

ABLESTACK Online Docs ABLESTACK-V4.0-4.0.15



GLUE 설정 가이드

GLUE를 설정하는 방법에 대한 안내입니다.

🚺 Danger

이 문서는 관리자용 문서입니다. 관리자가 아닌 사용자가 동작시 문제가 발생할수도 있습니다.

SSL/TLS 지원

모든 GLUE의 HTTP 연결은 SSL/TLS를 통해 보안을 유지하는것을 기본으로 합니다.

자체 서명 인증서를 새로 생성하기 위해서는 다음과 같은 명령으로 생성할 수 있습니다.

```
$ ceph dashboard create-self-signed-cert
```

🕗 Note

대부분의 브라우저들은 이러한 자체 서명 인증서에 대하여 신뢰할 수 없는 인증서로 표시하며, 신규 연결시 확인과정이 필요합니다.

자체서명 인증서에 대한 경고를 제거하고, 정규 인증서를 사용하기 위해서는 다음과 같은 작업이 필요합니다.

1. 인증서 키 쌍 생성

2. 인증서 인증

3. 인증서 적용

다음은 인증서 키 쌍을 생성하기 위한 예시입니다. 다른 도구를 사용하여 키 쌍을 생성하고 인증기관의 인증을 받는 과정은 생략 합니다.

```
$ openssl req -new -nodes -x509 \
-subj "/O=IT/CN=ceph-mgr-dashboard" -days 3650 \
-keyout GLUE.key -out GLUE.crt -extensions v3_ca
```

위와 같은 작업을 진행하면 GLUE.key, GLUE.crt 파일이 생성됩니다. 이러한 GLUE.crt 파일은 CA(인증기관)에 의해 인증받 아야 합니다. 인증을 받은 뒤 다음 명령어를 통해 해당 인증서를 사용할 수 있습니다.

```
$ ceph dashboard set-ssl-certificate -i GLUE.crt
$ ceph dashboard set-ssl-certificate-key -i GLUE.key
```

만약 각각의 manager 에 대해 별도의 인증서가 발급되었다면, 다음과 같은 방법으로 등록할 수 있습니다.(\$name 은 manager 의 이름입니다. 보통 hostname이 사용됩니다.)

```
$ ceph dashboard set-ssl-certificate $name -i GLUE.crt
$ ceph dashboard set-ssl-certificate-key $name -i GLUE.key
```

다음의 방법으로 SSL 설정을 비활성화 시킬 수 도 있습니다.

이것은 GLUE가 SSL을 지원하지 않는 proxy 뒤에 있거나, 기타 필요한 경우에 사용됩니다. 프록시 설정 문서를 통해 자세한 내용을 확인하세요.

✔ Warning 위 방법을 통해 SSL을 비활성화한 경우, 사용자명과 암호가 암호화되지 않은 상태로 전달됩니다. ✔ Note SSL 인증서와 키를 변경한 경우 반드시 manager 프로세스를 재시작 해야 합니다. 이 과정은 ceph mgr fail mgr 명령을 사용하 거나 다음과 같은 GLUE 명령을 사용해 비활성화 후 활성화 하는 방법으로 적용할 수 있습니다. \$ ceph mgr module disable dashboard \$ ceph mgr module disable dashboard

호스트명과 port

다른 웹 어플리케이션과 같이 GLUE는 TCP/IP 주소와 TCP 포트가 사용됩니다.

기본적으로 ceph-mgr 데몬이 (특히 현재 활성 상태인 mgr이) 8443(혹은 SSL을 사용하지 않는다면 8080)번 포트를 사용해 GLUE를 제공합니다.

TCP/IP 주소가 별도로 특정되지 않았다면 웹앱은 ..., 즉 모든 IPv4및 IPv6 주소로 연결대기 상태가 됩니다.

이러한 기본값은 다음과 같은 전역 설정 변경으로 설정할 수 있습니다.

```
$ ceph config set mgr mgr/GLUE/server_addr $IP
$ ceph config set mgr mgr/GLUE/server_port $PORT
$ ceph config set mgr mgr/GLUE/ssl_server_port $PORT
```

ceph-mgr 이 각각의 GLUE 인스턴스를 제공하므로 이 값은 다음과 같이 별도로 설정 해야 할 수 있습니다.

```
$ ceph config set mgr mgr/GLUE/$name/server_addr $IP
$ ceph config set mgr mgr/GLUE/$name/server_port $PORT
$ ceph config set mgr mgr/GLUE/$name/ssl_server_port $PORT
```

🕗 Note

ceph mgr services 명령은 현재 설정된 서비스의 연결점을 안내해줍니다. dashboard 키를 통해 현재 GLUE에 접속할 수 있는 주소를 얻을 수 있습니다.

사용자명과 비밀번호

GLUE는 로그인을 하기 위한 사용자를 추가하는 명령어를 제공합니다. 생성되는 계정은 하나 이상의 역할이 지정되어야 합니다. GLUE는 사전에 정의된 *system role*을 제공합니다. 자세한 내용은 사용자 및 역할관리 를 참고하세요.

관리자 역할의 사용자를 만들고 싶으면 다음 명령어를 입력하면 됩니다.

\$ceph dashboard ac-user-create <username> -i <file-containing-password> administrator

사용자 잠금

만약 여러번의 잘못된 로그인 시도가 있다면 사용자의 계정은 brute-force 공격이나 dictionary 공격을 방지하기 위해 계정에 잠금을 걸게 된다. 이러한 잠금 설정을 변경하기 위해서 다음 명령어를 사용할 수 있습니다.

```
$ ceph dashboard get-account-lockout-attempts
$ ceph bashboard set-account-lockout-attempts <value:int>
```

🛕 Warning

이 기능은 다음과 같이 시도횟수를 0으로 변경하면 해제됩니다. 하지만 이 기능을 해제하면, brute-force 공격이나 dictionary 공격에 취약해집니다.

 $\$ ceph dashboard set-account-lockout-attempts 0

사용자 잠금 해제

만약 사용자가 여러번의 잘못된 로그인 시도로 인해 잠겼다면, 관리자가 다음 명령어를 사용하여 잠금을 해제 할 수 있습니다.

```
$ ceph dashboard ac-user-enable <username>
```

GLUE 접속

사용자는 자바스크립트가 사용가능한 웹 브라우저를 통해 http(s)://<SCVM IP>:<PORT(기본값:8443)> 으로 GLUE에 접근 가능합니다.

GLUE의 기본 사용자 계정은 ablecloud/password 입니다.

Object Gateway 관리 콘솔 활성화

Object Gateway 관리 기능을 사용하려면 system 플래그가 지정된 사용자 계정이 필요합니다. 만약 아직 system 사용자가 없다면 다음과 같이 생성할 수 있습니다.

\$ radosgw-admin user create --uid=<user_id> --display-name=<display_name> --system

그 다음 표시되는 access_key 와 secret_key 를 기록해 둡니다.

기존 사용자의 키를 얻고자 한다면 다음과 같이 하면 됩니다.

```
$ radosgw-admin user info --uid=<user_id\>
```

여러개의 Object Gateway가 있다면 각각 사용자의 인증정보가 있어야 합니다. 다음과 같이 인증정보를 GLUE에 등록할 수 있 습니다.

```
$ echo -n "{'<daemon1.id\>': '<user1-access-key\>', '<daemon2.id\>': '<user2-access-key\>',
...}" > <file-containing-access-key>
$ echo -n "{'<daemon1.id\>': '<user1-secret-key\>', '<daemon2.id\>': '<user2-secret-key\>',
...}" > <file-containing-secret-key>
$ ceph dashboard set-rgw-api-access-key -i <file-containing-access-key>
$ ceph dashboard set-rgw-api-secret-key -i <file-containing-secret-key>
```

🕗 Note

단일 게이트웨이의 경우 다음과 같이 지정할 수 도 있습니다.

```
$ echo -n "<access-key>" > <file-containing-access-key>
$ echo -n "<secret-key>" > <file-containing-secret-key>
```

단일 RGW 접속점이 있는 간단한 구성에서는 위 작업만 수행하면 GLUE를 통해 Object Gateway 관리 기능을 사용할 수 있습니 다.

만일 여러개의 Object Gateway가 있는경우 아래 작업을 통해 기본값을 설정 해 주어야 합니다.

```
$ ceph dashboard set-rgw-api-host <host>
$ ceph dashboard set-rgw-api-port <port>
```

추가로 다음 설정이 필요 할 수도 있습니다.

```
$ ceph dashboard set-rgw-api-scheme <scheme> # http or https
$ ceph dashboard set-rgw-api-admin-resource <admin_resource>
```

다음 설정을 사용해 GLUE가 자체서명 인증서를 사용한 호스트의 접속을 서명되지 않았거나, 호스트이름이 일치하지 않는다고 거부하는것을 방지해야 합니다.

```
$ ceph GLUE set-rgw-api-ssl-verify False
```

만약 Object Gateway가 요청을 처리하는데 시간이 오래 걸려 timeout이 발생한다면 다음과 같이 시간을 지정할 수 있습니다.

\$ ceph dashboard set-rest-requests-timeout <seconds>

기본값은 45초 입니다.

iSCSI관리 활성화

GLUE는 ceph-iscsi 로 구성된 iSCSI target을 rbd-target-api 의 REST API를 이용하여 관리할 수 있습니다.

```
🕗 Note
```

GLUE의 iSCSI관리 기능은 ceph-iscsi 프로젝트의 최종 3개 버전을 지원합니다.

ceph-iscsi REST API가 HTTPS mode로 설정되고 자체서명인증서를 사용한다면 GLUE가 ceph-iscsi API에 접근할때 거부 하지 않도록 방지해야 합니다.

이러한 SSL 확인 기능을 해제하기 위해서 다음과 같이 합니다.

```
\ ceph dashboard set-iscsi-api-ssl-verification false
```

활성화된 iSCSI gateway는 다음과 같이 등록해주어야 합니다.

\$ ceph dashboard iscsi-gateway-list
\$ # 새로운 Gateway URL은 다음과 같은 형식으로 넣습니다. <scheme>://<username>:<password>@<host>[:port]
\$ ceph dashboard iscsi-gateway-add -i <file-containing-gateway-url> [<gateway_name>]
\$ ceph dashboard iscsi-gateway-rm <gateway_name>

GLUE 내장 Grafana 활성화

Grafana 는 Prometheus 로 부터 데이터를 받아옵니다. Prometheus 는 mgr-prometheus 모듈이 제공하며, 이것은 Node exporter 를 사용해 장비의 측정값을 수집합니다.

🕗 Note

Prometheus의 보안 모델은 신뢰되지 않은 사용자가 HTTP 엔드포인트와 로그에 접속할 수 있다고 가정합니다. 신뢰할 수 없는 사용자는 Prometheus가 수집하는 모든 데이터 및 디버깅 정보를 접근할 수 있습니다. 하지만 이것은 읽기 전용 작업으로 제한됩니다. 자세한 내용은 Prometheus의 보안모델을 참고하세요.

cephadm을 사용한 설치 및 설정

Grafana와 Prometheus는 cephadm 을 사용하여 설치가 가능합니다. 이들은 cephadm 을 사용하여 자동으로 설정까지 완료됩니다. mgr-cephadm-monitoring 문서를 참고하여 Grafana와 Prometheus의 설치 및 구성방법을 확인하세요.

수동 설치 및 구성

아래 설명하는 과정은 Grafana와 Prometheus를 수동으로 구성하는 방법입니다.Prometheus, Grafana, 그리고 Node exporter를 노드에 설치한 다음, 아래 과정을 통해 설정을 진행합니다.

1. Ceph Manager 모듈의 Ceph Exporter를 다음 명령을 통해 실행합니다.

\$ ceph mgr module enable prometheus

자세한 내용은 mgr-prometheus 를 참고하세요.

2. Prometheus에 다음과 같은 수집정책을 설정합니다.

```
global:
    scrape_interval: 5s
scrape_configs:
    - job_name: 'prometheus'
    static_configs:
        - targets: ['localhost:9090']
- job_name: 'ceph'
    static_configs:
        - targets: ['localhost:9283']
- job_name: 'node-exporter'
    static_configs:
        - targets: ['localhost:9100']
```

🕗 Note

위 예시에서 Prometheus는 자기자신(9090), Ceph manager module prometheus 의 ceph 내부 정보(9283), Node Exporter의 OS와 하드웨어 정보(9100)을 수집합니다. 설정에 따라 Node Exporter의 host명을 변경하거나, 추가 설정을 할 수 있습니다.

또한 Ceph의 정보를 얻기 위해 prometheus mgr 모듈을 하나 이상 등록할 *필요는* 없습니다. 하지만 모든 Ceph manager를 등록하는것이 권장 되는데, 이것은 내부의 HA(High Availability)구조를 활성화 하여 일부 Ceph Manager가 중단되더라도 다른 Manager를 통해 정보를 수집할 수 있기 때문입니다.

3. Prometheus를 Grafana에 Grafana Web UI 를 사용해 데이터 소스로 추가합니다.

4. vonage-status-panel 과 grafana-piechart-panel plugins을 설치합니다.

\$ grafana-cli plugins install vonage-status-panel \$ grafana-cli plugins install grafana-piechart-panel

5. Grafana에 dashboard를 추가합니다.:

dashboard JSON 파일을 사용하여 Grafana에 대시보드를 추가할 수 있습니다.

```
wget https://raw.githubusercontent.com/ceph/ceph/master/monitoring/grafana/GLUEs/<GLUE-
name>.json
```

dashboard JSON 파일은 여기에서 찾을 수 있습니다.

예를 들어 ceph-cluster overview dashboard를 추가하고자 한다면

wget https://raw.githubusercontent.com/ceph/ceph/master/monitoring/grafana/GLUEs/cephcluster.json 를 사용할 수 있습니다.

혹은 직접 새로운 dashboard를 생성할 수도 있습니다.

6. /etc/grafana/grafana.ini 에서 익명 모드를 사용할 수 있습니다.

```
[auth.anonymous]
enabled = true
org_name = Main Org.
org_role = Viewer
```

6.2.0-beta1 버전 이상의 Grafana에는 allow_embedding 옵션이 추가되었습니다. 이 옵션은 반드시 true 로 되어 있어 야 GLUE에 내장할 수 있습니다. 기본값은 false 입니다.

```
[security]
allow_embedding = true
```

RBD-Image monitoring 활성화

RBD 이미지의 모니터링은 기본적으로 비활성화 되어있고, 성능에 상당한 영향을 줍니다. 자세한 내용은 prometheus-rbd-iostatistics 을 참고하세요. 비활성화 된 경우 Grafana의 overview와 상세 dashboard가 표시되지 않습니다.

dashboard 설정

Grafana와 Prometheus를 설치한 뒤, Grafana의 연결정보를 GLUE에 등록해야 합니다. Grafana의 URL을 GLUE에 등록하기 위해 다음 명령을 사용합니다.

\$ ceph dashboard set-grafana-api-url <grafana-server-url> # default: ''

URL 형식은 다음과 같습니다 <protocol>:<IP-address>:<port>

🕗 Note

GLUE는 Grafana dashboard를 iframe 으로 내장합니다. 만약 Grafana가 SSL/TLS없이 설정되었다면, 대부분의 브라우저는 보 안되지 않은 콘텐츠를 SSL을 지원하는 페이지(GLUE는 기본적으로 SSL이 적용됩니다)에 내장하는것을 차단하기 때문에 사용에 지 장이 있을 수 있습니다. 만약 내장 Grafana dashboard가 보이지 않는다면, 브라우저의 문서를 통해 이러한 혼합 content를 허용 하도록 해야 합니다. 혹은 SSL/TLS를 Grafana에 적용하는것을 고려하세요.

Grafana에 자체서명 인증서를 사용하는경우 GLUE가 연결을 거부하지 않도록 다음과 같은 명령이 필요합니다.

```
$ ceph GLUE set-grafana-api-ssl-verify False
```

직접 Grafana에 접근하여 클러스터를 모니터링 할 수도 있습니다.

✓ Note GLUE에서 다음 명령을 사용하여 위에서 설정한 설정정보를 초기화 시킬 수 있습니다. \$ ceph dashboard reset-grafana-api-url

브라우저를 위한 대체 URL

GLUE는 Grafana dashboard를 화면상에 보여주기 이전부터 Grafana의 존재를 확인하기 위해 URL을 필요로 합니다. 그렇기 때문에 다음과 같이 2시점의 연결이 필요하게 됩니다.

• Backend(Ceph Mgr module): 요청한 그래프의 존재를 확인하기 위해 필요합니다. 이 요청이 정상적으로 처리되면, Frontend에 Grafana에 접근이 가능하다고 알립니다. • Frontend: Grafana 그래프에 iframe을 사용하여 직접 접속합니다. 이 요청은 GLUE를 거치지 않고, 사용자의 브라우저에 서 처리됩니다.

이제 사용자 브라우저가 GLUE에 설정된 Grafana주소에 접근하기 어려운 상황을 가정해 봅시다. 이 문제를 해결하기 위해 Frontend(사용자 브라우저)가 접근할 수 있는 Grafana의 주소를 추가로 등록 해 주면 됩니다. cephadm (cephadm을 사용하 여 설치한 경우)에 등록하는 GRAFANA_API_URL 과 달리 이 설정은 자동으로 변경되지 않습니다.

이런 경우를 해결하기 위해 다음 명령어를 사용할 수 있습니다.

\$ ceph dashboard set-grafana-frontend-api-url <grafana-server-url<>

이 옵션에 아무 값도 설정되지 않은경우 GRAFANA_API_URL 의 값으로 접속을 시도합니다. 옵션에 값이 설정되어있다면, 설정된 주소의 Grafana에 접속합니다.

Single Sign-On (SSO) 설정

GLUE는 SAML 2.0 프로토콜을 사용한 외부 인증을 지원합니다. 먼저 GLUE에 적절한 역할과 그 역할에 연결된 사용자가 생성되어야 합니다. 하지만 인증과정은 외부 인증 제공자(IdP: Identity Provider)에 의해 진행됩니다.

🕗 Note

GLUE SSO지원은 onelogin의 python-saml 라이브러리에 제공됩니다. 이 라이브러리가 시스템에 설치되었는지 확인하세요

SSO는 다음과 같이 설정할 수 있습니다.

```
$ ceph dashboard sso setup saml2 <ceph_GLUE_base_url> <idp_metadata> {<idp_username_attribute>}
{<idp_entity_id>} {<sp_x_509_cert>} {<sp_private_key>}
```

Parameters:

- <ceph_GLUE_base_url>: GLUE 에 접속하는 기본 URL(e.g., https://cephGLUE.local)
- <idp_metadata>: 원격(http://, https://)이나 로컬(file://)IdP metadata XML 경로(e.g., https://myidp/metadata, file:///home/myuser/metadata.xml).
- **<idp_username_attribute>** (optional): 요청 중 사용자명을 갖고 오는 attribute 이름. 기본값은 uid.
- **<idp_entity_id>** *(optional)*: IdP metadata에 하나 이상의 entity가 있는경우.
- <sp_x_509_cert> / <sp_private_key> (optional): GLUE Service 제공자가 서명과 암호화에 사용할 인증서 파일경 로

🕗 Note

SAML 요청의 요청자 값은 다음과 같은 패턴으로 만들어집니다.

<ceph_GLUE_base_url>/auth/saml2/metadata

현재 설정된 SAML 2.0 구성을 확인하려면 다음 명령어를 사용합니다.

🕗 Note

onelogin_setting 에 대한 자세한 내용은 onelogin documentation 을 참고하세요.

추가 명령어

```
# SSO 설정 확인
$ ceph GLUE sso status
# SSO 비활성화
$ ceph GLUE sso disable
# SSO 활성화
$ ceph GLUE sso enable sam12
```

Prometheus를 사용한 경고 설정

Prometheus 경고 기능을 사용하려면 먼저 alerting rules 을 설정해야 합니다. 이 기능은 Alertmanager 에서 관리합니다. 만약 Alertmanager가 설치되지 않았다면 설치를 먼저 진행해야 Prometheus로부터 경고를 받을 수 있습니다.

Alertmanager기능을 다음과 같은 3가지 모드로 사용할 수 있습니다.

- 1. dashboard의 알림만 받기
- 2. Prometheus Alertmanager API를 사용한 알림 받기
- 3. 두가지 알림 모두 받기

세가지 모드 모두 경고에 대한 알림을 받을 수 있습니다. 3번의 모두 받기의 경우 알림이 두번 오지는 않습니다. 침묵(silence)기 능을 사용하기 위해서는 API기능을 사용하는 2번, 3번 중 선택해야 합니다.

1. dashboard의 알림만 받기

이 방법은 Alertmanager의 설정 에 따라 알림을 받습니다. 경고가 발생하면 GLUE에 알림이 표시됩니다. 하지만 경고를 관리 할 수는 없습니다. GLUE 수신자를 추가하고 새로운 전송경로를 AlertManager의 설정에 넣습니다. 설정파일은 다음과 같이 구성 되어야 합니다.

```
route:
    receiver: 'ceph-dashboard'
...
receivers:
    - name: 'ceph-dashboard'
    webhook_configs:
    - url: '<url-to-GLUE\>/api/prometheus_receiver'
```

Alertmanager에 SSL 인증서를 설정하는것이 좋습니다. 자세한 내용은 문서">http-config>문서 를 참고하세요.

1. Prometheus Alertmanager API를 사용한 알림 받기

경고와 침묵(silence)를 관리 할 수 있고, "Cluster" 메뉴의 "Monitoring" 섹션에 "Active Alerts", "All Alerts", "Silences" 탭 이 생성됩니다. 경고는 이름, 작업, 중요성, 상태, 발생시간으로 정렬이 가능합니다. 사용자의 구성에 따라 Alertmanager가 알림 을 전송한 시기를 알 수는 없습니다.

침묵(Silence) 또한 id, 생성자, 상태, 시작/수정/종료 시간에 따라 정렬이 가능합니다. 침묵은 다양한 방법으로 만들어지고, 파기 될 수 있습니다.

1. 처음부터 생성

- 2. 선택된 경고로 부터 생성
- 3. 파기된 침묵으로 재생성
- 4. 기존 침묵 수정(새로 생성하고 기존의 것을 파기)

이 모드를 사용하려면 Alertmanager server의 호스트 및 포트를 지정해야 합니다.

\$ ceph dashboard set-alertmanager-api-host <alertmanager-host:port> # default: ''

예시:

\$ ceph dashboard set-alertmanager-api-host 'http://localhost:9093'

모든 설정된 경고를 보기 위해서 Prometheus API에 URL을 설정해야 합니다. 이 API를 사용하면 UI가 새로운 침묵을 해당 경고 와 일치하는지 확인하는데 도움이됩니다.

\$ ceph dashboard set-prometheus-api-host <prometheus-host:port\> # default: ''

예시:

\$ ceph dashboard set-prometheus-api-host 'http://localhost:9090'

설정한 다음 GLUE 창이나 탭을 새로고침 합니다.

1. 두가지 알림 모두 받기

이 모드는 중복된 알림이 서로를 방해하는일이 발생하지 않도록 구성되어야 합니다.

Prometheus와 Alertmanager에 자체서명 인증서를 사용하는경우 인증서 검증을 비활성화 하여 GLUE가 연결을 거부하지 않 도록 해야합니다.

• Prometheus:

\$ ceph dashboard set-prometheus-api-ssl-verify False

• Alertmanager:

\$ ceph dashboard set-alertmanager-api-ssl-verify False

ABLESTACK Online Docs