Nowadays, it is essential for cloud administrators to leverage centralized logging systems to better understand their environments, learn usage patterns, and identify future potential problems. Of course, these are just some of the functions a centralized logging strategy provides, all which help IT organizations become more productive. However, in order to provide these insightful services in-house, there is significant management effort, including daily management, backups, high availability, hardening, updating, encryption in transit and at rest, and storage management.

In order to eliminate some of the management effort of standing up a centralized logging solution, this blog post provides a walk through for creating of a near real-time event management solution running on native AWS and open-source platforms, focused on monitoring Windows based Amazon EC2 instances. The solution not only addresses the primary need of monitoring, but does so without the need of expensive third-party products.

Step by Step

Steps for this procedure include:

1. Launch an Amazon Elasticsearch Service domain.
2. Install and configure the Winlogbeat agent offered by Elastic.co in an Amazon EC2 running Windows instances.
3. Customize Logs visualization on Kibana.

1. Launch an Amazon Elasticsearch Service domain.

1. Open the AWS Console Elasticsearch Service Dashboard
2. Click-in **"Create a new domain".**
3. Enter of the **Domain Name** and select the version Elasticsearch **6.0 or earlier**.
4. Clique em **Next.**
5. On Configure Cluster

Node Configuration
- Instance Count: 1
- Instance Type: m4.large.elasticsearch

Storage
- Storage Type: EBS
- EBS Volume Type: General Purpose (SSD)
- EBS Volume Size: 100 GB

Snapshot Configuration
- Automated snapshot start hour: 00:00 UTC (Default)

6. Click-in **Next.**
7. On Network Configuration.
8. Select **VPC Access (Recommended)**

- Select the VPC, Subnet and Security Groups in which the Elasticsearch cluster will be launched. (The Amazon ElasticSearch Service uses TCP port 443 and must be released in the selected Security Group).

- Kibana Authentication will not be used in this demo, leave it blank.

- On Access Policy: **Do not require signing request with IAM credential** (Allows associated security groups within your VPC full access to the domain).

9. Click-in **Next.**
10. Click-in **Confirm** and the Amazon Elasticsearch domain will be launch.

While the Amazon Elasticsearch Service is launching, configure the agent on the Amazon EC2.

2. Install and configure the Winlogbeat agent offered by Elastic.co on Amazon EC2 Instances.

1. Access Elasticsearch Winlogbeat and download the x64 installer.

2. Extract the contents in the "C:\Program Files" directory and rename the extracted directory to Winlogbeat.

```
PS C:\Program Files\Winlogbeat> ls


    Directory: C:\Program Files\Winlogbeat


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
d----         10/28/2018   3:46 AM            data
d----         10/28/2018   3:22 AM            kibana
d----         10/28/2018   6:21 PM            logs
-----          9/26/2018  12:51 PM         41 .build_hash.txt
-----          9/26/2018  12:50 PM      12544 fields.yml
-----          9/26/2018  12:51 PM        582 install-service-winlogbeat.ps1
-----          9/26/2018  12:39 PM      13675 LICENSE.txt
-----          9/26/2018  12:39 PM     148778 NOTICE.txt
-----          9/26/2018  12:51 PM        825 README.md
-----          9/26/2018  12:51 PM        254 uninstall-service-winlogbeat.ps1
-----          9/26/2018  12:51 PM   33539072 winlogbeat.exe
-----          9/26/2018  12:50 PM      42150 winlogbeat.reference.yml
-a---         10/28/2018   7:06 PM        518 winlogbeat.yml
```

3. Within the Winlogbeat directory (renamed earlier), there is a file called **winlogbeat.yml**, open it for editing.

4. In the **winlogbeat.event_logs** section, it should contain the name of the logs that will be sent to the Amazon Elasticsearch service.

```
#========================== 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
winlogbeat.event_logs:
  - name: Application
    ignore_older: 72h
  - name: Security
  - name: System
```

**Note: Use the following command in PowerShell to access the name of all event logs available in the operating system:*
Get-WinEvent -Listlog * \| Format-List -Property LogName > C:\Logs.txt

