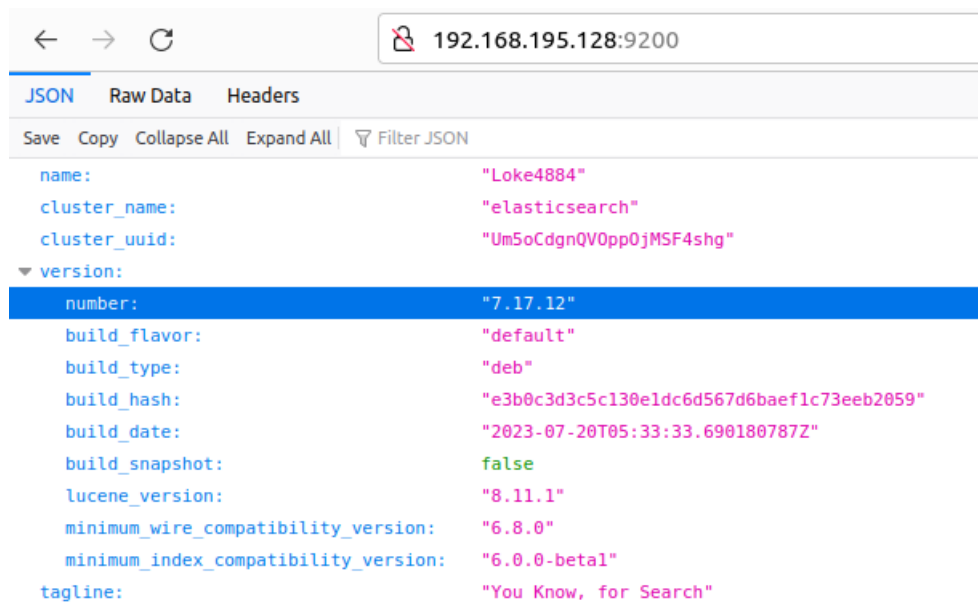


Download winlogbeat version which matches to yours elasticsearch version



Elasticsearch version : 7.17.12

Hence download only winlogbeat version : 7.17.12

<https://www.elastic.co/downloads/past-releases/winlogbeat-7-17-12>

1. Download the Winlogbeat zip file
2. Extract the contents into C:\Program Files.
3. Rename the winlogbeat-<version> directory to Winlogbeat.
4. Open a PowerShell prompt as an Administrator (right-click on the PowerShell icon and select Run As Administrator).

Open Powershell in Administration mode

Go to path where WinLogbeat is saved

cd "C:\Program Files\Winlogbeat"

```
PS C:\WINDOWS\system32> cd "C:\Program Files\Winlogbeat"
PS C:\Program Files\Winlogbeat>
```

Install winlogbeat

.\install-service-winlogbeat.ps1

```
PS C:\Program Files\Winlogbeat> .\install-service-winlogbeat.ps1
.\install-service-winlogbeat.ps1 : File C:\Program Files\Winlogbeat\install-service-winlogbeat.ps1 cannot be loaded. The file C:\Program Files\Winlogbeat\install-service-winlogbeat.ps1 is not digitally signed.
You cannot run this script on the current system. For more information about running scripts and setting execution policy, see about_Execution_Policies at https://go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ .\install-service-winlogbeat.ps1
+ ~~~~~
+ CategoryInfo          : SecurityError: (:) [], PSSecurityException
+ FullyQualifiedErrorId : UnauthorizedAccess
```

script execution is disabled on your system, you need to set the execution policy for the current session to allow the script to run.

powershell -ExecutionPolicy Bypass -File .\install-service-winlogbeat.ps1

```
PS C:\Program Files\Winlogbeat> powershell -ExecutionPolicy Bypass -File .\install-service-winlogbeat.ps1

Status      Name      DisplayName
-----
Stopped     winlogbeat winlogbeat
```

go to path : C:\Program Files\Winlogbeat

open winlogbeat.yml

In winlogbeat.yml file there is winlogbeat.event_logs which captures the list which has give to winlogbeat.event_logs

```

winlogbeat.event_logs:
  - name: Application
    ignore_older: 72h

  - name: System

  - name: Security
    processors:
      - script:
          lang: javascript
          id: security
          file: ${path.home}/module/security/config/winlogbeat-security.js

  - name: Microsoft-Windows-Sysmon/Operational
    processors:
      - script:
          lang: javascript
          id: sysmon
          file: ${path.home}/module/sysmon/config/winlogbeat-sysmon.js

  - name: Windows PowerShell
    event_id: 400, 403, 600, 800
    processors:
      - script:
          lang: javascript
          id: powershell
          file: ${path.home}/module/powershell/config/winlogbeat-powershell.js

```

You can manually add which even logs you want

To know event name

Just give this command in the PowerShell

Get-winEvent -ListLog * | Format-List -Property LogName

```

PS C:\Program Files\Winlogbeat> Get-winEvent -ListLog * | Format-List -Property LogName

LogName : Windows PowerShell
LogName : System
LogName : Security
LogName : OneApp_IGCC
LogName : OAlerts
LogName : Key Management Service
LogName : Internet Explorer
LogName : IntelAudioServiceLog
LogName : HP Analytics
LogName : HardwareEvents
LogName : Application
LogName : Windows Networking Vpn Plugin Platform/OperationalVerbose

```

You can add manually by :

For example:

- Name: Security

Modify the settings under output.elasticsearch,kibana,Dashboards in the C:\Program Files\Winlogbeat\winlogbeat.yml file to point to your Elasticsearch installation.

Configure kibana in winlogbeat.yml by given kibana's ip and port on which server its running

```
# ===== 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: "http://192.168.195.128:5601"

