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: 2024-10-15

OpenShift Dedicated 4 環境のプランニング

Dedicated 4 のプランニングの概要

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 制限およびスケーラビリティー

このドキュメントでは、OpenShift Dedicated クラスターでテストされたクラスターの最大値について、最大値のテストに使用されたテスト環境と設定に関する情報とともに詳しく説明します。コントロールプレーンとインフラストラクチャーノードのサイズ設定とスケーリングに関する情報も提供されます。

1.1. クラスターの最大数

OpenShift Dedicated クラスターのインストールを計画するときは、以下のテスト済みオブジェクトの最大値を考慮してください。この表は、OpenShift Dedicated クラスターでテストされた各タイプの最大制限を示しています。

これらのガイドラインは、複数のアベイラビリティーゾーン設定のコンピューティング (ワーカーとも呼ばれる) ノード 180 個のクラスターに基づいています。小規模なクラスターの場合、最大値はこれより低くなります。

表1.1 テスト済みのクラスターの最大値

最大値のタイプ	4.x テスト済みの最大値
Pod 数 [1]	25,000
ノードあたりの Pod 数	250
コアあたりの Pod 数	デフォルト値はありません。
namespace 数 [2]	5,000
namespace あたりの Pod 数 [3]	25,000
サービス数 [4]	10,000
namespace ごとのサービス数	5,000
サービスごとのバックエンド数	5,000
namespace ごとのデプロイメント数 [3]	2,000

1. ここで表示される Pod 数はテスト用の Pod 数です。実際の Pod 数は、アプリケーションのメモリー、CPU、およびストレージ要件により異なります。

2. 有効なプロジェクトが多数ある場合は、キースペースが過度に大きくなり、スペースのクォータを超過すると、etcd はパフォーマンスの低下による影響を受ける可能性があります。etcd ストレージを利用できるようにするには、デフラグを含む etcd の定期的なメンテナンスを行うことが強く推奨されます。

3. システムには、状態遷移への対応として、指定された namespace 内のすべてのオブジェクトに対して反復処理する必要がある制御ループがいくつかあります。単一の namespace にタイプのオブジェクトの数が多くなると、ループのコストが上昇し、状態変更を処理する速度が低下し

ます。この制限については、アプリケーションの各種要件を満たすのに十分な CPU、メモリー、およびディスクがシステムにあることが前提となっています。

4. 各サービスポートと各サービスのバックエンドには、**iptables** に対応するエントリーがあります。特定のサービスのバックエンド数は、エンドポイントのオブジェクトサイズに影響があり、その結果、システム全体に送信されるデータサイズにも影響を与えます。

1.2. OPENSHIFT CONTAINER PLATFORM テスト環境および設定

以下の表は、AWS クラウドプラットフォームについてクラスターの最大値をテストする OpenShift Container Platform 環境および設定をリスト表示しています。

Node	タイプ	仮想 CPU	RAM(GiB)	ディスクタイプ	ディスクサイズ(GiB)/IOPS	数	リージョン
コントロールプレーン/etcd [1]	m5.4xlarge	16	64	gp3	350 / 1,000	3	us-west-2
インフラストラクチャーノード [2]	r5.2xlarge	8	64	gp3	300 / 900	3	us-west-2
ワークロード [3]	m5.2xlarge	8	32	gp3	350 / 900	3	us-west-2
Compute nodes	m5.2xlarge	8	32	gp3	350 / 900	102	us-west-2

1. io1 ディスクは、4.10 より前のすべてのバージョンでコントロールプレーン/etcd ノードに使用されます。

2. Prometheus は使用状況パターンに応じて大量のメモリーを要求できるため、インフラストラクチャーノードはモニタリングコンポーネントをホストするために使用されます。

3. ワークロードノードは、パフォーマンスとスケーラビリティーのワークロードジェネレーターを実行するための専用ノードです。

より大きなクラスターサイズとより多くのオブジェクト数に到達できる可能性があります。ただし、インフラストラクチャーノードのサイズによって、Prometheus で利用できるメモリー量が制限されます。オブジェクトの作成、変更、または削除時に、Prometheus はメトリックをそのメモリーに保存してから、ディスクでメトリックを永続化する前に 3 時間保存されます。オブジェクトの作成、変更、削除のレートが高すぎると、Prometheus はメモリーリソースがないために負荷がかかり、失敗する可能性があります。

