OpenShift Dedicated 4

OpenShift Dedicated 소개

OpenShift Dedicated 아키텍처 개요

Last Updated: 2024-09-04

OpenShift Dedicated 4 OpenShift Dedicated 소개

OpenShift Dedicated 아키텍처 개요

법적 공지

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at
http://creativecommons.org/licenses/by-sa/3.0/
. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

초록

이 문서에서는 OpenShift Dedicated의 플랫폼 및 애플리케이션 아키텍처에 대한 개요를 제공합니다.

차례

1장. OPENSHIFT DEDICATED 이해

Kubernetes에 기반을 둔 OpenShift Dedicated는 클라우드 서비스로 제공되는 완전한 OpenShift Container Platform 클러스터이며 고가용성을 위해 구성되며 단일 고객 전용으로 구성됩니다.

1.1. OPENSHIFT DEDICATED 개요

OpenShift Dedicated는 Red Hat에서 관리하며 AWS(Amazon Web Services) 또는 GCP(Google Cloud Platform)에서 호스팅됩니다. 각 OpenShift Dedicated 클러스터에는 완전히 관리되는 컨트롤 플레인(Control 및 인프라 노드), Red Hat 사이트 안정성 엔지니어(SRE), 프리미엄 Red Hat 지원, 로깅, 메트릭, 모니터링, 알림 포털 및 클러스터 포털과 같은 클러스터 서비스가 포함되어 있습니다.

OpenShift Dedicated는 다음과 같은 향상된 기능을 포함하여 Kubernetes에 엔터프라이즈급 개선 사항을 제공합니다.

- OpenShift Dedicated 클러스터는 AWS 또는 GCP 환경에 배포되며 애플리케이션 관리의 하이브리드 접근 방식의 일부로 사용할 수 있습니다.
- 통합된 Red Hat 기술. OpenShift Dedicated의 주요 구성 요소는 Red Hat Enterprise Linux 및 관련 Red Hat 기술을 기반으로 합니다. OpenShift Dedicated는 Red Hat의 엔터프라이즈급 소프트웨어에 대한 강력한 테스트 및 인증 이니셔티브의 이점을 제공합니다.
- 오픈 소스 개발 모델. 개발은 공개적으로 완료되었으며 소스 코드는 공개 소프트웨어 리포지토리에서 구할 수 있습니다. 이 오픈 협업을 통해 빠른 혁신과 개발을 촉진할 수 있습니다.

OpenShift Container Platform에서 컨테이너화된 Kubernetes 애플리케이션을 빌드하고 배포할 때 생성할 수 있는 자산 옵션에 대한 자세한 내용은 OpenShift Container Platform 개발 이해 를 참조하십시오.

1.1.1. 사용자 정의 운영 체제

OpenShift Dedicated는 CoreOS 및 Red Hat Atomic Host 운영 체제의 최상의 기능과 기능을 결합하는 컨테이너 지향 운영 체제인 RHCOS(Red Hat Enterprise Linux CoreOS)를 사용합니다. RHCOS는 OpenShift Dedicated에서 컨테이너화된 애플리케이션을 실행하도록 특별히 설계되었으며 새로운 툴과 함께 작동하여 빠른 설치, Operator 기반 관리 및 단순화된 업그레이드를 제공합니다.

RHCOS는 다음을 포함합니다.

- OpenShift Dedicated가 머신을 처음 시작하고 구성하기 위한 최초 부팅 시스템 구성으로 사용하는 Ignition
- 운영 체제와 밀접하게 통합되어 효율적이고 최적화된 Kubernetes 환경을 제공하는 Kubernetes 기본 컨테이너 런타임 구현인 CRI-O. CRI-O는 컨테이너 실행, 중지 및 다시 시작 기능을 제공합니다.
- 컨테이너 시작 및 모니터링을 담당하는 Kubernetes의 기본 노드 에이전트인 Kubelet

1.1.2. 기타 주요 기능

Operator는 OpenShift Dedicated 코드 베이스의 기본 단위이자 애플리케이션 및 애플리케이션에서 사용할 소프트웨어 구성 요소를 편리하게 배포할 수 있는 방법입니다. OpenShift Dedicated에서 Operator는 플랫폼 기반 역할을 하며 운영 체제 및 컨트롤 플레인 애플리케이션을 수동으로 업그레이드할 필요가 없습니다. Cluster Version Operator 및 Machine Config Operator와 같은 OpenShift Dedicated Operator를 사용하면 중요한 구성 요소를 클러스터 전체로 관리할 수 있습니다.

OLM(Operator Lifecycle Manager)과 OperatorHub에서는 애플리케이션을 개발 및 배포하는 사용자에게 Operator를 저장하고 배포하는 기능을 제공합니다.

Red Hat Quay Container Registry는 대부분의 컨테이너 이미지와 Operator를 OpenShift Dedicated 클러스터에 제공하는 Quay.io 컨테이너 레지스트리입니다. Quay.io는 수백만 개의 이미지와 태그를 저장하는 Red Hat Quay의 공개 레지스트리 버전입니다.

OpenShift Dedicated의 Kubernetes의 기타 개선 사항에는 소프트웨어 정의 네트워킹(SDN), 인증, 로그 집계, 모니터링 및 라우팅 개선 사항이 포함됩니다. OpenShift Dedicated에서는 포괄적인 웹 콘솔 및 사용자 정의 OpenShift CLI(**oc**) 인터페이스도 제공합니다.

1.1.3. OpenShift Dedicated에 대한 인터넷 및 Telemetry 액세스

OpenShift Dedicated에서 클러스터를 설치하고 업그레이드하려면 인터넷 액세스가 필요합니다.

Telemetry 서비스를 통해 서브스크립션 관리 자동화를 활성화하고 클러스터 상태를 모니터링하고, 지원 및 고객 환경을 개선하기 위해 OpenShift Dedicated 클러스터에서 Red Hat으로 정보가 전송됩니다.

Telemetry 서비스는 자동으로 실행되며 클러스터가 Red Hat OpenShift Cluster Manager에 등록됩니다. OpenShift Dedicated에서는 원격 상태 보고가 항상 활성화되어 있으며 옵트아웃할 수 없습니다. Red Hat SRE(Site Reliability Engineering) 팀에서는 OpenShift Dedicated 클러스터에 대한 효과적인 지원을 제공하기 위해 정보가 필요합니다.

추가 리소스

- OpenShift Dedicated 클러스터의 Telemetry 및 원격 상태 모니터링에 대한 자세한 내용은 원격 상태 모니터링정보를 참조하십시오.

2장. 정책 및 서비스 정의

2.1. OPENSHIFT DEDICATED 서비스 정의

2.1.1. 계정 관리

2.1.1.1. 청구 옵션

고객은 OSD(OpenShift Dedicated)의 연간 서브스크립션을 구입하거나 클라우드 마켓플레이스를 통해 온디맨드로 사용할 수 있는 옵션이 있습니다. 고객은 고객 클라우드 서브스크립션(CCS)이라는 자체 클라우드 인프라 계정을 가져오거나 Red Hat이 소유한 클라우드 공급자 계정에 배포할 수 있습니다. 아래 표에서는 청구 및 지원되는 배포 옵션에 대한 추가 정보를 제공합니다.

OSD 서브스크립션 유형	클라우드 인프라 계정	청구됨
Red Hat을 통한 연간 고정 용량 서브스크립션	Red Hat 클라우드 계정	OSD 서브스크립션 및 클라우드 인프라 모두에 사용되는 Red Hat
	고객의 클라우드 계정	OSD 서브스크립션 사용을 위해 Red Hat 클라우드 인프라 사용을 위한 클라우드 공급자
Google Cloud Marketplace를 통한 온디맨드 사용 기반 사용	고객의 Google Cloud 계정	클라우드 인프라 및 Red Hat OSD 서브스크립션 모두를 위한 Google Cloud
Red Hat Marketplace를 통한 온디맨드 사용량 기반 사용	고객의 클라우드 계정	OSD 서브스크립션 사용을 위해 Red Hat 클라우드 인프라 사용을 위한 클라우드 공급자

중요

CSS(Customer Cloud Subscription)라고 하는 자체 클라우드 인프라 계정을 사용하는 고객은 클라우드 인프라 비용을 줄이기 위해 예약된 인스턴스(RI) 컴퓨팅 인스턴스를 사전 구매하거나 제공해야 합니다.

다음을 포함하여 OpenShift Dedicated 클러스터에 대한 추가 리소스를 구입할 수 있습니다.

- 추가 노드 (머신 풀을 사용하여 다른 유형 및 크기일 수 있음)
- Middleware(JBoss EAP, JBoss Fuse 등) - 특정 미들웨어 구성 요소에 따른 추가 가격
- 500GB 단위로의 추가 저장 공간(표준만 해당, 100GB 포함)
- 추가 12TiB 네트워크 I/O (표준 12TB 포함)

- 서비스용 로드 밸런서는 4 번들에서 사용할 수 있습니다. HTTP/SNI 트래픽 또는 비표준 포트(표준 전용)를 활성화합니다.

2.1.1.2. 클러스터 셀프 서비스

고객은 필요한 서브스크립션을 이미 구매한 경우 OpenShift Cluster Manager 에서 클러스터를 생성, 확장 및 삭제할 수 있습니다.

Red Hat OpenShift Cluster Manager에서 사용 가능한 작업은 클러스터 내에서 직접 수행할 수 없습니다. 이로 인해 모든 작업이 자동으로 되돌아가는 것을 포함하여 불리한 영향을 미칠 수 있습니다.

2.1.1.3. 클라우드 공급자

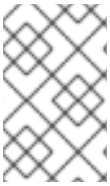
OpenShift Dedicated는 다음 클라우드 공급자에서 OpenShift Container Platform 클러스터를 관리형 서비스로 제공합니다.

- AWS(Amazon Web Services)
- GCP(Google Cloud Platform)

2.1.1.4. 인스턴스 유형

단일 가용성 영역 클러스터에는 단일 가용성 영역에 배포된 고객 클라우드 서브스크립션(CCS) 클러스터에 최소 2개의 작업자 노드가 필요합니다. 표준 클러스터에는 최소 4개의 작업자 노드가 필요합니다. 이 4개의 작업자 노드는 기본 서브스크립션에 포함되어 있습니다.

여러 가용성 영역 클러스터에는 각각 3개의 가용성 영역에 배포된 고객 클라우드 서브스크립션(CCS) 클러스터에 최소 3개의 작업자 노드가 필요합니다. 표준 클러스터에는 최소 9개의 작업자 노드가 필요합니다. 이 9개의 작업자 노드는 기본 서브스크립션에 포함되어 있으며 적절한 노드 배포를 유지하려면 추가 노드를 3의 다중에서 구입해야 합니다.



참고

단일 OpenShift Dedicated 머신 풀 내의 모든 작업자 노드는 동일한 유형과 크기여야 합니다. 그러나 OpenShift Dedicated 클러스터 내의 여러 머신 풀의 작업자 노드는 다양한 유형과 크기일 수 있습니다.

컨트롤 플레인 및 인프라 노드도 Red Hat에서 제공합니다. etcd 및 API 관련 워크로드를 처리하는 컨트롤 플레인 노드가 3개 이상 있습니다. 메트릭, 라우팅, 웹 콘솔 및 기타 워크로드를 처리하는 인프라 노드가 두 개 이상 있습니다. 컨트롤 플레인 및 인프라 노드에서 워크로드를 실행하지 않아야 합니다. 실행하려는 워크로드는 작업자 노드에 배포해야 합니다. 작업자 노드에 배포해야 하는 Red Hat 워크로드에 대한 자세한 내용은 아래 Red Hat Operator 지원 섹션을 참조하십시오.

참고

약 1 vCPU 코어 및 1GiB의 메모리는 각 작업자 노드에 예약되며 할당 가능한 리소스에서 제거됩니다. 이는 기본 플랫폼에서 요구하는 프로세스를 실행하는 데 필요합니다. 여기에는 udev, kubelet, 컨테이너 런타임 등과 같은 시스템 데몬과 커널 예약 계정이 포함됩니다. 감사 로그 집계, 지표 수집, DNS, 이미지 레지스트리, SDN 등과 같은 OpenShift Container Platform 코어 시스템은 클러스터의 안정성과 유지 관리를 위해 추가 할당 가능한 리소스를 사용할 수 있습니다. 소비되는 추가 리소스는 사용량에 따라 다를 수 있습니다.

중요

OpenShift Dedicated 4.11부터 기본 Pod당 PID 제한은 **4096** 입니다. 이 PID 제한을 활성화하려면 OpenShift Dedicated 클러스터를 이 버전 이상으로 업그레이드해야 합니다. 4.11 이전 버전을 실행하는 OpenShift Dedicated 클러스터는 기본 PID 제한을 **1024** 로 제한합니다.

OpenShift Dedicated 클러스터에서는 Pod별 PID 제한을 구성할 수 없습니다.

추가 리소스

- Red Hat Operator 지원

2.1.1.5. Customer Cloud Subscription 클러스터의 AWS 인스턴스 유형

OpenShift Dedicated는 AWS에서 다음과 같은 작업자 노드 인스턴스 유형 및 크기를 제공합니다.

예 2.1. 일반 목적

- m5.metal (96ovn vCPU, 384GiB)
- m5.xlarge (4 vCPU, 16GiB)
- m5.2xlarge (8 vCPU, 32GiB)
- m5.4xlarge (16 vCPU, 64GiB)
- m5.8xlarge(32 vCPU, 128GiB)
- m5.12xlarge(48 vCPU, 192GiB)
- m5.16xlarge(64 vCPU, 256GiB)
- m5.24xlarge (96 vCPU, 384GiB)
- m5a.xlarge (4 vCPU, 16GiB)
- m5a.2xlarge (8 vCPU, 32GiB)
- m5a.4xlarge (16 vCPU, 64GiB)
- m5a.8xlarge(32 vCPU, 128GiB)
- m5a.12xlarge(48 vCPU, 192GiB)
- m5a.16xlarge(64 vCPU, 256GiB)
- m5a.24xlarge (96 vCPU, 384GiB)
- m5ad.xlarge (4 vCPU, 16GiB)
- m5ad.2xlarge (8 vCPU, 32GiB)
- m5ad.4xlarge (16 vCPU, 64GiB)
- m5ad.8xlarge(32 vCPU, 128GiB)

- m5ad.12xlarge (48 vCPU, 192GiB)
- m5ad.16xlarge (64 vCPU, 256GiB)
- m5ad.24xlarge (96 vCPU, 384GiB)
- m5d.metal (96ovn vCPU, 384GiB)
- m5d.xlarge (4 vCPU, 16GiB)
- m5d.2xlarge (8 vCPU, 32GiB)
- m5d.4xlarge (16 vCPU, 64GiB)
- m5d.8xlarge(32 vCPU, 128GiB)
- m5d.12xlarge(48 vCPU, 192GiB)
- m5d.16xlarge(64 vCPU, 256GiB)
- m5d.24xlarge(96 vCPU, 384GiB)
- m5n.metal (96 vCPU, 384GiB)
- m5n.xlarge (4 vCPU, 16GiB)
- m5n.2xlarge (8 vCPU, 32GiB)
- m5n.4xlarge (16 vCPU, 64GiB)
- m5n.8xlarge(32 vCPU, 128GiB)
- m5n.12xlarge(48 vCPU, 192GiB)
- m5n.16xlarge(64 vCPU, 256GiB)
- m5n.24xlarge (96 vCPU, 384GiB)
- m5dn.metal (96 vCPU, 384GiB)
- m5dn.xlarge (4 vCPU, 16GiB)
- m5dn.2xlarge (8 vCPU, 32GiB)
- m5dn.4xlarge (16 vCPU, 64GiB)
- m5dn.8xlarge(32 vCPU, 128GiB)
- m5dn.12xlarge(48 vCPU, 192GiB)
- m5dn.16xlarge(64 vCPU, 256GiB)
- m5dn.24xlarge (96 vCPU, 384GiB)
- m5zn.metal (48 vCPU, 192GiB)
- m5zn.xlarge (4 vCPU, 16GiB)

- m5zn.2xlarge (8 vCPU, 32GiB)
- m5zn.3xlarge (12 vCPU, 48GiB)
- m5zn.6xlarge (24 vCPU, 96GiB)
- m5zn.12xlarge (48 vCPU, 192GiB)
- m6a.xlarge (4 vCPU, 16GiB)
- m6a.2xlarge (8 vCPU, 32GiB)
- m6a.4xlarge (16 vCPU, 64GiB)
- m6a.8xlarge(32 vCPU, 128GiB)
- m6a.12xlarge(48 vCPU, 192GiB)
- m6a.16xlarge(64 vCPU, 256GiB)
- m6a.24xlarge (96 vCPU, 384GiB)
- m6a.32xlarge(128 vCPU, 512GiB)
- m6a.48xlarge(192 vCPU, 768GiB)
- m6i.metal (128 vCPU, 512GiB)
- m6i.xlarge (4 vCPU, 16GiB)
- m6i.2xlarge (8 vCPU, 32GiB)
- m6i.4xlarge (16 vCPU, 64GiB)
- m6i.8xlarge(32 vCPU, 128GiB)
- m6i.12xlarge (48 vCPU, 192GiB)
- m6i.16xlarge(64 vCPU, 256GiB)
- m6i.24xlarge (96 vCPU, 384GiB)
- m6i.32xlarge(128 vCPU, 512GiB)
- m6id.xlarge (4 vCPU, 16GiB)
- m6id.2xlarge (8 vCPU, 32GiB)
- m6id.4xlarge (16 vCPU, 64GiB)
- m6id.8xlarge(32 vCPU, 128GiB)
- m6id.12xlarge (48 vCPU, 192GiB)
- m6id.16xlarge (64 vCPU, 256GiB)
- m6id.24xlarge (96 vCPU, 384GiB)

- m6id.32xlarge(128 vCPU, 512GiB)
- m7i.xlarge (4 vCPU, 16GiB)
- m7i.2xlarge (8 vCPU, 32GiB)
- m7i.4xlarge (16 vCPU, 64GiB)
- m7i.8xlarge(32 vCPU, 128GiB)
- m7i.12xlarge (48 vCPU, 192GiB)
- m7i.16xlarge (64 vCPU, 256GiB)
- m7i.24xlarge (96 vCPU, 384GiB)
- m7i.48xlarge (192 vCPU, 768GiB)
- m7i.metal-24xl (96 vCPU, 384GiB)
- m7i.metal-48xl (192 vCPU, 768GiB)
- m7i-flex.xlarge (4 vCPU, 16GiB)
- m7i-flex.2xlarge (8 vCPU, 32GiB)
- m7i-flex.4xlarge (16 vCPU, 64GiB)
- m7i-flex.8xlarge(32 vCPU, 128GiB)
- m7a.xlarge (4 vCPU, 16GiB)
- m7a.2xlarge (8 vCPU, 32GiB)
- m7a.4xlarge (16 vCPU, 64GiB)
- m7a.8xlarge(32 vCPU, 128GiB)
- m7a.12xlarge (48 vCPU, 192GiB)
- m7a.16xlarge (64 vCPU, 256GiB)
- m7a.24xlarge (96 vCPU, 384GiB)
- m7a.32xlarge(128 vCPU, 512GiB)
- m7a.48xlarge (192 vCPU, 768GiB)
- m7a.metal-48xl (192 vCPU, 768GiB)

이러한 인스턴스 유형은 48개의 물리적 코어에서 96개의 논리 프로세서를 제공합니다. 두 개의 물리적 Intel 소켓이 있는 단일 서버에서 실행됩니다.

