Check\_MK Handbook

Table of Contents

[1. Login to Check\_MK (Arcus HMGR v2) 3](#_Toc496538898)

[2. Adding Active Check Host 5](#_Toc496538899)

[2.1. Installing XINETD Service 5](#_Toc496538900)

[Centos / RedHat / Amazon Linux: 5](#_Toc496538901)

[Ubuntu Linux: 5](#_Toc496538902)

[SUSE Linux: 5](#_Toc496538903)

[Windows: 5](#_Toc496538904)

[2.2. Installing Check\_MK Agent 6](#_Toc496538905)

[Centos / RedHat / Amazon Linux: 6](#_Toc496538906)

[Ubuntu Linux: 6](#_Toc496538907)

[SUSE Linux: 6](#_Toc496538908)

[Windows: 6](#_Toc496538909)

[2.3. Adding Security Group Entry 7](#_Toc496538910)

[3. Adding Rules in Check\_MK 7](#_Toc496538911)

[3.1. Adding Hosts in Check\_MK 7](#_Toc496538912)

[Host Naming Convention 7](#_Toc496538913)

[3.2. Adding Host to Host Group in Check\_MK 11](#_Toc496538914)

[3.3. Adding Website Monitoring in Check\_MK 14](#_Toc496538915)

[Normal Website Monitoring (HTTP) 16](#_Toc496538916)

[Secure Website Monitoring (HTTPS) 18](#_Toc496538917)

[Custom Port Website Monitoring 18](#_Toc496538918)

[Custom Path Website Monitoring 19](#_Toc496538919)

[Web Content Monitoring 19](#_Toc496538920)

[3.4. Adding Contact Group in Check\_MK 20](#_Toc496538921)

3.5. Crating Notification Settings………………………………………………………………………………………………………………………21

[4. Adding Passive Check Host 22](#_Toc496538922)

[4.1. Adding Passive Check Hosts in Check\_MK Console 24](#_Toc496538923)

[4.2. Adding Security Group for Check\_MK Passive Checks 28](#_Toc496538924)

[5. Adding Cloud Watch Metrics 30](#_Toc496538925)

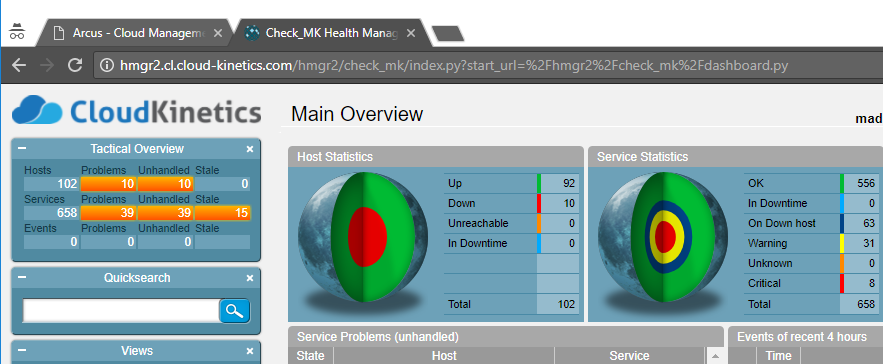
[6. Appendix 33](#_Toc496538926)

# Login to Check\_MK

URL: <http://13.127.51.135/checkmk/check_mk/>

Username: cmkadmin

Password: cmkadmin



# Adding Active Check Host

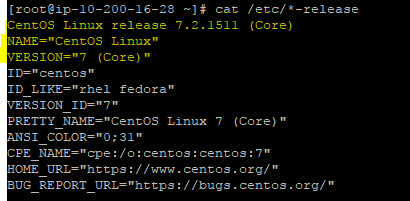
Active check hosts are the one where Check\_MK server will contact Check\_MK agents and get the data. Normally servers with Public IP is configured for Active Checks.

## Installing XINETD Service

xinetd service is used by Check\_MK agent to communicate to the Check\_MK server, to install xinetd service, and make sure the service is started, and enabled at boot. Verify the status of the service for confirmation.

Check what is the distribution of Linux and proceed with below.