1.3. コントロールプレーンとインフラストラクチャーノードのサイズ設定とスケーリング

OpenShift Dedicated クラスターをインストールすると、コントロールプレーンとインフラストラクチャーノードのサイズは、コンピュートノードの数によって自動的に決定されます。

インストール後にクラスター内のコンピュートノードの数を変更した場合、Red Hat サイトリライアビリティーエンジニアリング (SRE) チームは、クラスターの安定性を維持するために、必要に応じてコントロールプレーンとインフラストラクチャーノードをスケーリングします。

1.3.1. インストール中のノードのサイズ設定

インストールプロセス中に、コントロールプレーンとインフラストラクチャーノードのサイズが動的に計算されます。サイズ計算は、クラスター内のコンピュートノードの数に基づいています。

次の表に、インストール中に適用されるコントロールプレーンとインフラストラクチャーノードのサイズを示します。

AWS コントロールプレーンとインフラストラクチャーノードのサイズ：

コンピュートノードの数	コントロールプレーンのサイズ	インフラストラクチャーノードのサイズ
1 から 25	m5.2xlarge	r5.xlarge
26 から 100	m5.4xlarge	r5.2xlarge
101 から 180	m5.8xlarge	r5.4xlarge

GCP コントロールプレーンとインフラストラクチャーノードのサイズ

コンピュートノードの数	コントロールプレーンのサイズ	インフラストラクチャーノードのサイズ
1 から 25	custom-8-32768	custom-4-32768-ext
26 から 100	custom-16-65536	custom-8-65536-ext
101 から 180	custom-32-131072	custom-16-131072-ext

2024 年 6 月 21 日以降に作成されたクラスターの GCP 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サイズ：

コンピュートノードの数	コントロールプレーンのサイズ	インフラストラクチャーノードのサイズ
1 から 25	n2-standard-8	n2-highmem-4
26 から 100	n2-standard-16	n2-highmem-8
101 から 180	n2-standard-32	n2-highmem-16

注記

OpenShift Dedicated のコンピュートノードの最大数は 180 です。

1.3.2. インストール後のノードのスケーリング

インストール後にコンピュートノードの数を変更した場合、コントロールプレーンとインフラストラクチャーノードは、必要に応じて Red Hat Site Reliability Engineer (SRE) チームによってスケーリングされます。ノードは、プラットフォームの安定性を維持するためにスケーリングされます。

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のインストール後のスケーリング要件は、ケースごとに評価されます。ノードリソースの消費および受信アラートの考慮が行われます。

コントロールプレーンノードのサイズ変更のアラートのルール

サイズ変更アラートは、次の状況が発生した場合に、クラスター内のコントロールプレーンノードに対してトリガーされます。

- クラスターでコントロールプレーンノードが平均 66% を超える使用率を維持している。

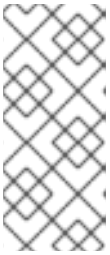
注記

OpenShift Dedicated のコンピュートノードの最大数は 180 です。

インフラストラクチャーノードのサイズ変更アラートのルール

CPU またはメモリーの使用率が継続して高い場合、クラスター内のインフラストラクチャーノードに対してサイズ変更アラートがトリガーされます。このように継続して使用率が高い状態が続いているのは、以下の場合です。

- 2 つのインフラストラクチャーノードを使用する 1 つのアベイラビリティーゾーンを持つクラスターで、インフラストラクチャーノードが平均 50% を超える使用率を維持している。
- 3 つのインフラストラクチャーノードを使用する複数のアベイラビリティーゾーンを持つクラスターで、インフラストラクチャーノードが平均 66% を超える使用率を維持している。



注記

OpenShift Dedicated のコンピュートノードの最大数は 180 です。

サイズ変更アラートは、使用率が高い状態が継続した場合にのみ表示されます。ノードが一時的にダウンして他のノードがスケールアップするなど、短期間に使用量が急増した場合には、これらのアラートはトリガーされません。

