

Service EPG Configuration Examples

For more information on service EPGs, see:

- Cloud Service Endpoint Groups
- Creating a Service EPG Using the Cisco Cloud Network Controller GUI
- Creating a Service EPG Using the REST API

The following sections provide configuration examples for service EPGs.

• Azure Kubernetes Services (AKS) Service EPG Configuration Example, on page 1

Azure Kubernetes Services (AKS) Service EPG Configuration Example

This section provides procedures for configuring an example service EPG with the following settings:

- Service Type: Azure Kubernetes Services (AKS)
 - Azure Kubernetes Services (AKS) requires access to other services.
 - Cisco Cloud Network Controller automates the programming of the rules.
- **Deployment type**: Cloud Native Managed. In this type of deployment, the service is instantiated in your VNet or subnet (created through the Cisco Cloud Network Controller). For example, an Azure Kubernetes Services (AKS) service could be deployed in a subnet that is managed by the Cisco Cloud Network Controller.
- Access type: Private

The procedures to configure this example service EPG for AKS are provided in the following sections.

Creating a Subnet in the Cloud Context Profile

These procedures describe how to create a subnet in a cloud context profile to be used by the Azure Kubernetes Services (AKS) service EPG. You will be making configurations through the Cisco Cloud Network Controller GUI in these procedures.

Before you begin

- In one browser window, log into your Cisco Cloud Network Controller GUI.
- In another browser window, log into your Azure account for the Cisco Cloud Network Controller infra tenant and go to the Azure management portal:

https://portal.azure.com/#home

- Step 1In the Cisco Cloud Network Controller GUI, click the Intent icon.The Intent menu appears.
- Step 2Click the drop-down arrow below the Intent search box and choose Application Management.A list of Application Management options appear in the Intent menu.
- Step 3 From the Application Management list in the Intent menu, click Create Cloud Context Profile.

The Create Cloud Context Profile window appears.

Name * Tenant * Select Tenant > Description Select Region * Select Region > VHF * Select VRP > CIDR Block Range Subnets Primary Viet Gateway Router	Name *	
Tenart * Select Tenant > Description Settings Region * Select Region > VRF * Select VRF > CIDR * CIDR Block Range Subnets Primary VNet Gateway Router Enabled	Tenant * Select Region * Select NPF > Select VPF > Select VPF > Select VPF > Select Region > VRF * Select Region > VRF * Select Region > Selec	
Settings Region * Setect Region > VVFF * CIDR Block Range Subnets Primary VNet Gateway Router	Description Settings Region * Select Region > VRF * Select VRF > Conserved C	
Settings Region * Select Region > VRF * Select VRF > CIDR Block Range CID	Settings Region * Select Region > VRF * Select VRF > OURDe *	
Settings Region * Select Region > VRF* Select VRF > CIDR s* CIDR Block Range Submets Primary VNet Gateway Router Enabled	Settings Region * Select Region > VRF+ Select VRF > Conser	
Region * Select Region > VPF * Select VFF > CIDRs * CIDR Block Range Subnets Primary VNet Gateway Router Enabled	Region * Select Region > VRF * Select VRF >	
VRF * Select VRF > CIDRs * CIDRs * CIDR Block Range Subnets Primary VNet Gateway Router Enabled	VRF* Select VRF>	
CIDRs * CIDR Block Range Subnets Primary VNet Gateway Router Enabled	CIDRs *	
CIDR Block Range Subnets Primary		
VNet Gateway Router Enabled	CIDR Block Range Subnets Primary	Subnets Primary
Enabled	VNet Gateway Router	
	Enabled	
VNet Peering	VNet Peering	

Step 4 Enter the following information in the **Create Cloud Context Profile** window.

- Name: Enter the name of the cloud context profile. For example, ct_ctxprofile_eastus.
- Tenant: Click Select Tenant, choose a tenant for the cloud context profile for this use case, then click Select.
- Region: Click Select Region, choose the region (for example, eastus), then click Select.
- VRF: Click Select VRF, select the appropriate VRF, then click Select.
- Add CIDR: Enter the CIDR information.
- a. Click Add CIDR.

b. Enter the address in the CIDR Block Range field.

For example, 30.1.0.0/16.

- c. Uncheck (disable) the Primary check box.
- d. Click Add Subnet and enter the subnet address in the Address field.

