

Micro segmentation en ACI

Esta guía describe el funcionamiento y configuración de micro segmentación (useg) en ACI.

Descripción

Micro segmentation es una funcionalidad que permite asignar a uno o más *endpoints* dentro de una zona lógica de seguridad basado en distintos atributos, permitiendo aplicar permisos específicos a los *endpoints* que correspondan a los atributos definidos.

Para información a detalle acerca de los escenarios soportados y restricciones, podemos consultar el siguiente documento:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/virtualization/b_ACI_Virtualization_Guide_2_1_1/b_ACI_Virtualization_Guide_2_1_1_capter_0100.html#concept_9800A6F28C8C4DBF883C0D0C3F016C2B

Casos de Uso

Por defecto el EPG (Endpoint Group) es usado como unidad de aplicación de políticas de control en la Fábrica de ACI, permitiendo la comunicación libre entre los miembros del mismo. uSeg permite crear un nuevo subgrupo dentro del EPG (llamado Base EPG) para proveer políticas específicas a los *endpoints* que cumplan con los atributos que definan al uSeg EPG. Por ejemplo, dentro el EPG Web, se podría definir un uSeg EPG para separar a los endpoints dependiendo de la nomenclatura de la Virtual Machine (Vm), teniendo así un Useg para las Vms cuyo nombre comience con “Prod-” y otro para las Vms que empiecen con “Dev-”, a los cuáles podremos asignar políticas específicas. Otro caso de uso es cuando se tienen EPGs para los Servidores Web y de Base de Datos, cada uno con servidores Linux y Windows; En caso de ser afectado por un virus, la micro segmentación nos permitirá separar los EPGs de acuerdo al Sistema operativo de la Vm, al cual podríamos aislar o proveer más restricciones para comunicarse con los demás EPGs.

Funcionamiento de *Micro segmentation* en ACI

- 1 El usuario configura un dominio de VMM usando DVS, AVS o Microsoft vSwitch en el APIC.
- 2 El APIC se conecta a VCenter o SCVMM y realiza lo siguiente:
 - a Crea una instancia de AVS, VMWare DVS o Microsoft VSwitch
 - b Obtiene el inventario de Hypervisors y VMs desde VCenter o SCVMM
- 3 El usuario crea el EPG base y lo asocia al Dominio de VMM, esto genera una nueva encapsulación, este EPG base no contiene atributos de ninguna clase.

4 El usuario crea un uSeg EPG y lo asocia al Dominio VMM. El uSeg EPG no aparece en vCenter o SCVMM como un port group. El uSeg EPG contiene uno o varios atributos que son utilizados para comparar el inventario que se tiene. Si una VM coincide con los atributos, el APIC la asigna dinámicamente al uSeg EPG. Los endpoints son transferidos desde el EPG Base al uSeg, si éste último es eliminado, los endpoints regresan al EPG Base.

Atributos para Micro segmentación en ACI

Existen dos tipos de atributos, los basados en Red y los basados en Virtual Machine (VM)

Atributos de Red

Los atributos de Red pueden ser direcciones MAC o direcciones IP. Podemos definir más de una dirección MAC o IP dentro del uSeg EPG. Para la dirección IP, se puede definir una subred o una dirección específica.

Atributos de VM

Estos atributos se refieren a la información que el Vcenter o SCVMM tiene sobre las máquinas virtuales mediante el inventario que es compartido con el APIC. Los atributos de VM incluyen:

- Dominio VMM
- Sistema Operativo
- Identificador de Hypervisor
- Datacenter en Vcenter, Cloud en SCVMM
- Identificador de VM
- Nombre de VM
- Dn de vNIC (Domain name)

En adición a nombrar el atributo de VM, debemos definir las siguientes características al momento de crearlo:

1. Tipo de Atributo, ya sea VM o Hypervisor
2. Especificar un operador, ya sea **Equals** (Igual a) o **Starts with** (Empieza con)
3. Especificar el valor del atributo, ya sea el id de un vNic o el nombre del Sistema operativo

Atributos personalizados

Al usar AVS o DVS, Vcenter permite definir un "Custom Attribute" a una o varias VMs, lo cual permite que el uSeg EPG sea definido por estos atributos definidos desde Vcenter.

Precedencia de Atributos

La siguiente tabla ilustra el orden que es tomado en cuenta para aplicar los atributos definidos para clasificar un uSeg EPG

| Attribute | Type | Precedence Order | Example |
|---|---------|---|------------------------------|
| MAC Address Filter | Network | 1- Cisco AVS/Microsoft vSwitch 2- VMware VDS | 5c:01:23:ab:cd:ef |
| IP Address Filter | Network | 1- VMware VDS 2- Cisco AVS/Microsoft vSwitch | 192.168.33.77 10.1.0.0/16 |
| VNic Dn (vNIC domain name) | VM | 3 | a1:23:45:67:89:0b |
| VM Identifier | VM | 4 | VM-598 |
| VM Name | VM | 5 | HR_VDI_VM1 |
| Hypervisor Identifier | VM | 6 | host-25 |
| VMM Domain | VM | 7 | AVS-SJC-DC1 |
| Datacenter | VM | 8 | SJC-DC1 |
| Custom Attribute (Cisco AVS and VMware VDS only) | VM | 9 | SG_DMZ |
| Operating System | VM | 10 | Windows 2008 |

De igual forma, los operadores también tienen un orden definido para ser aplicados, la siguiente tabla describe el orden:

| Operator Type | Precedence Order |
|---------------|------------------|
| Equals | 1 |
| Contains | 2 |
| Starts With | 3 |
| Ends With | 4 |

Configurando Micro segmentación en ACI

Equipos y versiones utilizadas

Versión Apic 3.1(1i)

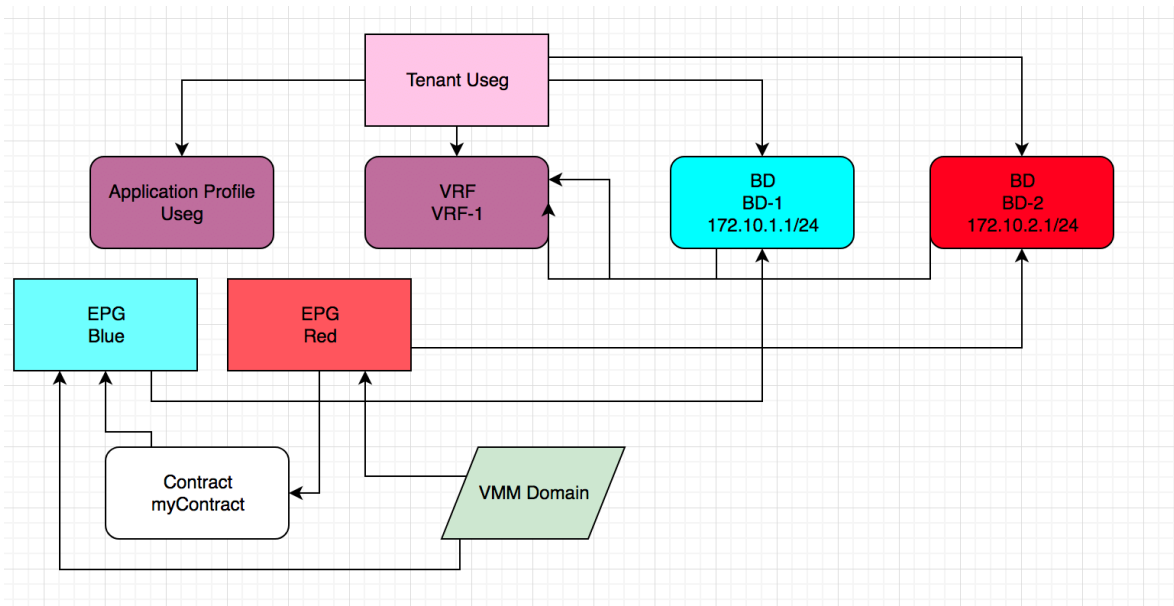
Versión Switches 13.1(1i)

