OpenShift Dedicated 4

환경 계획

Dedicated 4의 계획 개요

Last Updated: 2024-09-19

OpenShift Dedicated 4 환경 계획

Dedicated 4의 계획 개요

법적 공지

초록

이 문서에서는 OpenShift Dedicated 클러스터 배포에 대한 계획 고려 사항을 설명합니다.

차례

1장. 제한 및 확장성

이 문서에서는 OpenShift Dedicated 클러스터의 테스트된 클러스터 최대값과 최대값을 테스트하는 데 사용되는 테스트 환경 및 구성에 대한 정보를 자세히 설명합니다. 컨트롤 플레인 및 인프라 노드 크기 조정 및 스케일링에 대한 정보도 제공됩니다.

1.1. ROSA 테스트된 클러스터 최대값

OpenShift Dedicated 클러스터 설치를 계획할 때 다음과 같은 테스트된 오브젝트 최대값을 고려하십시오. 테이블은 OpenShift Dedicated 클러스터에서 테스트된 각 유형에 대한 최대 제한을 지정합니다.

이러한 지침은 다중 가용성 영역 구성의 102 컴퓨팅 노드 (작업자라고도 함)의 클러스터를 기반으로 합니다. 크기가 작은 클러스터의 경우 최대값이 더 낮습니다.

참고

모든 테스트에 사용되는 OpenShift Container Platform 버전은 OCP 4.8.0입니다.

표 1.1. 테스트된 클러스터 최대값

최대값 유형	4.8 테스트된 최대값
노드 수	102
Pod 수 [1]	20,400
노드당 Pod 수	250
코어당 Pod 수	기본값이 없습니다.
네임스페이스 수 [2]	3,400
네임스페이스당 Pod 수 [3]	20,400
서비스 수 [4]	10,000
네임스페이스당 서비스 수	10,000
서비스당 백엔드 수	10,000
네임스페이스당 배포 수 [3]	1,000

1. 여기에 표시된 Pod 수는 테스트 Pod 수입니다. 실제 Pod 수는 애플리케이션 메모리, CPU 및 스토리지 요구사항에 따라 달라집니다.

2. 활성 프로젝트 수가 많은 경우 키 공간이 지나치게 커져서 공간 할당량을 초과하면 etcd 성능이 저하될 수 있습니다. etcd 스토리지를 사용할 수 있도록 조각 모음을 포함하여 etcd를 정기적으로 유지보수하는 것이 좋습니다.

3. 시스템에는 일부 상태 변경에 대한 대응으로 지정된 네임스페이스의 모든 오브젝트에서 반복해야 하는 컨트롤 루프가 많습니다. 단일 네임스페이스에 형식의 오브젝트가 많으면 루프 비용이 많이 들고 상태 변경 처리 속도가 느려질 수 있습니다. 이 제한을 적용하면 애플리케이션 요구사항을 충족하기에 충분한 CPU, 메모리 및 디스크가 시스템에 있다고 가정합니다.

4. 각 서비스 포트와 각 서비스 백엔드는 iptables에 해당 항목이 있습니다. 지정된 서비스의 백엔드 수는 끝점 오브젝트의 크기에 영향을 미치므로 시스템 전체에서 전송되는 데이터의 크기에 영향을 미칩니다.

OpenShift Container Platform 4.8에서는 CPU 코어의 절반(500밀리코어)이 이전 버전의 OpenShift Container Platform과 비교하여 시스템에 의해 예약되어 있습니다.

1.2. OPENSHIFT CONTAINER PLATFORM 테스트 환경 및 구성

다음 표에는 AWS 클라우드 플랫폼에서 클러스터 최대값을 테스트하는 OpenShift Container Platform 환경 및 구성이 나열되어 있습니다.

노드	유형	vCPU	RAM(GiB)	디스크 유형	디스크 크기(GiB)/IOPS	수량	리전
컨트롤 플레인/etcd [1]	m5.4xlarge	16	64	io1	350 / 1,000	3	us-west-2
인프라 노드 [2]	r5.2xlarge	8	64	gp3	300 / 900	3	us-west-2
워크로드 [3]	m5.2xlarge	8	32	gp3	350 / 900	3	us-west-2
컴퓨팅 노드	m5.2xlarge	8	32	gp3	350 / 900	102	us-west-2

1. etcd는 I/O 집약적이고 대기 시간에 민감하기 때문에 io1 디스크는 컨트롤 플레인/etcd 노드에 사용됩니다. 사용량에 따라 더 많은 수의 IOPS가 필요할 수 있습니다.

2. Prometheus는 사용 패턴에 따라 대량의 메모리를 요청할 수 있기 때문에 인프라 노드는 모니터링 구성 요소를 호스팅하는 데 사용됩니다.

3. 워크로드 노드는 성능 및 확장 가능한 워크로드 생성기 실행 전용입니다.

더 큰 클러스터 크기 및 오브젝트 수가 많을 수 있습니다. 그러나 인프라 노드의 크기 조정에서는 Prometheus에서 사용할 수 있는 메모리 양을 제한합니다. 오브젝트를 생성, 수정 또는 삭제할 때 Prometheus는 디스크의 지표를 유지하기 위해 약 3시간 동안 해당 메모리에 지표를 저장합니다. 오브젝트 생성, 수정 또는 삭제 비율이 너무 높으면 메모리 리소스가 부족하여 Prometheus가 압도되고 실패할 수 있습니다.

1.3. 컨트롤 플레인 및 인프라 노드 크기 조정 및 스케일링

OpenShift Dedicated 클러스터를 설치할 때 컨트롤 플레인 및 인프라 노드의 크기 조정은 컴퓨팅 노드 수에 따라 자동으로 결정됩니다.

설치 후 클러스터의 컴퓨팅 노드 수를 변경하면 Red Hat site Reliability Engineering(SRE) 팀이 클러스터의 안정성을 유지하기 위해 필요에 따라 컨트롤 플레인 및 인프라 노드를 스케일링합니다.

1.3.1. 설치 중 노드 크기 조정

설치 프로세스 중에 컨트롤 플레인 및 인프라 노드의 크기 조정이 동적으로 계산됩니다. 크기 조정 계산은 클러스터의 컴퓨팅 노드 수를 기반으로 합니다.

다음 표에는 설치 중에 적용되는 컨트롤 플레인 및 인프라 노드 크기 조정이 나열되어 있습니다.