For example, 30.1.0.0/17. Note that AKS cluster requires 338 addresses.

- e. Click Add.
- VNet Gateway Router: Leave the box unchecked (unselected) for this field.
- VNet Peering: Check this box to enable VNet peering.

Step 5 Click **Save** when finished.

What to do next

Go to Creating the Cloud Service EPG for AKS, on page 3.

Creating the Cloud Service EPG for AKS

These procedures describe how to create the cloud service EPG with the Azure Kubernetes Services (AKS) service type. You will be making configurations through the Cisco Cloud Network Controller GUI in these procedures.

Before you begin

Complete the procedures in Creating a Subnet in the Cloud Context Profile, on page 1 before proceeding with these procedures.

Step 1 In the Cisco Cloud Network Controller GUI, click the **Intent** icon.

The Intent menu appears.

- Step 2Click the drop-down arrow below the Intent search box and choose Application Management.A list of Application Management options appear in the Intent menu.
- Step 3From the Application Management list in the Intent menu, click Create EPG.The Create EPG window appears.

Create EPO	G			- ×
	General			
	Name *			
	Tenant * Select Tenant > Application Profile * Select Application Profile > Description		D ₂	
	Settings			
	Type * Application External Service VRF * Select VRF >			
	Endpoints			
	Endpoint Selectors			
	Name	Match Expression		
	Add Endpoint Selector			
				Cancel Save

Step 4 Enter the following information in the **Create EPG** window.

- Name: Enter the name of the cloud service EPG. For example, svc-Hub-AzureAKS.
- Tenant: Click Select Tenant, choose a tenant for the cloud service EPG for this use case, then click Select.
- Application Profile: Click Select Application Profile, choose the application profile, then click Select.
- Type: Choose Service as the EPG type.
- VRF: Click Select VRF, select the appropriate VRF, then click Select.
- Service Type : Choose the Azure Kubernetes Services (AKS) service type.
- Deployment Type: Choose the Cloud Native Managed deployment type.
- Access Type: Choose the Private access type.

Step 5 Click Add Endpoint Selector.

The Add Endpoint Selector window appears.

For this use case, we will be creating an endpoint selector where the IP address matches the subnet information configured in the previous step, 30.1.0.0/17. Having the IP address in the endpoint selector match the subnet in the previous step allows the Cisco Cloud Network Controller to program the NSG to allow all of the required rules for this service type.

- Step 6 In the Add Endpoint Selector window, enter a name in the Name field.
- **Step 7** Click the **Key** drop-down list to choose a key.

At this time, **IP** is the only option available as a key for this access type.

- **Step 8** Click the **Operator** drop-down list and choose **equals**.
- **Step 9** In the Value field, enter 30.1.0.0/17, then click the check mark to validate the entry.
- Step 10 Click Add.

Step 11 Click Save when finished.

What to do next

Go to Verifying the Outbound Security Rules, on page 5.

Verifying the Outbound Security Rules

These procedures describe how to verify that the necessary outbound security rules are getting configured correctly. The Cisco Cloud Network Controller configures all of the outbound security rules in Azure that are needed for AKS to be deployed in the Azure portal.

Before you begin

Complete the procedures in Creating the Cloud Service EPG for AKS, on page 3 before proceeding with these procedures.

Step 1 In the Azure portal, navigate to the network security group for the subnet that was automatically created:

- a) Navigate to appropriate resource group.
- b) Select the subnet that was used for the AKS service EPG.
- c) Locate the necessary outbound security group.
- **Step 2** Locate the **Outbound security rules** area in the page and verify that the outbound security rules for the NSG are configured correctly.

For more information on the outbound security rules, see:

https://docs.microsoft.com/en-us/azure/aks/limit-egress-traffic

What to do next

Go to Creating a Kubernetes Service, on page 5.

Creating a Kubernetes Service

These procedures describes how to create a Kubernetes service. You will be making configurations through the Azure portal in these procedures.



Note

The following procedure describes how to create a Kubernetes service through the Azure portal. An alternative method for creating a Kubernetes service is also provided in the Using Azure Kubernetes Service with Cisco Cloud Network Controller document.

Before you begin

Complete the procedures in Verifying the Outbound Security Rules, on page 5 before proceeding with these procedures.

Step 1 In the Azure portal, search for the term Kubernetes Service by Microsoft and click on the search result.