SRE チームは、ノードでのリソース消費の増加を管理するなど、追加の理由でコントロールプレーンとインフラストラクチャーノードをスケーリングする場合があります。

1.3.3. 大規模なクラスターのサイズに関する考慮事項

大規模なクラスターの場合、インフラストラクチャーノードのサイズ設定はスケーラビリティーに大きな影響を与える要因になる可能性があります。指定のしきい値に影響を与える要因には、etcd バージョンやストレージデータ形式などの多数の要因があります。

これらの制限を超えても、クラスターが障害が発生するとは限りません。ほとんど場合、これらの制限値を超えると、パフォーマンスが全体的に低下します。

第2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。

2.1. 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 のサイトリライアビリティーエンジニアリング (SRE) には、AWS Organization 内の SCP に対する制御がありません。

2.2. 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。

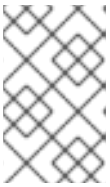
2.2.1. Account

- 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 にリスト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 の使用に関する制限を課すことができない場合があります。制限を課すことにより、Red Hat のインシデントへの対応が大幅に妨げられます。
- Red Hat は AWS にモニタ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。
- お客様が提供した同じ AWS アカウント内でネイティブ AWS サービスをデプロイできます。

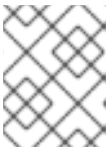


注記

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、これは必須ではありません。

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 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、顧客が提供した AWS アカウントへの AWS コンソールアクセス権が必要です。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 で利用可能なアクションは、お客様によって提供される AWS アカウントで直接実行することはできません。

2.2.3. 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、AWS サポートを代行してリクエストする権限をお客様から受けます。
- Red Hat は、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お客様から受けます。
- 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 AWS アカウントに固有のもので、お客様が指定する AWS アカウントには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。

2.3. 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 で **アクセスキー ID** および **シークレットアクセスキー** を指定する必要があります。

2.4. 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
	Amazon CloudWatch	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 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:*"
```

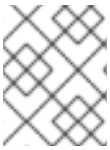
```
        ],
        "Resource": [
            "*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "logs:*"
        ],
        "Resource": [
            "*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "support:*"
        ],
        "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": [
            "*"
        ]
    }
  ]
}
```

2.5. 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。

2.5.1. 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": "*"
        }
    ]
}
```

2.5.2. 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。

2.5.3. 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。**network-mgmt** ロールは、Customer Cloud Subscription (CCS) 以外のクラスターにのみ適用されます。以下のポリシーはロールに割り当てられます。
    - AmazonEC2ReadOnlyAccess
    - CustomerAdministratorAccess
- **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

2.6. 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リストは、OpenShift Container Platform ドキュメント を参照してください。

2.6.1. 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)
- 複数の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)
    - 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)

2.6.2. 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:

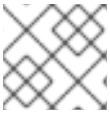
- コントロールプレーンボリューム
  - サイズ: 350 GB
  - タイプ: io1
  - 1 秒あたりの入出力操作: 1000
- インフラストラクチャーボリューム
  - サイズ: 300 GB
  - タイプ: gp2
  - 1 秒あたりの I/O 処理数: 900
- ワーカーボリューム
  - サイズ: 300 GB
  - タイプ: gp2
  - 1 秒あたりの I/O 処理数: 900

2.6.3. Elastic Load Balancing (ELB) ロードバランサー

API 用に最大 2 つのネットワークロードバランサー、アプリケーションルーター用に最大 2 つのクラシックロードバランサー。詳細は、AWS に関する ELB ドキュメント を参照してください。

