* **Beat 설치 매뉴얼**

1. **Beat 종류**

|  |  |  |  |
| --- | --- | --- | --- |
| **Beat 명** | **용도** | **사용 시스템** | **비고** |
| Winlogbeat | Windows 서버 시스템 로그 수집(Security, system log) | 스마트워크 Windows Server 전체 |  |
| Metricbeat(Windows) | Windows OS Metric(CPU, Memory, Disk usage등) 수집 | 스마트워크 Windows Server 전체 |  |
| Filebeat(Windows) | Windows MSSQL Error Log, IIS 로그 수집 | 스마트워크 메신저 MSSQL DB 서버, SharePoint DB 서버, SharePoint Search 서버 | HSNCSPSC1P  HSNCSQL01  HSNCSPDB1P |
| Metricbeat(Linux) | Windows OS Metric(CPU, Memory, Disk usage등) 수집 | 스마트워크 Linux Server 전체 |  |
| FileBeat(Linux) | Oracle alert log, listener log  WEB/WAS Server, Error log, access log  OS system log | 스마트워크 Linux Server 전체 |  |

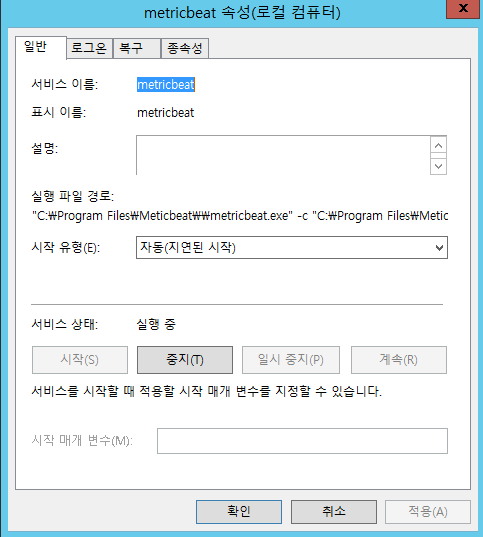
1. **Windows Metricbeat 설치 방법**
2. Meticbeat.zip 파일을 windows server C:\Program Files\Meticbeat에 업로드 한다.
3. metricbeat.yml 내용을 서버 설정에 맞게 수정

- fields: 설정에서 ip, tier, log\_type, company\_name, system\_name, server\_name을 수정한다.

- output.kafaka: 설정에서 topic을 수정한다.

1. C:\Program Files\Meticbeat에 install-service-metricbeat.ps1 명령어를 실행하여 Windows Service에 metricbeat를 등록한다.
2. Windows 서비스에서 metricbeat를 찾아 설정정보에서 시작유형을 지연된 시작으로 변경하고 서비스를 시작한다.

- 시작유형 : 자동(지연된 시작) 설정



1. 수정 사항 상세

#================================ Custom fields ===================

fields\_under\_root: true

fields:

ip: 172.19.115.101 # 서버 IP 입력

tier: OS

log\_type: windows\_metric

company\_name: HWCC # 계열사 명 입력

system\_name: smartwork

server\_name: HCC-DBS01P # 서버 명 입력

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

output.kafka:

hosts: ["172.16.5.97:9092","172.16.5.100:9092","172.16.5.101:9092"]

topic: 'hwcc\_metric\_topic' # 로그 데이터를 저장하기 위한 Kafka topic 입력

workers: 1

bulk\_max\_size: 10240

broker\_timeout: 5s

partition.round\_robin:

