Send Windows logs to Elastic Stack using Winlogbeat and Sysmon

Original:

<https://kifarunix.com/send-windows-logs-to-elastic-stack-using-winlogbeat-and-sysmon/>

**Intro**

**This document was modified by JJK to allow these ELK system to accept inputs from Windows 7 and Windows Server 2012 PCs via Winlogbeat and Sysmon to display them in Kibana. Some changes for the Windows PCs are covered in the Appendices**

**Install Ubuntu 18.04 LTS**

**Download the server ISO via** [**https://ubuntu.com/download/desktop/thank-you?version=18.04.3&architecture=amd64**](https://ubuntu.com/download/desktop/thank-you?version=18.04.3&architecture=amd64) **We will be installing the VM into a VMware vSphere cluster. Use 2 vCPUs, 8GB RAM, at least 300GB vDisk, and put the VM on the same network (subbet) as PCs.**

**Set Static IP**

#### Ubuntu Server

To configure a static IP address on your Ubuntu 18.04 server you need to modify a relevant netplan network configuration file within /etc/netplan/ directory.

# This file describes the network interfaces available on your system

# For more information, see netplan(5).

network:

version: 2

renderer: networkd

ethernets:

enp0s3:

dhcp4: no

addresses: [192.168.1.158/24]

gateway4: 192.168.1.1

nameservers:

addresses: [8.8.8.8,8.8.4.4]

Once ready apply changes with:

$ sudo netplan apply

In case you run into some issues execute:

$ sudo netplan --debug apply

**Getting Started**

In this guide, we are going to learn how to send Windows logs to Elastic Stack server using Winlogbeat and Sysmon. [Winlogbeat](https://www.elastic.co/guide/en/beats/winlogbeat/current/_winlogbeat_overview.html) is an Elastic Beat that is used to collect windows system application, security, system or hardware events. Sysmon (*System Monitor*) on the other hand is a windows application that is used to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time

In order to visualize and analyze the events collected by Winlogbeat/Sysmon, you need to have setup your Elastic Stack.

Send Windows Logs to Elastic Stack Using Winlogbeat and Sysmon

Install Winlogbeat and Sysmon on Windows 7

In this guide, we are going to use several Windows 7 and a Windows Serever 2012 PC as our Windows systems. Therefore, you need to install both **Winlogbeat** and **Sysmon** on these PCs in order to ship events to Elastic stack server.

Install Winlogbeat on Windows 7

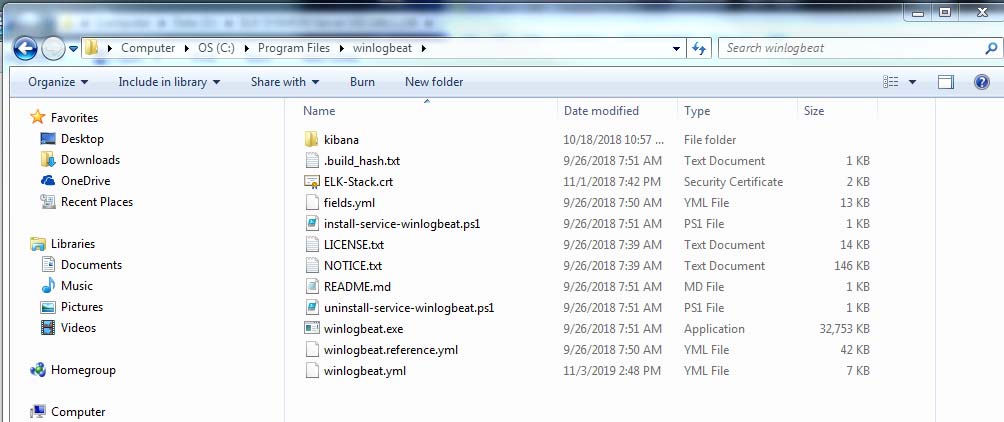
**Perform the below steps on each Windows PC.**

Navigate to Winlogbeat [downloads page](https://artifacts.elastic.co/downloads/beats/winlogbeat/winlogbeat-7.2.0-windows-x86_64.zip) and download Winlogbeat zip file.

