Winlogbeat setup steps:

Steps:

1. Download winlogbeat : https://www.elastic.co/downloads/beats/winlogbeat
2. From Powershell:

```
cd 'C:\Program Files\Winlogbeat'
```

```
.\install-service-winlogbeat.ps1
```

3. Connect to elasticstack:
   Edit the winlogbeat.yml with below

```
output.elasticsearch:
  hosts: ["https://myEShost:9200"]
  username: "winlogbeat_internal"
  password: "YOUR_PASSWORD"
  ssl:
    enabled: true
    ca_trusted_fingerprint:
"b9a10bbe64ee9826abeda6546fc988c8bf798b41957c33d05db736716513dc9c"
```

If you plan to use our pre-built Kibana dashboards, configure the Kibana endpoint. Skip this step if Kibana is running on the same host as Elasticsearch.

```
  setup.kibana:
    host: "mykibanahost:5601"
    username: "my_kibana_user"
    password: "{pwd}"
```

Under `winlogbeat.event_log`, specify a list of event logs to monitor. By default, Winlogbeat monitors application, security, and system logs.

```
winlogbeat.event_logs:
  - name: Application
  - name: Security
  - name: System
```

After you save your configuration file, test it with the following command.

```
PS C:\Program Files\Winlogbeat> .\winlogbeat.exe test config -c
.\winlogbeat.yml -e
```

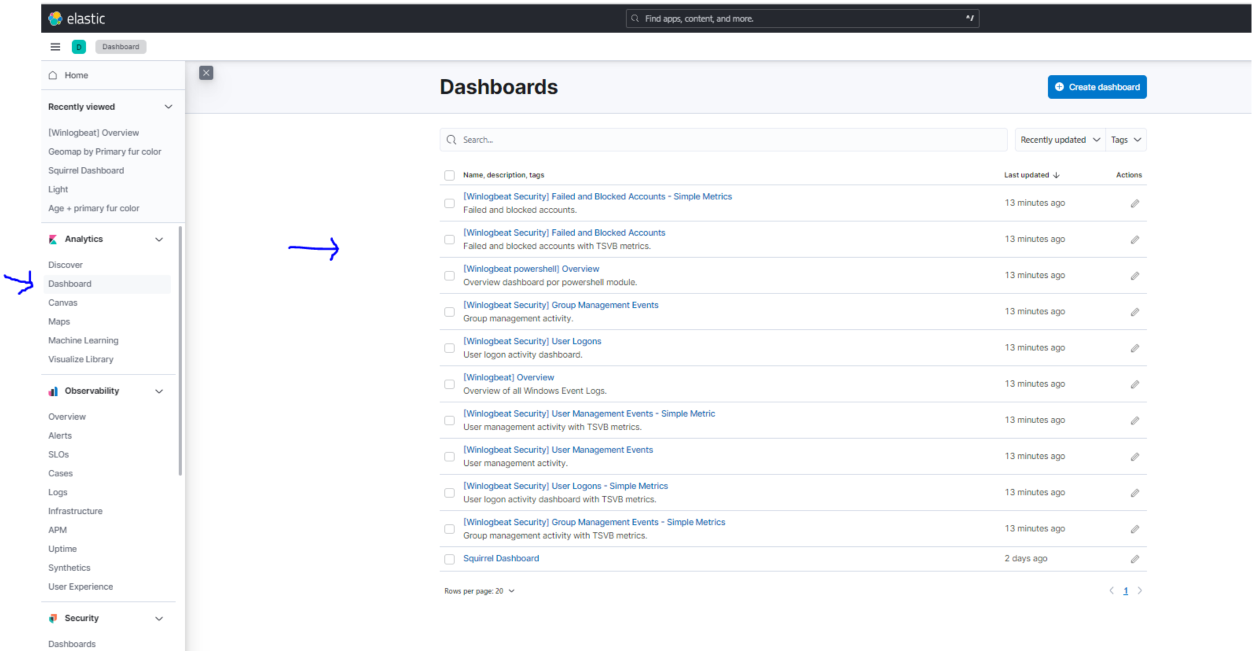
Winlogbeat comes with predefined assets for parsing, indexing, and visualizing your data. To load these assets:

1. Make sure the user specified in `winlogbeat.yml` is [authorized to set up Winlogbeat]().
2. From the installation directory, run:

```
PS > .\winlogbeat.exe setup -e
```

```
Start-Service winlogbeat
```

