Minimum User Privileges

This appendix contains the following topics:

Minimum User Privileges on vSphere

The following tables provide the minimal set of privileges that are required by the vSphere user to execute the relevant operations in vCenter:

When using vSphere with HyperFlex

Roles	Privileges	Entities	Propagate to Children
Administrator		vCenter	No

Roles	Privileges	Entities	Propagate to Children
	Datastore.AllocateSpace Datastore.FileManagement Network.Assign Resource.AssignVMToPool StorageProfile.View System.Anonymous System.Read System.View VApp.ApplicationConfig VApp.Import VApp.InstanceConfig VApp.ManagedByConfig VApp.PowerOff VApp.PowerOn VApp.ResourceConfig VApp.Suspend VirtualMachine.Config.AddExistingDisk VirtualMachine.Config.AddNewDisk VirtualMachine.Config.AddRemoveDevice VirtualMachine.Config.AdvancedConfig VirtualMachine.Config.CPUCount VirtualMachine.Config.DiskExtend VirtualMachine.Config.ManagedBy VirtualMachine.Config.Memory VirtualMachine.Config.RawDevice VirtualMachine.Config.RemoveDisk VirtualMachine.Config.Rename VirtualMachine.Config.Resource VirtualMachine.Config.Settings VirtualMachine.Interact.PowerOff VirtualMachine.Interact.PowerOn VirtualMachine.Inventory.Create		

Roles	Privileges	Entities	Propagate to Children
	VirtualMachine.Inventory.CreateFromExisting VirtualMachine.Inventory.Delete VirtualMachine.Provisioning.Clone VirtualMachine.Provisioning.CreateTemplateFromVM VirtualMachine.Provisioning.DeployTemplate		

Roles	Privileges	Entities	Propagate to Children
ccp-datacenter		Datastore	Yes

Roles	Privileges	Entities	Propagate to Children
	Datastore.AllocateSpace Datastore.FileManagement Network.Assign Resource.AssignVMToPool StorageProfile.View System.Anonymous System.Read System.View VApp.ApplicationConfig VApp.Import VApp.InstanceConfig VApp.ManagedByConfig VApp.PowerOff VApp.PowerOn VApp.ResourceConfig VApp.Suspend VirtualMachine.Config.AddExistingDisk VirtualMachine.Config.AddNewDisk VirtualMachine.Config.AddRemoveDevice VirtualMachine.Config.AdvancedConfig VirtualMachine.Config.CPUCount VirtualMachine.Config.DiskExtend VirtualMachine.Config.ManagedBy VirtualMachine.Config.Memory VirtualMachine.Config.RawDevice VirtualMachine.Config.RemoveDisk VirtualMachine.Config.Rename VirtualMachine.Config.Resource VirtualMachine.Config.Settings VirtualMachine.Interact.PowerOff VirtualMachine.Interact.PowerOn VirtualMachine.Inventory.Create		

Roles	Privileges	Entities	Propagate to Children
	VirtualMachine.Inventory.CreateFromExisting VirtualMachine.Inventory.Delete VirtualMachine.Provisioning.Clone VirtualMachine.Provisioning.CreateTemplateFromVM VirtualMachine.Provisioning.DeployTemplate		

For more information on adding a vSphere provider profile, see Adding vSphere Provider Profile.

When using vSphere without Hyperflex

Roles	Privileges	Entities	Propagate to Children
ccp-vcenter	Extension.Register Extension.Unregister Extension.Update StorageProfile.View System.Anonymous System.Read System.View	vCenter	No

Roles	Privileges	Entities	Propagate to Children
ccp-datacenter		Datastore	Yes

Roles	Privileges	Entities	Propagate to Children
	Datastore.AllocateSpace Datastore.FileManagement Network.Assign Resource.AssignVMToPool StorageProfile.View System.Anonymous System.Read System.View VApp.ApplicationConfig VApp.Import VApp.InstanceConfig VApp.ManagedByConfig VApp.PowerOff VApp.PowerOn VApp.ResourceConfig VApp.Suspend VirtualMachine.Config.AddExistingDisk VirtualMachine.Config.AddNewDisk VirtualMachine.Config.AddRemoveDevice VirtualMachine.Config.AdvancedConfig VirtualMachine.Config.CPUCount VirtualMachine.Config.DiskExtend VirtualMachine.Config.ManagedBy VirtualMachine.Config.Memory VirtualMachine.Config.RawDevice VirtualMachine.Config.RemoveDisk VirtualMachine.Config.Rename VirtualMachine.Config.Resource VirtualMachine.Config.Settings VirtualMachine.Interact.PowerOff VirtualMachine.Interact.PowerOn VirtualMachine.Inventory.Create		

Roles	Privileges	Entities	Propagate to Children
	VirtualMachine.Inventory.CreateFromExisting VirtualMachine.Inventory.Delete VirtualMachine.Provisioning.Clone VirtualMachine.Provisioning.CreateTemplateFromVM VirtualMachine.Provisioning.DeployTemplate		

For more information on adding a vSphere provider profile, see Adding vSphere Provider Profile.

Minimum User Privileges on AWS

The following table provides the minimal set of privileges that are required by an AWS user to create the EKS and EC2 resources.

Roles	Privileges (* Indicates full access)	Entities	Propagate to Children
aws-role	cloudformation	*	No
	elasticloadbalancing	*	
	autoscaling	*	
	ec2	*	
	eks	*	
	ecr	*	
	ecs	*	
	s3	*	
	iam	List*	
		Get*	
		PassRole	
		AddRoleToInstanceProfile	
		RemoveRoleFromInstanceProfile	
		CreateRole	
		CreateInstanceProfile	
		DeleteInstanceProfile	
		DeleteRole	
		DeleteRolePolicy	
		AttachRolePolicy	
		DetachRolePolicy	
		PutRolePolicy	
		AccessKey	
		MFA	

For more information on configuring the necessary permissions, see Configuring Permissions for AWS Account.

For more information on adding an Amazon provider profile, see Adding Amazon Provider Profile.

Minimum User Privileges on AKS

For using Cisco Container Platform with Azure Kubernetes Service, you must use a Service Principal with an **Owner** role.

For more information on adding an Azure provider profile, see Adding Azure Provider Profile

User Privileges on GKE

For using Cisco Container Platform with GKE, you must use a service account with the permissions as described in Creating Service Account.

Erase User Data

You need to erase user data and return a cluster to a clean state when its physical media is replaced or removed. When working with **Virtual Volumes**, deleting or overwriting a file is not adequate for completely erasing user data. File systems do not overwrite the disk blocks that contain data. This means that deletion of a VM or datastore does not erase user data. In order to securely erase user data, you need to erase the physical storage underlying the datastore.

For more information on securely erasing user data from a cluster, see the latest documentation from your storage vendor.