The Kubernetes Service page appears.

Step 2 Click **Create** in the **Kubernetes Service** page.

The Create Kubernetes cluster page appears.

Home > Kubernetes services >

Create Kubernetes cluster

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ①		~
Resource group * ①	Company and the	\sim
	Create new	
Cluster details		
Kubernetes cluster name * 🕕	100	
Region * ①	(US) East US 2	\sim
Availability zones ①	Zones 1,2,3	\checkmark
Kubernetes version * 🕕	1.18.10 (default)	\sim

Primary node pool

The number and size of nodes in the primary node pool in your cluster. For production workloads, at least 3 nodes are recommended for resiliency. For development or test workloads, only one node is required. If you would like to add additional node pools or to see additional configuration options for this node pool, go to the 'Node pools' tab above. You will be able to add additional node pools after creating your cluster. Learn more about node pools in Azure Kubernetes Service

Node size * ①	Standard DS2 v2 Change size	
Node count * 🕕	0	1

- **Step 3** In the **Basics** tab, configure the following areas:
 - Subscription: Select the appropriate subscription.
 - Resource Group: Select the appropriate resource group.
 - Kubernetes cluster name: Enter a unique name for this Kubernetes cluster.
 - Region: Select the appropriate region.
 - Kubernetes version: Leave the default selection as-is.
 - Node size: Leave the default selection as-is.

• Node count: Verify that the scroll bar is all the way to the left so that the entry for this field is 1.

Step 4 Click Next: Node pools. Leave the default entries as-is and click Next: Authentication to advance to the Authentication tab.

Home > Kubernetes services >		Configure service principal	×
Create Kubernetes clus	ter		
Basics Node pools Authenticatis Cluster infrastructure The duster infrastructure authentication of the duster. This can be either a service pri Authentication method Service principal * O	Metworking Integrations Tags Review + create working integrations Tags Review + create working integrations and the structure standard to compare for a system assigned managed identity cf. Service principal Configure service principal	Service principal Create new Use existing Service principal client ID * Service principal client secret * Service principal client secret *	
Kubernetes authentication and author Authentication and authorization are used user may do once authenticated. Learn m Role-based access control (RBAC)	tation by the kubernetes duster to control user access to the duster as well as what the size about Kubernetes authentication of © Enabled © Disabled		
Node pool OS disk encryption By default, all disks in AKS are encrypted a supply your own keys using a disk encrypt encrypt the OS disks for all node pools in	t rest with Microsoft-managed keys. For additional control over encryption, you can on set backed by an Azure Key Yault. The disk encryption set will be used to the cluster. Learn more d		
Encryption type	(Default) Encryption at-rest with a platform-managed key		
Review + create < Prev	ious Next : Networking >	Ok	

Step 5 In the **Authentication** tab, configure the following areas:

• Authentication method: Choose Service principal.

The Service principal field appears.

• Service principal: Click Configure service principal.

In the Configure service principal window, configure the following areas:

• Service principal: Choose either Create new or Use existing.

If you choose Use existing, enter the following information for the existing service principal:

- Service principal client ID
- Service principal client secret
- **Note** Make a note of the entries that you enter in these two fields. You will be using the entries in these fields later in these procedures.

Click OK to return to the Authentication tab in the Create Kubernetes cluster window.

- Role-based acces control (RBAC): Choose Enabled.
- AKS-managed Azure Active Directory: Choose Disabled.
- Encryption type: Leave the default selection as-is.
- **Step 6** Click **Next: Networking** to advance to the **Networking** tab.

