ABLESTACK Online Docs

ABLESTACK-V4.0-4.0.15

사용자 및 역할 관리

사용자 및 역할 관리

Danger

이 문서는 기술지원 용도의 문서입니다. 기술지원 엔지니어가 아닌 사용자가 조작할 때 시스템에 문제가 발생할 수 있습니다.

사용자 및 역할 관리에서는 다음과 같은 기능을 제공합니다.

비밀번호 정책

비밀번호 정책은 기본적으로 다음의 항목을 포함하여 활성화됩니다.

- 최소 비밀번호 길이가 N 이상인가요?
- 기존 비밀번호와 신규 비밀번호가 다른가요?

비밀번호 정책은 다음의 명령어를 이용하여 활성화 또는 비활성화 할 수 있습니다.

```
ceph dashboard set-pwd-policy-enabled <true|false>
```

다음의 명령어를 이용하여 개별 검사 항목도 켜거나 끌 수 있습니다.

```
ceph dashboard set-pwd-policy-check-length-enabled <true|false>
```

```
ceph dashboard set-pwd-policy-check-oldpwd-enabled <true|false>
```

```
ceph dashboard set-pwd-policy-check-username-enabled <true|false>
```

```
ceph dashboard set-pwd-policy-check-exclusion-list-enabled <true|false>
```

```
ceph dashboard set-pwd-policy-check-complexity-enabled <true|false>
```

```
ceph dashboard set-pwd-policy-check-sequential-chars-enabled <true|false>
```

```
ceph dashboard set-pwd-policy-check-repetitive-chars-enabled <true|false>
```

또한 다음의 명령어를 사용하여 비밀번호 정책의 옵션을 설정할 수 있습니다.

- 비밀번호 최소 길이 (기본값 : 8)

  ```
  ceph dashboard set-pwd-policy-min-length <N>
  ```

- 비밀번호 복잡도 (기본값 : 10)

  ```
  ceph dashboard set-pwd-policy-min-complexity <N>
  ```

비밀번호 복잡도는 비밀번호 각 문자를 분류하여 계산됩니다. 복잡도는 0부터 시작되며, 문자는 다음 규칙에 따라 등급이 지정됩니다.

- 비밀번호 복잡도 규칙

  문자가 숫자이면 1이 증가합니다.

  문자가 소문자 ASCII 문자이면 1이 증가합니다.

  문자가 대문자 ASCII 문자이면 2가 증가합니다.

  문자가 다음과 같은 특수 문자이면 3이 증가합니다. `!"#$%&'()*+,-./:;<=>?@[\]^_`~

  문자가 위 규칙에 포함되지 않는 경우 5가 증가합니다.

비밀번호에 특정 단어를 포함하지 않게 할 수 있습니다. 여러개의 단어는 쉼표로 구분합니다.

```
ceph dashboard set-pwd-policy-exclusion-list <word>[,...]
```

사용자 계정

Glue 대시보드는 여러 사용자 계정을 지원합니다. 각 사용자 계정은 사용자 이름과 비밀번호로 구성되며 옵션으로 이름과 이메일 주소를 입력할 수 있습니다. 웹 UI를 통해 새 사용자가 생성 된 경우 사용자가 처음 로그인 할 때 새 암호를 할당해야하는 옵션을 설정할 수 있습니다. 사용자 계정은 모니터의 구성 데이터베이스에 저장되며 모든 ceph-mgr 인스턴스에서 사용할 수 있습니다.

사용자 계정을 관리하기 위한 CLI 명령은 다음과 같습니다.

- 사용자 표시

  ```
  ceph dashboard ac-user-show [<username>]
  ```

- 사용자 생성

  ```
  ceph dashboard ac-user-create [--enabled] [--force-password] [--pwd_update_required]
  <username> -i <file-containing-password> [<rolename>] [<name>] [<email>]
  [<pwd_expiration_date>]
  ```

  > **Info**
  >
  > force-password 옵션을 사용하여 비밀번호 정책 검사를 우회할 수 있습니다.
  >
  > 새로 생성된 사용자가 처음 로그인 할 때 비밀번호를 변경하도록 하려면 pwd_update_required 옵션을 사용합니다.

- 사용자 삭제

  ```
  ceph dashboard ac-user-delete <username>
  ```

- 비밀번호 변경

```
ceph dashboard ac-user-set-password [--force-password] <username> -i <file-containing-password>
```

- 비밀번호 해시 변경

```
ceph dashboard ac-user-set-password-hash <username> -i <file-containing-password-hash>
```

> **Info**
>
> 해시는 bcrupt 해시 및 솔트 값 이어야 합니다. 외부 데이터베이스에서 사용자를 가져오는데 사용할 수 있습니다.

- 사용자(이름 및 이메일) 수정

```
ceph dashboard ac-user-set-info <username> <name> <email>
```

- 사용자 비활성화

```
ceph dashboard ac-user-disable <username>
```

- 사용자 활성화

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

사용자 역할 및 권한

사용자 계정은 접근할 수 있는 대시보드 기능을 정의하는 역할 집합과 관련이 있습니다. 대시보드 기능 및 모듈은 보안 범위 안에서 그룹화 됩니다. 보안 범위는 사전 정의 되고 정적입니다. 현재 사용 가능한 보안 범위는 다음과 같습니다.

