OpenShift Dedicated 4

Planning your environment

An overview of planning for Dedicated 4

Last Updated: 2022-08-03

OpenShift Dedicated 4 Planning your environment

An overview of planning for Dedicated 4

Legal Notice

Abstract

This document provides planning considerations for OpenShift Dedicated cluster deployments.

Table of Contents

CHAPTER 1. CUSTOMER CLOUD SUBSCRIPTIONS ON AWS

OpenShift Dedicated provides a Customer Cloud Subscription (CCS) model that allows Red Hat to deploy and manage clusters into a customer's existing Amazon Web Service (AWS) account.

1.1. UNDERSTANDING CUSTOMER CLOUD SUBSCRIPTIONS ON AWS

To deploy OpenShift Dedicated into your existing Amazon Web Services (AWS) account using the Customer Cloud Subscription (CCS) model, Red Hat requires several prerequisites be met.

Red Hat recommends the usage of an AWS Organization to manage multiple AWS accounts. The AWS Organization, managed by the customer, hosts multiple AWS accounts. There is a root account in the organization that all accounts will refer to in the account hierarchy.

It is recommended for the OpenShift Dedicated cluster using a CCS model to be hosted in an AWS account within an AWS Organizational Unit. A service control policy (SCP) is created and applied to the AWS Organizational Unit that manages what services the AWS sub-accounts are permitted to access. The SCP applies only to available permissions within a single AWS account for all AWS sub-accounts within the Organizational Unit. It is also possible to apply a SCP to a single AWS account. All other accounts in the customer's AWS Organization are managed in whatever manner the customer requires. Red Hat Site Reliability Engineers (SRE) will not have any control over SCPs within the AWS Organization.

1.2. CUSTOMER REQUIREMENTS

OpenShift Dedicated clusters using a Customer Cloud Subscription (CCS) model on Amazon Web Services (AWS) must meet several prerequisites before they can be deployed.

1.2.1. Account

- The customer ensures that AWS limits are sufficient to support OpenShift Dedicated provisioned within the customer-provided AWS account.
- The customer-provided AWS account should be in the customer's AWS Organization with the applicable service control policy (SCP) applied.

  NOTE

  It is not a requirement that the customer-provided account be within an AWS Organization or for the SCP to be applied, however Red Hat must be able to perform all the actions listed in the SCP without restriction.

- The customer-provided AWS account must not be transferable to Red Hat.
- The customer may not impose AWS usage restrictions on Red Hat activities. Imposing restrictions severely hinders Red Hat's ability to respond to incidents.
- Red Hat deploys monitoring into AWS to alert Red Hat when a highly privileged account, such as a root account, logs into the customer-provided AWS account.
- The customer can deploy native AWS services within the same customer-provided AWS account.

NOTE

Customers are encouraged, but not mandated, to deploy resources in a Virtual Private Cloud (VPC) separate from the VPC hosting OpenShift Dedicated and other Red Hat supported services.

1.2.2. Access requirements

- To appropriately manage the OpenShift Dedicated service, Red Hat must have the **AdministratorAccess** policy applied to the administrator role at all times.

  NOTE

  This policy only provides Red Hat with permissions and capabilities to change resources in the customer-provided AWS account.

- Red Hat must have AWS console access to the customer-provided AWS account. This access is protected and managed by Red Hat.

- The customer must not utilize the AWS account to elevate their permissions within the OpenShift Dedicated cluster.

- Actions available in OpenShift Cluster Manager must not be directly performed in the customer-provided AWS account.

1.2.3. Support requirements

- Red Hat recommends that the customer have at least Business Support from AWS.

- Red Hat has authority from the customer to request AWS support on their behalf.

- Red Hat has authority from the customer to request AWS resource limit increases on the customer-provided account.

- Red Hat manages the restrictions, limitations, expectations, and defaults for all OpenShift Dedicated clusters in the same manner, unless otherwise specified in this requirements section.

1.2.4. Security requirements

- The customer-provided IAM credentials must be unique to the customer-provided AWS account and must not be stored anywhere in the customer-provided AWS account.

- Volume snapshots will remain within the customer-provided AWS account and customer-specified region.

- Red Hat must have ingress access to EC2 hosts and the API server through white-listed Red Hat machines.

