# **Check\_MK Monitoring Setup for Azure Servers**

This document contains the steps involved in enabling monitoring for Public and Private subnet servers launched in Azure account.

Table of Contents

[**Check\_MK Monitoring Setup** 1](#_Toc504404064)

[1. Adding Active Check Host 2](#_Toc504404065)

[**1.1.** Installing Check\_MK Agent 2](#_Toc504404066)

[**1.2.** Adding Security Group Entry in Azure Portal 2](#_Toc504404067)

[**1.3.** Adding Firewall Rules in Bastion/Jumpbox Server 2](#_Toc504404068)

[**1.4.** Adding Host in Check\_MK 3](#_Toc504404069)

[2. Adding Passive Check Host 5](#_Toc504404070)

[**2.1.** Bastion/Jumpbox Server Configuration: 5](#_Toc504404071)

[**2.2.** Adding Security Group Entry in Azure Portal 7](#_Toc504404072)

[**2.3.** Private Subnet Servers Configuration: 8](#_Toc504404073)

[**2.4.** Adding new host in Check\_MK console: 9](#_Toc504404074)

# 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 Check\_MK Agent

Download the agent from check\_mk console and install it in public subnet server

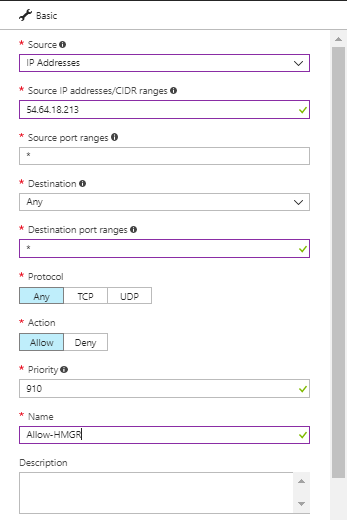
## Adding Security Group Entry in Azure Portal

Create new rules in Jumpbox subnet/server NSG and allow below 2 rules.

# Allow ICMP and port (6556) in Jumpbox subnet NSG (Inbound& Outbound) to HMGR server IP (54.64.18.213/32).

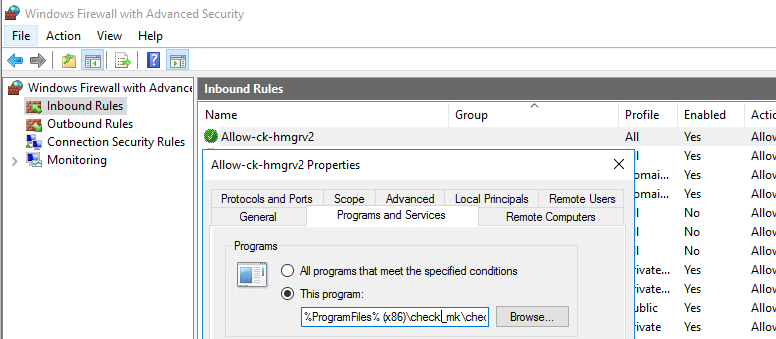
# Allow ICMP and port (6556) in Jumpbox server NSG (Inbound) to HMGR server IP (54.64.18.213/32).

