

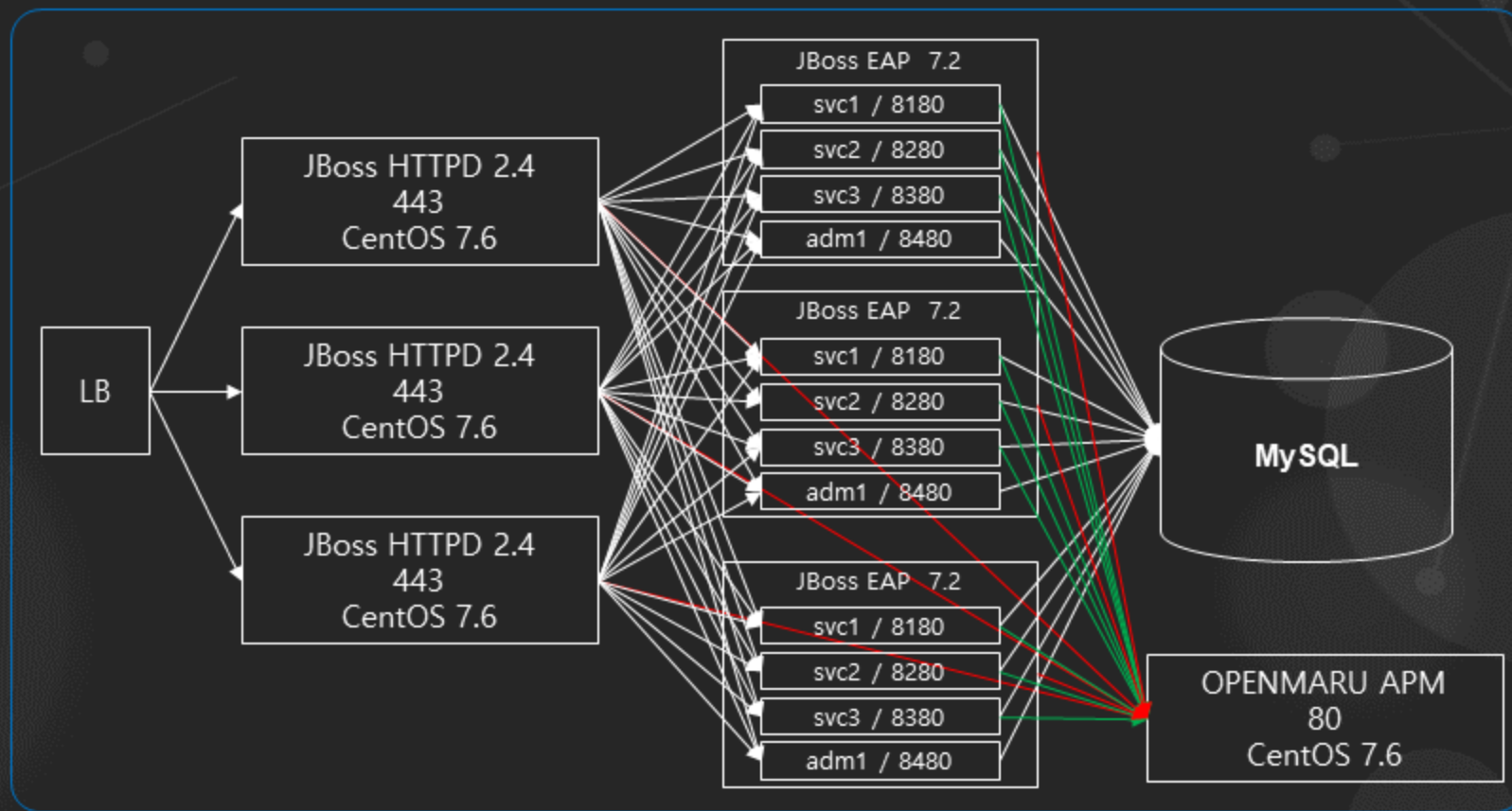
# 컨테이너 환경 로그 통합 데모

- 목적
  - 기존 시스템 및 어플리케이션 로그를 분석하는 방법과 EFK를 이용한 로그 분석 비교 데모로 차이점을 확실히 알기 위함입니다.
- 내용
  - 컨테이너 환경에서 몇번의 클릭만으로 EFK 스택이 배포되는 모습을 확인할 수 있습니다.
  - EFK를 통해 수많은 컨테이너들의 로그를 통합수집하고 시각화하는 모습을 보여줍니다.



