Flow type

NetFlow V9 <= Select v5,v9, IPFIX types.

NetFlow V5

NetFlow V9

SFlow V5

IPFIX

Endpoints Simulate Source & Destination IP segment. [+ Add endpoints](#)

Source	Src. ports	Destination	Dest. ports	Protocol	⋮
192.168.99.1/32	9099	192.168.99.2/32	443	TCP	⋮

Run generator

Start generating flow v9 traffics...

Running status

Statistics

packets sent	bytes sent	flow records sent	packets per second
7,890	45.15 MB	15,780	5.00

Orion server 172.17.32.14:9099

Node simulation Enabled

Simulated nodes 172.16.15.99

Average flows per second 10

SNMP interfaces 8

Flow type NetFlow V9

Sampling rate 1:1

NBAR 2 Disabled

Source endpoints	Source ports	Destination endpoints	Destination ports	Protocol
192.168.99.1/32	9099	192.168.99.2/32	443	TCP

Stop generator

6.5 Configure listeners

Configure folwview generator to create test flow traffic on UDP port 9995 (v5), 9996(v9, 9997(IPFIX)

Main Console

Create

Management

Data Collection

Templates

Automation

Presets

Import/Export

FlowView

Listeners

Filters

Schedules

Databases

General Templates

Listener [edit: zz_Simulate_9099]

Listener Name ? zz_Simulate_9099

Allowed Host Range ? 172.16.15.99

Port ? 9099

Protocol ? UDP Protocol

Enabled ? AUTO start this new listener

Inbound Streams and Status Verify status is UP. Version, Last Updated

Name	Address	Status	Version	Templates	Last Updated
Stream [172.16.15.99]	172.16.15.99	Up	v9	1	2024-09-30 17:24:06

systemctl status flow-capture

```
● flow-capture.service - Flow Capture Service for Cacti
   Loaded: loaded (/etc/systemd/system/flow-capture.service; enabled; preset: disabled)
   Active: active (running) since Mon 2024-09-30 17:10:10 CST; 24min ago
     Main PID: 2499 (php)
       Tasks: 2 (limit: 153762)
      Memory: 40.5M
        CPU: 13.356s
       CGroup: /system.slice/flow-capture.service
           └─2499 /usr/bin/php -q /usr/share/cacti/plugins/flowview/service/flow-capture --systemd
              ├─2501 /usr/bin/php -q /usr/share/cacti/plugins/flowview/flow_collector.php --listener-id=1

Sep 30 17:10:10 twtpsvhq014.tpvaoc.com systemd[1]: Started Flow Capture Service for Cacti.
Sep 30 17:10:11 twtpsvhq014.tpvaoc.com php[2499]: NOTE: Starting Flow Collection
Sep 30 17:10:11 twtpsvhq014.tpvaoc.com php[2499]: NOTE: Launching cacti-flow-capture as '/usr/share/cacti/plugins/flowview/flow_collector.php --listener-id=1'
Sep 30 17:15:11 twtpsvhq014.tpvaoc.com php[2499]: NOTE: Checking for new or gone listeners
Sep 30 17:20:11 twtpsvhq014.tpvaoc.com php[2499]: NOTE: Checking for new or gone listeners
Sep 30 17:25:11 twtpsvhq014.tpvaoc.com php[2499]: NOTE: Checking for new or gone listeners
Sep 30 17:30:11 twtpsvhq014.tpvaoc.com php[2499]: NOTE: Checking for new or gone listeners
```

6.6 Configure filters

Create filters map to listeners, “Stream Address” IP & Max. Row “Top 15” must be assigned to increase stability.