Here allowed all traffic to HMGR server IP

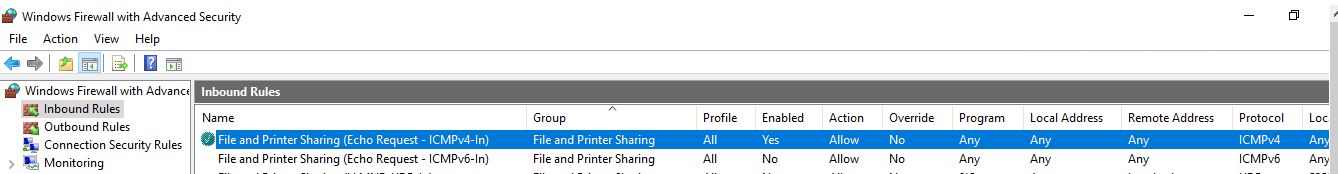


## Adding Firewall Rules in Bastion/Jumpbox Server

# Add new inbound rule and allow check\_mk agent (.exe) program.

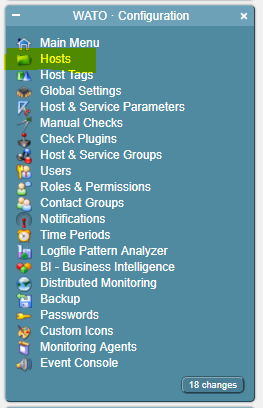


# Enable File and Printer sharing for ICMP



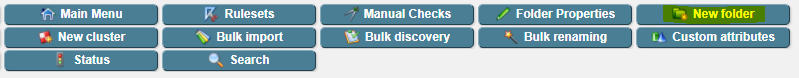
## Adding Host in Check\_MK

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

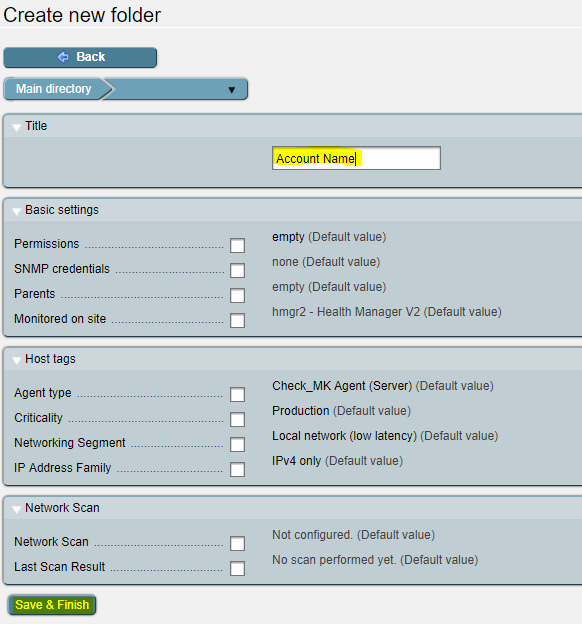


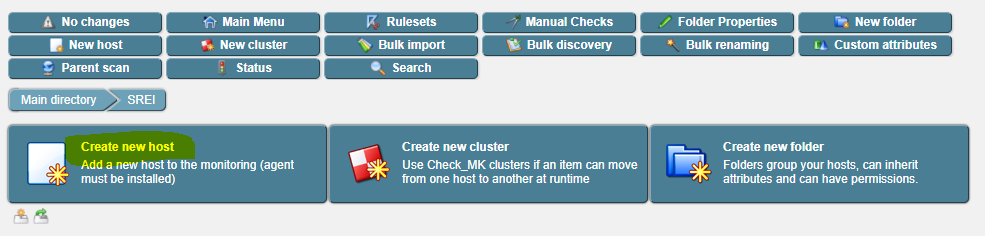
Click the Account Folder if it’s there, if not create a new folder for that account.

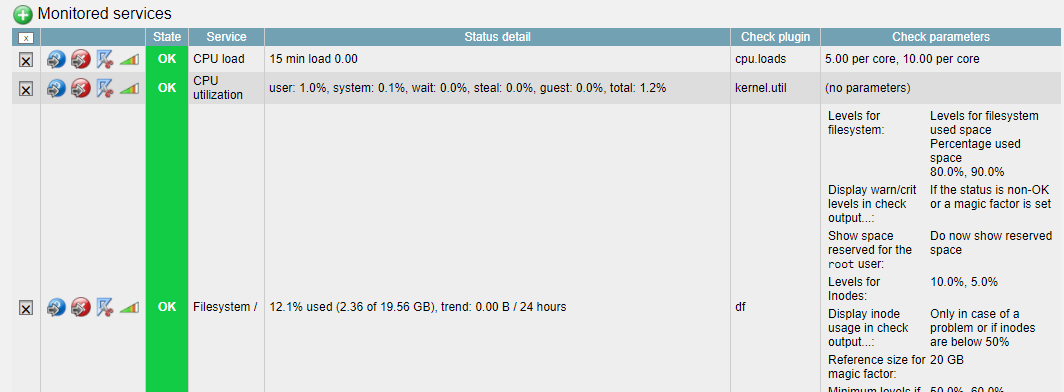
Create a new folder by clicking the New Folder in Host Menu.



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

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.

