OpenShift Dedicated 4

環境のプランニング

Dedicated 4 のプランニングの概要

Last Updated: 2022-11-21

OpenShift Dedicated 4 環境のプランニング

Dedicated 4 のプランニングの概要

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律上の通知

概要

このドキュメントでは、OpenShift Dedicated クラスターのデプロイメントのプランニングに関する考慮事項を説明します。

目次

第1章 AWS での CUSTOMER CLOUD SUBSCRIPTION

OpenShift Dedicated は、Red Hat がクラスターをお客様の既存の Amazon Web Service (AWS) アカウントにデプロイおよび管理できるようにする Customer Cloud Subscription (CCS) モデルを提供します。

1.1. AWS での CUSTOMER CLOUD SUBSCRIPTION について

Customer Cloud Subscription (CCS) モデルを使用して OpenShift Dedicated を既存の Amazon Web Services (AWS) アカウントにデプロイする場合、Red Hat では複数の前提条件を満たす必要があります。

Red Hat では、複数の AWS アカウントを管理するために AWS Organization を使用することを推奨します。お客様が管理する AWS Organization は、複数の AWS アカウントをホストします。組織には、すべてのアカウントがアカウント階層で参照する組織には root アカウントがあります。

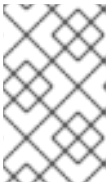
OpenShift Dedicated クラスターは、AWS Organizational Unit 内の AWS アカウントでホストされる CCS モデルを使用することが推奨されます。Service Control Policy (SCP) が作成され、AWS サブアカウントのアクセスが許可されるサービスを管理する AWS Organizational Unit に適用されます。SCP は、Organizational Unit 内のすべての AWS サブアカウントの単一の AWS アカウント内で利用可能なパーミッションにのみ適用されます。SCP を単一の AWS アカウントに適用することもできます。お客様の AWS Organization 内の他のすべてのアカウントは、お客様が必要とされる方法に応じて管理されます。Red Hat のサイト信頼性エンジニアリング (SRE) には、AWS Organization 内の SCP に対する制御がありません。

1.2. お客様の要件

Amazon Web Services (AWS) で Customer Cloud Subscription (CCS) モデルを使用する OpenShift Dedicated クラスターは、デプロイする前に複数の前提条件を満たす必要があります。

1.2.1. アカウント

- お客様は、お客様が指定する AWS アカウント内でプロビジョニングされる OpenShift Dedicated をサポートするには、AWS の制限 が十分に保証されます。
- お客様が提供した AWS アカウントは、該当するサービスコントロールポリシー (SCP) が適用されたお客様の AWS Organization 組織にある必要があります。

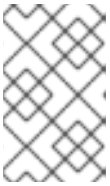


注記

お客様が提供したアカウントが AWS Organization 内にあることや SCP を適用することは要件ではありませんが、Red Hat が制限なしで SCP に一覧表示されるすべてのアクションを実行できるようにする必要があります。

- お客様が指定する AWS アカウントは、Red Hat に転送できません。
- お客様は、Red Hat の各種アクティビティーに対して AWS の使用についての制限を課すことができない場合があります。制限を課すと、Red Hat がインシデントに対応する能力が大幅に妨げられます。
- Red Hat は AWS にモニターリングをデプロイして、root アカウントなどの特権の高いアカウントがお客様が指定する AWS アカウントにログインしたときに Red Hat に警告します。

- お客様は、同じお客様が指定する AWS アカウント内にネイティブ AWS サービスをデプロイすることができます。



注記

OpenShift Dedicated やその他の Red Hat がサポートするサービスをホストする VPC とは別の Virtual Private Cloud (VPC) でリソースをデプロイすることが推奨されますが、これは義務ではありません。

1.2.2. アクセス要件

- OpenShift Dedicated サービスを適切に管理するには、Red Hat では **AdministratorAccess** ポリシーを管理者ロールに常に適用する必要があります。

注記

このポリシーは、お客様が指定する AWS アカウントのリソースを変更するためのパーミッションおよび機能を Red Hat に提供します。

- Red Hat には、お客様が指定する AWS アカウントへの AWS コンソールへのアクセスが必要です。このアクセスは、Red Hat によって保護され、管理されます。
- お客様は AWS アカウントを使用して OpenShift Dedicated クラスター内でパーミッションを昇格させることはできません。
- OpenShift Cluster Manager Hybrid Cloud Console で利用可能なアクションは、顧客提供の AWS アカウントで直接実行しないでください。