Command: **cat /etc/\*-release**



### Centos / RedHat / Amazon Linux:

yum install xinetd

chkconfig xinetd on

service xinetd start

service xinetd status

### Ubuntu Linux:

apt-get install xinetd

service xinetd start

update-rc.d xinetd defaults

update-rc.d xinetd enable

service xinetd status

http://13.127.51.135/checkmk/check\_mk/agents/check-mk-agent\_1.4.0p12-1\_all.deb

### SUSE Linux:

zypper install xinetd

chkconfig xinetd on

service xinetd start

service xinetd status

### Windows:

Not Applicable (Windows doesn’t use XINETD service for Communication)

## Installing Check\_MK Agent

To install Check\_MK Agent, we download the agent package from the Check\_MK server and then install the package.

After installation of package, make sure the service is listening in port 6556 and able to fetch data locally by the agent.

### Centos / RedHat / Amazon Linux:

<http://hmgr.1cloudhub.com/checkmk/check_mk/agents/check-mk-agent-1.4.0p12-1.noarch.rpm>

yum install check-mk-agent-1.4.0p12-1.noarch.rpm -y

netstat -plnt | grep 6556

check\_mk\_agent

### Ubuntu Linux:

wget http://13.127.51.135/checkmk/check\_mk/agents/check-mk-agent\_1.4.0p12-1\_all.deb

dpkg -i check-mk-agent\_1.4.0p12-1\_all.deb

netstat -plnt | grep 6556

check\_mk\_agent

### SUSE Linux:

wget http://13.127.51.135/checkmk/check\_mk/agents/check-mk-agent\_1.4.0p12-1\_all.deb

zypper install check-mk-agent-1.4.0p9-1.noarch.rpm

netstat -plnt | grep 6556

check\_mk\_agent

### Windows:

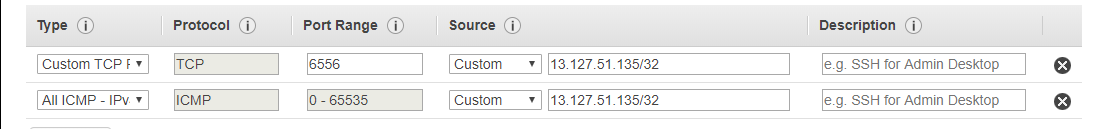
Download the agent from the browser and install the agent.

## Adding Security Group Entry

We must open ports for communication between the Check\_MK Server & Client. Add the below rules in security group of the EC2 Instance. Please find the below snip for reference and add it exactly same.

Port 6556 is used by Check\_MK Server (13.127.51.135).

1. Add ‘**Custom TCP**’ rule: **6556** for Check\_MK Server IP **13.127.51.135/32**
2. Add ‘**ALL ICMP**’ rule: **0-65635** for Check\_MK Server IP **13.127.51.135/32**
3. For all rules, Add Description as “**CK-Monitoring System IP**”



# Adding Rules in Check\_MK

Check\_MK works by rule based, for each and every customization it is managed by rules. Hence, we need to create rule to add host to host group, add rules to manage threshold, add rules to monitor websites etc and apply it to hosts that were added.

## Adding Hosts in Check\_MK

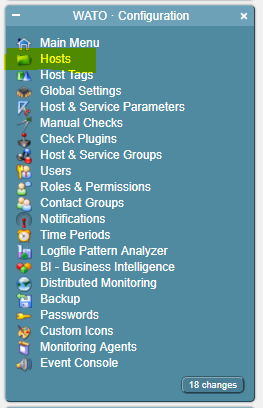
We need to create a host that needs to be monitored by Check\_MK.

### Host Naming Convention

<AccountName>-<Environment>-<Application Type / Name>-<Type of Asset>-<Count>

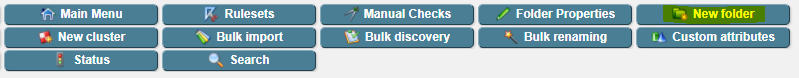
1. Account Name – Name of the Customer, in All Caps or Short Name in Caps or Actual Name
2. Environment – It could be Prod (Production), Stg (Staging), Dev (Development), Uat (User Acceptance Test)
3. Application Type – Web Server, App Name, Etc.. Ex: HybrisAdmin, HybrisApp
4. Type of Asset – Server , Database , ELB, ALB, Etc.
5. Count – (Optional) Number of Asset like Razer-Prod-HybrisApp-Server-01

Click the Host in WATO Menu found in Left Bottom of the Home Page.

