

3.

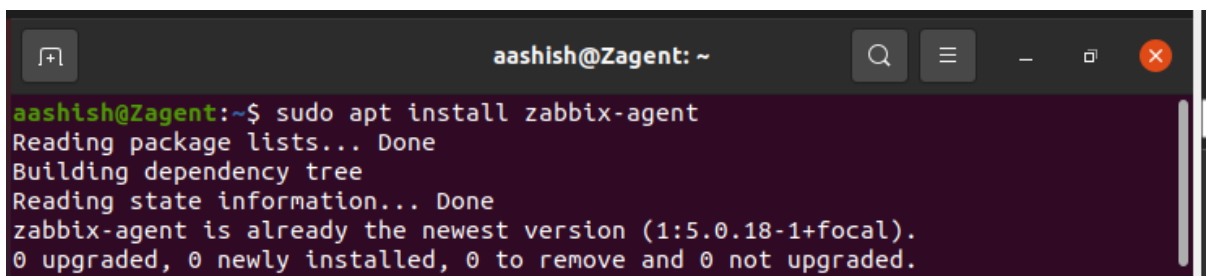
Install Latest Zabbix Agent on VM or host machine or server itself to fetch logs, steps include:

- Run as active check agent
- Add a logging item to the same template for fetching /var/log/syslog(Ubuntu) or /var/log/messages (CentOS)
- Fetch those logs from the host (Make sure required permissions are set for zabbix-agent to pull logs)
- Provide agent configuration file & screenshots for target machine graph & logs

Answer:

To install the zabbix-agent on same VM, we use following command;

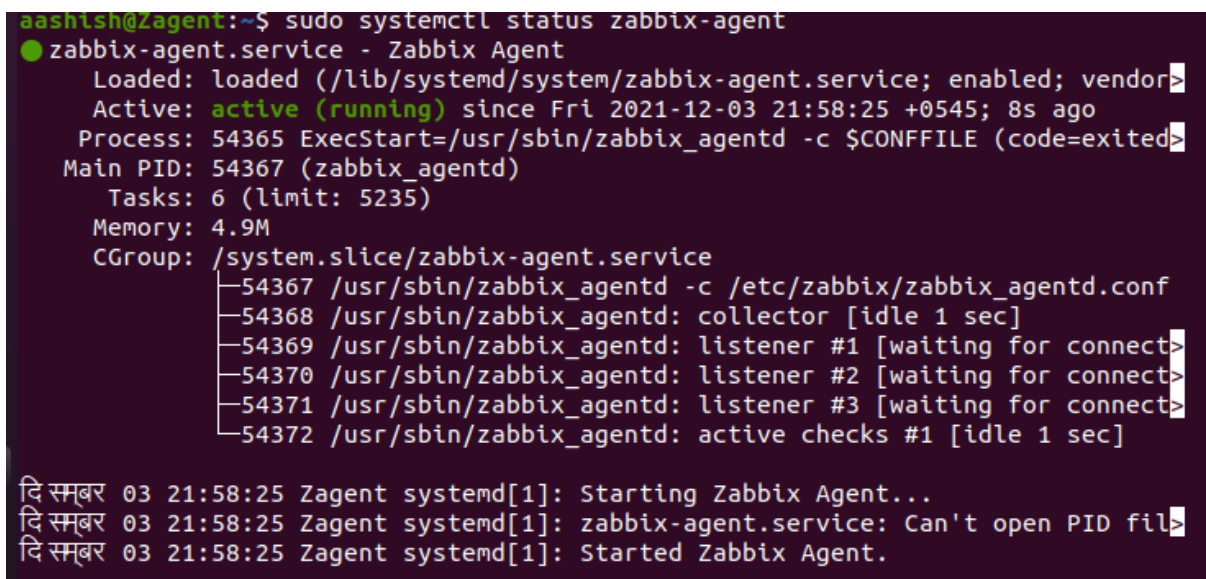
- sudo apt-get install zabbix-agent



```
aashish@Zagent: ~  
aashish@Zagent:~$ sudo apt install zabbix-agent  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
zabbix-agent is already the newest version (1:5.0.18-1+focal).  
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

To check the zabbix-agent status, we use following command;

- sudo systemctl status zabbix-agent



```
aashish@Zagent:~$ sudo systemctl status zabbix-agent  
● zabbix-agent.service - Zabbix Agent  
   Loaded: loaded (/lib/systemd/system/zabbix-agent.service; enabled; vendor preset: enabled)  
   Active: active (running) since Fri 2021-12-03 21:58:25 +0545; 8s ago  
     Process: 54365 ExecStart=/usr/sbin/zabbix_agentd -c $CONFFILE (code=exited, status=0/SUCCESS)  
    Main PID: 54367 (zabbix_agentd)  
      Tasks: 6 (limit: 5235)  
     Memory: 4.9M  
    CGroup: /system.slice/zabbix-agent.service  
            └─54367 /usr/sbin/zabbix_agentd -c /etc/zabbix/zabbix_agentd.conf  
              └─54368 /usr/sbin/zabbix_agentd: collector [idle 1 sec]  
                └─54369 /usr/sbin/zabbix_agentd: listener #1 [waiting for connect]  
                  └─54370 /usr/sbin/zabbix_agentd: listener #2 [waiting for connect]  
                    └─54371 /usr/sbin/zabbix_agentd: listener #3 [waiting for connect]  
                      └─54372 /usr/sbin/zabbix_agentd: active checks #1 [idle 1 sec]  
  