For adding Host to Host Group in Check\_MK, refer to Check\_MK\_V1.2 document (Section 3.2) available in owncloud [ownCloud\CK-All\Managed Services\SOP](file:///D:\ownCloud\CK-All\Managed%20Services\SOP\Check_MK_V1.2.docx)

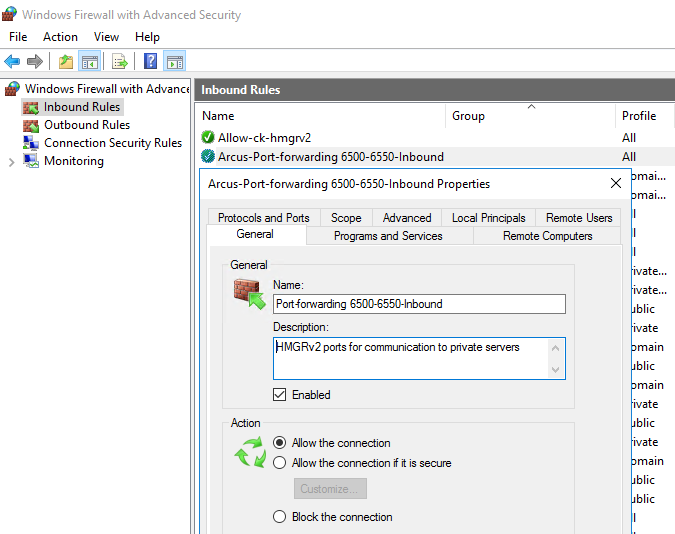
# Adding Passive Check Host

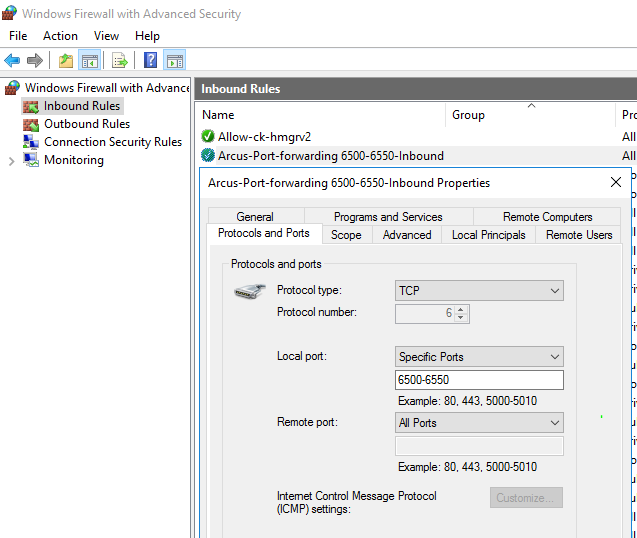
## Bastion/Jumpbox Server Configuration:

Step 1: In Bastion server download and install check\_mk (windows) agent and allow below inbound rule in Windows Firewall.

Add new inbound rule for port-fordwarding as below

# Add new inbound rule and port range 6500-6550.





Step 2: Run command prompt as Administrator and execute below commands for port forwarding.

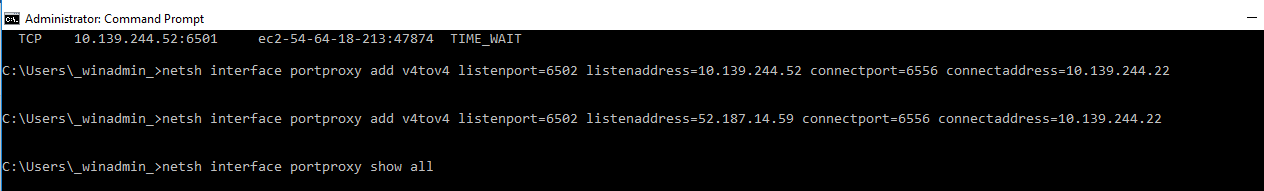
Replace listenport and Private Server IP accordingly for each private server

Commands:

# netsh interface portproxy add v4tov4 listenport=6501 listenaddress=<Jumpbox PublicIP> connectport=6556 connectaddress=<Private ServerIP>

# netsh interface portproxy add v4tov4 listenport=6501 listenaddress=<Jumpbox PrivateIP> connectport=6556 connectaddress=< Private ServerIP >

# netsh interface portproxy show all

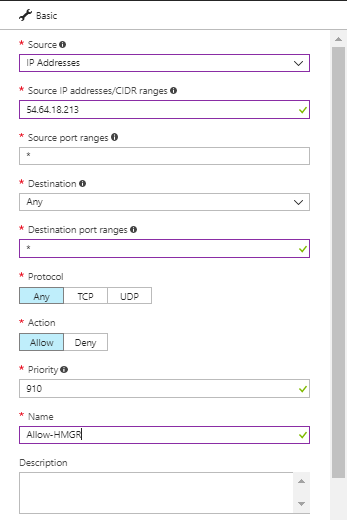


## Adding Security Group Entry in Azure Portal

Step 1: Create new rules in Jumpbox subnet NSG and allow below 2 rules.