2.6.4. 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。

2.6.5. 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。

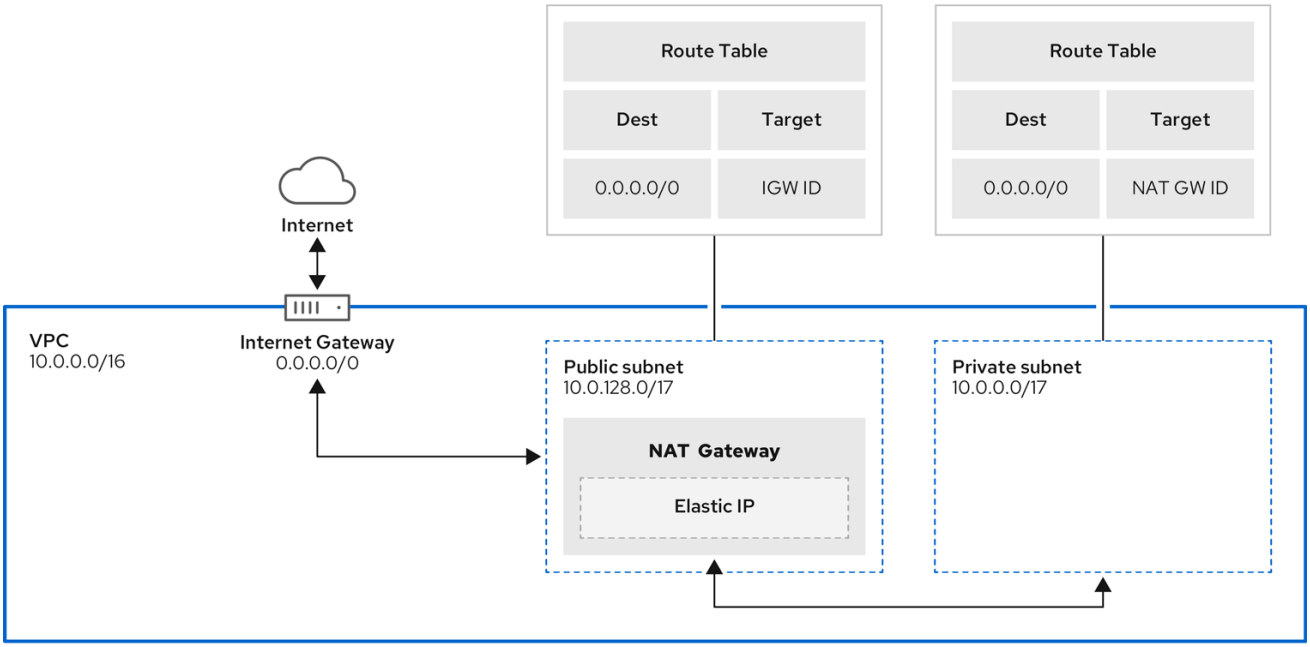
- **サブネット**: 単一アベイラビリティーゾーンがあるクラスターの 2 つのサブネット、または複数のアベイラビリティーゾーンがあるクラスターの 6 つのサブネット。

注記

パブリックサブネット は、インターネットゲートウェイを介してインターネットに直接接続します。**プライベートサブネット** は、ネットワークアドレス変換 (NAT) ゲートウェイを介してインターネットに接続します。

- **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。

2.6.5.1. サンプル VPC アーキテクチャー



2.6.6. 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。

2.6.6.1. 追加のカスタムセキュリティーグループ

非マネージド VPC を使用してクラスターを作成する場合は、クラスターの作成中にカスタムセキュリティーグループを追加できます。カスタムセキュリティーグループには次の制限があります。

- クラスターを作成する前に、AWS でカスタムセキュリティーグループを作成する必要があります。詳細は、Amazon EC2 security groups for Linux instances を参照してください。
- カスタムセキュリティーグループを、クラスターのインストール先の VPC に関連付ける必要があります。カスタムセキュリティーグループを別の VPC に関連付けることはできません。

- カスタムセキュリティーグループを追加する場合は、VPC の追加クォータをリクエストする必要がある場合があります。AWS クォータ引き上げのリクエストについては、Requesting a quota increase を参照してください。

2.7. AWS ファイアウォールの前提条件

ファイアウォールを使用して OpenShift Dedicated からの Egress トラフィックを制御している場合は、以下の特定のドメインとポートの組み合わせへのアクセスを許可するようにファイアウォールを設定する必要があります。OpenShift Dedicated がフルマネージドの OpenShift サービスを提供するには、このアクセスが必要です。