Check kibana for inbuilt dashboards



Dashboards

□	Name, description, tags	Last updated ↓	Actions
□	[Winlogbeat Security] Failed and Blocked Accounts - Simple Metrics Failed and blocked accounts.	13 minutes ago	✎
□	[Winlogbeat Security] Failed and Blocked Accounts Failed and blocked accounts with TSVB metrics.	13 minutes ago	✎
□	[Winlogbeat powershell] Overview Overview dashboard por powershell module.	13 minutes ago	✎
□	[Winlogbeat Security] Group Management Events Group management activity.	13 minutes ago	✎
□	[Winlogbeat Security] User Logons User logon activity dashboard.	13 minutes ago	✎
□	[Winlogbeat] Overview Overview of all Windows Event Logs.	13 minutes ago	✎
□	[Winlogbeat Security] User Management Events - Simple Metric User management activity with TSVB metrics.	13 minutes ago	✎
□	[Winlogbeat Security] User Management Events User management activity.	13 minutes ago	✎
□	[Winlogbeat Security] User Logons - Simple Metrics User logon activity dashboard with TSVB metrics.	13 minutes ago	✎
□	[Winlogbeat Security] Group Management Events - Simple Metrics Group management activity with TSVB metrics.	13 minutes ago	✎
□	Squirrel Dashboard	2 days ago	✎

Metric Beat installation Steps:

1. Download the metricbeat from here: https://www.elastic.co/downloads/beats/metricbeat

2. Run powershell as admin and perform below:

```
3. PS > cd 'C:\Program Files\Metricbeat'
4. PS C:\Program Files\Metricbeat> .\install-service-metricbeat.ps1
```

3. Connect to elasticsearch:

```
4. output.elasticsearch:
5.   hosts: ["https://myEShost:9200"]
6.   username: "metricbeat_internal"
7.   password: "YOUR_PASSWORD"
8.   ssl:
9.     enabled: true
10.        ca_trusted_fingerprint:
   "b9a10bbe64ee9826abeda6546fc988c8bf798b41957c33d05db736716513dc9c"
```

If you plan to use our pre-built Kibana dashboards, configure the Kibana endpoint. Skip this step if Kibana is running on the same host as Elasticsearch.

```
  setup.kibana:
    host: "mykibanahost:5601"
    username: "my_kibana_user"
    password: "{pwd}"
```

5. Enable and setup metric collection modules:

```
6. PS > .\metricbeat.exe modules list
7. PS > .\metricbeat.exe modules enable nginx
```

6. Metricbeat comes with predefined assets for parsing, indexing, and visualizing your data. To load these assets:

   1. Make sure the user specified in `metricbeat.yml` is authorized to set up Metricbeat.
   2. From the installation directory, run:

      DEB RPM MacOS Linux Windows

```
PS > .\metricbeat.exe setup -e
```

Before starting Metricbeat, modify the user credentials in `metricbeat.yml` and specify a user who is authorized to publish events.

To start Metricbeat, run:

DEB RPM MacOS Linux Windows

```
PS C:\Program Files\metricbeat> Start-Service metricbeat
```

View in kibana:

File Beat installation Steps:

1. Download the Filebeat from here : https://www.elastic.co/downloads/beats/filebeat
2. From the PowerShell prompt, run the following commands to install Filebeat as a Windows service:

```
PS > cd 'C:\Program Files\Filebeat'
PS C:\Program Files\Filebeat> .\install-service-filebeat.ps1
```

3. Set the host and port where Filebeat can find the Elasticsearch installation, and set the username and password of a user who is authorized to set up Filebeat. For example:

```
output.elasticsearch:
  hosts: ["https://myEShost:9200"]
  username: "filebeat_internal"
  password: "YOUR_PASSWORD"
  ssl:
    enabled: true
    ca_trusted_fingerprint: "b9a10bbe64ee9826abeda6546fc988c8bf798b41957c33d05db736716513dc9c"
```

4. If you plan to use our pre-built Kibana dashboards, configure the Kibana endpoint. Skip this step if Kibana is running on the same host as Elasticsearch.

```
setup.kibana:
    host: "mykibanahost:5601"
    username: "my_kibana_user"
    password: "{pwd}"
```

5. Collect log data: Identify the modules you need to enable. To see a list of available modules, run:

   DEB RPM MacOS Linux Windows

```
PS > .\filebeat.exe modules list
```

6. From the installation directory, enable one or more modules. For example, the following command enables the `nginx` module config:

   DEB RPM MacOS Linux Windows

```
PS > .\filebeat.exe modules enable nginx
```

7. In the module config under `modules.d`, change the module settings to match your environment. You must enable at least one fileset in the module. **Filesets are disabled by default.**

For example, log locations are set based on the OS. If your logs aren't in default locations, set the `paths` variable:

```
- module: nginx
  access:
    enabled: true
    var.paths: ["/var/log/nginx/access.log*"]
```

8. Filebeat comes with predefined assets for parsing, indexing, and visualizing your data. To load these assets:

1. Make sure the user specified in `filebeat.yml` is authorized to set up Filebeat.
2. From the installation directory, run:

   DEB RPM MacOS Linux Windows

```
PS > .\filebeat.exe setup -e
```

9. Before starting Filebeat, modify the user credentials in `filebeat.yml` and specify a user who is authorized to publish events.

To start Filebeat, run:

DEB RPM MacOS Linux Windows

```
PS C:\Program Files\filebeat> Start-Service filebeat
```

10. View data in kibana