asics Node pools Authenticat	ion Networking	Integrations	Tags	Keview + create	
/ou can change networking settings for network using either the 'Kubenet' or 'Az	your cluster, including e ure CNI' options:	enabling HTTP app	olication r	routing and configuring	your
 The kubenet networking plug-in The Azure CNI networking plug-i Application pods are connected c 	creates a new VNet for n allows clusters to use irectly to the VNet, whi	your cluster using a new or existing ich allows for nativ	g default v VNet wit ve integra	values. h customizable address tion with VNet features	es.
Learn more about networking in Azure K	ubernetes Service				
Network configuration 🛈	Kubenet Azure CNI				
	Azure CNI				
	 Azure CNI The Azure CNI pl pod on a node, v value is set for po per node for each 	lugin requires an II which can more qu ods per node. Con h node pool on th	P address iickly exha isider mo e "Node	from the subnet below aust available IP address difying the default value pools" tab. Learn more	r for each ses if a high es for pods பீ
Virtual network * ①	 Azure CNI The Azure CNI pl pod on a node, v value is set for po per node for each 	lugin requires an ll which can more qu ods per node. Con h node pool on th	P address uickly exha sider mo e "Node	from the subnet below aust available IP addres: difying the default value pools" tab. Learn more	of for each ses if a high es for pods ♂
Virtual network * ①	 Azure CNI The Azure CNI pl pod on a node, v value is set for po per node for each Create new 	lugin requires an II vhich can more qu ods per node. Con h node pool on th	P address iickly exha sider mo e "Node	from the subnet below aust available IP address difying the default value pools" tab. Learn more	for each ses if a high es for pods ♂
Virtual network * ① Cluster subnet * ①	Azure CNI Azure CNI pl pod on a node, v value is set for pr per node for eacl Create new	lugin requires an Il vhich can more qu ods per node. Con h node pool on th	P address uickly exha usider mo e "Node	from the subnet below aust available IP addres difying the default value pools" tab. Learn more	r for each ses if a high es for pods ♂ ✓
Virtual network * ① Cluster subnet * ①	Azure CNI Azure CNI pl pod on a node, v value is set for po per node for eacl Create new Manage subnet con	lugin requires an Il which can more qu ods per node. Con h node pool on th inde pool on th	P address iickly exh isider mo e "Node	from the subnet below aust available IP addres difying the default value pools" tab. Learn more	v for each ses if a high ss for pods ♂ ∨
Virtual network * ① Cluster subnet * ① Kubernetes service address range * ①	Azure CNI Azure CNI pi pod on a node, v value is set for po per node for each Create new Manage subnet con	lugin requires an II vhich can more qu ods per node. Con h node pool on th node pool on th	P address iickly exhi sider mode e "Node	from the subnet below aust available IP address difying the default value pools" tab. Learn more	r for each ses if a high ss for pods ♂ ✓
Virtual network * ① Cluster subnet * ① Kubernetes service address range * ① Kubernetes DNS service IP address * ①	Azure CNI Azure CNI pl pod on a node, v value is set for po per node for eacl Create new Manage subnet con	lugin requires an II vhich can more qu ods per node. Con h node pool on th node pool on th	P address uickly exh isider mo e "Node	from the subnet below aust available IP address difying the default value pools" tab. Learn more	r for each ses if a high ss for pods ♂ ✓
Virtual network * ① Cluster subnet * ① Kubernetes service address range * ① Kubernetes DNS service IP address * ① Docker Bridge address * ①	Azure CNI Azure CNI Azure CNI pl pod on a node, v value is set for po per node for eacl Create new Manage subnet con	lugin requires an Il vhich can more qu ods per node. Con h node pool on th ifiguration	P address uickly exh sider mor e "Node Node	from the subnet below aust available IP address difying the default value pools" tab. Learn more	v for each ses if a high ss for pods ♂ ✓

- **Step 7** In the **Networking** tab, configure the following areas:
 - Network configuration: Choose Azure CNI.
 - Virtual network: Choose the corresponding virtual network.
 - Cluster subnet: Choose the Cisco Cloud Network Controller -managed subnet.
 - Kubernetes service address range: Leave the default selection as-is, or change the entry, if necessary.
 - Kubernetes DNS service IP address: Leave the default selection as-is, or change the entry, if necessary.
 - Docker Bridge address: Leave the default selection as-is, or change the entry, if necessary.
 - DNS name prefix: Leave the default selection as-is, or change the entry, if necessary.
 - · Load balancer: Standard
 - Enable HTTP application routing: Leave the default selection as-is (not enabled), or change the entry, if necessary.
 - Enable Private cluster: Leave the default selection as-is (not enabled), or change the entry, if necessary.
- **Step 8** Click **Next: Integration**, then **Next: Tags**, to advance through those screens without changing any of the default entries, then click **Next: Review+Create**.

Step 9 In the **Review+Create** window, click **Create**, then click **Create** again after the validations pass to create the Kubernetes cluster.

You will see the message Deployment is in progress and the Overview screen for the Kubernetes service will appear.