दि सम्बर 03 21:58:25 Zagent systemd[1]: Starting Zabbix Agent...  
दि सम्बर 03 21:58:25 Zagent systemd[1]: zabbix-agent.service: Can't open PID file  
दि सम्बर 03 21:58:25 Zagent systemd[1]: Started Zabbix Agent.
```

I have created a zabbix-agent using Auto registration action check. For that we edit zabbix-agentd.conf file in /etc/zabbix as follows;

- **sudo nano /etc/zabbix/zabbix-agentd.conf**
- **Server=127.0.0.1**

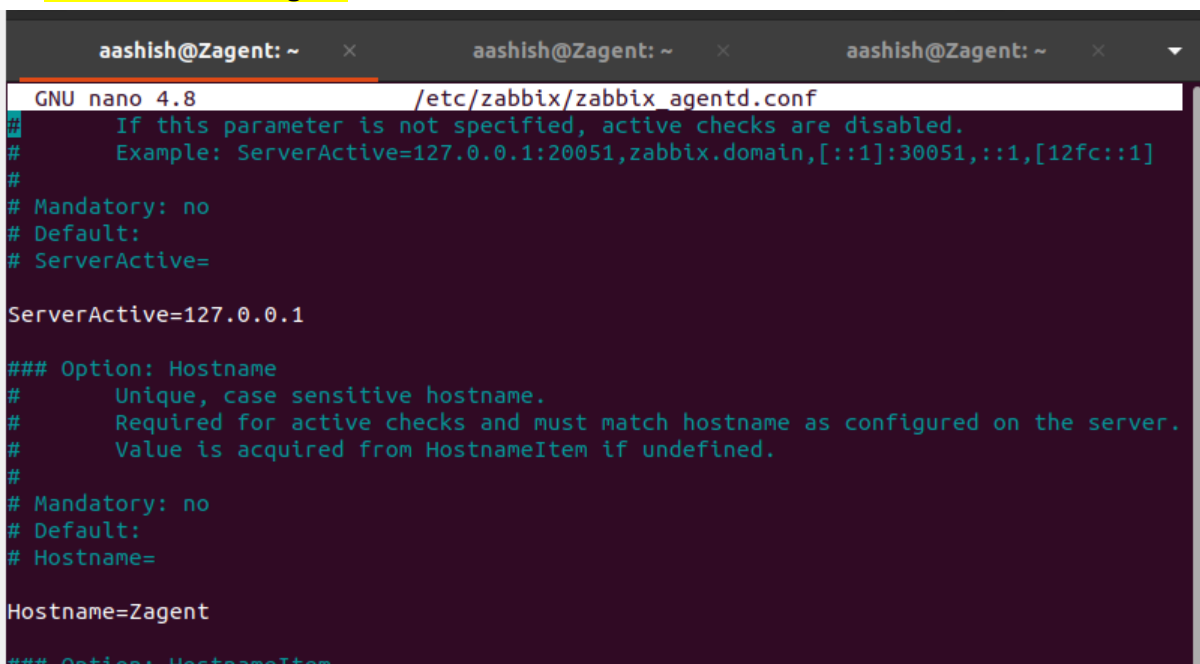


```
aashish@Zagent: ~ x aashish@Zagent: ~ x aashish@Zagent: ~ x
GNU nano 4.8 /etc/zabbix/zabbix_agentd.conf
# List of comma delimited IP addresses, optionally in CIDR notation, or DNS name
# Incoming connections will be accepted only from the hosts listed here.
# If IPv6 support is enabled then '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1'
# and '::/0' will allow any IPv4 or IPv6 address.
# '0.0.0.0/0' can be used to allow any IPv4 address.
# Example: Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com
#
# Mandatory: yes, if StartAgents is not explicitly set to 0
# Default:
# Server=

Server=127.0.0.1
```

Next, we add following lines;

- **ServerActive=127.0.0.1**
- **Hostname=Zagent**



```
aashish@Zagent: ~ x aashish@Zagent: ~ x aashish@Zagent: ~ x
GNU nano 4.8 /etc/zabbix/zabbix_agentd.conf
# If this parameter is not specified, active checks are disabled.
# Example: ServerActive=127.0.0.1:20051,zabbix.domain,[::1]:30051,::1,[12fc::1]
#
# Mandatory: no
# Default:
# ServerActive=

ServerActive=127.0.0.1

### Option: Hostname
# Unique, case sensitive hostname.
# Required for active checks and must match hostname as configured on the server.
# Value is acquired from HostnameItem if undefined.
#
# Mandatory: no
# Default:
# Hostname=

Hostname=Zagent

### Option: HostnameItem
```

Again, we add **HostMetadataItem** and **HostMetadata** as follows;

```
aashish@Zagent: ~ x aashish@Zagent: ~ x aashish@Zagent: ~ x
GNU nano 4.8 /etc/zabbix/zabbix_agentd.conf
#
# Mandatory: no
# Range: 0-255 characters
# Default:
# HostMetadata=

HostMetadata=Linux 21df83bf21bf0be663090bb8d4128558ab9b95fba66a6dbf834f8b91ae5e08ae

### Option: HostMetadataItem
#
# Optional parameter that defines an item used for getting host metadata.
# Host metadata is used at host auto-registration process.
# During an auto-registration request an agent will log a warning message if
# the value returned by specified item is over limit of 255 characters.
# This option is only used when HostMetadata is not defined.
#
# Mandatory: no
# Default:
# HostMetadataItem=

HostMetadataItem=release
```

Next, we add **UserParameter** also defining the OS release.

