

KB LEVEL: SVR	KB ARTICLE	KB NUMBER: 2019-04
	<i>How to add Windows Agents to Wazuh Server</i>	

KB Category:	Internal		
Author:	Alvinn Medrano	Date:	04/12/2019

Problem Description:	N/A
Symptoms and Cause of the issue:	N/A

Procedure:

Step 1: Log in to Windows server via SSH then enter credentials.

- Username : root
- Password : !D*****5

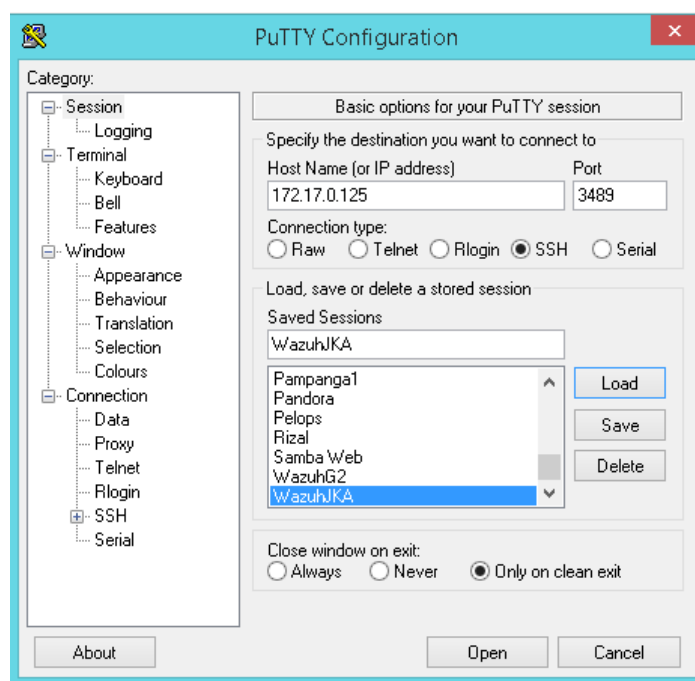


Figure 1



Figure 2

KB LEVEL: SVR	KB ARTICLE	KB NUMBER: 2019-04
	<i>How to add Windows Agents to Wazuh Server</i>	

Step 2: On the manager, run `manage_agents`

```
$ /var/ossec/bin/manage_agents

*****
* Wazuh v2.0 Agent manager.                *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q:
```

Figure 3

Step 3: Press A and Enter to add an agent. You'll be asked for the agent's name (*use the agent hostname or another arbitrary name*), its IP and the agent ID (*you can leave this field empty to auto-assign an ID*).

```
[root@jka-vlin-fim01 ~]# /var/ossec/bin/./manage_agents

*****
* Wazuh v3.8.2 Agent manager.                *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: a

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
    * A name for the new agent: JKA-VWIN-DCD1
    * The IP Address of the new agent: 172.17.0.121
Confirm adding it?(y/n): y
```

Figure 4

KB LEVEL: SVR	KB ARTICLE	KB NUMBER: 2019-04
	<i>How to add Windows Agents to Wazuh Server</i>	

Step 5: Then select E to extract key for an agent. Type in the Agent ID.

```
*****
* Wazuh v3.8.2 Agent manager.                *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: e

Available agents:
  ID: 001, Name: JKA-VWIN-DC01, IP: 172.17.0.121
  ID: 002, Name: JKA-VWIN-WSUS01, IP: 172.17.0.123
Provide the ID of the agent to extract the key (or '\q' to quit): 001
```

Figure 5

Step 5: Copy the key.

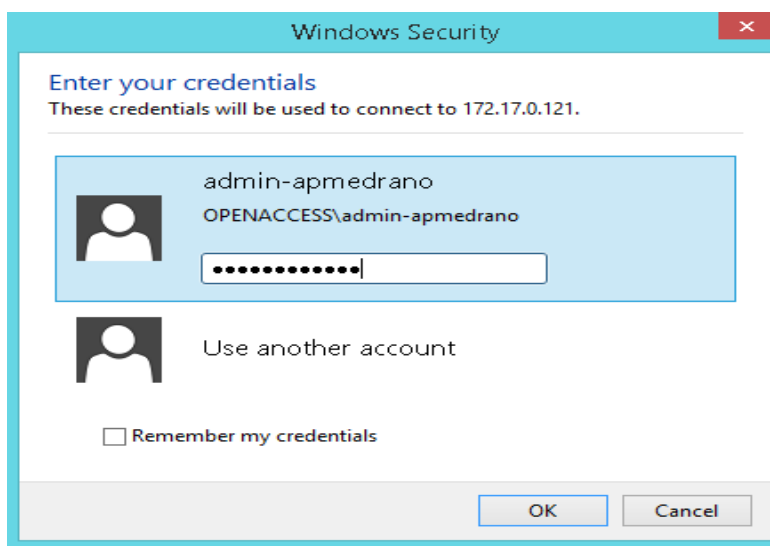
```
Provide the ID of the agent to extract the Key (or '\q' to quit): 001

Agent key information for '001' is:
MDAxIEpLQs1WV01OLURDMDEgMTcyLjE3LjAuMTIxIDAyMjMxOGYyYTMyOWRhNGE4MjJiMGRjYTk5ZmE4
ZjhjZTdkNTUxMjg4OTJhOGM1NzZmODl1YTdiY2MONTk3NWY=

** Press ENTER to return to the main menu.
```

Figure 6

Step 5: After copying RDP The Windows Server and use your admin credentials.