Once the download is done, extract the Winlogbeat zipped file, **winlogbeat-7.2.0-windows-x86\_64.zip**.

When you extract, you should get a folder, **winlogbeat-7.2.0-windows-x86\_64**.

Move the **winlogbeat-7.2.0-windows-x86\_64** directory to **C:\Program Files** and rename it to **Winlogbeat**. Your directory should look like as in below:



Next, to install Winlogbeat on Windows 7, you need to execute the **install-service-winlogbeat.ps1** installation script. Hence, open the **Powershell** as the administrator and change to Winlogbeat directory by executing the command below;

cd C:\'Program Files'\Winlogbeat

Next, run the Winlogbeat installer as shown below;

.\install-service-winlogbeat.ps1

If you get the error, **cannot be loaded because the execution of scripts is disabled on this system**, as shown below, you need to enable the script execution.

PS C:\Program Files\Winlogbeat> .\install-service-winlogbeat.ps1

File C:\Program Files\Winlogbeat\install-service-winlogbeat.ps1 cannot be loaded because the execution of scripts is disabled on this system. Please see "get-help about\_signing" for more details.

At line:1 char:33

+ .\install-service-winlogbeat.ps1 <<<<

+ CategoryInfo : NotSpecified: (:) [], PSSecurityException

+ FullyQualifiedErrorId : RuntimeException

As a result, you need to execute the Winlogbeat script with unrestricted execution policy as shown in the command below:

PS C:\Program Files\Winlogbeat> PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-winlogbeat.ps1

Status Name DisplayName

------ ---- -----------

Stopped winlogbeat winlogbeat

Install Sysmon on Windows 7

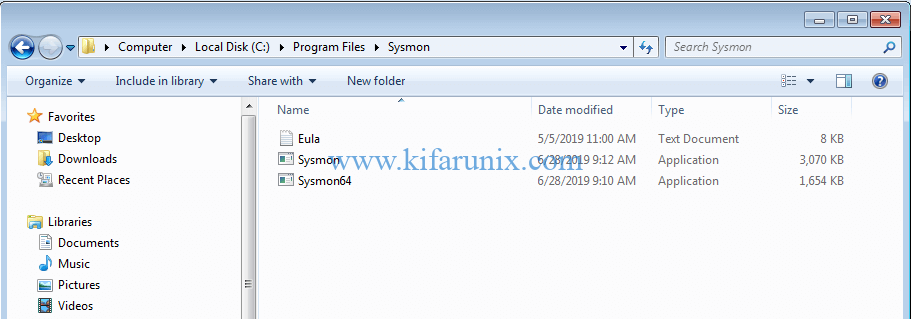
**Perform the below steps on each Windows PC.**

Download Sysmon from the [downloads page](https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon).

Once the download is complete, extract the contents of the zipped file to **C:\Program Files** directory.

**Note: In my case, C:\sysinternals\sysmon\ was created and the PATH variable was changed to include this location/**

Once the extraction is done, your folder should look like as in below;

[](https://kifarunix.com/wp-content/uploads/2019/07/install-sysmon-windows-7.png)

Install Sysmon with md5 and sha256 hashing of process created, log loading of modules and monitoring network connections, open a **CMD** as an administrator and navigate to **C:\Program Files\Sysmon** and execute the command below:

cd C:\Program Files\Sysmon

C:\Program Files\Sysmon> sysmon -i -accepteula -h md5,sha256,imphash -l -n

System Monitor v10.2 - System activity monitor

Copyright (C) 2014-2019 Mark Russinovich and Thomas Garnier

Sysinternals - www.sysinternals.com

Sysmon installed.

SysmonDrv installed.

Starting SysmonDrv.

SysmonDrv started.

Starting Sysmon...

Sysmon started.