```
aashish@Zagent: ~ x aashish@Zagent: ~ x aashish@Zagent: ~ x
GNU nano 4.8 /etc/zabbix/zabbix_agentd.conf
### Option: UserParameter
#
# User-defined parameter to monitor. There can be several user-defined parameter>
# Format: UserParameter=<key>,<shell command>
# See 'zabbix_agentd' directory for examples.
#
# Mandatory: no
# Default:
# UserParameter=
UserParameter=release,cat /etc/lsb-release
##### LOADABLE MODULES #####
```

We can check OS release of Ubuntu as follows;

```
aashish@Zagent: ~ x aashish@Zagent: ~ x aashish@Zagent: ~ x
aashish@Zagent:~$ cat /etc/lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=20.04
DISTRIB_CODENAME=focal
DISTRIB_DESCRIPTION="Ubuntu 20.04.3 LTS"
```

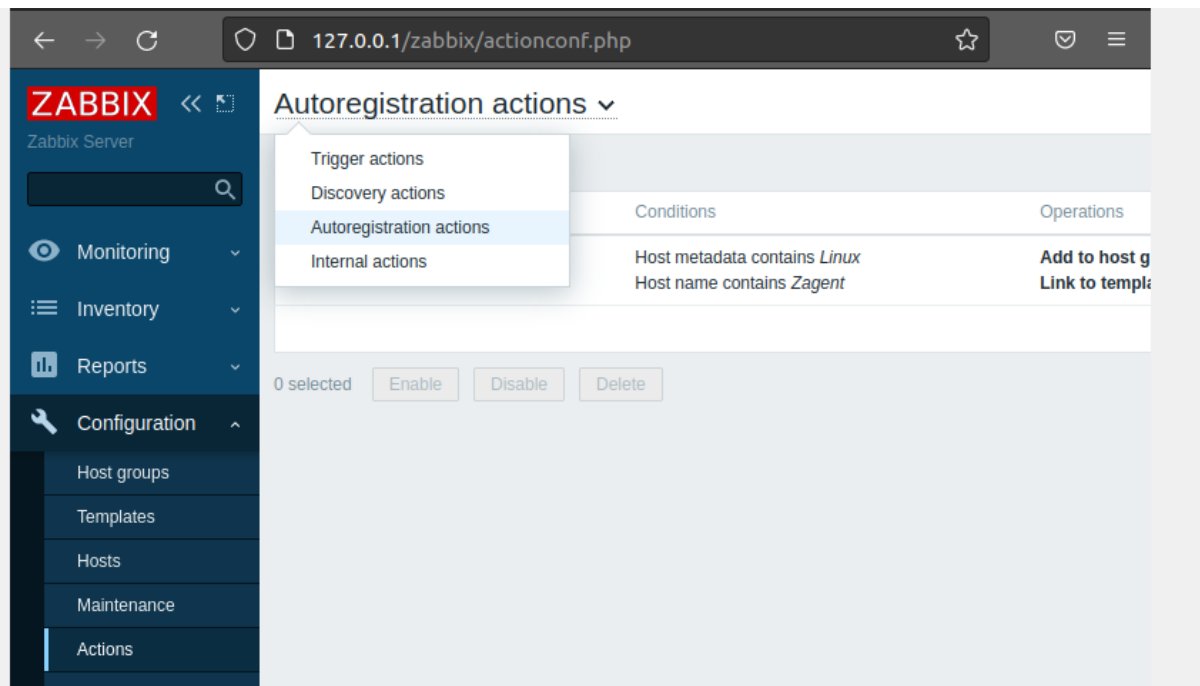
Next, we reload the zabbix-server config cache using the following command;