Modelo Switch N9K-C93180YC-EX

Versión Vcenter 6.0

Descripción

Para este ejemplo utilizaremos una integración de VMM ya existente, utilizando un par de EPGs bajo un mismo tenant para revisar como configurar micro segmentación desde un EPG base funcional. De manera inicial contamos con el siguiente esquema lógico:



La configuración del Tenant se encuentra definida en el siguiente xml:

```
<imdata totalCount="1">
```

```

    <fvTenant descr="" dn="uni/tn-uSeg" name="uSeg" nameAlias=""
ownerKey="" ownerTag="">
    <fvAp descr="" name="Useg" nameAlias="" ownerKey="" ownerTag=""
prio="unspecified">
    <fvAEPg descr="" floodOnEncap="disabled" fwdCtrl=""
isAttrBasedEPg="no" matchT="AtleastOne" name="Red" nameAlias=""
pcEnfPref="unenforced" prefGrMemb="exclude" prio="unspecified">
    <fvRsBd tnFvBDName="BD-2"/>
    <fvRsCustQosPol tnQosCustomPolName=""/>
    <fvRsDomAtt classPref="encap" delimiter="" encap="unknown"
encapMode="auto" epgCos="Cos0" epgCosPref="disabled" instrImedcy="lazy"
netflowDir="both" netflowPref="disabled" primaryEncap="unknown"
primaryEncapInner="unknown" resImedcy="lazy"
secondaryEncapInner="unknown" switchingMode="native" tDn="uni/vmmp-
VMware/dom-VcenterVsw"/>
    </fvAEPg>
    <fvAEPg descr="" floodOnEncap="disabled" fwdCtrl=""
isAttrBasedEPg="no" matchT="AtleastOne" name="Blue" nameAlias=""
pcEnfPref="unenforced" prefGrMemb="exclude" prio="unspecified">
    <fvRsBd tnFvBDName="BD-1"/>
    <fvRsCustQosPol tnQosCustomPolName=""/>
    <fvRsDomAtt classPref="useg" delimiter="" encap="unknown"
encapMode="auto" epgCos="Cos0" epgCosPref="disabled"
instrImedcy="immediate" netflowDir="both" netflowPref="disabled"
primaryEncap="unknown" primaryEncapInner="unknown" resImedcy="immediate"
secondaryEncapInner="unknown" switchingMode="native" tDn="uni/vmmp-
VMware/dom-VcenterVsw"/>
    </fvAEPg>
    </fvAp>
    <fvRsTenantMonPol tnMonEPGPolName=""/>
    <fvBD OptimizeWanBandwidth="no" arpFlood="no" descr="" epClear="no"
epMoveDetectMode="" intersiteBumTrafficAllow="no" intersiteL2Stretch="no"
ipLearning="yes" limitIpLearnToSubnets="yes" llAddr="::"
mac="00:22:BD:F8:19:FF" mcastAllow="no" multiDstPktAct="bd-flood"
name="BD-1" nameAlias="" ownerKey="" ownerTag="" type="regular"
unicastRoute="yes" unkMacUcastAct="proxy" unkMcastAct="flood" vmac="not-
applicable">
    <fvRsBDToNdP tnNdIfPolName=""/>
    <fvRsBdToEpRet resolveAct="resolve" tnFvEpRetPolName=""/>
    <fvRsCtx tnFvCtxName="VRF-1"/>
    <fvRsIgmprsn tnIgmprsnPolName=""/>
    <fvSubnet ctrl="" descr="" ip="172.16.1.1/24" name="" nameAlias=""
preferred="no" scope="private" virtual="no"/>
    </fvBD>
    <fvBD OptimizeWanBandwidth="no" arpFlood="no" descr="" epClear="no"
epMoveDetectMode="" intersiteBumTrafficAllow="no" intersiteL2Stretch="no"
ipLearning="yes" limitIpLearnToSubnets="yes" llAddr="::"
mac="00:22:BD:F8:19:FF" mcastAllow="no" multiDstPktAct="bd-flood"
name="BD-2" nameAlias="" ownerKey="" ownerTag="" type="regular"
unicastRoute="yes" unkMacUcastAct="proxy" unkMcastAct="flood" vmac="not-
applicable">
    <fvRsBDToNdP tnNdIfPolName=""/>
    <fvRsBdToEpRet resolveAct="resolve" tnFvEpRetPolName=""/>
    <fvRsCtx tnFvCtxName="VRF-1"/>
    <fvRsIgmprsn tnIgmprsnPolName=""/>
    <fvSubnet ctrl="" descr="" ip="172.16.2.1/24" name="" nameAlias=""
preferred="no" scope="private" virtual="no"/>

```

```

</fvBD>
<fvCtx bdEnforcedEnable="no" descr="" knwMcastAct="permit" name="VRF-
1" nameAlias="" ownerKey="" ownerTag="" pcEnfDir="ingress"
pcEnfPref="enforced">
  <fvRsBgpCtxPol tnBgpCtxPolName=""/>
  <fvRsCtxToExtRouteTagPol tnL3extRouteTagPolName=""/>
  <fvRsCtxToEpRet tnFvEpRetPolName=""/>
  <fvRsOspfCtxPol tnOspfCtxPolName=""/>
  <vzAny descr="" matchT="AtleastOne" name="" nameAlias=""
prefGrMemb="disabled"/>
  <fvRsVrfValidationPol tnL3extVrfValidationPolName=""/>
</fvCtx>
<vnsSvcCont/>
<vzBrCP descr="" name="myContract" nameAlias="" ownerKey=""
ownerTag="" prio="unspecified" scope="global" targetDscp="unspecified">
  <vzSubj consMatchT="AtleastOne" descr="" name="permitAll"
nameAlias="" prio="unspecified" provMatchT="AtleastOne" revFltPorts="yes"
targetDscp="unspecified">
    <vzRsSubjFiltAtt directives="" tnVzFilterName="default"/>
  </vzSubj>
</vzBrCP>
</fvTenant>
</imdata>

```

La configuración del Tenant integra el DVS de VMWare en Dos EPGs, Red y Blue. Cada EPG está asociado a diferentes Bridge Domains, con una Interface Vlan en cada uno actuando como el Default Gateway para cada EPG. Los Bridge Domains están asociados a las misma VRF. Los EPGs podrán comunicarse entre ellos a través de un contrato que los vincula. El comportamiento de la red antes de la configuración de Micro segmentación se puede verificar de la siguiente manera:

EPG Blue

| End Point | MAC | IP | Learning Source | Hosting Server | Reporting Controller Name | Interface | Multicast Address | Encap |
|-----------|-------------------|-------------|-----------------|----------------|---------------------------|---|-------------------|-----------|
| CentOs-2 | 00:50:56:88:5C:FD | 172.16.1.23 | learned vmm | 10.88.247.33 | vcenter | Pod-1/Node-104/VcenterPO (learned,vmm) | --- | vlan-1660 |
| CentOs-1 | 00:50:56:88:80:F8 | 172.16.1.29 | learned vmm | 10.88.247.34 | vcenter | Pod-1/Node-101-102/VcenterVPC (learned,vmm) | --- | vlan-1660 |
| RedHat-4 | 00:50:56:9A:9A:ED | 172.16.1.77 | learned vmm | 10.88.247.33 | vcenter | Pod-1/Node-104/VcenterPO (learned,vmm) | --- | vlan-1660 |

Tenemos 3 Máquinas virtuales , el atributo “Learning source” marca que los endpoints están activos en la Fábrica (learned).