  # Kibana Space ID
  # ID of the Kibana Space into which the dashboards should be loaded. By default,
  # the Default Space will be used.
  #space.id:
```

Make setup.dashboards.enabled: true

```
# ===== 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` command.
setup.dashboards.enabled: true

# 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:
```

Configure elasticsearch in winlogbeat.yml by given elasticsearch's ip and port on which server its running and give username and password which you given for elastic search login credentials

```
# ----- Elasticsearch Output -----
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["http://192.168.195.128:9200"]

  # Protocol - either `http` (default) or `https`.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  username: "elastic"
  password: "3c6pLbiXhKoZrvNudjgd"
```

To check winlogbeat.yml configuration

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

```
PS C:\Program Files\Winlogbeat> .\winlogbeat.exe test config -c .\winlogbeat.yml -e
2023-09-17T21:37:45.074+0530 INFO instance/beat.go:698 Home path: [C:\Program Files\Winlogbeat] Config path: [C:\Program Files\Winlogbeat] Data path: [C:\Program Files\Winlogbeat\data] Logs path: [C:\Program Files\Winlogbeat\logs] Hostfs Path: [/]
2023-09-17T21:37:45.076+0530 INFO instance/beat.go:706 Beat ID: 09769b23-5a48-42c3-a301-83887b925fd2
2023-09-17T21:37:45.113+0530 WARN [add_cloud_metadata] add_cloud_metadata/provider_aws_ec2.go:79 read token request for getting IMDSv2 token returns empty: Put "http://169.254.169.254/latest/api/oken": dial tcp 169.254.169.254:80: connect: A socket operation was attempted to an unreachable network.. No token in the metadata request will be used.
2023-09-17T21:37:45.113+0530 INFO [beat] instance/beat.go:1052 Beat info {"system_info": {"beat": {"path": {"config": "C:\\Program Files\\Winlogbeat", "data": "C:\\Program Files\\Winlogbeat\\data", "home": "C:\\Program Files\\Winlogbeat", "logs": "C:\\Program Files\\Winlogbeat\\logs"}, "type": "winlogbeat", "uuid": "09769b23-5a48-42c3-a301-83887b925fd2"}}}
2023-09-17T21:37:45.113+0530 INFO [beat] instance/beat.go:1061 Build info {"system_info": {"build": {"commit": "50d7b818d6765543bb4e995018c26670871a046d", "libbeat": "7.17.12", "time": "2023-07-18 20:08:06.000Z", "version": "7.17.12"}}}
2023-09-17T21:37:45.114+0530 INFO [beat] instance/beat.go:1064 Go runtime info {"system_info": {"go": {"os": "windows", "arch": "amd64", "max_procs": 8, "version": "go1.19.10"}}}
2023-09-17T21:37:45.114+0530 INFO [add_cloud_metadata] add_cloud_metadata/add_cloud_metadata.go:101 add_cloud_metadata: hosting provider type not detected.
2023-09-17T21:37:45.131+0530 INFO [beat] instance/beat.go:1070 Host info {"system_info": {"host": {"architecture": "x86_64", "boot_time": "2023-09-17T07:47:43+05:30", "name": "Loke4884", "ip": ["fe80::b19:c43d:2d81:95df", "169.254.209.109", "fe80::7ae9:409e:f3f0:f72", "169.254.90.202", "fe80::5faa:b6f5:c121:572e", "169.254.117.95", "fe80::6b58:2447:7252:c7b5", "192.168.128.1", "fe80::deb1:2274:25ee:91f8", "192.168.195.1", "2409:4070:2dc0:16a:ac7e:ec00:a48c:a4f4", "2409:4070:2dc0:16a:507a:d412:1c16:d178", "fe80::e7d2:74:9200:1bf3", "192.168.118.18", "::1", "127.0.0.1"], "kernel_version": "10.0.22621.2283 (WinBuild.160101.0800)", "mac": ["00:ff:8f:b9:ed:f8", "92:e8:68:1e:9c:23", "92:e8:68:1e:9c:33", "00:50:56:c0:00:01", "00:50:56:c0:00:08", "dc:30:70:68:1e:10"], "os": {"type": "windows", "family": "windows", "platform": "windows", "name": "Windows 11 Home Single Language", "version": "10.0", "major": 10, "minor": 0, "patch": 0, "build": "22621.2283"}, "timezone": "IST", "timezone_offset_sec": 19800, "id": "7d1a2ece-0d45-4127-a72f-648770a85b8b"}}}
2023-09-17T21:37:45.132+0530 INFO [beat] instance/beat.go:1099 Process info {"system_info": {"process": {"cwd": "C:\\Program Files\\Winlogbeat", "exe": "C:\\Program Files\\Winlogbeat\\winlogbeat.exe", "name": "winlogbeat.exe", "pid": 23332, "ppid": 11460, "start_time": "2023-09-17T21:37:44.036+0530"}}}
2023-09-17T21:37:45.132+0530 INFO instance/beat.go:292 Setup Beat: winlogbeat; Version: 7.17.12
2023-09-17T21:37:45.133+0530 INFO [index-management] idxmgmt/std.go:184 Set output.elasticsearch.index to 'winlogbeat-7.17.12' as ILM is enabled.
2023-09-17T21:37:45.133+0530 INFO [esclientleg] eslegclient/connection.go:105 elasticsearch url: http://192.168.195.128:9200
2023-09-17T21:37:45.133+0530 INFO [publisher] pipeline/module.go:113 Beat name: Loke4884
2023-09-17T21:37:45.134+0530 INFO [winlogbeat] beater/winlogbeat.go:66 State will be read from and persisted to C:\Program Files\Winlogbeat\data\winlogbeat.yml
2023-09-17T21:37:45.160+0530 WARN [cfgwarn] registered_domain/registered_domain.go:61 BETA: The registered_domain processor is beta.
2023-09-17T21:37:45.198+0530 WARN [cfgwarn] registered_domain/registered_domain.go:61 BETA: The registered_domain processor is beta.
Config OK
```

Setup winlogbeat

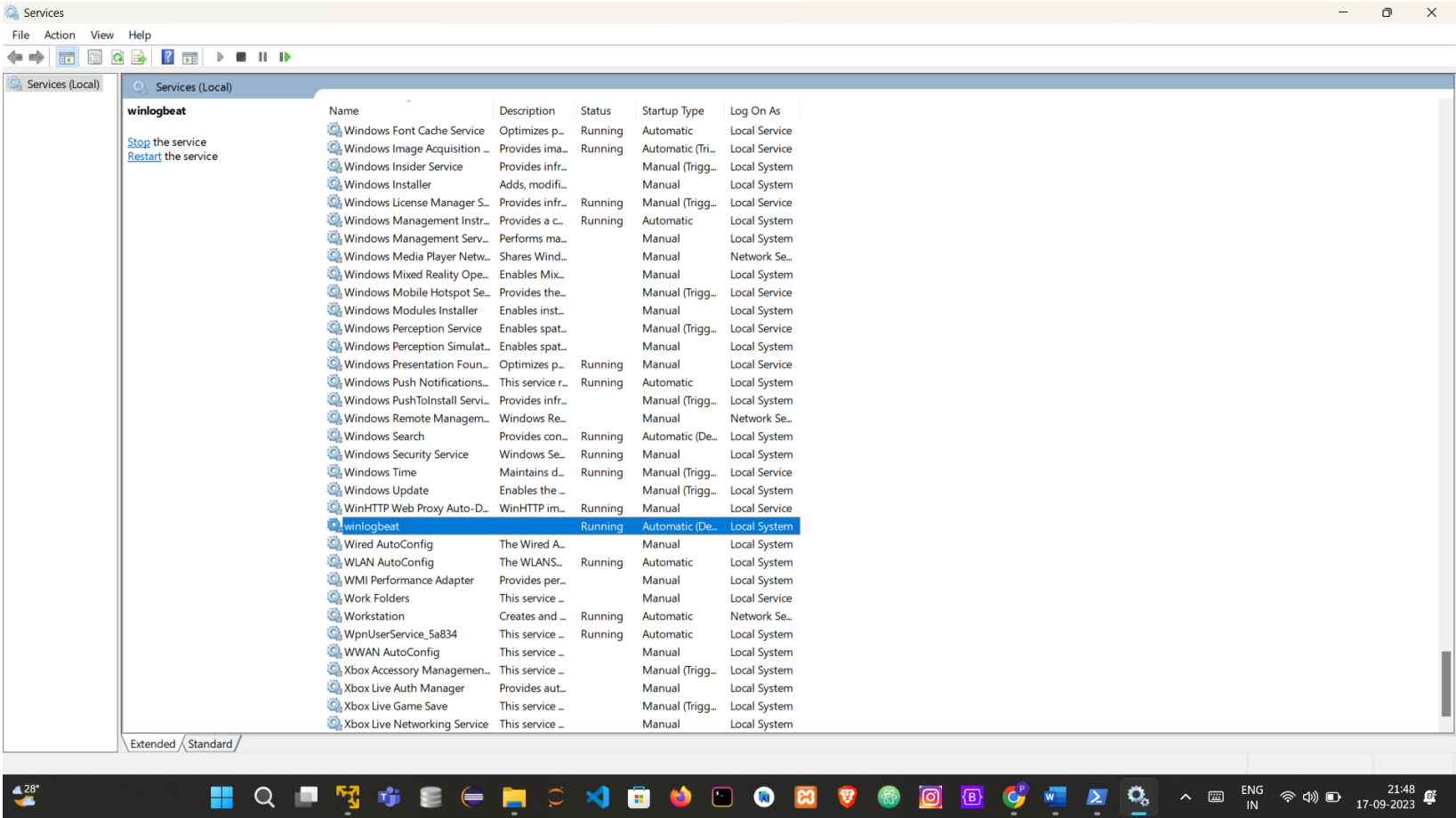
.\winlogbeat.exe setup --dashboards