1.2.3. サポート要件

- Red Hat では、お客様が少なくとも AWS の ビジネスサポート を用意することを推奨します。
- Red Hat は、お客様より、お客様の代わりに AWS サポートを要求する許可を受けている場合があります。
- Red Hat は、お客様から、お客様が指定するアカウントで AWS リソース制限の引き上げを要求する権限を受けます。
- Red Hat は、この要件のセクションで特に指定されていない限り、すべての OpenShift Dedicated クラスターの制限、期待、およびデフォルトを同じ方法で管理します。

1.2.4. セキュリティー要件

- お客様が指定する IAM 認証情報はお客様が指定する AWS アカウントに固有のもので、お客様が指定する AWS アカウントのどこにも保存しないでください。
- ボリュームスナップショットは、お客様が指定する AWS アカウントおよびお客様が指定するリージョン内に残ります。
- Red Hat には、ホワイトリストの Red Hat マシンを使用して EC2 ホストおよび API サーバーへの ingress アクセスが必要です。
- Red Hat では、Red Hat が管理する中央ロギングスタックにシステムおよび監査ログを転送できるようにするために egress が必要です。

1.3. 必要なお客様の手順

Customer Cloud Subscription (CCS) モデルにより、Red Hat は OpenShift Dedicated をお客様の Amazon Web Services (AWS) アカウントにデプロイおよび管理できるようにします。Red Hat では、これらのサービスを提供するために複数の前提条件が必要です。

手順

1. お客様が AWS Organization を使用している場合、組織内の AWS アカウントを使用するか、新規のアカウントを作成する 必要があります。
2. Red Hat が必要なアクションを実行できるようにするには、Service Control Policy (SCP) を作成するか、AWS アカウントに適用されているものがないことを確認する必要があります。
3. SCP を AWS アカウントに 割り当て ます。
4. AWS アカウント内で、以下の要件で **osdCcsAdmin** IAM ユーザーを 作成する 必要があります。
   - このユーザーは、少なくとも **プログラムによるアクセス** が有効になっている必要があります。
   - このユーザーには、**AdministratorAccess** ポリシーが割り当てられている必要があります。
5. IAM ユーザー認証情報を Red Hat に提供します。
   - OpenShift Cluster Manager Hybrid Cloud Console で **アクセスキー ID** と **シークレットアクセスキー** を提供する必要があります。

1.4. 最低限必要な SERVICE CONTROL POLICY (SCP)

Service Control Policy (SCP) の管理は、お客様の責任です。これらのポリシーは AWS Organization で維持され、割り当てられる AWS アカウント内で利用可能なサービスを管理します。

必須/オプション	サービス	アクション	効果
必須	Amazon EC2	すべて	許可
	Amazon EC2 Auto Scaling	すべて	許可
	Amazon S3	すべて	許可
	アイデンティティーおよびアクセス管理	すべて	許可
	Elastic Load Balancing	すべて	許可
	Elastic Load Balancing V2	すべて	許可

必須/オプション	サービス	アクション	効果
	Amazon CloudWatch	すべて	許可
	Amazon CloudWatch Events	すべて	許可
	Amazon CloudWatch Logs	すべて	許可
	AWS Support	すべて	許可
	AWS Key Management Service	すべて	許可
	AWS Security Token Service	すべて	許可
	AWS Resource Tagging	すべて	許可
	AWS Route53 DNS	すべて	許可
	AWS Service Quotas	ListServices GetRequestedServiceQuotaChange GetServiceQuota RequestServiceQuotaIncrease ListServiceQuotas	許可
オプション	AWS Billing	ViewAccount Viewbilling ViewUsage	許可
	AWS Cost and Usage Report	すべて	許可
	AWS Cost Explorer Services	すべて	許可

```
{
    "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:*"
```

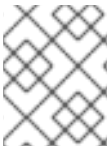
```
        ],
        "Resource": [
            "*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "logs:*"
        ],
        "Resource": [
            "*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "support:*"
        ],
        "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. AWS の RED HAT 管理 IAM リファレンス

Red Hat は、IAM ポリシー、IAM ユーザー、IAM ロールなどの以下の Amazon Web Services (AWS) リソースを作成し、管理します。

1.5.1. IAM ポリシー



注記

IAM ポリシーは、OpenShift Dedicated の機能の変更に伴って変更されることがあります。

- **AdministratorAccess** ポリシーは管理ロールによって使用されます。このポリシーは、お客様が指定する AWS アカウントで OpenShift Dedicated クラスターを管理するために必要なアクセスを Red Hat に提供します。

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

- **CustomerAdministratorAccess** ロールは、AWS アカウント内のサービスのサブセットを管理するためのお客様アクセスを提供します。現時点では、以下が可能になります。
  - VPC ピアリング
  - VPN 設定
  - 直接接続 (サービスコントロールポリシーを通じて許可されている場合にのみ使用可能)