Home >					
A microsoft.aks-	Overview	\$			
	📋 Delete 🚫 Cancel 🏦 Rede	eploy 💍 Refresh			
👶 Overview	𝔅 We'd love your feedback! →				
😫 Inputs					
š≣ Outputs	Deployment is ir	n progress			
🖻 Template	Deployment name: Subscription: Resource group:	Auko-20210115141025 A108	Start time: 1/15/2021, 2:14:17 PM Correlation ID:		
	 Deployment details (Down 	load)			
	Resource	Туре	Status	Operation details	
	No results.				

Wait until the Kubernetes service is deployed successfully before proceeding (the amount of time it takes to deploy varies). Once this process is completed, the main AKS service will be in your original resource group. Azure will also create an additional resource group specifically for the Kubernetes service, with all of the agentpools VM scales set.

What to do next

Go to Verifying the New Kubernetes Service, on page 9.

Verifying the New Kubernetes Service

These procedures describe how to verify that the new Kubernetes service is in the resource group that was created specifically for the Kubernetes service.

Before you begin

Complete the procedures in Creating a Kubernetes Service, on page 5 before proceeding with these procedures.

- **Step 1** In the Azure portal, click on **Resource groups** in the left nav bar to navigate to the resource groups page.
- **Step 2** In the **Resource groups** page, locate the resource group that was created specifically for the Kubernetes service and click the link for that resource group.

The resource group created specifically for the Kubernetes service will have the following format:

MC_resourcegroupname_clustername_region

Where:

- *resourcegroupname* is the name of the resource group created specifically for the Kubernetes service (MC_aks is the resource group name used by default by Azure)
- clustername is the Kubernetes cluster name that you provided in Step 3, on page 6 in Creating a Kubernetes Service, on page 5.
- region is the region that you selected in Step 3, on page 6 in Creating a Kubernetes Service, on page 5.

For example:

MC_aks_acme-aks-cluster_centralus

The Overview page for the Kubernetes service resource group appears.

Step 3 Locate the line for the **Virtual machine scale set** and click on that link.

This is where the AKS agent is running.

Home > Subscriptions >	>			D9
MC_capic_ Resource group	*			× 1 2
Search (Cmd+/) «	🕂 Add 💷 Edit columns 📋 Delete resource group 🕐 Refresh 🞍 Export to CSV 😵 Open query	$ $ \otimes Assign tags \rightarrow Move \vee $ $ \square Delete	\downarrow Export template \heartsuit Feedback	Open in mobile
(ii) Overview	↑ Essentials			JSON View 6 IBM 7 RC
Activity log	Subscription (change) : ACI-AZURE-QA110	Deployments : 1 Succeeded		8 AD 9 DD
Access control (IAM)	Subscription ID :	Location : East US 2		10 AA 11 DA
Tags	Tags (change) : Click here to add tags			12 13
🗲 Events	Filter by name Type == all X Location == all X Hg Add filter			14 15 16
Settings	Showing 1 to 4 of 4 records.		No grouping V List v	iew V 18
Deployments	Name ↑↓	Туре ↑↓	Location ↑↓	20 21
Policies		Public IP address	East US 2	23
Se Properties	🗌 🌒 aks-agentpool	Network security group	East US 2	25
🔒 Locks	🗌 🎭 aks-agentpool-	Virtual machine scale set	East US 2	27 28
Cost Management	🗌 💠 kubernetes	Load balancer	East US 2	30
S. Cost analysis				32
Cost alerts (preview)				34
Budgets				36
Advisor recommendations				.38
Monitoring				Re
Insights (preview)				
💵 Alerts				
na Metrics	< Previous Page 1 v of 1 Next >			

Step 4 In the left nav bar, click on **Instances** to display the virtual machine instances for this Kubernetes service resource group.

Home > Subscriptions >									
aks-agentpool	-vmss Instances			×					
(2: Search (Crnd+/) ≪) Start (² : Restart] Stop (³), Reimage (³) Delete ↑ Upgrade (³) Referabl <i>Q</i>) Protection Policy									
Noverview	D Search virtual machine instances								
Activity log	Name	Computer name	Status Health sta	te Provisioning state Protection policy					
⁹ α Access control (IAM)	aks-agentpool-	aks-agentpool- vmss000000	Running	Succeeded					
Tags	aks-agentpoolvmss_1	aks-agentpool -vmss000001	Running	Succeeded					
Diagnose and solve problems	aks-agentpool -vmss_2	aks-agentpool -vmss000002	Running	Succeeded					

Step 5 Click on any of the three instances in this window, then verify that the IP address shown in the **Private IP address** field matches your hub subnet IP address.