```
PS C:\Program Files\Winlogbeat> .\winlogbeat.exe setup --dashboards
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
```

Start winlogbeat as service

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

Check whether winlogbeat is running as service



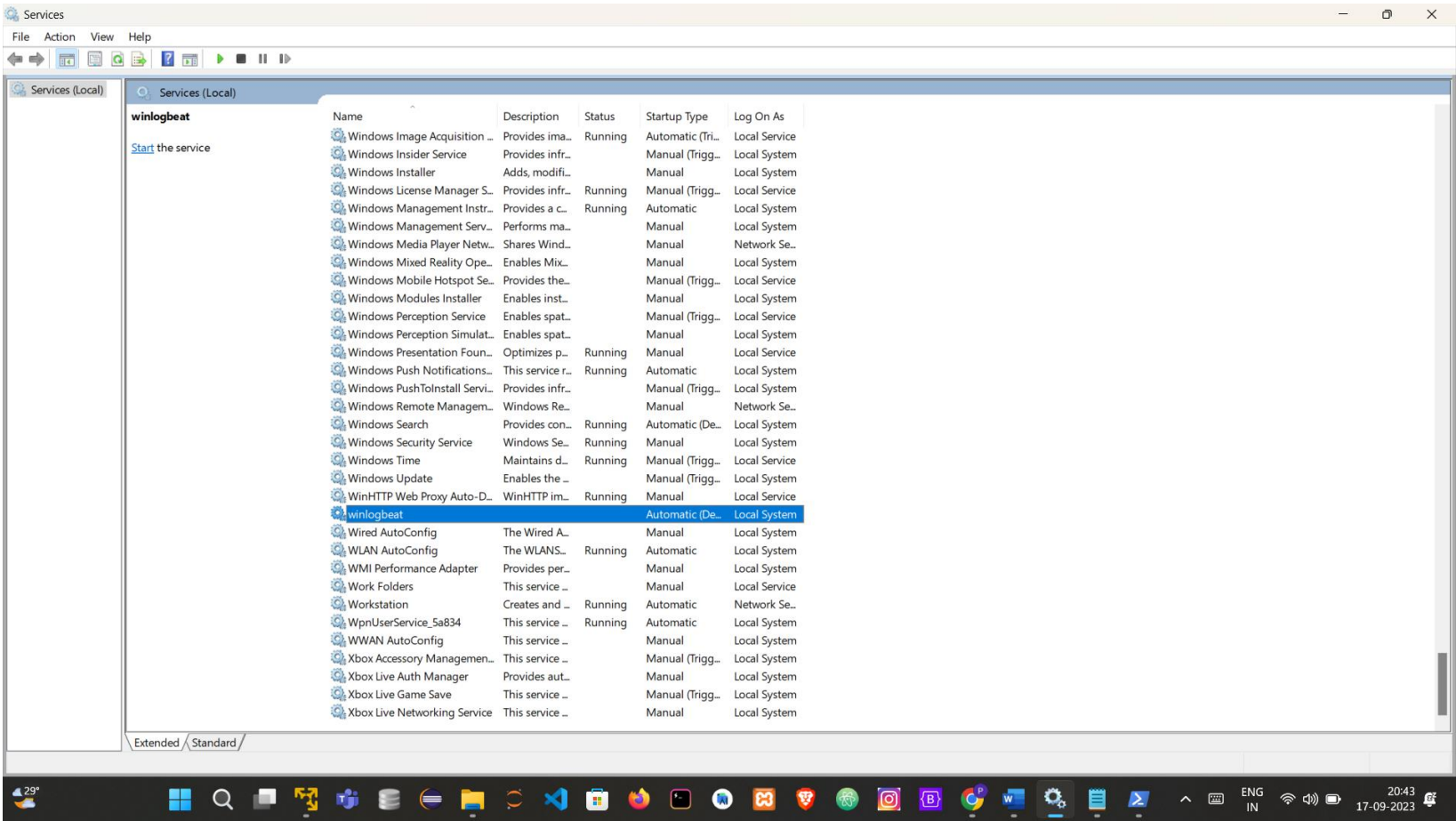
If you have any misconfigurations then have to stop winlogbeat