```
{
    "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": "*"
        }
    ]
}
```

- 有効にされている場合、**BillingReadOnlyAccess** ロールは、アカウントの請求情報および使用状況に関する情報を表示するための読み取り専用アクセスを提供します。
  請求および使用状況のアクセスは、AWS Organization の root アカウントが有効になっている場合にのみ付与されます。これは任意のステップであり、読み取り専用の請求および使用方法のアクセスを有効にし、このプロファイルとそれを使用するロールには影響を与えません。このロールが有効になっていない場合は、ユーザーに請求および使用状況の情報は表示されません。請求データへのアクセスを有効にする方法 については、このチュートリアルを参照してください。

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

1.5.2. IAM ユーザー

osdManagedAdmin ユーザーは、お客様が指定する AWS アカウントの制御直後に作成されます。これは、OpenShift Dedicated クラスターのインストールを実行するユーザーです。

1.5.3. IAM ロール

- **network-mgmt** ロールは、別の AWS アカウントを介して AWS アカウントへの管理アクセスを提供します。また、読み取り専用のロールと同じアクセスを持ちます。以下のポリシーはロールに割り当てられます。
    - AmazonEC2ReadOnlyAccess
    - 顧客管理者アクセス
- **read-only** ロールは、別の AWS アカウントを介して AWS アカウントへのカスタマーフェデレーションの読み取り専用アクセスを提供します。以下のポリシーはロールに割り当てられます。
    - AWSAccountUsageReportAccess
    - AmazonEC2ReadOnlyAccess
    - AmazonS3ReadOnlyAccess
    - IAMReadOnlyAccess
    - BillingReadOnlyAccess

1.6. プロビジョニングされた AWS インフラストラクチャー

これは、デプロイされた OpenShift Dedicated クラスター上のプロビジョニングされた Amazon Web Services (AWS) コンポーネントの概要です。プロビジョニングされたすべての AWS コンポーネントの詳細な一覧は、OpenShift Container Platform ドキュメント を参照してください。

1.6.1. AWS Elastic Computing (EC2) インスタンス

AWS EC2 インスタンスは、AWS パブリッククラウドで OpenShift Dedicated のコントロールプレーン機能およびデータプレーン機能をデプロイするために必要になります。インスタンスタイプは、ワーカーノードの数に応じてコントロールプレーンおよびインフラストラクチャーノードによって異なる場合があります。

- 単一アベイラビリティーゾーン
    - 3 m5.2xlarge 最小 (コントロールプレーンノード)
    - 2 r5.xlarge 最小 (インフラストラクチャーノード)
    - 2 m5.xlarge 最小だが高い変数 (ワーカーノード)
- Multiple availability zones
    - 3 m5.2xlarge 最小 (コントロールプレーンノード)
    - 3 r5.xlarge 最小 (インフラストラクチャーノード)
    - 3 m5.xlarge 最小だが高い変数 (ワーカーノード)

1.6.2. AWS Elastic Block Store (EBS) ストレージ

Amazon EBS ブロックストレージは、ローカルノードストレージおよび永続ボリュームストレージの両方に使用されます。

各 EC2 インスタンスのボリューム要件:

- コントロールプレーンボリューム
  - サイズ: 350 GB
  - タイプ: io1
  - 1 秒あたりの入出力操作: 1000
- インフラストラクチャーボリューム
  - サイズ: 300 GB
  - タイプ: gp2
  - 1 秒あたりの I/O 処理数: 900
- ワーカーボリューム
  - サイズ: 300 GB
  - タイプ: gp2
  - 1 秒あたりの I/O 処理数: 900

1.6.3. Elastic Load Balancer

API 用に最大 2 つの Network Elastic Load Balancers (ELB) と、アプリケーションルーター用に最大 2 つの Classic ELB。詳細は、AWS についての ELB ドキュメント を参照してください。

1.6.4. S3 ストレージ