컴퓨팅 노드 수	컨트롤 플레인 크기	인프라 노드 크기
1~25	m5.2xlarge	r5.xlarge
26~100	m5.4xlarge	r5.2xlarge
101 ~ 180 [1]	m5.8xlarge	r5.4xlarge

1. OpenShift Dedicated의 최대 컴퓨팅 노드 수는 180입니다.

1.3.2. 설치 후 노드 스케일링

설치 후 컴퓨팅 노드 수를 변경하면 필요에 따라 컨트롤 플레인 및 인프라 노드가 Red Hat SRE(Site Reliability Engineering) 팀에 의해 확장됩니다. 플랫폼의 안정성을 유지하기 위해 노드가 확장됩니다.

컨트롤 플레인 및 인프라 노드에 대한 설치 후 확장 요구 사항은 사례별로 평가됩니다. 노드 리소스 사용 및 수신 경고가 고려됩니다.

컨트롤 플레인 노드 크기 조정 경고 규칙

다음 시나리오 중 하나가 true인 경우 클러스터의 컨트롤 플레인 노드에 대해 경고 크기 조정이 트리거됩니다.

- 각 컨트롤 플레인 노드에는 16GiB 이상의 RAM이 있으며 컴퓨팅 노드는 25개 미만이며, 101개 미만의 컴퓨팅 노드가 있습니다.
- 각 컨트롤 플레인 노드에는 32GiB 이상의 RAM이 있으며 컴퓨팅 노드가 100개 이상 있습니다.

참고

ROSA의 최대 컴퓨팅 노드 수는 180입니다.

인프라 노드 크기 조정 경고 규칙

다음 시나리오 중 하나가 true인 경우 클러스터의 인프라 노드에 대해 경고 크기 조정이 트리거됩니다.

- 각 인프라 노드에는 16GiB 이상의 RAM 또는 CPU가 5개 미만이며, 컴퓨팅 노드는 25개 미만의 계산 노드가 있습니다.

- 각 인프라 노드에는 32GiB RAM 또는 9개 미만의 CPU가 있으며 컴퓨팅 노드가 100개 이상 있습니다.

참고

OpenShift Dedicated의 최대 컴퓨팅 노드 수는 180입니다.

예를 들어 노드의 리소스 사용량 증가를 관리하기 위해 SRE 팀은 추가 이유로 컨트롤 플레인 및 인프라 노드를 확장할 수 있습니다.

1.3.3. 대규모 클러스터 크기 조정

대규모 클러스터의 경우 인프라 노드 크기 조정이 확장성에 큰 영향을 미칠 수 있습니다. etcd 버전 또는 스토리지 데이터 형식을 비롯하여 명시된 임계값에 영향을 주는 요인은 여러 가지가 있습니다.

이러한 제한을 초과해도 클러스터가 실패할 수 있음을 나타내는 것은 아닙니다. 대부분의 경우 이러한 수치를 초과하면 전체 성능이 저하됩니다.

2장. AWS의 CUSTOMER CLOUD 서브스크립션

OpenShift Dedicated는 Red Hat이 고객의 기존 AWS(Amazon Web Service) 계정으로 클러스터를 배포 및 관리할 수 있는 CCS(Customer Cloud Subscription) 모델을 제공합니다.

2.1. AWS의 CUSTOMER CLOUD 서브스크립션 이해

고객 클라우드 서브스크립션(CCS) 모델을 사용하여 기존 Amazon Web Services(AWS) 계정에 OpenShift Dedicated를 배포하려면 Red Hat에서 몇 가지 사전 요구 사항을 충족해야 합니다.

Red Hat은 AWS 조직을 사용하여 여러 AWS 계정을 관리할 것을 권장합니다. 고객이 관리하는 AWS 조직은 여러 AWS 계정을 호스팅합니다. 조직에는 모든 계정이 계정 계층에서 참조할 루트 계정이 있습니다.

CCS 모델을 사용하는 OpenShift Dedicated 클러스터는 AWS 조직 단위 내의 AWS 계정에서 호스팅하는 것이 좋습니다. AWS 하위 계정에서 액세스할 수 있는 서비스를 관리하는 AWS Organizational Unit에 SCP(서비스 제어 정책)가 생성되고 적용됩니다. SCP는 조직 단위 내의 모든 AWS 하위 계정에 대해 단일 AWS 계정 내에서 사용 가능한 권한에만 적용됩니다. SCP를 단일 AWS 계정에 적용할 수도 있습니다. 고객의 AWS 조직의 다른 모든 계정은 고객이 요구하는 방식으로 관리합니다. Red Hat SRE(Site Reliability Engineer)는 AWS 조직 내에서 SCP를 제어할 수 없습니다.

2.2. 고객 요구사항

AWS(Amazon Web Services)에서 CCS(Customer Cloud Subscription) 모델을 사용하는 OpenShift Dedicated 클러스터는 배포하기 전에 몇 가지 사전 요구 사항을 충족해야 합니다.

2.2.1. 계정

- 고객은 AWS 제한이 고객이 제공하는 AWS 계정 내에서 프로비저닝한 OpenShift Dedicated를 지원하기에 충분합니다.
- 고객이 제공하는 AWS 계정은 해당 SCP(서비스 제어 정책)가 적용된 고객의 AWS 조직에 있어야 합니다.

참고

고객이 제공하는 계정이 AWS 조직 내에 있거나 SCP를 적용할 필요는 없지만 Red Hat은 제한 없이 SCP에 나열된 모든 조치를 수행할 수 있어야 합니다.

- 고객이 제공하는 AWS 계정은 Red Hat으로 이전할 수 없습니다.
- 고객은 Red Hat 활동에 AWS 사용 제한을 적용하지 않을 수 있습니다. 제한 사항을 초래하는 경우 Red Hat의 사고 대응에 심각한 영향을 미칠 수 있습니다.
- Red Hat은 AWS에 모니터링을 배포하여 루트 계정과 같은 권한이 높은 계정이 고객 제공 AWS 계정에 로그인할 때 Red Hat에 경고합니다.
- 고객은 동일한 고객이 제공하는 AWS 계정 내에서 기본 AWS 서비스를 배포할 수 있습니다.

참고

고객은 OpenShift Dedicated 및 기타 Red Hat 지원 서비스를 호스팅하는 VPC와 별도로 VPC(Virtual Private Cloud)에 리소스를 배포하는 것이 좋지만 필수는 아닙니다.

2.2.2. 액세스 요구 사항

- OpenShift Dedicated 서비스를 적절하게 관리하려면 Red Hat은 관리자 역할에 항상 **AdministratorAccess** 정책을 적용해야 합니다.