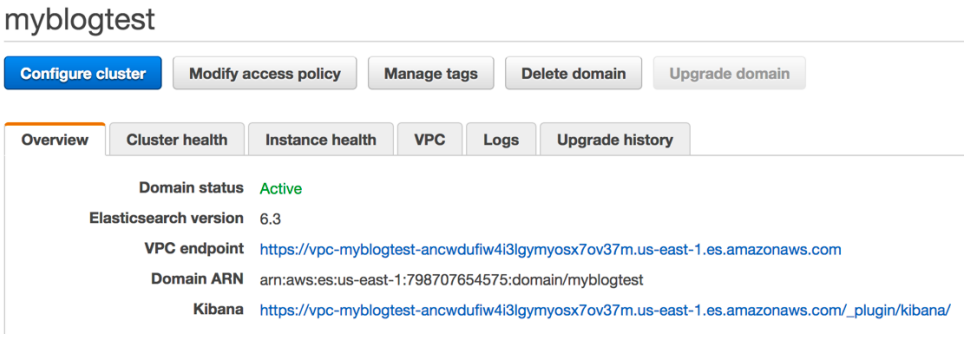
In the **output.elasticsearch** section, you must contain the URL of the Amazon Elasticsearch Service domain. **Port 443 must be specified as in the image below**, otherwise the agent will attempt to use the default port of Elasticsearch (9300/tcp).

```
#----------------------------- Elasticsearch output ------------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["https://vpc-myblogtest-ancwdufiw4i3lgymyosx7ov37m.us-east-1.es.amazonaws.com:443"]

  # Optional protocol and basic auth credentials.
  #protocol: "https"
  #username: "elastic"
  #password: "changeme"
```

In the **setup.kibana** section, you must contain the URL of the domain. Port 443 must be specified as in the image above (**before /_plugin/kibana**). The URL must be entered exactly as in the image below (in quotation marks).

```
# 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: "https://vpc-myblogtest-ancwdufiw4i3lgymyosx7ov37m.us-east-1.es.amazonaws.com:443/_plugin/kibana/"
```

** Note: The Amazon Elasticsearch Service and Kibana URLs are available in the administration console of the Elasticsearch domain just created in step 1.*



5. After the winlogbeat.yml file properly configured, now is the time to install the agent.

6. Open Powershell as administrator and navigate to the "C:\Program Files\ Winlogbeat" directory
   Run the installation script: **.\install-service-winlogbeat.ps1**

```
Administrator: Windows PowerShell
PS C:\Program Files\Winlogbet> .\install-service-winlogbeat.ps1

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


PS C:\Program Files\Winlogbet> _
```

   *Note: If script execution fails due to operating system policy restriction, run Setup with the following command:
   PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-winlogbeat.ps1

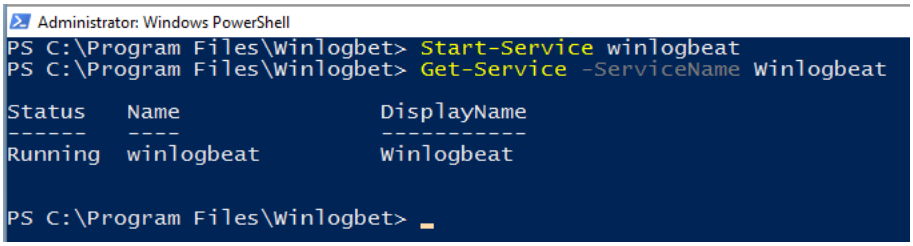
7. If successfully installed, the Service Status will appear as Stopped. Verify that the configuration file has no syntax error with the following command:
   .\winlogbeat.exe test config -c .\winlogbeat.yml

```
Administrator: Windows PowerShell
PS C:\Program Files\Winlogbeat> .\winlogbeat.exe test config -c .\winlogbeat.yml
Config OK
```

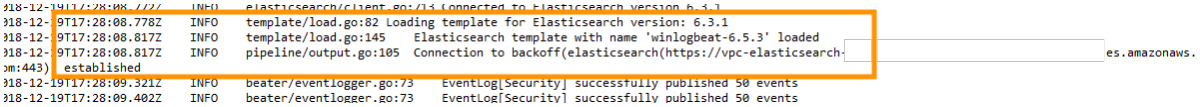
8. Run the command to import the Kibana dashboard and look if the output is Loaded dashboards.
   .\winlogbeat.exe setup –dashboards

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

9. Without errors in the configuration file and dashboards imported, start the service with the following command:
   Start-Service winlogbeat