イメージレジストリーおよび Elastic Block Store (EBS) ボリュームスナップショットは、AWS S3 ストレージでサポートされます。リソースのプルーニングは、S3 の使用とクラスターのパフォーマンスを最適化するために定期的に実行されます。

注記

それぞれ 2TB の一般的なサイズの 2 つのバケットが必要です。

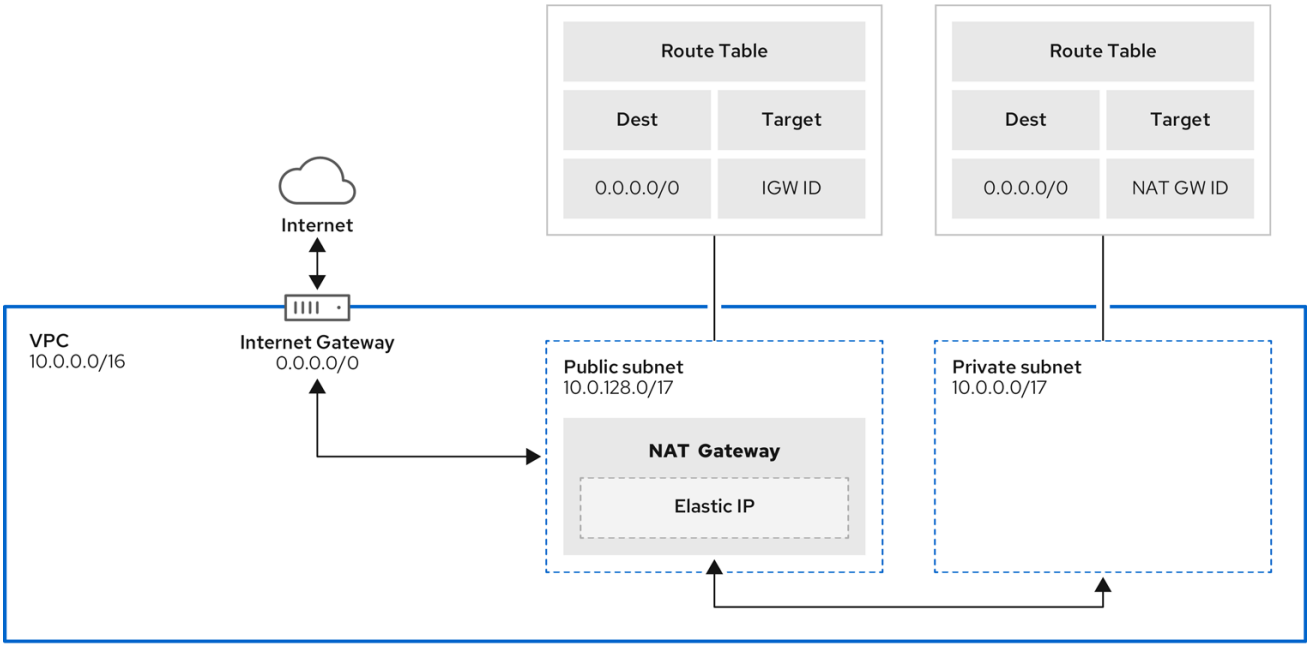
1.6.5. VPC

お客様はクラスターごとに 1 つの VPC を確認できるはずです。さらに、VPC には以下の設定が必要です。

- **サブネット**: 単一アベイラビリティーゾーンがあるクラスターの 2 つのサブネット、または複数のアベイラビリティーゾーンがあるクラスターの 6 つのサブネット。
- **ルートテーブル**: プライベートサブネットごとに 1 つのルートテーブルと、クラスターごとに 1 つの追加テーブル。

- **インターネットゲートウェイ**: クラスターごとに 1 つのインターネットゲートウェイ。
- **NAT ゲートウェイ**: パブリックサブネットごとに 1 つの NAT ゲートウェイ。

1.6.5.1. サンプル VPC アーキテクチャー



1.6.6. セキュリティーグループ

AWS セキュリティーグループは、プロトコルおよびポートアクセスレベルでセキュリティーを提供します。これらは EC2 インスタンスおよび Elastic Load Balancing に関連付けられます。各セキュリティーグループには、EC2 インスタンスの送受信トラフィックをフィルターリングする一連のルールが含まれます。OpenShift Container Platform インストール に必要なポートがネットワーク上で開いており、ホスト間のアクセスを許可するように設定されていることを確認する必要があります。

1.7. AWS アカウントの制限

OpenShift Dedicated クラスターは数多くの Amazon Web Services (AWS) コンポーネントを使用し、デフォルトの サービス制限 は、OpenShift Dedicated クラスターをインストールする機能に影響を与えます。特定のクラスター設定を使用し、クラスターを特定の AWS リージョンにデプロイするか、またはアカウントを使って複数のクラスターを実行する場合、AWS アカウントの追加リソースを要求することが必要になる場合があります。

以下の表は、OpenShift Dedicated クラスターのインストールおよび実行機能に影響を与える可能性のある AWS コンポーネントについてまとめています。

コンポーネント	デフォルトで利用できるクラスターの数	デフォルトの AWS の制限	説明

コンポーネント	デフォルトで利用できるクラスターの数	デフォルトの AWS の制限	説明
インスタンスの制限	変動あり。	変動あり。	少なくとも、各クラスターは次のインスタンスを作成します。 ● 1 つのブートストラップマシン。これはインストール後に削除されます。 ● 3 つのコントロールプレーンノード。 ● 1 つのアベイラビリティゾーンに 2 つのインフラストラクチャーノード。マルチアベイラビリティゾーンに 3 つのインフラストラクチャーノード。 ● 1 つのアベイラビリティゾーンに 2 つのワーカーノード。マルチアベイラビリティゾーンに 3 つのワーカーノード これらのインスタンスタイプの数は、新規アカウントのデフォルト制限内の値です。追加のワーカーノードをデプロイし、大規模なワークロードをデプロイするか、異なるインスタンスタイプを使用するには、アカウントの制限を見直し、クラスターが必要なマシンをデプロイできることを確認します。 ほとんどのリージョンでは、ブートストラップおよびワーカーマシンは **m4.large** マシンを使用し、コントロールプレーンマシンは **m4.xlarge** インスタンスを使用します。これらのインスタンスタイプをサポートしないすべてのリージョンを含む一部のリージョンでは、**m5.large** および **m5.xlarge** インスタンスが代わりに使用されます。

コンポーネント	デフォルトで利用できるクラスターの数	デフォルトの AWS の制限	説明
Elastic IP (EIP)	0 - 1	アカウントごとに 5 つの EIP	クラスターを高可用性設定でプロビジョニングするために、インストールプログラムはそれぞれのリージョン内のアベイラビリティーゾーン にパブリックおよびプライベートのサブネットを作成します。各プライベートサブネットには NAT ゲートウェイ が必要であり、各 NAT ゲートウェイには別個の Elastic IP が必要です。AWS リージョンマップ を確認して、各リージョンにあるアベイラビリティーゾーンの数を判別します。デフォルトの高可用性を利用するには、少なくとも 3 つのアベイラビリティーゾーンがあるリージョンにクラスターをインストールします。アベイラビリティーゾーンが 6 つ以上あるリージョンにクラスターをインストールするには、EIP 制限を引き上げる必要があります。 **重要** **us-east-1** リージョンを使用するには、アカウントの EIP 制限を引き上げる必要があります。