참고

이 정책은 고객이 제공하는 AWS 계정의 리소스를 변경할 수 있는 권한 및 기능만 Red Hat에 제공합니다.

- Red Hat은 고객이 제공하는 AWS 계정에 대한 AWS 콘솔 액세스 권한이 있어야 합니다. 이 액세스는 Red Hat에서 보호 및 관리합니다.
- 고객은 AWS 계정을 사용하여 OpenShift Dedicated 클러스터 내에서 권한을 강화해서는 안 됩니다.
- OpenShift Cluster Manager Hybrid Cloud Console 에서 제공되는 작업은 고객이 제공하는 AWS 계정에서 직접 수행해서는 안 됩니다.

2.2.3. 지원 요구사항

- Red Hat은 고객이 최소한 AWS의 비즈니스 지원을 받을 것을 권장합니다.
- Red Hat은 고객으로부터 AWS 지원을 요청할 권한을 갖습니다.
- Red Hat은 고객 제공 계정에서 AWS 리소스 제한을 요청할 권한이 있습니다.
- Red Hat은 이 요구 사항 섹션에 달리 지정하지 않는 한 모든 OpenShift Dedicated 클러스터의 제한 사항, 제한 사항, 기대치 및 기본값을 동일한 방식으로 관리합니다.

2.2.4. 보안 요구사항

- 고객이 제공하는 IAM 인증 정보는 고객이 제공하는 AWS 계정에 고유해야 하며 고객이 제공한 AWS 계정의 어느 곳에도 저장해서는 안 됩니다.
- 볼륨 스냅샷은 고객이 제공하는 AWS 계정 및 고객 지정 리전 내에 유지됩니다.
- Red Hat은 허용 목록에 있는 Red Hat 시스템을 통해 EC2 호스트 및 API 서버에 대한 수신 액세스 권한이 있어야 합니다.
- Red Hat은 시스템 및 감사 로그를 Red Hat 관리 중앙 로깅 스택으로 전달할 수 있는 송신이 있어야 합니다.

2.3. 필요한 고객 절차

CCCS(Customer Cloud Subscription) 모델을 사용하면 Red Hat에서 OpenShift Dedicated를 고객의 AWS(Amazon Web Services) 계정으로 배포 및 관리할 수 있습니다. Red Hat은 이러한 서비스를 제공하기 위해 여러 가지 사전 요구 사항이 필요합니다.

절차

1. 고객이 AWS 조직을 사용하는 경우 조직 내에서 AWS 계정을 사용하거나 새 조직을 생성해야 합니다.

2. Red Hat이 필요한 작업을 수행할 수 있도록 하려면 SCP(서비스 제어 정책)를 생성하거나 AWS 계정에 적용되지 않았는지 확인해야 합니다.
3. AWS 계정에 SCP를 연결합니다.
4. AWS 계정 내에서 다음 요구 사항에 따라 **osdCcsAdmin** IAM 사용자를 생성해야 합니다.
   - 이 사용자는 최소한 **프로그래밍 방식으로 액세스를** 사용하도록 설정해야 합니다.
   - 이 사용자에게는 **AdministratorAccess** 정책이 연결되어 있어야 합니다.
5. Red Hat에 IAM 사용자 자격 증명을 제공합니다.
   - OpenShift Cluster Manager 하이브리드 클라우드 콘솔에서 **액세스 키 ID 및 시크릿 액세스 키**를 제공해야 합니다.

2.4. 최소 SCP(필수 서비스 제어 정책)

SCP(서비스 제어 정책) 관리는 고객의 책임입니다. 이러한 정책은 AWS 조직에서 유지 관리되며 연결된 AWS 계정 내에서 사용할 수 있는 서비스를 제어합니다.

필수/선택 사항	Service	작업	효과
필수 항목	Amazon EC2	All	허용
	Amazon EC2 Auto Scaling	All	허용
	Amazon S3	All	허용
	ID 및 액세스 관리	All	허용
	Elastic Load Balancing	All	허용
	Elastic Load Balancing V2	All	허용
	Amazon CloudWatch	All	허용
	Amazon CloudWatch Events	All	허용
	Amazon CloudWatch Logs	All	허용
	AWS 지원	All	허용
	AWS 키 관리 서비스	All	허용
	AWS 보안 토큰 서비스	All	허용