```
- sudo zabbix_server -R config_cache_reload
```

```
aashish@Zagent:~$ sudo zabbix_server -R config_cache_reload
zabbix_server [10115]: command sent successfully
```

Then, we move to the zabbix frontend part to setup auto registration action as follows;

We click on the **configuration -> actions -> Autoregistration actions**

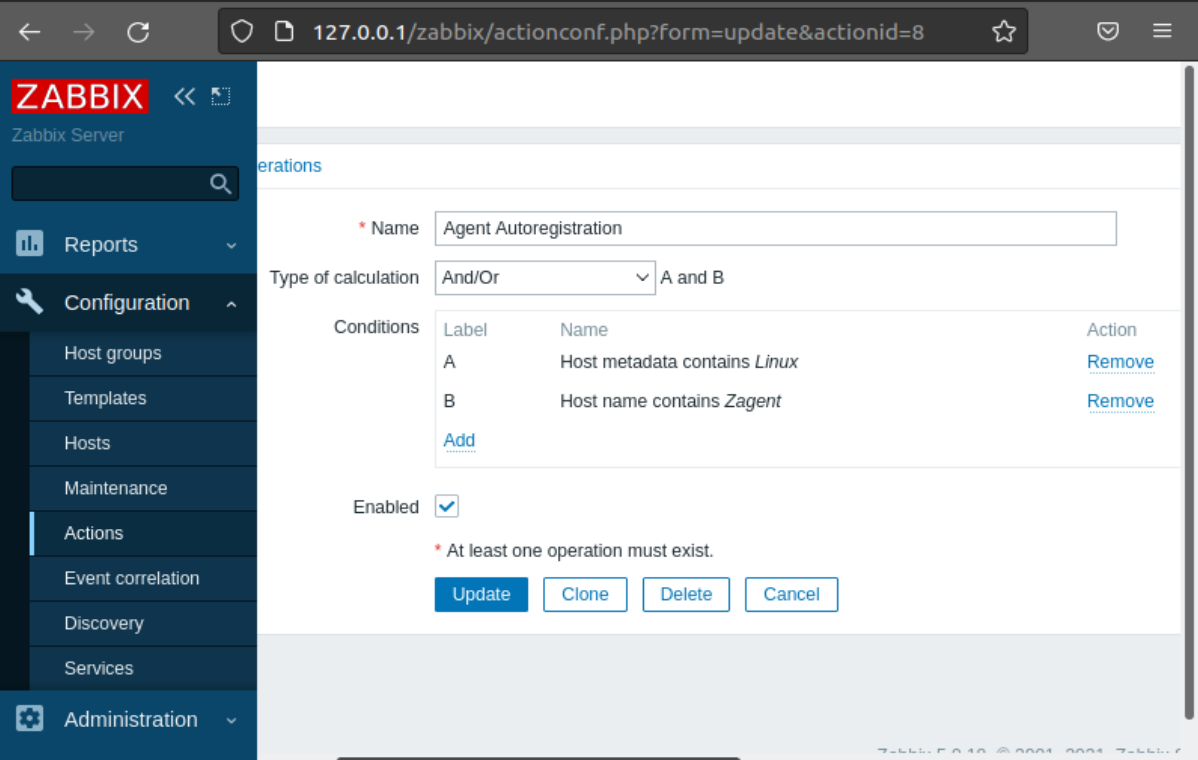


The screenshot shows the Zabbix web interface at the URL `127.0.0.1/zabbix/actionconf.php`. The left sidebar contains the navigation menu with the following items: Monitoring, Inventory, Reports, Configuration (expanded), Host groups, Templates, Hosts, Maintenance, and Actions. The main content area is titled "Autoregistration actions" and features a dropdown menu with the following options: Trigger actions, Discovery actions, Autoregistration actions (selected), and Internal actions. Below the dropdown, there is a table with two columns: "Conditions" and "Operations". The table contains one row with the following data:

Conditions	Operations
Host metadata contains <i>Linux</i> Host name contains <i>Zagent</i>	Add to host g Link to templa

At the bottom of the table, there is a status bar that reads "0 selected" and three buttons: "Enable", "Disable", and "Delete".

Next, we create an action named **Agent Autoregistration** with the conditions shown in figure below;