# Allow ICMP and port range (6500-6550) in Jumbox Snet NSG (Inbound/Outbound) to HMGR server IP.

Here allowed all traffic to HMGR server IP

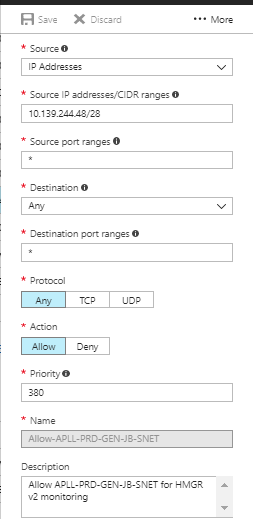


## Private Subnet Servers Configuration:

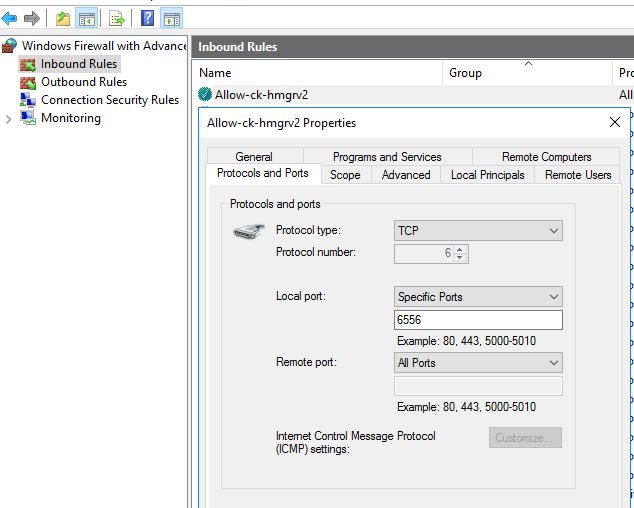
Step 1: Download and install check\_mk windows agent in private server.

Step 2: Create new rule in Private server subnet NSG and allow below port.

# Allow ICMP and port 6556 to Jumpbox server/Snet (Inbound)



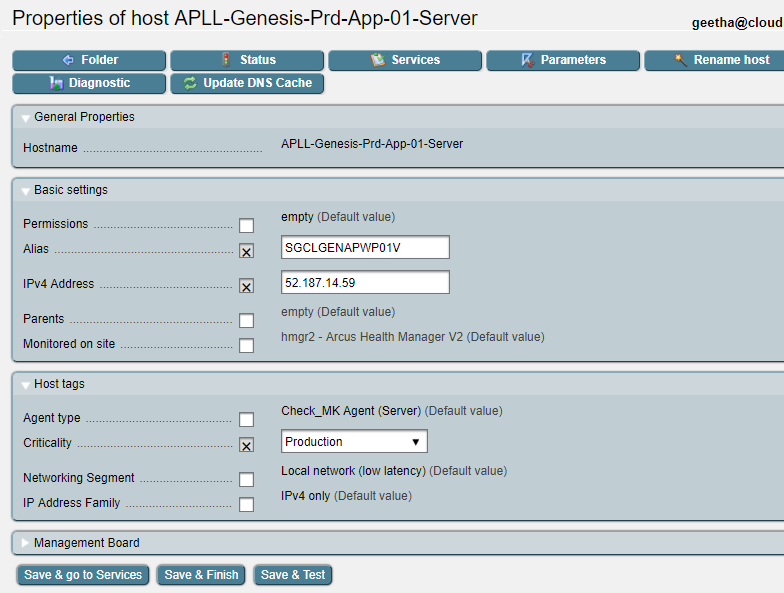
Step 3: Create new Inbound rule in windows firewall and allow port 6556.



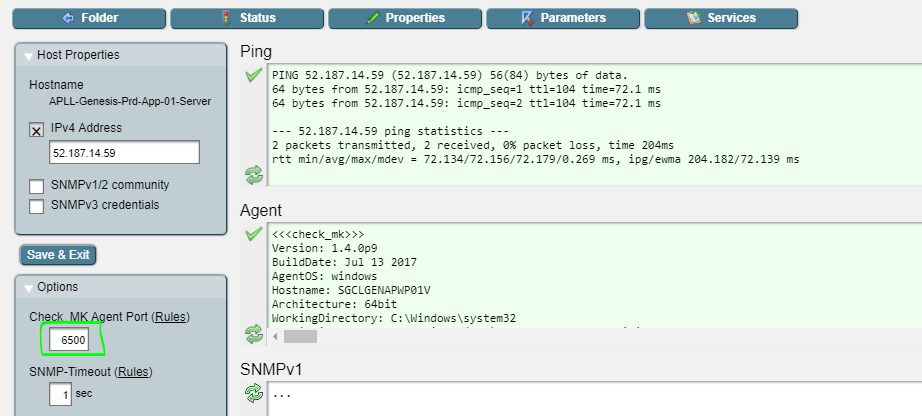
## Adding new host in Check\_MK console:

Step 1: In HMGR console, go to Hosts Folder and add new host, provide Hostname and Alias name(Optional).