EPG Red

| End Point | MAC | IP | Learning Source | Hosting Server | Reporting Controller Name | Interface | Multicast Address | Encap |
|-----------|-------------------|-------------|-----------------|----------------|---------------------------|---|-------------------|-----------|
| RedHat-6 | 00:50:56:88:4D:37 | 172.16.2.70 | learned vmm | 10.88.247.34 | vcenter | Pod-1/Node-101-102/VcenterVPC (learned... | --- | vlan-1572 |
| RedHat-5 | 00:50:56:9A:D2:27 | 172.16.2.20 | learned vmm | 10.88.247.34 | vcenter | Pod-1/Node-101-102/VcenterVPC (learned... | --- | vlan-1572 |

En este EPG también contamos con dos Endpoints activos, los cuales se pueden comunicar entre sí mediante el contrato configurado.

Desde la consola de la Máquina virtual CentOS-2 podemos alcanzar a los Endpoints del EPG Red:

```
root@centos:~# ifconfig eth3
eth3: flags=4096<UP,BROADCAST,RUNNING,MULTICAST> mtu=1500
    inet addr:172.16.1.23 Bcast:172.16.1.255 Mask:255.255.0
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:117 errors:0 dropped:0 overruns:0 frame:0
    TX packets:109 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:14474 (14.1 KiB) TX bytes:13322 (13.0 KiB)

root@centos ~# ping 172.16.2.20
PING 172.16.2.20 (172.16.2.20) bytes of data:
54 bytes from 172.16.2.20: icmp_seq=1 ttl=62 time=0.516 ms
54 bytes from 172.16.2.20: icmp_seq=2 ttl=62 time=0.487 ms
--- 172.16.2.20 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1543ms
rtt min/avg/max/mdev = 0.487/0.501/0.516/0.026 ms

root@centos ~# ping 172.16.2.70
PING 172.16.2.70 (172.16.2.70) bytes of data:
54 bytes from 172.16.2.70: icmp_seq=1 ttl=62 time=0.509 ms
54 bytes from 172.16.2.70: icmp_seq=2 ttl=62 time=0.485 ms
54 bytes from 172.16.2.70: icmp_seq=3 ttl=62 time=0.500 ms
--- 172.16.2.70 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2195ms
rtt min/avg/max/mdev = 0.485/0.498/0.509/0.009 ms
```

La máquina virtual RedHat-6, del EPG Red también puede alcanzar los endpoints del EPG Blue.

```
root@localhost:~# ping 172.16.1.23
PING 172.16.1.23 (172.16.1.23) 56(84) bytes of data:
64 bytes from 172.16.1.23: icmp_seq=1 ttl=61 time=2.02 ms
64 bytes from 172.16.1.23: icmp_seq=2 ttl=61 time=0.351 ms
--- 172.16.1.23 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.351/1.188/2.025/0.837 ms

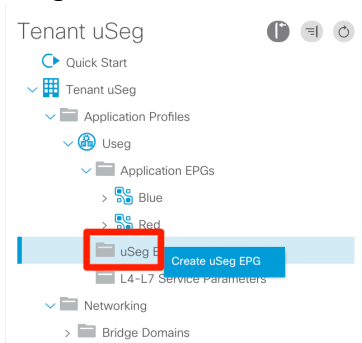
root@localhost ~# ping 172.16.1.29
PING 172.16.1.29 (172.16.1.29) 56(84) bytes of data:
64 bytes from 172.16.1.29: icmp_seq=1 ttl=62 time=2.39 ms
64 bytes from 172.16.1.29: icmp_seq=2 ttl=62 time=0.339 ms
--- 172.16.1.29 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.339/1.367/2.395/1.028 ms

root@localhost ~# ping 172.16.1.77
PING 172.16.1.77 (172.16.1.77) 56(84) bytes of data:
54 bytes from 172.16.1.77: icmp_seq=1 ttl=61 time=3.02 ms
54 bytes from 172.16.1.77: icmp_seq=2 ttl=61 time=0.436 ms
--- 172.16.1.77 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.436/1.730/3.025/1.295 ms
```

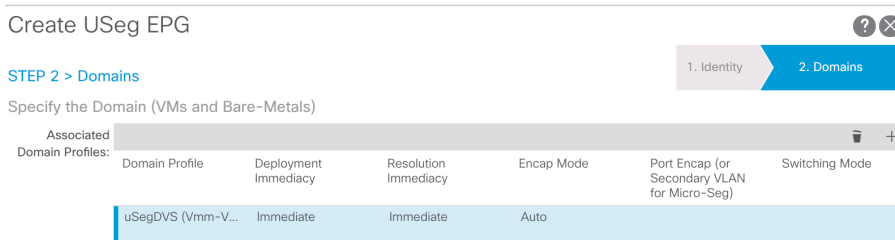
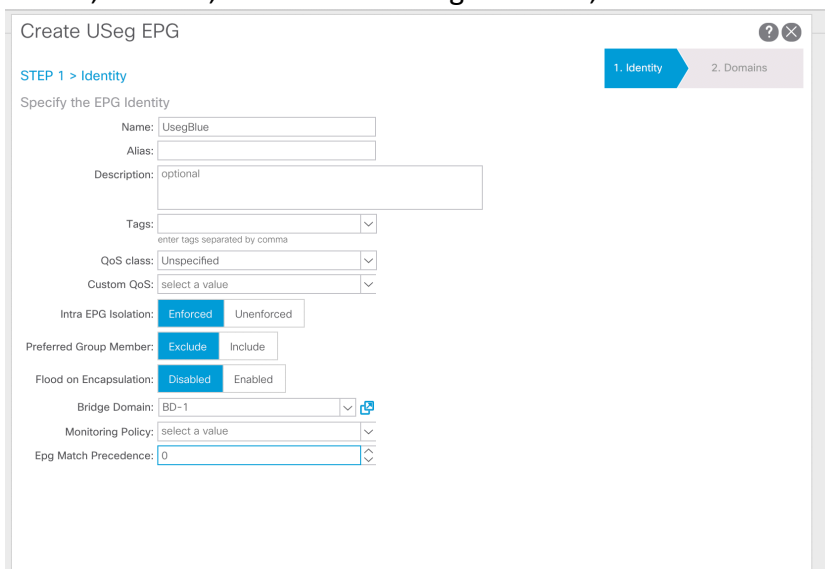
Habilitando Microsegmentación.

Como nota, las capturas de pantalla mostrarán diferente información IP para las Máquinas virtuales. La configuración actual es la misma: 2 EPGs base sin useg habilitado. Ambos EPGs, Red y Blue están asociados a un solo dominio de VMM. La comunicación entre ambos está habilitada mediante un contrato que permite todo el tráfico.