reachable\_only: false

required\_acks: 1

compression: gzip

max\_message\_bytes: 1000000

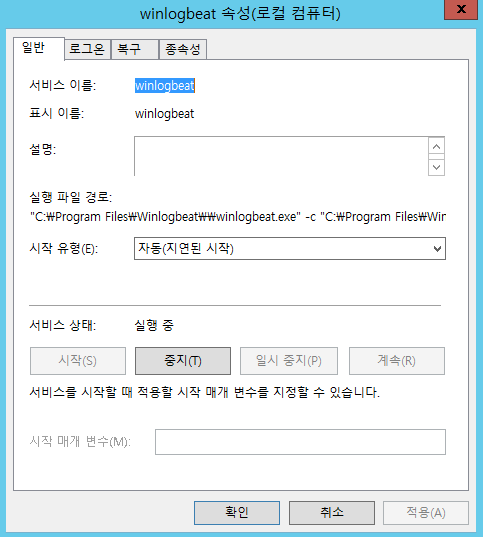
1. **Winlogbeat 설치 방법**
2. Winlogbeat.zip 파일을 windows server C:\Program Files\Winlogbeat에 업로드 한다.
3. winlogbeat.yml 내용을 서버 설정에 맞게 수정

- fields: 설정에서 ip, tier, log\_type, company\_name, system\_name, server\_name을 수정한다.

- output.kafaka: 설정에서 topic을 수정한다.

1. C:\Program Files\Winlogbeat 에 install-service-winlogbeat.ps1 명령어를 실행하여 Windows Service에 winlogbeat를 등록한다.
2. Windows 서비스에서 winlogbeat를 찾아 설정정보에서 시작유형을 지연된 시작으로 변경하고 서비스를 시작한다.

- 시작유형 : 자동(지연된 시작) 설정



1. 수정사항 상세

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

winlogbeat.event\_logs:

# - name: Application

#

# - name: Security

# ignore\_older: 72h

- name: Security

- name: System

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

#================================ Custom ========================

fields:

ip: 172.19.115.101

tier: OS

log\_type: windows\_log

company\_name: HWCC

system\_name: smartwork

server\_name: HCC-DBS01P

fields\_under\_root: true

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

#-------------------------- Kafka output ------------------------------

output.kafka:

hosts: ["172.16.5.97:9092","172.16.5.100:9092","172.16.5.101:9092"]

topic: 'hwcc\_log\_topic'

workers: 1

bulk\_max\_size: 10240

broker\_timeout: 5s

partition.round\_robin:

reachable\_only: false

required\_acks: 1

compression: gzip

max\_message\_bytes: 1000000

1. **Filebeat(Windows) 설치 방법**
2. Filebeat\_mssql\_lyncdb.zip 파일을 windows server C:\Program Files\Filebeat에 업로드 한다.
3. filebeat.yml 내용을 서버 설정에 맞게 수정

- fields: 설정에서 ip, tier, log\_type, company\_name, system\_name, server\_name을 수정한다.

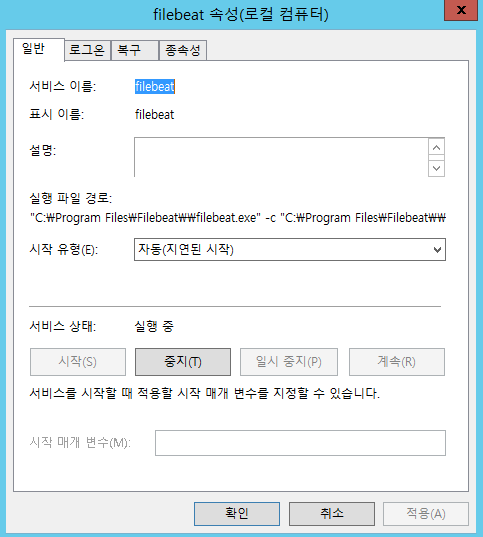
- output.kafaka: 설정에서 topic을 수정한다.

- path: 설정에 MSSQL ERROR로그 위치를 정확하게 변경한다.

IIS ERROR로그 위치를 정확하게 변경한다.

1. C:\Program Files\Filebeat 에 install-service-filebeat.ps1 명령어를 실행하여 Windows Service에 filebeat를 등록한다.
2. Windows 서비스에서 filebeat를 찾아 설정정보에서 시작유형을 지연된 시작으로 변경하고 서비스를 시작한다.

