Red Hat Advanced Cluster Management for Kubernetes 2.5

릴리스 노트

릴리스 노트에서 새로운 기능, 에라타 업데이트, 알려진 문제, 사용 중단 및 제거, tcpdump 및 FIPS 준비 상태에 대한 제품 고려 사항에 대해 알아보십시오.

Last Updated: 2023-09-18

Red Hat Advanced Cluster Management for Kubernetes 2.5 릴리스 노트

릴리스 노트에서 새로운 기능, 에라타 업데이트, 알려진 문제, 사용 중단 및 제거, tcpdump 및 FIPS 준비 상태에 대한 제품 고려 사항에 대해 알아보십시오.

법적 공지

초록

릴리스 노트에서 새로운 기능, 에라타 업데이트, 알려진 문제, 사용 중단 및 제거, tcpdump 및 FIPS 준비 상태에 대한 제품 고려 사항에 대해 알아보십시오.

차례

1장. 릴리스 노트

중요: Red Hat Advanced Cluster Management의 2.5 및 이전 버전이 제거되어 더 이상 지원되지 않습니다. 버전 2.5 및 이전 버전에 대한 문서는 업데이트되지 않습니다. 이 문서는 사용 가능한 상태로 남아 있을 수 있지만 에라타 또는 기타 사용 가능한 업데이트없이 더 이상 사용되지 않습니다.

모범 사례: Red Hat Advanced Cluster Management의 최신 버전으로 업그레이드합니다.

- Red Hat Advanced Cluster Management for Kubernetes의 새로운 기능
- 에라타 업데이트
- 알려진 문제 및 제한 사항
- 중단 및 제거
- Red Hat Advanced Cluster Management for Kubernetes 고려 사항의 requirements 준비
- FIPS 준비

1.1. RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES의 새로운 기능

Red Hat Advanced Cluster Management for Kubernetes는 기본 거버넌스, 클러스터 라이프사이클 관리 및 애플리케이션 라이프사이클 관리 기능을 통해 전체 Kubernetes 도메인을 가시성을 제공합니다. 이번 릴리스에서는 더 많은 환경에서 클러스터 관리, 애플리케이션의 GitOps 통합 등으로 이동할 수 있습니다.

중요: 일부 기능 및 구성 요소는 기술 프리뷰 로 확인 및 릴리스됩니다.

이 릴리스의 새로운 기능에 대해 자세히 알아보십시오.

- welcome to Red Hat Advanced Cluster Management for Kubernetes에서 Kubernetes용 Red Hat Advanced Cluster Management에 대한 개요를 확인하십시오.
- 오픈 소스 *오픈 클러스터 관리* 리포지토리는 오픈 커뮤니티의 상호 작용, 성장 및 기여를 위한 준비가 되어 있습니다. 참여하려면 open-cluster-management.io 를 참조하십시오. 자세한 내용은 GitHub 리포지토리에 액세스할 수 있습니다.
- 제품의 주요 구성 요소에 대한 자세한 내용은 Multicluster 아키텍처 주제를 참조하십시오.
- 시작하기 안내서는 *문제 해결 가이드* 뿐만 아니라 시작할 수 있는 일반적인 작업을 참조합니다.
- 웹 콘솔
  - 가시성
- 클러스터
- 애플리케이션
- 거버넌스

1.1.1. 웹 콘솔

- 콘솔 사이드바 탐색은 다른 제품과 일치하며 더 나은 사용자 환경을 제공합니다. 탐색에서 다양한 제품 기능에 액세스할 수 있습니다. 또한 *Search* 는 *홈* 탭의 탐색에서 사용할 수 있으며 더 이상 헤더에서 사용할 수 없습니다.

- Red Hat OpenShift Container Platform 4.10 릴리스 및 더 많은 하이브리드 콘솔을 사용하면 동적 플러그인을 사용할 수 있습니다. 런타임 시 로드된 클러스터에 동적 플러그인을 생성하고 배포하기 위해 OpenShift Container Platform 웹 콘솔에 동적 플러그인 추가 에 대한 OpenShift Container Platform 설명서를 참조하십시오.

- **참고:** OpenShift Container Platform 버전 4.8에서 4.10까지 플러그인을 활성화하지 않으면 *Perspective switcher* 에서 Red Hat Advanced Cluster Management를 사용할 수 있습니다. Red Hat Advanced Cluster Management 콘솔에 대한 자세한 내용은 콘솔 개요를 참조하십시오.

- Red Hat Advanced Cluster Management 플러그인은 일반적으로 OpenShift Container Platform 콘솔에서 활성화할 수 있습니다. 콘솔 개요 에서 이를 활성화하는 방법을 알아보십시오.

1.1.1.1. 가시성

- Red Hat Advanced Cluster Management는 OpenShift Container Platform 버전 3.11 Grafana 대시보드를 지원합니다. 자세한 내용은 *관찰 기능 활성화 의 MultiClusterObservability CR 생성* 섹션을 참조하십시오.

- 관찰 서비스에 사용하는 오브젝트 저장소에 액세스하기 위해 인증서를 사용자 지정합니다. 자세한 내용은 오브젝트 저장소에 액세스하기 위한 인증서 사용자 지정을 참조하십시오.

- 보안 서비스 토큰 자격 증명을 사용하여 관찰 서비스를 구성합니다. 구성할 사항에 대한 자세한 내용은 Observability API 를 참조하십시오.

- observability 서비스를 사용하여 메트릭을 외부 엔드포인트로 내보낼 수 있습니다. 자세한 내용은 외부 엔드포인트로 메트릭 내보내기 에서 참조하십시오.

- 단일 노드 OpenShift(SNO) 클러스터에 대한 동적 지표 수집이 지원됩니다. 자세한 내용은 단일 노드 OpenShift 클러스터에 대한 동적 지표를 참조하십시오.

1.1.2. 클러스터

- Red Hat Advanced Cluster Management를 통해 Submariner 멀티 클러스터 네트워킹 서비스를 통합하는 일부 기능을 일반적으로 사용할 수 있습니다. 자세한 내용은 Submariner 다중 클러스터 네트워킹 및 서비스 검색을 참조하십시오.

- Submariner 애드온을 활성화할 때 Globalnet 컨트롤러가 중복된 CIDR을 해결하도록 활성화합니다. 자세한 내용은 Globalnet 을 참조하십시오.

- hub 클러스터를 호스팅하고 AMQP(Advanced RISC Machine) 아키텍처에서 클러스터를 가져오고 관리합니다.

- Central Infrastucture Management는 베어 메탈, Red Hat OpenStack Platform, VMware vSphere 환경 또는 사용자 프로비저닝 인프라(UPI) 방법을 사용하여 설치된 경우 플랫폼이 **None** 입니다.

- 클러스터 생성 프로세스 중에 인프라 환경에 호스트를 검색하고 추가할 수 있습니다. 자세한 내용은 온-프레미스 환경에서 클러스터 만들기 를 참조하십시오.