前提条件

- AWS Virtual Private Cloud (VPC) に Amazon S3 ゲートウェイエンドポイントを設定した。このエンドポイントは、クラスターから Amazon S3 サービスへのリクエストを完了するために必要です。

手順

1. パッケージとツールのインストールおよびダウンロードに使用される以下の URL を許可リストに指定します。

ドメイン	ポート	機能
registry.redhat.io	443	コアコンテナーイメージを指定します。
quay.io	443	コアコンテナーイメージを指定します。
cdn01.quay.io	443	コアコンテナーイメージを指定します。
cdn02.quay.io	443	コアコンテナーイメージを指定します。
cdn03.quay.io	443	コアコンテナーイメージを指定します。
sso.redhat.com	443	必須。**https://console.redhat.com/openshift** サイトでは、**sso.redhat.com** からの認証を使用してプルシークレットをダウンロードし、Red Hat SaaS ソリューションを使用してサブスクリプション、クラスターインベントリー、チャージバックレポートなどのモニタリングを行います。
quay-registry.s3.amazonaws.com	443	コアコンテナーイメージを指定します。
quayio-production-s3.s3.amazonaws.com	443	コアコンテナーイメージを指定します。
openshift.org	443	Red Hat Enterprise Linux CoreOS (RHCOS) イメージを提供します。

ドメイン	ポート	機能
registry.access.redhat.com	443	Red Hat Ecosytem Catalog に保存されているすべてのコンテナーイメージをホストします。さらに、レジストリーは、開発者が OpenShift および Kubernetes 上で構築するのに役立つ **odo** CLI ツールへのアクセスを提供します。
access.redhat.com	443	必須。コンテナークライアントが **registry.access.redhat.com** からイメージを取得するときにイメージを検証するために必要な署名ストアをホストします。
registry.connect.redhat.com	443	すべてのサードパーティーのイメージと認定 Operator に必要です。
console.redhat.com	443	必須。クラスターと OpenShift Console Manager との間の対話が、スケジューリングアップグレードなどの機能を有効にすることを許可します。
sso.redhat.com	443	**https://console.redhat.com/openshift** サイトは、**sso.redhat.com** からの認証を使用します。
pull.q1w2.quay.rhcloud.com	443	quay.io が利用できない場合のフォールバックとして、コアコンテナーイメージを提供します。
.q1w2.quay.rhcloud.com	443	quay.io が利用できない場合のフォールバックとして、コアコンテナーイメージを提供します。
www.okd.io	443	**openshift.org** サイトは **www.okd.io** にリダイレクトされます。
www.redhat.com	443	**sso.redhat.com** サイトは **www.redhat.com** にリダイレクトされます。
aws.amazon.com	443	**iam.amazonaws.com** および **sts.amazonaws.com** サイトは **aws.amazon.com** にリダイレクトされます。

ドメイン	ポート	機能
catalog.redhat.com	443	**registry.access.redhat.com** および **https://registry.redhat.io** サイトは **catalog.redhat.com** にリダイレクトされます。
dvbwgdztaeq9o.cloudfront.net [1]	443	マネージド OIDC 設定を使用した STS 実装で、ROSA が使用します。

1. リソースのリダイレクトが必要な大規模なクラウドフロントの停止が発生した場合、**cloudfront.net** の前の英数字の文字列が変更される可能性があります。

2. 次のテレメトリー URL を許可リストします。

ドメイン	ポート	機能
cert-api.access.redhat.com	443	テレメトリーで必要です。
api.access.redhat.com	443	テレメトリーで必要です。
infogw.api.openshift.com	443	テレメトリーで必要です。
console.redhat.com	443	Telemetry と Red Hat Insights で必要です。
cloud.redhat.com/api/ingress	443	Telemetry と Red Hat Insights で必要です。
observatorium-mst.api.openshift.com	443	マネージド OpenShift 固有のテレメトリーに使用されます。
observatorium.api.openshift.com	443	マネージド OpenShift 固有のテレメトリーに使用されます。

