

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

Installing zabbix agent in the same host(Zabbix-server)

sudo apt install zabbix-agent

```
bibek@ubuntu-zabbix:~$ sudo apt install zabbix-agent
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  zabbix-agent
0 upgraded, 1 newly installed, 0 to remove and 23 not upgraded.
Need to get 210 kB of archives.
After this operation, 843 kB of additional disk space will be used.
Get:1 http://repo.zabbix.com/zabbix/5.0/ubuntu focal/main amd64 zabbix-agent
Fetched 210 kB in 2s (102 kB/s)
Selecting previously unselected package zabbix-agent.
(Reading database ... 178657 files and directories currently installed.)
Preparing to unpack .../zabbix-agent_1%3a5.0.18-1+focal_amd64.deb ...
Unpacking zabbix-agent (1:5.0.18-1+focal) ...
Setting up zabbix-agent (1:5.0.18-1+focal) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for systemd (245.4-4ubuntu3.13) ...
bibek@ubuntu-zabbix:~$ cd /etc/zabbix/
bibek@ubuntu-zabbix:/etc/zabbix$ ls
apache.conf  web  zabbix_agentd.conf  zabbix_agentd.d  zabbix_server.conf
```

Configuring Zabbix agent configuration

sudo vi /etc/zabbix/zabbix_agentd.conf

ServerActive=192.168.1.147

Hostname=ubuntu-zabbix

Restarting zabbix-agent service

sudo systemctl restart zabbix-agent.service

Configuration >> Host >> Create Host

Give the **host-name** same as we have given in the configuration file

Select Groups - **Linux Servers**

Interfaces - Agent <IP> - for Active Check Port - 10051

Host Templates IPMI Tags Macros Inventory Encryption

* Host name

Visible name

* Groups
type here to search

* Interfaces

Type	IP address	DNS name	Connect to	Port	Default
Agent	<input type="text" value="192.168.1.147"/>	<input type="text"/>	<input type="button" value="IP"/> <input type="button" value="DNS"/>	<input type="text" value="10051"/>	<input checked="" type="radio"/> Remove

[Add](#)

Description

Monitored by proxy

Enabled ☒

Selecting Template - Template OS Linux by Zabbix agent active

Host Templates IPMI Tags Macros Inventory Encryption

Linked templates

Name	Action
------	--------

Link new templates

type here to search

After creating host

<input type="checkbox"/>	Name ▲	Applications	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates	Status	Availability	Agent encryption
<input type="checkbox"/>	ubuntu-zabbix	Applications 15	Items 63	Triggers 22	Graphs 13	Discovery 3	Web	192.168.1.147:10051		Template OS Linux by Zabbix agent active (Template Module Linux block devices by Zabbix agent active, Template Module Linux CPU by Zabbix agent active, Template Module Linux filesystems by Zabbix	Enabled	ZBX SNMP JMX IPMI	NONE

Giving access to Zabbix user to read log of syslog

Syslog is accessed (read) by adm group

Adding Zabbix user to adm group

sudo usermod -aG adm zabbix

```

bibek@ubuntu-zabbix:/var/log$ cat /etc/passwd | grep zabbix
zabbix:x:132:140::/var/lib/zabbix/:/usr/sbin/nologin
bibek@ubuntu-zabbix:/var/log$ sudo usermod -aG adm zabbix
[sudo] password for bibek:
bibek@ubuntu-zabbix:/var/log$ |||

```

Restarting the zabbix-agent service

sudo systemctl restart zabbix-agent.service

Checking whether zabbix can access syslog or not

sudo -H -u zabbix bash -c 'tail -f /var/log/syslog'

```

bibek@ubuntu-zabbix:/var/log$ sudo systemctl restart zabbix-agent.service
bibek@ubuntu-zabbix:/var/log$ sudo -H -u zabbix bash -c 'tail -f /var/log/syslog'
Dec  2 22:13:38 ubuntu-zabbix whoopsie[766]: [22:13:38] online
Dec  2 22:13:47 ubuntu-zabbix systemd[1]: NetworkManager-dispatcher.service: Succeeded.
Dec  2 22:17:01 ubuntu-zabbix CRON[4190]: (root) CMD ( cd / && run-parts --report /etc/cron.hourly)
Dec  2 22:27:07 ubuntu-zabbix systemd[1]: Stopping Zabbix Agent...
Dec  2 22:27:07 ubuntu-zabbix systemd[1]: zabbix-agent.service: Succeeded.
Dec  2 22:27:07 ubuntu-zabbix systemd[1]: Stopped Zabbix Agent.
Dec  2 22:27:07 ubuntu-zabbix systemd[1]: Starting Zabbix Agent...

```

Here we can see it can fetch syslog through zabbix user

Creating Item to get syslog from ubuntu-host

Configuration >> Hosts >> Items >> **Create Item**

Name - ubuntu-sys-log, **Type** - Zabbix agent (active), **Key** - log[/var/log/syslog,,,,,,,,], **New Application** - Name

Items

All hosts / ubuntu-zabbix Enabled ZBX SNMP JMX IPMI Applications 15 Items 63 Triggers 22 Graphs 13 Discovery rules 3 Web scenarios

Item Preprocessing

* Name

Type

Zabbix agent (active)

* Key

Select

Type of information

Log

* Update interval

Custom intervals

Type	Interval	Period	Action
Flexible	Scheduling	50s	1-7,00:00-24:00

Add

* History storage period

Do not keep history

Storage period

Log time format

New application

Applications

General

Interface enp0s3

Monitoring >> Latest Data >> syslogs (ubuntu sys logs) >> History

ubuntu-zabbix	syslogs (1 item)			
	ubuntu-sys-logs	2021-12-03 00:19:14	Dec 3 00:18:46 ubuntu-za...	History
ubuntu-zabbix	Zabbix raw items (3 items)			
	sda: Disk read time (rate)	2021-12-03 00:23:10	0	-0.02668
	sda: Disk write time (rate)	2021-12-03 00:23:10	0.07842	-0.01859
	sda: Get stats			

We can see the **logs** coming from the **ubuntu-zabbix** server through **zabbix-agent**.

ubuntu-zabbix: ubuntu-sys-logs		View as Values	As plain text
		Zoom out	Last 1 hour
From	now-1h		
To	now		
		Apply	
		Last 2 days Yesterday Today Last 5 minute	
		Last 7 days Day before yesterday Today so far Last 15 minu	
		Last 30 days This day last week This week Last 30 minu	
		Last 3 months Previous week This week so far Last 1 hour	
		Last 6 months Previous month This month Last 3 hours	
		Last 1 year Previous year This month so far Last 6 hours	
		Last 2 years This year This year so far Last 12 hours	
Timestamp	Local time	Value	
2021-12-02 22:34:09	Dec 1 01:49:28	metricbeat tracker-miner-f[851]: Unable to get XDG user directory path for special directory &PICTURES. Ignoring this location.	
2021-12-02 22:34:09	Dec 1 01:49:28	metricbeat dbus-daemon[1461]: [session uid=1000 pid=1461] Activating via systemd: service name='org.gtk.vfs.GoaVolumeMonitor' unit='gvfs-goa-volume-monitor.service' requested by ':1.1' (uid=1000 pid=1060 comm="/usr/libexec/tracker-miner-fs " label="unconfined")	
2021-12-02 22:34:09	Dec 1 01:49:28	metricbeat tracker-miner-f[851]: Unable to get XDG user directory path for special directory &MUSIC. Ignoring this location.	
2021-12-02 22:34:09	Dec 1 01:49:28	metricbeat dbus-daemon[1461]: [session uid=1000 pid=1461] Successfully activated service 'org.gtk.vfs.MTfVolumeMonitor'	
2021-12-02 22:34:09	Dec 1 01:49:28	metricbeat tracker-miner-f[851]: Unable to get XDG user directory path for special directory &DOCUMENTS. Ignoring this	

Timestamp	Local time	Value
2021-12-03 00:19:14	Dec 3 00:18:46	ubuntu-zabbix systemd[1]: NetworkManager-dispatcher.service: Succeeded.
2021-12-03 00:19:14	Dec 3 00:18:37	ubuntu-zabbix whoopsie[766]: [00:18:37] online
2021-12-03 00:19:14	Dec 3 00:18:35	ubuntu-zabbix whoopsie[766]: [00:18:35] Found usable connection: /org/freedesktop/Netw
2021-12-03 00:19:14	Dec 3 00:18:35	ubuntu-zabbix whoopsie[766]: [00:18:35] Not a paid data plan: /org/freedesktop/Netw
2021-12-03 00:19:14	Dec 3 00:18:35	ubuntu-zabbix whoopsie[766]: [00:18:35] The default IPv4 route is: /org/freedesktop
2021-12-03 00:19:14	Dec 3 00:18:35	ubuntu-zabbix NetworkManager[569]: <info> [1638470015.7229] manager: NetworkManage
2021-12-03 00:19:14	Dec 3 00:18:35	ubuntu-zabbix systemd[1]: Started Network Manager Script Dispatcher Service.
2021-12-03 00:19:14	Dec 3 00:18:35	ubuntu-zabbix dbus-daemon[568]: [system] Successfully activated service 'org.freede
2021-12-03 00:19:14	Dec 3 00:18:35	ubuntu-zabbix systemd[1]: Starting Network Manager Script Dispatcher Service...