

Egress IPs für Projekte definieren

Auf OpenShift ist es möglich eine IP zu hinterlegen, welche für den kompletten Outgoing Traffic eines Projektes genutzt wird. Hierzu wurde ein Range definiert, aus dem bei Bedarf eine IP einem Projekt zugewiesen werden kann. (**Achtung: Diese Lösung ist nicht HA und sollte nicht für produktiven Workload genutzt werden**)

Es gibt grundsätzlich zwei Möglichkeiten, den Outgoing Traffic auf OpenShift zu managen

Egress Router

Damit ein Egress Router deployed werden kann, müssen die `securitycontextconstraints.security.openshift.io` angepasst werden. Dadurch wird ermöglicht, dass der Pod `ipfailover` machen kann und die IP auf dem entsprechenden Pod/Node anhängt wird. Das bedeutet aber auch, dass dieser Pod als Root Container läuft und direkt von den Projekt Admins gemanaged werden muss. Dies ist gemäss unserer Richtlinien (Keine Container unter Root für nicht Infrastruktur Komponenten) untersagt.

Static IPs for External Project Traffic (Erst ab OSE 3.10 HA möglich)

Schritt 1 - Ist Stand anschauen und sichern

```
# oc get netnamespace > egress_ips_namespace.txt
# oc get hostsubnet > egress_ips_hosts.txt
```

Reservierter Range:

172.18.184.129-172.18.184.247 (IP_AUS_EH_RANGE)

172.28.184.129-172.28.184.247 (IP_AUS_ZF_RANGE)

Schritt 2 - Nächste freie IP auswählen.

```
# oc get hostsubnet
```

NAME	HOST	HOST IP	SUBNET	EGRESS
IPS				
vosie1.pnet.ch	vosie1.pnet.ch	172.18.184.15	10.127.68.0/25	
[172.18.184.129]				
vosie2.pnet.ch	vosie2.pnet.ch	172.18.184.17	10.127.69.0/25	[]
vosiz1.pnet.ch	vosiz1.pnet.ch	172.28.184.17	10.127.70.0/25	
[172.28.184.129]				
vosiz2.pnet.ch	vosiz2.pnet.ch	172.28.184.11	10.127.71.0/25	[]
vosme1.pnet.ch	vosme1.pnet.ch	172.27.148.13	10.127.66.0/25	[]

vosme2.pnet.ch	vosme2.pnet.ch	172.27.148.12	10.127.65.0/25	[]
vosmz1.pnet.ch	vosmz1.pnet.ch	172.31.148.12	10.127.64.0/25	[]
vosne1.pnet.ch	vosne1.pnet.ch	172.18.184.14	10.127.67.0/25	[]
vosne2.pnet.ch	vosne2.pnet.ch	172.18.184.13	10.127.73.0/25	[]
vosne3.pnet.ch	vosne3.pnet.ch	172.18.184.11	10.127.74.0/25	[]
vosne4.pnet.ch	vosne4.pnet.ch	172.18.184.12	10.127.78.0/25	[]
vosnz1.pnet.ch	vosnz1.pnet.ch	172.28.184.12	10.127.76.0/25	[]
vosnz2.pnet.ch	vosnz2.pnet.ch	172.28.184.15	10.127.72.0/25	[]
vosnz3.pnet.ch	vosnz3.pnet.ch	172.28.184.16	10.127.75.0/25	[]
vosnz4.pnet.ch	vosnz4.pnet.ch	172.28.184.14	10.127.77.0/25	[]

Schritt 3 - Egress IP einem Node hinzufügen. (Bestehende IPs nicht löschen!)

- Für IP von Engehalde

```
# oc patch hostsubnet vosiel.pnet.ch -p '{"egressIPs": ["ALLE BISHER DEFINIERTEN IPs!!!!", "IP_AUS_EH_RANGE"]}'
```

- Für IP von Zofingen

```
# oc patch hostsubnet vosiz1.pnet.ch -p '{"egressIPs": ["ALLE BISHER DEFINIERTEN IPs!!!!", "IP_AUS_ZF_RANGE"]}'
```

Schritt 4 - IP an Namespace anhängen

```
# oc patch netnamespace egress-test -p '{"egressIPs": ["RESERVIERTE_IP_EH", "RESERVIERTE_IP_ZF"]}'
```

Beispiel

```
oc patch hostsubnet vosiel.pnet.ch -p '{"egressIPs": ["172.18.184.129", "172.18.184.130", "172.18.184.131", "172.18.184.132"]}'
oc patch hostsubnet vosiz1.pnet.ch -p '{"egressIPs": ["172.28.184.129", "172.28.184.130", "172.28.184.131", "172.28.184.132"]}'
oc patch netnamespace abegglenma-test-egress -p '{"egressIPs": ["172.18.184.129", "172.28.184.129"]}'
```

Last update: **2019/02/21 13:37**