- 이제 일반적으로 사용 가능한 **ManagedClusterSet** 을 사용하여 그룹의 모든 관리 클러스터에 대한 액세스를 관리합니다. **ManagedClusterSet** 은 세트에 특별히 할당되지 않은 모든 관리 클러스터에 대해 **기본** 관리 클러스터 세트를 생성합니다. 자세한 내용은 ManagedClusterSet 생성 및 관리를 참조하십시오.

- 클레임에 즉시 사용할 수 있는 클러스터 풀에서 여러 클러스터를 지정합니다. 자세한 내용은 클러스터 풀 스케일링 을 참조하십시오.
- Red Hat Advanced Cluster Management를 사용하여 Red Hat Virtualization에서 OpenShift Container Platform 클러스터를 생성합니다. 자세한 내용은 Red Hat Virtualization에서 클러스터 생성을 참조하십시오.
- 테인트 및 톨러레이션을 사용하여 관리 클러스터 및 관리형 클러스터 세트의 배치를 제어합니다. 자세한 내용은 테인트 및 허용 오차를 사용하여 관리 클러스터 배치를 참조하십시오.
- 확장 가능한 예약을 사용하여 클러스터 배치를 제어합니다. 자세한 내용은 확장 가능 예약을 참조하십시오.
- **backup-restore-enabled** 정책을 사용하여 백업 및 복원 구성 요소를 복구하는 방법을 알아봅니다. 자세한 내용은 정책을 사용한 백업 유효성 검사를 참조하십시오.
- Red Hat Advanced Cluster Management 검색을 사용하여 OpenShift Cluster Manager 에서 사용할 수 있는 OpenShift 4 클러스터를 찾습니다. Discovery는 일반적으로 사용할 수 있으며 API는 **v1alpha1** 에서 **v1** 로 업데이트됩니다.
  - 검색 후 관리할 클러스터를 가져올 수 있습니다. Discovery 서비스는 백엔드 및 콘솔 사용에 Discover Operator를 사용합니다. Discovery 서비스 도입 을 참조하십시오.
- Red Hat Advanced Cluster Management 콘솔을 사용하여 VMware vSphere 또는 Red Hat OpenStack Platform 클러스터를 생성할 때 인증 정보에 연결이 끊긴 클러스터의 속성을 지정할 수 있습니다. 자세한 내용은 VMware vSphere에 대한 인증 정보 생성 및 Red Hat OpenStack에 대한 인증 정보 생성을 참조하십시오.

인증 정보에서 프록시 연결의 속성을 지정합니다. 자세한 내용은 인증 정보 관리 개요에서 인프라 공급자에 대한 인증 정보 주제를 참조하십시오.

- *멀티 클러스터 엔진 Operator* 는 일반적으로 클러스터 관리를 개선하는 소프트웨어 운영자로 사용할 수 있습니다. 멀티 클러스터 엔진 Operator는 클라우드 및 데이터 센터 전반에서 Red Hat OpenShift Container Platform 및 Kubernetes 클러스터 라이프사이클 관리를 지원합니다. Red Hat OpenShift Container Platform은 멀티 클러스터 엔진 Operator의 전제 조건입니다.

기술 프리뷰:

기술 프리뷰로 사용할 수 있는 다음 클러스터 기능을 참조하십시오.

- **Managed-ServiceAccount** 구성 요소를 사용하면 관리 클러스터에서 서비스 계정을 생성하고 삭제할 수 있습니다. 구성 요소는 기본적으로 비활성화되어 있습니다.
  - 자세한 내용은 ManagedServiceAccount 추가 기능 활성화(기술 프리뷰) 의 *다중 클러스터 엔진 Operator* 설명서를 참조하십시오.
  - 자세한 내용은 MultiClusterHub 고급 구성의 Red Hat Advanced Cluster Management 설명서를 참조하십시오.
- **hypershift** 애드온을 사용하면 워크로드와 관리를 분리하여 대규모 OpenShift Container Platform 컨트롤 플레인을 호스팅할 수 있습니다. 구성 요소는 기본적으로 비활성화되어 있습니다.
  - 자세한 내용은 Hypershift 애드온(기술 프리뷰) 의 *다중 클러스터 엔진 Operator* 설명서를 참조하십시오.
  - 자세한 내용은 Hypershift 애드온(기술 프리뷰) 및 호스트된 컨트롤 플레인 클러스터 사용 (기술 프리뷰) 에서 Red Hat Advanced Cluster Management 설명서를 참조하십시오.

- HyperShift를 사용하여 호스트된 컨트롤 플레인 클러스터를 관리하고 프로비저닝합니다. 자세한 내용은 호스팅 컨트롤 플레인 클러스터 사용(기술 프리뷰) 을 참조하십시오.

다른 클러스터 주제의 경우 클러스터 관리를 참조하십시오.

1.1.3. 애플리케이션

- 배치 및 배치 결정 API가 **v1alpha1** 에서 **v1beta1** 로 업그레이드됩니다. 배치는 서브스크립션 및 애플리케이션 세트가 전달되는 **ClusterSet** 에 가입해야 하는 대상 클러스터를 정의합니다. **고급 구성의 콘솔에서 이 내용을 확인합니다**.

- 단일 애플리케이션 개요의 개별 탭에서 토폴로지에 액세스하여 모든 항목을 동시에 볼 수 있습니다. 토폴로지를 **읽고 각 토폴로지 요소를 확인하는 방법에서 토폴로지**에 대해 알아봅니다.

- **ApplicationSet** 은 이제 Argo CD 애플리케이션에 대한 다중 클러스터 지원을 추가하는 Argo CD의 하위 프로젝트로 일반적으로 사용할 수 있습니다. 제품 콘솔 편집기에서 **ApplicationSet** 을 생성할 수 있습니다. 애플리케이션 모델 및 정의를 참조하십시오.

- hub 클러스터의 관리 클러스터 및 **subscriptionReports** 의 상태는 가볍고 확장 가능합니다. 다음 세 가지 유형의 대체 상태 보고서를 참조하십시오.

  - 패키지 수준 **SubscriptionStatus**: 이는 **appsub** 네임스페이스의 애플리케이션에서 배포한 모든 리소스에 대해 자세한 상태가 있는 관리 클러스터의 애플리케이션 패키지 상태입니다.

  - 클러스터 수준 **SubscriptionReport**: 특정 클러스터에 배포된 모든 애플리케이션에 대한 전체 상태 보고서입니다.

  - 애플리케이션 수준 **SubscriptionReport**: 특정 애플리케이션이 배포되는 모든 관리 클러스터에 대한 전반적인 상태 보고서입니다.
    자세한 내용은 서브스크립션 보고서를 참조하십시오.

다른 애플리케이션 주제의 경우 애플리케이션 관리를 참조하십시오.

