```
resource "aws_security_group" "k8s_master_sg" {
  name        = "k8s_master_sg"
  description = "Security group for Kubernetes master"
  vpc_id      = aws_vpc.main.id

  ingress {
    from_port   = 6443
    to_port     = 6443
    protocol    = "tcp"
    cidr_blocks = ["0.0.0.0/0"]
  }
  ingress {
    from_port   = 12250
    to_port     = 12550
    protocol    = "tcp"
    cidr_blocks = ["0.0.0.0/0"]
  }
  ingress {
    from_port   = 12255
    to_port     = 12555
    protocol    = "tcp"
    cidr_blocks = ["0.0.0.0/0"]
  }
  ingress {
    from_port   = 12257
    to_port     = 12557
```

```
  protocol    = "tcp"
  cidr_blocks = ["0.0.0.0/0"]
}
ingress {
  from_port   = 30000
  to_port     = 32767
  protocol    = "tcp"
  cidr_blocks = ["0.0.0.0/0"]
}
# New ingress rule for SSH access
ingress {
  from_port   = 22
  to_port     = 22
  protocol    = "tcp"
  cidr_blocks = ["0.0.0.0/0"]  # Adjust this to a more restricted CIDR block for enhanced security
}

# Prometheus
ingress {
  from_port   = 9090
  to_port     = 9090
  protocol    = "tcp"
  cidr_blocks = ["199.204.135.66/32"] # Replace <your_ip> with your IP address
}

# Grafana
```

```
  ingress {
    from_port   = 3000
    to_port     = 3000
    protocol    = "tcp"
    cidr_blocks = ["199.204.135.66/32"] # Replace <your_ip> with your IP address
  }
  ingress {
    from_port   = 8080
    to_port     = 8080
    protocol    = "tcp"
    cidr_blocks = ["0.0.0.0/0"] # Adjust as necessary for security
  }
  egress {
    from_port   = 0
    to_port     = 0
    protocol    = "-1"
    cidr_blocks = ["0.0.0.0/0"]
  }
}

resource "aws_security_group" "k8s_worker_sg" {
  name        = "k8s_worker_sg"
  description = "Security group for Kubernetes workers"
  vpc_id      = aws_vpc.main.id
  # Prometheus
  ingress {
```

```
  from_port   = 9090
  to_port     = 9090
  protocol    = "tcp"
  cidr_blocks = ["199.204.135.66/32"] # Replace <your_ip> with your IP address
}

# Grafana
ingress {
  from_port   = 3000
  to_port     = 3000
  protocol    = "tcp"
  cidr_blocks = ["199.204.135.66/32"] # Replace <your_ip> with your IP address
}
# Allow all internal traffic for Kubernetes communication
ingress {
  from_port   = 0
  to_port     = 0
  protocol    = "-1"
  cidr_blocks = [aws_vpc.main.cidr_block]
}

# Allow external SSH and Kubernetes API access
ingress {
  from_port   = 22
  to_port     = 22
  protocol    = "tcp"
```

```
    cidr_blocks = ["0.0.0.0/0"]
  }

  # Allow external SSH and Kubernetes API access
  ingress {
    from_port   = 8000
    to_port     = 8000
    protocol    = "tcp"
    cidr_blocks = ["0.0.0.0/0"]
  }
  ingress {
    from_port   = 30000
    to_port     = 32767
    protocol    = "tcp"
    cidr_blocks = ["199.204.135.66/32"]
  }

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