```
PS C:\Program Files\Winlogbeat> Stop-Service winlogbeat
Stop-Service : Service 'winlogbeat (winlogbeat)' cannot be stopped due to the following error: Cannot stop winlogbeat service on computer '.'.
At line:1 char:1
+ Stop-Service winlogbeat
+ ~~~~~
+ CategoryInfo          : CloseError: (System.ServiceProcess.ServiceController:ServiceController) [Stop-Service], ServiceCommandException
+ FullyQualifiedErrorId : CouldNotStopService,Microsoft.PowerShell.Commands.StopServiceCommand

PS C:\Program Files\Winlogbeat> Get-Process -Name "winlogbeat"

Handles   NPM(K)    PM(K)      WS(K)      CPU(s)      Id  SI ProcessName
-----
288        23      82924      75288       3.63     9468  0 winlogbeat

PS C:\Program Files\Winlogbeat> Stop-Process -Name "winlogbeat" -Force
PS C:\Program Files\Winlogbeat> Stop-Service winlogbeat
```



Restart winlogbeat

```
PS C:\Program Files\Winlogbeat> Restart-Service winlogbeat
```

Steps to delete winlogbeat

```
PS C:\Program Files\Winlogbeat> powershell -ExecutionPolicy Bypass -File .\uninstall-service-winlogbeat.ps1
WARNING: Waiting for service 'winlogbeat (winlogbeat)' to stop...
WARNING: Waiting for service 'winlogbeat (winlogbeat)' to stop...
WARNING: Waiting for service 'winlogbeat (winlogbeat)' to stop...
PS C:\Program Files\Winlogbeat> Stop-Service winlogbeat
Stop-Service : Service 'winlogbeat (winlogbeat)' cannot be stopped due to the following error: Cannot stop winlogbeat
service on computer '.'.
At line:1 char:1
+ Stop-Service winlogbeat
+ ~~~~~
+ CategoryInfo          : CloseError: (System.ServiceProcess.ServiceController:ServiceController) [Stop-Service],
ServiceCommandException
+ FullyQualifiedErrorId : CouldNotStopService,Microsoft.PowerShell.Commands.StopServiceCommand