In IPv4 Address give Jumpbox server Public IP then click on Save and test



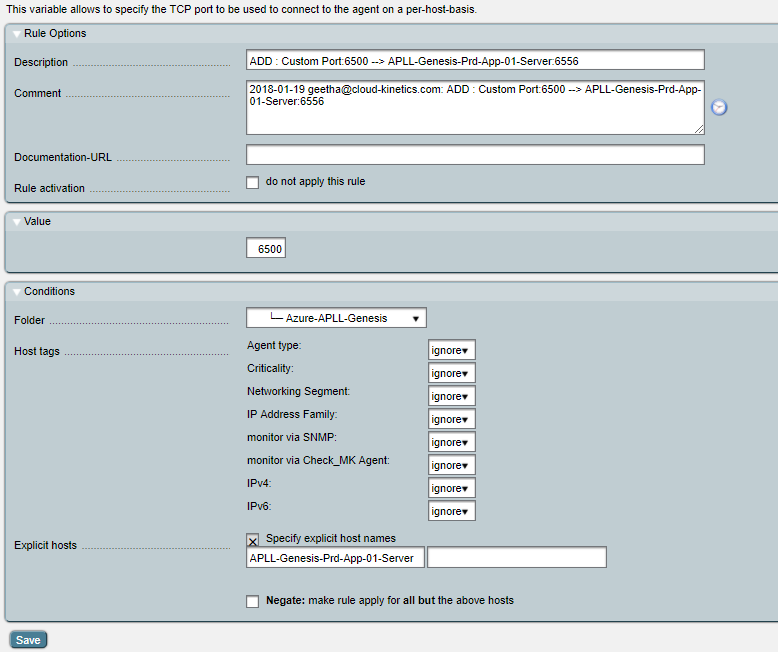
Change the check\_mk agent port and test then click on Parameters to customize server monitoring port.



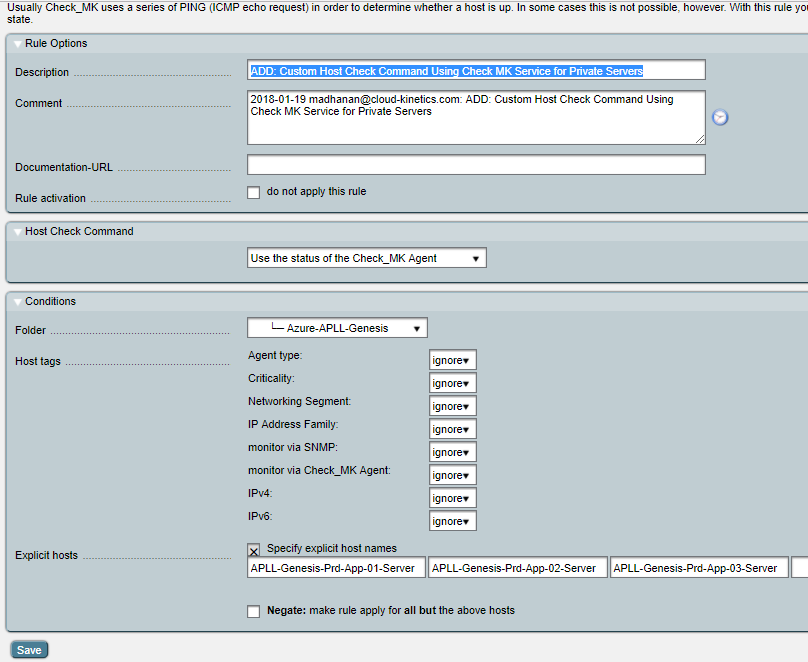
Step 2: Go to Parameters and make the changes as follows

# Create host specific rule

# Change [TCP port for connection to Check\_MK agent](http://hmgr2.cl.cloud-kinetics.com/hmgr2/check_mk/wato.py?folder=azure-apll-genesis&host=APLL-Genesis-Prd-App-01-Server&item=Tm9uZQ%3D%3D&mode=edit_ruleset&varname=agent_ports) running in Private server and save



# Go to Host group parameters config &click on host check command, then add the new host and save



Step 3: In Services, enable the services to be monitored.