All three instances shown in this window should have an IP address from the subnet that you selected in Step 7, on page 8 in Creating a Kubernetes Service, on page 5.

Anne > Subscriptions > aks-agentpool- Scale set instance	·vmss_() 0 \$			×
	💋 Connect þ S	start 🦿 Restart 🔲 Stop 🚯 Reimage 📋 Delete ↑ Upgrade 🔑 Protection	Policy		
Overview	↑ Essentials				JSON View
- etc	Instance ID	: 0	Public IP address	1	
setungs	Status	: Running, 1 more	Private IP address	: D	
2 Networking	Location	: East US 2 (Zone 1)	Public IP address (IPv6)	-	
5 Connect	Provisioning state	: Succeeded	Private IP address (IPv6)	11-	
B Disks	Latest model applied	: Yes	Virtual network/subnet	samp tone complete and one size little. It	
Properties	Computer name	: aks-agentpool -vmss000000	Disk	I BE OPTIME TO BE OPTIME TO BE A TO BE AND	
	Fault domain	:1	Protection Policy	14	
Monitoring	SKU	: Standard_DS2_v2	Health state	1-	
Insights	Tags (chapped)	and the second sec	-	a second and a second second	
Metrics	collo (complia)	subsets successively represent to a fight of		a second to a second grant the second	

Step 6 Navigate back to the Overview page for the Kubernetes service resource group, then locate the kubernetes entry, shown with Load balancer as the Type, and click that link.

The Overview page for the Kubernetes load balancer appears.

Step 7 In the left nav bar, click **Backend pools** to view the AKS agents.

Home > Subscriptions > Kubernetes Backene	d pools	> kubernetes					×
Search (Cmd+/) «	🕂 Add 💍 Refresh						
Overview Activity log	Backend pool	Virtual machine	Virtual machine status	Network interface	Private IP address	Availability zone	
Access control (IAM)	∼aksOutboundBackendPool	(3 vi					
Tags		aks-agentpoolvms	s (in Running	aks-agentpool- vmss	101111	1	
Diagnose and solve problems		aks-agentpoolvms	s (in Running	aks-agentpool-	Marca - 10	2	
		aks-agentpoolvms	s (in Running	aks-agentpoolvmss	1010120	3	
Settings	∨kubernetes (3 virtual mach	nes)					
Frontend IP configuration		aks-agentpoolvms	s (in Running	aks-agentpoolvmss	Married Workshop	1	
Backend pools		aks-agentpoolvms	s (in Running	aks-agentpoolvmss	March 110	2	
🐐 Health probes		aks-agentpoolvms	s (in Running	aks-agentpoolvmss	10111120	3	
S= Load balancing rular							

Step 8



- a) In the Azure portal, navigate back to the infra resource group.
- b) Choose **Group by type** for the records shown in the Overview page for the infra resource group.
- c) Scroll down until you see the **Virtual machine** area and click on the virtual machine for the consumer in your contract.

The Overview window for that virtual machine appears.

d) In the left nav bar, under Settings, click Networking.

The Networking window for that virtual machine appears, with information on the inbound and outbound port rules.

e) Click on the **Outbound port rules** tab, then click on one of the outbound port rules listed in the table.

A window slides in from the right, displaying additional information on these outbound port rules. For example, the entry in the Destination IP addresses/CIDR ranges area provides information on the addresses that are associated with the AKS cluster.

What to do next

Go to Installing the Azure and AKS CLI, on page 11.

Installing the Azure and AKS CLI

These procedures describe how to install the Azure and AKS CLI.

Before you begin

Complete the procedures in Verifying the New Kubernetes Service, on page 9 before proceeding with these procedures.

Step 1 On the consumer VM that has internet access, install the Azure CLI.