Virtual Private Cloud (VPC)	5	リージョンごとに 5 つの VPC	各クラスターは独自の VPC を作成します。
Elastic Load Balancing (ELB/NLB)	3	リージョンごとに 20	デフォルトで、各クラスターは、プライマリー API サーバーの内部および外部のネットワークロードバランサーおよびルーターの単一の Classic Elastic Load Balancer を作成します。追加の Kubernetes LoadBalancer Service オブジェクトをデプロイすると、追加の ロードバランサー が作成されます。
NAT ゲートウェイ	5	アベイラビリティゾーンごとに 5 つ	クラスターは各アベイラビリティーゾーンに 1 つの NAT ゲートウェイをデプロイします。

コンポーネント	デフォルトで利用できるクラスターの数	デフォルトの AWS の制限	説明
Elastic Network Interface (ENI)	12 以上	リージョンごとに 350	デフォルトのインストールは 21 の ENI を作成し、リージョンの各アベイラビリティーゾーンに 1 つの ENI を作成します。たとえば、**us-east-1** リージョンには 6 つのアベイラビリティーゾーンが含まれるため、そのゾーンにデプロイされるクラスターは 27 の ENI を使用します。AWS リージョンマップを確認して、各リージョンにあるアベイラビリティーゾーンの数を判別します。 追加の ENI が、クラスターの使用およびデプロイされたワークロード別に作成される追加のマシンおよび Elastic Load Balancer について作成されます。
VPC ゲートウェイ	20	アカウントごとに 20	各クラスターは、S3 アクセス用の単一の VPC ゲートウェイを作成します。
S3 バケット	99	アカウントごとに 100 バケット	インストールプロセスでは 1 つの一時的なバケットを作成し、各クラスターのレジストリーコンポーネントがバケットを作成するため、AWS アカウントごとに 99 の OpenShift Dedicated クラスターのみを作成できます。
セキュリティーグループ	250	アカウントごとに 2,500	各クラスターは、10 の個別のセキュリティーグループを作成します。

第2章 GCP での CUSTOMER CLOUD SUBSCRIPTION

Red Hat は、お客様が管理する Google Cloud Platform (GCP) プロジェクトを使用して、すべての GCP リソースを整理することを推奨します。プロジェクトには、ユーザーおよび API のセットと、それらの API の請求、認証、およびモニターリングの設定が含まれます。

OpenShift Dedicated CCS クラスターを GCP 組織内の GCP プロジェクトでホストしておくことがベストプラクティスです。組織リソースは、GCP リソース階層のルートノードであり、組織に属するすべてのリソースは組織ノードでグループ化されます。付与された特定のロールを持つ IAM サービスアカウントが作成され、GCP プロジェクトに適用されます。API を呼び出す場合、通常は認証にサービスアカウントキーを指定します。各サービスアカウントは特定のプロジェクトによって所有されますが、サービスアカウントは他のプロジェクトのリソースにアクセスするためにロールを提供できます。

2.1. GCP での CUSTOMER CLOUD SUBSCRIPTION について

Red Hat OpenShift Dedicated は、Red Hat が OpenShift Dedicated をお客様の既存の Google Cloud Platform (GCP) アカウントにデプロイおよび管理できるようにする Customer Cloud Subscription (CCS) モデルを提供します。Red Hat では、このサービスを提供するために複数の前提条件を満たす必要があります。

Red Hat は、GCP リソースをすべて編成するために、顧客が管理する GCP プロジェクトを使用することを推奨します。プロジェクトには、ユーザーおよび API のセットと、それらの API の請求、認証、およびモニターリングの設定が含まれます。

OpenShift Dedicated クラスターは、GCP 組織内の GCP プロジェクトで CCS モデルを使用することが推奨されます。組織リソースは、GCP リソース階層のルートノードであり、組織に属するすべてのリソースは組織ノードでグループ化されます。付与された特定のロールを持つ IAM サービスアカウントが作成され、GCP プロジェクトに適用されます。API を呼び出す場合、通常は認証にサービスアカウントキーを指定します。各サービスアカウントは特定のプロジェクトによって所有されますが、サービスアカウントは他のプロジェクトのリソースにアクセスするためにロールを提供できます。

2.2. お客様の要件