Result of 4 filters

Filter Name	Listener	Report Type	ID	Sort Field	Resolution
zz_Simulate_9099	zz_Simulate_9099	Source/Destination IP	1	Bytes	Y
All 1 Filters					

Click “FlowView” => Select Filter & Listener => Click “GO” => Click “Table”

Source DNS	Dest DNS	Source IP	Dest IP	Flows	Bytes	Packets	Bytes/Packet
ip-192-168-99-1.private.net	ip-192-168-99-2.private.net	192.168.99.1	192.168.99.2	1,418	4,254,000	14,180	300

a. Show flowview DB table size & row number

#Show flowview DB table size & row number

```
mysql -uroot -e "SELECT t.table_name AS `Table`, ROUND(((t.data_length + t.index_length) / 1024 / 1024), 2) AS `Size (MB)`, t.table_rows AS `Rows` FROM information_schema.tables t WHERE t.table_schema = 'flowview' ORDER BY (t.data_length + t.index_length) DESC;"
```

Table	Size (MB)	Rows
plugin_flowview_irr_inetnum	6468.88	6076708
plugin_flowview_irr_route	1099.82	4165912
plugin_flowview_raw_202421511	675.35	2458674
plugin_flowview_raw_202421510	669.52	2433973
plugin_flowview_raw_202421500	669.21	2435004
plugin_flowview_raw_202421509	666.79	2422586
plugin_flowview_raw_202421508	666.03	2419226
plugin_flowview_raw_202421507	662.62	2404484
plugin_flowview_raw_202421505	661.58	2400437
plugin_flowview_raw_202421504	661.52	2400879
plugin_flowview_raw_202421506	661.32	2399050
plugin_flowview_raw_202421501	660.09	2398581
plugin_flowview_raw_202421502	657.93	2389060
plugin_flowview_raw_202421503	655.13	2378987
plugin_flowview_raw_202421423	515.02	1878653
plugin_flowview_irr_domain	485.66	1183215
plugin_flowview_irr_role	68.68	146182

6.7 Configure listeners

Configure folwview generator to create test flow traffic on UDP port 9099 (v9)

`systemctl status flow-capture`

```
● flow-capture.service - Flow Capture Service for Cacti
   Loaded: loaded (/etc/systemd/system/flow-capture.service; enabled; preset: disabled)
   Active: active (running) since Mon 2024-09-30 17:10:10 CST; 24min ago
     Main PID: 2499 (php)
        Tasks: 2 (limit: 15376)
       Memory: 40.5M
          CPU: 13.356s
         CGroup: /system.slice/flow-capture.service
             └─2499 /usr/bin/php -q /usr/share/cacti/plugins/flowview/service/flow-capture --systemd
                  ├─2501 /usr/bin/php -q /usr/share/cacti/plugins/flowview/flow_collector.php --listener-id=1

Sep 30 17:10:10 twtppsvhq014.tpvaoc.com systemd[1]: Started Flow Capture Service for Cacti.
Sep 30 17:10:11 twtppsvhq014.tpvaoc.com php[2499]: NOTE: Starting Flow Collection
Sep 30 17:10:11 twtppsvhq014.tpvaoc.com php[2499]: NOTE: Launching cacti-flow-capture as '/usr/share/cacti/plugins/flowview/flow_collector.php --listener-id=1'
Sep 30 17:15:11 twtppsvhq014.tpvaoc.com php[2499]: NOTE: Checking for new or gone listeners
Sep 30 17:20:11 twtppsvhq014.tpvaoc.com php[2499]: NOTE: Checking for new or gone listeners
Sep 30 17:25:11 twtppsvhq014.tpvaoc.com php[2499]: NOTE: Checking for new or gone listeners
Sep 30 17:30:11 twtppsvhq014.tpvaoc.com php[2499]: NOTE: Checking for new or gone listeners
```

6.8 Configure filters

Create filters map to listeners, “Stream Address” IP & Max. Row “Top 15” must be assigned to increase stability.