예 2.2. Burstable 일반 목적

- t3.xlarge (4 vCPU, 16GiB)

- t3.2xlarge (8 vCPU, 32GiB)
- t3a.xlarge (4 vCPU, 16GiB)
- t3a.2xlarge (8 vCPU, 32GiB)

예 2.3. 메모리 집약적

- x1.16xlarge(64 vCPU, 976GiB)
- X1.32xlarge(128 vCPU, 1952GiB)
- X1e.xlarge (4 vCPU, 122GiB)
- X1e.2xlarge (8 vCPU, 244GiB)
- X1e.4xlarge (16 vCPU, 488GiB)
- X1e.8xlarge(32 vCPU, 976GiB)
- X1e.16xlarge(64 vCPU, 1,952GiB)
- X1e.32xlarge(128 vCPU, 3,904GiB)
- x2idn.16xlarge (64 vCPU, 1024GiB)
- X2idn.24xlarge (96 vCPU, 1536GiB)
- x2idn.32xlarge(128 vCPU, 2048GiB)
- x2iedn.xlarge (4 vCPU, 128GiB)
- X2iedn.2xlarge (8 vCPU, 256GiB)
- X2iedn.4xlarge (16 vCPU, 512GiB)
- X2iedn.8xlarge(32 vCPU, 1024GiB)
- x2iedn.16xlarge (64 vCPU, 2048GiB)
- X2iedn.24xlarge (96 vCPU, 3072GiB)
- x2iedn.32xlarge(128 vCPU, 4096GiB)
- X2iezn.2xlarge (8 vCPU, 256GiB)
- X2iezn.4xlarge (16vCPU, 512GiB)
- X2iezn.6xlarge (24vCPU, 768GiB)
- X2iezn.8xlarge(32vCPU, 1,024GiB)
- X2iezn.12xlarge (48vCPU, 1,536GiB)
- x2idn.metal(128vCPU, 2,048GiB)
- x2iedn.metal (128vCPU, 4,096GiB)

- x2iezn.metal (48 vCPU, 1,536GiB)

예 2.4. 최적화된 메모리

- r4.xlarge (4 vCPU, 30.5GiB)
- r4.2xlarge (8 vCPU, 61GiB)
- r4.4xlarge (16 vCPU, 122GiB)
- r4.8xlarge(32 vCPU, 244GiB)
- r4.16xlarge(64 vCPU, 488GiB)
- r5.metal (96ECDHE vCPU, 768GiB)
- r5.xlarge (4 vCPU, 32GiB)
- r5.2xlarge (8 vCPU, 64GiB)
- r5.4xlarge (16 vCPU, 128GiB)
- r5.8xlarge(32 vCPU, 256GiB)
- r5.12xlarge (48 vCPU, 384GiB)
- r5.16xlarge(64 vCPU, 512GiB)
- r5.24xlarge (96 vCPU, 768GiB)
- r5a.xlarge (4 vCPU, 32GiB)
- r5a.2xlarge (8 vCPU, 64GiB)
- r5a.4xlarge (16 vCPU, 128GiB)
- r5a.8xlarge(32 vCPU, 256GiB)
- r5a.12xlarge(48 vCPU, 384GiB)
- r5a.16xlarge(64 vCPU, 512GiB)
- r5a.24xlarge(96 vCPU, 768GiB)
- r5ad.xlarge (4 vCPU, 32GiB)
- r5ad.2xlarge (8 vCPU, 64GiB)
- r5ad.4xlarge (16 vCPU, 128GiB)
- r5ad.8xlarge(32 vCPU, 256GiB)
- r5ad.12xlarge(48 vCPU, 384GiB)
- r5ad.16xlarge(64 vCPU, 512GiB)
- r5ad.24xlarge (96 vCPU, 768GiB)

- r5d.metal (96ECDHE vCPU, 768GiB)
- r5d.xlarge (4 vCPU, 32GiB)
- r5d.2xlarge (8 vCPU, 64GiB)
- r5d.4xlarge (16 vCPU, 128GiB)
- r5d.8xlarge(32 vCPU, 256GiB)
- r5d.12xlarge(48 vCPU, 384GiB)
- r5d.16xlarge(64 vCPU, 512GiB)
- r5d.24xlarge(96 vCPU, 768GiB)
- r5n.metal (96 vCPU, 768GiB)
- r5n.xlarge (4 vCPU, 32GiB)
- r5n.2xlarge (8 vCPU, 64GiB)
- r5n.4xlarge (16 vCPU, 128GiB)
- r5n.8xlarge(32 vCPU, 256GiB)
- r5n.12xlarge(48 vCPU, 384GiB)
- r5n.16xlarge(64 vCPU, 512GiB)
- r5n.24xlarge (96 vCPU, 768GiB)
- r5dn.metal (96 vCPU, 768GiB)
- r5dn.xlarge (4 vCPU, 32GiB)
- r5dn.2xlarge (8 vCPU, 64GiB)
- r5dn.4xlarge (16 vCPU, 128GiB)
- r5dn.8xlarge(32 vCPU, 256GiB)
- r5dn.12xlarge(48 vCPU, 384GiB)
- r5dn.16xlarge(64 vCPU, 512GiB)
- r5dn.24xlarge (96 vCPU, 768GiB)
- r6a.xlarge (4 vCPU, 32GiB)
- r6a.2xlarge (8 vCPU, 64GiB)
- r6a.4xlarge (16 vCPU, 128GiB)
- r6a.8xlarge(32 vCPU, 256GiB)
- r6a.12xlarge(48 vCPU, 384GiB)

- r6a.16xlarge(64 vCPU, 512GiB)
- r6a.24xlarge (96 vCPU, 768GiB)
- r6a.32xlarge(128 vCPU, 1,024GiB)
- r6a.48xlarge(192 vCPU, 1,536GiB)
- r6i.metal (128 vCPU, 1,024GiB)
- r6i.xlarge (4 vCPU, 32GiB)
- r6i.2xlarge (8 vCPU, 64GiB)
- r6i.4xlarge (16 vCPU, 128GiB)
- r6i.8xlarge(32 vCPU, 256GiB)
- r6i.12xlarge(48 vCPU, 384GiB)
- r6i.16xlarge(64 vCPU, 512GiB)
- r6i.24xlarge (96 vCPU, 768GiB)
- r6i.32xlarge(128 vCPU, 1,024GiB)
- r6id.xlarge (4 vCPU, 32GiB)
- r6id.2xlarge (8 vCPU, 64GiB)
- r6id.4xlarge (16 vCPU, 128GiB)
- r6id.8xlarge(32 vCPU, 256GiB)
- r6id.12xlarge (48 vCPU, 384GiB)
- r6id.16xlarge (64 vCPU, 512GiB)
- r6id.24xlarge (96 vCPU, 768GiB)
- r6id.32xlarge(128 vCPU, 1,024GiB)
- z1d.metal (48ECDHE vCPU, 384GiB)
- z1d.xlarge (4 vCPU, 32GiB)
- z1d.2xlarge (8 vCPU, 64GiB)
- z1d.3xlarge (12 vCPU, 96GiB)
- z1d.6xlarge (24 vCPU, 192GiB)
- z1d.12xlarge(48 vCPU, 384GiB)
- r7iz.xlarge (4 vCPU, 32GiB)
- r7iz.2xlarge (8 vCPU, 64GiB)

- r7iz.4xlarge (16 vCPU, 128GiB)
- r7iz.8xlarge(32 vCPU, 256GiB)
- r7iz.12xlarge (48 vCPU, 384GiB)
- r7iz.16xlarge (64 vCPU, 512GiB)
- r7iz.32xlarge(128 vCPU, 1024GiB)
- r7iz.metal-16xl (64 vCPU, 512GiB)
- r7iz.metal-32xl (128 vCPU, 1024GiB)

이러한 인스턴스 유형은 48개의 물리적 코어에서 96개의 논리 프로세서를 제공합니다. 두 개의 물리적 Intel 소켓이 있는 단일 서버에서 실행됩니다.

이 인스턴스 유형은 24개의 물리적 코어에서 48개의 논리 프로세서를 제공합니다.

예 2.5. 가속화된 컴퓨팅

- p3.2xlarge (8 vCPU, 61GiB)
- p3.8xlarge(32 vCPU, 244GiB)
- p3.16xlarge(64 vCPU, 488GiB)
- p3dn.24xlarge (96 vCPU, 768GiB)
- p4d.24xlarge(96 vCPU, 1,152GiB)
- p4de.24xlarge (96 vCPU, 1,152GiB)
- p5.48xlarge(192 vCPU, 2,048GiB)
- g4dn.xlarge (4 vCPU, 16GiB)
- g4dn.2xlarge (8 vCPU, 32GiB)
- g4dn.4xlarge (16 vCPU, 64GiB)
- g4dn.8xlarge(32 vCPU, 128GiB)
- g4dn.12xlarge(48 vCPU, 192GiB)
- g4dn.16xlarge(64 vCPU, 256GiB)
- g4dn.metal (96 vCPU, 384GiB)
- g5.xlarge (4 vCPU, 16GiB)
- g5.2xlarge (8 vCPU, 32GiB)
- g5.4xlarge (16 vCPU, 64GiB)
- g5.8xlarge(32 vCPU, 128GiB)

- g5.16xlarge(64 vCPU, 256GiB)
- g5.12xlarge(48 vCPU, 192GiB)
- g5.24xlarge(96 vCPU, 384GiB)
- g5.48xlarge(192 vCPU, 768GiB)
- dl1.24xlarge (96 vCPU, 768GiB)

ECDHE Intel specific; Nvidia의 적용을 받지 않음

AWS에서는 GPU 인스턴스 유형 소프트웨어 스택에 대한 지원이 제공됩니다. AWS 서비스 할당량이 원하는 GPU 인스턴스 유형을 수용할 수 있는지 확인합니다.

예 2.6. 컴퓨팅 최적화

- c5.metal (96 vCPU, 192GiB)
- c5.xlarge (4 vCPU, 8GiB)
- c5.2xlarge (8 vCPU, 16GiB)
- c5.4xlarge (16 vCPU, 32GiB)
- c5.9xlarge(36 vCPU, 72GiB)
- c5.12xlarge(48 vCPU, 96GiB)
- c5.18xlarge (72 vCPU, 144GiB)
- c5.24xlarge (96 vCPU, 192GiB)
- c5d.metal (96 vCPU, 192GiB)
- c5d.xlarge (4 vCPU, 8GiB)
- c5d.2xlarge (8 vCPU, 16GiB)
- c5d.4xlarge (16 vCPU, 32GiB)
- c5d.9xlarge(36 vCPU, 72GiB)
- c5d.12xlarge(48 vCPU, 96GiB)
- c5d.18xlarge(72 vCPU, 144GiB)
- c5d.24xlarge (96 vCPU, 192GiB)
- c5a.xlarge (4 vCPU, 8GiB)
- c5a.2xlarge (8 vCPU, 16GiB)
- c5a.4xlarge (16 vCPU, 32GiB)
- c5a.8xlarge(32 vCPU, 64GiB)

- c5a.12xlarge(48 vCPU, 96GiB)
- c5a.16xlarge(64 vCPU, 128GiB)
- c5a.24xlarge (96 vCPU, 192GiB)
- c5ad.xlarge (4 vCPU, 8GiB)
- c5ad.2xlarge (8 vCPU, 16GiB)
- c5ad.4xlarge (16 vCPU, 32GiB)
- c5ad.8xlarge(32 vCPU, 64GiB)
- c5ad.12xlarge(48 vCPU, 96GiB)
- c5ad.16xlarge (64 vCPU, 128GiB)
- c5ad.24xlarge (96 vCPU, 192GiB)
- c5n.metal (72 vCPU, 192GiB)
- c5n.xlarge (4 vCPU, 10.5GiB)
- c5n.2xlarge (8 vCPU, 21GiB)
- c5n.4xlarge (16 vCPU, 42GiB)
- c5n.9xlarge(36 vCPU, 96GiB)
- c5n.18xlarge (72 vCPU, 192GiB)
- c6a.xlarge (4 vCPU, 8GiB)
- c6a.2xlarge (8 vCPU, 16GiB)
- c6a.4xlarge (16 vCPU, 32GiB)
- c6a.8xlarge(32 vCPU, 64GiB)
- c6a.12xlarge(48 vCPU, 96GiB)
- c6a.16xlarge(64 vCPU, 128GiB)
- c6a.24xlarge (96 vCPU, 192GiB)
- c6a.32xlarge(128 vCPU, 256GiB)
- c6a.48xlarge(192 vCPU, 384GiB)
- c6i.metal (128 vCPU, 256GiB)
- c6i.xlarge (4 vCPU, 8GiB)
- c6i.2xlarge (8 vCPU, 16GiB)
- c6i.4xlarge (16 vCPU, 32GiB)

- c6i.8xlarge(32 vCPU, 64GiB)
- c6i.12xlarge (48 vCPU, 96GiB)
- c6i.16xlarge (64 vCPU, 128GiB)
- c6i.24xlarge (96 vCPU, 192GiB)
- c6i.32xlarge(128 vCPU, 256GiB)
- c6id.xlarge (4 vCPU, 8GiB)
- c6id.2xlarge (8 vCPU, 16GiB)
- c6id.4xlarge (16 vCPU, 32GiB)
- c6id.8xlarge(32 vCPU, 64GiB)
- c6id.12xlarge (48 vCPU, 96GiB)
- c6id.16xlarge (64 vCPU, 128GiB)
- c6id.24xlarge (96 vCPU, 192GiB)
- c6id.32xlarge(128 vCPU, 256GiB)

예 2.7. 최적화된 스토리지

- i3.metal (72ECDHE vCPU, 512GiB)
- i3.xlarge (4 vCPU, 30.5GiB)
- i3.2xlarge (8 vCPU, 61GiB)
- i3.4xlarge (16 vCPU, 122GiB)
- i3.8xlarge(32 vCPU, 244GiB)
- i3.16xlarge(64 vCPU, 488GiB)
- i3en.metal (96 vCPU, 768GiB)
- i3en.xlarge (4 vCPU, 32GiB)
- i3en.2xlarge (8 vCPU, 64GiB)
- i3en.3xlarge (12 vCPU, 96GiB)
- i3en.6xlarge (24 vCPU, 192GiB)
- i3en.12xlarge(48 vCPU, 384GiB)
- i3en.24xlarge (96 vCPU, 768GiB)
- i4i.xlarge (4 vCPU, 32GiB)
- i4i.2xlarge (8 vCPU, 64GiB)

- i4i.4xlarge (16 vCPU, 128GiB)
- i4i.8xlarge(32 vCPU, 256GiB)
- i4i.12xlarge (48 vCPU, 384GiB)
- i4i.16xlarge (64 vCPU, 512GiB)
- i4i.24xlarge (96 vCPU, 768GiB)
- i4i.32xlarge(128 vCPU, 1024GiB)
- i4i.metal(128 vCPU, 1024GiB)

이 인스턴스 유형은 36 개의 물리적 코어에서 72 개의 논리 프로세서를 제공합니다.

참고

가상 인스턴스 유형은 ".metal" 인스턴스 유형보다 더 빨리 초기화됩니다.

예 2.8. 높은 메모리

- U-3tb1.56xlarge (224 vCPU, 3,072GiB)
- U-6tb1.56xlarge (224 vCPU, 6,144GiB)
- U-6tb1.112xlarge (448 vCPU, 6,144GiB)
- U-6tb1.metal (448 vCPU, 6,144GiB)
- U-9tb1.112xlarge (448 vCPU, 9,216GiB)
- U-9tb1.metal (448 vCPU, 9,216GiB)
- U-12tb1.112xlarge (448 vCPU, 12,288GiB)
- U-12tb1.metal (448 vCPU, 12,288GiB)
- U-18tb1.metal (448 vCPU, 18,432GiB)
- U-24tb1.metal (448 vCPU, 24,576GiB)

추가 리소스

- AWS 인스턴스 유형

2.1.1.6. 표준 클러스터의 AWS 인스턴스 유형

OpenShift Dedicated는 AWS에서 다음과 같은 작업자 노드 유형 및 크기를 제공합니다.

예 2.9. 일반 목적

- m5.xlarge (4 vCPU, 16GiB)

- m5.2xlarge (8 vCPU, 32GiB)
- m5.4xlarge (16 vCPU, 64GiB)

예 2.10. 메모리 최적화

- r5.xlarge (4 vCPU, 32GiB)
- r5.2xlarge (8 vCPU, 64GiB)
- r5.4xlarge (16 vCPU, 128GiB)

예 2.11. compute- optimization

- c5.2xlarge (8 vCPU, 16GiB)
- c5.4xlarge (16 vCPU, 32GiB)

2.1.1.7. Google Cloud 컴퓨팅 유형

OpenShift Dedicated는 다른 클라우드 인스턴스 유형과 동일한 공통 CPU 및 메모리 용량을 가지도록 선택한 Google Cloud에서 다음과 같은 작업자 노드 유형과 크기를 제공합니다.