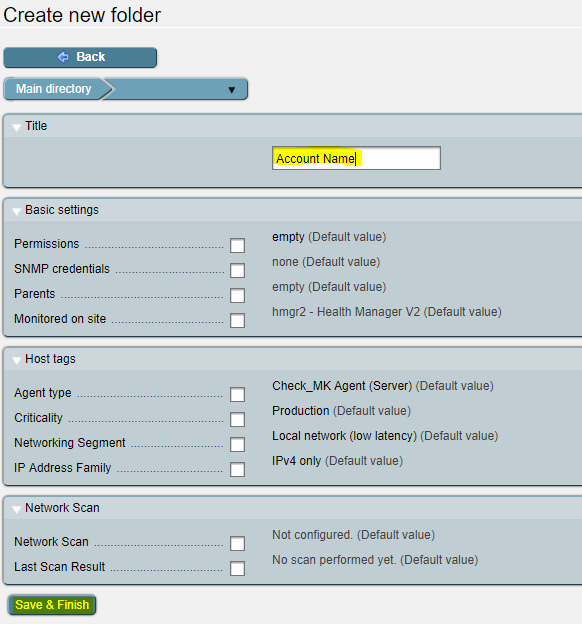


Click the Account Folder if it’s there, if not create a new folder for that account.

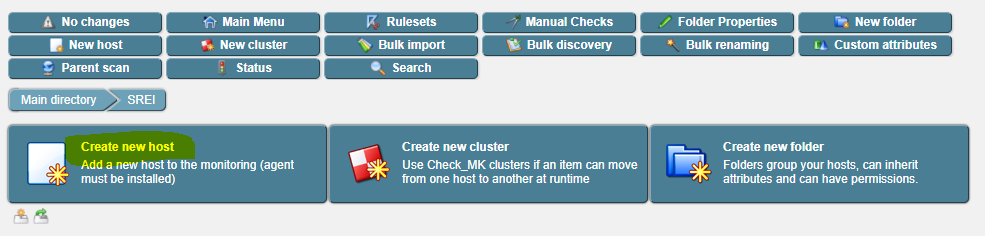
Create a new folder by clicking the New Folder in Host Menu.



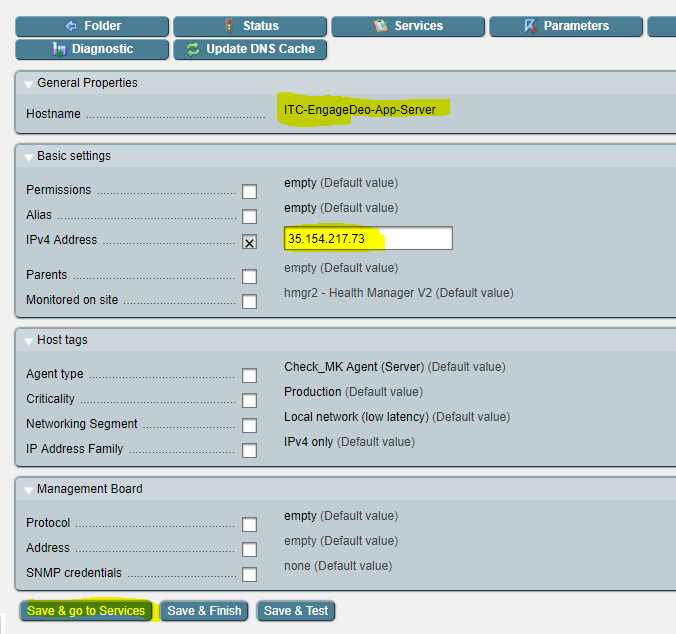
Enter the name of the account for which the host need to be added.



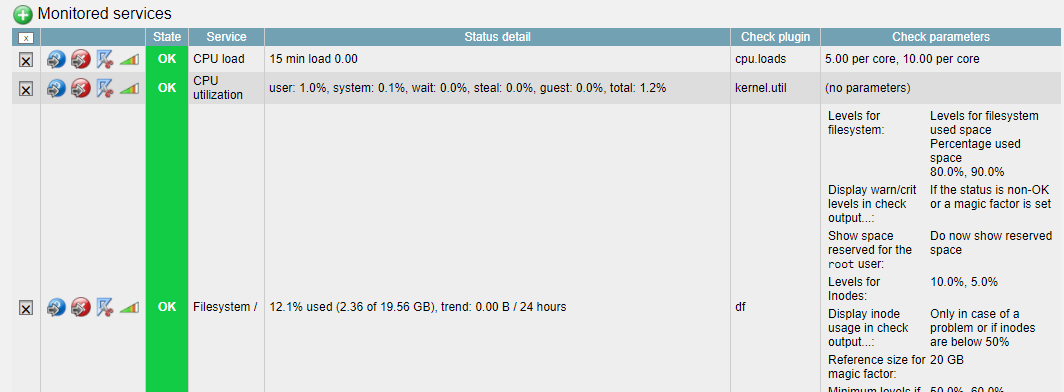
After creation of account folder, Double Click the account folder and Click New Host, and add the Hostname and IP Address