Result

Filter Name	Listener	Report Type	ID	Sort Field	Resolution
zz_Simulate_9099	zz_Simulate_9099	Source/Destination IP	1	Bytes	Y

All 1 Filters

6.9 Statistical Report

Click "FlowView" => Select Filter & Listener => Click "GO" => Click "Table"

Source DNS	Dest DNS	Source IP	Dest IP	Flows	Bytes	Packets	Bytes/Packet
ip-192-168-99-1.private.net	ip-192-168-99-2.private.net	192.168.99.1	192.168.99.2	1,418	4,254,000	14,180	300

6.10 Check DB size & Row numbers

#Show flowview DB table size & row number

```
mysql -uroot -e "SELECT t.table_name AS `Table`, ROUND(((t.data_length + t.index_length) / 1024 / 1024), 2) AS `Size (MB)`, t.table_rows AS `Rows` FROM information_schema.tables t WHERE t.table_schema = 'flowview' ORDER BY (t.data_length + t.index_length) DESC;"
```

Table	Size (MB)	Rows
plugin_flowview_irr_inetnum	6468.88	6076708
plugin_flowview_irr_route	1099.82	4165912
plugin_flowview_raw_202421511	675.35	2458674
plugin_flowview_raw_202421510	669.52	2433973
plugin_flowview_raw_202421500	669.21	2435004
plugin_flowview_raw_202421509	666.79	2422586
plugin_flowview_raw_202421508	666.03	2419226
plugin_flowview_raw_202421507	662.62	2404484
plugin_flowview_raw_202421505	661.58	2400437
plugin_flowview_raw_202421504	661.52	2400879
plugin_flowview_raw_202421506	661.32	2399050
plugin_flowview_raw_202421501	660.09	2398581
plugin_flowview_raw_202421502	657.93	2389060
plugin_flowview_raw_202421503	655.13	2378987
plugin_flowview_raw_202421423	515.02	1878653
plugin_flowview_irr_domain	485.66	1183215
plugin_flowview_irr_role	68.68	146182

6.11 Sample flow export configuration on Cisco SW & Fortigate

Cisco Switch:

```

flow record TPV-Flow-Record
match ipv4 destination address
match ipv4 source address
match transport source-port
match transport destination-port
match ipv4 protocol
match interface input
match ipv4 tos
match flow direction
collect counter bytes long
collect counter packets long
collect transport tcp flags
collect timestamp absolute first
collect timestamp absolute last
collect interface output
!
!
flow record TPV-Flow-Record-OUT

```

```
match ipv4 destination address
match ipv4 source address
match transport source-port
match transport destination-port
match ipv4 protocol
match interface output
match ipv4 tos
match flow direction
collect counter bytes long
collect counter packets long
collect transport tcp flags
collect timestamp absolute first
collect timestamp absolute last
collect interface input
!
!
flow exporter FNExp
destination 172.17.32.16
source Vlan99
transport udp 2055
!
!
flow exporter test
destination 172.17.32.14
source Vlan99
transport udp 2055
!
!
flow monitor FlowMonitor1
exporter FNExp
exporter test
record TPV-Flow-Record
!
!
flow monitor FlowMonitorOUT
exporter FNExp
exporter test
record TPV-Flow-Record-OUT
!
!
sampler sampler1
description sample at 50%
mode random 1 out-of 2
!
!
interface GigabitEthernet1/1/2
```

```
switchport trunk allowed vlan 99
switchport mode trunk
ip flow monitor FlowMonitor1 sampler sampler1 input
ip flow monitor FlowMonitorOUT sampler sampler1 output
channel-group 2 mode active
```

```
interface GigabitEthernet2/1/2
switchport trunk allowed vlan 99
switchport mode trunk
ip flow monitor FlowMonitor1 sampler sampler1 input
ip flow monitor FlowMonitorOUT sampler sampler1 output
channel-group 2 mode active
```

Fortigate Firewall:

```
FG3H1E5819903613 (global) # show system netflow
config system netflow
    set collector-ip 172.17.32.14
    set collector-port 9005
    set source-ip 172.17.32.100
    set active-flow-timeout 60
    set inactive-flow-timeout 10
end
```

```
FG3H1E5819903613 (global) # show system interface "port3"
config system interface
    edit "port3"
        set vdom "root"
        set ip 172.17.32.100 255.255.255.0
        set allowaccess ping https snmp
        set type physical
        set netflow-sampler both
        set sflow-sampler enable
        set sample-rate 50
        set explicit-web-proxy enable
        set description "LAN"
        set alias "lan"
        set device-identification enable
        set role lan
        set snmp-index 5
    next
end
```