マネージドクラスターでは、テレメトリーを有効にして、Red Hat が問題に迅速に対応し、顧客をより適切にサポートし、製品のアップグレードがクラスターに与える影響をよりよく理解できるようにする必要があります。Red Hat によるリモートヘルスモニタリングデータの使用方法の詳細は **関連情報** セクションの **リモートヘルスモニタリングについて** を参照してください。

3. 次の Amazon Web Services (AWS) API URI を許可リストします。

ドメイン	ポート	機能
.amazonaws.com	443	AWS サービスおよびリソースへのアクセスに必要です。

または、Amazon Web Services (AWS) API にワイルドカードを使用しない場合は、次の URL を許可リストに追加する必要があります。

ドメイン	ポート	機能
ec2.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
events.<aws_region>.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
iam.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
route53.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
sts.amazonaws.com	443	AWS STS のグローバルエンドポイントを使用するように設定されたクラスターの場合は、AWS 環境にクラスターをインストールおよび管理するために使用されます。
sts.<aws_region>.amazonaws.com	443	AWS STS の地域化されたエンドポイントを使用するように設定されたクラスターの場合は、AWS 環境にクラスターをインストールおよび管理するために使用されます。詳細は、AWS STS の地域化されたエンドポイント を参照してください。
tagging.us-east-1.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。このエンドポイントは、クラスターがデプロイメントされているリージョンに関係なく、常に us-east-1 です。
ec2.<aws_region>.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
elasticloadbalancing.<aws_region>.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
servicequotas.<aws_region>.amazonaws.com	443	必須。サービスをデプロイするためのクォータを確認するのに使用されます。
tagging.<aws_region>.amazonaws.com	443	タグの形式で AWS リソースに関するメタデータを割り当てることができます。

4. 以下の OpenShift URL を許可リストします。

ドメイン	ポート	機能
mirror.openshift.com	443	ミラーリングされたインストールのコンテンツおよびイメージへのアクセスに使用されます。Cluster Version Operator (CVO) には単一の機能ソースのみが必要ですが、このサイトはリリースイメージ署名のソースでもあります。
storage.googleapis.com/openshift-release (推奨)	443	mirror.openshift.com/ の代替サイト。quay.io からプルするイメージを把握するのにクラスターが使用するプラットフォームリリース署名をダウンロードするのに使用されます。
api.openshift.com	443	クラスターに更新が利用可能かどうかを確認するのに使用されます。

5. 次のサイトリライアビリティーエンジニアリング (SRE) および管理 URL を許可リストします。

ドメイン	ポート	機能
api.pagerduty.com	443	このアラートサービスは、クラスター内の alertmanager が使用します。これにより、Red Hat SRE に対してイベントの SRE 通知に関するアラートが送信されます。
events.pagerduty.com	443	このアラートサービスは、クラスター内の alertmanager が使用します。これにより、Red Hat SRE に対してイベントの SRE 通知に関するアラートが送信されます。
api.deadmanssnitch.com	443	クラスターが利用可能かどうかを示す定期的な ping を送信して、OpenShift Dedicated が使用するアラートサービス。
nosnch.in	443	クラスターが利用可能かどうかを示す定期的な ping を送信して、OpenShift Dedicated が使用するアラートサービス。

ドメイン	ポート	機能
.osdsecuritylogs.splunkcloud.com または **inputs1.osdsecuritylogs.splunkcloud.cominputs2.osdsecuritylogs.splunkcloud.cominputs4.osdsecuritylogs.splunkcloud.cominputs5.osdsecuritylogs.splunkcloud.cominputs6.osdsecuritylogs.splunkcloud.cominputs7.osdsecuritylogs.splunkcloud.cominputs8.osdsecuritylogs.splunkcloud.cominputs9.osdsecuritylogs.splunkcloud.cominputs10.osdsecuritylogs.splunkcloud.cominputs11.osdsecuritylogs.splunkcloud.cominputs12.osdsecuritylogs.splunkcloud.cominputs13.osdsecuritylogs.splunkcloud.cominputs14.osdsecuritylogs.splunkcloud.cominputs15.osdsecuritylogs.splunkcloud.com**	9997	**splunk-forwarder-operator** によって使用され、ログベースのアラートについて Red Hat SRE が使用するロギング転送エンドポイントとして使用されます。
http-inputs-osdsecuritylogs.splunkcloud.com	443	必須。**splunk-forwarder-operator** によって使用され、ログベースのアラートについて Red Hat SRE が使用するロギング転送エンドポイントとして使用されます。
sftp.access.redhat.com (推奨)	22	**must-gather-operator** が、クラスターに関する問題のトラブルシューティングに役立つ診断ログをアップロードするのに使用される SFTP サーバー。