Google Cloud Platform (GCP) で Customer Cloud Subscription (CCS) モデルを使用する OpenShift Dedicated クラスターは、デプロイする前に複数の前提条件を満たす必要があります。

2.2.1. アカウント

- お客様は、お客様が指定する GCP アカウント内でプロビジョニングされる OpenShift Dedicated をサポートするには、Google Cloud の制限 が十分に保証されます。
- 顧客が提供する GCP アカウントは、該当するサービスアカウントが適用されたお客様の Google Cloud 組織にある必要があります。
- お客様が指定する GCP アカウントは、Red Hat に譲渡することはできません。
- お客様は、Red Hat のアクティビティーに対して GCP の使用制限を課すことができない場合があります。制限を課すと、Red Hat がインシデントに対応する能力が大幅に妨げられます。
- Red Hat は、モニターリングを GCP にデプロイして、root アカウントなどの特権の高いアカウントが顧客提供の GCP アカウントにログインしたときに Red Hat に警告します。
- お客様は、同じ顧客が提供する GCP アカウント内にネイティブ GCP サービスをデプロイすることができます。

注記

OpenShift Dedicated やその他の Red Hat がサポートするサービスをホストする VPC とは別の Virtual Private Cloud (VPC) でリソースをデプロイすることが推奨されますが、これは義務ではありません。

2.2.2. アクセス要件

- OpenShift Dedicated サービスを適切に管理するには、Red Hat では **AdministratorAccess** ポリシーを管理者ロールに常に適用する必要があります。

注記

このポリシーは、お客様が指定する GCP アカウントのリソースを変更するためのパーミッションおよび機能を Red Hat に提供します。

- Red Hat には、お客様が指定する GCP アカウントに対する GCP コンソールへのアクセスが必要です。このアクセスは、Red Hat によって保護され、管理されます。
- お客様は、GCP アカウントを使用して OpenShift Dedicated クラスター内でパーミッションを昇格させることはできません。
- OpenShift Cluster Manager Hybrid Cloud Console で利用可能なアクションは、顧客提供の GCP アカウントで直接実行しないでください。

2.2.3. サポート要件

- Red Hat では、お客様が GCP からの製品サポート が少なくともあることを推奨しています。
- Red Hat には、お客様に代わって GCP サポートを要求する権限があります。
- Red Hat は、お客様から、お客様が指定するアカウントで AWS リソース制限の引き上げを要求する権限を受けます。
- Red Hat は、この要件のセクションで特に指定されていない限り、すべての OpenShift Dedicated クラスターの制限、期待、およびデフォルトを同じ方法で管理します。

2.2.4. セキュリティー要件

- お客様が指定する IAM 認証情報は、お客様が指定する GCP アカウントに固有の認証情報を使用し、お客様が指定する GCP アカウントのどこにも保存しないでください。
- ボリュームスナップショットは、お客様が指定する GCP アカウントおよびお客様が指定するリージョン内に残ります。
- Red Hat には、ホワイトリスト指定された Red Hat マシンを使用して API サーバーへの ingress アクセスが必要です。
- Red Hat では、Red Hat が管理する中央ロギングスタックにシステムおよび監査ログを転送できるようにするために egress が必要です。

2.3. 必要なお客様の手順

Customer Cloud Subscription (CCS) モデルを使用すると、Red Hat は OpenShift Dedicated をお客様の Google Cloud Platform (GCP) プロジェクト にデプロイし、管理することができます。Red Hat では、これらのサービスを提供するために複数の前提条件が必要です。

警告

GCP プロジェクトで OpenShift Dedicated を使用するには、次の GCP 組織ポリシーの制約を設定することはできません。

- **constraints/iam.allowedPolicyMemberDomains**
- **Constraints/storage.uniformBucketLevelAccess**
- **Constraints/compute.restrictLoadBalancerCreationForTypes**
- **Constraint/compute.vmExternalIpAccess** (このポリシー制約は、インストール中のみサポートされていません。インストール後にポリシー制約を再度有効にすることができます。)

手順