참고

e2 및 **a2** 컴퓨팅 유형은 CCS에서만 사용할 수 있습니다.

예 2.12. 일반 목적

- Custom-4-16384 (4 vCPU, 16GiB)
- Custom-8-32768 (8 vCPU, 32GiB)
- custom-16-65536 (16 vCPU, 64GiB)
- custom-32-131072(32 vCPU, 128GiB)
- custom-48-199608 (48 vCPU, 192GiB)
- custom-64-262144 (64 vCPU, 256GiB)
- custom-96-393216 (96 vCPU, 384GiB)
- e2-standard-4 (4 vCPU, 16GiB)
- n2-standard-4 (4 vCPU, 16GiB)
- e2-standard-8 (8 vCPU, 32GiB)
- n2-standard-8 (8 vCPU, 32GiB)
- e2-standard-16 (16 vCPU, 64GiB)

- n2-standard-16 (16 vCPU, 64GiB)
- e2-standard-32(32 vCPU, 128GiB)
- n2-standard-32(32 vCPU, 128GiB)
- n2-standard-48 (48 vCPU, 192GiB)
- n2-standard-64 (64 vCPU, 256GiB)
- n2-standard-80 (80 vCPU, 320GiB)
- n2-standard-96 (96 vCPU, 384GiB)
- n2-standard-128(128 vCPU, 512GiB)

예 2.13. 메모리 최적화

- custom-4-32768-ext (4 vCPU, 32GiB)
- custom-8-65536-ext (8 vCPU, 64GiB)
- custom-16-131072-ext (16 vCPU, 128GiB)
- e2-highmem-4 (4 vCPU, 32GiB)
- e2-highmem-8 (8 vCPU, 64GiB)
- e2-highmem-16 (16 vCPU, 128GiB)
- n2-highmem-4 (vCPU, 32GiB)
- n2-highmem-8 (8 vCPU, 64GiB)
- n2-highmem-16 (16 vCPU, 128GiB)
- n2-highmem-32(32 vCPU, 256GiB)
- n2-highmem-48 (48 vCPU, 384GiB)
- n2-highmem-64 (64 vCPU, 512GiB)
- n2-highmem-80 (80 vCPU, 640GiB)
- n2-highmem-96 (96 vCPU, 768GiB)
- n2-highmem-128(128 vCPU, 864GiB)

예 2.14. compute- optimization

- Custom-8-16384 (8 vCPU, 16GiB)
- custom-16-32768(16 vCPU, 32GiB)
- custom-36-73728 (36 vCPU, 72GiB)

- custom-48-98304 (48 vCPU, 96GiB)
- custom-72-147456 (72 vCPU, 144GiB)
- custom-96-196608 (96 vCPU, 192GiB)
- c2-standard-4 (4 vCPU, 16GiB)
- c2-standard-8 (8 vCPU, 32GiB)
- c2-standard-16 (16 vCPU, 64GiB)
- c2-standard-30 (30 vCPU, 120GiB)
- c2-standard-60 (60 vCPU, 240GiB)
- e2-highcpu-8 (8 vCPU, 8GiB)
- e2-highcpu-16 (16 vCPU, 16GiB)
- e2-highcpu-32(32 vCPU, 32GiB)
- n2-highcpu-8 (8 vCPU, 8GiB)
- n2-highcpu-16 (16 vCPU, 16GiB)
- n2-highcpu-32(32 vCPU, 32GiB)
- n2-highcpu-48 (48 vCPU, 48GiB)
- n2-highcpu-64 (64 vCPU, 64GiB)
- n2-highcpu-80 (80 vCPU, 80GiB)
- n2-highcpu-96 (96 vCPU, 96GiB)

예 2.15. 가속화된 컴퓨팅

- a2-highgpu-1g (12 vCPU, 85GiB)
- A2-highgpu-2g (24 vCPU,170 GiB)
- a2-highgpu-4g (48 vCPU, 340GiB)
- a2-highgpu-8g (96 vCPU, 680GiB)
- a2-megagpu-16g (96 vCPU, 1.33 TiB)
- a2-ultragpu-1g (12 vCPU,170 GiB)
- a2-ultragpu-2g (24 vCPU, 340GiB)
- a2-ultragpu-4g (48 vCPU, 680GiB)
- a2-ultragpu-8g (96 vCPU, 1360GiB)

2.1.1.8. 지역 및 가용성 영역

다음 AWS 리전은 OpenShift Container Platform 4에서 지원되며 OpenShift Dedicated에서 지원됩니다.

- af-south-1 (AWS opt-in 필요)
- ap-east-1 (홍콩, AWS 옵트인 필요)
- ap-northeast-1(도쿄)
- ap-northeast-2(서울)
- ap-northeast-3 (오사카)
- ap-south-1(뭄바이)
- ap-south-2 (Hyderabad, AWS opt-in 필요)
- ap-southeast-1(싱가포르)
- ap-southeast-2(시드니)
- ap-southeast-3 (AWS 옵트인 필요)
- ap-southeast-4 (Melbourne, AWS 옵트인 필요)
- ca-central-1 (캐나다)
- eu-central-1(프랑크푸르트)
- eu-central-2(Zurich, AWS 옵트인 필요)
- eu-north-1(스톡홀름)
- eu-south-1 (AWS 옵트인 필요)
- eu-south-2 (스페인, AWS 옵트인 필요)
- eu-west-1(아일랜드)
- eu-west-2(런던)
- eu-west-3(파리)
- me-central-1(UAE, AWS 옵트인 필요)
- me-south-1 (Bahrain, AWS opt-in 필요)
- sa-east-1(상파울루)
- us-east-1(버지니아 북부)
- us-east-2(오하이오)
- us-west-1(캘리포니아 북부)
- us-west-2(오레곤)

현재 지원되는 Google Cloud 리전은 다음과 같습니다.

- asia-east1, Changhua County, Taiwan
- asia-east2, Hong Kong
- asia-northeast1, Tokyo, Japan
- asia-northeast2, Osaka, Japan
- asia-south1, Mumbai, India
- asia-south2, Delhi, India
- asia-southeast1, 싱가포르의 Jurong West
- australia-southeast1, Sydney, Australia
- australia-southeast2, 멜버른, 호주
- europe-north1, Hamina, Finland
- europe-west1, St. Ghislain, Belgium
- europe-west2, London, England, UK
- europe-west3, Frankfurt, Germany
- europe-west4, Eemshaven, Netherlands
- europe-west6, Zürich, Switzerland
- europe-west8, Milan, 이탈리아
- europe-west12, Turin, Italy
- europe-southwest1, Madrid, Spain
- northamerica-northeast1, Montréal, Québec, Canada
- southamerica-east1, Osasco (Sawo Paulo), 브라질
- southamerica-west1, Santiago, Chile
- us-central1, Council Bluffs, Iowa, USA
- us-east1, Moncks Corner, South Carolina, USA
- us-east4, Ashburn, Northern Virginia, USA
- us-west1, The Dalles, Oregon, USA
- us-west2, Los Angeles, California, USA
- me-central1, Doha, Qatar
- me-central2, Dammam, Saudi Arabia

다중 AZ 클러스터는 가용성 영역이 3개 이상인 리전에만 배포할 수 있습니다(AWS 및 Google Cloud 참조).

각 새로운 OpenShift Dedicated 클러스터는 단일 리전의 전용 VPC(Virtual Private Cloud) 내에 설치되며, 옵션은 단일 가용성 영역(Single-AZ) 또는 여러 가용 영역(Multi-AZ)에 배포할 수 있습니다. 이를 통해 클러스터 수준 네트워크 및 리소스 분리를 제공하고 VPN 연결 및 VPC 피어링과 같은 클라우드 공급자 VPC 설정을 활성화합니다. 영구 볼륨은 클라우드 블록 스토리지에서 지원되며 프로비저닝되는 가용성 영역에 따라 다릅니다. 영구 볼륨은 예약할 수 없는 Pod를 방지하기 위해 연결된 Pod 리소스가 특정 가용성 영역에 할당될 때까지 볼륨에 바인딩되지 않습니다. 가용성 영역별 리소스는 동일한 가용성 영역의 리소스에서만 사용할 수 있습니다.

주의

클러스터를 배포한 후에는 리전 및 단일 또는 다중 가용성 영역 선택 사항을 변경할 수 없습니다.

2.1.1.9. SLA(서비스 수준 계약)

서비스 자체에 대한 SLA는 Red Hat Enterprise Agreement 부록 4 (Online Subscription Services)의 부록 4 에 정의되어 있습니다.

2.1.1.10. 제한된 지원 상태

클러스터가 *제한된 지원* 상태로 전환되면 Red Hat은 더 이상 클러스터를 적극적으로 모니터링하지 않으며 SLA는 더 이상 적용되지 않으며 SLA에 대해 요청된 자립이 거부됩니다. 이는 더 이상 제품 지원이 없다는 의미는 아닙니다. 일부 경우 위반 요인을 수정하면 클러스터가 완전히 지원되는 상태로 돌아갈 수 있습니다. 그러나 다른 경우에는 클러스터를 삭제하고 다시 생성해야 할 수도 있습니다.

다음 시나리오를 포함하여 여러 가지 이유로 클러스터가 제한된 지원 상태로 전환될 수 있습니다.

라이프 사이클 종료일 전에 클러스터를 지원되는 버전으로 업그레이드하지 않는 경우

Red Hat은 라이프 사이클 종료일 이후 버전에 대해 런타임 또는 SLA를 보장하지 않습니다. 지속적인 지원을 받으려면 종료일 이전에 클러스터를 지원되는 버전으로 업그레이드하십시오. 라이프 사이클 종료일 이전에 클러스터를 업그레이드하지 않으면 클러스터가 지원되는 버전으로 업그레이드될 때까지 제한된 지원 상태로 전환됩니다.

Red Hat은 지원되지 않는 버전에서 지원되는 버전으로 업그레이드하기 위해 상업적으로 합리적인 지원을 제공합니다. 그러나 지원되는 업그레이드 경로를 더 이상 사용할 수 없는 경우 새 클러스터를 생성하고 워크로드를 마이그레이션해야 할 수 있습니다.

기본 OpenShift Dedicated 구성 요소 또는 Red Hat에서 설치 및 관리하는 기타 구성 요소를 제거하거나 교체하는 경우

클러스터 관리자 권한을 사용한 경우 Red Hat은 인프라 서비스, 서비스 가용성 또는 데이터 손실에 영향을 미치는 사용자 또는 사용자의 권한이 있는 사용자의 조치에 대해 책임을 지지 않습니다. Red Hat에서 이러한 작업을 감지하면 클러스터가 제한된 지원 상태로 전환될 수 있습니다. Red Hat은 상태 변경을 알리며 클러스터를 삭제하고 다시 생성해야 할 수 있는 수정 단계를 탐색할 수 있는 조치를 되돌리거나 지원 케이스를 생성해야 합니다.

클러스터가 제한된 지원 상태로 전환되거나 추가 지원이 필요한 특정 작업에 대한 질문이 있는 경우 지원 티켓을 엽니다.

2.1.1.11. 지원

OpenShift Dedicated에는 Red Hat 고객 포털을 사용하여 액세스할 수 있는 Red Hat 프리미엄 지원이 포함되어 있습니다.

OpenShift Dedicated에 대한 지원 관련 사항에 대한 자세한 내용은 지원 범위 페이지를 참조하십시오.

지원 응답 시간은 OpenShift Dedicated SLA 를 참조하십시오.

2.1.2. 로깅

OpenShift Dedicated는 AWS(Amazon Cloud Logging) 또는 GCP(Google Cloud Logging)에 대한 선택적 통합 로그 전달 기능을 제공합니다.

자세한 내용은 로그 수집 및 전달 정보를 참조하십시오.

2.1.2.1. 클러스터 감사 로깅

통합이 활성화된 경우 AWS의 Amazon Cloud Logging 또는 GCP의 Google Cloud Logging을 통해 클러스터 감사 로그를 사용할 수 있습니다. 통합이 활성화되지 않은 경우 지원 케이스를 열어 감사 로그를 요청할 수 있습니다. 감사 로그 요청은 21 일을 초과하지 않는 날짜 및 시간 범위를 지정해야 합니다. 감사 로그를 요청할 때 고객은 감사 로그의 크기가 하루에 최대GB임을 알고 있어야 합니다.

2.1.2.2. 애플리케이션 로깅

STDOUT 으로 전송된 애플리케이션 로그는 설치된 경우 클러스터 로깅 스택을 통해 AWS의 Amazon Cloud Logging 또는 Google Cloud Logging(Google Cloud Logging)으로 전달됩니다.

2.1.3. 모니터링

2.1.3.1. 클러스터 메트릭

OpenShift Dedicated 클러스터에는 CPU, 메모리 및 네트워크 기반 메트릭을 포함한 클러스터 모니터링을 위한 통합된 Prometheus/Grafana 스택이 제공됩니다. 웹 콘솔을 통해 액세스할 수 있으며 Grafana 대시보드를 통해 클러스터 수준 상태 및 용량/사용을 볼 수도 있습니다. 이러한 메트릭을 사용하면 OpenShift Dedicated 사용자가 제공하는 CPU 또는 메모리 메트릭을 기반으로 수평 Pod 자동 스케일링을 수행할 수 있습니다.

2.1.3.2. 클러스터 알림

클러스터 알림은 클러스터의 상태, 상태 또는 성능에 대한 메시지입니다.

클러스터 알림은 Red Hat site Reliability Engineering(SRE)이 관리형 클러스터의 상태에 대해 귀하와 통신하는 기본 방법입니다. SRE는 클러스터 알림을 사용하여 클러스터 문제를 해결하거나 방지하기 위해 작업을 수행하도록 요청할 수도 있습니다.

클러스터 소유자 및 관리자는 클러스터가 정상 상태로 유지되고 지원되는지 확인하기 위해 클러스터 알림을 정기적으로 검토하고 조치를 취해야 합니다.

클러스터의 클러스터 **기록 탭에서 Red Hat Hybrid Cloud Console에서 클러스터**알림을 볼 수 있습니다. 기본적으로 클러스터 소유자만 이메일로 클러스터 알림을 수신합니다. 다른 사용자가 클러스터 알림 이메일을 수신해야 하는 경우 각 사용자를 클러스터에 대한 알림 연락처로 추가합니다.

2.1.4. 네트워킹

2.1.4.1. 애플리케이션용 사용자 정의 도메인

주의

OpenShift Dedicated 4.14부터 Custom Domain Operator는 더 이상 사용되지 않습니다. OpenShift Dedicated 4.14 이상에서 Ingress를 관리하려면 Ingress Operator를 사용합니다. OpenShift Dedicated 4.13 및 이전 버전에서는 기능이 변경되지 않습니다.

경로에 사용자 지정 호스트 이름을 사용하려면 CNAME(정규 이름) 레코드를 생성하여 DNS 공급자를 업데이트해야 합니다. CNAME 레코드는 OpenShift 표준 라우터 호스트 이름을 사용자 정의 도메인에 매핑해야 합니다. 경로를 생성한 후 OpenShift 정식 라우터 호스트 이름은 **경로 세부 정보** 페이지에 표시됩니다. 또는 와일드카드 CNAME 레코드를 한 번 생성하여 지정된 호스트 이름의 모든 하위 도메인을 클러스터의 라우터로 라우팅할 수 있습니다.

2.1.4.2. 클러스터 서비스의 사용자 정의 도메인

사용자 정의 도메인 및 하위 도메인은 플랫폼 서비스 경로(예: API 또는 웹 콘솔 경로 또는 기본 애플리케이션 경로)에는 사용할 수 없습니다.

2.1.4.3. 도메인 검증 인증서

OpenShift Dedicated에는 클러스터의 내부 및 외부 서비스 모두에 필요한 TLS 보안 인증서가 포함되어 있습니다. 외부 경로의 경우 각 클러스터에 제공 및 설치된 두 개의 별도의 TLS 와일드카드 인증서가 있습니다. 하나는 웹 콘솔과 라우팅 기본 호스트 이름, API 끝점에 대한 두 번째 인증서입니다. *Let's Encrypt* 는 인증서에 사용되는 인증 기관입니다. 클러스터 내의 경로(예: 내부 API 끝점)는 클러스터의 내장 인증 기관에서 서명한 TLS 인증서를 사용하며 TLS 인증서를 신뢰하기 위해 모든 Pod에서 CA 번들을 사용할 수 있어야 합니다.

2.1.4.4. 빌드를 위한 사용자 정의 인증 기관

OpenShift Dedicated에서는 이미지 레지스트리에서 이미지를 가져올 때 빌드에서 신뢰하는 사용자 정의 인증 기관 사용을 지원합니다.

2.1.4.5. 로드 밸런서

OpenShift Dedicated는 최대 5개의 로드 밸런서를 사용합니다.

- 클러스터 내부이고 내부 클러스터 통신을 위해 트래픽의 균형을 조정하는 데 사용되는 내부 컨트롤 플레인 로드 밸런서입니다.
- OpenShift Container Platform 및 Kubernetes API에 액세스하는 데 사용되는 외부 컨트롤 플레인 로드 밸런서입니다. 이 로드 밸런서는 Red Hat OpenShift Cluster Manager에서 비활성화할 수 있습니다. 이 로드 밸런서가 비활성화된 경우 Red Hat은 내부 제어 로드 밸런서를 가리키도록 API DNS를 재구성합니다.
- Red Hat에서 클러스터 관리용으로 예약한 Red Hat의 외부 컨트롤 플레인 로드 밸런서입니다. 액세스는 엄격하게 제어되며 허용되는 bastion 호스트에서만 통신이 가능합니다.
- URL의 **앱에** 표시된 기본 애플리케이션 로드 밸런서인 기본 라우터/수신 로드 밸런서입니다. 기본

로드 밸런서는 인터넷을 통해 공개적으로 액세스하거나 기존 개인 연결을 통해 비공개로만 액세스하도록 OpenShift Cluster Manager에서 구성할 수 있습니다. 클러스터의 모든 애플리케이션 경로는 로깅 UI, 지표 API 및 레지스트리와 같은 클러스터 서비스를 포함하여 기본 라우터 로드 밸런서에 노출됩니다.