- Red Hat must have egress allowed to forward system and audit logs to a Red Hat managed central logging stack.

1.3. REQUIRED CUSTOMER PROCEDURE

The Customer Cloud Subscription (CCS) model allows Red Hat to deploy and manage OpenShift Dedicated into a customer's Amazon Web Services (AWS) account. Red Hat requires several prerequisites in order to provide these services.

Procedure

1. If the customer is using AWS Organizations, you must either use an AWS account within your organization or create a new one .
2. To ensure that Red Hat can perform necessary actions, you must either create a service control policy (SCP) or ensure that none is applied to the AWS account.
3. Attach the SCP to the AWS account.
4. Within the AWS account, you must create an **osdCcsAdmin** IAM user with the following requirements:
   - This user needs at least **Programmatic access** enabled.
   - This user must have the **AdministratorAccess** policy attached to it.
5. Provide the IAM user credentials to Red Hat.
   - You must provide the **access key ID** and **secret access key** in OpenShift Cluster Manager.

1.4. MINIMUM REQUIRED SERVICE CONTROL POLICY (SCP)

Service control policy (SCP) management is the responsibility of the customer. These policies are maintained in the AWS Organization and control what services are available within the attached AWS accounts.

Required/optional	Service	Actions	Effect
Required	Amazon EC2	All	Allow
	Amazon EC2 Auto Scaling	All	Allow
	Amazon S3	All	Allow
	Identity And Access Management	All	Allow
	Elastic Load Balancing	All	Allow
	Elastic Load Balancing V2	All	Allow
	Amazon CloudWatch	All	Allow
	Amazon CloudWatch Events	All	Allow

Required/optional	Service	Actions	Effect
	Amazon CloudWatch Logs	All	Allow
	AWS Support	All	Allow
	AWS Key Management Service	All	Allow
	AWS Security Token Service	All	Allow
	AWS Resource Tagging	All	Allow
	AWS Route53 DNS	All	Allow
	AWS Service Quotas	ListServices GetRequestedServiceQuotaChange GetServiceQuota RequestServiceQuotaIncrease ListServiceQuotas	Allow
Optional	AWS Billing	ViewAccount Viewbilling ViewUsage	Allow
	AWS Cost and Usage Report	All	Allow
	AWS Cost Explorer Services	All	Allow

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "autoscaling:*"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:*"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:*"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:*"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:*"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "events:*"
            ],
            "Resource": [
                "*"
            ]
        },
    {
      "Effect": "Allow",
      "Action": [
        "logs:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "support:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "sts:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "tag:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "route53:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
            "Action": [
                "servicequotas:ListServices",
                "servicequotas:GetRequestedServiceQuotaChange",
                "servicequotas:GetServiceQuota",
                "servicequotas:RequestServiceQuotaIncrease",
                "servicequotas:ListServiceQuotas"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

1.5. RED HAT MANAGED IAM REFERENCES FOR AWS

Red Hat is responsible for creating and managing the following Amazon Web Services (AWS) resources: IAM policies, IAM users, and IAM roles.

1.5.1. IAM policies

NOTE

IAM policies are subject to modification as the capabilities of OpenShift Dedicated change.

- The **AdministratorAccess** policy is used by the administration role. This policy provides Red Hat the access necessary to administer the OpenShift Dedicated cluster in the customer-provided AWS account.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "*",
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

- The **CustomerAdministratorAccess** role provides the customer access to administer a subset of services within the AWS account. At this time, the following are allowed:
    - VPC Peering
    - VPN Setup
    - Direct Connect (only available if granted through the service control policy)

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVpnGateway",
        "ec2:DescribeVpnConnections",
        "ec2:AcceptVpcPeeringConnection",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:CreateVpnConnectionRoute",
        "ec2:RejectVpcPeeringConnection",
        "ec2:DetachVpnGateway",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DescribeVpcs",
        "ec2:CreateVpnGateway",
        "ec2:ModifyVpcPeeringConnectionOptions",
        "ec2:DeleteVpnConnection",
        "ec2:CreateVpcPeeringConnection",
        "ec2:DescribeVpnGateways",
        "ec2:CreateVpnConnection",
        "ec2:DescribeRouteTables",
        "ec2:CreateTags",
        "ec2:CreateRoute",
     "directconnect:*"
      ],
      "Resource": "*"
    }
  ]
}
```

- If enabled, the **BillingReadOnlyAccess** role provides read-only access to view billing and usage information for the account.
  Billing and usage access is only granted if the root account in the AWS Organization has it enabled. This is an optional step the customer must perform to enable read-only billing and usage access and does not impact the creation of this profile and the role that uses it. If this role is not enabled, users will not see billing and usage information. See this tutorial on how to enable access to billing data.

