How to Install Winlogbeat

Task. Install Winlogbeat.

Purpose. Winlogbeat is one method of shipping Windows events from a Windows Event Collector (WEC) server to an Elastic-based Security Incident and Event Management (SIEM) server like Security Onion (SO).

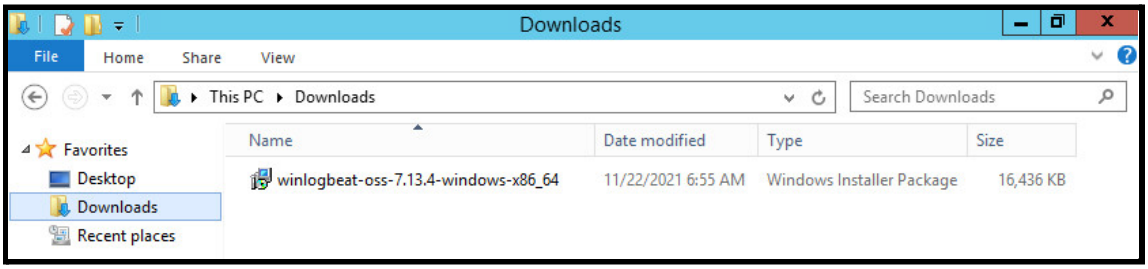
Conditions. You have access and administrator privileges to a WEC server. You have access to the correct version of Winlogbeat. You have access and administrator privileges to a SO Manager Node.

Standard. You were able to install Winlogbeat.

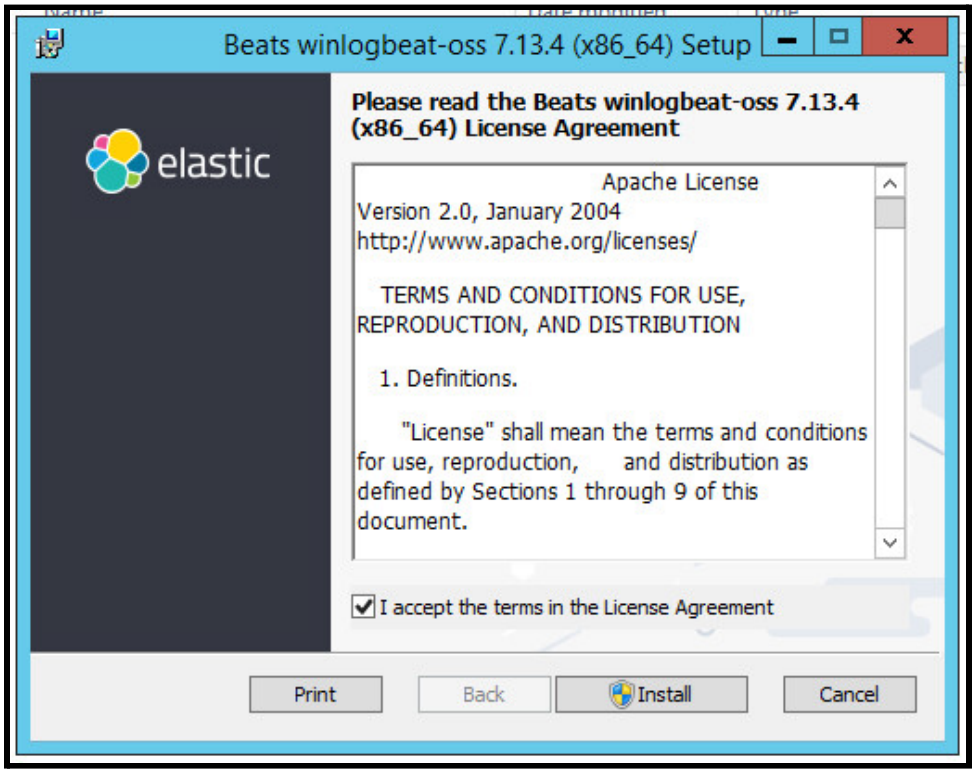
Step 1. Login to the SO Manager Node using your administrator account. Type “sudo so-allow” and provide your password when prompted. Type the letter “b” and press “Enter.” Type the IP address of your WEC server and press “Enter.” Logoff your SO Manager Node.

```
[victorfernandez@evilcorpids1 ~]$ sudo so-allow
[sudo] password for victorfernandez:
This program allows you to add a firewall rule to allow connections from a new I
P address.

Choose the role for the IP or Range you would like to add

[a] - Analyst - ports 80/tcp and 443/tcp
[b] - Logstash Beat - port 5044/tcp
[e] - Elasticsearch REST API - port 9200/tcp
[f] - Strelka frontend - port 57314/tcp
[o] - Osquery endpoint - port 8090/tcp
[s] - Syslog device - 514/tcp/udp
[w] - Wazuh agent - port 1514/tcp/udp
[p] - Wazuh API - port 55000/tcp
[r] - Wazuh registration service - 1515/tcp

Please enter your selection:
b
Enter a single ip address or range to allow (example: 10.10.10.10 or 10.10.0.0/1
6):
192.168.3.202
Adding 192.168.3.202 to the beats_endpoint role. This can take a few seconds
```