1.1.4. 거버넌스

- 선택적 YAML 필드인 **metadataComplianceType** 을 사용하여 다른 필드와 다른 오브젝트의 레이블 및 주석을 처리합니다. 자세한 내용은 정책 API 를 참조하십시오.

- 정책을 함께 그룹화하도록 설정합니다. 정책 세트 컨트롤러를 참조하십시오.

- 정책 생성에 정책 세트 생성이 지원됩니다. 정책 생성기를 참조하십시오.

- **보호 기능을 사용하여 허브 클러스터 정책 템플릿에 있는 중요한 데이터를 보호할** 수 있습니다. 또한 **fromSecret** 기능을 이제 허브 클러스터 정책 템플릿에서 사용할 수 있습니다. 자세한 내용은 보호 기능 섹션을 참조하십시오.

대시보드 및 정책 프레임워크에 대한 자세한 내용은 감독을 참조하십시오. ../../html-single/governance#governance

1.1.5. 애드온

- Red Hat OpenStack Platform 클러스터에 Submariner를 배포합니다. 자세한 내용은 Red Hat OpenStack Platform for Submariner 준비를 참조하십시오.

자세한 내용은 릴리스 노트 로 이동하십시오.

1.2. 확인된 문제

Kubernetes용 Red Hat Advanced Cluster Management의 알려진 문제를 검토합니다. 다음 목록에는 이 릴리스의 알려진 문제 또는 이전 릴리스에서 계속된 알려진 문제가 포함되어 있습니다. Red Hat OpenShift Container Platform 클러스터의 경우 OpenShift Container Platform 알려진 문제를 참조하십시오.

- 알려진 문제 문서
- 설치 알려진 문제
- 웹 콘솔의 알려진 문제
  - 가시성 알려진 문제
- 클러스터 관리 알려진 문제
- 애플리케이션 관리 알려진 문제
- 거버넌스 알려진 문제
- 알려진 문제 백업 및 복원
- Submariner 알려진 문제

1.2.1. 알려진 문제 문서

1.2.1.1. 고객 포털의 문서 링크에서 상위 수준 섹션에 링크할 수 있습니다.

경우에 따라 고객 포털의 Red Hat Advanced Cluster Management 설명서의 다른 섹션에 대한 내부 링크가 이름이 지정된 섹션에 직접 연결되지 않는 경우도 있습니다. 일부 경우에서는 링크가 가장 높은 수준 섹션으로 확인됩니다.

이 경우 지정된 섹션을 수동으로 확인하거나 다음 단계를 완료하여 해결할 수 있습니다.

1. 확인하지 않는 링크를 올바른 섹션으로 복사하여 브라우저 주소 표시줄에 붙여넣습니다. 예를 들면 **https://access.redhat.com/documentation/en-us/red_hat_advanced_cluster_management_for_kubernetes/2.5/html/clusters/index#volsync** 일 수 있습니다.

2. 링크에서 html을 **html -single** 로 바꿉니다. 새 URL을 읽을 수 있어야 합니다. **https://access.redhat.com/documentation/en-us/red_hat_advanced_cluster_management_for_kubernetes/2.5/html-single/clusters/index#volsync**

3. 새 URL로 링크하여 문서에서 지정된 섹션을 찾습니다.

1.2.2. 설치 알려진 문제

1.2.2.1. Red Hat Advanced Cluster Management를 업그레이드한 후에는 Pod가 백업되지 않을 수 있습니다.

Red Hat Advanced Cluster Management를 새 버전으로 업그레이드한 후 **StatefulSet** 에 속하는 일부 Pod는 **failed** 상태로 유지될 수 있습니다. 이 드물게 발생하는 경우는 알려진 Kubernetes 문제로 인해 발생합니다.

이 문제에 대한 해결 방법으로 실패한 Pod를 삭제합니다. Kubernetes는 올바른 설정으로 자동으로 다시 시작됩니다.

1.2.2.2. OpenShift Container Platform 클러스터 업그레이드 실패 상태

OpenShift Container Platform 클러스터가 업그레이드 단계에 있는 경우 클러스터 Pod가 재시작되고 클러스터가 1-5분의 변형에 대해 **업그레이드 실패** 상태로 남아 있을 수 있습니다. 이 동작은 예상되고 몇 분 후에 해결됩니다.

1.2.2.3. 업그레이드 후 두 개의 클러스터 Curator 컨트롤러가 동시에 실행됨

2.4.x에서 2.5.0으로 업그레이드한 후 두 개의 클러스터 큐레이터 컨트롤러가 동시에 실행될 수 있습니다. 클러스터 라이프사이클 **Ansible 통합을** 위한 일부 prehook 및 posthooks에 대해 두 개 이상의 AnsibleJob이 생성되었습니다. 이 문제를 해결하려면 다음 절차를 참조하십시오.

1. 실행 중인 클러스터 Curator 컨트롤러가 두 개 있는지 확인합니다. 다중 클러스터 엔진 Operator의 **multicluster-engine** 네임스페이스와 **open-cluster-management** 네임스페이스가 포함된 다음 명령을 실행합니다.

```
kubectl -n multicluster-engine get deploy cluster-curator-controller
```

```
kubectl -n open-cluster-management get deploy cluster-curator-controller
```

2. 두 개의 클러스터 Curator 컨트롤러가 실행 중인 경우 **open-cluster-management** 네임스페이스에서 **cluster-curator-controller** 를 삭제합니다. 다음 명령을 실행합니다.

```
kubectl -n open-cluster-management delete deploy cluster-curator-controller
```

1.2.2.4. 작동하지 않는 MultiClusterEngine 버튼 생성

Red Hat OpenShift Container Platform 콘솔에서 Kubernetes용 Red Hat Advanced Cluster Management for Kubernetes를 설치하면 다음 메시지가 포함된 팝업 창이 표시됩니다.

MultiClusterEngine required

이 Operator를 사용할 MultiClusterEngine 인스턴스를 생성합니다.

팝업 창의 **Create MultiClusterEngine** 버튼이 작동하지 않을 수 있습니다. 이 문제를 해결하려면 Provided APIs 섹션의 MultiClusterEngine 타일에서 **인스턴스 생성을** 선택합니다.

1.2.3. 웹 콘솔의 알려진 문제

1.2.3.1. Red Hat Advanced Cluster Management 버전 2.5.x에서 다크 모드가 지원되지 않음

Red Hat Advanced Cluster Management 버전 2.5.2 이상 2.5.x 버전은 Red Hat OpenShift Container Platform 버전 4.11에서 지원되지만 다크 모드는 Red Hat Advanced Cluster Management 2.5.x에서 지원되지 않습니다. 설정에서 다크 모드를 비활성화하거나 Red Hat Advanced Cluster Management 버전 2.6로 업그레이드하여 다크 모드를 활성화합니다.