- 선택 사항: URL의 **apps2** 에 표시된 보조 애플리케이션 로드 밸런서인 보조 라우터/수신 로드 밸런서입니다. 보조 로드 밸런서는 인터넷을 통해 공개적으로 액세스하거나 기존 개인 연결을 통해 비공개로만 액세스하도록 OpenShift Cluster Manager에서 구성할 수 있습니다. 이 라우터 로드 밸런서에 대해 'Label match'가 구성된 경우 이 레이블과 일치하는 애플리케이션 경로만 이 라우터 로드 밸런서에 노출됩니다. 그렇지 않으면 모든 애플리케이션 경로도 이 라우터 로드 밸런서에 노출됩니다.

- 선택 사항: HTTP/SNI 트래픽 또는 비표준 포트 사용과 같은 고급 인그레스 기능을 활성화하기 위해 OpenShift Dedicated에서 실행되는 서비스에 매핑될 수 있는 서비스의 로드 밸런서입니다. 이는 표준 클러스터의 경우 4 그룹에서 구입하거나 CCS(Customer Cloud Subscription) 클러스터에 비용을 부과하지 않고 프로비저닝할 수 있지만 각 AWS 계정에는 각 클러스터 내에서 사용할 수 있는 Classic Load Balancer의 수를 제한하는 할당량이 있습니다.

2.1.4.6. 네트워크 사용량

표준 OpenShift Dedicated 클러스터의 경우 네트워크 사용량은 인바운드, VPC 피어링, VPN 및 AZ 트래픽 간의 데이터 전송을 기반으로 측정됩니다. 표준 OpenShift Dedicated 기본 클러스터에서 12TB의 네트워크 I/O가 제공됩니다. 추가 네트워크 I/O는 12TB 단위로 구매할 수 있습니다. CCS OpenShift Dedicated 클러스터의 경우 네트워크 사용량은 모니터링되지 않으며 클라우드 공급자가 직접 청구합니다.

2.1.4.7. 클러스터 인그레스

프로젝트 관리자는 IP 허용 목록을 통한 수신 제어를 포함하여 다양한 용도로 경로 주석을 추가할 수 있습니다.

ovs-networkpolicy 플러그인을 활용하는 **NetworkPolicy** 오브젝트를 사용하여 Ingress 정책을 변경할 수도 있습니다. 이를 통해 동일한 클러스터의 Pod와 동일한 네임스페이스에도 Pod 수준을 포함하여 수신 네트워크 정책을 완전히 제어할 수 있습니다.

모든 클러스터 Ingress 트래픽은 정의된 로드 밸런서를 통과합니다. 클라우드 구성에 의해 모든 노드에 대한 직접 액세스가 차단됩니다.

2.1.4.8. 클러스터 송신

EgressNetworkPolicy 오브젝트를 통한 Pod 송신 트래픽 제어를 사용하여 OpenShift Dedicated에서 아웃바운드 트래픽을 방지하거나 제한할 수 있습니다.

컨트롤 플레인 및 인프라 노드의 공용 아웃바운드 트래픽이 필요하며 클러스터 이미지 보안 및 클러스터 모니터링을 유지 관리하는 데 필요합니다. 이렇게 하려면 **0.0.0.0/0** 경로가 인터넷 게이트웨이에만 속해야 합니다. 이 범위를 프라이빗 연결을 통해 라우팅할 수 없습니다.

OpenShift Dedicated 클러스터는 NAT 게이트웨이를 사용하여 클러스터를 나가는 모든 공용 아웃바운드 트래픽에 대한 공용 고정 IP를 제공합니다. 클러스터가 배포된 각 서브넷은 별도의 NAT 게이트웨이를 수신합니다. 여러 가용성 영역이 있는 AWS에 배포된 클러스터의 경우 클러스터 송신 트래픽에 대해 최대 3개의 고유한 고정 IP 주소가 존재할 수 있습니다. 가용성 영역 토폴로지에 관계없이 Google Cloud에 배포된 클러스터의 경우 작업자 노드 송신 트래픽에 대한 고정 IP 주소가 1개입니다. 클러스터 내부에 남아 있거나 공용 인터넷으로 나가지 않는 트래픽은 NAT 게이트웨이를 통과하지 않으며 트래픽이 시작된 노드에 속하는 소스 IP 주소를 갖습니다. 노드 IP 주소는 동적이므로 고객은 개인 리소스에 액세스할 때 개별 IP 주소를 허용 목록에 사용하지 않아야 합니다.

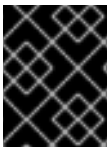
고객은 클러스터에서 Pod를 실행한 다음 외부 서비스를 쿼리하여 공용 고정 IP 주소를 확인할 수 있습니다. 예를 들면 다음과 같습니다.

```
$ oc run ip-lookup --image=busybox -i -t --restart=Never --rm -- /bin/sh -c "/bin/nslookup -type=a
myip.opendns.com resolver1.opendns.com | grep -E 'Address: [0-9.]+'"
```

2.1.4.9. 클라우드 네트워크 구성

OpenShift Dedicated를 사용하면 여러 클라우드 공급자 관리형 기술을 통해 프라이빗 네트워크 연결을 구성할 수 있습니다.

- VPN 연결
- AWS VPC 피어링
- AWS Transit Gateway
- AWS Direct Connect
- Google Cloud VPC 네트워크 피어링
- Google Cloud Classic VPN
- Google Cloud HA VPN



중요

Red Hat SREs는 사설 네트워크 연결을 모니터링하지 않습니다. 이러한 연결을 모니터링하는 것은 고객의 책임입니다.

2.1.4.10. DNS 전달

프라이빗 클라우드 네트워크 구성이 있는 OpenShift Dedicated 클러스터의 경우 고객은 명시적으로 제공된 도메인에 대해 쿼리해야 하는 프라이빗 연결에서 사용할 수 있는 내부 DNS 서버를 지정할 수 있습니다.

2.1.4.11. 네트워크 검증

네트워크 확인 검사는 기존 VPC(Virtual Private Cloud)에 OpenShift Dedicated 클러스터를 배포하거나 클러스터에 새로 추가된 서브넷을 사용하여 추가 머신 풀을 생성할 때 자동으로 실행됩니다. 이 검사에서는 네트워크 구성을 검증하고 오류를 강조 표시하므로 배포 전에 구성 문제를 해결할 수 있습니다.

네트워크 확인 검사를 수동으로 실행하여 기존 클러스터의 구성을 검증할 수도 있습니다.

추가 리소스

- 네트워크 확인 검사에 대한 자세한 내용은 네트워크 확인을 참조하십시오.

2.1.5. 스토리지

2.1.5.1. encrypted-at-rest OS/node 스토리지

컨트롤 플레인 노드는 encrypted-at-rest-EBS 스토리지를 사용합니다.

2.1.5.2. encrypted-at-rest PV

PV(영구 볼륨)에 사용되는 EBS 볼륨은 기본적으로 암호화된 볼륨입니다.

2.1.5.3. 블록 스토리지(RWO)

PV(영구 볼륨)는 AWS EBS 및 Google Cloud 영구 디스크 블록 스토리지에서 지원합니다. 이 블록 스토리지는 RWO(ReadWriteOnce) 액세스 모드를 사용합니다. 표준 OpenShift Dedicated 기본 클러스터에서 PV에 100GB의 블록 스토리지가 제공되며 애플리케이션 요청에 따라 동적으로 프로비저닝 및 재활용됩니다. 추가 영구 스토리지는 500GB 단위로 구매할 수 있습니다.

PV는 한 번에 단일 노드에만 연결할 수 있으며 프로비저닝된 가용성 영역과 관련이 있지만 가용성 영역의 모든 노드에 연결할 수 있습니다.

각 클라우드 공급자에는 단일 노드에 연결할 수 있는 PV 수에 대한 자체 제한이 있습니다. 자세한 내용은 AWS 인스턴스 유형 제한 또는 Google Cloud Platform 사용자 정의 머신 유형을 참조하십시오.

2.1.5.4. 공유 스토리지(RWX)

AWS CSI 드라이버는 AWS에서 OpenShift Dedicated에 RWX 지원을 제공하는 데 사용할 수 있습니다. 커뮤니티 Operator가 설정을 단순화하기 위해 제공됩니다. 자세한 내용은 AWS Dedicated 및 Red Hat OpenShift Service용 AWS EFS 설정을 참조하십시오.

2.1.6. 플랫폼

2.1.6.1. 클러스터 백업 정책

중요

고객은 애플리케이션 및 애플리케이션 데이터에 대한 백업 계획을 가지고 있어야 합니다.

애플리케이션 및 애플리케이션 데이터 백업은 OpenShift Dedicated 서비스의 일부가 아닙니다. 각 OpenShift Dedicated 클러스터의 모든 Kubernetes 오브젝트는 클러스터가 작동하지 않는 경우 신속하게 복구할 수 있도록 백업됩니다.

백업은 클러스터와 동일한 계정에 있는 보안 개체 스토리지(Multi-AZ) 버킷에 저장됩니다. Red Hat Enterprise Linux CoreOS는 OpenShift Container Platform 클러스터에서 완전히 관리되고 노드의 루트 볼륨에 저장해서는 안되므로 노드 루트 볼륨이 백업되지 않습니다.

다음 표에서는 백업 빈도를 보여줍니다.

구성 요소	스냅샷 빈도	보존	참고
전체 오브젝트 저장소 백업	매일 0100 UTC	7일	이는 모든 Kubernetes 오브젝트의 전체 백업입니다. 이 백업 일정에는 PV(영구 볼륨)가 백업되지 않습니다.

구성 요소	스냅샷 빈도	보존	참고
전체 오브젝트 저장소 백업	weekly on Mondays at 0200 UTC	30일	이는 모든 Kubernetes 오브젝트의 전체 백업입니다. 이 백업 일정에는 PV가 백업되지 않습니다.
전체 오브젝트 저장소 백업	시간 경과 후 17분	24시간	이는 모든 Kubernetes 오브젝트의 전체 백업입니다. 이 백업 일정에는 PV가 백업되지 않습니다.

2.1.6.2. 자동 확장

노드 자동 스케일링은 OpenShift Dedicated에서 사용할 수 있습니다. 클러스터에서 노드 자동 스케일링에 대한 자세한 내용은 클러스터에서 노드 자동 스케일링 정보를 참조하십시오.

2.1.6.3. 데몬 세트

고객은 OpenShift Dedicated에서 DaemonSet을 생성하고 실행할 수 있습니다. DaemonSets를 작업자 노드에서만 실행하도록 제한하려면 다음 nodeSelector를 사용합니다.

```
...
spec:
  nodeSelector:
    role: worker
...
```

2.1.6.4. 다중 가용성 영역

여러 가용성 영역 클러스터에서 제어 노드는 가용성 영역에 분산되어 있으며 각 가용성 영역에는 세 개 이상의 작업자 노드가 필요합니다.

2.1.6.5. 노드 라벨

사용자 정의 노드 레이블은 노드 생성 중에 Red Hat에서 생성하며 현재 OpenShift Dedicated 클러스터에서 변경할 수 없습니다.

2.1.6.6. OpenShift 버전

OpenShift Dedicated는 서비스로 실행되며 최신 OpenShift Container Platform 버전으로 최신 상태로 유지됩니다.

2.1.6.7. 업그레이드

업그레이드 정책 및 절차에 대한 자세한 내용은 OpenShift Dedicated 라이프 사이클 을 참조하십시오.

2.1.6.8. Windows 컨테이너

현재 OpenShift Dedicated에서는 Windows 컨테이너를 사용할 수 없습니다.

2.1.6.9. 컨테이너 엔진

OpenShift Dedicated는 OpenShift 4에서 실행되며 사용 가능한 유일한 컨테이너 엔진으로 CRI-O 를 사용합니다.

2.1.6.10. 운영 체제

OpenShift Dedicated는 OpenShift 4에서 실행되며 모든 컨트롤 플레인 및 작업자 노드의 운영 체제로 Red Hat Enterprise Linux CoreOS를 사용합니다.

2.1.6.11. Red Hat Operator 지원

일반적으로 Red Hat 워크로드는 Operator Hub를 통해 제공되는 Red Hat 제공 Operator를 참조합니다. Red Hat 워크로드는 Red Hat SRE 팀에서 관리하지 않으며 작업자 노드에 배포해야 합니다. 이러한 Operator에는 추가 Red Hat 서브스크립션이 필요할 수 있으며 추가 클라우드 인프라 비용이 발생할 수 있습니다. Red Hat에서 제공하는 Operator의 예는 다음과 같습니다.

- Red Hat Quay
- Red Hat Advanced Cluster Management
- Red Hat Advanced Cluster Security
- Red Hat OpenShift Service Mesh
- OpenShift Serverless
- Red Hat OpenShift Logging
- Red Hat OpenShift Pipelines

2.1.6.12. Kubernetes Operator 지원

OperatorHub 마켓플레이스에 나열된 모든 Operator를 설치할 수 있어야 합니다. Red Hat Operator를 포함하여 OperatorHub에서 설치한 Operator는 OpenShift Dedicated 서비스의 일부로 SRE를 관리하지 않습니다. 지정된 Operator의 지원 가능성에 대한 자세한 내용은 Red Hat 고객 포털 을 참조하십시오.

2.1.7. 보안

이 섹션에서는 OpenShift Dedicated 보안을 위한 서비스 정의에 대한 정보를 제공합니다.

2.1.7.1. 인증 공급자

클러스터에 대한 인증은 Red Hat OpenShift Cluster Manager 클러스터 생성 프로세스의 일부로 구성됩니다. OpenShift는 ID 공급자가 아니며 클러스터에 대한 모든 액세스는 고객이 통합 솔루션의 일부로 관리해야 합니다. 동시에 프로비저닝된 여러 ID 공급자를 프로비저닝하는 것이 지원됩니다. 지원되는 ID 공급자는 다음과 같습니다.

- GitHub 또는 GitHub Enterprise OAuth
- GitLab OAuth
- Google OAuth
- LDAP

- OpenID connect

2.1.7.2. 권한 있는 컨테이너

권한 있는 컨테이너는 OpenShift Dedicated에서 기본적으로 사용할 수 없습니다. **anyuid** 및 **nonroot** 보안 컨텍스트 제약 조건은 **dedicated-admins** 그룹의 멤버에서 사용할 수 있으며 많은 사용 사례를 처리해야 합니다. 권한 있는 컨테이너는 **cluster-admin** 사용자만 사용할 수 있습니다.

2.1.7.3. 고객 관리자

OpenShift Dedicated는 일반 사용자 외에도 **dedicated-admin** 이라는 OpenShift Dedicated 전용 그룹에 대한 액세스를 제공합니다. **dedicated-admin** 그룹의 멤버인 클러스터의 모든 사용자:

- 클러스터의 모든 고객 생성 프로젝트에 대한 관리자 액세스 권한이 있어야 합니다.
- 클러스터의 리소스 할당량 및 제한을 관리할 수 있습니다.
- **NetworkPolicy** 오브젝트를 추가하고 관리할 수 있습니다.
- 스케줄러 정보를 포함하여 클러스터의 특정 노드 및 PV에 대한 정보를 볼 수 있습니다.
- 클러스터에서 예약된 **dedicated-admin** 프로젝트에 액세스할 수 있으므로 승격된 권한이 있는 서비스 계정을 생성할 수 있으며 클러스터에서 프로젝트의 기본 제한 및 할당량을 업데이트할 수도 있습니다.
- OperatorHub에서 Operator를 설치할 수 있습니다(* 모든 ***.operators.coreos.com** API 그룹의 동사).

2.1.7.4. 클러스터 관리 역할

CCO(Customer Cloud Subscription)를 사용하는 OpenShift Dedicated의 관리자는 **cluster-admin** 역할에 액세스할 수 있습니다. **cluster-admin** 역할을 사용하여 계정에 로그인하는 동안 클러스터를 제어하고 구성할 수 있는 무제한 액세스 권한이 대부분 있습니다. 클러스터의 불안정을 방지하기 위해 Webhook로 차단되거나 OpenShift Cluster Manager에서 관리되기 때문에 클러스터 내 변경 사항을 덮어쓰는 몇 가지 구성이 있습니다.

2.1.7.5. 프로젝트 셀프 서비스

기본적으로 모든 사용자는 프로젝트를 생성, 업데이트 및 삭제할 수 있습니다. **dedicated-admin** 그룹의 멤버가 인증된 사용자에서 self-provisioner 역할을 제거하는 경우 이를 제한할 수 있습니다.

```
$ oc adm policy remove-cluster-role-from-group self-provisioner system:authenticated:oauth
```

적용을 통해 제한 사항을 되돌릴 수 있습니다.

```
$ oc adm policy add-cluster-role-to-group self-provisioner system:authenticated:oauth
```

2.1.7.6. 규정 준수

OpenShift Dedicated는 보안 및 제어를 위한 일반적인 업계 모범 사례를 따릅니다. 인증은 다음 표에 설명되어 있습니다.

표 2.1. OpenShift Dedicated의 보안 및 제어 인증

컴플라이언스	AWS의 OpenShift Dedicated	GCP의 OpenShift Dedicated
HIPAA 정규화된	제공됨 (고객 클라우드 서브스크립션만)	제공됨 (고객 클라우드 서브스크립션만)
ISO 27001	제공됨	제공됨
PCI DSS	제공됨	제공됨
SOC 2 Type 2	제공됨	제공됨

2.1.7.7. 네트워크 보안

각 OpenShift Dedicated 클러스터는 방화벽 규칙(AWS Security Groups 또는 Google Cloud Compute Engine 방화벽 규칙)을 사용하여 클라우드 인프라 수준에서 보안 네트워크 구성으로 보호됩니다. AWS의 OpenShift Dedicated 고객도 AWS Shield Standard 를 사용하여 DDoS 공격으로부터 보호됩니다. 마찬가지로 GCP의 OpenShift Dedicated에서 사용하는 모든 GCP 로드 밸런서 및 공용 IP 주소는 Google Cloud Armor Standard 를 사용하여 DDoS 공격으로부터 보호됩니다.