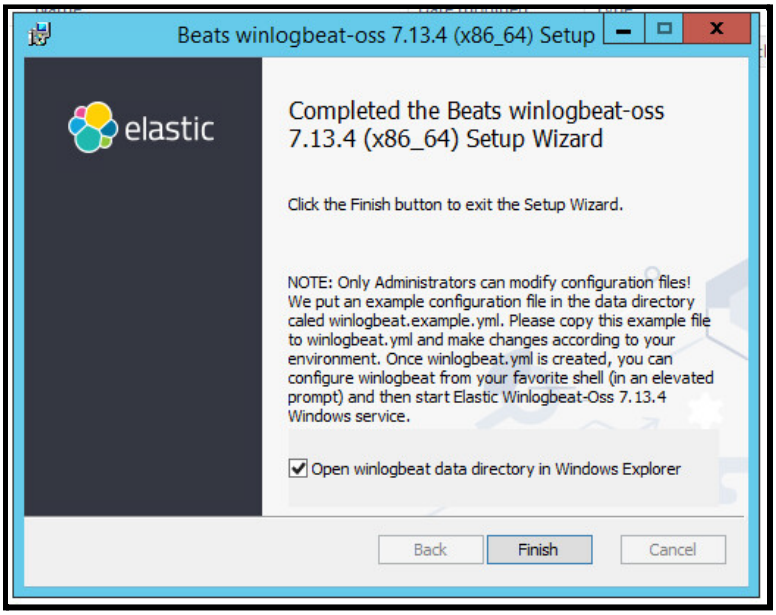
Step 2. Login to the WEC server using your administrator account. Download Winlogbeat to the “Downloads” folder.



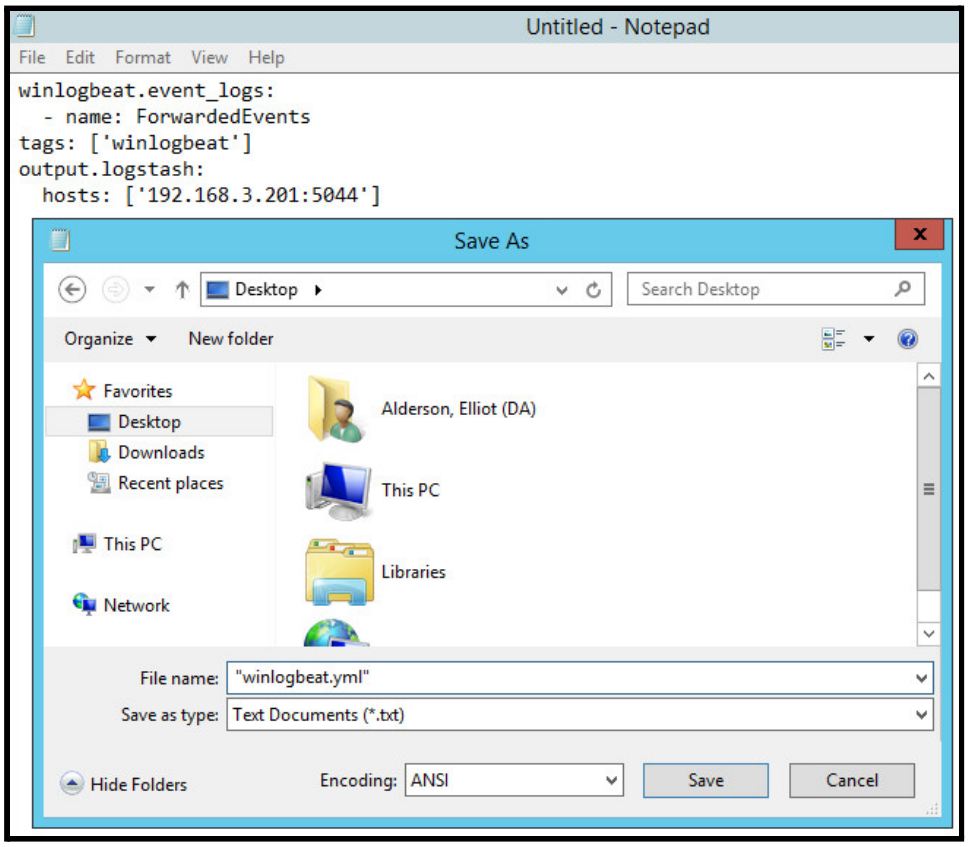
Step 3. Double-click the Winlogbeat Windows Installer Package to execute it. Click “I accept the terms in the License Agreement” and click “Install.”