필수/선택 사항	Service	작업	효과
	AWS 리소스 태그	All	허용
	AWS Route53 DNS	All	허용
	AWS Service Quotas	ListServices GetRequestedServiceQuotaChange GetServiceQuota RequestServiceQuotaIncrease ListServiceQuotas	허용
선택 사항	AWS billinging	ViewAccount Viewbilling ViewUsage	허용
	AWS Cost and Usage Report	All	허용
	AWS Cost Explorer Services	All	허용

```
{
    "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. AWS에 대한 RED HAT 관리 IAM 참조

Red Hat은 IAM 정책, IAM 사용자 및 IAM 역할 등 AWS(Amazon Web Services) 리소스를 생성하고 관리합니다.

2.5.1. IAM 정책

참고

IAM 정책은 OpenShift Dedicated의 기능 변경으로 변경될 수 있습니다.

- **AdministratorAccess** 정책은 관리 역할에서 사용합니다. 이 정책은 Red Hat에 고객이 제공하는 AWS 계정에서 OpenShift Dedicated 클러스터를 관리하는 데 필요한 액세스 권한을 제공합니다.

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

- **CustomerAdministratorAccess** 역할은 고객에게 AWS 계정 내에서 서비스의 하위 집합을 관리할 수 있는 액세스 권한을 제공합니다. 이 시점에서는 다음이 허용됩니다.
  - VPC 피어링
  - VPN 설정
  - 직접 연결(서비스 제어 정책을 통해 부여된 경우에만 사용 가능)

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

- enabled인 경우 Terming **ReadOnlyAccess** 역할은 계정에 대한 청구 및 사용 정보를 볼 수 있는 읽기 전용 액세스를 제공합니다.
  청구 및 사용 액세스 권한은 AWS 조직의 루트 계정에 활성화된 경우에만 부여됩니다. 이는 고객이 읽기 전용 청구 및 사용 액세스를 활성화하기 위해 수행해야 하는 선택적 단계이며 이 프로필 생성과 이를 사용하는 역할에는 영향을 미치지 않습니다. 이 역할을 사용하지 않으면 사용자는 청구 및 사용 정보를 볼 수 없습니다. 청구 데이터에 대한 액세스를 활성화하는 방법에 대한 이 튜토리얼을 참조하십시오.

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

2.5.2. IAM 사용자

osdManagedAdmin 사용자는 고객이 제공한 AWS 계정을 제어한 후 즉시 생성됩니다. OpenShift Dedicated 클러스터 설치를 수행할 사용자입니다.

2.5.3. IAM 역할

- **network-mgmt** 역할은 별도의 AWS 계정을 통해 AWS 계정에 대한 고객 관리 액세스 권한을 제공합니다. 또한 읽기 전용 역할과 동일한 액세스 권한을 갖습니다. **network-mgmt** 역할은 비 고객 클라우드 서브스크립션(CCS) 클러스터에만 적용됩니다. 다음 정책이 역할에 연결되어 있습니다.
  - AmazonEC2ReadOnlyAccess
  - CustomerAdministratorAccess
- **읽기 전용** 역할은 별도의 AWS 계정을 통해 AWS 계정에 대한 고객 제공 읽기 전용 권한을 제공합니다. 다음 정책이 역할에 연결되어 있습니다.
  - AWSAccountUsageReportAccess

- AmazonEC2ReadOnlyAccess
- AmazonS3ReadOnlyAccess
- IAMReadOnlyAccess
- BillingReadOnlyAccess

2.6. 프로비저닝된 AWS 인프라

배포된 OpenShift Dedicated 클러스터에 프로비저닝된 AWS(Amazon Web Services) 구성 요소에 대한 개요입니다. 프로비저닝된 모든 AWS 구성 요소의 자세한 목록은 OpenShift Container Platform 설명서를 참조하십시오.

2.6.1. AWS EC2(Elastic Computing) 인스턴스

AWS EC2 인스턴스는 AWS 퍼블릭 클라우드에서 OpenShift Dedicated의 컨트롤 플레인 및 데이터 플레인 기능을 배포해야 합니다. 작업자 노드 수에 따라 컨트롤 플레인 및 인프라 노드에 따라 인스턴스 유형이 다를 수 있습니다.

- 단일 가용성 영역
  - 최소 3개의 m5.2xlarge (컨트롤 플레인 노드)
  - 2개의 r5.xlarge 최소 (인프라 노드)
  - 2 m5.xlarge 최소 하지만 높은 변수(작업자 노드)
- 다중 가용성 영역
  - 최소 3개의 m5.2xlarge (컨트롤 플레인 노드)
  - 3개의 r5.xlarge 최소 (인프라 노드)
  - 3개의 m5.xlarge 최소 하지만 높은 변수(작업자 노드)

2.6.2. AWS EBS(Elastic Block Store) 스토리지

Amazon EBS 블록 스토리지는 로컬 노드 스토리지 및 영구 볼륨 스토리지 모두에 사용됩니다.

각 EC2 인스턴스의 볼륨 요구 사항:

- 컨트롤 플레인 볼륨
  - 크기: 350GB
  - 유형: io1
  - 초당 입력/출력 작업: 1000
- 인프라 볼륨
  - 크기: 300GB
  - 유형: gp2
  - 초당 입력/출력 작업: 900

- 작업자 볼륨
  - 크기: 300GB
  - 유형: gp2
  - 초당 입력/출력 작업: 900

2.6.3. Elastic 로드 밸런서

API용 최대 두 개의 NLB(Network Load Balancer)와 애플리케이션 라우터용 최대 2개의 클래식 로드 밸런서(CLB)입니다. 자세한 내용은 AWS에 대한 ELB 설명서를 참조하십시오.

2.6.4. S3 스토리지

이미지 레지스트리 및 EBS(Elastic Block Store) 볼륨 스냅샷은 AWS S3 스토리지에서 지원합니다. 리소스 정리는 S3 사용량 및 클러스터 성능을 최적화하기 위해 정기적으로 수행됩니다.