- 보안 범위

  host : Hosts메뉴 항목 과 관련된 모든 기능을 포함합니다.

  config-opt : Ceph 구성 옵션 관리와 관련된 모든 기능을 포함합니다.

  pool : 풀 관리와 관련된 모든 기능을 포함합니다.

  osd : OSD 관리와 관련된 모든 기능을 포함합니다.

  monitor : 모니터 관리와 관련된 모든 기능을 포함합니다.

  rbd-image : RBD 이미지 관리와 관련된 모든 기능을 포함합니다.

  rbd-mirroring : RBD 미러링 관리와 관련된 모든 기능을 포함합니다.

  iscsi : iSCSI 관리와 관련된 모든 기능을 포함합니다.

  rgw : RGW (RADOS Gateway) 관리와 관련된 모든 기능을 포함합니다.

  cephfs : CephFS 관리와 관련된 모든 기능을 포함합니다.

  manager : Ceph Manager 관리와 관련된 모든 기능을 포함합니다.

  log : Ceph 로그 관리와 관련된 모든 기능을 포함합니다.

grafana : Grafana 프록시와 관련된 모든 기능을 포함합니다.

prometheus : Prometheus 경보 관리와 관련된 모든 기능을 포함합니다.

dashboard-settings : 대시보드 설정을 변경할 수 있습니다.

역할은 보안 범위와 권한 사이의 매핑 집합을 지정합니다. 다음과 같은 네 가지 유형의 권한이 있습니다.

- 권한 유형

  읽기 (read)

  생성 (create)

  업데이트 (update)

  삭제 (delete)

다음은 파이썬 딕셔너리 형태의 역할 사양의 예시입니다.

```
# example of a role
{
  'role': 'my_new_role',
  'description': 'My new role',
  'scopes_permissions': {
    'pool': ['read', 'create'],
    'rbd-image': ['read', 'create', 'update', 'delete']
  }
}
```

위의 역할은 사용자에게 풀 관리와 관련된 기능에 대한 읽기 및 생성 권한과 RBD 이미지 관리와 관련된 기능에 대한 전체 권한이 있음을 나타냅니다.

대시 보드는 새로운 Ceph Dashboard 설치에서 즉시 사용할 수있는 시스템 역할 이라고하는 사전 정의 된 역할 세트를 제공 합니다.

- 시스템 역할 목록

  administrator : 모든 보안 범위에 대한 전체 권한을 허용합니다.

  read-only : 대시 보드 설정을 제외한 모든 보안 범위에 대한 읽기 권한을 허용합니다.

  block-manager : rbd-image , rbd-mirroring 및 iscsi 범위에 대한 전체 권한을 허용합니다.

  rgw-manager : rgw 범위에 대한 전체 권한을 허용합니다.

  cluster-manager : hosts , osd , monitor , manager 및 config-opt 범위에 대한 전체 권한을 허용합니다.

  pool-manager : 풀 범위에 대한 전체 권한을 허용합니다.

  cephfs-manager : cephfs 범위에 대한 전체 권한을 허용합니다.

사용 가능한 역할 목록은 다음의 명령어를 이용하여 검색할 수 있습니다.

```
ceph dashboard ac-role-show [<rolename\>]
```

CLI를 이용하여 새로운 역할을 만들 수 있습니다. 사용 가능한 명령어는 다음과 같습니다.

- 역할 생성

```
ceph dashboard ac-role-create <rolename\> [<description\>]
```

- 역할 삭제

```
ceph dashboard ac-role-delete <rolename\>
```

- 역할에 범위 권한 추가

```
ceph dashboard ac-role-add-scope-perms <rolename\> <scopename\> <permission\>
[<permission\>...]
```

- 역할에서 범위 권한 삭제

```
ceph dashboard ac-role-del-scope-perms <rolename\> <scopename\>
```

사용자에게 역할을 지정하려면 다음의 명령어를 이용합니다.

- 사용자 역할 설정

```
ceph dashboard ac-user-set-roles <username\> <rolename\> [<rolename\>...]
```

- 사용자에게 역할 추가

```
ceph dashboard ac-user-add-roles <username\> <rolename\> [<rolename\>...]
```

- 사용자의 역할 삭제

```
ceph dashboard ac-user-del-roles <username\> <rolename\> [<rolename\>...]
```

사용자 및 사용자 지정 역할 생성 예시

이 섹션에서는 RBD 이미지를 관리하고 Ceph 풀을 만들 수 있으며 다른 범위에 대한 읽기 전용 액세스 권한이있는 사용자 계정을 생성하는 명령의 전체 예를 보여줍니다.

사용자 계정을 생성하고 역할을 생성하려면:

1. 사용자를 생성합니다.

```
ceph dashboard ac-user-create bob -i <file-containing-password\>
```

2. 역할을 생성하고 범위 권한을 지정합니다.

```
ceph dashboard ac-role-create rbd/pool-manager
```

```
ceph dashboard ac-role-add-scope-perms rbd/pool-manager rbd-image read create update delete
```

```
ceph dashboard ac-role-add-scope-perms rbd/pool-manager pool read create
```

3. 사용자에게 역할을 할당합니다.

```
ceph dashboard ac-user-set-roles bob rbd/pool-manager read-only
```

ABLESTACK Online Docs