1. OpenShift Dedicated クラスターをホストする Google Cloud プロジェクトを作成 します。

注記

プロジェクト名は 10 文字以下である必要があります。

2. OpenShift Dedicated クラスターをホストするプロジェクトで以下の必要な API を 有効にします。

表2.1 必要な API サービス

API サービス	コンソールサービス名
Cloud Deployment Manager V2 API	**deploymentmanager.googleapis.com**
Compute Engine API	**compute.googleapis.com**
Google Cloud API	**cloudapis.googleapis.com**
Cloud Resource Manager API	**cloudresourcemanager.googleapis.com**
Google DNS API	**dns.googleapis.com**
ネットワークセキュリティー API	**networksecurity.googleapis.com**
IAM Service Account Credentials API	**iamcredentials.googleapis.com**

API サービス	コンソールサービス名
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**
Cloud Storage	**storage-component.googleapis.com**

3. Red Hat が必要なアクションを実行できるようにするには、GCP プロジェクトに **osd-ccs-admin** IAM サービスアカウント ユーザーを作成する必要があります。
以下のロールを サービスアカウントに付与する 必要があります。

表2.2 必要なロール

ロール	コンソールロール名
Compute 管理者	**roles/compute.admin**
DNS 管理者	**roles/dns.admin**
組織ポリシービューアー	**roles/orgpolicy.policyViewer**
Owner	**roles/owner**
プロジェクト IAM 管理者	**roles/resourcemanager.projectIamAdmin**
サービス管理管理者	**roles/servicemanagement.admin**
サービス使用状況の管理	**roles/serviceusage.serviceUsageAdmin**
ストレージ管理者	**roles/storage.admin**

4. **osd-ccs-admin** IAM サービスアカウントの サービスアカウントキー を作成します。キーは **osServiceAccount.json** という名前のファイルにエクスポートします。この JSON ファイルは、クラスターの作成時に Red Hat OpenShift Cluster Manager にアップロードされます。

2.4. RED HAT 管理 GOOGLE CLOUD リソース

Red Hat は、以下の IAM Google Cloud Platform (GCP) リソースを作成し、管理します。

2.4.1. IAM サービスアカウントおよびロール

osd-managed-admin IAM サービスアカウントは、お客様が指定する GCP アカウントを制御した直後に作成されます。これは、OpenShift Dedicated クラスターのインストールを実行するユーザーです。

以下のロールがサービスアカウントに割り当てられます。

表2.3 osd-managed-admin の IAM ロール

ロール	コンソールロール名	説明
Compute 管理者	**roles/compute.admin**	すべての Compute Engine リソースを完全に制御します。
DNS 管理者	**roles/dns.admin**	すべての Cloud DNS リソースに読み取り/書き込みアクセスを提供します。
セキュリティー管理者	**roles/iam.securityAdmin**	IAM ポリシーを取得し、設定するためのパーミッションを持つセキュリティー管理者ロール。
ストレージ管理者	**roles/storage.admin**	オブジェクトおよびバケットを完全に制御します。 個別の **バケット** に適用される場合、制御はバケット内の指定されたバケットおよびオブジェクトにのみ適用されます。
サービスアカウント管理者	**roles/iam.serviceAccountAdmin**	サービスアカウントを作成および管理します。
サービスアカウントキー管理者	**roles/iam.serviceAccountKeyAdmin**	サービスアカウントキーを作成して管理 (ローテーション) します。
サービスアカウントユーザー	**roles/iam.serviceAccountUser**	サービスアカウントとして操作を実行します。