참고

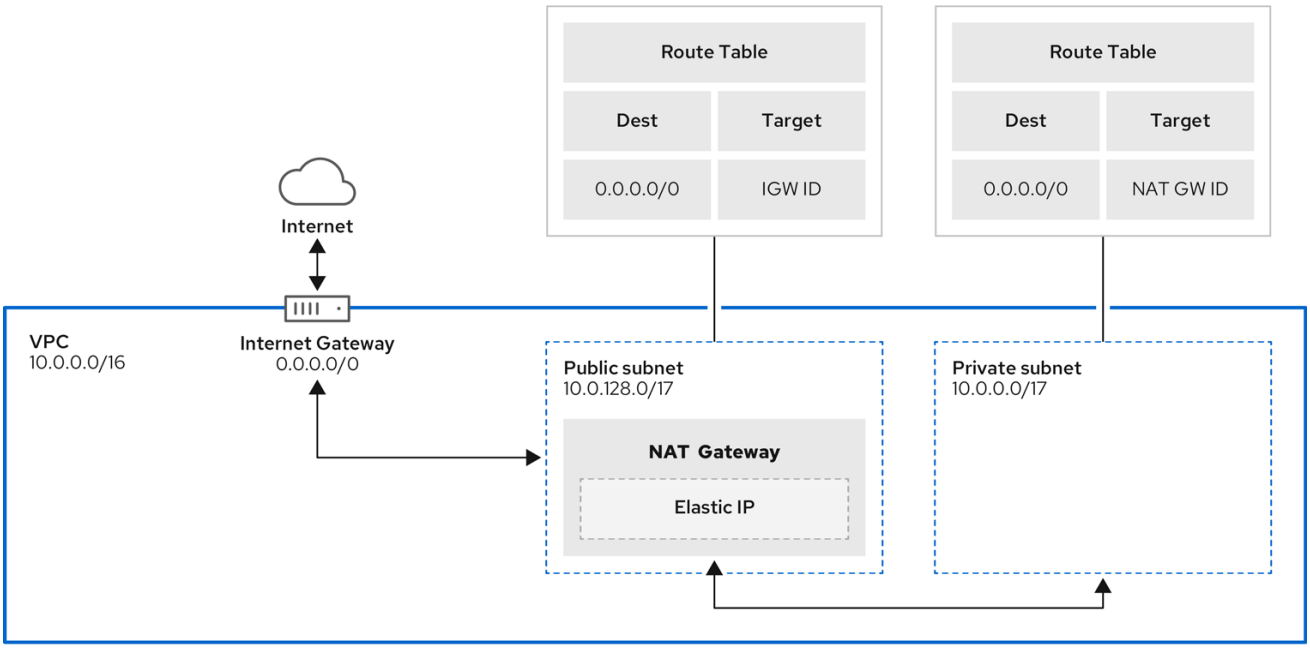
일반적인 크기가 2TB인 경우 각각 두 개의 버킷이 필요합니다.

2.6.5. VPC

고객은 클러스터당 하나의 VPC를 확인해야 합니다. 또한 VPC에는 다음 구성이 필요합니다.

- **서브넷: 단일 가용성 영역이 있는 클러스터의** 두 서브넷 또는 여러 가용성 영역이 있는 클러스터의 경우 6개의 서브넷입니다.
- **라우팅 테이블**: 프라이빗 서브넷당 하나의 라우팅 테이블과 클러스터당 하나의 추가 테이블입니다.
- **인터넷 게이트웨이**: 클러스터당 하나의 인터넷 게이트웨이.
- **NAT 게이트웨이**: 퍼블릭 서브넷당 하나의 NAT 게이트웨이.

2.6.5.1. 샘플 VPC 아키텍처



2.6.6. 보안 그룹

AWS 보안 그룹은 프로토콜 및 포트 액세스 수준의 보안을 제공하며 EC2 인스턴스 및 Elastic Load Balancing과 연결됩니다. 각 보안 그룹에는 EC2 인스턴스가 들어오고 나가는 트래픽을 필터링하는 규칙 세트가 포함되어 있습니다. OpenShift Container Platform 설치에 필요한 포트가 네트워크에서 열려 있고 호스트 간 액세스를 허용하도록 구성되어 있는지 확인해야 합니다.

2.7. AWS 계정 제한

OpenShift Dedicated 클러스터는 여러 AWS(Amazon Web Services) 구성 요소를 사용하며 기본 서비스 제한은 OpenShift Dedicated 클러스터 설치 기능에 영향을 미칩니다. 특정 클러스터 구성을 사용하거나 특정 AWS 리전에 클러스터를 배포하거나 사용자 계정에서 여러 클러스터를 실행하는 경우 AWS 계정의 추가 리소스를 요청해야 할 수 있습니다.

다음 표에는 OpenShift Dedicated 클러스터를 설치하고 실행하는 데 영향을 미칠 수 있는 AWS 구성 요소 제한이 요약되어 있습니다.

구성 요소	기본적으로 사용 가능한 클러스터 수	기본 AWS 제한	설명

구성 요소	기본적으로 사용 가능한 클러스터 수	기본 AWS 제한	설명
인스턴스 제한	변동 가능	변동 가능	최소한 각 클러스터는 다음 인스턴스를 생성합니다. ● 설치 후 제거되는 하나의 부트스트랩 시스템 ● 컨트롤 플레인 노드 세 개 ● 단일 가용성 영역의 두 개의 인프라 노드, 멀티 가용성 영역의 세 개의 인프라 노드 ● 단일 가용성 영역의 작업자 노드 두 개, 멀티 가용성 영역의 작업자 노드 세 개 이러한 인스턴스 유형 수는 새 계정의 기본 제한 내에 있습니다. 더 많은 작업자 노드를 배포하거나, 대규모 워크로드를 배포하거나, 다른 인스턴스 유형을 사용하려면 계정 제한을 검토하여 클러스터가 필요한 시스템을 배포할 수 있는지 확인합니다. 대부분의 리전에서 부트스트랩 및 작업자 시스템은 **m4.large** 시스템을 사용하고 컨트롤 플레인 시스템은 **m4.xlarge** 인스턴스를 사용합니다. 이러한 인스턴스 유형을 지원하지 않는 모든 리전을 포함한 일부 리전에서는 **m5.large** 및 **m5.xlarge** 인스턴스를 대신 사용합니다.
탄력적 IP(EIP)	0 ~1	계정 당 EIP 5개	설치 프로그램은 클러스터를 고가용성 구성으로 프로비저닝하기 위해 각각의 리전 내 가용성 영역의 퍼블릭 및 프라이빗 서브넷을 만듭니다. 각 프라이빗 서브넷에는 NAT 게이트웨이 가 필요하며 각 NAT 게이트웨이에는 별도의 탄력적 IP 가 필요합니다. 각 리전의 가용성 영역 수를 판별하려면 AWS 영역 지도를 검토합니다. 기본 고가용성을 활용하려면 세 개 이상의 가용성 영역이 있는 리전에 클러스터를 설치합니다. 여섯 개 이상의 가용성 영역이 있는 리전에 클러스터를 설치하려면 EIP 제한을 늘려야 합니다.  **중요** **us-east-1** 리전을 사용하려면 계정의 EIP 제한을 늘려야 합니다.
가상 사설 클라우드(VPC)	5	리전당 VPC 5개	각 클러스터마다 자체 VPC를 생성합니다.

구성 요소	기본적으로 사용 가능한 클러스터 수	기본 AWS 제한	설명
탄력적 로드 밸런싱(ELB/NLB)	3	리전당 20개	기본적으로 각 클러스터는 기본 API 서버에 대한 내부 및 외부 네트워크 로드 밸런서를 생성하고 라우터용 단일 클래식 탄력적 로드 밸런서를 생성합니다. Kubernetes LoadBalancer Service 개체를 더 배포하면 추가 로드 밸런서가 생성됩니다.
NAT 게이트웨이	5	가용성 영역당 5개	클러스터는 각 가용성 영역에 하나의 NAT 게이트웨이를 배포합니다.
탄력적 네트워크 인터페이스(ENI)	12개 이상	리전당 350개	기본 설치는 21개의 ENI와 함께 리전 내 각 가용성 영역마다 하나의 ENI를 생성합니다. 예를 들어 **us-east-1** 리전에는 여섯 개의 가용성 영역이 있으므로 해당 영역에 배포되는 클러스터는 27개의 ENI를 사용합니다. 각 리전의 가용성 영역 수를 판별하려면 AWS 영역 지도를 검토합니다. 클러스터 사용 및 배포된 워크로드에 의해 생성되는 추가 시스템 및 탄력적 로드 밸런서마다 추가 ENI가 생성됩니다.
VPC 게이트웨이	20	계정당 20개	각 클러스터는 S3 액세스를 위한 단일 VPC 게이트웨이를 생성합니다.
S3 버킷	99	계정당 버킷 100개	설치 프로세스에서 임시 버킷을 생성하고 각 클러스터의 레지스트리 구성 요소가 버킷을 생성하므로 AWS 계정당 OpenShift Dedicated 클러스터를 99개만 생성할 수 있습니다.
보안 그룹	250	계정당 2,500개	클러스터마다 10개의 개별 보안 그룹을 생성합니다.

3장. GCP의 CUSTOMER CLOUD 서브스크립션

Red Hat은 고객이 관리하는 GCP(Google Cloud Platform) 프로젝트를 사용하여 모든 GCP 리소스를 구성하는 것이 좋습니다. 프로젝트는 일련의 사용자 및 API와 해당 API의 청구, 인증 및 모니터링 설정으로 구성됩니다.