2.1.7.8. etcd 암호화

OpenShift Dedicated에서 컨트롤 플레인 스토리지는 기본적으로 암호화되어 etcd 볼륨의 암호화가 포함됩니다. 이 스토리지 수준 암호화는 클라우드 공급자의 스토리지 계층을 통해 제공됩니다.

etcd 암호화를 활성화하여 etcd의 키 값을 암호화하지만 키를 암호화할 수도 없습니다. etcd 암호화를 활성화하면 다음 Kubernetes API 서버 및 OpenShift API 서버 리소스가 암호화됩니다.

- 보안
- 구성 맵
- 라우트
- OAuth 액세스 토큰
- OAuth 승인 토큰

etcd 암호화 기능은 기본적으로 활성화되어 있지 않으며 클러스터 설치 시에만 활성화할 수 있습니다. etcd 암호화가 활성화된 상태에서도 etcd 키 값은 컨트롤 플레인 노드 또는 **cluster-admin** 권한에 액세스할 수 있는 모든 사용자가 액세스할 수 있습니다.

중요

etcd의 키 값에 etcd 암호화를 활성화하면 약 20%의 성능 오버헤드가 발생합니다. 오버헤드는 etcd 볼륨을 암호화하는 기본 컨트롤 플레인 스토리지 암호화 외에도 이 두 번째 암호화 계층이 도입된 결과입니다. 특히 사용 사례에 필요한 경우에만 etcd 암호화를 활성화하는 것이 좋습니다.

2.2. 책임 할당 매트릭스

OpenShift Dedicated 관리 서비스에 대한 Red Hat, 클라우드 공급자 및 고객 책임을 이해합니다.

2.2.1. OpenShift Dedicated에 대한 설명

Red Hat은 OpenShift Dedicated 서비스를 관리하는 반면 고객은 특정 측면과 관련하여 책임을 공유합니다. OpenShift Dedicated 서비스는 Red Hat 또는 고객 소유 클라우드 서비스 공급자 계정에서 생성된 퍼블릭 클라우드 리소스에서 호스팅되는 원격으로 액세스할 수 있으며 Red Hat이 소유한 기본 플랫폼 및 데이터 보안이 있습니다.

중요

클러스터에서 **cluster-admin** 역할이 활성화되어 있는 경우 Red Hat Enterprise Agreement 부록 4 (Online Subscription Services) 의 책임 및 제외 노트를 참조하십시오.

리소스	사고 및 운영 관리	변경 관리	ID 및 액세스 관리	보안 및 규정 준수	재해 복구
고객 데이터	고객	고객	고객	고객	고객
고객 애플리케이션	고객	고객	고객	고객	고객
개발자 서비스	고객	고객	고객	고객	고객
플랫폼 모니터링	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
로깅	Red Hat	shared	shared	shared	Red Hat
애플리케이션 네트워킹	shared	shared	shared	Red Hat	Red Hat
클러스터 네트워킹	Red Hat	shared	shared	Red Hat	Red Hat
가상 네트워킹	shared	shared	shared	shared	shared
컨트롤 플레인 및 인프라 노드	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
작업자 노드	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
클러스터 버전	Red Hat	shared	Red Hat	Red Hat	Red Hat
용량 관리	Red Hat	shared	Red Hat	Red Hat	Red Hat
가상 스토리지	Red Hat 및 클라우드 공급자	Red Hat 및 클라우드 공급자	Red Hat 및 클라우드 공급자	Red Hat 및 클라우드 공급자	Red Hat 및 클라우드 공급자
물리적 인프라 및 보안	클라우드 공급자	클라우드 공급자	클라우드 공급자	클라우드 공급자	클라우드 공급자

2.2.2. 공유 책임 매트릭스

고객 및 Red Hat은 OpenShift Dedicated 클러스터의 모니터링 및 유지 관리를 담당합니다. 이 문서는 영역과 작업 단위를 설명합니다.

2.2.2.1. 사고 및 운영 관리

고객은 고객 애플리케이션 데이터의 사고 및 운영 관리 및 고객이 클러스터 네트워크 또는 가상 네트워크에 대해 구성한 사용자 지정 네트워킹을 담당합니다.

리소스	Red Hat 책임	고객 책임
애플리케이션 네트워킹	클라우드 로드 밸런서 및 기본 OpenShift 라우터 서비스를 모니터링하고 경고에 응답합니다.	• 서비스 로드 밸런서 끝점의 상태 모니터링 • 애플리케이션 경로 및 그 뒤에 있는 엔드 포인트의 상태를 모니터링합니다. • Red Hat에 시스템 중단 보고.
가상 네트워킹	기본 플랫폼 네트워킹에 필요한 클라우드 로드 밸런서, 서브넷 및 퍼블릭 클라우드 구성 요소를 모니터링하고 경고에 응답합니다.	잠재적인 문제 또는 보안 위협에 대한 VPC에서 VPC 연결, VPN 연결 또는 직접 연결을 통해 선택적으로 구성된 네트워크 트래픽을 모니터링합니다.

2.2.2.2. 변경 관리

Red Hat은 고객이 제어할 클러스터 인프라 및 서비스를 변경하고 컨트롤 플레인 노드, 인프라 노드 및 서비스, 작업자 노드의 버전을 유지 관리하는 역할을 담당합니다. 고객은 인프라 변경 요청을 시작하고 클러스터에서 선택적 서비스 및 네트워킹 구성을 설치 및 유지 관리하고 고객 데이터 및 고객 애플리케이션에 대한 모든 변경을 담당합니다.

리소스	Red Hat 책임	고객 책임
로깅	• 플랫폼 감사 로그를 중앙에서 집계하고 모니터링합니다. • 고객이 기본 애플리케이션 로깅을 위해 로깅 스택을 배포할 수 있도록 로깅 Operator를 제공하고 유지 관리합니다. • 고객 요청에 따라 감사 로그를 제공합니다.	• 클러스터에 선택적 기본 애플리케이션 로깅 Operator를 설치합니다. • 사이드카 컨테이너 또는 타사 로깅 애플리케이션과 같은 선택적 앱 로깅 솔루션을 설치, 구성 및 유지 관리합니다. • 로깅 스택 또는 클러스터의 안정성에 영향을 미치는 경우 고객 애플리케이션에서 생성되는 애플리케이션 로그의 크기와 빈도를 조정합니다. • 특정 문제 조사를 위해 지원 케이스를 통해 플랫폼 감사 로그를 요청합니다.

리소스	Red Hat 책임	고객 책임
애플리케이션 네트워킹	• 퍼블릭 클라우드 로드 밸런서를 설정합니다. 필요한 경우 프라이빗 로드 밸런서와 최대 1개의 추가 로드 밸런서를 설정하는 기능을 제공합니다. • 기본 OpenShift 라우터 서비스를 설정합니다. 라우터를 프라이빗으로 설정하고 하나의 추가 라우터 shard를 추가하는 기능을 제공합니다. • 기본 내부 pod 트래픽에 대한 OpenShift SDN 구성 요소를 설치, 구성 및 유지 관리합니다. • 고객이 **NetworkPolicy** 및 **EgressNetworkPolicy** (firewall) 오브젝트를 관리할 수 있는 기능을 제공합니다.	• **NetworkPolicy** 오브젝트를 사용하여 프로젝트 및 Pod 네트워크, Pod 수신 및 Pod 송신에 대한 기본 Pod 네트워크 권한을 구성합니다. • Red Hat OpenShift Cluster Manager를 사용하여 기본 애플리케이션 경로에 대한 프라이빗 로드 밸런서를 요청합니다. • OpenShift Cluster Manager를 사용하여 최대 하나의 추가 퍼블릭 또는 프라이빗 라우터 shard 및 해당 로드 밸런서를 구성합니다. • 특정 서비스에 대한 추가 서비스 로드 밸런서를 요청하고 구성합니다. • 필요한 모든 DNS 전달 규칙을 구성합니다.
클러스터 네트워킹	• 퍼블릭 또는 프라이빗 서비스 엔드포인트와 같은 클러스터 관리 구성 요소와 가상 네트워킹 구성 요소와의 통합이 필요합니다. • 작업자, 인프라 및 컨트롤 플레인 노드 간의 내부 클러스터 통신에 필요한 내부 네트워킹 구성 요소를 설정합니다.	• 클러스터를 프로비저닝할 때 OpenShift Cluster Manager를 통해 필요한 경우 시스템 CIDR, 서비스 CIDR 및 Pod CIDR에 대한 기본이 아닌 IP 주소 범위 옵션을 제공합니다. • 클러스터 생성 시 또는 OpenShift Cluster Manager를 통해 클러스터 생성 후 API 서비스 엔드포인트를 공개 또는 비공개로 요청합니다.

리소스	Red Hat 책임	고객 책임
가상 네트워킹	• 가상 프라이빗 클라우드, 서브넷, 로드 밸런서, 인터넷 게이트웨이, NAT 게이트웨이 등을 포함하여 클러스터를 프로비저닝하는 데 필요한 가상 네트워킹 구성 요소를 설정하고 구성합니다. • 고객이 온프레미스 리소스와 VPC 연결, OpenShift Cluster Manager를 통해 필요에 따라 직접 연결을 관리할 수 있는 기능을 제공합니다. • 고객이 서비스 로드 밸런서와 함께 사용할 퍼블릭 클라우드 로드 밸런서를 생성하고 배포할 수 있습니다.	• VPC에서 VPC 연결, VPN 연결 또는 직접 연결과 같은 선택적 퍼블릭 클라우드 네트워킹 구성 요소를 설정하고 유지 관리합니다. • 특정 서비스에 대한 추가 서비스 로드 밸런서를 요청하고 구성합니다.
클러스터 버전	• 업그레이드 스케줄링 프로세스를 활성화합니다. • 업그레이드 진행 상황을 모니터링하고 발생한 모든 문제를 해결합니다. • 마이너 및 유지 관리 업그레이드를 위해 변경 로그 및 릴리스 정보를 게시합니다.	• 유지 관리 버전 업그레이드를 즉시 예약하거나 향후 자동 업그레이드가 가능합니다. • 마이너 버전 업그레이드를 승인하고 예약합니다. • 클러스터 버전이 지원되는 마이너 버전을 사용하고 있는지 확인합니다. • 마이너 및 유지 관리 버전에서 고객 애플리케이션을 테스트하여 호환성을 보장합니다.
용량 관리	• 컨트롤 플레인(컨트롤 플레인 노드 및 인프라 노드)의 사용률을 모니터링합니다. • 컨트롤 플레인 노드를 확장하거나 크기를 조정하여 서비스 품질을 유지합니다. • 네트워크, 스토리지 및 컴퓨팅 용량을 포함한 고객 리소스의 사용률을 모니터링합니다. 클러스터 리소스에 필요한 변경 사항(예: 확장, 추가 스토리지 등)에 대한 자동 스케일링 기능이 활성화되어 있지 않은 경우.	• 제공된 OpenShift Cluster Manager 제어를 사용하여 필요에 따라 추가 작업자 노드를 추가하거나 제거합니다. • 클러스터 리소스 요구 사항에 대한 Red Hat 알림에 응답합니다.

2.2.2.3. 액세스 및 ID 권한 부여

액세스 및 ID 권한 부여 매트릭스에는 클러스터, 애플리케이션 및 인프라 리소스에 대한 권한 있는 액세스를 관리하는 책임이 포함됩니다. 여기에는 액세스 제어 메커니즘, 인증, 권한 부여 및 리소스에 대한 액세스 관리와 같은 작업이 포함됩니다.

리소스	Red Hat 책임	고객 책임
로깅	• 플랫폼 감사 로그를 위해 업계 표준 기반 계층화된 내부 액세스 프로세스를 준수합니다. • 기본 OpenShift RBAC 기능을 제공합니다.	• 프로젝트에 대한 액세스 권한을 제어하고 프로젝트의 애플리케이션 로그를 확장함으로써 OpenShift RBAC를 구성합니다. • 타사 또는 사용자 지정 애플리케이션 로깅 솔루션의 경우 고객은 액세스 관리를 담당합니다.
애플리케이션 네트워킹	네이티브 OpenShift RBAC 및 **dedicated-admin** 기능을 제공합니다.	• 필요에 따라 경로 구성에 대한 액세스를 제어하도록 OpenShift dedicated-admins 및 RBAC를 구성합니다. • OpenShift Cluster Manager에 대한 액세스 권한을 부여하도록 Red Hat 조직의 조직 관리자를 관리합니다. OpenShift Cluster Manager는 라우터 옵션을 구성하고 서비스 로드 밸런서 할당량을 제공하는 데 사용됩니다.
클러스터 네트워킹	• OpenShift Cluster Manager를 통해 고객 액세스 제어 제공. • 네이티브 OpenShift RBAC 및 **dedicated-admin** 기능을 제공합니다.	• Red Hat 계정의 Red Hat 조직 멤버십을 관리합니다. • OpenShift Cluster Manager에 대한 액세스 권한을 부여하도록 Red Hat 조직의 조직 관리자를 관리합니다. • 필요에 따라 경로 구성에 대한 액세스를 제어하도록 OpenShift dedicated-admins 및 RBAC를 구성합니다.
가상 네트워킹	OpenShift Cluster Manager를 통해 고객 액세스 제어 제공.	OpenShift Cluster Manager를 통해 퍼블릭 클라우드 구성 요소에 대한 선택적 사용자 액세스를 관리합니다.

2.2.2.4. 보안 및 규정 준수

다음은 규정 준수와 관련된 책임 및 제어입니다.

리소스	Red Hat 책임	고객 책임
로깅	클러스터 감사 로그를 Red Hat SIEM에 전송하여 보안 이벤트를 분석합니다. 법의학 분석을 지원하기 위해 정의된 기간 동안 감사 로그를 유지합니다.	보안 이벤트에 대한 애플리케이션 로그를 분석합니다. 기본 로깅 스택에서 제공하는 것보다 오래 보존해야 하는 경우 로깅 사이드카 컨테이너 또는 타사 로깅 애플리케이션을 통해 애플리케이션 로그를 외부 엔드포인트에 보냅니다.
가상 네트워킹	• 잠재적인 문제 및 보안 위협에 대해 가상 네트워킹 구성 요소를 모니터링합니다. • 추가 모니터링 및 보호를 위해 추가 퍼블릭 클라우드 공급자 툴을 활용합니다.	• 잠재적인 문제 및 보안 위협에 대해 선택적으로 구성된 가상 네트워킹 구성 요소를 모니터링합니다. • 필요에 따라 필요한 방화벽 규칙 또는 데이터 센터 보호를 구성합니다.

2.2.2.5. 재해 복구

재해 복구에는 데이터 및 구성 백업, 재해 복구 환경에 데이터 및 구성 복제, 재해 이벤트에 대한 장애 조치(failover)가 포함됩니다.

리소스	Red Hat 책임	고객 책임
가상 네트워킹	플랫폼이 작동하는 데 필요한 영향을 받는 가상 네트워크 구성 요소를 복원하거나 다시 생성합니다.	• 퍼블릭 클라우드 공급자가 권장하는 대로 중단을 방지할 수 있는 터널을 두 개 이상 사용하여 가상 네트워킹 연결을 구성합니다. • 여러 클러스터와 함께 글로벌 로드 밸런서를 사용하는 경우 페일오버 DNS 및 로드 밸런싱을 유지합니다.

2.2.3. 데이터 및 애플리케이션에 대한 고객 책임

고객은 OpenShift Dedicated에 배포하는 애플리케이션, 워크로드 및 데이터를 담당합니다. 그러나 Red Hat은 고객이 플랫폼에서 데이터 및 애플리케이션을 관리할 수 있도록 다양한 도구를 제공합니다.

리소스	Red Hat 책임	고객 책임

리소스	Red Hat 책임	고객 책임
고객 데이터	• 데이터 암호화를 위한 플랫폼 수준 표준을 유지 관리합니다. • 시크릿과 같은 애플리케이션 데이터를 관리하는 데 도움이 되도록 OpenShift 구성 요소를 제공합니다. • AWS RDS 또는 Google Cloud SQL과 같은 타사 데이터 서비스 통합을 활성화하여 클러스터 및/또는 클라우드 공급자 외부의 데이터를 저장 및 관리할 수 있습니다.	플랫폼에 저장된 모든 고객 데이터 및 고객 애플리케이션이 이러한 데이터를 소비하고 노출하는 방법에 대한 책임을 유지합니다.
고객 애플리케이션	• 고객이 컨테이너화된 애플리케이션을 배포 및 관리하기 위해 OpenShift 및 Kubernetes API에 액세스할 수 있도록 OpenShift 구성 요소가 설치된 클러스터를 프로비저닝합니다. • 고객 배포가 Red Hat Container Catalog 레지스트리에서 이미지를 가져올 수 있도록 이미지 가져오기 보안이 포함된 클러스터를 생성합니다. • 고객이 커뮤니티, 타사 및 Red Hat 서비스를 클러스터에 추가하기 위해 Operator를 설정하는 데 사용할 수 있는 OpenShift API를 제공합니다. • 고객 애플리케이션과 함께 사용할 영구 볼륨을 지원하는 스토리지 클래스 및 플러그인을 제공합니다. • 고객이 애플리케이션을 배포 및 관리하기 위해 클러스터에 애플리케이션 컨테이너 이미지를 안전하게 저장할 수 있도록 컨테이너 이미지 레지스트리를 제공합니다.	• 고객 및 타사 애플리케이션, 데이터 및 전체 라이프사이클에 대한 책임을 유지합니다. • 고객이 Operator 또는 외부 이미지를 사용하여 Red Hat, 커뮤니티, 타사, 자체 또는 기타 서비스를 클러스터에 추가하는 경우 고객은 이러한 서비스 및 적절한 공급자(Red Hat 포함)와 협력하여 문제를 해결합니다. • 제공된 툴과 기능을 사용하여 구성 및 배포, 최신 리소스 요청 및 제한 유지, 애플리케이션 실행을 위한 충분한 리소스를 확보할 클러스터 크기, 권한을 설정하고, 다른 서비스와 통합하며, 외부적으로 제공하는 이미지 스트림 또는 템플릿을 관리하고, 데이터를 저장, 백업 및 복원하며, 고가용성 및 복원 워크로드를 관리하는 것입니다. • 메트릭을 수집하고 경고를 생성하기 위한 설치 및 운영 소프트웨어를 포함하여 OpenShift Dedicated에서 실행되는 애플리케이션 모니터링 책임을 유지합니다.