1.2.3.2. Kubernetes Operator 버전 2.0.x의 멀티 클러스터 엔진에서 다크 모드가 지원되지 않음

Kubernetes Operator 버전 2.0.2 및 이후 2.0.x 버전의 멀티 클러스터 엔진은 Red Hat OpenShift Container Platform 버전 4.11에서 지원되지만, Kubernetes Operator 2.0.x의 멀티 클러스터 엔진에서 다크

모드가 지원되지 않습니다. 설정에서 다크 모드를 비활성화하거나 Kubernetes Operator 버전 2.1의 다중 클러스터 엔진으로 업그레이드하여 다크 모드를 활성화합니다.

1.2.3.3. LDAP 사용자 이름은 대소문자를 구분합니다.

LDAP 사용자 이름은 대소문자를 구분합니다. LDAP 디렉터리에 구성된 방식과 정확히 이름을 사용해야 합니다.

1.2.3.4. Firefox 이전 버전에서 콘솔 기능이 표시되지 않을 수 있음

이 제품은 Mozilla Firefox 74.0 또는 Linux, macOS 및 Windows에서 사용할 수 있는 최신 버전을 지원합니다. 최상의 콘솔 호환성을 위해 최신 버전으로 업그레이드합니다.

1.2.3.5. 검색 사용자 지정의 스토리지 크기 제한 사항

searchcustomization CR에서 스토리지 크기를 업데이트하면 PVC 구성이 변경되지 않습니다. 스토리지 크기를 업데이트해야 하는 경우 다음 명령으로 PVC (<***storageclassname>-search-redisgraph-0***)를 업데이트합니다.

```
oc edit pvc <storageclassname>-search-redisgraph-0
```

1.2.3.6. 검색 쿼리 구문 분석 오류

환경이 크고 스케일링에 대한 테스트가 더 필요한 경우 검색 쿼리가 시간 초과되어 오류 메시지가 표시될 수 있습니다. 이 오류는 검색 쿼리를 기다리는 동안 30초 후에 표시됩니다.

다음 명령을 사용하여 시간 초과를 확장합니다.

```
kubectl annotate route multicloud-console haproxy.router.openshift.io/timeout=Xs
```

1.2.3.7. 클러스터 세트의 네임스페이스 바인딩을 편집할 수 없음

admin 역할로 설정된 클러스터 세트의 네임스페이스 바인딩을 편집하면 다음 메시지와 유사한 오류가 발생할 수 있습니다.

ResourceError: managedclustersetbindings.cluster.open-cluster-management.io "<cluster-set>"는 허용되지 않습니다. 사용자 "<user>" cannot create/delete resource "managedclustersetbindings" in API group "cluster.open-cluster-management.io" in the namespace "<namespace>".

문제를 해결하려면 바인딩하려는 네임스페이스에서 **ManagedClusterSetBinding** 리소스를 생성하거나 삭제할 수 있는 권한이 있어야 합니다. 역할 바인딩을 사용하면 네임스페이스로 설정된 클러스터만 바인딩할 수 있습니다.

1.2.3.8. 클러스터 세부 정보의 거짓 스케일링 경고

콘솔에서 클러스터 세부 정보를 볼 때 노드 또는 *머신 풀* 탭에 다음 메시지가 표시될 수 있습니다.

현재 작업자 노드가 이 클러스터에서 제거되고 있습니다. 시스템 보기 버튼을 클릭하여 스케일링 작업의 상태를 확인합니다(이 콘솔에 변경 사항이 반영되는 데 몇 분이 걸릴 수 있음).

시스템 풀이 없는 경우 UPI(User Provisioned Infrastructure) 설치를 사용하는 공급자의 경우 false 경고를 무시합니다. 컨트롤 플레인에 포함되지 않은 작업자 노드가 있는 경우 경고가 표시됩니다. 작업자 노드가

시스템 풀을 스케일링하는 대신 클러스터에 직접 추가되는 경우 IPI(Installer Provisioned Infrastructure) 설치를 사용하여 프로비저닝된 클러스터에 대해 false 경고가 표시될 수도 있습니다.

1.2.4. 가시성 알려진 문제

1.2.4.1. 서비스 수준 개요 대시보드의 중복 로컬 클러스터

다양한 허브 클러스터에서 동일한 S3 스토리지를 사용하여 Red Hat Advanced Cluster Management 관찰 기능을 배포하는 경우 *중복된* **로컬 클러스터를** 탐지하여 *Kubernetes/Service-Level Overview/API Server* 대시보드에 표시할 수 있습니다. 중복된 클러스터는 다음 패널 내의 결과에 영향을 *미칩니다. 상위 클러스터, SLO를 초과하는 클러스터 수 및 SLO를 충족하는 클러스터 수입니다.* **local-cluster는** 공유 S3 스토리지와 관련된 고유한 클러스터입니다. 여러 **로컬 클러스터가 대시보드에 표시되지 않도록 하려면 각 고유 허브 클러스터에서 hub 클러스터 전용** S3 버킷을 사용하여 관찰 기능을 배포하는 것이 좋습니다.

1.2.4.2. Observability Endpoint Operator가 이미지를 가져오지 못했습니다.

MultiClusterObservability CustomResource(CR)에 배포할 pull-secret을 생성하고 **open-cluster-management-observability** 네임스페이스에 pull-secret이 없는 경우 observability 끝점 Operator가 실패합니다. 새 클러스터를 가져오거나 Red Hat Advanced Cluster Management로 생성된 Hive 클러스터를 가져오는 경우, 관리형 클러스터에서 수동으로 풀 이미지 시크릿을 생성해야 합니다.

자세한 내용은 관찰 기능 활성화를 참조하십시오.

1.2.4.3. ROKS 및 HyperShift 클러스터의 데이터가 없습니다.

Red Hat Advanced Cluster Management 관찰 기능은 기본 제공 대시보드 내의 일부 패널에 ROKS 클러스터 및 HyperShift 클러스터의 데이터를 표시하지 않습니다. 이는 ROKS와 HyperShift가 관리하는 서버에서 API Server 메트릭을 노출하지 않기 때문입니다. 다음 Grafana 대시보드에는 ROKS 및 HyperShift 클러스터를 지원하지 않는 패널이 포함되어 있습니다. **Kubernetes/API 서버,Kubernetes/Compute Resources/Workload,Kubernetes/Compute Resources/Namespace(Workload)**

1.2.4.4. ROKS 및 HyperShift 클러스터에서 etcd 데이터가 없습니다.

ROKS 클러스터 및 HyperShift 클러스터의 경우 Red Hat Advanced Cluster Management 관찰 기능은 대시보드의 *etcd* 패널에 데이터를 표시하지 않습니다.