El primer paso será crear el Useg EPG. Esto se configura dentro del Application profile, Useg EPGs:



La información requerida es similar a la de un EPG normal, donde se definen el dominio a utilizar, nombre, asociación al Bridge Domain, etc.



| Domain Profile | Deployment Immediacy | Resolution Immediacy | Encap Mode | Port Encap (or Secondary VLAN for Micro-Seg) | Switching Mode |
|-------------------|----------------------|----------------------|------------|--|----------------|
| uSegDVS (Vmm-V... | Immediate | Immediate | Auto | | |

Name – Nombre del uSeg EPG

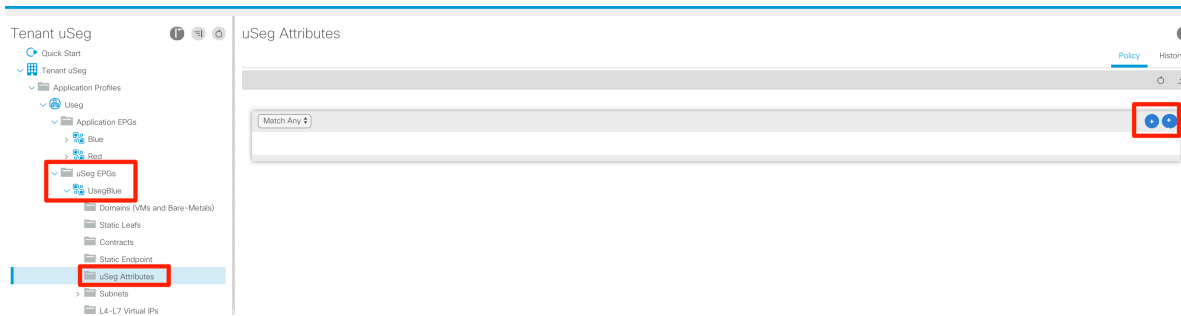
Intra EPG isolation – Habilita el aislamiento entre los endpoints del EPG.

Bridge domain – Nombre del Bridge domain, debe ser el mismo que el del EPG Base

EPG Match Precedence – Este atributo permite ordenar diferentes uSeg, aplicando la precedencia al valor más bajo (0, cero)

Domain profile – Dominio utilizado para el EPG.

Una vez que el uSeg EPG sea creado, podemos agregar las cláusulas de atributos para clasificar. Esto se hace al agregar los **uSeg Attributes**:



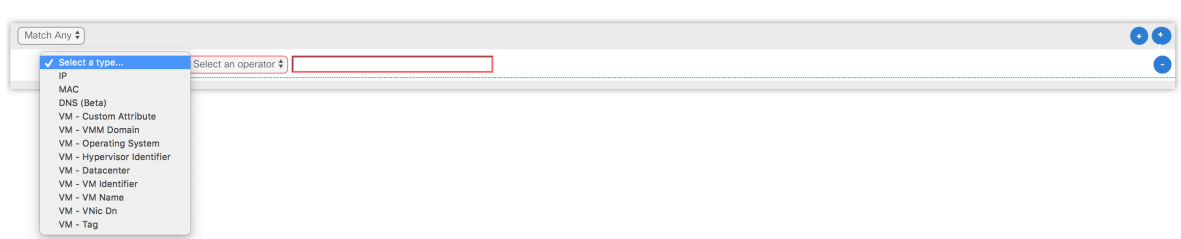
Para poder generar una regla de clasificación, debemos agregar por lo menos una regla de atributos.



Primero debemos definir el tipo de match:

Match any – Default, permite clasificar al endpoint dentro del uSeg si hace match con al menos una regla.

Match all – El endpoint debe coincidir en su valor de atributo con todas la reglas para ser clasificado dentro del uSeg.



La siguiente lista muestra los atributos de red(IP, MAC) y de Máquina Virtual (Prefijo VM-) disponibles para clasificar el endpoint.



Por último debemos configurar el operador para el atributo. Para los atributos de Red, sólo el operado *Equals* está disponible

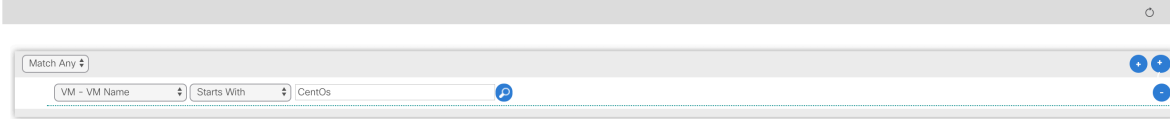
Equals – El valor asignado debe ser igual para la clasificación del endpoint

Contains – La VM contiene el valor dentro del atributo de VM

Ends with – La VM termina con el valor definido en el atributo de VM

Starts with – La VM comienza con el valor definido en el atributo de VM

En este ejemplo, se configurará un regla que clasifique dentro del uSeg EPG a cualquier Máquina virtual cuyo nombre comience con el Valor **CentOs**:

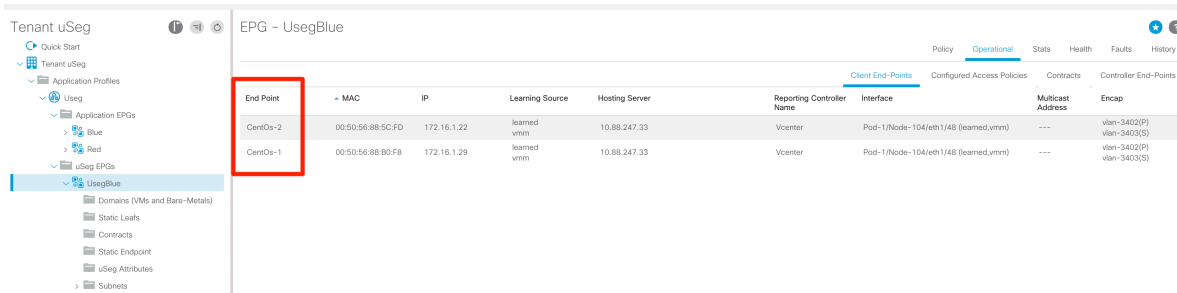


El objeto resultante es el siguiente:

```
<fvAEPg descr="" dn="uni/tn-uSeg/ap-Useg/epg-UsegBlue"
floodOnEncap="disabled" fwdCtrl="" isAttrBasedEPg="yes"
matchT="AtleastOne" name="UsegBlue" nameAlias="" pcEnfPref="enforced"
prefGrMemb="exclude" prio="unspecified">
  <fvCrtrn descr="" match="any" name="default" nameAlias="" ownerKey=""
ownerTag="" prec="0">
    <fvVmAttr category="" descr="" labelName="" name="0" nameAlias=""
operator="startsWith" ownerKey="" ownerTag="" type="vm-name"
value="CentOs"/>>
  </fvCrtrn>
  <fvRsBd tnFvBDName="BD-1"/>
  <fvRsCustQosPol tnQosCustomPolName=""/>
  <fvRsDomAtt classPref="encap" delimiter="" encap="unknown"
encapMode="auto" epgCos="Cos0" epgCosPref="disabled"
instrImedcy="immediate" netflowDir="both" netflowPref="disabled"
primaryEncap="unknown" primaryEncapInner="unknown" resImedcy="immediate"
secondaryEncapInner="unknown" switchingMode="native" tDn="uni/vmmp-
VMware/dom-uSegDVS"/>
</fvAEPg>
```

El objeto **fvCrtrn** define al tipo de Match, y dentro de éste se tiene al objeto **fvVmAttr** ya que el tipo de atributo es VM, el objeto sería **fvIpAttr** si éste fuera de tipo Red. El objeto de atributo(*vm-name*) contiene tanto al operador (*Starts with*) y el Valor (*CentOs*).