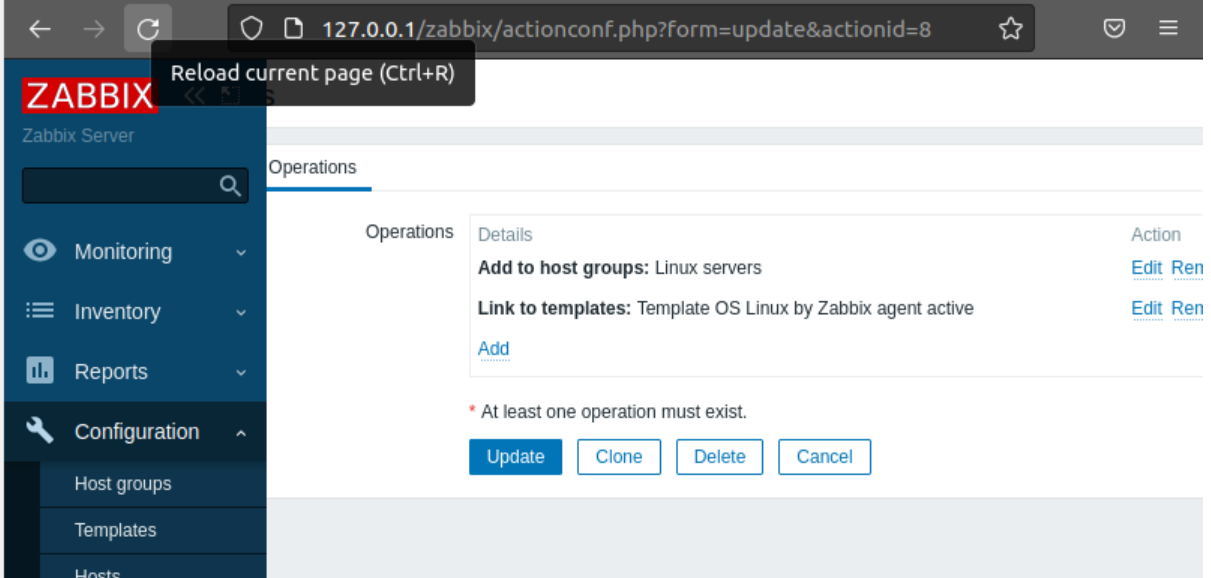


The screenshot shows the Zabbix web interface for configuring an action. The browser address bar displays `127.0.0.1/zabbix/actionconf.php?form=update&actionid=8`. The left sidebar contains the Zabbix logo and a menu with categories: Reports, Configuration, and Administration. The 'Configuration' menu is expanded, showing options like Host groups, Templates, Hosts, Maintenance, Actions, Event correlation, Discovery, and Services. The main content area is titled 'Operations' and contains the following fields and controls:

- Name:** A text input field containing 'Agent Autoregistration'.
- Type of calculation:** A dropdown menu set to 'And/Or' with a sub-label 'A and B'.
- Conditions:** A table with three columns: Label, Name, and Action.

Label	Name	Action
A	Host metadata contains <i>Linux</i>	Remove
B	Host name contains <i>Zabbix</i>	Remove
Add		
- Enabled:** A checkbox that is checked.
- Message:** A red asterisk followed by the text '* At least one operation must exist.'
- Buttons:** 'Update', 'Clone', 'Delete', and 'Cancel'.

Then, we save and add the operations as follows;

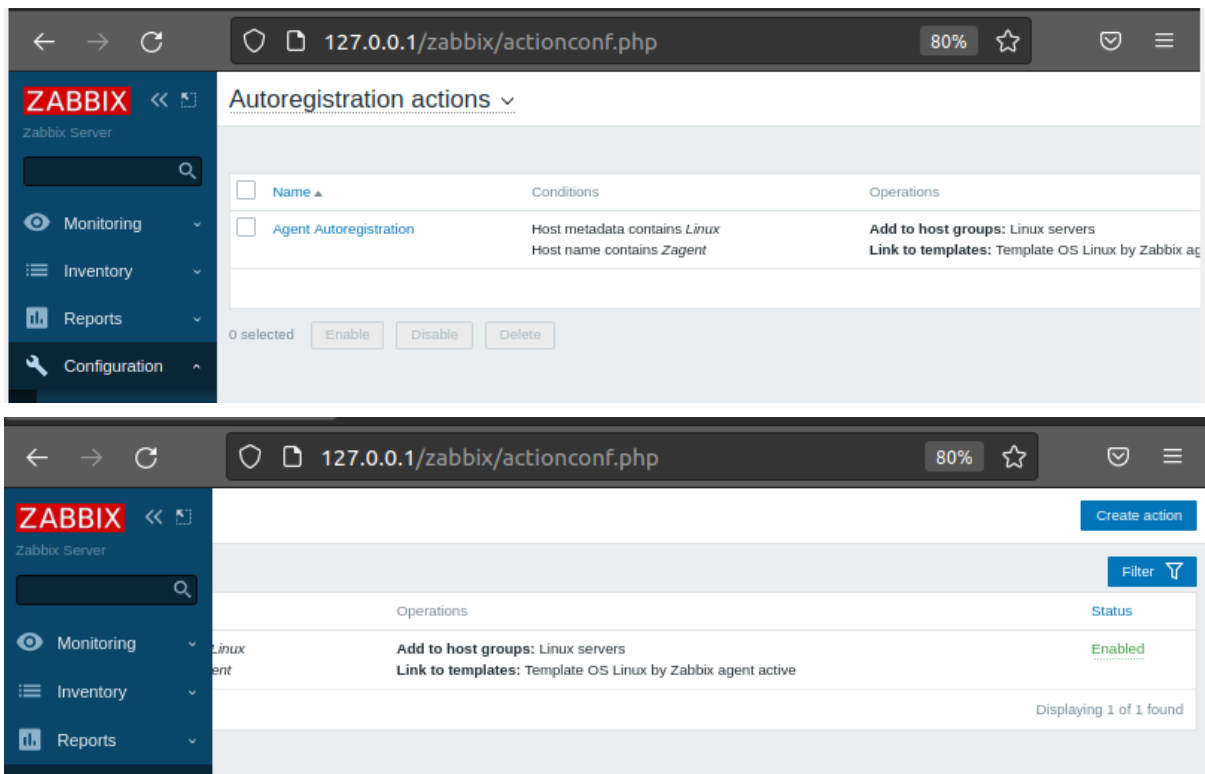