KB LEVEL: SVR	KB ARTICLE	KB NUMBER: 2019-04
	<i>How to add Windows Agents to Wazuh Server</i>	

Figure 7

Step 6: Log in to the file server storage using you administrator account then got the path for the Wazuh Agent executable installer then install to the server .

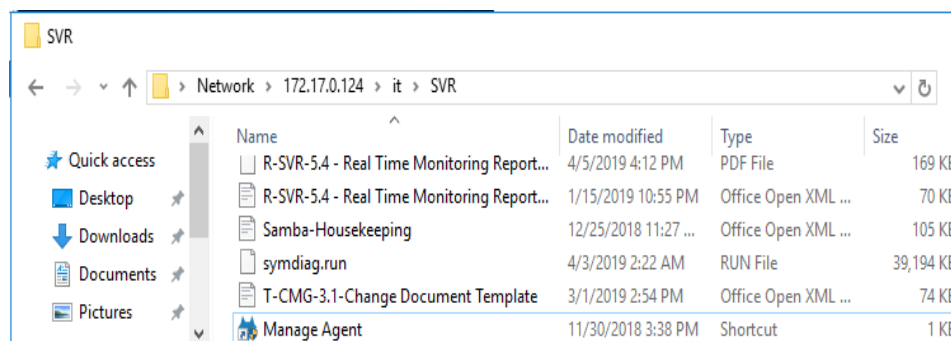


Figure 8

Step 7: Go to windows icon select OSSEC then click on Manage agent.

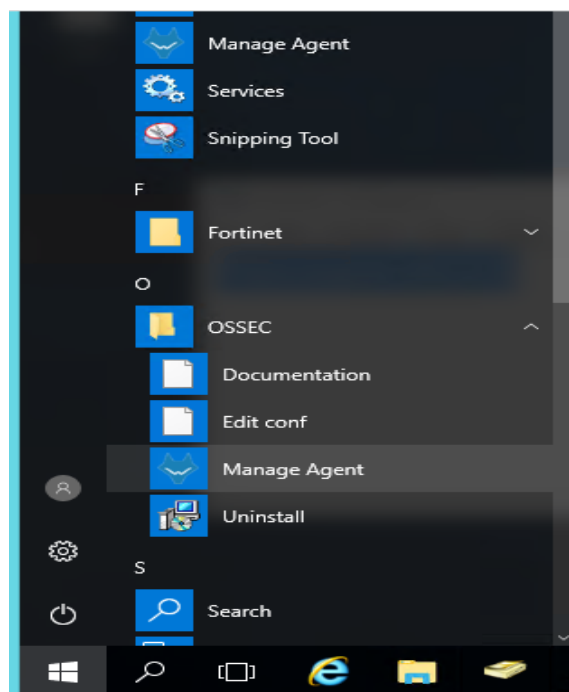


Figure 9

KB LEVEL: SVR	KB ARTICLE	KB NUMBER: 2019-04
	<i>How to add Windows Agents to Wazuh Server</i>	

Step 7: Paste the key to the authentication key then hit save.

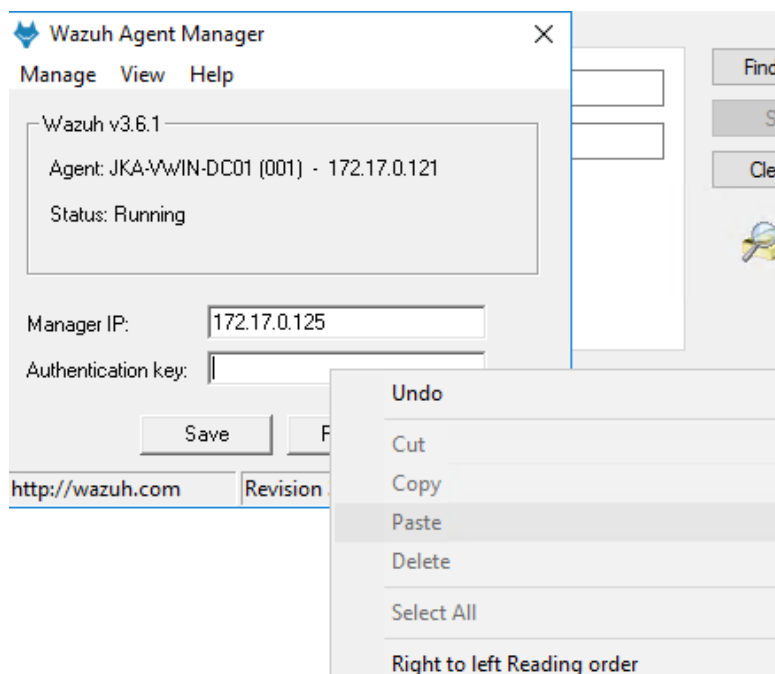


Figure 10

Step 8: After saving go to manage then select restart.