Después crear el objeto, la vista *operational* nos mostrará las Máquinas virtuales CentOs-1 y CentOs-2, ya que ambas coinciden con la regla creada:



| End Point | MAC | IP | Learning Source | Hosting Server | Reporting Controller | Interface | Multicast Address | Encap |
|-----------|-------------------|-------------|-----------------|----------------|----------------------|--------------------------------------|-------------------|------------------------------|
| CentOs-2 | 00:50:56:88:5C:FD | 172.16.1.22 | learned vmm | 10.88.247.33 | Vcenter | Pod-1/Node-104/eth1/48 (learned,vmm) | --- | vlan-3402(P) vlan-3403(S) |
| CentOs-1 | 00:50:56:88:80:F8 | 172.16.1.29 | learned vmm | 10.88.247.33 | Vcenter | Pod-1/Node-104/eth1/48 (learned,vmm) | --- | vlan-3402(P) vlan-3403(S) |

El EPG Blue muestra sólo un Endpoint:

| Endpoint | MAC | IP | Learning Source | Hosting Server | Reporting Controller Name | Interface | Multicast Address | Encap |
|----------|-------------------|-------------|-----------------|----------------|---------------------------|--------------------------------------|-------------------|------------------------------|
| RedHat-4 | 00:50:56:9A:9A:ED | 172.16.1.77 | learned vmm | 10.88.247.33 | Vcenter | Pod-1/Node-104/eth1/48 [learned.vmm] | --- | vlan-3402(P) vlan-3403(S) |

La comunicación vista entre la Máquinas virtuales cambió, ya que las 2 VMs de CentOS ahora forman parte del uSeg EPG (llamado UsegBlue) y no del EPG Base (Blue), ninguna de éstas puede comunicarse con los endpoints del EPG Red. Ya que éste uSeg EPG no tiene contrato alguno, sólo la Máquina virtual residual del Base EPG puede comunicarse con el EPG Red:

RedHat-4:

```
root@localhost:~# ping 172.16.1.22
64 bytes from 172.16.1.22: icmp_seq=2893 ttl=63 time=0.317 ms
64 bytes from 172.16.1.22: icmp_seq=2894 ttl=63 time=0.374 ms
64 bytes from 172.16.1.22: icmp_seq=2895 ttl=63 time=0.279 ms
64 bytes from 172.16.1.22: icmp_seq=2896 ttl=63 time=0.315 ms
64 bytes from 172.16.1.22: icmp_seq=2897 ttl=63 time=0.284 ms
64 bytes from 172.16.1.22: icmp_seq=2898 ttl=63 time=0.245 ms
64 bytes from 172.16.1.22: icmp_seq=2899 ttl=63 time=0.282 ms
64 bytes from 172.16.1.22: icmp_seq=2900 ttl=63 time=0.246 ms
64 bytes from 172.16.1.22: icmp_seq=2901 ttl=63 time=0.300 ms
64 bytes from 172.16.1.22: icmp_seq=2902 ttl=63 time=0.290 ms
64 bytes from 172.16.1.22: icmp_seq=2903 ttl=63 time=0.301 ms
64 bytes from 172.16.1.22: icmp_seq=2904 ttl=63 time=0.258 ms
64 bytes from 172.16.1.22: icmp_seq=2905 ttl=63 time=0.255 ms
--- 172.16.1.22 ping statistics ---
3850 packets transmitted, 2844 received, 26% packet loss, time 3850250ms
rtt min/avg/max/mdev = 0.154/0.345/7.113/0.194 ms
root@localhost ~# ping 172.16.1.22
PING 172.16.1.22 (172.16.1.22) 56(84) bytes of data:
--- 172.16.1.22 ping statistics ---
314 packets transmitted, 0 received, 100% packet loss, time 313050ms

root@localhost ~# ping 172.16.2.67
64 bytes from 172.16.2.67: icmp_seq=14 ttl=63 time=0.247 ms
64 bytes from 172.16.2.67: icmp_seq=15 ttl=63 time=0.361 ms
64 bytes from 172.16.2.67: icmp_seq=16 ttl=63 time=0.229 ms
64 bytes from 172.16.2.67: icmp_seq=17 ttl=63 time=0.243 ms
64 bytes from 172.16.2.67: icmp_seq=18 ttl=63 time=0.327 ms
64 bytes from 172.16.2.67: icmp_seq=19 ttl=63 time=0.290 ms
64 bytes from 172.16.2.67: icmp_seq=20 ttl=63 time=0.331 ms
64 bytes from 172.16.2.67: icmp_seq=21 ttl=63 time=0.292 ms
64 bytes from 172.16.2.67: icmp_seq=22 ttl=63 time=0.316 ms
64 bytes from 172.16.2.67: icmp_seq=23 ttl=63 time=0.271 ms
64 bytes from 172.16.2.67: icmp_seq=24 ttl=63 time=0.263 ms
64 bytes from 172.16.2.67: icmp_seq=25 ttl=63 time=0.353 ms
64 bytes from 172.16.2.67: icmp_seq=26 ttl=63 time=0.273 ms
64 bytes from 172.16.2.67: icmp_seq=27 ttl=63 time=0.324 ms
```

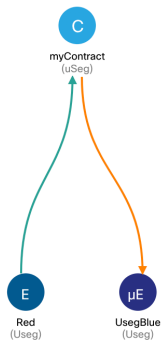
La VM puede comunicarse con la subred 172.16.20/24 (EPG red), pero con el Host 172.16.1.22(CentOs-2), ya que no hay contrato entre el Base y el uSeg EPG.

CentOs-1:

```
pod2@centos:~  
File Edit View Search Terminal Help  
64 bytes from 172.16.2.25: icmp_seq=5109 ttl=64 time=0.355 ms  
64 bytes from 172.16.2.25: icmp_seq=5110 ttl=64 time=0.349 ms  
64 bytes from 172.16.2.25: icmp_seq=5111 ttl=64 time=0.326 ms  
64 bytes from 172.16.2.25: icmp_seq=5112 ttl=64 time=0.325 ms  
64 bytes from 172.16.2.25: icmp_seq=5113 ttl=64 time=0.308 ms  
64 bytes from 172.16.2.25: icmp_seq=5114 ttl=64 time=0.308 ms  
64 bytes from 172.16.2.25: icmp_seq=5115 ttl=64 time=0.357 ms  
64 bytes from 172.16.2.25: icmp_seq=5116 ttl=64 time=0.332 ms  
64 bytes from 172.16.2.25: icmp_seq=5117 ttl=64 time=0.351 ms  
64 bytes from 172.16.2.25: icmp_seq=5118 ttl=64 time=0.354 ms  
64 bytes from 172.16.2.25: icmp_seq=5119 ttl=64 time=0.343 ms  
64 bytes from 172.16.2.25: icmp_seq=5120 ttl=64 time=0.366 ms  
64 bytes from 172.16.2.25: icmp_seq=5121 ttl=64 time=0.346 ms  
64 bytes from 172.16.2.25: icmp_seq=5122 ttl=64 time=0.335 ms  
64 bytes from 172.16.2.25: icmp_seq=5123 ttl=64 time=0.335 ms  
64 bytes from 172.16.2.25: icmp_seq=5124 ttl=64 time=0.265 ms  
64 bytes from 172.16.2.25: icmp_seq=5125 ttl=64 time=0.350 ms  
^C  
--- 172.16.2.25 ping statistics ---  
6017 packets transmitted, 4563 received, 24% packet loss, time 385ms  
rtt min/avg/max/mdev = 0.179/0.294/2.372/0.385ms  
pod2@centos ~]$ ping 172.16.2.25  
PING 172.16.2.25 (172.16.2.25) 56(84) bytes of data:  
^C  
--- 172.16.1.77 ping statistics ---  
6014 packets transmitted, 3239 received, +225 errors, 46% packet loss, time 6013ms  
rtt min/avg/max/mdev = 0.054/1.247/2001.301/39.303 ms, pipe 3  
pod2@centos ~]$ ping 172.16.1.77  
PING 172.16.1.77 (172.16.1.77) 56(84) bytes of data:  
^C  
pod2@centos:~  
File Edit View Search Terminal Help  
[pod2@centos ~]$ ping 172.16.1.22  
PING 172.16.1.22 (172.16.1.22) 56(84) bytes of data:  
^C
```

Aún cuando la VM se encuentra activa en la Fábrica, no puede comunicarse. Esto se explica ya que el uSeg EPG (**UsegBlue**) no tiene contratos hacia su EPG base (**Blue**, 172.16.1.77), ni hacia el EPG **Red** (172.16.2.0/24). Ya que la configuración del uSeg EPG habilitó el “*Intra-EPG isolation*” tampoco se puede comunicar con otro endpoint dentro del uSeg EPG(172.16.1.22).