Click on Save & go to services

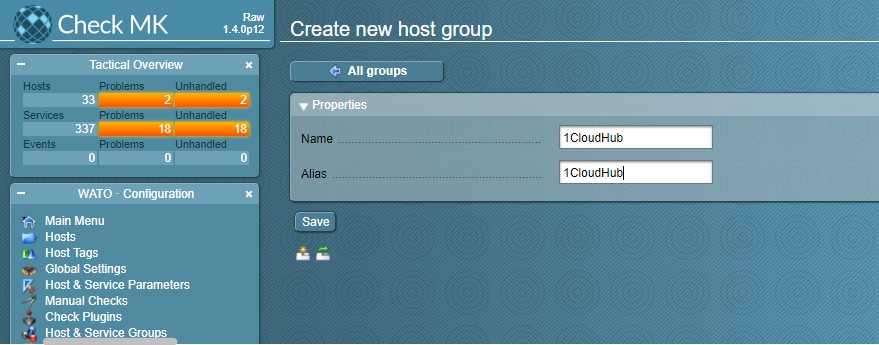


Immediately Check\_MK will get the data from Agent. Currently we monitor CPU Load, CPU Utilization, FileSystem’s Disk Space, Memory, Number of Threads, Uptime.

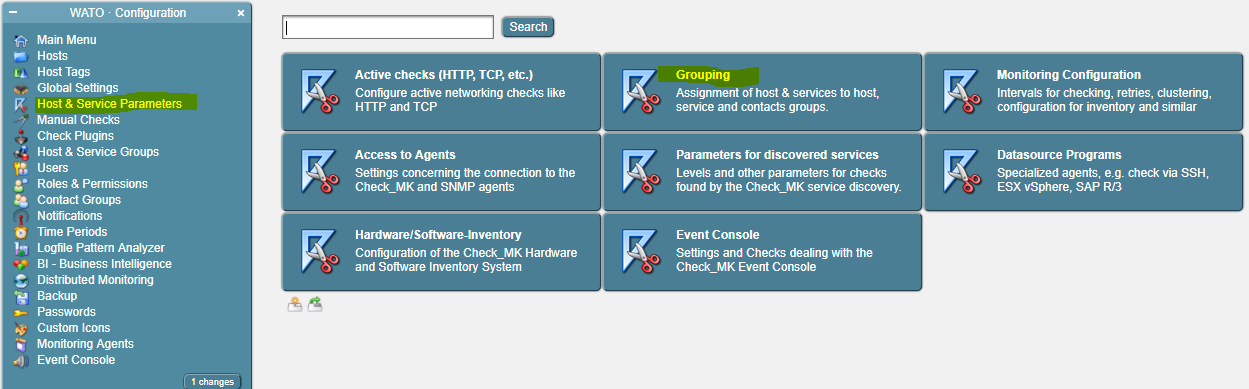


## Adding Host to Host Group in Check\_MK

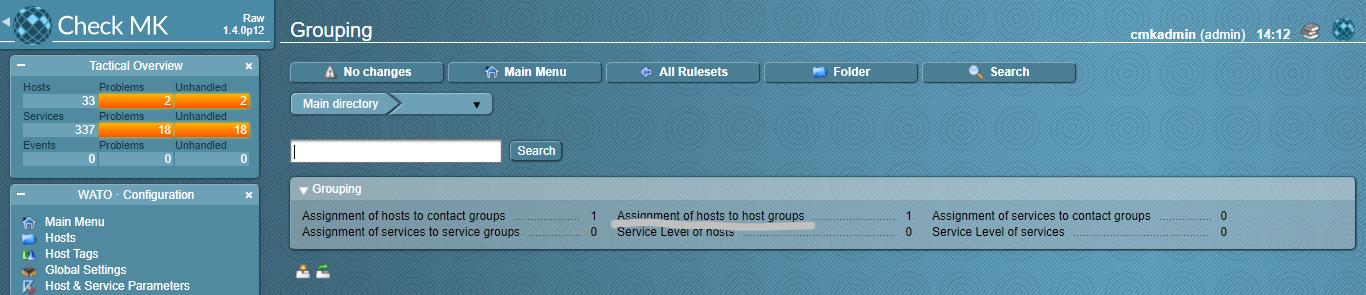
Click the Host and Service Groups in the Left side WATO – Configuration Panel and create a Host Group

