WinLogBeat for Dummies

How to install winlogbeat

Necessary Skills: Powershell file manipulation, general powershell usage, notepad, vim

Goal: Send complete logs to a designated host. Search up important events with Kibana.

Steps:

Below are the instructions for installing and setting up winlogbeat

---------WITH CHOCOLATEY-------

1. Enter the command for installing winlogbeat:
   ```
   PS C:\ choco install winlogbeat
   ```

2. Make your way to where winlogbeat is installed
   ```
   PS C:\ cd C:\ProgramData\chocolatey\lib\winlogbeat\tools
   ```

3. Now you should be able to edit the `winlogbeat.yml`
   ```
   PS C:\ProgramData\chocolatey\lib\winlogbeat\tools> vim
   winlogbeat.yml
   ```

4. Hit `i` to enter insert mode in vim
5. Find the section labeled “#----------ElasticSearch output----------”
6. Comment the output.elastic and the host line.
7. Find the section labeled “#----------Logstash output----------”
8. Uncomment the “output.logstash” line
9. The host “localhost:” section should be replaced with <name of server>:<port>
10. Hit `escape` to exit insert mode, and then `:wq` to save and exit
11. Finally back on powershell, type the command to start winlogbeat

    ```
    PS C:\> Start-Service winlogbeat
    ```

Steps:

Below are the instructions for installing winlogbeat

---------WITHOUT CHOCOLATEY--

These steps use Powershell with administrative permissions.

1. Download the binary:

```
> iwr

‘https://artifacts.elastic.co/downloads/beats/winlogbeat/wi
nlogbeat-7.4.1-windows-x86_64.zip’ -OutFile winbeat.zip
```

If this fails with an error “Could not create secure TLS connection, try:

```
> [Net.ServicePointManager]::SecurityProtocol = "tls12,

tls11, tls"
```

2. Run commands:
   ```
   > Expand-Archive winbeat.zip winlogbeat
   cd winlogbeat
   mv winlogbeat-7.4.1-windows-x86_64 ‘C:\Program
        Files\Winlogbeat`
   ```
3. Run command:
   ```
   > cd `C:\Program Files\Winlogbeat`
   >/install-service-winlogbeat.ps1
   ```
4. Edit the config file:
   ```
   > Notepad winlogbeat.yml
   ```
   Note: it may be a Bad Idea to edit this with notepad, as
   notepad breaks the line endings. Try vscode or notepad++, nano if using SSH.
5. Under the “Elasticsearch output” section, you must fill in the “hosts”, username, and password
6. Run command:

```
Start-Service winlogbeat
```

7. You should now be sending logs to ELK.

Debug by looking at the logs folder in the Winlogbeat install directory.

Kibana Searches

So you got windows event logs forwarded into your ELK stack? Good job! Here are some events to watch out for.

Note that you can also look through logs by using Event Viewer from a domain-joined workstation.

Administrator Logins

Event 4672 is an administrator login. However, each computer in a domain has a service account that will automatically login every so often. Filter for administrative logins by specific users:
> (winlog.event_id:4672 AND user.name:<user name>)

New User Sessions

When a new user session starts, it generates an event with a code of 4674.

SSH Logins
> (winlog.event_data.LogonType:8 AND winlog.event_id:4624)
The LogonType of 8 is used for SSH, and a few other things

GUI
When the screen is unlocked, event type 7 is created
> (winlog.event_data.LogonType:7 AND winlog.event_id:4624)
If the field Network Information: Source Network Address is present in the log message, that indicates an RDP login.

Error Name	ID
4740	Account Lockouts
4728, 4732, 4756	User Added to Privileged Groups
4724	Successful Account Login
4625	Failed User Account Login
4648	Account Login with Explicit Credentials

System Changes/Firewall Changes

Updates Installed
> (winlog.event_id: 19)

Firewall Changes

Error Name	ID
2004	Firewall Rule Add
2005	Firewall Rule Change
2006, 2003	Firewall Rule Deleted

Creating An Alert

- Go to Alerting\Monitors\Create monitor
- Define monitor using extraction query and set the index equal to ‘logstash-winlogbeat-*’
- For a specific event:

```
{
      "size": 0,
      "query": {
      "match": {
            "event_id":<id>
      }
      }
}
```

To get the event log name in order to tell WinLogBeat to collect a specific event log:

```
Get-WinEvent -ListLog * | Format-List -Property LogName
```

Gets the log name, and then lists them under the winlogbeat config file in the winlogbeat.event_logs section