For more information, see:

https://docs.microsoft.com/en-us/cli/azure/install-azure-cli-linux

For example, to install the Azure CLI in an Ubuntu Linux VM in Azure:

curl -sL https://aka.ms/InstallAzureCliDeb | sudo bash

Step 2 Download and install **kubectl**, the Kubernetes command-line tool, and **kubelogin**, a client-go credential (exec) plugin implementing azure authentication:

az aks install-cli

Step 3 Log in with the service principle information that you entered in Step 5, on page 7 in Creating a Kubernetes Service, on page 5 in these procedures:

```
# az login --service-principal --username <service_principal_client_id>
--password '<service_principal_client_secret>' --tenant <tenant_ID>
```

Where:

- <*service_principal_client_id*> is the entry from the **Service principal client ID** field in Step 5, on page 7 in Creating a Kubernetes Service, on page 5.
- <service_principal_client_secret> is the entry from the Service principal client secret field in Step 5, on page 7 in Creating a Kubernetes Service, on page 5.
- <*tenant_ID*> is the tenant associated with the service principal (the Azure Active Directory tenant ID). To locate the tenant ID information for this command:
- **a.** Sign in to the Azure portal.
- b. Select Azure Active Directory.
- c. Select Properties.
- d. Scroll down to the Tenant ID field. Your tenant ID is displayed in the box.

For more information, see:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-to-find-tenant

For example:

```
# az login --service-principal --username 12a3b456-7c89-1234-5de6-7f89012gh3i4
--password 'secretkey12341234!' --tenant 98765zy4-xwv-3ut2-1uts-rq0pon98m765
```

Step 4 Set a subscription to be the current active subscription.

az account set --subscription <AKS_rg_subscription_ID>

Where *<AKS_rg_subscription_ID>* is the subscription ID of the resource group that Azure created for the Kubernetes service in Verifying the New Kubernetes Service, on page 9.

For example:

az account set --subscription 56klm789n-o0p1-234q-5r6s-7t890123u4v5

Step 5 From the consumer VM, enter the following to log in and connect to AKS.

root@hub-vm:/home/CNC# az aks get-credentials --resource-group <resource_group> --name
<AKS_cluster_name> --admin

Where:

- <*resource_group*> is the name of the infra resource group
- <*AKS_cluster_name*> is the name for the Kubernetes cluster that was entered in Step 3, on page 6 in Creating a Kubernetes Service, on page 5

For example:

A message similar to the following appears:

Merged "azureaksclus-admin" as current context in /root/.kube/config

Step 6 Check the internal IP addresses of each of the nodes.

root@hub-vm:/home/CNC# kubectl get nodes -o wide

Output similar to the following appears:

NAME	STATUS	ROLES	AGE	VERSION	INTERNAL-IP	EXTERNAL-IP	OS-IMAGE	KERNAL-VERSION	CONTAINER-RUNTIME
aks-agentpool-12345678-vmss000000	Ready	agent	14h	v1.17.9	30.1.1.1	<none></none>	Ubuntu 16.04.7 LTS	4.15.0-1092-azure	docker://19.3.12
aks-agentpool-12345678-vmss000001	Ready	agent	14h	v1.17.9	30.1.1.21	<none></none>	Ubuntu 16.04.7 LTS	4.15.0-1092-azure	docker://19.3.12
aks-agentpool-12345678-vmss000002	Ready	agent	14h	v1.17.9	30.1.1.31	<none></none>	Ubuntu 16.04.7 LTS	4.15.0-1092-azure	docker://19.3.12

The IP addresses listed in the INTERNAL-IP column are in your hub subnet.

- Note In the example output above, the entries in the EXTERNAL-IP column are shown as <none> because the Access Type was set to Private in Step 4, on page 4 in Creating the Cloud Service EPG for AKS, on page 3. IP addresses would be displayed in the EXTERNAL-IP column if the Access Type is set to Public and Private.
- **Step 7** (Optional) Assign an admin role to a new user, if necessary.
 - a) In the Azure portal, navigate back to the infra resource group.
 - b) In the records area in the page, scroll down until you find the Kubernetes service entries.
 - c) Click on the Kubernetes service that you configured.

The Overview page for that Kubernetes service is displayed.

d) In the left nav bar, click on Access Control (IAM).

The Access Control (IAM) for that Kubernetes service is displayed.

- e) Click + Add, then select Add role assignment from the drop-down menu.
- f) In the Add role assignment page, make the following selections:
 - In the Role field, select Azure Kubernetes Service Cluster Admin Role from the drop-down menu.
 - In the Assign access to field, select User, group, or service principal.
 - Select the appropriate key.
- g) Click Save at the bottom of the screen.