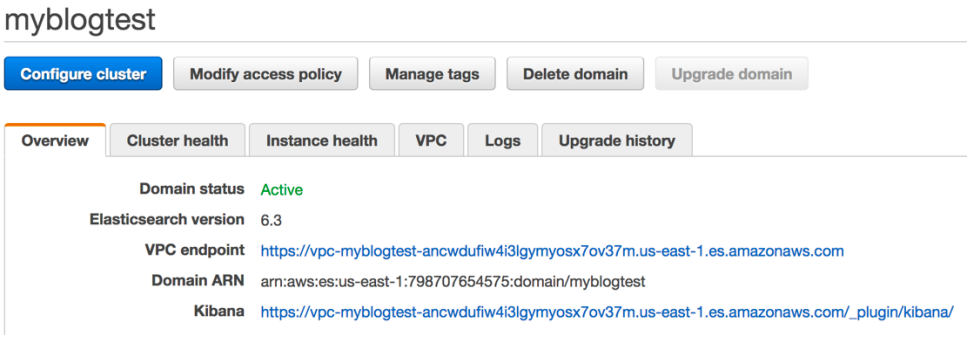
10. Verify that the agent has successfully connected to the Amazon Elasticsearch Service by analyzing the log generated in the agent in "C:\ProgramData\winlogbeat\Logs" file and search for Connection to backoff with Established result.



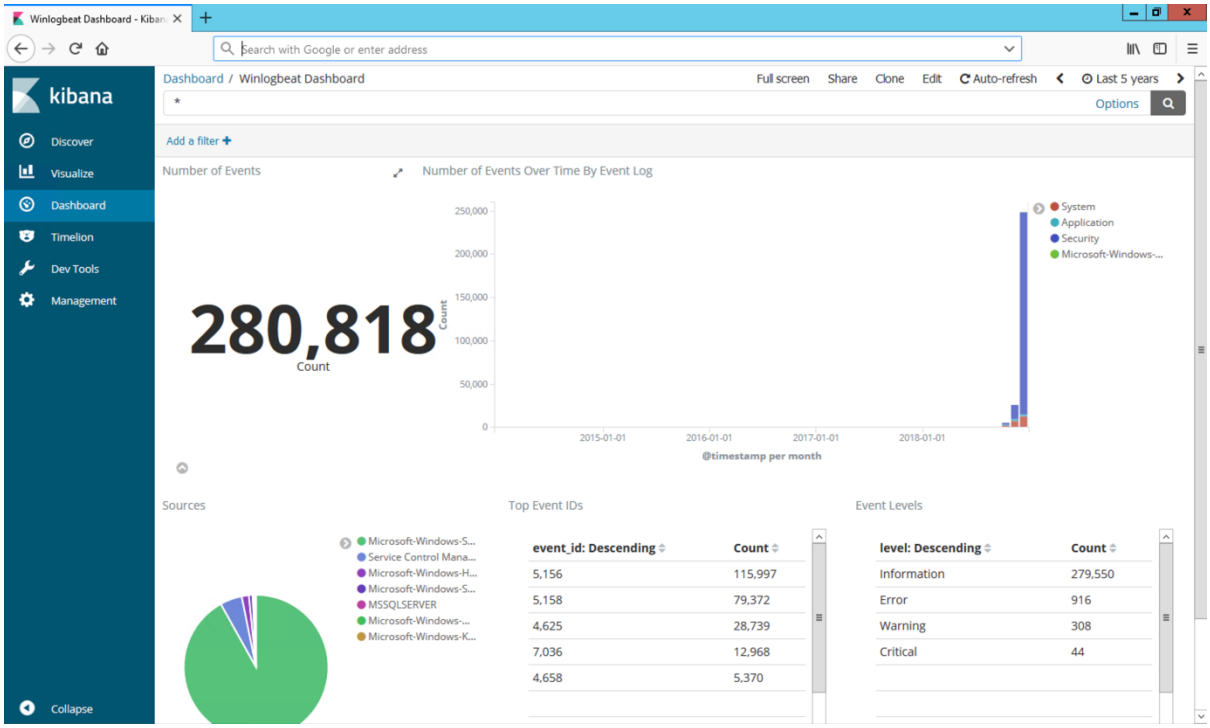
3. Customize Logs visualization on Kibana

Logs should start being sent to the Amazon ElasticSearch Service and you can already create insights about the environment.

1. Access Kibana through a browser of an Amazon EC2 Windows instance at the Kibana address entered in the administration console of the Amazon Elasticsearch Service domain.