2.3. OPENSHIFT DEDICATED의 프로세스 및 보안 이해

2.3.1. 클러스터 알림 검토 및 작업

클러스터 알림은 클러스터의 상태, 상태 또는 성능에 대한 메시지입니다.

클러스터 알림은 Red Hat site Reliability Engineering(SRE)이 관리형 클러스터의 상태에 대해 귀하와 통신하는 기본 방법입니다. SRE는 클러스터 알림을 사용하여 클러스터 문제를 해결하거나 방지하기 위해 작업을 수행하도록 요청할 수도 있습니다.

클러스터 소유자 및 관리자는 클러스터가 정상 상태로 유지되고 지원되는지 확인하기 위해 클러스터 알림을 정기적으로 검토하고 조치를 취해야 합니다.

클러스터의 클러스터 **기록 탭에서 Red Hat Hybrid Cloud Console에서 클러스터**알림을 볼 수 있습니다. 기본적으로 클러스터 소유자만 이메일로 클러스터 알림을 수신합니다. 다른 사용자가 클러스터 알림 이메일을 수신해야 하는 경우 각 사용자를 클러스터에 대한 알림 연락처로 추가합니다.

2.3.1.1. 클러스터 알림 정책

클러스터 알림은 클러스터의 상태와 영향을 미치는 높은 영향을 미치는 이벤트에 대한 정보를 유지하도록 설계되었습니다.

대부분의 클러스터 알림은 자동으로 생성되고 전송되어 즉시 문제에 대한 정보 또는 클러스터 상태에 대한 중요한 변경 사항을 확인할 수 있습니다.

특정 상황에서 Red Hat 사이트 안정성 엔지니어링(SRE)은 클러스터 알림을 생성하고 전송하여 복잡한 문제에 대한 추가 컨텍스트 및 지침을 제공합니다.

영향을 받지 않는 이벤트, 위험이 낮은 보안 업데이트, 일상적인 운영 및 유지 관리 또는 SRE가 신속하게 해결하는 일시적인 문제에 대해서는 클러스터 알림이 전송되지 않습니다.

Red Hat 서비스는 다음과 같은 경우 자동으로 알림을 보냅니다.

- 원격 상태 모니터링 또는 환경 확인 검사에서는 작업자 노드에 디스크 공간이 부족한 경우와 같이 클러스터에서 문제를 감지합니다.
- 예를 들어 예정된 유지 관리 또는 업그레이드가 시작되는 경우 심각한 클러스터 라이프 사이클 이벤트가 발생하거나 클러스터 작업이 이벤트의 영향을 받지만 고객의 개입은 필요하지 않습니다.
- 예를 들어 클러스터 소유권 또는 관리 제어가 한 사용자에서 다른 사용자로 전송되는 경우와 같이 중요한 클러스터 관리 변경이 발생합니다.
- 예를 들어 Red Hat이 클러스터에서 서브스크립션 조건 또는 기능을 업데이트할 때 클러스터 서브스크립션이 변경 또는 업데이트됩니다.

SRE는 다음과 같은 경우 알림을 생성하고 보냅니다.

- 사고로 인해 클러스터의 가용성 또는 성능에 영향을 미치는 성능 저하 또는 중단이 발생합니다(예: 클라우드 공급자의 경우 지역 중단). SRE는 사고 해결 진행 상황을 알려주기 위해 후속 알림을 보냅니다.
- 클러스터에서 보안 취약점, 보안 위반 또는 비정상적인 활동이 감지됩니다.
- Red Hat은 변경 사항이 생성 중이거나 클러스터 불안정성을 초래할 수 있음을 감지합니다.
- Red Hat은 워크로드가 클러스터에서 성능 저하 또는 불안정성을 초래하고 있음을 감지합니다.

2.3.2. 사고 및 운영 관리

이 문서에서는 OpenShift Dedicated 관리 서비스에 대한 Red Hat 책임을 자세히 설명합니다. 클라우드 공급자는 클라우드 공급자가 제공하는 서비스를 실행하는 하드웨어 인프라를 보호할 책임이 있습니다. 고객은 고객 애플리케이션 데이터의 사고 및 운영 관리 및 고객이 클러스터 네트워크 또는 가상 네트워크에 대해 구성한 사용자 지정 네트워킹을 담당합니다.

2.3.2.1. 플랫폼 모니터링

Red Hat 사이트 안정성 엔지니어(SRE)는 모든 OpenShift Dedicated 클러스터 구성 요소, SRE 서비스 및 기본 클라우드 공급자 계정에 대해 중앙 집중식 모니터링 및 경고 시스템을 유지 관리합니다. 플랫폼 감사 로그는 중앙 집중식 SIEM(보안 정보 및 이벤트 모니터링) 시스템으로 안전하게 전달되며, 여기서 SRE 팀에 구성된 경고를 트리거하고 수동 검토도 수행할 수 있습니다. 감사 로그는 SIEM에서 1년 동안 유지됩니다. 지정된 클러스터에 대한 감사 로그는 클러스터를 삭제할 때 삭제되지 않습니다.

2.3.2.2. 사고 관리

사고는 하나 이상의 Red Hat 서비스의 성능 저하 또는 중단을 초래하는 이벤트입니다. 이러한 사고는 중앙 집중식 모니터링 및 경고 시스템에 의해 직접 또는 SRE 팀의 구성원에 의해 지원 케이스를 통해 고객 또는 CEE(Customer Experience and Engagement)에 의해 발생할 수 있습니다.

서비스 및 고객에 미치는 영향에 따라 보안 사고는 심각도 별로 분류됩니다.

Red Hat에서 새로운 사고를 관리하는 방법에 대한 일반적인 워크플로:

1. SRE 첫 번째 응답자는 새로운 사고에 대한 경고를 받고 있으며 초기 조사를 시작합니다.
2. 초기 조사 후 사고의 선두주자가 할당되며, 이는 복구 노력을 조정합니다.
3. 사고 리더는 관련 알림 또는 지원 케이스 업데이트를 포함하여 모든 통신을 관리하고 복구와 관련된 조정을 관리합니다.
4. 이 사고는 복구되었습니다.
5. 사고는 문서화되어 있으며 근본적인 원인 분석은 사고 후 5 일 이내에 수행됩니다.
6. 근본 원인 분석 (RCA) 초안 문서는 사고 후 7 일 이내에 고객과 공유됩니다.

2.3.2.3. 백업 및 복구

모든 OpenShift Dedicated 클러스터는 클라우드 공급자 스냅샷을 사용하여 백업됩니다. 특히 PV(영구 볼륨)에 저장된 고객 데이터는 포함되지 않습니다. 모든 스냅샷은 적절한 클라우드 공급자 스냅샷 API를 사용하여 수행되며 클러스터와 동일한 계정에서 보안 오브젝트 스토리지 버킷(AWS의 S3 및 Google Cloud의 GCS)에 업로드됩니다.

구성 요소	스냅샷 빈도	보존	참고
전체 오브젝트 저장소 백업	daily	7일	이는 etcd와 같은 모든 Kubernetes 오브젝트의 전체 백업입니다. 이 백업 일정에는 PV가 백업되지 않습니다.
	weekly	30일	
전체 오브젝트 저장소 백업	hourly	24시간	이는 etcd와 같은 모든 Kubernetes 오브젝트의 전체 백업입니다. 이 백업 일정에는 PV가 백업되지 않습니다.
노드 루트 볼륨	Never	해당 없음	노드는 단기적으로 간주됩니다. 중요한 것은 노드의 루트 볼륨에 저장해야 합니다.

- Red Hat은 PREO (Resupation Point Objective) 또는 RTO (RTO)에 커밋하지 않습니다.
- 고객은 데이터의 정기적인 백업을 수행할 책임이 있습니다.
- 고객은 Kubernetes 모범 사례를 따르는 워크로드를 사용하여 다중 AZ 클러스터를 배포하여 한 리전 내에서 고가용성을 보장해야 합니다.
- 전체 클라우드 리전을 사용할 수 없는 경우 고객은 다른 지역에 새 클러스터를 설치하고 백업 데이터를 사용하여 앱을 복원해야 합니다.

2.3.2.4. 클러스터 용량

클러스터 용량을 평가하고 관리하는 것은 Red Hat과 고객 간에 공유됩니다. Red Hat SRE는 클러스터의 모든 컨트롤 플레인 및 인프라 노드의 용량을 담당합니다.

Red Hat SRE는 업그레이드 중 및 클러스터 경고에 대한 응답으로 클러스터 용량도 평가합니다. 용량에 대한 클러스터 업그레이드의 영향은 업그레이드 테스트 프로세스의 일부로 평가되어 클러스터에 새로 추가된 용량의 부정적인 영향을 받지 않도록 합니다. 클러스터 업그레이드 중에 업그레이드 프로세스 중에 총 클러스터 용량을 유지하도록 추가 작업자 노드가 추가됩니다.

SRE 직원의 용량 평가는 특정 기간 동안 사용 임계 값을 초과하면 클러스터의 경고에 대한 응답으로도 수행됩니다. 이러한 경고는 고객에게 통지가 발생할 수도 있습니다.

2.3.3. 변경 관리

이 섹션에서는 클러스터 및 구성 변경, 패치 및 릴리스를 관리하는 방법에 대한 정책에 대해 설명합니다.

2.3.3.1. 고객 시작 변경

클러스터 배포, 작업자 노드 확장 또는 클러스터 삭제와 같은 셀프 서비스 기능을 사용하여 변경 사항을 시작할 수 있습니다.

변경 내역은 OpenShift **Cluster** Manager **개요 탭**의 클러스터 기록 섹션에서 캡처되며 사용자가 확인할 수 있습니다. 변경 내역에는 다음이 포함되지만 이에 국한되지는 않으며 다음 변경 사항의 로그가 포함됩니다.

- ID 공급자 추가 또는 제거
- **dedicated-admins** 그룹에 사용자 추가 또는 제거
- 클러스터 컴퓨팅 노드 확장
- 클러스터 로드 밸런서 스케일링
- 클러스터 영구 스토리지 스케일링
- 클러스터 업그레이드

다음 구성 요소에 대해 OpenShift Cluster Manager의 변경 사항을 방지하여 유지 관리 제외를 구현할 수 있습니다.

- 클러스터 삭제
- ID 공급자 추가, 수정 또는 제거
- 승격된 그룹에서 사용자 추가, 수정 또는 제거

- 애드온 설치 또는 제거
- 클러스터 네트워킹 구성 수정
- 머신 풀 추가, 수정 또는 제거
- 사용자 워크로드 모니터링 활성화 또는 비활성화
- 업그레이드 시작

중요

유지 관리 제외를 적용하려면 머신 풀 자동 스케일링 또는 자동 업그레이드 정책을 비활성화해야 합니다. 유지 관리 제외가 해제된 후 필요에 따라 머신 풀 자동 스케일링 또는 자동 업그레이드 정책 활성화를 진행합니다.

2.3.3.2. Red Hat 시작 변경

Red Hat SRE(사이트 안정성 엔지니어링)는 GitOps 워크플로우 및 완전히 자동화된 CI/CD 파이프라인을 사용하여 OpenShift Dedicated의 인프라, 코드 및 구성을 관리합니다. 이 프로세스를 통해 Red Hat은 고객에게 부정적인 영향을 미치지 않고 지속적으로 서비스 개선을 지속적으로 개선할 수 있습니다.

제안된 모든 변경 사항은 점검 즉시 일련의 자동 검증을 거칩니다. 그런 다음 변경 사항이 자동화된 통합 테스트를 받는 스테이징 환경에 배포됩니다. 마지막으로 변경 사항이 프로덕션 환경에 배포됩니다. 각 단계는 완전히 자동화됩니다.

승인된 SRE 검토자는 각 단계에 대한 진행을 승인해야 합니다. 검토자는 변경 사항을 제안한 동일한 개인일 수 없습니다. 모든 변경 사항 및 승인은 GitOps 워크플로우의 일부로 완전히 감사할 수 있습니다.

기능 플래그를 사용하여 지정된 클러스터 또는 고객에 대한 새 기능의 가용성을 제어하는 일부 변경 사항이 증분적으로 릴리스됩니다.

2.3.3.3. 패치 관리

OpenShift Container Platform 소프트웨어 및 기본 변경 불가능한 RHCOS(Red Hat Enterprise Linux CoreOS) 운영 체제 이미지는 일반 z-stream 업그레이드의 버그 및 취약점에 대해 패치됩니다. OpenShift Container Platform 설명서에서 RHCOS 아키텍처에 대해 자세히 알아보십시오.

2.3.3.4. 릴리스 관리

Red Hat은 클러스터를 자동으로 업그레이드하지 않습니다. OpenShift Cluster Manager 웹 콘솔을 사용하여 클러스터를 정기적인 간격으로 업그레이드하거나 (개인 업그레이드) 한 번만 예약할 수 있습니다. Red Hat은 클러스터가 심각한 영향 CVE의 영향을 받는 경우에만 클러스터를 새 z-stream 버전으로 강제로 업그레이드할 수 있습니다. OpenShift Cluster Manager 웹 콘솔에서 모든 클러스터 업그레이드 이벤트 기록을 검토할 수 있습니다. 릴리스에 대한 자세한 내용은 라이프 사이클 정책을 참조하십시오.

2.3.4. 보안 및 규정 준수

보안 및 규정 준수에는 보안 제어 및 컴플라이언스 인증 구현과 같은 작업이 포함됩니다.

2.3.4.1. 데이터 분류

Red Hat은 데이터 분류 표준을 정의하고 준수하여 데이터의 민감도를 결정하고 수집, 사용, 전송 및 처리되는 데이터의 기밀성 및 무결성에 대한 내재적인 위험을 강조합니다. 고객 소유 데이터는 최고 수준의 민감도 및 처리 요구 사항으로 분류됩니다.

2.3.4.2. 데이터 관리

OpenShift Dedicated는 AWS KMS(Key Management Service) 및 Google Cloud KMS와 같은 클라우드 공급자 서비스를 사용하여 영구 데이터의 암호화 키를 안전하게 관리할 수 있습니다. 이러한 키는 모든 컨트롤 플레인, 인프라 및 작업자 노드 루트 볼륨을 암호화하는 데 사용됩니다. 고객은 설치시 루트 볼륨을 암호화하기 위해 자체 KMS 키를 지정할 수 있습니다. PV(영구 볼륨)는 키 관리를 위해 KMS도 사용합니다. 고객은 KMS 키 AMI(Amazon Resource Name) 또는 ID를 참조하여 새 **StorageClass** 를 생성하여 PV를 암호화하기 위해 자체 KMS 키를 지정할 수 있습니다.

고객이 OpenShift Dedicated 클러스터를 삭제하면 컨트롤 플레인 데이터 볼륨 및 고객 애플리케이션 데이터 볼륨(예: PV)을 포함하여 모든 클러스터 데이터가 영구적으로 삭제됩니다.

2.3.4.3. 취약점 관리

Red Hat은 업계 표준 툴을 사용하여 OpenShift Dedicated의 주기적인 취약점 스캔을 수행합니다. 확인된 취약점은 심각도에 따라 타임라인에 따라 수정에 추적됩니다. 취약점 스캔 및 수정 활동에는 규정 준수 인증 감사 과정에서 타사 평가자가 확인할 수 있도록 문서화되어 있습니다.

2.3.4.4. 네트워크 보안

2.3.4.4.1. 방화벽 및 CloudEvent 보호

각 OpenShift Dedicated 클러스터는 방화벽 규칙(AWS Security Groups 또는 Google Cloud Compute Engine 방화벽 규칙)을 사용하여 클라우드 인프라 수준에서 보안 네트워크 구성으로 보호됩니다. AWS의 OpenShift Dedicated 고객도 AWS Shield Standard 를 사용하여 DDoS 공격으로부터 보호됩니다. 마찬가지로 GCP의 OpenShift Dedicated에서 사용하는 모든 GCP 로드 밸런서 및 공용 IP 주소는 Google Cloud Armor Standard 를 사용하여 DDoS 공격으로부터 보호됩니다.

2.3.4.4.2. 프라이빗 클러스터 및 네트워크 연결

고객은 선택적으로 인터넷에서 클러스터 컨트롤 플레인 또는 애플리케이션에 액세스할 수 없도록 OpenShift Dedicated 클러스터 끝점(웹 콘솔, API 및 애플리케이션 라우터)을 비공개로 구성할 수 있습니다.

AWS의 경우 고객은 AWS VPC 피어링, AWS VPN 또는 AWS Direct Connect를 통해 OpenShift Dedicated 클러스터에 대한 프라이빗 네트워크 연결을 구성할 수 있습니다.

참고

현재 Google Cloud의 OpenShift Dedicated 클러스터에서 프라이빗 클러스터는 지원되지 않습니다.

2.3.4.4.3. 클러스터 네트워크 액세스 제어

NetworkPolicy 오브젝트와 OpenShift SDN을 사용하여 프로젝트별로 세분화된 네트워크 액세스 제어 규칙을 구성할 수 있습니다.

2.3.4.5. Penetration 테스트

Red Hat은 OpenShift Dedicated에 대해 주기적인 침투 테스트를 수행합니다. 테스트는 산업 표준 툴과 모범 사례를 사용하여 독립적인 내부 팀에서 수행합니다.

발견된 문제는 심각도에 따라 우선 순위가 지정됩니다. 오픈 소스 프로젝트에 속하는 모든 문제는 해결을 위해 커뮤니티와 공유됩니다.

2.3.4.6. 컴플라이언스

OpenShift Dedicated는 보안 및 제어를 위한 일반적인 업계 모범 사례를 따릅니다. 인증은 다음 표에 설명되어 있습니다.