Probando la comunicación usando uSeg EPGs
Ahora procederemos a eliminar el contrato entre el EPG **Blue** (*Consumer*) y el EPG **Red** (*Provider*), moviendo la asociación entre el EPG **UsegBlue** (*Consumer*) y el EPG **Red** (*Provider*). En teoría los endpoints del EPG **UsegBlue** podrán comunicarse con **Red**, pero no entre el EPG **Blue** y el **Red**.



RedHat-4:

```
root@localhost:~  
64 bytes from 172.16.1.22: icmp_seq=2899 ttl=63 time=0.282 ms  
64 bytes from 172.16.1.22: icmp_seq=2900 ttl=63 time=0.246 ms  
64 bytes from 172.16.1.22: icmp_seq=2901 ttl=63 time=0.300 ms  
64 bytes from 172.16.1.22: icmp_seq=2902 ttl=63 time=0.290 ms  
64 bytes from 172.16.1.22: icmp_seq=2903 ttl=63 time=0.301 ms  
64 bytes from 172.16.1.22: icmp_seq=2904 ttl=63 time=0.258 ms  
64 bytes from 172.16.1.22: icmp_seq=2905 ttl=63 time=0.255 ms  
--- 172.16.1.22 ping statistics ---  
3850 packets transmitted, 2844 received, 26%  
rtt min/avg/max/mdev = 0.154/0.345/7.113/0.1  
[root@localhost ~]# ping 172.16.1.22  
PING 172.16.1.22 (172.16.1.22) 56(84) bytes  
--- 172.16.1.22 ping statistics ---  
314 packets transmitted, 0 received, 100% pa  
[root@localhost ~]#  
[root@localhost ~]#  
root@localhost ~]#  
root@localhost ~]# ping 172.16.1.22  
PING 172.16.1.22 (172.16.1.22) 56(84) bytes  
64 bytes from 172.16.2.25: icmp_seq=1054 ttl=63 time=0.342 ms  
64 bytes from 172.16.2.25: icmp_seq=1055 ttl=63 time=0.329 ms  
64 bytes from 172.16.2.25: icmp_seq=1056 ttl=63 time=0.372 ms  
64 bytes from 172.16.2.25: icmp_seq=1057 ttl=63 time=0.223 ms  
64 bytes from 172.16.2.25: icmp_seq=1058 ttl=63 time=0.402 ms  
64 bytes from 172.16.2.25: icmp_seq=1059 ttl=63 time=0.270 ms  
64 bytes from 172.16.2.25: icmp_seq=1060 ttl=63 time=0.408 ms  
64 bytes from 172.16.2.25: icmp_seq=1061 ttl=63 time=0.350 ms  
64 bytes from 172.16.2.25: icmp_seq=1062 ttl=63 time=0.372 ms  
64 bytes from 172.16.2.25: icmp_seq=1063 ttl=63 time=0.399 ms  
64 bytes from 172.16.2.25: icmp_seq=1064 ttl=63 time=0.299 ms  
64 bytes from 172.16.2.25: icmp_seq=1065 ttl=63 time=0.396 ms  
64 bytes from 172.16.2.25: icmp_seq=1066 ttl=63 time=0.296 ms  
64 bytes from 172.16.2.25: icmp_seq=1067 ttl=63 time=0.366 ms  
64 bytes from 172.16.2.25: icmp_seq=1068 ttl=63 time=0.355 ms  
64 bytes from 172.16.2.25: icmp_seq=1069 ttl=63 time=0.301 ms  
64 bytes from 172.16.2.25: icmp_seq=1070 ttl=63 time=0.400 ms  
--- 172.16.2.25 ping statistics ---  
226 packets transmitted, 1070 received, 12% packet loss, time 1225462ms  
rtt min/avg/max/mdev = 0.156/0.340/1.141/0.076 ms  
root@localhost ~]# ping 172.16.2.25  
PING 172.16.2.25 (172.16.2.25) 56(84) bytes of data.  
64 bytes from 172.16.2.67: icmp_seq=1071 ttl=63 time=0.355 ms  
64 bytes from 172.16.2.67: icmp_seq=1072 ttl=63 time=0.301 ms  
64 bytes from 172.16.2.67: icmp_seq=1073 ttl=63 time=0.355 ms  
64 bytes from 172.16.2.67: icmp_seq=1074 ttl=63 time=0.301 ms  
64 bytes from 172.16.2.67: icmp_seq=1075 ttl=63 time=0.355 ms  
64 bytes from 172.16.2.67: icmp_seq=1076 ttl=63 time=0.301 ms  
64 bytes from 172.16.2.67: icmp_seq=1077 ttl=63 time=0.355 ms  
64 bytes from 172.16.2.67: icmp_seq=1078 ttl=63 time=0.301 ms  
64 bytes from 172.16.2.67: icmp_seq=1079 ttl=63 time=0.355 ms  
64 bytes from 172.16.2.67: icmp_seq=1080 ttl=63 time=0.301 ms  
--- 172.16.2.67 ping statistics ---  
186 packets transmitted, 1038 received, 46% packet loss, time 1225462ms  
rtt min/avg/max/mdev = 0.152/0.282/0.470/0.043 ms  
root@localhost ~]# ping 172.16.2.67  
PING 172.16.2.67 (172.16.2.67) 56(84) bytes of data.  
64 bytes from 172.16.2.25: icmp_seq=1081 ttl=63 time=0.355 ms  
64 bytes from 172.16.2.25: icmp_seq=1082 ttl=63 time=0.301 ms  
64 bytes from 172.16.2.25: icmp_seq=1083 ttl=63 time=0.355 ms  
64 bytes from 172.16.2.25: icmp_seq=1084 ttl=63 time=0.301 ms  
64 bytes from 172.16.2.25: icmp_seq=1085 ttl=63 time=0.355 ms  
64 bytes from 172.16.2.25: icmp_seq=1086 ttl=63 time=0.301 ms  
64 bytes from 172.16.2.25: icmp_seq=1087 ttl=63 time=0.355 ms  
64 bytes from 172.16.2.25: icmp_seq=1088 ttl=63 time=0.301 ms  
64 bytes from 172.16.2.25: icmp_seq=1089 ttl=63 time=0.355 ms  
64 bytes from 172.16.2.25: icmp_seq=1090 ttl=63 time=0.301 ms  
--- 172.16.2.25 ping statistics ---  
226 packets transmitted, 1070 received, 12% packet loss, time 1225462ms  
rtt min/avg/max/mdev = 0.156/0.340/1.141/0.076 ms  
root@localhost ~]# ping 172.16.2.25  
PING 172.16.2.25 (172.16.2.25) 56(84) bytes of data.
```