MSA, 오토스케일링 다 좋은데..  
그렇게 쪼개놓으면 모니터링 대상이 기존환경 대비  
몇십, 몇백배 늘어나는거 아닌가요?  
이걸 다 어떻게 관리하죠?

# VM 환경 시스템 구성도



PaaS 운영

VM 환경에서 Log 모니터링



## VM환경에서 로그 분석 과정...

1. SSH 접속 툴(putty, secureCRT, Xshell 등) 다운로드
2. 문제가 있는 서버에 IP 혹은 Domain Name 확인
3. 서버에 접속 ID / PW 알아내기
4. 서버에 로그인
5. Tomcat 설치 경로 확인하기
6. Tomcat 설정을 확인해서 로그 파일 위치 찾기
7. 어떤 로그를 봐야할 지 판단하기
8. 해당 로그 파일을 열어 확인하기

# VM환경에서 로그 분석 데모

```
2. demo_web x 3. demo_was x 4. demo_was x +
192.168.23.40 - - [06/Nov/2020:01:08:07 +0900] "GET /simple HTTP/1.1" 302 -
192.168.23.40 - - [06/Nov/2020:01:08:08 +0900] "GET /favicon.ico HTTP/1.1" 200 21630
192.168.23.40 - - [06/Nov/2020:01:08:21 +0900] "GET /favicon.ico HTTP/1.1" 200 21630
192.168.23.40 - - [06/Nov/2020:01:08:21 +0900] "GET /favicon.ico HTTP/1.1" 200 21630
192.168.23.40 - - [06/Nov/2020:01:08:28 +0900] "GET /favicon.ico HTTP/1.1" 200 21630
192.168.23.40 - - [06/Nov/2020:01:08:53 +0900] "GET /simple/index.jsp HTTP/1.1" 200 61
192.168.23.40 - - [06/Nov/2020:01:08:53 +0900] "GET /favicon.ico HTTP/1.1" 200 21630
192.168.23.40 - - [06/Nov/2020:01:08:56 +0900] "GET /simple/index.jsp HTTP/1.1" 200 61
192.168.23.40 - - [06/Nov/2020:01:08:56 +0900] "GET /favicon.ico HTTP/1.1" 200 21630

==> localhost_access_log.2020-11-07.txt <==
::1 - - [07/Nov/2020:02:10:58 +0900] "GET /index.jsp HTTP/1.1" 200 11195
::1 - - [07/Nov/2020:02:11:03 +0900] "GET /simple HTTP/1.1" 302 -
::1 - - [07/Nov/2020:02:13:02 +0900] "GET /simple/session.jsp HTTP/1.1" 200 2020

==> localhost_access_log.2020-11-10.txt <==