  ```
  {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "aws-portal:ViewAccount",
          "aws-portal:ViewBilling"
        ],
        "Resource": "*"
      }
    ]
  }
  ```

1.5.2. IAM users

The **osdManagedAdmin** user is created immediately after taking control of the customer-provided AWS account. This is the user that will perform the OpenShift Dedicated cluster installation.

1.5.3. IAM roles

- The **network-mgmt** role provides customer-federated administrative access to the AWS account through a separate AWS account. It also has the same access as a read-only role. The following policies are attached to the role:
  - AmazonEC2ReadOnlyAccess
  - CustomerAdministratorAccess
- The **read-only** role provides customer-federated read-only access to the AWS account through a separate AWS account. The following policies are attached to the role:
  - AWSAccountUsageReportAccess
  - AmazonEC2ReadOnlyAccess
  - AmazonS3ReadOnlyAccess
  - IAMReadOnlyAccess
  - BillingReadOnlyAccess

1.6. PROVISIONED AWS INFRASTRUCTURE

This is an overview of the provisioned Amazon Web Services (AWS) components on a deployed OpenShift Dedicated cluster. For a more detailed listing of all provisioned AWS components, see the OpenShift Container Platform documentation.

1.6.1. AWS Elastic Computing (EC2) instances

AWS EC2 instances are required to deploy the control plane and data plane functions of OpenShift Dedicated in the AWS public cloud. Instance types might vary for control plane and infrastructure nodes depending on worker node count.

- Single availability zone
  - 3 m5.2xlarge minimum (control plane nodes)
  - 2 r5.xlarge minimum (infrastructure nodes)
  - 2 m5.xlarge minimum but highly variable (worker nodes)
- Multiple availability zones
  - 3 m5.2xlarge minimum (control plane nodes)
  - 3 r5.xlarge minimum (infrastructure nodes)
  - 3 m5.xlarge minimum but highly variable (worker nodes)

1.6.2. AWS Elastic Block Store (EBS) storage

Amazon EBS block storage is used for both local node storage and persistent volume storage.

Volume requirements for each EC2 instance:

- Control plane volumes
  - Size: 350 GB
  - Type: io1
  - Input/output operations per second: 1000
- Infrastructure volumes
  - Size: 300 GB
  - Type: gp2
  - Input/output operations per second: 900
- Worker volumes
  - Size: 300 GB
  - Type: gp2
  - Input/output operations per second: 900

1.6.3. Elastic load balancers

Up to two Network Elastic Load Balancers (ELBs) for API and up to two Classic ELBs for application router. For more information, see the ELB documentation for AWS.

1.6.4. S3 storage

The image registry and Elastic Block Store (EBS) volume snapshots are backed by AWS S3 storage. Pruning of resources is performed regularly to optimize S3 usage and cluster performance.

NOTE

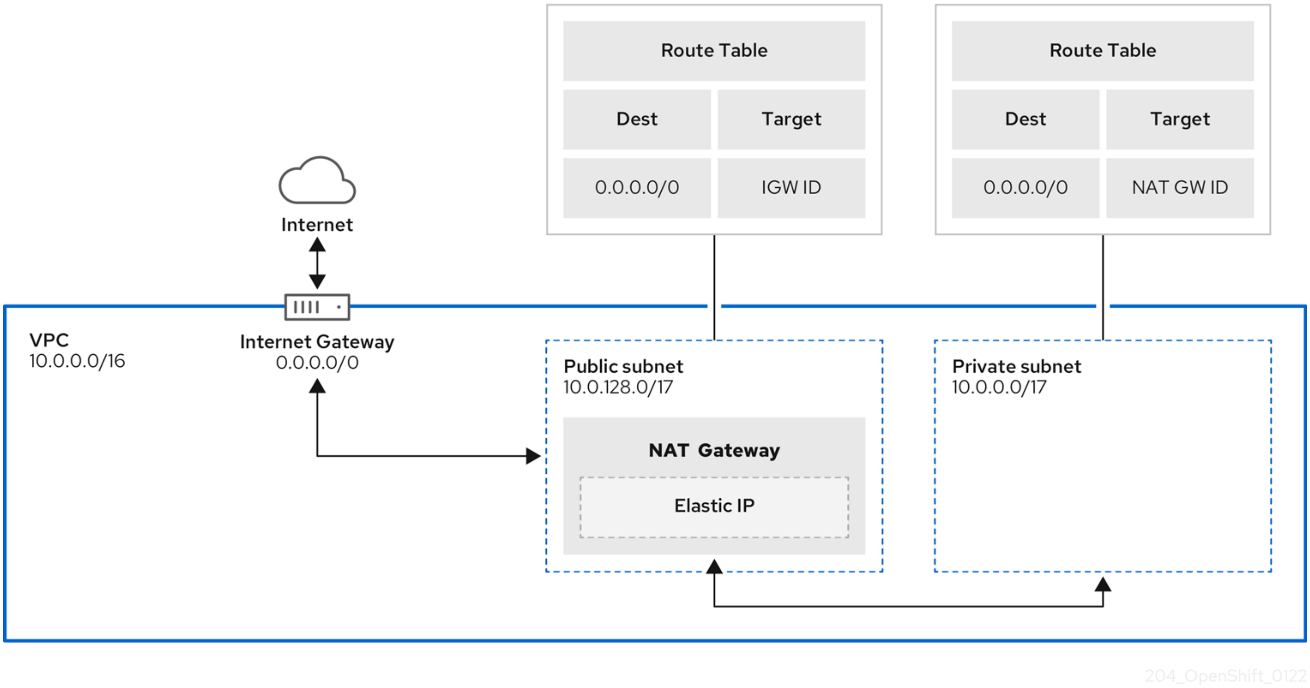
Two buckets are required with a typical size of 2 TB each.

1.6.5. VPC

Customers should expect to see one VPC per cluster. Additionally, the VPC needs the following configurations:

- **Subnets**: Two subnets for a cluster with a single availability zone, or six subnets for a cluster with multiple availability zones.
- **Router tables**: One router table per private subnet, and one additional table per cluster.
- **Internet gateways**: One Internet Gateway per cluster.
- **NAT gateways**: One NAT Gateway per public subnet.

1.6.5.1. Sample VPC Architecture



1.6.6. Security groups

AWS security groups provide security at the protocol and port-access level; they are associated with EC2 instances and Elastic Load Balancing. Each security group contains a set of rules that filter traffic coming in and out of an EC2 instance. You must ensure the ports required for the OpenShift Container Platform installation are open on your network and configured to allow access between hosts.

1.7. AWS ACCOUNT LIMITS