OpenShift Dedicated CCS 클러스터가 GCP 조직 내의 GCP 프로젝트에서 호스팅되는 것이 가장 좋습니다. 조직 리소스는 GCP 리소스 계층의 루트 노드이며 조직에 속한 모든 리소스는 조직 노드에 그룹화됩니다. 부여된 특정 역할이 있는 IAM 서비스 계정이 생성되어 GCP 프로젝트에 적용됩니다. API를 호출할 때 일반적으로 인증을 위한 서비스 계정 키를 제공합니다. 각 서비스 계정은 특정 프로젝트에서 소유하지만 서비스 계정에 다른 프로젝트의 리소스에 액세스할 수 있는 역할이 제공될 수 있습니다.

3.1. GCP의 고객 클라우드 서브스크립션 이해

Red Hat OpenShift Dedicated는 Red Hat이 고객의 기존 GCP(Google Cloud Platform) 계정에 OpenShift Dedicated를 배포 및 관리할 수 있는 CCS(Customer Cloud Subscription) 모델을 제공합니다. 이 서비스를 제공하려면 Red Hat에서 몇 가지 사전 요구 사항을 충족해야 합니다.

Red Hat은 고객이 관리하는 GCP 프로젝트를 사용하여 모든 GCP 리소스를 구성하는 것이 좋습니다. 프로젝트는 일련의 사용자 및 API와 해당 API의 청구, 인증 및 모니터링 설정으로 구성됩니다.

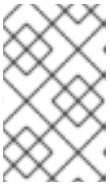
CCS 모델을 사용하는 OpenShift Dedicated 클러스터는 GCP 조직 내의 GCP 프로젝트에서 호스팅하는 것이 좋습니다. 조직 리소스는 GCP 리소스 계층의 루트 노드이며 조직에 속한 모든 리소스는 조직 노드에 그룹화됩니다. 부여된 특정 역할이 있는 IAM 서비스 계정이 생성되어 GCP 프로젝트에 적용됩니다. API를 호출할 때 일반적으로 인증을 위한 서비스 계정 키를 제공합니다. 각 서비스 계정은 특정 프로젝트에서 소유하지만 서비스 계정에 다른 프로젝트의 리소스에 액세스할 수 있는 역할이 제공될 수 있습니다.

3.2. 고객 요구사항

GCP(Google Cloud Platform)에서 CCS(Customer Cloud Subscription) 모델을 사용하는 OpenShift Dedicated 클러스터는 배포하기 전에 몇 가지 사전 요구 사항을 충족해야 합니다.

3.2.1. 계정

- 고객은 고객이 제공하는 GCP 계정에서 프로비저닝한 OpenShift Dedicated를 지원하기에 Google Cloud 제한이 충분한지 확인합니다.
- 고객이 제공하는 GCP 계정은 해당 서비스 계정이 적용된 고객의 Google Cloud Organization에 있어야 합니다.
- 고객 제공 GCP 계정을 Red Hat으로 양도할 수 없습니다.
- 고객은 Red Hat 활동에 GCP 사용 제한을 적용하지 않을 수 있습니다. 제한 사항을 초래하는 경우 Red Hat의 사고 대응에 심각한 영향을 미칠 수 있습니다.
- Red Hat은 root 계정과 같은 고도의 권한이 있는 계정이 고객 제공 GCP 계정에 로그인할 때 Red Hat에 경고하기 위해 GCP에 모니터링을 배포합니다.
- 고객은 동일한 고객 제공 GCP 계정 내에 기본 GCP 서비스를 배포할 수 있습니다.



참고

고객은 OpenShift Dedicated 및 기타 Red Hat 지원 서비스를 호스팅하는 VPC와 별도로 VPC(Virtual Private Cloud)에 리소스를 배포하는 것이 좋지만 필수는 아닙니다.

3.2.2. 액세스 요구 사항

- OpenShift Dedicated 서비스를 적절하게 관리하려면 Red Hat은 관리자 역할에 항상 **AdministratorAccess** 정책을 적용해야 합니다.

참고

이 정책은 고객 제공 GCP 계정의 리소스를 변경할 수 있는 권한 및 기능만 Red Hat에 제공합니다.

- Red Hat은 고객이 제공하는 GCP 계정에 대한 GCP 콘솔 액세스 권한이 있어야 합니다. 이 액세스는 Red Hat에서 보호 및 관리합니다.
- 고객은 GCP 계정을 사용하여 OpenShift Dedicated 클러스터 내에서 권한을 승격해서는 안 됩니다.
- OpenShift Cluster Manager Hybrid Cloud Console 에서 사용 가능한 작업은 고객이 제공하는 GCP 계정에서 직접 수행할 수 없어야 합니다.

3.2.3. 지원 요구사항

- Red Hat은 고객이 GCP 이상의 제품 지원을 받을 것을 권장합니다. https://cloud.google.com/support
- Red Hat은 고객을 대신하여 GCP 지원을 요청할 권한을 가지고 있습니다.
- Red Hat은 고객이 제공하는 계정에서 GCP 리소스 제한을 요청할 권한이 있습니다.
- Red Hat은 이 요구 사항 섹션에 달리 지정하지 않는 한 모든 OpenShift Dedicated 클러스터의 제한 사항, 제한 사항, 기대치 및 기본값을 동일한 방식으로 관리합니다.

3.2.4. 보안 요구사항

- 고객이 제공하는 IAM 인증 정보는 고객이 제공하는 GCP 계정에 고유해야 하며 고객이 제공하는 GCP 계정의 어느 곳에도 저장해서는 안 됩니다.
- 볼륨 스냅샷은 고객이 제공하는 GCP 계정 및 고객 지정 리전 내에 유지됩니다.
- Red Hat은 허용 목록에 있는 Red Hat 시스템을 통해 API 서버에 대한 수신 액세스 권한이 있어야 합니다.
- Red Hat은 시스템 및 감사 로그를 Red Hat 관리 중앙 로깅 스택으로 전달할 수 있는 송신이 있어야 합니다.

3.3. 필요한 고객 절차

CCCS(Customer Cloud Subscription) 모델을 사용하면 Red Hat에서 OpenShift Dedicated를 고객의 GCP(Google Cloud Platform) 프로젝트에 배포 및 관리할 수 있습니다. Red Hat은 이러한 서비스를 제공하기 위해 여러 가지 사전 요구 사항이 필요합니다.

주의

GCP 프로젝트에서 OpenShift Dedicated를 사용하려면 다음 GCP 조직 정책 제약 조건을 적용할 수 없습니다.

- **constraints/iam.allowedPolicyMemberDomains**
- **constraints/compute.restrictLoadBalancerCreationForTypes**
- **constraints/compute.requireShieldedVm**