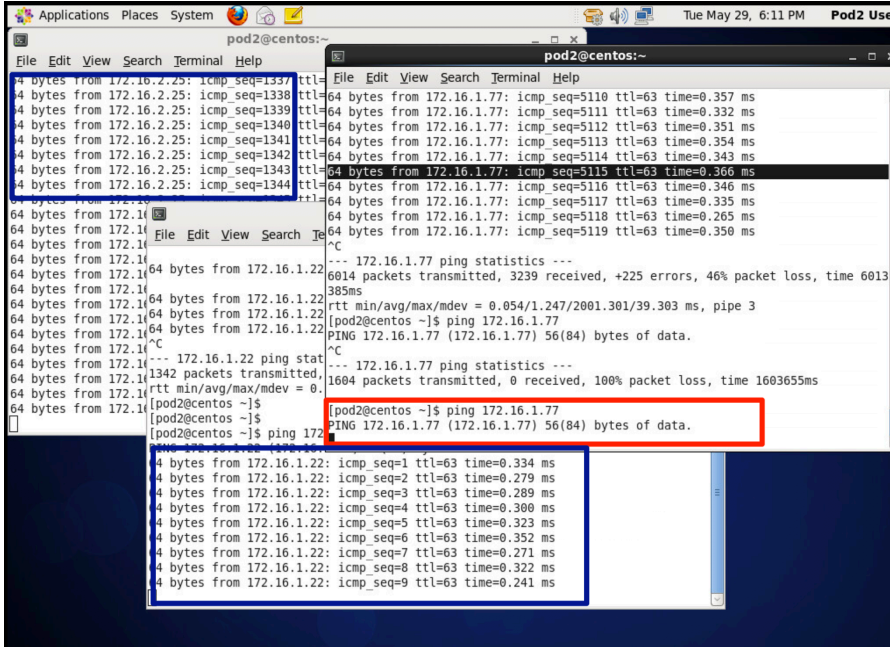
Ya que el EPG **Blue** no tiene contratos hacia Red (172.16.2.0/24) ni hacia UsegBlue (172.16.1.22), la máquina no puede comunicarse con ningún host.

CentOS-1:

```
pod2@centos:~  
64 bytes from 172.16.2.25: icmp_seq=1601 ttl=63 time=0.357 ms  
64 bytes from 172.16.2.25: icmp_seq=1602 ttl=63 time=0.332 ms  
64 bytes from 172.16.2.25: icmp_seq=1603 ttl=63 time=0.351 ms  
64 bytes from 172.16.2.25: icmp_seq=1604 ttl=63 time=0.354 ms  
--- 172.16.2.25 ping statistics ---  
604 packets transmitted, 195 received, 67% packet loss, time 6013 ms  
rtt min/avg/max/mdev = 0.179/0.307/0.434/0.046 ms  
pod2@centos ~]# ping 172.16.2.25  
PING 172.16.2.25 (172.16.2.25) 56(84) bytes of data.  
4 bytes from 172.16.2.25: icmp_seq=1 ttl=63 time=0.265 ms  
4 bytes from 172.16.2.25: icmp_seq=2 ttl=63 time=0.350 ms  
4 bytes from 172.16.2.25: icmp_seq=3 ttl=63 time=0.357 ms  
4 bytes from 172.16.2.25: icmp_seq=4 ttl=63 time=0.332 ms  
4 bytes from 172.16.2.25: icmp_seq=5 ttl=63 time=0.351 ms  
4 bytes from 172.16.2.25: icmp_seq=6 ttl=63 time=0.354 ms  
4 bytes from 172.16.2.25: icmp_seq=7 ttl=63 time=0.343 ms  
4 bytes from 172.16.2.25: icmp_seq=8 ttl=63 time=0.366 ms  
4 bytes from 172.16.2.25: icmp_seq=9 ttl=63 time=0.346 ms  
4 bytes from 172.16.2.25: icmp_seq=10 ttl=63 time=0.335 ms  
4 bytes from 172.16.2.25: icmp_seq=11 ttl=63 time=0.265 ms  
4 bytes from 172.16.2.25: icmp_seq=12 ttl=63 time=0.350 ms  
4 bytes from 172.16.2.25: icmp_seq=13 ttl=63 time=0.357 ms  
--- 172.16.1.77 ping statistics ---  
6014 packets transmitted, 3239 received, 46% packet loss, time 6013 ms  
rtt min/avg/max/mdev = 0.054/1.247/2001.301/39.303 ms, pipe 3  
[pod2@centos ~]# ping 172.16.1.77  
PING 172.16.1.77 (172.16.1.77) 56(84) bytes of data.  
--- 172.16.1.77 ping statistics ---  
1604 packets transmitted, 0 received, 100% packet loss, time 1603655ms  
pod2@centos ~]# ping 172.16.1.77  
PING 172.16.1.77 (172.16.1.77) 56(84) bytes of data.  
pod2@centos ~]# ping 172.16.1.22  
PING 172.16.1.22 (172.16.1.22) 56(84) bytes of data.  
--- 172.16.1.22 ping statistics ---  
1570 packets transmitted, 0 received, 100% packet loss, time 1569368ms  
pod2@centos ~]# ping 172.16.1.22  
PING 172.16.1.22 (172.16.1.22) 56(84) bytes of data.
```

El tráfico hacia **Red**(172.16.2.0/24) ahora está permitido. El tráfico hacia el EPG Base, **Blue** (172.16.1.77) sigue sin permitirse ya que no hay contratos. Tampoco hacia el **UsegBlue** (172.16.1.22), ya que el “**Intra-EPG isolation**” sigue activo.

Si deshabilitamos el “**Intra-EPG isolation**”, entonces la VM podrá comunicarse con la IP 172.16.1.22 del **UsegBlue**:

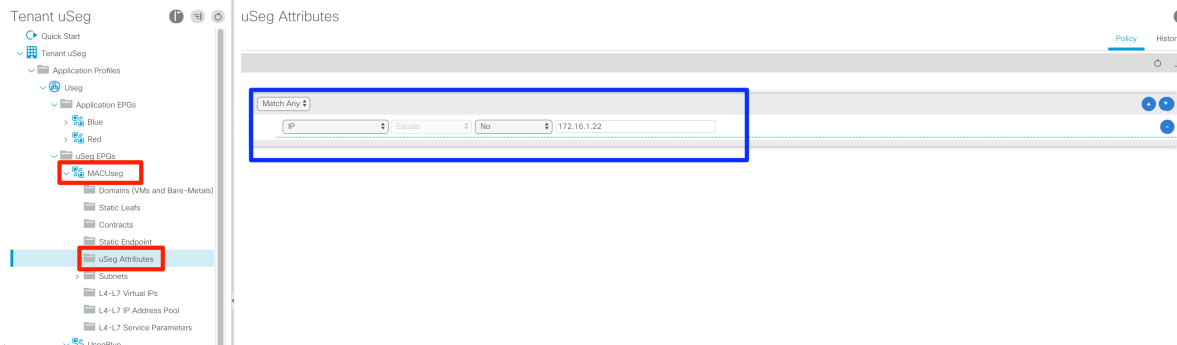


Creando diferentes uSeg EPGs con Atributos de Red y VM

Como último ejemplo, vamos a configurar un segundo uSeg EPG, llamado **MACUseg**, en el cual configuraremos un atributo del tipo Red, haciendo un match con la dirección MAC de una de las Máquinas virtuales del EPG **Blue**. Recordando las reglas de Microsegmentación:

| Attribute | Type | Precedence Order | Example |
|----------------------------|---------|---|------------------------------|
| MAC Address Filter | Network | 1- Cisco AVS/Microsoft vSwitch 2- VMware VDS | 5c:01:23:ab:cd:ef |
| IP Address Filter | Network | 1- VMware VDS 2- Cisco AVS/Microsoft vSwitch | 192.168.33.77 10.1.0.0/16 |
| VNic Dn (vNIC domain name) | VM | 3 | a1:23:45:67:89:0b |
| VM Identifier | VM | 4 | VM-598 |
| VM Name | VM | 5 | HR_VDI_VM1 |