The OpenShift Dedicated cluster uses a number of Amazon Web Services (AWS) components, and the default service limits affect your ability to install OpenShift Dedicated clusters. If you use certain cluster configurations, deploy your cluster in certain AWS regions, or run multiple clusters from your account, you might need to request additional resources for your AWS account.

The following table summarizes the AWS components whose limits can impact your ability to install and run OpenShift Dedicated clusters.

Component	Number of clusters available by default	Default AWS limit	Description

Component	Number of clusters available by default	Default AWS limit	Description
Instance Limits	Varies	Varies	At a minimum, each cluster creates the following instances: - One bootstrap machine, which is removed after installation - Three control plane nodes - Two infrastructure nodes for a single availability zone; three infrascture nodes for multi-availability zones - Two worker nodes for a single availability zone; three worker nodes for multi-availability zones These instance type counts are within a new account's default limit. To deploy more worker nodes, deploy large workloads, or use a different instance type, review your account limits to ensure that your cluster can deploy the machines that you need. In most regions, the bootstrap and worker machines uses an **m4.large** machines and the control plane machines use **m4.xlarge** instances. In some regions, including all regions that do not support these instance types, **m5.large** and **m5.xlarge** instances are used instead.
Elastic IPs (EIPs)	0 to 1	5 EIPs per account	To provision the cluster in a highly available configuration, the installation program creates a public and private subnet for each availability zone within a region. Each private subnet requires a NAT Gateway, and each NAT gateway requires a separate elastic IP. Review the AWS region map to determine how many availability zones are in each region. To take advantage of the default high availability, install the cluster in a region with at least three availability zones. To install a cluster in a region with more than five availability zones, you must increase the EIP limit. IMPORTANT To use the **us-east-1** region, you must increase the EIP limit for your account.

Component	Number of clusters available by default	Default AWS limit	Description
Virtual Private Clouds (VPCs)	5	5 VPCs per region	Each cluster creates its own VPC.
Elastic Load Balancing (ELB/NLB)	3	20 per region	By default, each cluster creates internal and external network load balancers for the primary API server and a single classic elastic load balancer for the router. Deploying more Kubernetes LoadBalancer Service objects will create additional load balancers.
NAT Gateways	5	5 per availability zone	The cluster deploys one NAT gateway in each availability zone.
Elastic Network Interfaces (ENIs)	At least 12	350 per region	The default installation creates 21 ENIs and an ENI for each availability zone in your region. For example, the **us-east-1** region contains six availability zones, so a cluster that is deployed in that zone uses 27 ENIs. Review the AWS region map to determine how many availability zones are in each region. Additional ENIs are created for additional machines and elastic load balancers that are created by cluster usage and deployed workloads.
VPC Gateway	20	20 per account	Each cluster creates a single VPC Gateway for S3 access.
S3 buckets	99	100 buckets per account	Because the installation process creates a temporary bucket and the registry component in each cluster creates a bucket, you can create only 99 OpenShift Dedicated clusters per AWS account.
Security Groups	250	2,500 per account	Each cluster creates 10 distinct security groups.

CHAPTER 2. CUSTOMER CLOUD SUBSCRIPTIONS ON GCP

Red Hat recommends the usage of a Google Cloud Platform (GCP) project, managed by the customer, to organize all of your GCP resources. A project consists of a set of users and APIs, as well as billing, authentication, and monitoring settings for those APIs.