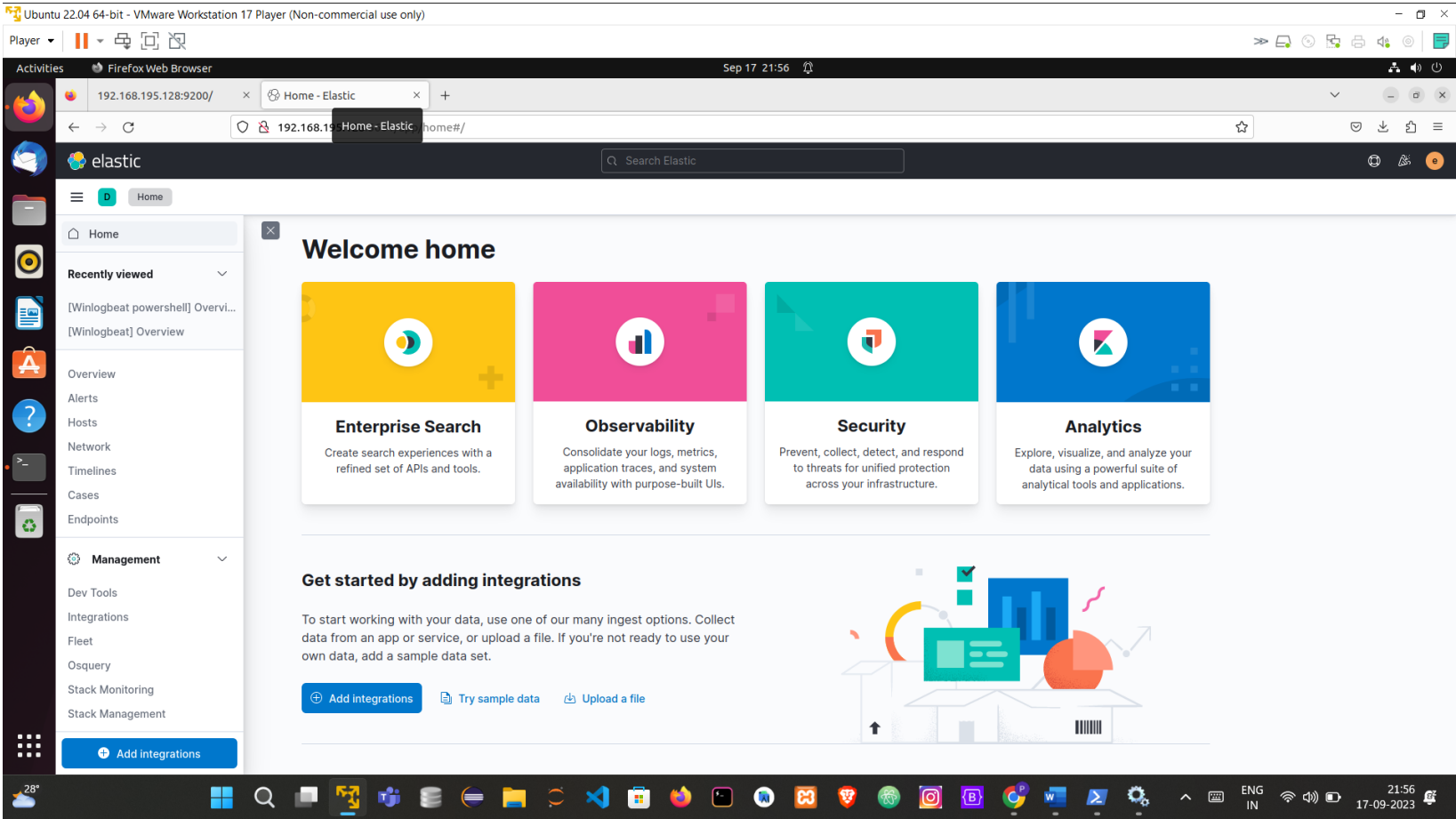
PS C:\Program Files\Winlogbeat> Get-Process -Name "winlogbeat"

Handles   NPM(K)    PM(K)      WS(K)      CPU(s)      Id  SI ProcessName
-----
291        23      85732      63272      15.53     15744  0 winlogbeat