- **제약 조건/compute.vmExternalIpAccess** (이 정책 제약 조건은 설치 중에만 지원되지 않습니다. 설치 후 정책 제약 조건을 다시 활성화할 수 있습니다.)

절차

1. OpenShift Dedicated 클러스터를 호스팅할 Google Cloud 프로젝트를 생성합니다.

참고

프로젝트 이름은 10자 미만이어야 합니다.

2. OpenShift Dedicated 클러스터를 호스팅하는 프로젝트에서 다음과 같은 필수 API를 활성화합니다.

표 3.1. 필수 API 서비스

API 서비스	콘솔 서비스 이름
Cloud Deployment Manager V2 API	**deploymentmanager.googleapis.com**
컴퓨팅 엔진 API	**compute.googleapis.com**
Google 클라우드 API	**cloudapis.googleapis.com**
클라우드 리소스 관리자 API	**cloudresourcemanager.googleapis.com**
Google DNS API	**dns.googleapis.com**
네트워크 보안 API	**networksecurity.googleapis.com**
IAM 서비스 계정 자격 증명 API	**iamcredentials.googleapis.com**

API 서비스	콘솔 서비스 이름
IAM(ID 및 액세스 관리) API	**iam.googleapis.com**
서비스 관리 API	**servicemanagement.googleapis.com**
서비스 사용량 API	**serviceusage.googleapis.com**
Google 클라우드 스토리지 JSON API	**storage-api.googleapis.com**
클라우드 스토리지	**storage-component.googleapis.com**

3. Red Hat이 필요한 작업을 수행할 수 있도록 GCP 프로젝트 내에서 **osd-ccs-admin** IAM 서비스 계정 사용자를 생성해야 합니다.
서비스 계정에 다음 역할을 부여해야 합니다 .

표 3.2. 필수 역할

Role	콘솔 역할 이름
컴퓨팅 관리자	**roles/compute.admin**
DNS 관리자	**roles/dns.admin**
조직 정책 뷰어	**roles/orgpolicy.policyViewer**
소유자	**역할/소유자**
프로젝트 IAM 관리자	**roles/resourcemanager.projectIamAdmin**
서비스 관리 관리자	**roles/servicemanagement.admin**
서비스 사용량 관리자	**roles/serviceusage.serviceUsageAdmin**
스토리지 관리자	**roles/storage.admin**

4. **osd-ccs-admin** IAM 서비스 계정에 대한 서비스 계정 키를 생성합니다 . **osServiceAccount.json**; 이 JSON 파일은 클러스터를 생성할 때 Red Hat OpenShift Cluster Manager에 업로드됩니다.

3.4. RED HAT 관리 GOOGLE CLOUD 리소스

Red Hat은 다음 IAM GCP(Google Cloud Platform) 리소스를 생성하고 관리합니다.

3.4.1. IAM 서비스 계정 및 역할

osd-managed-admin IAM 서비스 계정은 고객이 제공하는 GCP 계정을 제어하는 직후 생성됩니다. OpenShift Dedicated 클러스터 설치를 수행할 사용자입니다.

다음 역할이 서비스 계정에 연결되어 있습니다.

표 3.3. osd-managed-admin의 IAM 역할

Role	콘솔 역할 이름	설명
컴퓨팅 관리자	**roles/compute.admin**	모든 Compute Engine 리소스를 완벽하게 제어할 수 있습니다.
DNS 관리자	**roles/dns.admin**	모든 Cloud DNS 리소스에 대한 읽기-쓰기 액세스를 제공합니다.
보안 관리자	**roles/iam.securityAdmin**	IAM 정책을 가져오고 설정할 수 있는 권한이 있는 보안 관리자 역할입니다.
스토리지 관리자	**roles/storage.admin**	오브젝트 및 버킷을 완전히 제어할 수 있습니다. 개별 **버킷** 에 적용되는 경우 제어는 버킷 내의 지정된 버킷 및 오브젝트에만 적용됩니다.
서비스 계정 관리자	**roles/iam.serviceAccountAdmin**	서비스 계정을 생성하고 관리합니다.
서비스 계정 키 관리자	**roles/iam.serviceAccountKeyAdmin**	서비스 계정 키를 생성하고 관리합니다.
서비스 계정 사용자	**roles/iam.serviceAccountUser**	서비스 계정으로 작업을 실행합니다.

3.4.2. IAM 그룹 및 역할

sd-sre-platform-gcp-access Google 그룹에 GCP 프로젝트에 대한 액세스 권한이 부여되어 긴급 문제 해결을 위해 Red Hat 사이트 안정성 엔지니어링(SRE)이 콘솔에 액세스할 수 있습니다.

다음 역할이 그룹에 연결되어 있습니다.

표 3.4. sd-sre-platform-gcp-access의 IAM 역할

Role	콘솔 역할 이름	설명
컴퓨팅 관리자	**roles/compute.admin**	모든 Compute Engine 리소스를 완벽하게 제어할 수 있습니다.

Role	콘솔 역할 이름	설명
편집기	**역할/편집기**	상태를 수정하는 작업에 대한 모든 뷰어 권한과 권한을 제공합니다.
조직 정책 뷰어	**roles/orgpolicy.policyViewer**	리소스에 대한 조직 정책 보기에 대한 액세스 권한을 제공합니다.
프로젝트 IAM 관리자	**roles/resourcemanager.projectIamAdmin**	프로젝트의 IAM 정책을 관리할 수 있는 권한을 제공합니다.
할당량 관리자	**roles/servicemanagement.quotaAdmin**	서비스 할당량 관리에 대한 액세스를 제공합니다.
역할 관리자	**roles/iam.roleAdmin**	프로젝트의 모든 사용자 지정 역할에 대한 액세스를 제공합니다.
서비스 계정 관리자	**roles/iam.serviceAccountAdmin**	서비스 계정을 생성하고 관리합니다.
서비스 사용량 관리자	**roles/serviceusage.serviceUsageAdmin**	소비자 프로젝트에 대해 서비스 상태를 활성화, 비활성화, 검사, 작업을 검사하고, 할당량 및 청구를 사용하는 기능.
기술 지원 편집기	**roles/cloudsupport.techSupportEditor**	기술 지원 케이스에 대한 전체 읽기-쓰기 액세스를 제공합니다.

3.5. 프로비저닝된 GCP 인프라

이는 배포된 OpenShift Dedicated 클러스터에 프로비저닝된 GCP(Google Cloud Platform) 구성 요소에 대한 개요입니다. 프로비저닝된 모든 GCP 구성 요소의 자세한 목록은 OpenShift Container Platform 설명서 를 참조하십시오.

3.5.1. 컴퓨팅 인스턴스

GCP에서 OpenShift Dedicated의 컨트롤 플레인 및 데이터 플레인 기능을 배포하려면 GCP 컴퓨팅 인스턴스가 필요합니다. 작업자 노드 수에 따라 컨트롤 플레인 및 인프라 노드에 따라 인스턴스 유형이 다를 수 있습니다.

- 단일 가용성 영역
  - 인프라 노드 2개(사용자 정의 머신 유형: 4 vCPU 및 32GB RAM)
  - 컨트롤 플레인 노드 세 개 (사용자 정의 머신 유형: 8 vCPU 및 32GB RAM)

    - 작업자 노드 2개(사용자 정의 머신 유형: 4 vCPU 및 16GB RAM)
- 다중 가용성 영역
    - 인프라 노드 3개(사용자 정의 머신 유형: 4 vCPU 및 32GB RAM)
    - 컨트롤 플레인 노드 세 개 (사용자 정의 머신 유형: 8 vCPU 및 32GB RAM)
    - 작업자 노드 3개(사용자 정의 머신 유형: 4 vCPU 및 16GB RAM)

3.5.2. 스토리지

- 인프라 볼륨:
    - 128GB SSD 영구 디스크(인스턴스 삭제 시 삭제)
    - 110GB 표준 영구 디스크(인스턴스 삭제 시 중요)
- 작업자 볼륨:
    - 128GB SSD 영구 디스크(인스턴스 삭제 시 삭제)
- 컨트롤 플레인 볼륨:
    - 128GB SSD 영구 디스크(인스턴스 삭제 시 삭제)

3.5.3. VPC

- **서브넷:** 컨트롤 플레인 워크로드용 마스터 서브넷과 다른 모든 워크로드용 작업자 서브넷 1개입니다.
- **라우터 테이블:** VPC당 하나의 글로벌 경로 테이블.
- **인터넷 게이트웨이:** 클러스터당 하나의 인터넷 게이트웨이.
- **NAT 게이트웨이:** 마스터 NAT 게이트웨이 1개와 클러스터당 하나의 작업자 NAT 게이트웨이.

3.5.4. 서비스

GCP CCS 클러스터에서 다음 서비스를 활성화해야 합니다.

- **Deploymentmanager**
- **Compute**
- **Cloudapis**
- **Cloudresourcemanager**
- **DNS**
- **Iamcredentials**
- **IAM**
- **Servicemanagement**

- **Serviceusage**
- **Storage-api**
- **storage-component**

3.5.5. 권한

support 서비스 계정에 다음 역할을 추가해야 합니다.

- **compute.admin**
- **Dns.admin**
- **orgpolicy.policyViewer**
- **소유자**
- **resourcemanager.projectIamAdmin**
- **Servicemanagement.admin**
- **serviceusage.serviceUsageAdmin**
- **storage.admin**

3.6. GCP 계정 제한

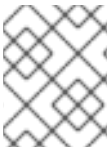
OpenShift Dedicated 클러스터는 여러 GCP(Google Cloud Platform) 구성 요소를 사용하지만 기본 할당량 은 OpenShift Dedicated 클러스터 설치 기능에 영향을 미치지 않습니다.

표준 OpenShift Dedicated 클러스터는 다음 리소스를 사용합니다. 일부 리소스는 부트스트랩 프로세스 중에만 필요하며 클러스터 배포 후 제거됩니다.

표 3.5. 기본 클러스터에서 사용되는 GCP 리소스

서비스	구성 요소	위치	필요한 총 리소스	부트스트랩 후 제거된 리소스
서비스 계정	IAM	글로벌	5	0
방화벽 규칙	컴퓨팅	글로벌	11	1
전달 규칙	컴퓨팅	글로벌	2	0
사용 중인 글로벌 IP 주소	컴퓨팅	글로벌	4	1
상태 검사	컴퓨팅	글로벌	3	0
이미지	컴퓨팅	글로벌	1	0
네트워크	컴퓨팅	글로벌	2	0

서비스	구성 요소	위치	필요한 총 리소스	부트스트랩 후 제거된 리소스
고정 IP 주소	컴퓨팅	리전	4	1
라우터	컴퓨팅	글로벌	1	0
라우트	컴퓨팅	글로벌	2	0
서브네트워크	컴퓨팅	글로벌	2	0
대상 풀	컴퓨팅	글로벌	3	0
CPU	컴퓨팅	리전	28	4
영구 디스크 SSD(GB)	컴퓨팅	리전	896	128



참고

설치하는 동안 할당량이 충분하지 않으면 설치 프로그램에서 초과된 할당량과 리전을 모두 안내하는 오류 메시지를 표시합니다.

실제 클러스터 크기, 예상 클러스터 증가, 계정과 연결된 다른 클러스터의 사용량을 모두 고려해야 합니다. CPU, 고정 IP 주소, 영구 디스크 SSD(스토리지) 할당량이 가장 부족하기 쉬운 할당량입니다.

다음 리전 중 하나에서 클러스터를 배포하려는 경우, 최대 스토리지 할당량을 초과할 것이며, CPU 할당량 제한을 초과할 가능성도 있습니다.

- asia-east2
- asia-northeast2
- asia-south1
- australia-southeast1
- europe-north1
- europe-west2
- europe-west3
- europe-west6
- northamerica-northeast1
- southamerica-east1
- us-west2

GCP 콘솔에서 리소스 할당량을 늘릴 수는 있지만 지원 티켓을 제출해야 할 수도 있습니다. OpenShift Dedicated 클러스터를 설치하기 전에 지원 티켓을 해결하기 위해 조기에 클러스터 크기를 계획해야 합니다.