It is a best practice for the OpenShift Dedicated CCS cluster to be hosted in a GCP project within a GCP organization. The Organization resource is the root node of the GCP resource hierarchy and all resources that belong to an organization are grouped under the organization node. An IAM service account with certain roles granted is created and applied to the GCP project. When you make calls to the API, you typically provide service account keys for authentication. Each service account is owned by a specific project, but service accounts can be provided roles to access resources for other projects.

2.1. UNDERSTANDING CUSTOMER CLOUD SUBSCRIPTIONS ON GCP

Red Hat OpenShift Dedicated provides a Customer Cloud Subscription (CCS) model that allows Red Hat to deploy and manage OpenShift Dedicated into a customer's existing Google Cloud Platform (GCP) account. Red Hat requires several prerequisites be met in order to provide this service.

Red Hat recommends the usage of GCP project, managed by the customer, to organize all of your GCP resources. A project consists of a set of users and APIs, as well as billing, authentication, and monitoring settings for those APIs.

It is recommended for the OpenShift Dedicated cluster using a CCS model to be hosted in a GCP project within a GCP organization. The Organization resource is the root node of the GCP resource hierarchy and all resources that belong to an organization are grouped under the organization node. An IAM service account with certain roles granted is created and applied to the GCP project. When you make calls to the API, you typically provide service account keys for authentication. Each service account is owned by a specific project, but service accounts can be provided roles to access resources for other projects.

2.2. CUSTOMER REQUIREMENTS

OpenShift Dedicated clusters using a Customer Cloud Subscription (CCS) model on Google Cloud Platform (GCP) must meet several prerequisites before they can be deployed.

2.2.1. Account

- The customer ensures that Google Cloud limits are sufficient to support OpenShift Dedicated provisioned within the customer-provided GCP account.
- The customer-provided GCP account should be in the customer's Google Cloud Organization with the applicable Service Account applied.
- The customer-provided GCP account must not be transferable to Red Hat.
- The customer may not impose GCP usage restrictions on Red Hat activities. Imposing restrictions severely hinders Red Hat's ability to respond to incidents.
- Red Hat deploys monitoring into GCP to alert Red Hat when a highly privileged account, such as a root account, logs into the customer-provided GCP account.
- The customer can deploy native GCP services within the same customer-provided GCP account.

NOTE

Customers are encouraged, but not mandated, to deploy resources in a Virtual Private Cloud (VPC) separate from the VPC hosting OpenShift Dedicated and other Red Hat supported services.

2.2.2. Access requirements

- To appropriately manage the OpenShift Dedicated service, Red Hat must have the **AdministratorAccess** policy applied to the administrator role at all times.

  NOTE

  This policy only provides Red Hat with permissions and capabilities to change resources in the customer-provided GCP account.

- Red Hat must have GCP console access to the customer-provided GCP account. This access is protected and managed by Red Hat.
- The customer must not utilize the GCP account to elevate their permissions within the OpenShift Dedicated cluster.
- Actions available in the OpenShift Cluster Manager must not be directly performed in the customer-provided GCP account.

2.2.3. Support requirements

- Red Hat recommends that the customer have at least Production Support from GCP.
- Red Hat has authority from the customer to request GCP support on their behalf.
- Red Hat has authority from the customer to request GCP resource limit increases on the customer-provided account.