표 2.2. OpenShift Dedicated의 보안 및 제어 인증

컴플라이언스	AWS의 OpenShift Dedicated	GCP의 OpenShift Dedicated
HIPAA 정규화된	제공됨 (고객 클라우드 서브스크립션만)	제공됨 (고객 클라우드 서브스크립션만)
ISO 27001	제공됨	제공됨
PCI DSS	제공됨	제공됨
SOC 2 Type 2	제공됨	제공됨

추가 리소스

- SRE residency에 대한 정보는 Red Hat Subprocessor List 를 참조하십시오.

2.3.5. 재해 복구

OpenShift Dedicated는 Pod, 작업자 노드, 인프라 노드, 컨트롤 플레인 노드 및 가용성 영역 수준에서 발생하는 오류에 대한 재해 복구를 제공합니다.

모든 재해 복구를 위해서는 고객이 원하는 가용성 수준을 고려하여 고가용성 애플리케이션, 스토리지 및 클러스터 아키텍처(예: 단일 영역 배포 vs. 다중 영역 배포)를 배포하는 모범 사례를 사용해야 합니다.

하나의 단일 영역 클러스터는 가용성 영역 또는 지역 중단 시 재해 방지 또는 복구를 제공하지 않습니다. 고객이 유지보수하는 장애 조치가 있는 여러 단일 영역 클러스터는 영역 또는 지역 수준에서의 중단을 설명할 수 있습니다.

하나의 다중 영역 클러스터는 전체 리전 중단 시 재해 방지 또는 복구를 제공하지 않습니다. 고객이 유지보수하는 장애 조치가 있는 여러 다중 영역 클러스터는 지역 수준에서의 중단을 설명할 수 있습니다.

2.3.6. 추가 리소스

- Red Hat 사이트 안정성 엔지니어링 (SRE) 팀 액세스에 대한 자세한 내용은 ID 및 액세스 관리를 참조하십시오.

2.4. SRE 및 서비스 계정 액세스

2.4.1. ID 및 액세스 관리

대부분의 SRE(사이트 안정성 엔지니어링) 팀은 자동화된 구성 관리를 통해 클러스터 Operator를 사용하여 수행됩니다.

2.4.1.1. 하위 프로세서

사용 가능한 하위 프로세서 목록은 Red Hat 고객 포털의 Red Hat 하위 프로세서 목록을 참조하십시오.

2.4.1.2. 모든 OpenShift Dedicated 클러스터에 대한 SRE 액세스

SRES는 프록시를 통해 OpenShift Dedicated 클러스터에 액세스합니다. 프록시는 로그인할 때 SREs에 대한 OpenShift Dedicated 클러스터에서 서비스 계정을 mints합니다. OpenShift Dedicated 클러스터에 대해 구성된 ID 공급자가 없으므로 SREs는 로컬 웹 콘솔 컨테이너를 실행하여 프록시에 액세스합니다. SRES는 클러스터 웹 콘솔에 직접 액세스하지 않습니다. SRES는 감사 가용성을 보장하기 위해 개별 사용자로 인증해야 합니다. 모든 인증 시도가 SIEM(Security Information and Event Management) 시스템에 기록됩니다.

2.4.1.3. OpenShift Dedicated에서 권한 있는 액세스 제어

Red Hat SRE는 OpenShift Dedicated 및 퍼블릭 클라우드 공급자 구성 요소에 액세스할 때 최소 권한 원칙을 따릅니다. 수동 SRE 액세스의 네 가지 기본 카테고리가 있습니다.

- 일반적인 2 단계 인증으로 Red Hat Customer Portal을 통한 SRE 관리자 액세스 권한 없음
- 정상적인 2 단계 인증으로 Red Hat 기업 SSO를 통한 SRE 관리자 액세스 및 권한 없는 고도.
- Red Hat SSO를 사용한 수동 승격인 OpenShift 승격. 모든 운영 SREs make에 대해 완전히 감사되고 관리 승인이 필요합니다.
- 클라우드 공급자 콘솔 또는 CLI 액세스를 위한 수동 승격인 클라우드 공급자 액세스 또는 승격. 액세스는 60분으로 제한되며 완전히 감사됩니다.

이러한 액세스 유형에는 각각 다른 구성 요소에 대한 액세스 수준이 있습니다.

구성 요소	일반적인 SRE 관리자 액세스(Red Hat 고객 포털)	일반적인 SRE 관리자 액세스(Red Hat SSO)	OpenShift 고도	클라우드 공급자 액세스
OpenShift Cluster Manager	R/W	액세스 권한 없음	액세스 권한 없음	액세스 권한 없음
OpenShift 웹 콘솔	액세스 권한 없음	R/W	R/W	액세스 권한 없음
노드 운영 체제	액세스 권한 없음	승격된 OS 및 네트워크 권한의 특정 목록입니다.	승격된 OS 및 네트워크 권한의 특정 목록입니다.	액세스 권한 없음
AWS Console	액세스 권한 없음	액세스 권한은 없지만 클라우드 공급자 액세스를 요청하는 데 사용되는 계정입니다.	액세스 권한 없음	SRE ID를 사용하는 모든 클라우드 공급자 권한.

2.4.1.4. 클라우드 인프라 계정에 대한 SRE 액세스

Red Hat 직원은 일상적인 OpenShift Dedicated 작업 과정에서 클라우드 인프라 계정에 액세스하지 않습니다. 긴급 문제 해결을 위해 Red Hat SRE는 클라우드 인프라 계정에 액세스하기 위한 잘 정의되고 감사 가능한 절차가 있습니다.

AWS에서 SREs는 AWS STS(보안 토큰 서비스)를 사용하여 **BYOCAdminAccess** 사용자에 대한 단기 AWS 액세스 토큰을 생성합니다. STS 토큰에 대한 액세스는 감사 기록 및 개별 사용자로 추적할 수 있습니다. **BYOCAdminAccess** 에는 **AdministratorAccess** IAM 정책이 연결되어 있습니다.

Google Cloud에서 SREs 액세스 리소스는 Red Hat SAML ID 공급자(IDP)에 대해 인증됩니다. IDP는 라이브 만료 기간이 있는 토큰을 인증합니다. 토큰 발행은 기업 Red Hat IT에서 감사할 수 있으며 개별 사용자와 다시 연결됩니다.

2.4.1.5. Red Hat 지원 액세스

Red Hat CEE 팀의 구성원은 일반적으로 클러스터의 일부에 대한 읽기 전용 액세스 권한을 갖습니다. 특히 CEE는 핵심 및 제품 네임스페이스에 대한 액세스를 제한하고 고객 네임스페이스에 대한 액세스 권한이 없습니다.

Role	코어 네임스페이스	계층화된 제품 네임스페이스	고객 네임스페이스	클라우드 인프라 계정*
OpenShift SRE	읽기: 모두 쓰기: Very 제한된 [1]	읽기: 모두 쓰기: 없음	읽기: None[2] 쓰기: 없음	읽기: 모두 [3] 모두 쓰기 [3]
CEE	읽기: 모두 쓰기: 없음	읽기: 모두 쓰기: 없음	읽기: None[2] 쓰기: 없음	읽기: 없음 쓰기: 없음
고객 관리자	읽기: 없음 쓰기: 없음	읽기: 없음 쓰기: 없음	읽기: 모두 쓰기: 모두	읽기: Limited[4] 쓰기: 제한됨[4]
고객 사용자	읽기: 없음 쓰기: 없음	읽기: 없음 쓰기: 없음	읽기: 제한됨[5] 쓰기: 제한됨[5]	읽기: 없음 쓰기: 없음
다른 모든 사람	읽기: 없음 쓰기: 없음	읽기: 없음 쓰기: 없음	읽기: 없음 쓰기: 없음	읽기: 없음 쓰기: 없음

Cloud Infrastructure Account는 기본 AWS 또는 Google Cloud 계정을 나타냅니다.

1. 실패한 배포, 클러스터 업그레이드, 잘못된 작업자 노드 교체와 같은 일반적인 사용 사례 처리로 제한됩니다.
2. Red Hat 직원은 기본적으로 고객 데이터에 액세스할 수 없습니다.
3. 클라우드 인프라 계정에 대한 SRE 액세스는 문서화된 문제 발생 시 예외적인 문제 해결을 위한 "중요" 절차입니다.
4. 고객 관리자는 Cloud Infrastructure Access를 통해 클라우드 인프라 계정 콘솔에 대한 액세스가 제한되어 있습니다.
5. 고객 관리자가 RBAC를 통해 부여한 항목 및 사용자가 생성한 네임스페이스로 제한됩니다.

2.4.1.6. 고객 액세스

고객 액세스는 고객이 생성한 네임스페이스 및 고객 관리자 역할에서 RBAC를 사용하여 부여하는 권한으로 제한됩니다. 기본 인프라 또는 제품 네임스페이스에 대한 액세스는 일반적으로 **cluster-admin** 액세스 없이 허용되지 않습니다. 고객 액세스 및 인증에 대한 자세한 내용은 설명서의 인증 이해 섹션에서 확인할 수 있습니다.

2.4.1.7. 액세스 승인 및 검토

새로운 SRE 사용자 액세스에는 관리 승인이 필요합니다. 분리되거나 전송된 SRE 계정은 자동화된 프로세스를 통해 권한 있는 사용자로 제거됩니다. 또한 SRE는 권한 있는 사용자 목록의 관리 서명을 포함하여 정기적인 액세스 검토를 수행합니다.

2.4.2. SRE 클러스터 액세스

OpenShift Dedicated 클러스터에 대한 SRE 액세스는 여러 필수 인증 계층을 통해 제어되며, 모두 엄격한 회사 정책에 의해 관리됩니다. 모든 인증 시도는 클러스터에 액세스하려고 하며 클러스터 내의 변경 사항은 해당 작업을 담당하는 SRE의 특정 계정 ID와 함께 감사 로그 내에 기록됩니다. 이러한 감사 로그는 고객의 클러스터에 대한 모든 변경 사항이 Red Hat의 관리 서비스 지침을 구성하는 엄격한 정책과 절차를 준수하는지 확인하는 데 도움이 됩니다.

아래에 제시된 정보는 SRE가 고객의 클러스터에 액세스하기 위해 수행해야 하는 프로세스에 대한 개요입니다.

- SRE는 Red Hat SSO(Cloud Services)에서 새로 고침 ID 토큰을 요청합니다. 이 요청이 인증됩니다. 토큰은 15분 동안 유효합니다. 토큰이 만료되면 토큰을 다시 새로고침하여 새 토큰을 수신할 수 있습니다. 새 토큰으로 새로 고침하는 기능은 무제한입니다. 그러나 새 토큰으로 새로 고침하는 기능은 비활성화 후 30일 후에 취소됩니다.

- SRE는 Red Hat VPN에 연결됩니다. VPN에 대한 인증은 Red Hat Corporate Identity and Access Management 시스템(RH IAM)에 의해 완료됩니다. RH IAM을 사용하면 SRE는 다중 요소이며 그룹 및 기존 온보딩 및 오프보딩 프로세스를 통해 조직당 내부적으로 관리할 수 있습니다. SRE가 인증 및 연결되면 SRE가 클라우드 서비스 플릿 관리 플레인에 액세스할 수 있습니다. 클라우드 서비스 플릿 관리 플레인을 변경하려면 많은 승인 계층이 필요하며 엄격한 회사 정책에 의해 유지 관리됩니다.

- 권한 부여가 완료되면 플릿 관리 플레인에 SRE 로그가 기록되고 플릿 관리 플레인에서 생성한 서비스 계정 토큰이 수신됩니다. 토큰은 15분 동안 유효합니다. 토큰이 더 이상 유효하지 않으면 삭제됩니다.

- 플릿 관리 플레인에 대한 액세스 권한이 부여된 SRE는 네트워크 구성에 따라 다양한 방법을 사용하여 클러스터에 액세스합니다.

    - 프라이빗 또는 공용 클러스터에 액세스: 포트 6443에서 암호화된 HTTP 연결을 사용하여 요청이 특정 NLB(Network Load Balancer)를 통해 전송됩니다.

    - PrivateLink 클러스터에 액세스: 요청이 Red Hat Transit Gateway로 전송되어 리전당 Red Hat VPC에 연결됩니다. 요청을 수신하는 VPC는 대상 프라이빗 클러스터 리전에 따라 달라집니다. VPC에는 고객의 PrivateLink 클러스터에 대한 PrivateLink 엔드포인트가 포함된 프라이빗 서브넷이 있습니다.

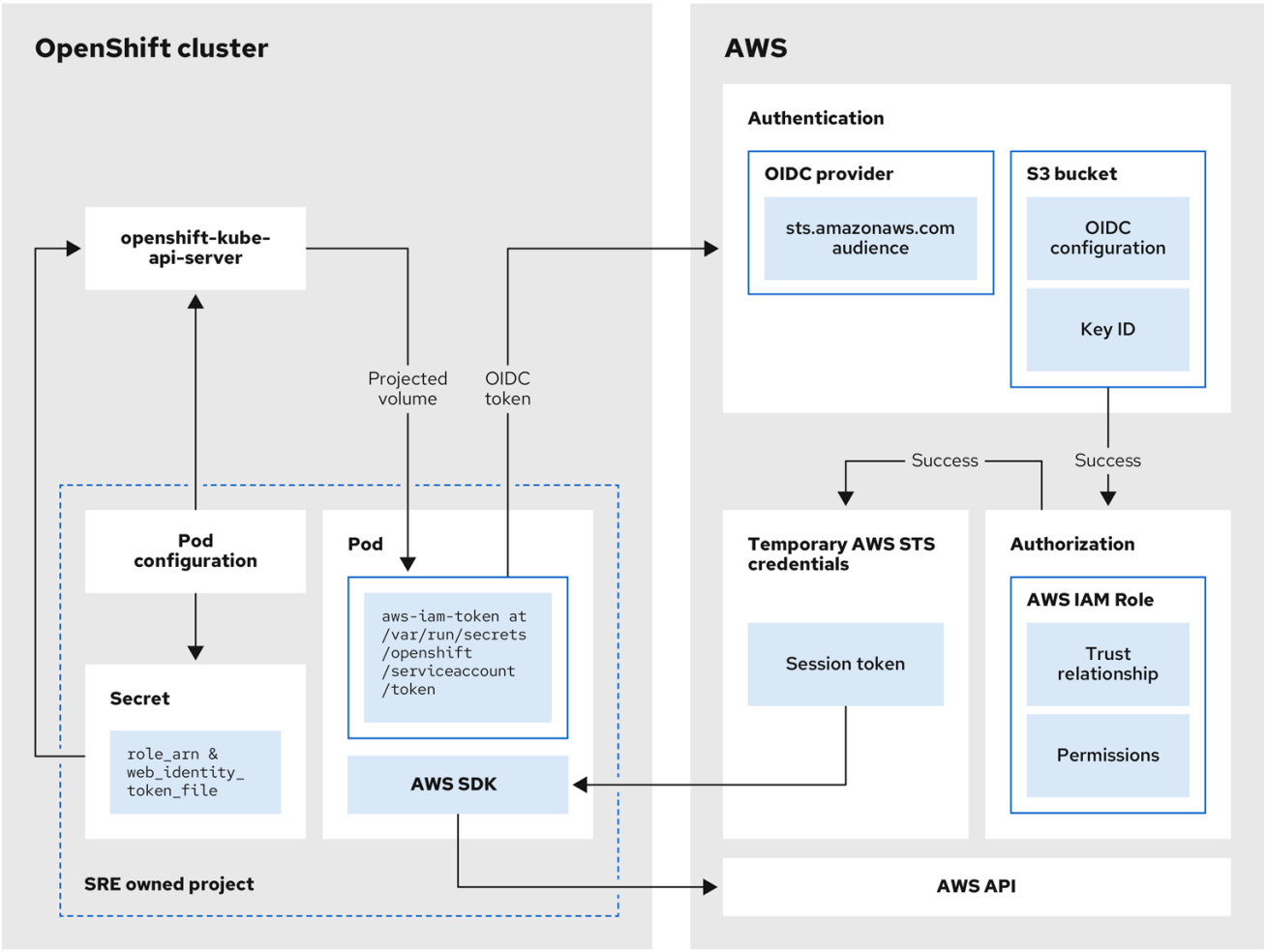
2.4.3. 서비스 계정에서 SRE 보유 프로젝트에서 AWS IAM 역할을 가정하는 방법

AWS STS(Security Token Service)를 사용하는 OpenShift Dedicated 클러스터를 설치하면 클러스터별 Operator AWS IAM(Identity and Access Management) 역할이 생성됩니다. 이러한 IAM 역할을 사용하면 OpenShift Dedicated 클러스터 Operator가 핵심 OpenShift 기능을 실행할 수 있습니다.

클러스터 Operator는 서비스 계정을 사용하여 IAM 역할을 가정합니다. 서비스 계정에서 IAM 역할을 가정하면 서비스 계정에서 클러스터 Operator의 Pod에서 사용할 임시 STS 인증 정보가 제공됩니다. assumed 역할에 필요한 AWS 권한이 있는 경우 서비스 계정에서 Pod에서 AWS SDK 작업을 실행할 수 있습니다.

SRE 보유 프로젝트에서 AWS IAM 역할을 가정하기 위한 워크플로우
다음 다이어그램은 SRE 보유 프로젝트에서 AWS IAM 역할을 가정하는 워크플로우를 보여줍니다.

그림 2.1. SRE 보유 프로젝트에서 AWS IAM 역할을 가정하기 위한 워크플로우



워크플로우에는 다음 단계가 있습니다.

1. 클러스터 Operator가 실행하는 각 프로젝트 내에서 Operator의 배포 사양에는 예상 서비스 계정 토큰에 대한 볼륨 마운트와 Pod에 대한 AWS 인증 정보 구성이 포함된 시크릿이 있습니다. 토큰은 오디언스 바인딩 및 시간 바인딩입니다. OpenShift Dedicated는 매시간 새 토큰을 생성하고 AWS SDK는 AWS 인증 정보 구성이 포함된 마운트된 시크릿을 읽습니다. 이 구성에는 마운트된 토큰 및 AWS IAM 역할 ARN의 경로가 있습니다. 시크릿의 인증 정보 구성에는 다음이 포함됩니다.