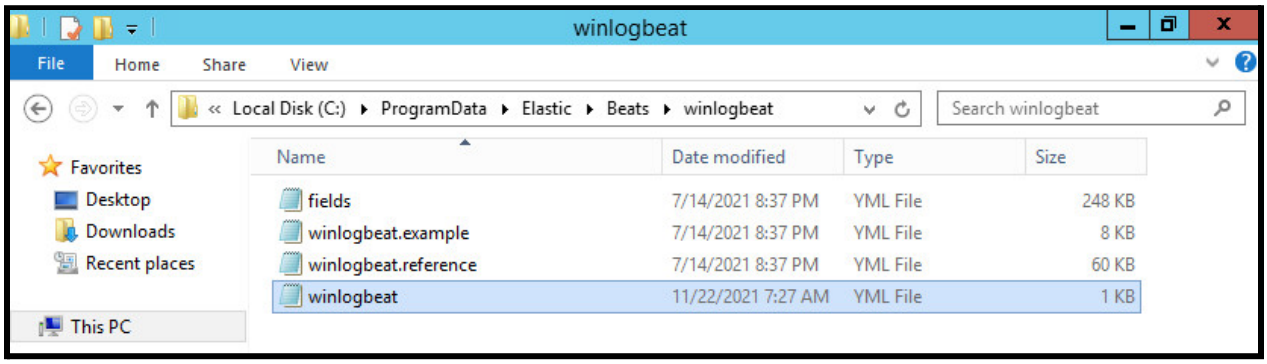
Step 4. Click “Open winlogbeat data directory in Windows Explorer” and click “Finish.”



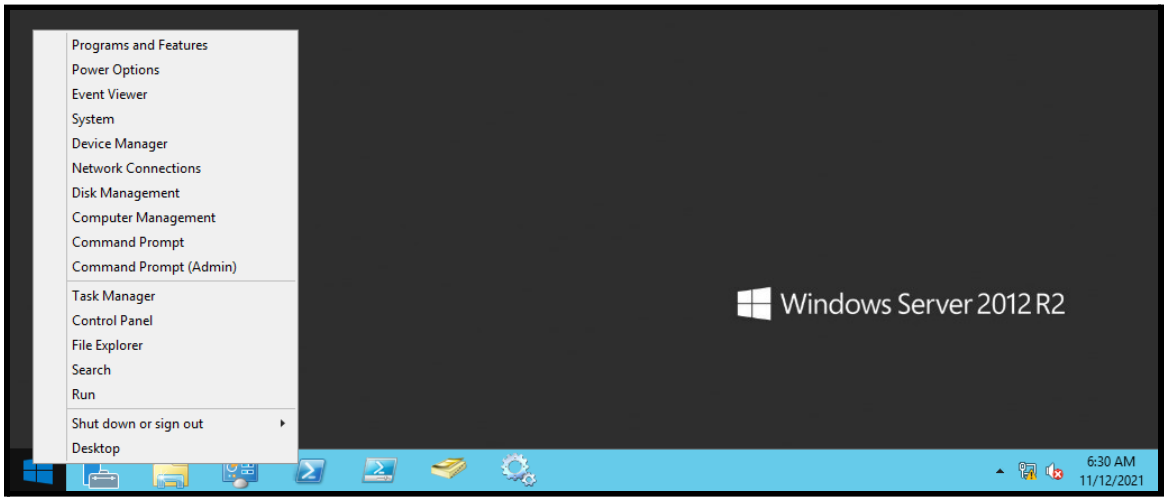
Step 5. Open “Notepad” and type the syntax shown below (replace the IP address with your SO Manager Node’s IP address). Save this file using the filename “winlogbeat.yml.”



Step 6. Copy/paste the file created in the previous step to the “winlogbeat” directory under the following path: “C:\ProgramData\Elastic\Beats\winlogbeat.”



Step 7. Right-click on the Windows icon in the bottom-left corner and select “Command Prompt (Admin).”



Step 8. Type “net start winlogbeat.”