- Red Hat manages the restrictions, limitations, expectations, and defaults for all OpenShift Dedicated clusters in the same manner, unless otherwise specified in this requirements section.

2.2.4. Security requirements

- The customer-provided IAM credentials must be unique to the customer-provided GCP account and must not be stored anywhere in the customer-provided GCP account.
- Volume snapshots will remain within the customer-provided GCP account and customer-specified region.
- Red Hat must have ingress access to the API server through white-listed Red Hat machines.
- Red Hat must have egress allowed to forward system and audit logs to a Red Hat managed central logging stack.

2.3. REQUIRED CUSTOMER PROCEDURE

The Customer Cloud Subscription (CCS) model allows Red Hat to deploy and manage OpenShift Dedicated into a customer's Google Cloud Platform (GCP) project. Red Hat requires several prerequisites in order to provide these services.

WARNING

To use OpenShift Dedicated in your GCP project, the GCP organizational policy constraint, **constraints/iam.allowedPolicyMemberDomains**, cannot be in place.

Procedure

1. Create a Google Cloud project to host the OpenShift Dedicated cluster.

   NOTE

   The project name must be 10 characters or less.

2. Enable the following required APIs in the project that hosts your OpenShift Dedicated cluster:

Table 2.1. Required API services

API service	Console service name
Cloud Deployment Manager V2 API	**deploymentmanager.googleapis.com**
Compute Engine API	**compute.googleapis.com**
Google Cloud APIs	**cloudapis.googleapis.com**
Cloud Resource Manager API	**cloudresourcemanager.googleapis.com**
Google DNS API	**dns.googleapis.com**
Network Security API	**networksecurity.googleapis.com**
IAM Service Account Credentials API	**iamcredentials.googleapis.com**
Identity and Access Management (IAM) API	**iam.googleapis.com**
Service Management API	**servicemanagement.googleapis.com**
Service Usage API	**serviceusage.googleapis.com**
Google Cloud Storage JSON API	**storage-api.googleapis.com**

API service	Console service name
Cloud Storage	**storage-component.googleapis.com**

3. To ensure that Red Hat can perform necessary actions, you must create an **osd-ccs-admin** IAM service account user within the GCP project.
   The following roles must be granted to the service account :

   Table 2.2. Required roles

Role	Console role name
Compute Admin	**roles/compute.admin**
DNS Admin	**roles/dns.admin**
Organizational Policy Viewer	**roles/orgpolicy.policyViewer**
Owner	**roles/owner**
Project IAM Admin	**roles/resourcemanager.projectIamAdmin**
Service Management Administrator	**roles/servicemanagement.admin**
Service Usage Admin	**roles/serviceusage.serviceUsageAdmin**
Storage Admin	**roles/storage.admin**

4. Create the service account key for the **osd-ccs-admin** IAM service account. Export the key to a file named **osServiceAccount.json**; this JSON file will be uploaded in Red Hat OpenShift Cluster Manager when you create your cluster.

2.4. RED HAT MANAGED GOOGLE CLOUD RESOURCES

Red Hat is responsible for creating and managing the following IAM Google Cloud Platform (GCP) resources.

2.4.1. IAM service account and roles

The **osd-managed-admin** IAM service account is created immediately after taking control of the customer-provided GCP account. This is the user that will perform the OpenShift Dedicated cluster installation.

The following roles are attached to the service account:

Table 2.3. IAM roles for osd-managed-admin

Role	Console role name	Description
Compute Admin	**roles/compute.admin**	Provides full control of all Compute Engine resources.
DNS Administrator	**roles/dns.admin**	Provides read-write access to all Cloud DNS resources.
Security Admin	**roles/iam.securityAdmin**	Security admin role, with permissions to get and set any IAM policy.