1.2.4.5. search-collector Pod별 CPU 사용량 증가

1000개의 클러스터를 관리하는 허브 클러스터에서 검색이 비활성화되면 메모리 부족 오류(OOM)로 인해 검색이 중단됩니다. **다음 단계를 완료합니다.**

1. **hub 클러스터에서 검색이 비활성화되어 있습니다. 즉 search-redisgraph-pod 가 배포되지 않음을 나타내는 경우 search-collector 배포를 0 개의 복제본으로 축소하여 메모리 사용량을 줄입니다.**

2. **hub 클러스터에서 검색을 활성화하면 search-redisgraph-pod 가 배포되었음을 나타내는 경우 search-collector 배포를 편집하여 할당된 메모리를 늘립니다.**

1.2.4.6. 잘못된 인증서로 인해 검색 Pod가 TLS 핸드셰이크를 완료하지 못했습니다.

드문 경우지만 인증서 변경 후 검색 Pod가 자동으로 재배포되지 않습니다. 이로 인해 서비스 Pod에서 인증서가 일치하지 않아 TLS(Transport Layer Security) 핸드셰이크가 실패합니다. 이 문제를 해결하려면 검색 Pod를 다시 시작하여 인증서를 재설정합니다.

1.2.4.7. Grafana 콘솔에서 메트릭을 사용할 수 없음

- Grafana 콘솔에서 주석 쿼리가 실패했습니다.

  Grafana 콘솔에서 특정 주석을 검색할 때 만료된 토큰으로 인해 다음 오류 메시지가 표시될 수 있습니다.

  "annotation Query Failed"

  브라우저를 새로 고치고 hub 클러스터에 로그인했는지 확인합니다.

- *rbac-query-proxy* Pod의 오류:

  managedcluster 리소스에 대한 무단 액세스 권한으로 인해 클러스터 또는 프로젝트를 쿼리할 때 다음과 같은 오류가 발생할 수 있습니다.

  프로젝트 또는 클러스터를 찾을 수 없음

  역할 권한을 확인하고 적절하게 업데이트합니다. 자세한 내용은 역할 기반 액세스 제어를 참조하십시오.

1.2.4.8. 관리형 클러스터에서 Prometheus 데이터 손실

기본적으로 OpenShift의 Prometheus는 임시 스토리지를 사용합니다. Prometheus는 다시 시작할 때마다 모든 지표 데이터가 손실됩니다.

Red Hat Advanced Cluster Management에서 관리하는 OpenShift Container Platform 관리 클러스터에서 관찰 기능이 활성화 또는 비활성화되면 observability 끝점 Operator는 로컬 Prometheus를 자동으로 다시 시작하는 alertmanager 구성을 추가하여 cluster-monitoring-config ConfigMap 을 업데이트합니다.

1.2.4.9. 순서가 없는 샘플을 수집하는 동안 오류 발생

가시성은 **Pod** 에서 다음 오류 메시지를 보고합니다.

> Error on ingesting out-of-order samples

오류 메시지는 메트릭 수집 간격 동안 관리 클러스터에서 보낸 시계열 데이터가 이전 수집 간격으로 보낸 시계열 데이터보다 오래되었음을 나타냅니다. 이 문제가 발생하면 **Thanos** 수신자에 의해 데이터가 삭제되고 **Grafana** 대시보드에 표시된 데이터에 차이가 발생할 수 있습니다. 오류가 자주 표시되는 경우 지표 컬렉션 간격을 더 높은 값으로 늘리는 것이 좋습니다. 예를 들어 간격을 **60** 초로 늘릴 수 있습니다.

이 문제는 시계열 간격이 **30**초와 같이 더 낮은 값으로 설정된 경우에만 발생합니다. 지표 수집 간격이 기본값 **300**초로 설정된 경우에는 이 문제가 표시되지 않습니다.

1.2.4.10. 관리 클러스터에서 Grafana 배포가 실패

매니페스트 크기가 **50000**바이트를 초과하는 경우 **Grafana** 인스턴스는 관리 클러스터에 배포되지 않습니다. 관찰 기능을 배포한 후 **Grafana**에 **local-cluster** 만 나타납니다.

1.2.5. 클러스터 관리 알려진 문제

클러스터 관리에 대한 다음과 같은 알려진 문제 및 제한 사항을 참조하십시오.

1.2.5.1. 클러스터 생성에 대한 연결이 끊긴 설치 설정을 입력할 수 없거나 입력한 경우 무시됩니다.

베어 메탈 공급자 및 연결이 끊긴 설치를 사용하여 클러스터를 생성할 때 연결 해제된 *설치의 구성* 섹션에 해당 인증 정보에 모든 설정을 저장해야 합니다. 클러스터 생성 콘솔 편집기에 입력할 수 없습니다.

VMware vSphere 또는 **Red Hat OpenStack Platform** 공급자와 연결이 끊긴 설치를 사용하여 클러스터를 생성할 때 인증서가 미러 레지스트리에 액세스해야 하는 경우 *연결이 끊긴 설치 섹션* 의 구성의 *추가 신뢰 번들* 필드에 입력해야 합니다. 클러스터 생성 콘솔 편집기에 해당 인증서를 입력하면 무시됩니다.

1.2.5.2. 연결이 끊긴 설치 프로그램이 있는 인증 정보에서 인증서를 구분하지 않음

베어 메탈, **VMware vSphere** 또는 **Red Hat OpenStack Platform** 공급자에 대한 인증 정보를 생성할 때 *설치 프로그램이 인증서를 구분하지 않으므로 프록시 및* 구성의 *추가 신뢰 번들* 필드에 동일한 값이 포함되어 있습니다. 이러한 기능은 독립적으로 사용할 수 있으며 프록시 및 연결이 끊긴 설치에 다른 인증서가 필요한 경우 필드에 여러 인증서를 입력할 수 있습니다.

1.2.5.3. 애드온을 제거할 때 관리된 클러스터에 대한 VPASync CSV 수동 제거가 필요합니다.

hub 클러스터에서 61Sync ManagedClusterAddOn 을 제거하면 관리 클러스터에서 desilSync Operator 서브스크립션을 제거하지만 CSV(클러스터 서비스 버전)는 제거하지 않습니다. 관리형 클러스터에서 CSV를 제거하려면 CloudEventSync를 제거할 각 관리형 클러스터에서 다음 명령을 실행합니다.

```
oc delete csv -n openshift-operators volsync-product.v0.4.0
```

다른 버전이 설치되어 있는 경우 v0.4.0 을 설치된 버전으로 교체합니다.

1.2.5.4. sushy-tools를 사용할 때 베어 메탈 관리 클러스터 프로비저닝 실패

sushy-tools를 사용하여 베어 메탈에 관리형 클러스터를 프로비저닝하면 프로비저닝에 실패할 수 있으며 가상 미디어 cd 쿼리에서 500 오류가 반환 될 수 있습니다. sushy-tools 사용은 장기 실행 클러스터에서 신뢰할 수 없습니다.