Configuring Winlogbeat

The main configuration file for Winlogbeat is **C:\Program Files\Winlogbeat\winlogbeat.yml** with the reference config file being **C:\Program Files\Winlogbeat\winlogbeat.reference.yml**.

My winlogbeat.yml file is listed in Appendix A.

As we are using Logstash, the Elasticsearch output was commented out and Logstash connection addresses was specified.

Winlogbeat configuration checks

Once done with configuration, save the file and run the configuration checks. To run the configuration checks, open Powershell as an administrator and execute the command below:

cd C:\'Program Files'\Winlogbeat

.\winlogbeat.exe test config -c .\winlogbeat.yml -e

If there is no error with the configuration, you should see the **Config Ok**.

...

2019-07-15T14:05:08.164+0300 INFO instance/beat.go:292 Setup Beat: winlogbeat; Version: 7.2.0

2019-07-15T14:05:08.192+0300 INFO [index-management] idxmgmt/std.go:178 Set output.elasticsearch.index t

o 'winlogbeat-7.2.0' as ILM is enabled.

2019-07-15T14:05:08.225+0300 INFO elasticsearch/client.go:166 Elasticsearch url: http://192.168.43.104:9200

2019-07-15T14:05:08.258+0300 INFO elasticsearch/client.go:166 Elasticsearch url: http://192.168.43.105:9200

2019-07-15T14:05:08.290+0300 INFO elasticsearch/client.go:166 Elasticsearch url: http://192.168.43.106:9200

2019-07-15T14:05:08.325+0300 INFO [publisher] pipeline/module.go:97 Beat name: winlogbeat

2019-07-15T14:05:08.356+0300 INFO beater/winlogbeat.go:69 State will be read from and persisted to C:\Program Files\Winlogbeat\data\.winlogbeat.yml