- 시작유형 : 자동(지연된 시작) 설정



1. 상세 수정사항

* MSSQL Error 로그

filebeat.prospectors:

#=====MSSQL log ======#

- input\_type: log

enabled: true

fields:

ip: 172.19.115.101

tier: DB

log\_type: db\_mssql\_error\_log

company\_name: HWCC

system\_name: smartwork

server\_name: HCC-DBS01P

fields\_under\_root: true

paths:

- D:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\Log\ERRORLOG

# tail\_files: true

scan\_frequency: 60s

encoding: utf-16le-bom

multiline.pattern: '^\d{4}-\d{2}-\d{2}[[:space:]]\d{2}:\d{2}:\d{2}.\d{2}[[:space:]]'

multiline.negate: true

multiline.match: after

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

output.kafka:

hosts: ["172.16.5.97:9092","172.16.5.100:9092","172.16.5.101:9092"]

topic: 'hwcc\_log\_topic'

workers: 1

bulk\_max\_size: 10240

broker\_timeout: 5s

partition.round\_robin:

reachable\_only: false

required\_acks: 1

compression: gzip

max\_message\_bytes: 1000000

* IIS 로그

filebeat.prospectors:

#=====IIS log ======#

- input\_type: log

enabled: true

fields\_under\_root: true

fields:

ip: 172.19.115.71

tier: IIS

log\_type: iis\_error

company\_name: HWCC

system\_name: smartwork

server\_name: HCC-SPSC01P

paths:

- d:\Logs\IIS\W3SVC1228100218\\*

- d:\Logs\IIS\W3SVC1906335817\\*

scan\_frequency: 60s

tail\_files: true

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

output.kafka:

hosts: ["172.16.5.97:9092","172.16.5.100:9092","172.16.5.101:9092"]

topic: 'hwcc\_log\_topic'

workers: 1

bulk\_max\_size: 10240

broker\_timeout: 5s

partition.round\_robin:

reachable\_only: false

required\_acks: 1

compression: gzip

max\_message\_bytes: 1000000

1. **Filebeat(Windows) 설치 방법**
2. metricbeat-5.6.2-linux-x86\_64.tar.gz 파일을 linux server /opt에 업로드 한다.
3. 파일 압축을 해제한다. tar –xzvf metricbeat-5.6.2-linux-x86\_64.tar.gz
4. metricbeat.yml 내용을 서버 설정에 맞게 수정

- fields: 설정에서 ip, tier, log\_type, company\_name, system\_name, server\_name을 수정한다.

- output.kafaka: 설정에서 topic을 수정한다.

1. /opt/Metricbeat/start\_metric.sh 명령어를 실행하여 beat를 실행한다.

종료시에는 stop\_metric.sh 명령어를 싱행하여 종료한다.

1. metric beat가 정상 기동되었는지 확인한다.

[root@HCC-EOWE01P Metricbeat]# ps -ef | grep metric\_os

root 27249 1 0 Oct11 ? 00:12:12 /opt/Metricbeat/metricbeat -E node.name=metric\_os -c /opt/Metricbeat/metricbeat.yml

1. 상세 수정 사항

* Linux OS log
* Webtob Log

#===== OS Message Log =====#

- input\_type: log

enabled: true

fields:

ip: 14.47.120.139

tier: OS

log\_type: linux\_message

company\_name: HWCC

system\_name: smartwork

server\_name: HCC-EOWE01P

fields\_under\_root: true

tail\_files: false

paths:

- /var/log/messages

scan\_frequency: 60s

기타 로그 등등…

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

output.kafka:

hosts: ["172.16.5.97:9092","172.16.5.100:9092","172.16.5.101:9092"]

topic: 'hwcc\_log\_topic'

workers: 1

bulk\_max\_size: 10240

broker\_timeout: 5s

partition.round\_robin:

reachable\_only: false

required\_acks: 1

compression: gzip

max\_message\_bytes: 1000000

* WAS 로그

#===== WEB Access Log =====#

- input\_type: log

enabled: true

fields:

ip: 14.47.120.139

tier: WEB

log\_type: webtob\_access

company\_name: HWCC

system\_name: smartwork

server\_name: HCC-EOWE01P

fields\_under\_root: true

tail\_files: false

paths:

- /data1/logs/web\_log/access.log\_\*

- /data1/logs/web\_log/neo/access.log\_\*

- /data1/logs/web\_log/neo\_ws/access.log\_\*

scan\_frequency: 60s기타 로그 등등…

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

output.kafka:

hosts: ["172.16.5.97:9092","172.16.5.100:9092","172.16.5.101:9092"]

topic: 'hwcc\_log\_topic'

workers: 1

bulk\_max\_size: 10240

broker\_timeout: 5s

partition.round\_robin:

reachable\_only: false

required\_acks: 1

compression: gzip

max\_message\_bytes: 1000000

* Oracle Alert Log

#===== WAS jeusServer Log =====#

- input\_type: log

enabled: true

fields:

ip: 172.19.115.52

tier: WAS

log\_type: jeus\_server

company\_name: HWCC

system\_name: smartwork

server\_name: HCC-EOWS01P

fields\_under\_root: true

# tail\_files: true

paths:

- /data1/logs/jeus\_log/nodeManager/JeusNodeManager.log

- /data1/logs/jeus\_log/adminServer/JeusServer.log

- /data1/logs/jeus\_log/alarm01/JeusServer.log

- /data1/logs/jeus\_log/api01/JeusServer.log

- /data1/logs/jeus\_log/bigmail01/JeusServer.log

- /data1/logs/jeus\_log/daemon01/JeusServer.log

- /data1/logs/jeus\_log/file01/JeusServer.log

- /data1/logs/jeus\_log/mneo01/JeusServer.log

- /data1/logs/jeus\_log/neo01a/JeusServer.log

- /data1/logs/jeus\_log/neo01b/JeusServer.log

- /data1/logs/jeus\_log/sns01/JeusServer.log

scan\_frequency: 60s

multiline.pattern: '^\[\d{4}.\d{2}.\d{2} \d{2}:\d{2}:\d{2}\]'

multiline.negate: true

multiline.match: after scan\_frequency: 60s기타 로그 등등…

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

output.kafka:

hosts: ["172.16.5.97:9092","172.16.5.100:9092","172.16.5.101:9092"]

topic: 'hwcc\_log\_topic'

workers: 1

bulk\_max\_size: 10240

broker\_timeout: 5s

partition.round\_robin:

reachable\_only: false

required\_acks: 1

compression: gzip

max\_message\_bytes: 1000000

#=====Alert Log ======#

- input\_type: log

enabled: true

fields:

ip: 172.19.115.57

tier: DB

log\_type: oracle\_alert

company\_name: HWCC

system\_name: smartwork

server\_name: HCC-EODB01P

fields\_under\_root: true

tail\_files: false

paths:

- /oracle/diag/rdbms/hcceodb/HCCEODB/alert/log.xml

scan\_frequency: 60s

multiline.pattern: '^<msg'

multiline.negate: true

multiline.match: after

……

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

output.kafka:

hosts: ["172.16.5.97:9092","172.16.5.100:9092","172.16.5.101:9092"]

topic: 'hwcc\_log\_topic'

workers: 1

bulk\_max\_size: 10240

broker\_timeout: 5s

partition.round\_robin:

reachable\_only: false

required\_acks: 1

compression: gzip

max\_message\_bytes: 1000000

**[참고 자료]**

1. **한화 케미칼 스마트워크 Beat 설치 정보**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Hostname** | **용도** | **metricbeat** | **winlogbeat** | **filebeat** | **filebeat 대상** |
| hccad01v | 케미칼 AD #1 | O | O |  |  |
| hccad02v | 케미칼 AD #2 | O | O |  |  |
| HCC-DBS01P | 케미칼 Lync DB SVR #1 | O | O | O | MS-SQL |
| HCC-DBS02P | 케미칼 Lync DB SVR #2 | O | O |  |  |
| HCC-EDGE01P | 케미칼 Lync Edge SVR #1 | O | O |  |  |
| HCC-EDGE02P | 케미칼 Lync Edge SVR #2 | O | O |  |  |
| HCC-EX01P | 케미칼 Exchange SVR #1 | O | O |  |  |
| HCC-EX02P | 케미칼 Exchange SVR #2 | O | O |  |  |
| HCC-LYNC01P | 케미칼 Front End SVR #1 | O | O |  |  |
| HCC-LYNC02P | 케미칼 Front End SVR #2 | O | O |  |  |
| HCC-OOS01P | 케미칼 Office Web SVR #1 | O | O |  |  |
| HCC-OOS02P | 케미칼 Office Web SVR #2 | O | O |  |  |
| HCC-SPDB01P | 케미칼 SharePoint DB SVR #1 | O | O | O | MS-SQL |
| HCC-SPDB02P | 케미칼 SharePoint DB SVR #2 | O | O |  |  |
| HCC-SPSC01P | 케미칼 SharePoint Search/App #1 | O | O | O | IIS |
| HCC-SPSC02P | 케미칼 SharePoint Search/App #2 | O | O | O | IIS |
| HCC-SPWF01P | 케미칼 SharePoint Front End #1 | O | O |  |  |
| HCC-SPWF02P | 케미칼 SharePoint Front End #2 | O | O |  |  |
| HCC-EODB01P | 케미칼 포탈 DB #1 | O |  | O | Oracle |
| HCC-EODB02P | 케미칼 포탈 DB #2 | O |  | O | Oracle |
| HCC-EOWE01P | 케미칼 포탈 외부 Web #1 | O |  | O | Webtob |
| HCC-EOWE02P | 케미칼 포탈 외부 Web #2 | O |  | O | Webtob |
| HCC-EOWS01P | 케미칼 포탈 내부 Web #1 | O |  | O | Webtob/Jeus |
| HCC-EOWS02P | 케미칼 포탈 내부 Web #2 | O |  | O | Webtob/Jeus |

1. **시스템 코드**

* 계열사 명 코드

|  |  |  |
| --- | --- | --- |
| **계열사명** | **코드** | **비고** |
| 한화시스템ICT | HWSICT |  |
| 갤러리아 | HWG |  |
| 케미칼 | HWCC |  |
| 토탈/종화 | HTG |  |
| 건설 | HWENC |  |
| 호텔앤드리조트 | HNR |  |
| 에너지 | HEC |  |
| 그룹공통 | HWCM |  |
| G11 | HG11 |  |
| 타임월드 | HTW |  |
| 면세점 | HDF |  |
| 도시개발 | HCID |  |
| 이글스 | HEG |  |
| 한화역사 | HYS |  |
| 한화63시티 | H63 |  |
| 인재경영원 | HRD |  |
| 여천NCC | YNC |  |
| 비앤비 | BNB |  |
| 경영기획실 | MPO |  |
| 가회동 | GAH |  |
| 한화컴파운드 | HCOM |  |
| 기타 | HWETC |  |

* 시스템코드

|  |  |  |
| --- | --- | --- |
| **시스템명** | **system\_name** | **비고** |
| 스마트워크 | smartwork |  |

* Kafka 토픽 코드

|  |  |  |  |
| --- | --- | --- | --- |
| **계열사** | **용도** | **topic** | **비고** |
| 한화시스템 ICT | metric 수집 | hwsict\_metric\_topic |  |
| log 데이터 수집 | hwsic\_log\_topic |  |
| G11 | metric 수집 | g11\_metric\_topic |  |
| log 데이터 수집 | g11\_log\_topic |  |
| 한화케미칼 | metric 수집 | hwcc\_metric\_topic |  |
| log 데이터 수집 | hwcc\_log\_topic |  |
| 한화갤러리아 | metric 수집 | hwg\_metric\_topic |  |
| log 데이터 수집 | hwg\_log\_topic |  |
| 한화호텔앤드리조트 | metric 수집 | hnr\_metric\_topic |  |
| log 데이터 수집 | hnr\_log\_topic |  |
| 한화토탈 | metric 수집 | htg\_metric\_topic |  |
| log 데이터 수집 | htg\_log\_topic |  |