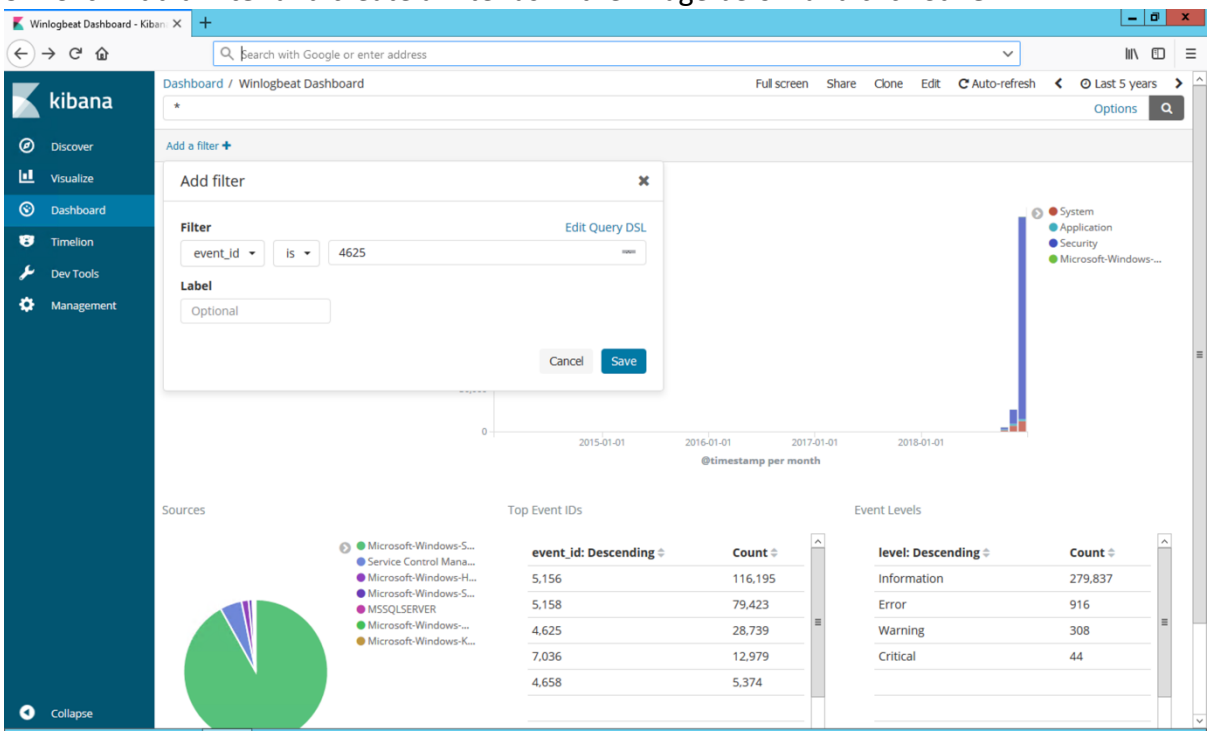
2. Navigate to the Dashboard tab and you will see the Dashboard named: **Winlogbeat Dashboard**, click on it and a screen similar to the one below will be displayed.



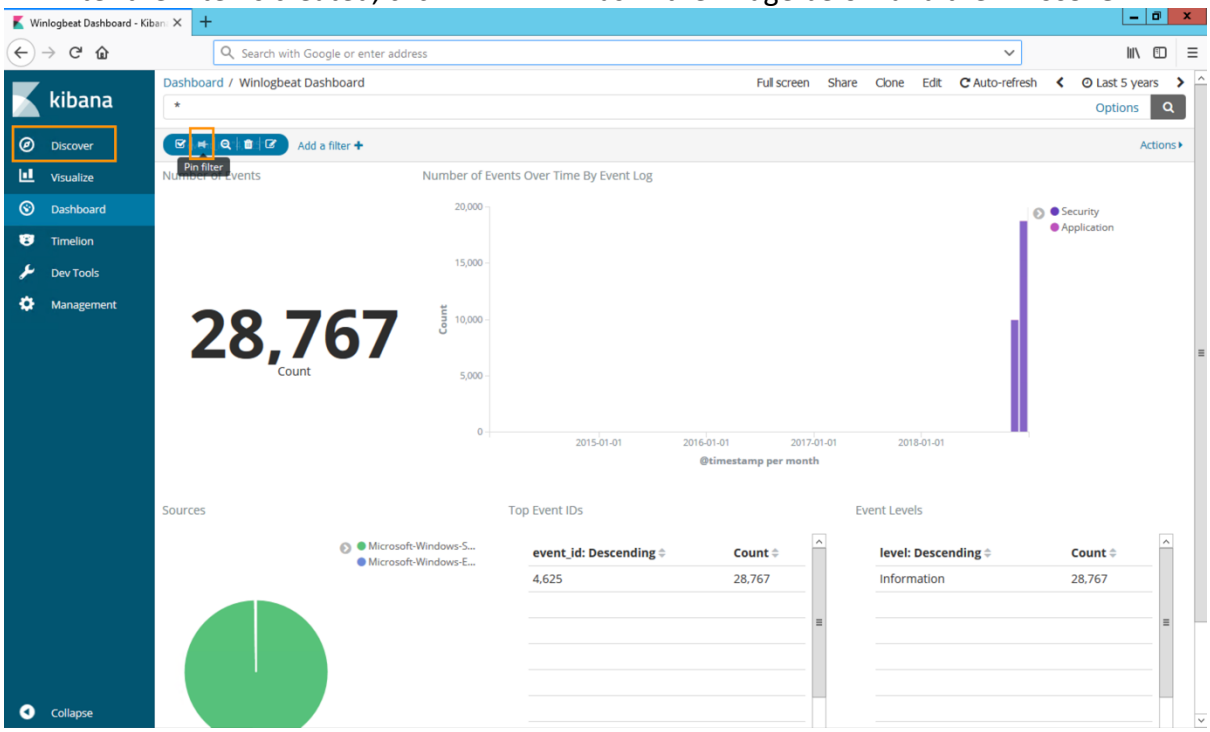
You now have an AWS-managed log centralization system, just set up your Amazon EC2 instances to send the logs to Amazon Elasticsearch Service and create the filters as needed.