Storage Admin	**roles/storage.admin**	Grants full control of objects and buckets. When applied to an individual **bucket**, control applies only to the specified bucket and objects within the bucket.
Service Account Admin	**roles/iam.serviceAccountAdmin**	Create and manage service accounts.
Service Account Key Admin	**roles/iam.serviceAccountKeyAdmin**	Create and manage (and rotate) service account keys.
Service Account User	**roles/iam.serviceAccountUser**	Run operations as the service account.

2.4.2. IAM group and roles

The **sd-sre-platform-gcp-access** Google group is granted access to the GCP project to allow Red Hat Site Reliability Engineering (SRE) access to the console for emergency troubleshooting purposes.

The following roles are attached to the group:

Table 2.4. IAM roles for sd-sre-platform-gcp-access

Role	Console role name	Description
Compute Admin	**roles/compute.admin**	Provides full control of all Compute Engine resources.
Editor	**roles/editor**	Provides all viewer permissions, plus permissions for actions that modify state.

Role	Console role name	Description
Organization Policy Viewer	**roles/orgpolicy.policyViewer**	Provides access to view Organization Policies on resources.
Project IAM Admin	**roles/resourcemanager.projectIamAdmin**	Provides permissions to administer IAM policies on projects.
Quota Administrator	**roles/servicemanagement.quotaAdmin**	Provides access to administer service quotas.
Role Administrator	**roles/iam.roleAdmin**	Provides access to all custom roles in the project.
Service Account Admin	**roles/iam.serviceAccountAdmin**	Create and manage service accounts.
Service Usage Admin	**roles/serviceusage.serviceUsageAdmin**	Ability to enable, disable, and inspect service states, inspect operations, and consume quota and billing for a consumer project.
Tech Support Editor	**roles/cloudsupport.techSupportEditor**	Provides full read-write access to technical support cases.

2.5. GCP ACCOUNT LIMITS

The OpenShift Dedicated cluster uses a number of Google Cloud Platform (GCP) components, but the default quotas do not affect your ability to install an OpenShift Dedicated cluster.

A standard OpenShift Dedicated cluster uses the following resources. Note that some resources are required only during the bootstrap process and are removed after the cluster deploys.

Table 2.5. GCP resources used in a default cluster

Service	Component	Location	Total resources required	Resources removed after bootstrap
Service account	IAM	Global	5	0
Firewall Rules	Compute	Global	11	1
Forwarding Rules	Compute	Global	2	0

Service	Component	Location	Total resources required	Resources removed after bootstrap
In-use global IP addresses	Compute	Global	4	1
Health checks	Compute	Global	3	0
Images	Compute	Global	1	0
Networks	Compute	Global	2	0
Static IP addresses	Compute	Region	4	1
Routers	Compute	Global	1	0
Routes	Compute	Global	2	0
Subnetworks	Compute	Global	2	0
Target Pools	Compute	Global	3	0
CPUs	Compute	Region	28	4
Persistent Disk SSD (GB)	Compute	Region	896	128

NOTE

If any of the quotas are insufficient during installation, the installation program displays an error that states both which quota was exceeded and the region.

Be sure to consider your actual cluster size, planned cluster growth, and any usage from other clusters that are associated with your account. The CPU, Static IP addresses, and Persistent Disk SSD (Storage) quotas are the ones that are most likely to be insufficient.

If you plan to deploy your cluster in one of the following regions, you will exceed the maximum storage quota and are likely to exceed the CPU quota limit:

- asia-east2
- asia-northeast2
- asia-south1
- australia-southeast1
- europe-north1

- europe-west2
- europe-west3
- europe-west6
- northamerica-northeast1
- southamerica-east1
- us-west2

You can increase resource quotas from the GCP console, but you might need to file a support ticket. Be sure to plan your cluster size early so that you can allow time to resolve the support ticket before you install your OpenShift Dedicated cluster.