최신 버전의 sushy-tools가 있는지 확인하고 sushy 에뮬레이터를 다시 시작하여 문제를 해결합니다.

1.2.5.5. OpenShift Container Platform 4.10에 베어 메탈 클러스터를 프로비저닝하면 듀얼 스택 허브에서 실패합니다.

OpenShift Container Platform 버전 4.10을 실행하는 듀얼 스택 허브에 베어 메탈 클러스터를 프로비저닝하면 프로비저닝에 실패하고 노드 검사 중에 'timeout reached while inspecting the node'라는 오류 메시지와 함께 프로비저닝이 실패합니다. 이 문제를 바이패스하려면 다음 예와 같이 install-config.yaml 파일에서 provisioning 네트워크를 비활성화합니다.

```
platform:
  baremetal:
    provisioningNetwork: "Disabled"
```

provisioning 네트워크에 대한 자세한 내용은 OpenShift Container Platform 설명서에서 provisioning 네트워크없이 배포를 참조하십시오.

1.2.5.6. 관리형 클러스터 세트를 삭제해도 라벨이 자동으로 제거되지는 않습니다.

ManagedClusterSet 을 삭제한 후 클러스터를 클러스터 세트에 연결하는 각 관리 클러스터에 추가된 레이블은 자동으로 제거되지 않습니다. 삭제된 관리 클러스터 세트에 포함된 각 관리 클러스터에서 레이블을 수동으로 제거합니다. 레이블은 cluster.open-cluster-management.io/clusterset:<ManagedClusterSet Name>과 유사합니다.

1.2.5.7. ClusterClaim 오류

ClusterPool 에 대해 **Hive ClusterClaim** 을 생성하고 수동으로 **ClusterClaimspec** 수명 필드를 잘못된 **golang** 시간 값으로 설정하는 경우 **Red Hat Advanced Cluster Management**는 **malformed** 클레임뿐만 아니라 모든 **ClusterClaims** 실행 및 조정을 중지합니다.

이 오류가 발생하면 **clusterclaim-controller Pod** 로그에 다음 내용이 표시됩니다. 이는 풀 이름과 유효하지 않은 라이프 사이클이 포함된 특정 예입니다.

```
E0203 07:10:38.266841       1 reflector.go:138] sigs.k8s.io/controller-
runtime/pkg/cache/internal/informers_map.go:224: Failed to watch *v1.ClusterClaim: failed to list
*v1.ClusterClaim: v1.ClusterClaimList.Items: []v1.ClusterClaim:
v1.ClusterClaim.v1.ClusterClaim.Spec: v1.ClusterClaimSpec.Lifetime: unmarshalerDecoder: time:
unknown unit "w" in duration "1w", error found in #10 byte of ...|time":"1w"}},{"apiVe|..., bigger context
...|clusterPoolName":"policy-aas-hubs","lifetime":"1w"}},
{"apiVersion":"hive.openshift.io/v1","kind":"Cl|...
```

유효하지 않은 클레임을 삭제할 수 있습니다.

잘못된 형식의 클레임이 삭제되면 추가 상호 작용 없이 클레임이 다시 조정되기 시작합니다.

1.2.5.8. 프로비저닝된 클러스터와 동기화되지 않는 제품 채널

clusterimageset 는 **fast** 채널에 있지만 프로비저닝된 클러스터는 **stable** 채널에 있습니다. 현재 제품은 프로비저닝된 **OpenShift Container Platform** 클러스터와 채널을 동기화하지 않습니다.

OpenShift Container Platform 콘솔에서 올바른 채널로 변경합니다. **Administration > Cluster Settings > Details Channel** 을 클릭합니다.

1.2.5.9. 사용자 정의 CA 인증서가 있는 관리형 클러스터의 복원 허브 클러스터에 대한 연결을 복원하지 못할 수 있습니다.

사용자 정의 **CA** 인증서로 클러스터를 관리하는 허브 클러스터의 백업을 복원한 후 관리형 클러스터와 허브 클러스터 간의 연결이 실패할 수 있습니다. 이는 복원된 허브 클러스터에서 **CA** 인증서가 백업되지 않았기 때문입니다. 연결을 복원하려면 관리 클러스터의 네임스페이스에 있는 사용자 정의 **CA** 인증서 정보를 복원된 허브 클러스터의 **< managed_cluster>-admin-kubeconfig** 시크릿에 복사합니다.

팁: 백업 사본을 생성하기 전에 이 **CA** 인증서를 **hub** 클러스터에 복사하면 백업 사본에 시크릿 정보가 포함됩니다. 나중에 백업 사본을 사용하여 복원하면 허브와 관리 클러스터 간의 연결이 자동으로 완료됩

니다.

1.2.5.10. local-cluster가 자동으로 다시 생성되지 않을 수 있습니다.

disableHubSelfManagement 가 **false** 로 설정된 동안 **local-cluster**가 삭제되면 **MulticlusterHub Operator**가 로컬 클러스터를 다시 생성합니다. 로컬 클러스터를 분리한 후 로컬 클러스터가 자동으로 다시 생성되지 않을 수 있습니다.

- 이 문제를 해결하려면 **MulticlusterHub Operator**에서 조사하는 리소스를 수정합니다. 다음 예제를 참조하십시오.

```
oc delete deployment multiclusterhub-repo -n <namespace>
```

- 로컬 클러스터를 올바르게 분리하려면 **MultiClusterHub** 에서 **disableHubSelfManagement** 를 **true**로 설정합니다.

1.2.5.11. 온-프레미스 클러스터를 만들 때 서브넷 선택

Red Hat Advanced Cluster Management 콘솔을 사용하여 온-프레미스 클러스터를 만드는 경우 클러스터에 사용 가능한 서브넷을 선택해야 합니다. 필수 필드로 표시되지 않습니다.

1.2.5.12. Google Cloud Platform의 클러스터 프로비저닝 실패

GCP(Google Cloud Platform)에 클러스터를 프로비저닝하려고 하면 다음 오류가 발생할 수 있습니다.

```
Cluster initialization failed because one or more operators are not functioning properly.
The cluster should be accessible for troubleshooting as detailed in the documentation linked below,
https://docs.openshift.com/container-platform/latest/support/troubleshooting/troubleshooting-installations.html
The 'wait-for install-complete' subcommand can then be used to continue the installation
```

클러스터 설치를 계속할 수 있는 **GCP** 프로젝트에서 **Network Security API** 를 활성화하여 이 오류를 해결할 수 있습니다.

1.2.5.13. Infrastructure Operator를 통한 클러스터 프로비저닝 실패

Infrastructure Operator를 사용하여 **OpenShift Container Platform** 클러스터를 생성할 때 **ISO** 이미지의 파일 이름이 너무 길 수 있습니다. 긴 이미지 이름으로 인해 이미지 프로비저닝 및 클러스터 프로비

저닝이 실패합니다. 이것이 문제인지 확인하려면 다음 단계를 완료합니다.