How about create a filter regarding Logon Failure (Event ID 4625)? With the Security logs configured as a shipping log in winlogbeat.yml, any unsuccessful logon attempt will generate an EventID 4625 and this will be filtered.

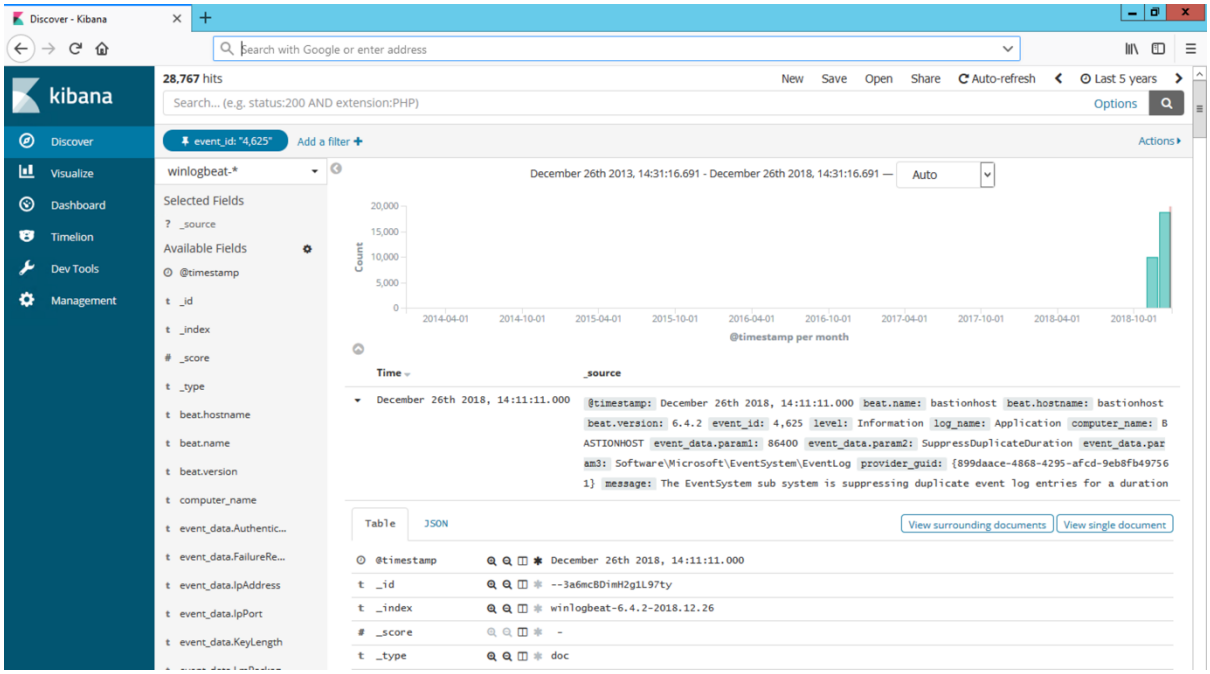
3. Click **Add a filter** and create a filter as in the image below and click **Save**.



4. After the filter is created, click **PIN FILTER** as in the image below and then **Discover**



It will now be possible to make a deeper understanding of each log and take the appropriate actions or corrections.



To learn more about Microsoft Workloads on AWS, go to:
https://aws.amazon.com/pt/solutionspace/microsoft-workloads/