2.4.2. IAM グループおよびロール

sd-sre-platform-gcp-access Google グループに、緊急トラブルシューティングの目的で Red Hat のサイト信頼性エンジニアリング (SRE) のコンソールへのアクセスが許可されるため、GCP プロジェクトへのアクセスが付与されます。

以下のロールがグループに割り当てられます。

表2.4 sd-sre-platform-gcp-access の IAM ロール

ロール	コンソールロール名	説明
Compute 管理者	**roles/compute.admin**	すべての Compute Engine リソースを完全に制御します。
エディター	**roles/editor**	すべてのビューアーパーミッション、および状態を変更するアクションのパーミッションを提供します。
組織ポリシービューアー	**roles/orgpolicy.policyViewer**	リソースに対する組織ポリシーの表示アクセスを提供します。
プロジェクト IAM 管理者	**roles/resourcemanager.projectIamAdmin**	プロジェクトの IAM ポリシーを管理するためのパーミッションを提供します。
クォータ管理者	**roles/servicemanagement.quotaAdmin**	サービスクォータを管理するアクセスを提供します。
ロール管理者	**roles/iam.roleAdmin**	プロジェクトのすべてのカスタムロールへのアクセスを提供します。
サービスアカウント管理者	**roles/iam.serviceAccountAdmin**	サービスアカウントを作成および管理します。
サービス使用状況の管理	**roles/serviceusage.serviceUsageAdmin**	サービス状態の有効化、無効化、および検査を行い、操作を検査し、コンシューマープロジェクトのクォータおよび請求書を使用する機能。
テクニカルサポートエディター	**roles/cloudsupport.techSupportEditor**	テクニカルサポートケースへの完全読み取り/書き込みアクセスを提供します。

2.5. GCP アカウントの制限

OpenShift Dedicated クラスターは多くの Google Cloud Platform (GCP) コンポーネントを使用しますが、デフォルトの クォータ は、OpenShift Dedicated クラスターのインストール機能に影響を与えません。

標準の OpenShift Dedicated クラスターは以下のリソースを使用します。一部のリソースはブートストラッププロセス時にのみ必要となり、クラスターのデプロイ後に削除されることに注意してください。

表2.5 デフォルトのクラスターで使用される GCP リソース

サービス	コンポーネント	場所	必要なリソースの合計	ブートストラップ後に削除されるリソース
サービスアカウント	IAM	グローバル	5	0
ファイアウォールのルール	コンピュート	グローバル	11	1
転送ルール	コンピュート	グローバル	2	0
使用中のグローバル IP アドレス	コンピュート	グローバル	4	1
ヘルスチェック	コンピュート	グローバル	3	0
イメージ	コンピュート	グローバル	1	0
ネットワーク	コンピュート	グローバル	2	0
静的 IP アドレス	コンピュート	リージョン	4	1
ルーター	コンピュート	グローバル	1	0
ルート	コンピュート	グローバル	2	0
サブネットワーク	コンピュート	グローバル	2	0
ターゲットプール	コンピュート	グローバル	3	0
CPU	コンピュート	リージョン	28	4
永続ディスク SSD (GB)	コンピュート	リージョン	896	128

注記

インストール時にクォータが十分ではない場合、インストールプログラムは超過したクォータとリージョンの両方を示すエラーを表示します。

実際のクラスターサイズ、計画されるクラスターの拡張、およびアカウントに関連付けられた他のクラスターからの使用法を考慮してください。CPU、静的 IP アドレス、および永続ディスク SSD (ストレージ) のクォータは、ほとんどの場合に不十分になる可能性のあるものです。

以下のリージョンのいずれかにクラスターをデプロイする予定の場合、ストレージクォータの最大値を超え、CPU クォータ制限を超える可能性が高くなります。

- asia-east2

- asia-northeast2
- asia-south1
- australia-southeast1
- europe-north1
- europe-west2
- europe-west3
- europe-west6
- northamerica-northeast1
- southamerica-east1
- us-west2

GCP コンソール からリソースクォータを増やすことは可能ですが、サポートチケットを作成する必要がある場合があります。OpenShift Dedicated クラスターをインストールする前にサポートチケットを解決できるように、クラスターのサイズを早期に計画してください。