PS C:\Program Files\Winlogbeat> Stop-Process -Name "winlogbeat" -Force
PS C:\Program Files\Winlogbeat> Stop-Service winlogbeat
PS C:\Program Files\Winlogbeat> powershell -ExecutionPolicy Bypass -File .\uninstall-service-winlogbeat.ps1
[SC] DeleteService SUCCESS
```


Go to kibana dashboard

Click on add integretions



Select beat only


All categories	144
AWS	4
Azure	4
Cloud	8
Communications	3
Config management	1
Containers	3
Custom	15
Database	22
Elastic Stack	14
File storage	5
Google Cloud	3
Kubernetes	3

If an integration is available for Elastic Agent and Beats, show:

- ☐ Recommended ?
- ☐ Elastic Agent only
- ☒ Beats only

Search winlog

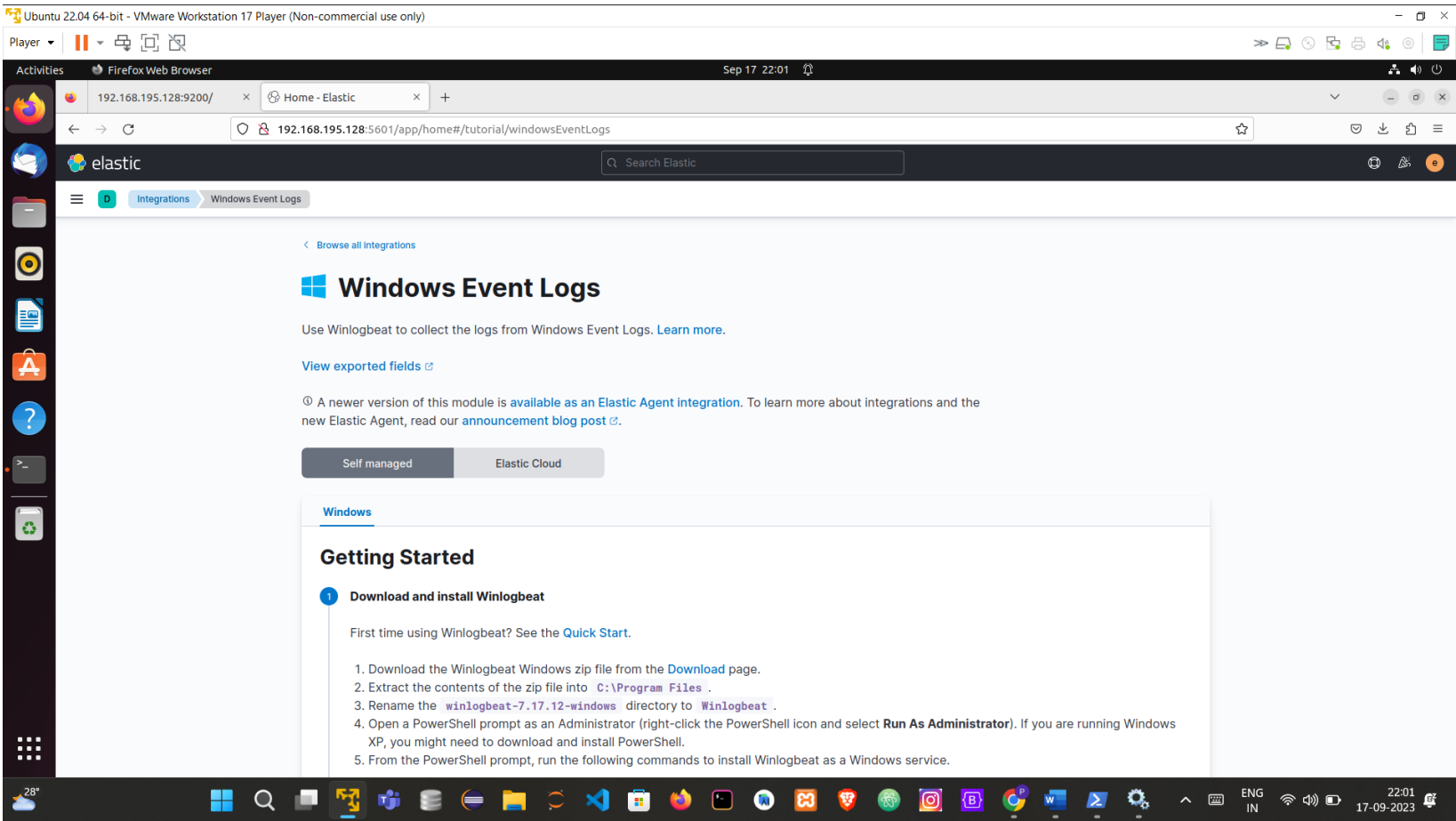
win|



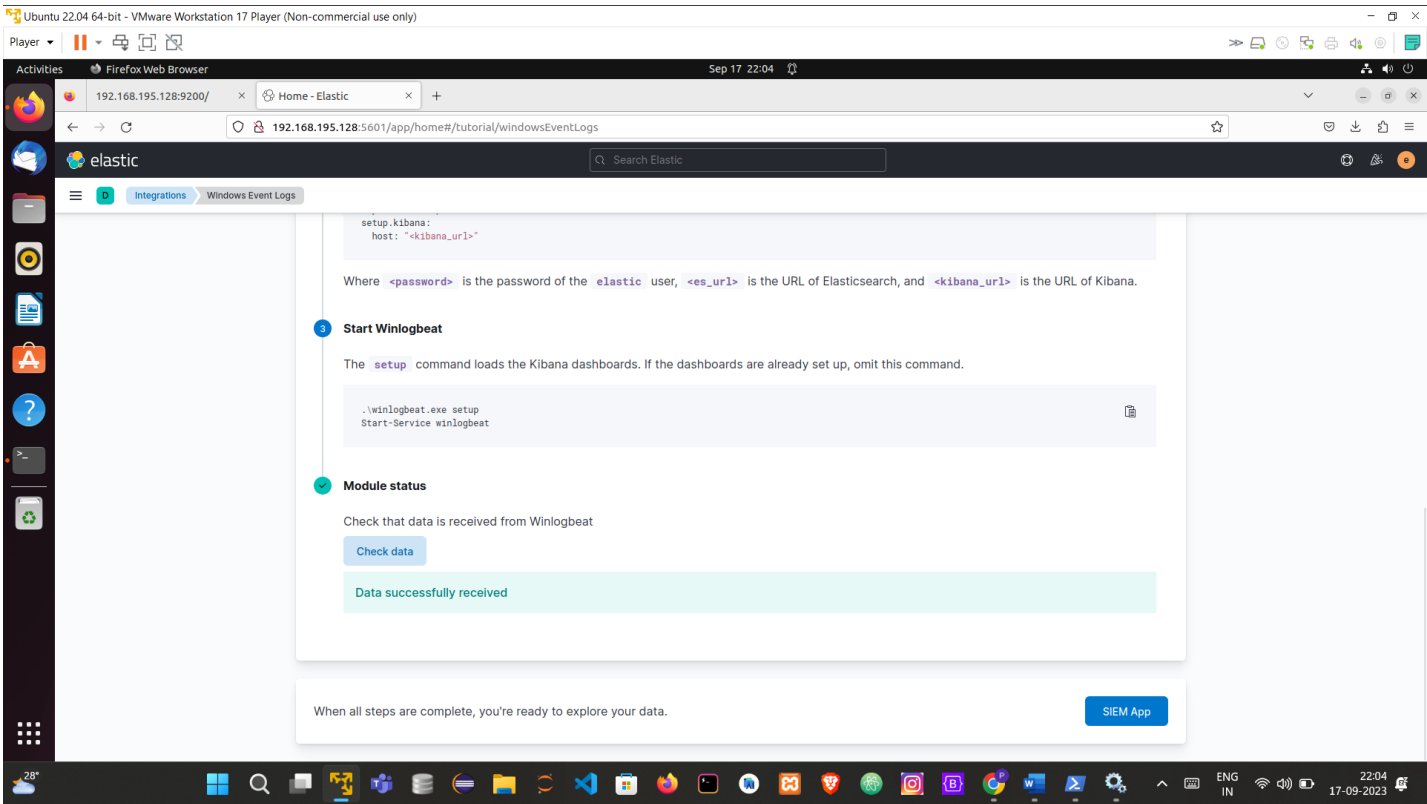
Windows Event Logs

Collect and parse logs from Windows Event Logs with WinLogBeat.

You will redirect to this page



Click on check data and next click on SIEM App



A new encryption key is generated for saved objects each time you start Kibana. Without a persistent key, you cannot delete or modify rules after Kibana restarts. To set a persistent key, add the `xpack.encryptedSavedObjects.encryptionKey` setting with any text value of 32 or more characters to the `kibana.yml` file.

Add the `xpack.encryptedSavedObjects.encryptionKey` setting with a text value of 32 or more characters. You can generate a secure key using a tool like `openssl` or any other method that produces a cryptographically secure random key. For example, you can generate a random 64-character key using `openssl`:

`openssl rand -hex 32`