1. 다음 명령을 실행하여 프로비저닝하는 클러스터의 베어 메탈 호스트 정보를 확인합니다.

```
oc get bmh -n <cluster_provisioning_namespace>
```

2. **describe** 명령을 실행하여 오류 정보를 확인합니다.

```
oc describe bmh -n <cluster_provisioning_namespace> <bmh_name>
```

3. 다음 예와 유사한 오류는 파일 이름의 길이가 문제임을 나타냅니다.

```
Status:
  Error Count:    1
  Error Message:  Image provisioning failed: ... [Errno 36] File name too long ...
```

이 문제가 발생하면 인프라 **Operator**가 이미지 서비스를 사용하지 않았기 때문에 일반적으로 다음 버전의 **OpenShift Container Platform**에 있습니다.

- **4.8.17** 이전
- **4.9.6** 이전

이 오류를 방지하려면 **OpenShift Container Platform**을 버전 **4.8.18** 이상 또는 **4.9.7** 이상으로 업그레이드하십시오.

1.2.5.14. Azure Government 클러스터를 사용할 수 없음

Azure Government 클러스터를 만들려고 하면 프로비저닝 **Pod** 로그에 다음과 같은 오류가 발생하여 실패합니다.

```
Confidential Client is not supported in Cross Cloud request
```

1.2.5.15. 다른 이름으로 다시 가져온 후 로컬 클러스터 상태 오프라인

실수로 다른 이름으로 **local-cluster** 라는 클러스터를 다시 가져오려고 하면 로컬 클러스터 상태 및 다

시 가져온 클러스터 디스플레이 오프라인에서.

이 경우 복구하려면 다음 단계를 완료합니다.

1. **hub** 클러스터에서 다음 명령을 실행하여 허브 클러스터의 자체 관리에 대한 설정을 일시적으로 편집합니다.

```
oc edit mch -n open-cluster-management multiclusterhub
```

2. **spec.disableSelfManagement=true** 설정을 추가합니다.

3. **hub** 클러스터에서 다음 명령을 실행하여 로컬 클러스터를 삭제하고 재배포합니다.

```
oc delete managedcluster local-cluster
```

4. 다음 명령을 입력하여 **local-cluster** 관리 설정을 제거합니다.

```
oc edit mch -n open-cluster-management multiclusterhub
```

5. 이전에 추가한 **spec.disableSelfManagement=true** 를 제거합니다.

1.2.5.16. 프록시 환경에서 Ansible 자동화로 클러스터 프로비저닝 실패

다음 조건이 모두 충족되면 관리형 클러스터를 자동으로 프로비저닝하도록 구성된 **AnsibleJob** 템플릿이 실패할 수 있습니다.

- **hub** 클러스터에는 클러스터 전체 프록시가 활성화되어 있습니다.
- **Ansible Tower**는 프록시를 통해서만 액세스할 수 있습니다.

1.2.5.17. klusterlet Operator의 버전은 hub 클러스터와 동일해야 합니다.

klusterlet Operator를 설치하여 관리형 클러스터를 가져오는 경우 **klusterlet Operator** 버전은 **hub** 클러스터 버전과 동일해야 합니다. 그렇지 않으면 **klusterlet Operator**가 작동하지 않습니다.

1.2.5.18. 관리형 클러스터 네임스페이스를 수동으로 삭제할 수 없음

관리 클러스터의 네임스페이스를 수동으로 삭제할 수 없습니다. 관리 대상 클러스터 네임스페이스는 관리 클러스터가 분리되면 자동으로 삭제됩니다. 관리 클러스터 네임스페이스를 분리하기 전에 관리형 클러스터 네임스페이스를 수동으로 삭제하면 관리 클러스터에 관리 클러스터를 삭제한 후 연속 종료 상태가 표시됩니다. 이 종료 관리 클러스터를 삭제하려면 분리한 관리 클러스터에서 종료자를 수동으로 제거합니다.

1.2.5.19. 버전 2.3으로 업그레이드한 후 클러스터에서 인증 정보를 변경할 수 없음

Red Hat Advanced Cluster Management를 버전 2.3으로 업그레이드한 후에는 업그레이드하기 전에 **Red Hat Advanced Cluster Management**에서 생성하고 관리하는 관리형 클러스터의 인증 정보 시크릿을 변경할 수 없습니다.

1.2.5.20. Hub 클러스터 및 관리형 클러스터 시계가 동기화되지 않음

Hub 클러스터 및 클러스터 시간을 동기화가 부족하여 콘솔에 표시되지 않고 결국 몇 분 내에 사용할 수 있습니다. **Red Hat OpenShift Container Platform** 허브 클러스터 시간이 올바르게 구성되었는지 확인합니다. 노드 사용자 지정을 참조하십시오.

1.2.5.21. 특정 버전의 IBM OpenShift Container Platform Kubernetes Service 클러스터 가져오기는 지원되지 않습니다.

IBM OpenShift Container Platform Kubernetes Service 버전 **3.11** 클러스터를 가져올 수 없습니다. 이후 버전의 **IBM OpenShift Kubernetes Service**가 지원됩니다.

1.2.5.22. OpenShift Container Platform 3.11 분리는 *open-cluster-management-agent*를 제거하지 않습니다.

OpenShift Container Platform 3.11에서 관리형 클러스터를 분리하면 **open-cluster-management-agent** 네임스페이스가 자동으로 삭제되지 않습니다. 다음 명령을 실행하여 네임스페이스를 수동으로 제거합니다.

```
oc delete ns open-cluster-management-agent
```

1.2.5.23. 프로비저닝된 클러스터에 대한 자동 시크릿 업데이트가 지원되지 않음

클라우드 공급자 액세스 키를 변경하면 네임스페이스에 프로비저닝된 클러스터 액세스 키가 업데이트되지 않습니다. 이는 관리 클러스터가 호스팅되는 클라우드 공급자에서 인증 정보가 만료되고 관리되는

클러스터를 삭제하려고 할 때 필요합니다. 이와 같은 문제가 발생하면 클라우드 공급자가 액세스 키를 업데이트하려면 다음 명령을 실행합니다.

- **AWS(Amazon Web Services)**

```
oc patch secret {CLUSTER-NAME}-aws-creds -n {CLUSTER-NAME} --type json -p='[{"op": "add", "path": "/stringData", "value":{"aws_access_key_id": "{YOUR-NEW-ACCESS-KEY-ID}","aws_secret_access_key":"{YOUR-NEW-aws_secret_access_key}"} }]'
```

- **GCP(Google Cloud Platform)**

클러스터를 제거하려고 할 때 **Invalid JWT Signature** 를 읽는 반복 로그 오류 메시지로 이 문제를 식별할 수 있습니다. 로그에 이 메시지가 포함된 경우 새 **Google Cloud Provider** 서비스 계정 **JSON** 키를 가져와서 다음 명령을 입력합니다.

```
oc set data secret/<CLUSTER-NAME>-gcp-creds -n <CLUSTER-NAME> --from-file=osServiceAccount.json=$HOME/.gcp/osServiceAccount.json
```

CLUSTER-NAME 을 클러스터 이름으로 바꿉니다.

