Epic Games - Cloud Developer Platform

IxM Terraform Guide

Downloaded from Epic Games Confluence
Date: 2025-07-12 04:07:17
Original URL: https://confluence-epicgames.atlassian.net/wiki/spaces/CDE/pages/81068326

Document Level Classification

200

Introduction

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.

Security group rules can be configured with Terraform using the official AWS provider.

Prefix lists are automatically shared with each Substrate AWS account. A prefix list is a container for one or more CIDR blocks. In IxM, these represent the public facing CIDRs of Substrate accounts, or other important networks like Epic offices and VPN.

You can use Terraform to make this change and store the configuration in Github.

Terraform Config

The first step is to use the managed prefix list data source to fetch the prefix list details. You can use multiple data sources for adding multiple rules

```
data "aws_ec2_managed_prefix_list" "office_and_vpn" {
  name = "ixm.office-and-vpn"
}

data "aws_ec2_managed_prefix_list" "account_abcd_dev" {
  name = "ixm.us-east-1.abcd-dev"
}
```

The second step is to use these prefix lists to create security group rules:

```
resource "aws_security_group" "new_security_group" {
  name        = "new_security_group"
  description = "Allow inbound traffic to my service"
  vpc_id      = aws_vpc.main.id

  ingress {
    description     = "TLS"
    from_port       = 443
    to_port         = 443
    protocol        = "tcp"
    prefix_list_ids = [data.aws_ec2_managed_prefix_list.office_and_vpn.
  }

  egress {
    from_port   = 0
    to_port     = 0
    protocol    = "-1"
    cidr_blocks = ["0.0.0.0/0"]
  }
}

resource "aws_security_group_rule" "account_abcd" {
  type              = "ingress"
  from_port         = 0
  to_port           = 65535
  protocol          = "tcp"
  prefix_list_ids   = [data.aws_ec2_managed_prefix_list.account_abcd_de
  security_group_id = "sg-123456"
}
```

Page Information:

Page ID: 81068326

Space: Cloud Developer Platform

Downloaded: 2025-07-12 04:07:17