The screenshot shows the Zabbix web interface for configuring an action, specifically the 'Operations' tab. The browser address bar displays `127.0.0.1/zabbix/actionconf.php?form=update&actionid=8`. A tooltip 'Reload current page (Ctrl+R)' is visible over the Zabbix logo. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Operations' and contains the following fields and controls:

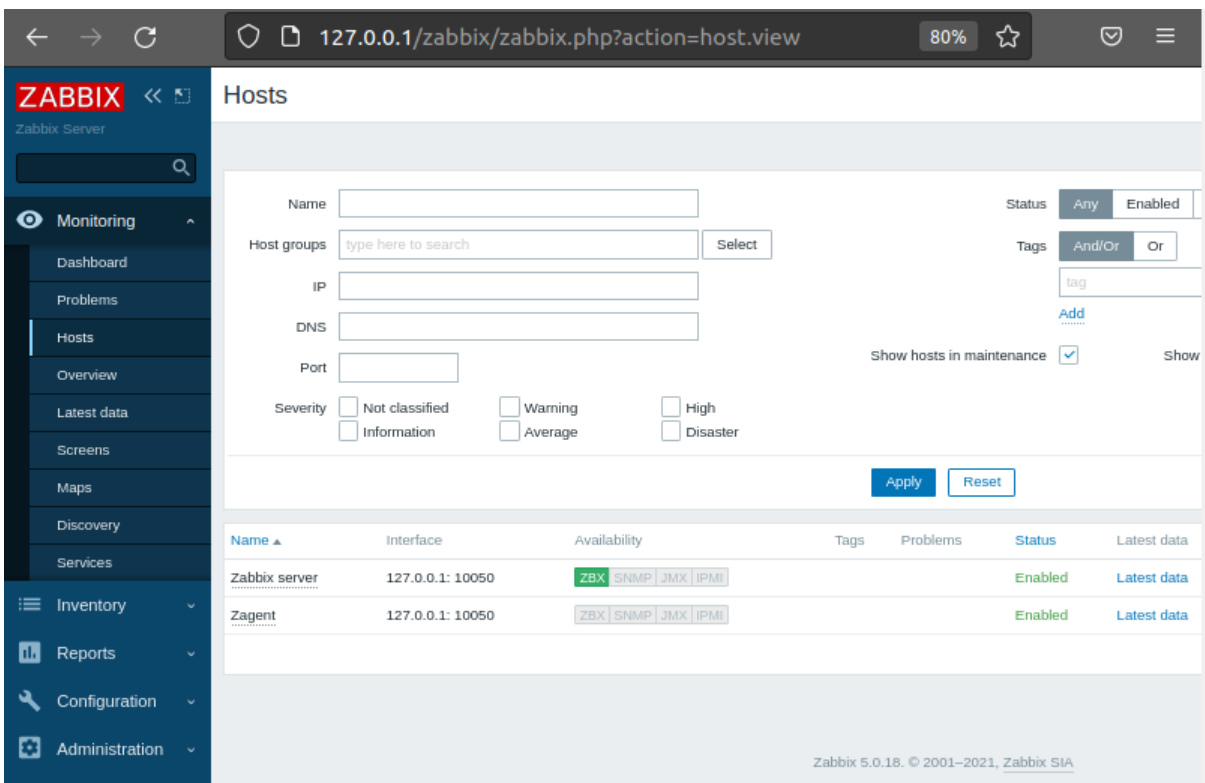
- Operations:** A table with three columns: Details, Action, and a sub-label 'Details'.

Details	Action	Details
Add to host groups: Linux servers	Edit Ren	
Link to templates: Template OS Linux by Zabbix agent active	Edit Ren	
Add		
- Message:** A red asterisk followed by the text '* At least one operation must exist.'
- Buttons:** 'Update', 'Clone', 'Delete', and 'Cancel'.

We save the operations and check the action created. Here, Agent Autoregistration action has been added successfully and its status is verified enabled.

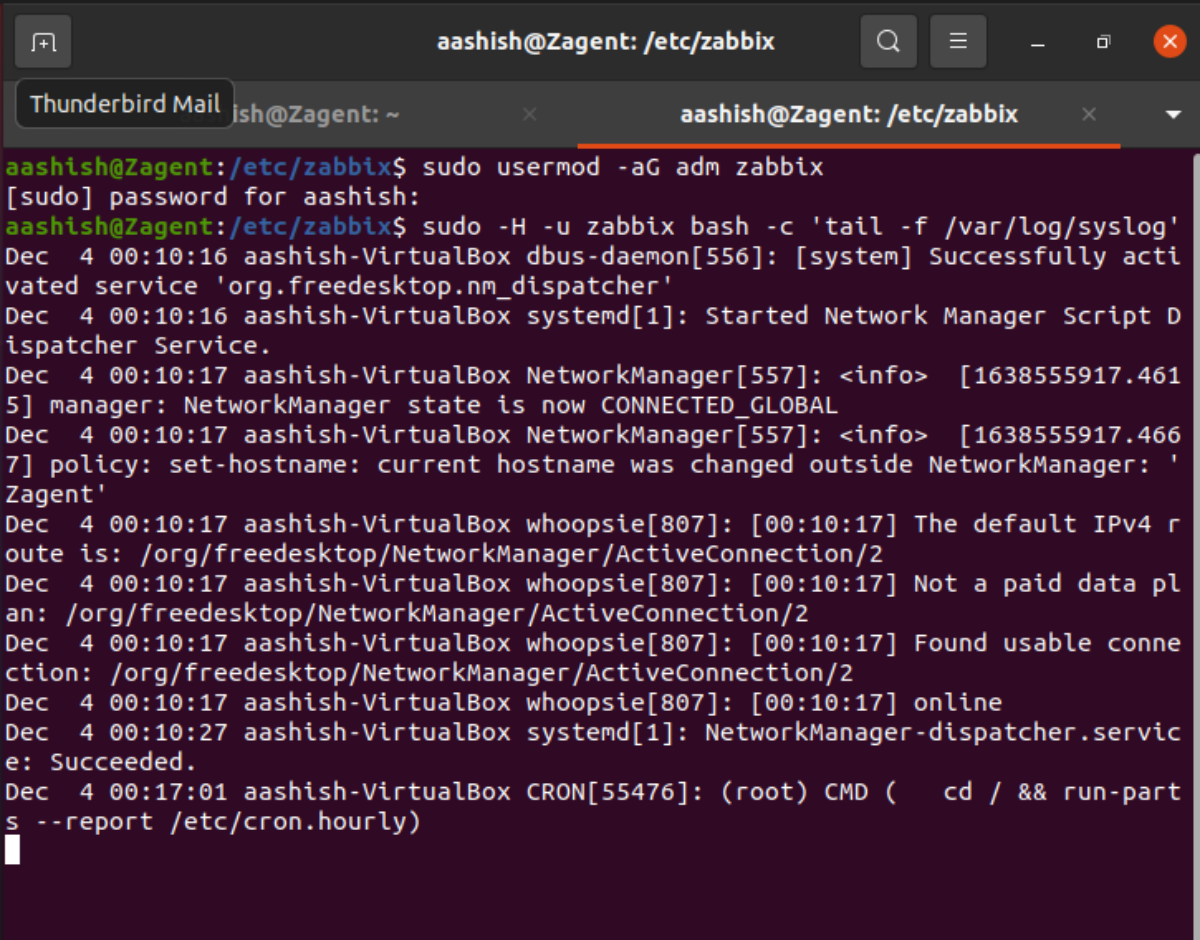


Next, we check the hosts from the monitoring option, we can see that the host named agent has been created using the auto registration action with enabled status.



Since, the host was created automatically using agent auto registration action. We give required privilege to zabbix user to fetch the logs via /var/log/syslog as follows;

- **sudo usermod -aG adm zabbix**
- **sudo -H -u zabbix bash -c 'tail -f /var/log/syslog'**