Config OK

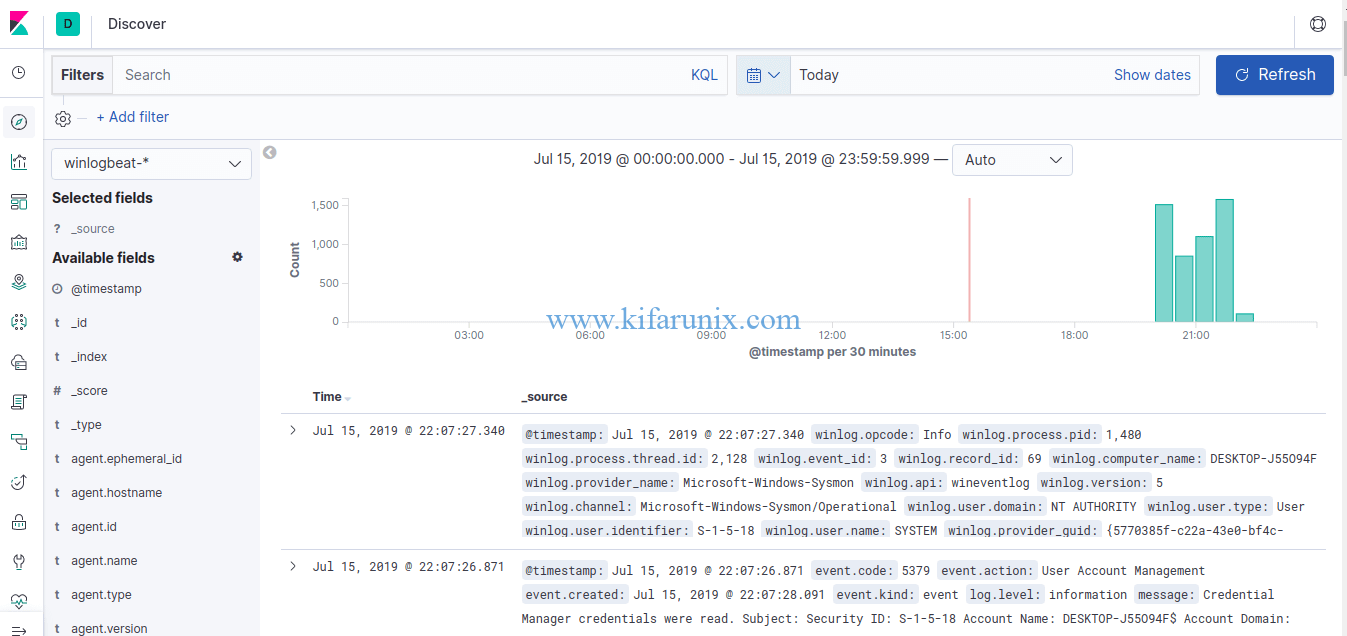
Running Winlogbeat

To start or stop Winlogbeat, navigate to install directory and execute the commands below respectively.

PS C:\Program Files\Winlogbeat> Start-Service winlogbeat

PS C:\Program Files\Winlogbeat> Stop-Service winlogbeat

You can also manage the Winlogbeat from system services. Your Windows events should now be showing up in Kibana:

[](https://kifarunix.com/wp-content/uploads/2019/07/winlogbeat-events.png)

It’s time to time to go to Kibana and create visualizations and dashboards.

That is all on how to send Windows logs to Elastic Stack using Winlogbeat and Sysmon. You can continue to explore Kibana dashboards to analyze your windows events. Enjoy

**Appendix A**

**Logstash Config Files**

**Path C:/Program Files/Winlogbeat/**

**File: winlogbeat.yml:**

###################### Winlogbeat Configuration Example ##########################

# This file is an example configuration file highlighting only the most common

# options. The winlogbeat.reference.yml file from the same directory contains all the

# supported options with more comments. You can use it as a reference.

#

# You can find the full configuration reference here:

# https://www.elastic.co/guide/en/beats/winlogbeat/index.html

#======================= Winlogbeat specific options ==========================

# event\_logs specifies a list of event logs to monitor as well as any

# accompanying options. The YAML data type of event\_logs is a list of

# dictionaries.

#

# The supported keys are name (required), tags, fields, fields\_under\_root,

# forwarded, ignore\_older, level, event\_id, provider, and include\_xml. Please

# visit the documentation for the complete details of each option.

# https://go.es.io/WinlogbeatConfig

#

# Modified by JJK 10/27/18 - based on https://www.syspanda.com/index.php/2017/02/07/setting-up-elasticsearch-5-x-sending-windows-logs-using-winlogbeat-5-x/

winlogbeat.event\_logs:

- name: Application

event\_id: 1000,1002,1001

ignore\_older: 72h

- name: Security

event\_id: 4740,4728,4732,4756,4735,4724,4625,4648,1102,4624,5038,6281

ignore\_older: 72h

- name: "Microsoft-Windows-TaskScheduler/Operational"

event\_id: 141,106,142,140,129

ignore\_older: 72h

- name: System

event\_id: 6,104,102,1102,4719,6005,7022,7023,7024,7025,7026,7031,7032,7034,7045,4697,7022,7023

ignore\_older: 72h

- name: Microsoft-Windows-Sysmon/Operational

ignore\_older: 72h

- name: "Microsoft-Windows-TerminalServices-RDPClient/Operational,Microsoft-Windows-TerminalServices-LocalSessionManager/Admin,Microsoft-Windows-TerminalServices-LocalSessionManager/Operational"

event\_id: 23,24,25,1102

ignore\_older: 72h

- name: "Microsoft-Windows-Windows Firewall With Advanced Security/ConnectionSecurity,Microsoft-Windows-Windows Firewall With Advanced Security/ConnectionSecurityVerbose,Microsoft-Windows-Windows Firewall With Advanced Security/Firewall,Microsoft-Windows-Windows Firewall With Advanced Security/FirewallVerbose,Microsoft-Windows-Windows Firewall With Advanced Security/Network Isolation Operational"

event\_id: 2004,2005,2006,2033,2009

ignore\_older: 72h

- name: "Microsoft-Windows-WindowsUpdateClient/Operational"

event\_id: 20,24,25,31,34,35

ignore\_older: 72h

#==================== Elasticsearch template setting ==========================

setup.template.settings:

index.number\_of\_shards: 3

#index.codec: best\_compression

#\_source.enabled: false

#================================ General =====================================

# The name of the shipper that publishes the network data. It can be used to group

# all the transactions sent by a single shipper in the web interface.

#name:

# The tags of the shipper are included in their own field with each

# transaction published.

#tags: ["service-X", "web-tier"]

# Optional fields that you can specify to add additional information to the

# output.

#fields:

# env: staging

#============================== Dashboards =====================================

# These settings control loading the sample dashboards to the Kibana index. Loading

# the dashboards is disabled by default and can be enabled either by setting the

# options here, or by using the `-setup` CLI flag or the `setup` command.

#setup.dashboards.enabled: false

# The URL from where to download the dashboards archive. By default this URL

# has a value which is computed based on the Beat name and version. For released

# versions, this URL points to the dashboard archive on the artifacts.elastic.co

# website.

#setup.dashboards.url:

#============================== Kibana =====================================

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.

# This requires a Kibana endpoint configuration.

setup.kibana:

# Kibana Host

# Scheme and port can be left out and will be set to the default (http and 5601)

# In case you specify and additional path, the scheme is required: http://localhost:5601/path

# IPv6 addresses should always be defined as: https://[2001:db8::1]:5601

#host: "localhost:5601"

#============================= Elastic Cloud ==================================

# These settings simplify using winlogbeat with the Elastic Cloud (https://cloud.elastic.co/).

# The cloud.id setting overwrites the `output.elasticsearch.hosts` and

# `setup.kibana.host` options.

# You can find the `cloud.id` in the Elastic Cloud web UI.

#cloud.id:

# The cloud.auth setting overwrites the `output.elasticsearch.username` and

# `output.elasticsearch.password` settings. The format is `<user>:<pass>`.

#cloud.auth:

#================================ Outputs =====================================

# Configure what output to use when sending the data collected by the beat.

#-------------------------- Elasticsearch output ------------------------------

#output.elasticsearch:

# Array of hosts to connect to.

# hosts: ["192.168.1.17:9200"]

# Optional protocol and basic auth credentials.

#protocol: "https"

#username: "elastic"

#password: "changeme"

#----------------------------- Logstash output --------------------------------

output.logstash:

# The Logstash hosts

hosts: ["192.168.1.158:5044"]

# Optional SSL. By default is off.

# List of root certificates for HTTPS server verifications

#ssl.certificate\_authorities: ["/etc/pki/root/ca.pem"]

ssl.certificate\_authorities: ["C:/Program Files/winlogbeat/ELK-Stack.crt"]

# Certificate for SSL client authentication

#ssl.certificate: "/etc/pki/client/cert.pem"

# Client Certificate Key

#ssl.key: "/etc/pki/client/cert.key"

#================================ Logging =====================================

# Sets log level. The default log level is info.

# Available log levels are: error, warning, info, debug

#logging.level: debug

# At debug level, you can selectively enable logging only for some components.

# To enable all selectors use ["\*"]. Examples of other selectors are "beat",

# "publish", "service".

#logging.selectors: ["\*"]

#============================== Xpack Monitoring ===============================

# winlogbeat can export internal metrics to a central Elasticsearch monitoring

# cluster. This requires xpack monitoring to be enabled in Elasticsearch. The

# reporting is disabled by default.

# Set to true to enable the monitoring reporter.

#xpack.monitoring.enabled: false

# Uncomment to send the metrics to Elasticsearch. Most settings from the

# Elasticsearch output are accepted here as well. Any setting that is not set is

# automatically inherited from the Elasticsearch output configuration, so if you

# have the Elasticsearch output configured, you can simply uncomment the

# following line.

#xpack.monitoring.elasticsearch: