IxM - CLI Reference

Document Level Classification

200

- Should I be using IxM?
- IxM common use-cases and CLI
- User Guide
    - Common tasks that use the ixm-cli inlude:
    - Authorize new security group rules
    - Viewing current service status
    - Revoke an existing security group rule
    - Modifying a security group directly
- Tutorial
    - Allowing traffic from account beee-live in fcfd-live

Should I be using IxM?

Since the rollout of the Service Network, most teams should be looking at migrating from internet facing load balancers to internal load balancers on

the Service Network. If your load balancer is on the Service Network you should no longer be using IxM and you should instead be managing ingress traffic using Ingress annotations. For instructions on using ingress annotations for internal load balancers reference Manage inbound network traffic to your Internal Application Load Balancer (with Service Network Annotations)

In cases where your load balancer is internet facing, teams should also be looking at managing ingress traffic with annotations instead of using IxM as this allows you to use IaC to manage access instead of relying on the IxM tool. For instructions on using ingress annotations for internet facing load balancers reference Manage inbound network traffic to your Public Application Load Balancer (with Security Groups, Prefix Lists, or Inbound CIDR annotations)

The documentation that follows is an old method of using Terraform and IxM to manage traffic to your load balancer. Using this method should be avoided in favor of one of the methods listed above using annotations.

IxM common use-cases and CLI

ixm-cli requires AWS credentials to the AWS account where your service runs. Setup your credentials using aop.

```
 Usage:
  ixm [command]

Available Commands:
  help        Help about any command
  pl          Retrieve information about IxM prefix lists
  service     Manage ingress rules for services using IxM prefix lists
  sg          Retrieve information about EC2 security groups
```

```
Flags:
  -h, --help             help for ixm
      --profile string   AWS profile
      --region string    AWS region (default "us-east-1")
  -v, --version          version for ixm

Use "ixm [command] --help" for more information about a command.
```

User Guide

The ixm-cli allows you to easily configure the security groups for your services running in AWS by using the set of pre-defined prefix lists.

To get started, download the latest release. You'll also need aop configured so that you have api access to your AWS account.

Common tasks that use the ixm-cli inlude:

- Authorizing additional entities to connect to your service, such as another team's AWS account or Epic VPN users.
- Viewing current services status including currently applied security group rules.
- Revoking existing security group rules from your service.

Each of these tasks are shown in more detail below.

Authorize new security group rules

First, you must decide which prefix lists contain the rules you want to add. The available prefix lists can be fetched using the `ixm pl status` command. Some common prefix lists that you may want to add are:

- `ixm.office-and-vpn` - IP CIDR ranges for Epic offices and VPN gateways. This allows Epic employees to connect to your service.

- `ixm.codefresh-agents` - IP CIDR range to allow codefresh build agents to connect to your service.
- `ixm.teamcity-agents` - Same as `ixm.codefresh-agents`, but for teamcity agents.
- `ixm.us-east-1.oldprod-dev` / `ixm.us-east-1.oldprod-live` - Public IP CIDR ranges for oldprod VPCs (NAT Gateways).

Note: For other services in the same account to access the target service, the prefix-list for your account (eg. `ixm.us-east-1.abcd-dev`) must be added to the target service's security group.

Once you've decided on the prefix list to use, execute the following command to add it to your service's security group. The `-s/--source` flag defines the source to use for the ingress rule. Multiple sources can be specified at a time.

```
ixm service authorize my-service.abcd.dev.use1a.on.epicgames.com -s ixm
```

The cli will prompt you to select a security group if more than one security group is attached to the service.

Finally, confirm the change to complete the modification

Viewing current service status

Use the following command to retrieve the current status for a service including any loadbalancer information and security group rules:

```
$ ixm service status my-service.abcd.dev.use1a.on.epicgames.com
Service Name        =  my-service.abcd.dev.use1a.on.epicgames.com
Load Balancer Name  =  d7c73355-teamonlineinfrapl-dea7
Status              =  active
Type                =  application
DNS Name            =  d7c73355-teamonlineinfrapl-dea7-1295862778.us-ea

Security Groups
Name                        ID                    Description
my-service-security-group   sg-0cb468d7cc58b5e68   a security group for m
```

```
Security Group Rules
ID                    Port Range  Protocol  Source
sg-0cb468d7cc58b5e68  0-65535     tcp       pl-0b866de39027894b0 (ixm.u
sg-0cb468d7cc58b5e68  0-65535     tcp       pl-07f9bae5386e99c4e (ixm.o
sg-0cb468d7cc58b5e68  0-65535     tcp       pl-0a9eb4e75f1665a3f (ixm.u
```

Revoke an existing security group rule

The process for revoking a security group rule is the reverse of authorization. After running the status command to determine the existing rules, use the following command to revoke the desired rule:

```
ixm service revoke my-service.abcd.dev.use1a.on.epicgames.com -s ixm.us
```

Modifying a security group directly

Most of the time you should use the `ixm service authorize/revoke` subcommands to modify security group rules because it alerts you about which load balancers will be affected by the change.

However, in some scenarios you might need to modify a security group directly. In that case, you can use the `ixm sg authorize/revoke` commands which work similarly to the service commands above.

```
ixm sg authorize sg-0cb468d7cc58b5e68 -s ixm.us-east-1.dead-dev-uam-aut
```

Tutorial

Allowing traffic from account beee-live in fcfd-live

After AWS SSO adoption in AOP, the login changed.

Building from source code

```
git clone https://github.ol.epicgames.net/substrate/ixm-cli
cd ixm-cli
make build
cd bin
ls
```

After having ixm installed

```
# Login
aop aws-sso generate
aws configure list-profiles
export AWS_PROFILE=fcfd-live-admin
aws sso login

# Checking the Status of the Service you want to enable
ixm service status developer-access-control-prod.fcfd.live.use1a.on.epi

#  Applying changes
ixm service authorize developer-access-control-prod.fcfd.live.use1a.on.
-s ixm.us-east-1.beee-live

# Checking the applied changes
ixm service status developer-access-control-prod.fcfd.live.use1a.on.epi
```