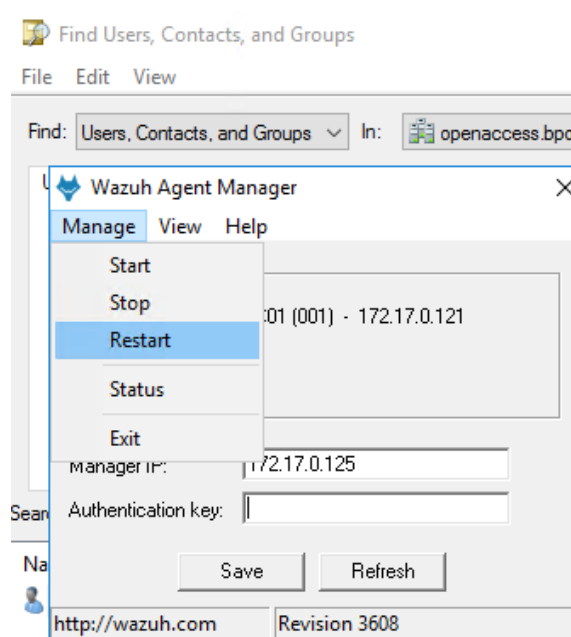


Figure 11

KB LEVEL: SVR	KB ARTICLE	KB NUMBER: 2019-04
	<i>How to add Windows Agents to Wazuh Server</i>	

Step 9: Go back to SSH 172.17.0.125 and execute the command below.

```
> service wazuh-manager restart
> /var/ossec/bin/ossec-control restart
```

Verification:

Step 1: Go to the <http://172.17.0.125:5601> in the browser and select Wazuh.

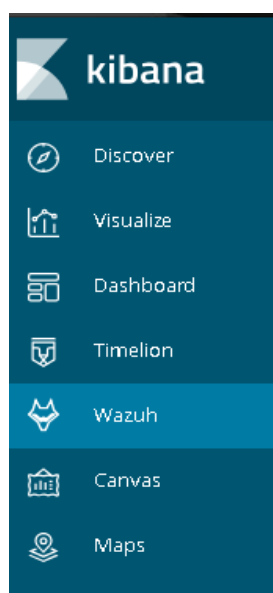


Figure 12

Step 1: Select agents then hit refresh to update the agents list.

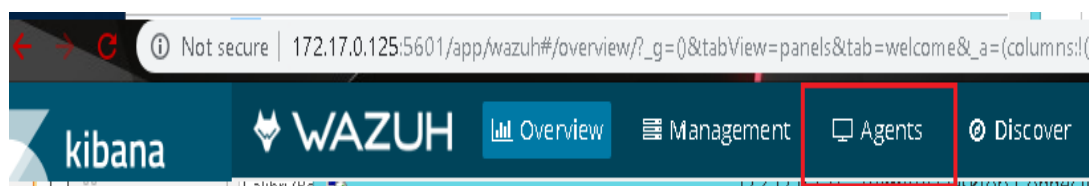


Figure 13

KB LEVEL: SVR	KB ARTICLE	KB NUMBER: 2019-04
	<i>How to add Windows Agents to Wazuh Server</i>	

Step 1: Agent are now added to Wazuh.

The screenshot displays the Wazuh Kibana interface. The top navigation bar includes links for Overview, Management, Agents, Discover, and Dev tools. The left sidebar contains icons for Discover, Visualize, Dashboard, Timeline, Wazuh, Canvas, Maps, and Machine Learning. The main content area is titled 'WAZUH' and shows the 'Agents' page. It features a status summary with 'Active' agents (2) and 'Disconnected' agents (0), along with 'Never connected' (0) and 'Agents coverage' (100.00%). Below this is a search bar and a table of agents. The table has columns for ID, Name, IP, Status, Group, OS name, OS version, Version, Registration date, Last keep alive, and Actions. One agent is listed with ID 001, Name JKA-VWIN-DC01, IP 172.17.0.121, Status Active, Group default, OS name Microsoft Windows Server..., OS version 10.0.14393, Wazuh version v3.6.1, Registration date 2019-04-12 06:57:11, and Last keep alive 2019-04-12 13:34:34.

Figure 14