6. オプションのサードパーティーコンテンツに対する次の URL を許可リストに追加します。

Domain	ポート	機能
registry.connect.redhat.com	443	すべてのサードパーティーのイメージと認定 Operator に必要です。
rhc4tp-prod-z8cxf-image-registry-us-east-1-evenkyleffocxqvofrk.s3.dualstack.us-east-1.amazonaws.com	443	**registry.connect.redhat.com** でホストされているコンテナーイメージにアクセスできます
oso-rhc4tp-docker-registry.s3-us-west-2.amazonaws.com	443	Sonatype Nexus、F5 Big IP Operator に必要です。

7. ビルドに必要な言語またはフレームワークのリソースを提供するサイトを許可リストに指定します。

8. OpenShift で使用される言語およびフレームワークに依存するアウトバウンド URL を許可リストに指定します。ファイアウォールまたはプロキシーで許可できる推奨 URL のリストは、OpenShift Outbound URLs to Allow を参照してください。

関連情報

- リモートヘルスモニタリングについて

2.8. 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、アカウントを使用し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
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)	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 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。 クラスターの使用量やデプロイされたワークロード別に作成された追加のマシンやロードバランサーに対して、追加の ENI が作成されます。
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。
Security Groups	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3章 GCP での CUSTOMER CLOUD SUBSCRIPTION

OpenShift Dedicated は、Red Hat が顧客の既存の Google Cloud Platform (GCP) アカウントにクラスターを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。

3.1. 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。

3.2. 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。

3.2.1. Account

- 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。制限を課すことにより、Red Hat のインシデントへの対応が大幅に妨げられます。
- Red Hat は、モニタリングを 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、これは必須ではありません。

3.2.2. 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 で利用可能なアクションは、お客様が指定する GCP アカウントで直接実行することはできません。

3.2.3. サポート要件

- Red Hat では、お客様が少なくとも GCP の 拡張サポート を受け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 GCP 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。

3.2.4. 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 は、許可リスト IP アドレスを介して API サーバーに Ingress アクエスできるようにする必要があります。

注記

許可リスト IP アドレスの詳細は、関連情報を参照してください。

- 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。

3.3. 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** (このポリシー制約は、Red Hat の **DIRECTORY_CUSTOMER_ID C02k0l5e8** が許可リストに含まれている場合にのみサポートされます。このポリシー制約は注意して使用してください。
- **constraints/compute.restrictLoadBalancerCreationForTypes**
- **constraints/compute.requireShieldedVm** (このポリシー制約は、最初のクラスター作成時に "Enable Secure Boot support for Shielded VMs" を選択してクラスターがインストールされている場合にのみサポートされます)。
- **constraints/compute.vmExternalIpAccess** (このポリシー制約はインストール後にのみサポートされます)。

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。
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3.1 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**
Identity and Access Management (IAM) API	**iam.googleapis.com**
Service Management API	**servicemanagement.googleapis.com**

API サービス	コンソールサービス名
Service Usage API	**serviceusage.googleapis.com**
Google Cloud Storage JSON API	**storage-api.googleapis.com**
Cloud Storage	**storage-component.googleapis.com**
Organization Policy API	**orgpolicy.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3.2 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**
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**
ロードバランサー計算の管理者	**roles/compute.loadBalancerAdmin**
ロール閲覧者	**roles/viewer**
ロール管理者	**roles/iam.roleAdmin**
セキュリティー管理者	**roles/iam.securityAdmin**
Service Account Key Admin	**roles/iam.serviceAccountKeyAdmin**
サービスアカウント管理者	**roles/iam.serviceAccountAdmin**
Service Account User	**roles/iam.serviceAccountUser**