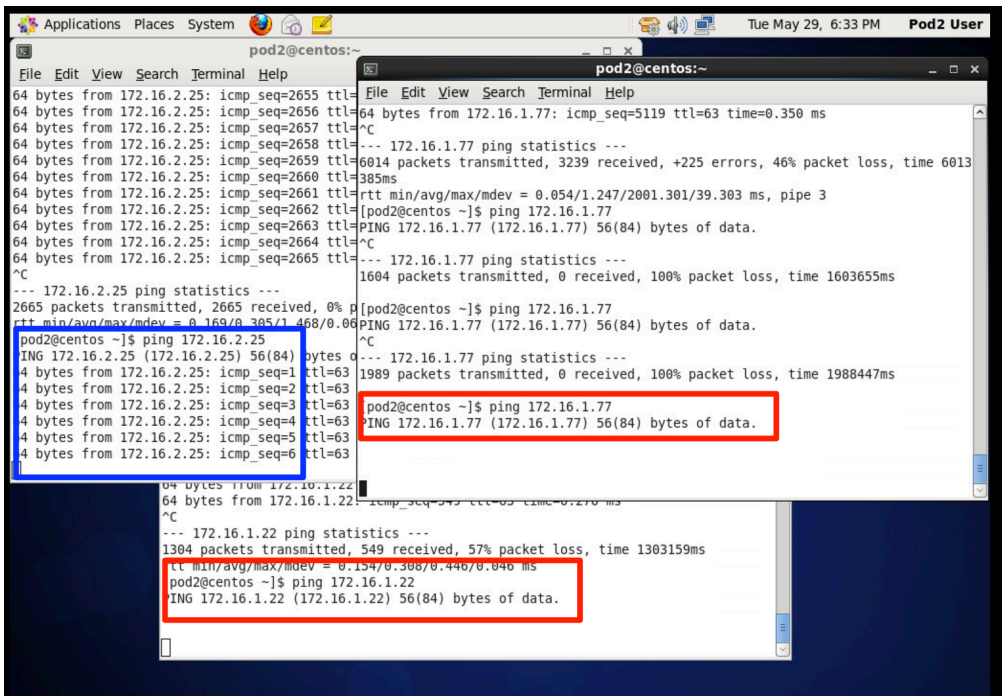
El atributo IP(tipo *Red*) tiene precedencia sobre el nombre de la Máquina Virtual (tipo *VM*)
 Al crear un segundo uSeg EPG, clasificando respecto a la dirección IP, cualquier endpoint que coincida con la regla dejará de ser parte del primer uSeg creado y formará parte del nuevo. En este caso, generamos la siguiente regla de clasificación:



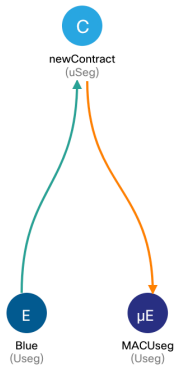
En seguida vemos que la máquina virtual con la dirección IP 172.16.1.22, CentOs-2 forma parte del EPG:

| End Point | MAC | IP | Learning Source | Hosting Server | Reporting Controller Name | Interface | Multicast Address | Encap |
|-----------|-------------------|-------------|-----------------|----------------|---------------------------|--------------------------------------|-------------------|------------------------------|
| CentOs-2 | 00:50:56:68:5C:FD | 172.16.1.22 | learned vmm | 10.88.247.33 | Vcenter | Pod-1/Node-104/eth1/48 (learned.vmm) | --- | vlan-3402(P) vlan-3403(S) |

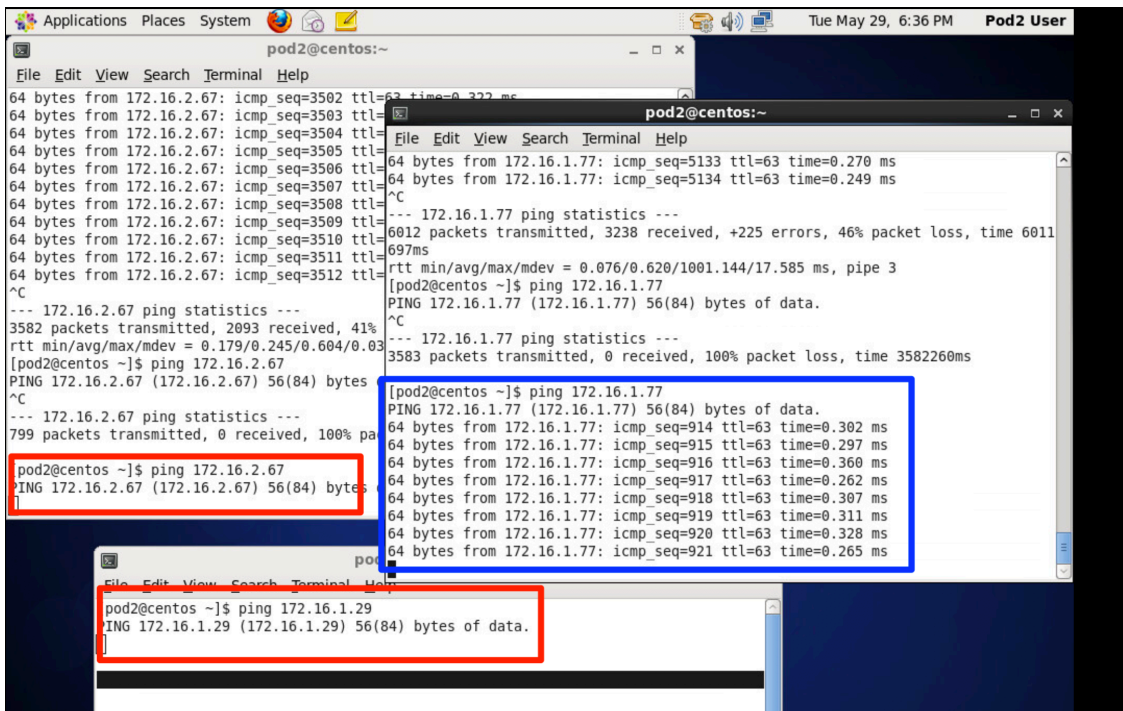
La comunicación de la VM CentOS-1 restringe la comunicación a la IP 172.16.1.22, ya que el endpoint ahora forma parte del segundo uSeg EPG:



Al generar un contrato entre el uSeg EPG **MACUseg** y el EPG **Blue**, podemos permitir que la máquina virtual CentOS-2 pueda comunicarse con la IP 172.16.1.77 (Redhat-4, EPG **Blue**):



CentOS-2:



Este ejemplo confirma la importancia del orden que los atributos tienen sobre los otros. Los endpoints serán clasificados bajo el uSeg EPG que primero coincida con la regla, en el orden predefinido, no en el orden en que fue creado el uSeg EPG.