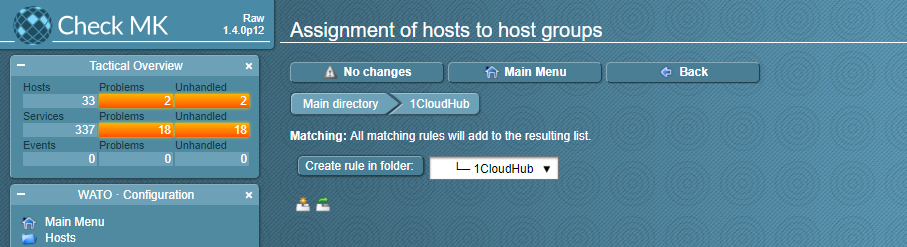


Click the Host and Service parameter option in WATO – Configuration panel in Left side and click the Grouping option

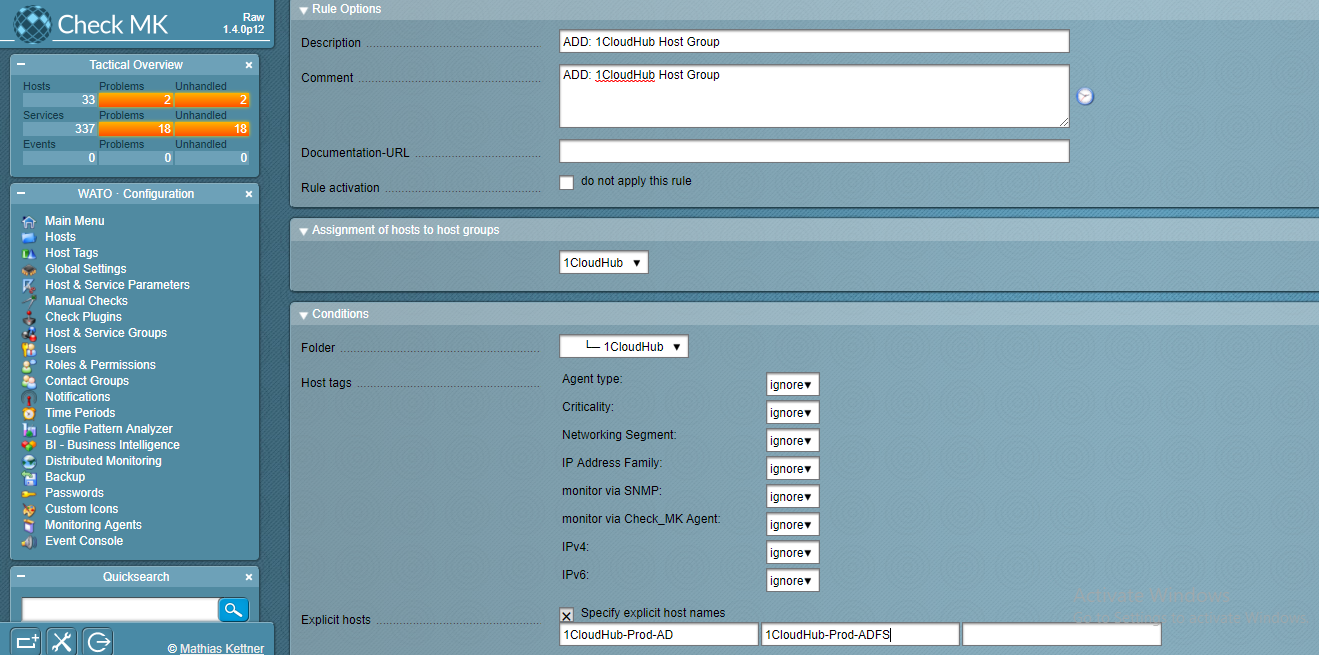


Click the Assignment of hosts to host group and Click the create rule in the bottom of the Page





Add a description ADD: CustomerName Host Group and select the group name, then add the host name in the below Explicit Host Text Box



Check in Host Group option then click the newly added Host, Validate the host accordingly.