```
root@Loke4884:/etc/apt/sources.list.d# openssl rand -hex 32
974ded0db2d58f260cfb720949480a20f1caaeb0886491b1f62f001bbfecae0d8
```

Edit `kibana.yml`

`nano /etc/kibana/kibana.yml`

```
root@Loke4884:/home/loke4884# nano /etc/kibana/kibana.yml
```

```
GNU nano 6.2 /etc/kibana/kibana.yml *
#elasticsearch.requestTimeout: 30000

# List of Kibana client-side headers to send to Elasticsearch. To send *no* client-side
# headers, set this value to [] (an empty list).
#elasticsearch.requestHeadersWhitelist: [ authorization ]

# Header names and values that are sent to Elasticsearch. Any custom headers cannot be overwritten
# by client-side headers, regardless of the elasticsearch.requestHeadersWhitelist configuration.
#elasticsearch.customHeaders: {}

# Time in milliseconds for Elasticsearch to wait for responses from shards. Set to 0 to disable.
#elasticsearch.shardTimeout: 30000

# Logs queries sent to Elasticsearch. Requires logging.verbose set to true.
#elasticsearch.logQueries: false

# Specifies the path where Kibana creates the process ID file.
#pid.file: /run/kibana/kibana.pid

# Enables you to specify a file where Kibana stores log output.
#logging.dest: stdout

# Set the value of this setting to true to suppress all logging output.
#logging.silent: false

# Set the value of this setting to true to suppress all logging output other than error messages.
#logging.quiet: false

# Set the value of this setting to true to log all events, including system usage information
# and all requests.
#logging.verbose: false

# Set the interval in milliseconds to sample system and process performance
# metrics. Minimum is 100ms. Defaults to 5000.
#ops.interval: 5000

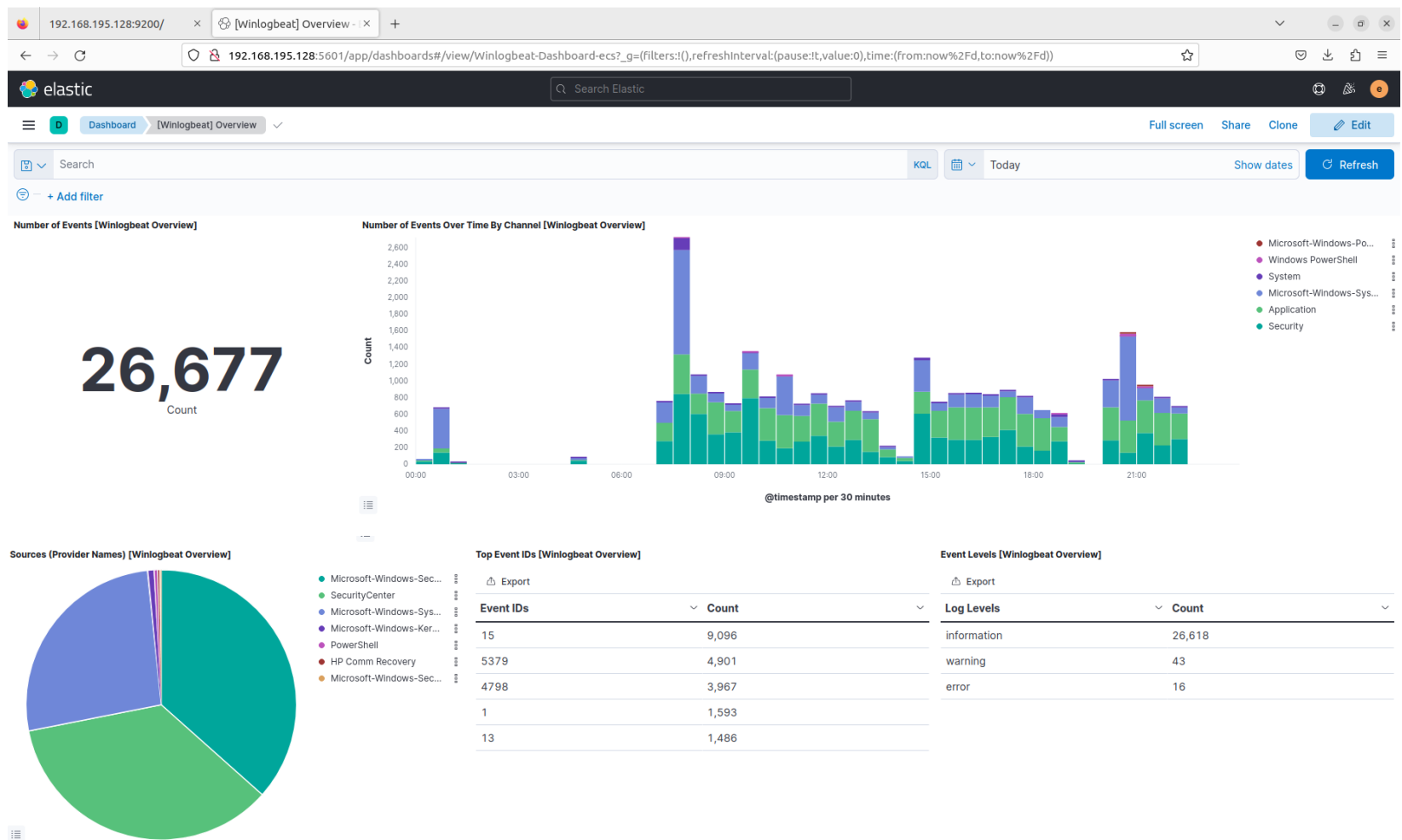
# Specifies locale to be used for all localizable strings, dates and number formats.
# Supported languages are the following: English - en , by default , Chinese - zh-CN .
#i18n.locale: "en"

xpack.encryptedSavedObjects.encryptionKey: "974ded0db2d58f260cfb720949480a20f1caaeb0886491b1f62f001bbfecae0d8"
```

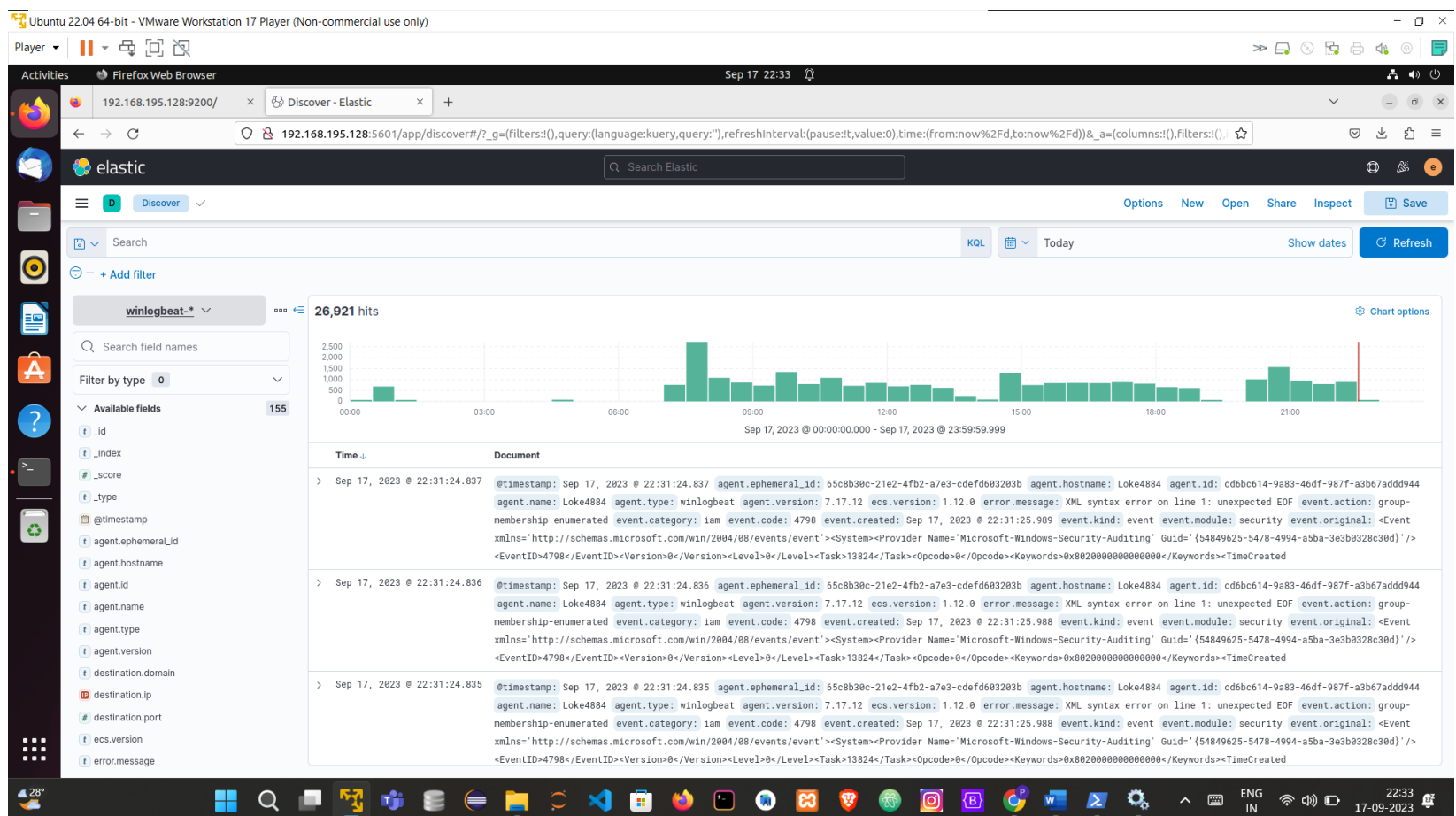
Restart kibana and elasticsearch

```
root@Loke4884:/home/loke4884# systemctl restart kibana
root@Loke4884:/home/loke4884# systemctl restart elasticsearch
```


Dashboard of logs collected by winlogbeat



Go to Discover and choose winlogbeat you can see logs collected



```
input {  
  beats {  
    port => 5044  
  }  
}  
  
filter {  
  # Add your Sysmon log processing here  
}  
  
output {  
  elasticsearch {  
    hosts => ["192.168.195.128:9200"] # Update with your Elasticsearch server information  
    index => "winlogbeat-%{+YYYY.MM.dd}" # Set the index name to "log"  
    user => "elastic"  
    password => "3c6pLbiXhKoZrvNudjgd"  
  }  
}
```