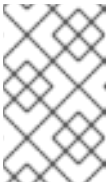
    - AWS SDK 작업을 실행하는 데 필요한 권한이 있는 IAM 역할에 대한 ARN이 있는 **$AWS_ARN_ROLE** 변수.

    - 서비스 계정의 OpenID Connect(OIDC) 토큰으로 Pod의 전체 경로가 있는 **$AWS_LOAD_IDENTITY_TOKEN_FILE** 변수. 전체 경로는 **/var/run/secrets/openshift/serviceaccount/token** 입니다.

2. 클러스터 Operator에서 AWS IAM 역할로 간주하여 AWS IAM 역할(예: EC2)을 가정해야 하는 경우 Operator에서 실행되는 AWS SDK 클라이언트 코드는 **AssumeRoleWithWebIdentity** API 호출을 호출합니다.

3. OIDC 토큰은 Pod에서 OIDC 공급자로 전달됩니다. 다음 요구 사항이 충족되면 공급자는 서비스 계정 ID를 인증합니다.

   - ID 서명은 유효하며 개인 키로 서명됩니다.
   - **sts.amazonaws.com** 대상은 OIDC 토큰에 나열되며 OIDC 공급자에 구성된 대상과 일치합니다.

     참고

     STS 클러스터를 사용하는 OpenShift Dedicated에서는 설치 중에 OIDC 공급자가 생성되고 기본적으로 서비스 계정 발행자로 설정됩니다.
     sts.amazonaws.com 대상은 OIDC 공급자에 기본적으로 설정됩니다.

   - OIDC 토큰이 만료되지 않았습니다.
   - 토큰의 발행자 값에는 OIDC 공급자의 URL이 있습니다.

4. 프로젝트 및 서비스 계정이 가정 중인 IAM 역할에 대한 신뢰 정책 범위에 있는 경우 권한 부여가 성공합니다.

5. 인증 및 권한 부여에 성공하면 AWS 액세스 토큰, 시크릿 키 및 세션 토큰 형식의 임시 AWS STS 인증 정보가 서비스 계정에서 사용할 수 있도록 Pod에 전달됩니다. 인증 정보를 사용하면 서비스 계정에 IAM 역할에 활성화된 AWS 권한이 일시적으로 부여됩니다.

6. 클러스터 Operator가 실행되면 Pod에서 AWS SDK를 사용하는 Operator는 예상 서비스 계정에 대한 경로가 있는 시크릿과 AWS IAM 역할 ARN을 사용하여 OIDC 공급자에 대해 인증합니다. OIDC 공급자는 AWS API에 대한 인증에 대한 임시 STS 자격 증명을 반환합니다.

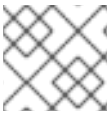
2.5. OPENSHIFT DEDICATED의 가용성 이해

가용성 및 재해 방지는 모든 애플리케이션 플랫폼에서 매우 중요한 요소입니다. OpenShift Dedicated는 여러 수준에서 장애에 대한 많은 보호 기능을 제공하지만 고객이 배포한 애플리케이션은 고가용성을 위해 적절하게 구성해야 합니다. 또한 발생할 수 있는 클라우드 공급자 중단을 고려하여 여러 가용성 영역에 클러스터를 배포하거나 장애 조치 메커니즘을 사용하여 여러 클러스터를 유지 관리하는 등 다른 옵션을 사용할 수 있습니다.

2.5.1. 잠재적인 실패 지점

OpenShift Container Platform에서는 다운타임으로부터 워크로드를 보호할 수 있는 다양한 기능과 옵션을 제공하지만 이러한 기능을 활용하기 위해서는 애플리케이션을 적절하게 조정해야 합니다.

OpenShift Dedicated는 Red Hat site Reliability Engineer(SRE) 지원 및 다중 영역 클러스터를 배포하는 옵션을 추가하여 여러 가지 일반적인 Kubernetes 문제를 추가로 보호할 수 있지만 컨테이너 또는 인프라가 여전히 실패할 수 있는 여러 가지 방법이 있습니다. 잠재적인 장애 지점을 이해하면 위험을 이해하고 애플리케이션과 클러스터를 각각의 특정 수준에서 필요에 따라 탄력적으로 조정할 수 있습니다.



참고

중단은 여러 수준의 인프라 및 클러스터 구성 요소에서 발생할 수 있습니다.

2.5.1.1. 컨테이너 또는 Pod 실패

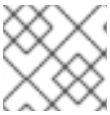
Pod는 설계상 짧은 기간 동안 존재해야 합니다. 애플리케이션 Pod의 여러 인스턴스가 실행되는 개별 Pod 또는 컨테이너의 문제로부터 보호되도록 서비스를 적절하게 스케일링합니다. 노드 스케줄러는 복원력을 추가로 개선하기 위해 이러한 워크로드가 서로 다른 작업자 노드에 분산되어 있는지도 확인할 수 있습니다.

가능한 Pod 오류를 처리할 때 스토리지가 애플리케이션에 연결된 방식을 이해하는 것도 중요합니다. 단일 포드에 연결된 단일 영구 볼륨은 포드 확장의 모든 이점을 활용할 수 없지만 복제된 데이터베이스, 데이터베이스 서비스 또는 공유 스토리지는 가능합니다.

계획된 유지 관리 기간(예: 업그레이드) 동안 애플리케이션의 중단을 방지하려면 Pod 중단 예산을 정의하는 것이 중요합니다. 이는 Kubernetes API의 일부이며 다른 오브젝트 유형과 마찬가지로 OpenShift CLI(**oc**)를 사용하여 관리할 수 있습니다. 유지 관리를 위해 노드를 드레이닝하는 것과 같이 작업 중에 pod에 대한 보안 제약 조건을 지정할 수 있습니다.

2.5.1.2. 작업자 노드 장애

작업자 노드는 애플리케이션 pod가 포함된 가상 머신입니다. 기본적으로 OpenShift Dedicated 클러스터에는 단일 가용성 영역 클러스터에 대해 최소 4개의 작업자 노드가 있습니다. 작업자 노드 오류가 발생하는 경우 기존 노드와 관련된 문제가 해결되거나 노드가 교체될 때까지 충분한 용량이 있는 한 작업자 노드가 작동되도록 Pod가 재배치됩니다. 더 많은 작업자 노드는 단일 노드 중단을 방지할 수 있으며 노드 장애가 발생할 경우 Pod를 다시 예약할 수 있는 적절한 클러스터 용량을 보장합니다.



참고

가능한 노드 오류를 처리할 때 스토리지의 영향을 이해하는 것도 중요합니다.

2.5.1.3. 클러스터 장애

OpenShift Dedicated 클러스터에는 3개 이상의 컨트롤 플레인 노드와 3개의 인프라 노드가 있으며, 이 노드는 단일 영역 또는 선택한 클러스터 유형에 따라 여러 영역에서 사전 구성되어 있습니다. 즉, 컨트롤 플레인 및 인프라 노드는 작업자 노드와 동일한 복원력을 가지며 Red Hat에서 완전히 관리할 수 있는 추가 이점이 있습니다.

완전한 컨트롤 플레인 노드 중단이 발생하면 OpenShift API가 작동하지 않으며 기존 작업자 노드 pod는 영향을 받지 않습니다. 그러나 Pod 또는 노드 중단이 동시에 발생하는 경우 새 Pod 또는 노드를 추가하거나 예약하기 전에 컨트롤 플레인 노드를 복구해야 합니다.

인프라 노드에서 실행되는 모든 서비스는 Red Hat에서 고가용성으로 구성하고 인프라 노드에 분산합니다. 완전한 인프라 중단이 발생하는 경우 이러한 노드가 복구될 때까지 이러한 서비스를 사용할 수 없습니다.

2.5.1.4. 영역 장애

퍼블릭 클라우드 공급자의 영역 오류는 작업자 노드, 블록 또는 공유 스토리지, 단일 가용성 영역과 관련된 로드 밸런서와 같은 모든 가상 구성 요소에 영향을 미칩니다. 영역 장애로부터 보호하기 위해 OpenShift Dedicated는 다중 가용 영역 클러스터라는 세 가지 가용성 영역에 분산된 클러스터에 대한 옵션을 제공합니다. 기존 상태 비저장 워크로드는 충분한 용량이 있는 경우 중단 시 영향을 받지 않는 영역에 재배포됩니다.

2.5.1.5. 스토리지 장애

상태 저장 애플리케이션을 배포한 경우 스토리지는 중요한 구성 요소이며 고가용성을 고려할 때 고려해야 합니다. 단일 블록 스토리지 PV는 Pod 수준에서도 중단을 방지할 수 없습니다. 스토리지의 가용성을 유지

하는 가장 좋은 방법은 복제된 스토리지 솔루션, 중단의 영향을 받지 않는 공유 스토리지 또는 클러스터와 무관한 데이터베이스 서비스를 사용하는 것입니다.

2.6. OPENSHIFT DEDICATED 업데이트 라이프 사이클

2.6.1. 개요

Red Hat은 고객 및 파트너사가 플랫폼에서 실행되는 애플리케이션을 효과적으로 계획, 배포 및 지원할 수 있도록 OpenShift Dedicated의 제품 라이프 사이클을 제공합니다. Red Hat은 투명성을 구현하기 위해 라이프 사이클을 공개하고 문제가 발생할 경우 이러한 정책에 예외가 있을 수 있습니다.

OpenShift Dedicated는 Red Hat OpenShift의 관리형 인스턴스이며 독립적인 릴리스 일정을 유지합니다. 관리형 오퍼링에 대한 자세한 내용은 OpenShift Dedicated 서비스 정의에서 확인할 수 있습니다. 특정 버전에 대한 보안 권고 및 버그 수정 권고의 가용성은 Red Hat OpenShift Container Platform 라이프 사이클 정책에 따라 다르며 OpenShift Dedicated 유지 관리 일정에 따라 다릅니다.

추가 리소스

- OpenShift Dedicated 서비스 정의

2.6.2. 정의

표 2.3. 버전 참조

버전 형식	메이저	마이너	패치	Major.minor.patch
	x	y	z	x.y.z
예제	4	5	21	4.5.21

주요 릴리스 또는 X 릴리스

주요 릴리스 또는 *X-release(X*.y.z)로만 참조됩니다.

예

- "major 릴리스 5" → 5.y.z
- "major 릴리스 4" → 4.y.z
- "major 릴리스 3" → 3.y.z

마이너 릴리스 또는 Y 릴리스

마이너 릴리스 또는 *Y-release(x.Y*.z)로만 참조됩니다.

예

- "최소 릴리스 4" → 4.4.z
- "minor 릴리스 5" → 4.5.z
- "minor 릴리스 6" → 4.6.z

패치 릴리스 또는 Z 릴리스

패치 릴리스 또는 *Z-release* (x.y.Z)라고 합니다.

예

- "마이너 릴리스 5의 패치 릴리스 14" → 4.5.14
- "마이너 릴리스 5의 패치 릴리스 25" → 4.5.25
- "마이너 릴리스 6의 패치 릴리스 26" → 4.6.26

2.6.3. 주요 버전 (X.y.z)

OpenShift Dedicated의 주요 버전(예: 버전 4)은 후속 주요 버전 릴리스 또는 제품 종료 후 1년 동안 지원됩니다.

예제

- 1월 1일 OpenShift Dedicated에서 버전 5를 사용할 수 있는 경우 12개월 동안 관리 클러스터에서 12개월까지 계속 실행할 수 있습니다. 이 기간 후에 클러스터를 업그레이드하거나 버전 5로 마이그레이션해야 합니다.

2.6.4. 마이너 버전 (x.Y.z)

Red Hat은 4.8 OpenShift Container Platform 마이너 버전부터는 지정된 마이너 버전의 정식 출시 후 최소 16개월 동안 모든 마이너 버전을 지원합니다. 패치 버전은 지원 기간의 영향을 받지 않습니다.

고객은 지원 기간이 종료 60일, 30일, 15일 전에 알림을 받습니다. 클러스터는 지원 기간이 종료되기 전에 지원되는 가장 오래된 마이너 버전의 최신 패치 버전으로 업그레이드해야 합니다. 그렇지 않으면 클러스터가 "제한된 지원" 상태가 됩니다.

예제

1. 고객의 클러스터는 현재 4.13.8에서 실행되고 있습니다. 4.13 마이너 버전은 2023년 5월 17일에 일반적으로 사용 가능하게 되었습니다.
2. 7월 19일, 8월 16일, 2024년 9월 2일, 고객은 클러스터가 지원되는 마이너 버전으로 업그레이드되지 않은 경우 2024년 9월 17일 "제한된 지원" 상태를 입력한다는 통지를 받습니다.
3. 클러스터는 2024년 9월 17일까지 4.14 이상으로 업그레이드해야 합니다.
4. 업그레이드가 수행되지 않은 경우 클러스터는 "제한된 지원" 상태로 표시됩니다.

2.6.5. 패치 버전 (x.y.Z)

마이너 버전이 지원되는 기간 동안 별도로 지정하지 않는 한 Red Hat은 모든 OpenShift Container Platform 패치 버전을 지원합니다.

플랫폼 보안 및 안정성의 이유로 패치 릴리스가 더 이상 사용되지 않을 수 있으므로 해당 릴리스의 설치를 방지하고 필수 업그레이드를 트리거할 수 있습니다.

예제

1. 4.7.6에는 중요한 CVE가 포함되어 있습니다.
2. CVE의 영향을 받는 모든 릴리스는 지원되는 패치 릴리스 목록에서 제거됩니다. 또한 4.7.6을 실행하는 모든 클러스터는 48시간 이내에 자동 업그레이드를 위해 예약됩니다.

2.6.6. 제한된 지원 상태

클러스터가 *제한된 지원* 상태로 전환되면 Red Hat은 더 이상 클러스터를 사전 모니터링하지 않으며 SLA는 더 이상 적용되지 않으며 SLA에 대해 요청된 크레딧이 거부됩니다. 이는 더 이상 제품 지원이 없다는 의미는 아닙니다. 일부 경우 위반 요인을 수정하면 클러스터가 완전히 지원되는 상태로 돌아갈 수 있습니다. 그러나 다른 경우에는 클러스터를 삭제하고 다시 생성해야 할 수도 있습니다.

다음 시나리오를 포함하여 여러 가지 이유로 클러스터가 제한된 지원 상태로 전환될 수 있습니다.

라이프 사이클 종료일 전에 클러스터를 지원되는 버전으로 업그레이드하지 않는 경우

Red Hat은 라이프 사이클 종료일 이후 버전에 대해 런타임 또는 SLA를 보장하지 않습니다. 지속적인 지원을 받으려면 만료일 이전에 클러스터를 지원되는 버전으로 업그레이드합니다. 지원 기간이 만료되기 전에 클러스터를 업그레이드하지 않으면 클러스터가 지원되는 버전으로 업그레이드할 때까지 제한된 지원 상태로 전환됩니다.
Red Hat은 지원되지 않는 버전에서 지원되는 버전으로 업그레이드하기 위해 상업적으로 합리적인 지원을 제공합니다. 그러나 지원되는 업그레이드 경로를 더 이상 사용할 수 없는 경우 새 클러스터를 생성하고 워크로드를 마이그레이션해야 할 수 있습니다.

기본 OpenShift Dedicated 구성 요소 또는 Red Hat에서 설치 및 관리하는 기타 구성 요소를 제거하거나 교체하는 경우

클러스터 관리자 권한이 사용된 경우 Red Hat은 인프라 서비스, 서비스 가용성 또는 데이터 손실에 영향을 미치는 사용자를 포함하여 인증된 사용자의 작업에 대해 책임을 지지 않습니다. Red Hat이 이러한 작업을 감지하면 클러스터가 제한된 지원 상태로 전환될 수 있습니다. Red Hat은 상태 변경 사항을 사용자에게 알려주며 클러스터를 삭제하고 다시 생성해야 하는 수정 단계를 살펴보기 위해 작업을 되돌리거나 지원 케이스를 생성해야 합니다.

클러스터가 제한된 지원 상태로 전환되거나 추가 지원이 필요한 특정 작업에 대한 질문이 있는 경우 지원 티켓을 엽니다.

2.6.7. 지원되는 버전 예외 정책

Red Hat은 새로운 버전 또는 기존 버전을 추가하거나 제거할 수 있는 권한을 보유하거나 향후 마이너 릴리스 버전을 지연할 수 있으며, 이는 사전 통지 없이 버그 또는 보안 문제에 영향을 미치는 하나 이상의 중요한 프로덕션에서 확인되었습니다.

2.6.8. 설치 정책

Red Hat은 최신 지원 릴리스를 설치하는 것을 권장하지만 OpenShift Dedicated에서는 이전 정책에서 적용되는 모든 지원 릴리스의 설치를 지원합니다.

2.6.9. 필수 업그레이드

심각하거나 중요한 CVE 또는 Red Hat에서 식별한 다른 버그가 클러스터의 보안 또는 안정성에 크게 영향을 미치는 경우 고객은 영업일 기준 2일 이내에 다음 지원 패치 릴리스로 업그레이드해야 합니다.

극단적인 상황에서 Red Hat은 환경에 대한 CVE의 심각성에 대한 평가에 따라 2 일 이내에 클러스터를 예약하거나 수동으로 업데이트하도록 고객에게 알립니다. 2 일 후 업데이트가 실행되지 않는 경우 Red Hat은 잠재적인 보안 위반 또는 불안정성을 완화하기 위해 클러스터를 최신 보안 패치 릴리스로 자동 업데이

트합니다. Red Hat은 자체 재량에 따라 지원 케이스 를 통해 고객이 요청한 경우 자동 업데이트를 일시적으로 지연할 수 있습니다.

2.6.10. 라이프 사이클 날짜

버전	정식 출시일 (GA)	종료일
4.16	2024년 7월 2일	2025년 11월 2일
4.15	2024년 2월 27일	2025년 6월 30일
4.14	2023년 10월 31일	2025년 2월 28일
4.13	2023년 5월 17일	2024년 9월 17일
4.12	2023년 1월 17일	2024년 7월 17일
4.11	2022년 8월 10일	2023년 12월 10일
4.10	2022년 3월 10일	2023년 9월 10일
4.9	2021년 10월 18일	2022년 12월 18일
4.8	2021년 7월 27일	2022년 9월 27일