192.168.23.227 - - [10/Nov/2020:23:05:45 +0900] "GET /simple/index.jsp HTTP/1.1" 200 61
192.168.23.227 - - [10/Nov/2020:23:05:47 +0900] "GET /simple/index.jsp HTTP/1.1" 200 61
192.168.23.227 - - [10/Nov/2020:23:05:49 +0900] "GET /simple/index.jsp HTTP/1.1" 200 61
192.168.23.227 - - [10/Nov/2020:23:05:51 +0900] "GET /simple/index.jsp HTTP/1.1" 200 61
192.168.23.227 - - [10/Nov/2020:23:05:53 +0900] "GET /simple/index.jsp HTTP/1.1" 200 61
192.168.23.227 - - [10/Nov/2020:23:05:55 +0900] "GET /simple/index.jsp HTTP/1.1" 200 61
192.168.23.227 - - [10/Nov/2020:23:05:57 +0900] "GET /simple/index.jsp HTTP/1.1" 200 61
192.168.23.227 - - [10/Nov/2020:23:05:59 +0900] "GET /simple/index.jsp HTTP/1.1" 200 61
192.168.23.227 - - [10/Nov/2020:23:06:01 +0900] "GET /simple/index.jsp HTTP/1.1" 200 61
192.168.23.227 - - [10/Nov/2020:23:06:03 +0900] "GET /simple/index.jsp HTTP/1.1" 200 61

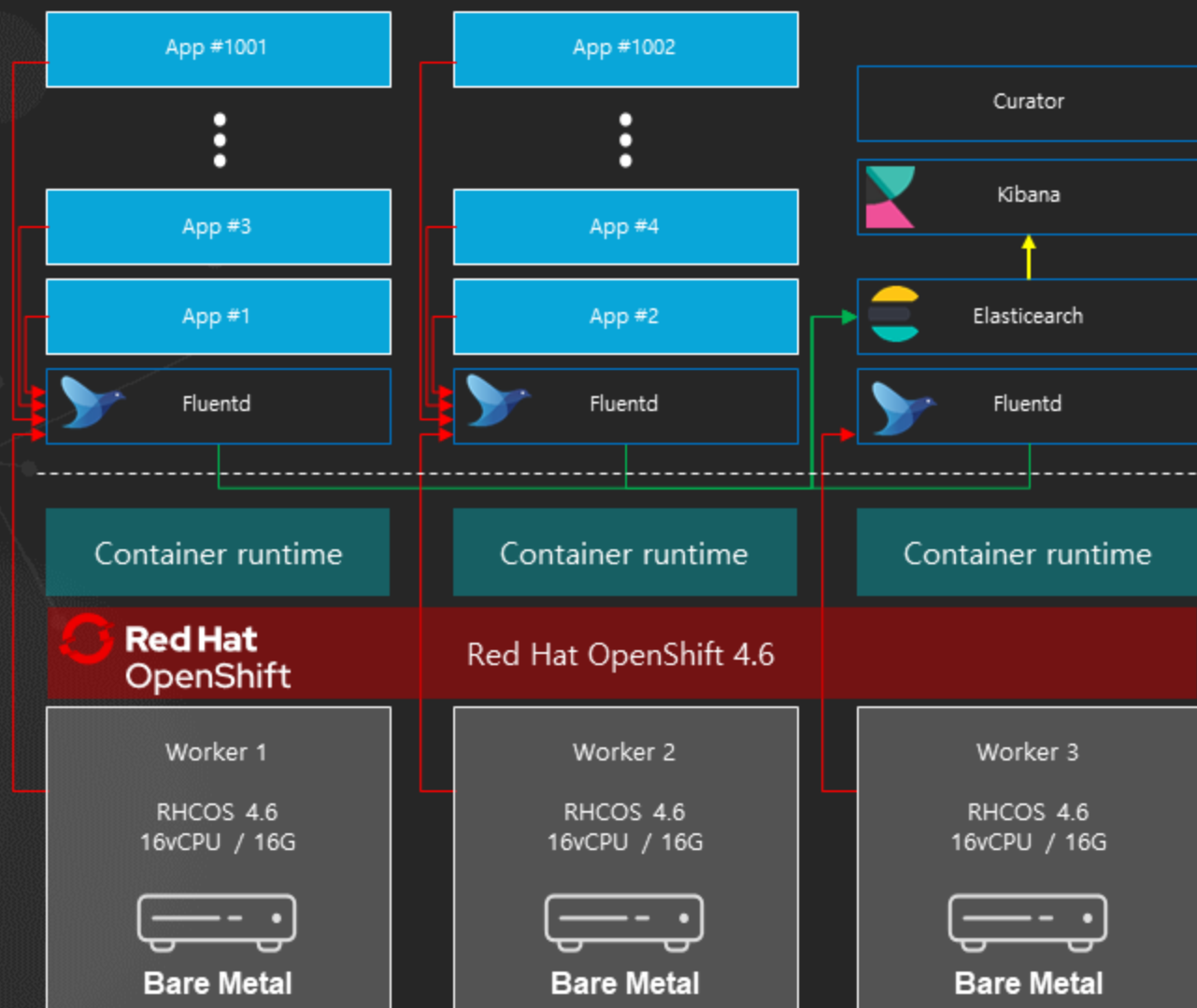
==> manager.2020-11-06.log <==
==> manager.2020-11-10.log <==
```



PaaS 운영

Container 환경에서 Log 모니터링

# Container 환경 테스트 구성도





# EFK 스택 원클릭 배포

The image shows a Red Hat OpenShift console interface and a terminal window. The console displays the 'Overview' page for a cluster, including details like Cluster API Address, Cluster ID, and Status. The Status section shows 'Cluster', 'Control Plane', and 'Operators' are all in a 'Ready' state. The Activity section shows recent events, including errors related to volume 'kibana' and successful image pulls.