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。

3.4. 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。

3.4.1. 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3.3 osd-managed-admin の IAM ロール

ロール	コンソールロール名	説明
Compute Admin	**roles/compute.admin**	すべての Compute Engine リソースを完全に制御します。
DNS Administrator	**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。
Security Admin	**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。
Storage Admin	**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。
Service Account Admin	**roles/iam.serviceAccountAdmin**	サービスアカウントを作成および管理します。
Service Account Key Admin	**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。
Service Account User	**roles/iam.serviceAccountUser**	サービスアカウントとして操作を実行します。
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。

3.4.2. 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 のサイトリライアビリティーエンジニアリング (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3.4 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 Admin	**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。
Service Account Admin	**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。

3.5. プロビジョニングされる GCP インフラストラクチャー

以下は、デプロイされた OpenShift Dedicated クラスターでプロビジョニングされる Google Cloud Platform (GCP) コンポーネントの概要です。プロビジョニングされるすべての GCP 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。

3.5.1. コンピュートインスタンス

GCP インスタンスは、GCP 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
  - 2 つのインフラノード (カスタムマシンタイプ: 4 つの vCPU と 32 GB の RAM)
  - 3 つのコントロールプレーンノード (カスタムマシンタイプ: 8 つの vCPU と 32 GB の RAM)
  - 2 つのワーカーノード (カスタムマシンタイプ: 4 つの vCPU と 16 GB の RAM)
- 複数のアベイラビリティーゾーン
  - 3 つのインフラノード (カスタムマシンタイプ: 4 つの vCPU と 32 GB の RAM)
  - 3 つのコントロールプレーンノード (カスタムマシンタイプ: 8 つの vCPU と 32 GB の RAM)
  - 3 つのワーカーノード (カスタムマシンタイプ: 4 つの vCPU と 16 GB の RAM)

3.5.2. ストレージ

- インフラストラクチャーのボリューム:
  - 300 GB SSD 永続ディスク (インスタンスの削除時に削除)
  - 110 GB の標準永続ディスク (インスタンスの削除時に保持)
- ワーカーのボリューム:
  - 300 GB SSD 永続ディスク (インスタンスの削除時に削除)
- コントロールプレーンのボリューム:
  - 350 GB SSD 永続ディスク (インスタンスの削除時に削除)

3.5.3. VPC

- **サブネット**: コントロールプレーンワークロード用の 1 つのマスターサブネットと、その他すべてのワークロード用の 1 つのワーカーサブネット。
- **ルーターテーブル**: VPC ごとに 1 つのグローバルルートテーブル。
- **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**: クラスターごとに 1 つのマスター NAT ゲートウェイと 1 つのワーカー NAT ゲートウェイ。

3.5.4. サービス

GCP CCS クラスターで次のサービスを有効にする必要があります。

- **deploymentmanager**
- **compute**
- **cloudapis**
- **cloudresourcemanager**
- **dns**
- **iamcredentials**
- **iam**
- **servicemanagement**
- **serviceusage**
- **storage-api**
- **storage-component**
- **orgpolicy**
- **networksecurity**

3.6. 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3.5 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	Compute	グローバル	11	1
転送ルール	Compute	グローバル	2	0
使用中のグローバル IP アドレス	Compute	グローバル	4	1

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
ヘルスチェック	Compute	グローバル	3	0
イメージ	Compute	グローバル	1	0
ネットワーク	Compute	グローバル	2	0
静的 IP アドレス	Compute	リージョン	4	1
ルーター	Compute	グローバル	1	0
ルート	Compute	グローバル	2	0
サブネットワーク	Compute	グローバル	2	0
ターゲットプール	Compute	グローバル	3	0
CPU	Compute	リージョン	28	4
永続ディスク SSD (GB)	Compute	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。

3.7. 関連情報

- SRE アクセスに必要な許可リスト IP アドレス