```
aashish@Zagent: /etc/zabbix
Thunderbird Mail aashish@Zagent: ~ aashish@Zagent: /etc/zabbix
aashish@Zagent:/etc/zabbix$ sudo usermod -aG adm zabbix
[sudo] password for aashish:
aashish@Zagent:/etc/zabbix$ sudo -H -u zabbix bash -c 'tail -f /var/log/syslog'
Dec  4 00:10:16 aashish-VirtualBox dbus-daemon[556]: [system] Successfully activated service 'org.freedesktop.nm_dispatcher'
Dec  4 00:10:16 aashish-VirtualBox systemd[1]: Started Network Manager Script Dispatcher Service.
Dec  4 00:10:17 aashish-VirtualBox NetworkManager[557]: <info> [1638555917.4615] manager: NetworkManager state is now CONNECTED_GLOBAL
Dec  4 00:10:17 aashish-VirtualBox NetworkManager[557]: <info> [1638555917.4667] policy: set-hostname: current hostname was changed outside NetworkManager: 'Zagent'
Dec  4 00:10:17 aashish-VirtualBox whoopsie[807]: [00:10:17] The default IPv4 route is: /org/freedesktop/NetworkManager/ActiveConnection/2
Dec  4 00:10:17 aashish-VirtualBox whoopsie[807]: [00:10:17] Not a paid data plan: /org/freedesktop/NetworkManager/ActiveConnection/2
Dec  4 00:10:17 aashish-VirtualBox whoopsie[807]: [00:10:17] Found usable connection: /org/freedesktop/NetworkManager/ActiveConnection/2
Dec  4 00:10:17 aashish-VirtualBox whoopsie[807]: [00:10:17] online
Dec  4 00:10:27 aashish-VirtualBox systemd[1]: NetworkManager-dispatcher.service: Succeeded.
Dec  4 00:17:01 aashish-VirtualBox CRON[55476]: (root) CMD ( cd / && run-parts --report /etc/cron.hourly)
```

To fetch the logs, we click on the configuration -> item -> create item from the created host as follows;

The screenshot shows the Zabbix web interface with the 'item' configuration page. The left sidebar contains navigation links: Monitoring, Inventory, Reports, Configuration, Administration, and Support. The 'Configuration' section is expanded, showing 'Host groups', 'Templates', 'Hosts', 'Maintenance', 'Actions', 'Event correlation', 'Discovery', and 'Services'. The 'Hosts' link is selected. The main content area shows the 'Create item' form with the following fields:

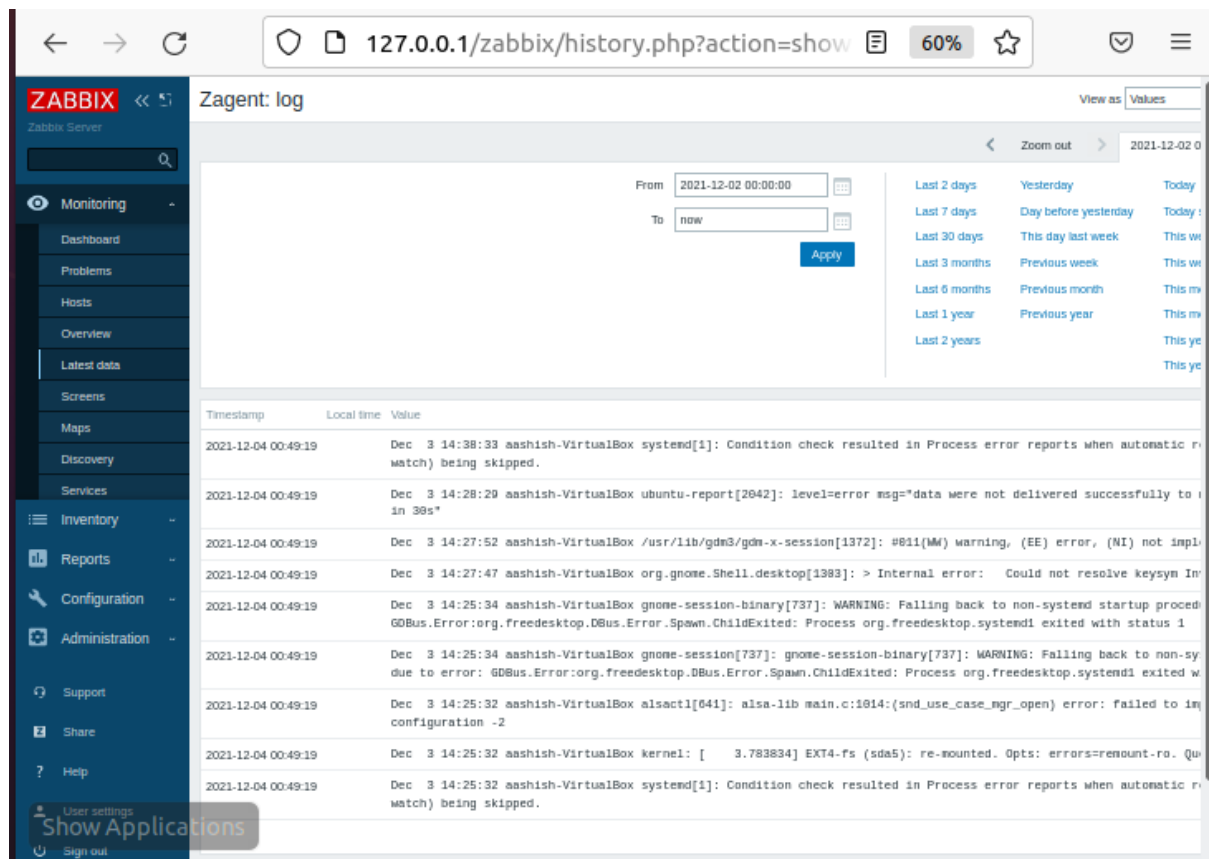
- Name: log
- Type: Zabbix agent (active)
- Key: log[/var/log/syslog.error]
- Type of information: Log
- Update interval: 5s
- Custom intervals: Flexible, Scheduling, 50s, 1-7,00:00-24:00
- History storage period: Do not keep history, Storage period, 90d
- Log time format:
- New application:
- Applications: -None-, CPU, Disk sda, Filesystem /, Filesystems, General, Interface enp0s3, Inventory, Memory, Monitoring agent
- Description:

Then we check the log data from monitoring -> Latest data -> log or syslog as follows;

The screenshot shows the 'Latest data' table in the Zabbix web interface. The table has columns: Name, Interface, Availability, Tags, Problems, Status, Latest data, Problems, Graphs, and Screens. The data is as follows:

Name	Interface	Availability	Tags	Problems	Status	Latest data	Problems	Graphs	Screens
Zabbix server	127.0.0.1: 10050	ZBX SNMP JMX IPMI		1	Enabled	Latest data	Problems 1	Graphs 18	Screens
Zagent	192.168.1.18: 10050	ZBX SNMP JMX IPMI			Enabled	Latest data	Problems	Graphs 13	Screens

Next, we click on the history to check the errors and alerts of syslog as follows;



The screenshot shows the Zabbix web interface at the URL `127.0.0.1/zabbix/history.php?action=show`. The page title is "Zagent: log". The left sidebar contains navigation links: Monitoring, Dashboard, Problems, Hosts, Overview, Latest data, Screens, Maps, Discovery, Services, Inventory, Reports, Configuration, Administration, Support, Share, and Help. The main content area displays a table of log entries. The table has three columns: Timestamp, Local time, and Value. The log entries show various error messages from the Zabbix agent, including warnings about condition checks and errors related to the GNOME desktop environment. A search bar and a "View as" dropdown are visible at the top right of the log area.

Timestamp	Local time	Value
2021-12-04 00:49:19	Dec 3 14:38:33	aashish-VirtualBox systemd[1]: Condition check resulted in Process error reports when automatic r (watch) being skipped.
2021-12-04 00:49:19	Dec 3 14:28:29	aashish-VirtualBox ubuntu-report[2642]: level=error msg="data were not delivered successfully to i in 38s"
2021-12-04 00:49:19	Dec 3 14:27:52	aashish-VirtualBox /usr/lib/gdm3/gdm-x-session[1372]: #811(MM) warning, (EE) error, (NI) not impl.
2021-12-04 00:49:19	Dec 3 14:27:47	aashish-VirtualBox org.gnome.Shell.desktop[1383]: > Internal error: Could not resolve keysym In
2021-12-04 00:49:19	Dec 3 14:25:34	aashish-VirtualBox gnome-session-binary[737]: WARNING: Falling back to non-systemd startup proced GDBus.Error:org.freedesktop.DBus.Error.Spawn.ChildExited: Process org.freedesktop.systemd1 exited with status 1
2021-12-04 00:49:19	Dec 3 14:25:34	aashish-VirtualBox gnome-session[737]: gnome-session-binary[737]: WARNING: Falling back to non-sy due to error: GDBus.Error:org.freedesktop.DBus.Error.Spawn.ChildExited: Process org.freedesktop.systemd1 exited w
2021-12-04 00:49:19	Dec 3 14:25:32	aashish-VirtualBox alsactl[641]: alsa-lib main.c:1814:(snd_use_case_mgr_open) error: failed to in configuration -2
2021-12-04 00:49:19	Dec 3 14:25:32	aashish-VirtualBox kernel: [3.783834] EXT4-fs (sda5): re-mounted. Opts: errors=remount-ro. Qu
2021-12-04 00:49:19	Dec 3 14:25:32	aashish-VirtualBox systemd[1]: Condition check resulted in Process error reports when automatic r (watch) being skipped.

To check the graphs, we can simply click on graph as see the graphs as follows;