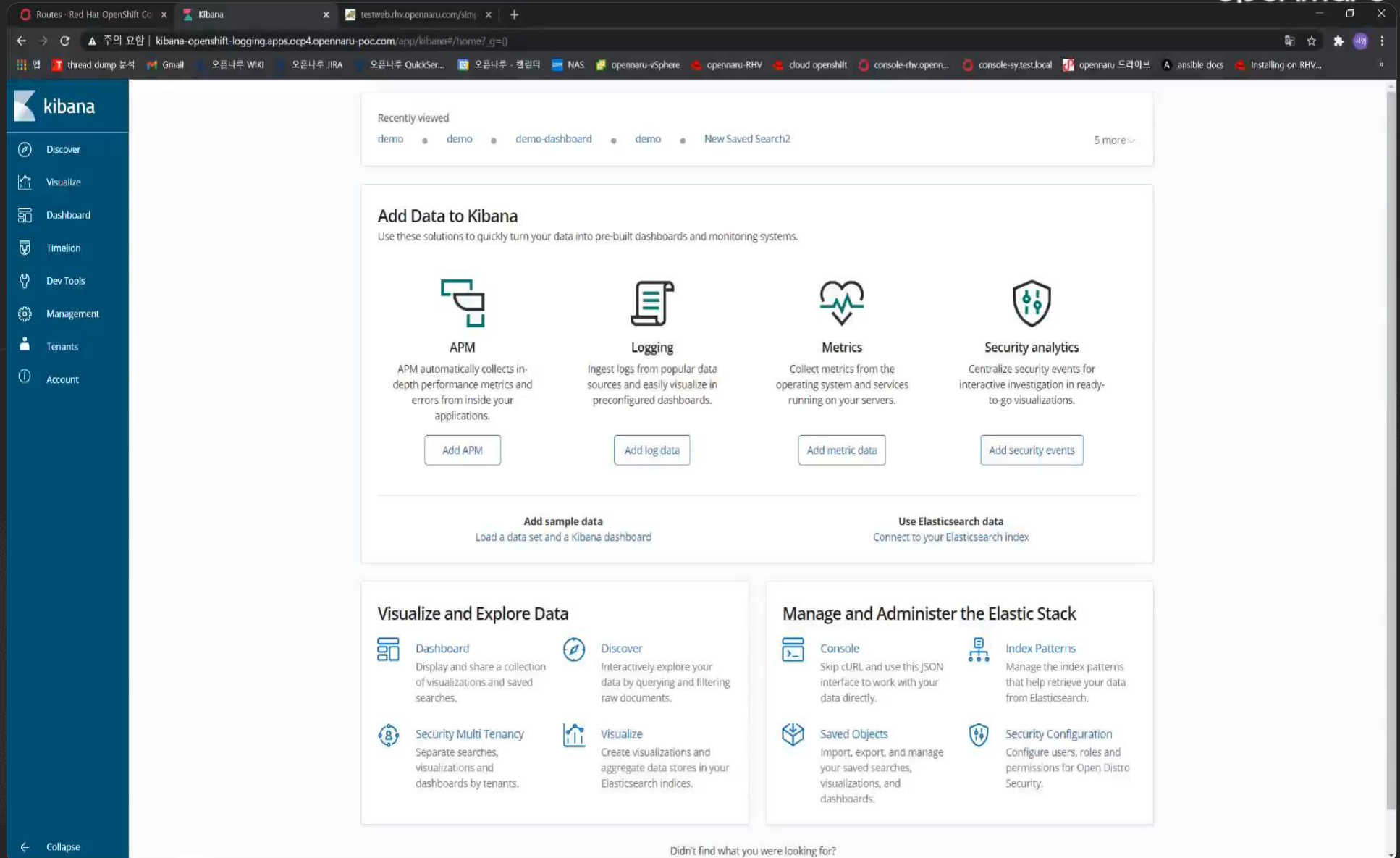
The terminal window shows the following text:

```
Openshift 환경에서 EFK 스택 손쉽게 배포하기

Persistent Volume (Storage)는 미리 준비된 환경입니다.
기본 설정 및 권장사항은
RAM 16G x 3
DISK 200G 이니, 본 환경에서는 스택을 낮춰서 진행하였습니다.

1. Elasticsearch + Fluentd + Kibana Operator 설치
2. ClusterLogging Operator 설치
3. ClusterLogging 인스턴스 생성
```

# Kibana를 통한 로그검색과 데이터시각화



The screenshot shows the Kibana dashboard interface. On the left is a dark blue sidebar with the 'kibana' logo and navigation links: Discover, Visualize, Dashboard, Timelion, Dev Tools, Management, Tenants, and Account. The main content area is white and features several sections:

- Recently viewed:** A horizontal list of recently viewed dashboards including 'demo', 'demo', 'demo-dashboard', 'demo', and 'New Saved Search2', with a '5 more' link.
- Add Data to Kibana:** A section with the heading 'Add Data to Kibana' and the subtext 'Use these solutions to quickly turn your data into pre-built dashboards and monitoring systems.' It contains four cards:
  - APM:** 'APM automatically collects in-depth performance metrics and errors from inside your applications.' Button: 'Add APM'.
  - Logging:** 'Ingest logs from popular data sources and easily visualize in preconfigured dashboards.' Button: 'Add log data'.
  - Metrics:** 'Collect metrics from the operating system and services running on your servers.' Button: 'Add metric data'.
  - Security analytics:** 'Centralize security events for interactive investigation in ready-to-go visualizations.' Button: 'Add security events'.
- Add sample data:** 'Load a data set and a Kibana dashboard'.
- Use Elasticsearch data:** 'Connect to your Elasticsearch index'.
- Visualize and Explore Data:** A section with four cards:
  - Dashboard:** 'Display and share a collection of visualizations and saved searches.'
  - Discover:** 'Interactively explore your data by querying and filtering raw documents.'
  - Security Multi Tenancy:** 'Separate searches, visualizations and dashboards by tenants.'
  - Visualize:** 'Create visualizations and aggregate data stores in your Elasticsearch indices.'
- Manage and Administer the Elastic Stack:** A section with four cards:
  - Console:** 'Skip cURL and use this JSON interface to work with your data directly.'
  - Index Patterns:** 'Manage the index patterns that help retrieve your data from Elasticsearch.'
  - Saved Objects:** 'Import, export, and manage your saved searches, visualizations, and dashboards.'
  - Security Configuration:** 'Configure users, roles and permissions for Open Distro Security.'

At the bottom of the main content area, there is a search bar with the text 'Didn't find what you were looking for?' and a 'Collapse' button in the sidebar.



PaaS 운영

# VM vs Container 로그모니터링 데모 결과



## VM + 로그통합 미적용 환경

1. SSH 접속 툴(putty, secureCRT, Xshell 등) 다운로드
2. 문제가 있는 서버에 IP 혹은 Domain Name 확인
3. 서버에 접속 ID / PW 알아내기
4. 서버에 로그인
5. Tomcat 설치 경로 확인하기
6. Tomcat 설정을 확인해서 로그 파일 위치 찾기
7. 어떤 로그를 봐야할 지 판단하기
8. 해당 로그 파일을 열어 확인하기
9. 특정 로그를 찾을 때까지 모든 Instance 에서 수차례 반복

## Container + EFK 환경

1. kibana 로그인
2. 특정로그 검색조건 적용
3. 검색결과 확인

**Complete !**

**Complete !**



openmaru

제품 / 서비스에 관한 문의

- 콜 센터 : 02-469-5426 ( 휴대폰 : 010-2243-3394 )
- 전자 메일 : [sales@openmaru.com](mailto:sales@openmaru.com)