$HOME/.gcp/osServiceAccount.json 파일의 경로를 새 **Google Cloud Provider** 서비스 계정 **JSON** 키가 포함된 파일의 경로로 바꿉니다.

- **Microsoft Azure**

```
oc set data secret/{CLUSTER-NAME}-azure-creds -n {CLUSTER-NAME} --from-file=osServiceAccount.json=$HOME/.azure/osServiceAccount.json
```

- **VMware vSphere**

```
oc patch secret {CLUSTER-NAME}-vsphere-creds -n {CLUSTER-NAME} --type json -p='[{"op": "add", "path": "/stringData", "value":{"username": "{YOUR-NEW-VMware-username}","password":"{YOUR-NEW-VMware-password}"} }]'
```

1.2.5.24. 관리형 클러스터의 노드 정보를 검색에서 볼 수 없음

검색은 **hub** 클러스터에서 리소스에 대한 **RBAC**를 매핑합니다. **Red Hat Advanced Cluster Management**의 사용자 **RBAC** 설정에 따라 관리 클러스터의 노드 데이터가 표시되지 않을 수 있습니다.

검색 결과는 클러스터의 노드 *페이지에 표시되는 내용과 다를* 수 있습니다.

1.2.5.25. 클러스터 삭제 프로세스가 완료되지 않음

관리형 클러스터를 제거해도 1시간 후에도 상태가 **Destroying** 이 계속 표시되고 클러스터는 삭제되지 않습니다. 이 문제를 해결하려면 다음 단계를 완료합니다.

1. 클라우드에 고립된 리소스가 없는지 수동으로 확인하고 관리 클러스터와 연결된 모든 공급자 리소스가 정리되었는지 확인합니다.
2. 다음 명령을 입력하여 제거 중인 관리형 클러스터에 대한 **ClusterDeployment** 정보를 엽니다.

```
oc edit clusterdeployment/<mycluster> -n <namespace>
```

   mycluster 를 제거 중인 관리형 클러스터의 이름으로 교체합니다.

   namespace 를 관리 클러스터의 네임스페이스로 바꿉니다.

3. **hive.openshift.io/deprovision** 종료자를 제거하여 클라우드에서 클러스터 리소스를 정리하려는 프로세스를 강제 중지합니다.
4. 변경 사항을 저장하고 **ClusterDeployment** 가 사라졌는지 확인합니다.
5. 다음 명령을 실행하여 관리형 클러스터의 네임스페이스를 수동으로 제거합니다.

```
oc delete ns <namespace>
```

   namespace 를 관리 클러스터의 네임스페이스로 바꿉니다.

1.2.5.26. 콘솔과 함께 OpenShift Container Platform Dedicated에서 OpenShift Container Platform 관리 클러스터를 업그레이드할 수 없음

Red Hat Advanced Cluster Management 콘솔을 사용하여 **OpenShift Container Platform Dedicated** 환경에 있는 **OpenShift Container Platform** 관리 클러스터를 업그레이드할 수 없습니다.

1.2.5.27. 작업 관리자 애드온 검색 세부 정보

특정 관리 클러스터에서 특정 리소스에 대한 검색 세부 정보 페이지가 실패할 수 있습니다. 관리 클러스터의 **work-manager** 애드온이 **Available** 상태인지 확인해야 검색할 수 있습니다.

1.2.5.28. IBM Power 또는 IBM Z 시스템 허브 클러스터와 Ansible Tower 통합을 사용할 수 없음

Ansible Automation Platform Resource Operator 에서 **ppc64le** 또는 **s390x** 이미지를 제공하지 않으므로 **Kubernetes** 허브용 **Red Hat Advanced Cluster Management for Kubernetes hub** 클러스터가 **IBM Power** 또는 **IBM Z** 시스템에서 실행되는 경우 **Ansible Tower** 통합을 사용할 수 없습니다.

1.2.5.29. Red Hat OpenShift Container Platform 관리형 클러스터에 LoadBalancer가 활성화되어 있어야 합니다.

Red Hat OpenShift Container Platform 및 비**OpenShift Container Platform** 클러스터 모두 **Pod** 로그 기능을 지원하지만 이 기능을 사용하려면 **OpenShift Container Platform** 클러스터가 **LoadBalancer** 를 활성화해야 합니다. **LoadBalancer** 를 활성화하려면 다음 단계를 완료합니다.

1. 클라우드 공급자에는 서로 다른 **LoadBalancer** 구성이 있습니다. 자세한 내용은 클라우드 공급자 설명서를 참조하십시오.

2. **managedClusterInfo** 상태의 **loggingEndpoint** 를 확인하여 **Red Hat Advanced Cluster Management**에서 **LoadBalancer** 가 활성화되어 있는지 확인합니다.

3. 다음 명령을 실행하여 **loggingEndpoint.IP** 또는 **loggingEndpoint.Host** 에 유효한 **IP** 주소 또는 호스트 이름이 있는지 확인합니다.

```
oc get managedclusterinfo <clusterName> -n <clusterNamespace> -o json | jq -r
'.status.loggingEndpoint'
```

LoadBalancer 유형에 대한 자세한 내용은 **Kubernetes** 문서의 *서비스* 페이지를 참조하십시오.

1.2.5.30. 업그레이드 후 cluster-proxy-addon이 시작되지 않음

버전 **2.4.x**에서 **2.5.0**으로 업그레이드한 후 **cluster-proxy-addon** 이 시작되지 않고 **cluster-proxy-addon-manager** 가 **nil** 포인터 예외를 발생시킵니다.

이 문제를 해결하려면 다음 단계를 완료하십시오.

1. **cluster-proxy-addon** 을 비활성화합니다. 자세한 내용은 고급 구성을 참조하십시오.
2. **open-cluster-management** 네임스페이스에서 **cluster-proxy-signer** 시크릿을 삭제합니다.
3. **cluster-proxy-addon** 을 활성화합니다.

1.2.6. 애플리케이션 관리 알려진 문제

애플리케이션 라이프사이클 구성 요소에 대한 다음 알려진 문제를 참조하십시오.

1.2.6.1. Application ObjectBucket 채널 유형은 허용 및 거부 목록을 사용할 수 없습니다.

subscription-admin 역할에 **ObjectBucket** 채널 유형으로 허용 및 거부 목록을 지정할 수 없습니다. 다른 채널 유형에서 서브스크립션의 허용 및 거부 목록은 배포할 수 없는 **Kubernetes** 리소스 및 **Kubernetes** 리소스를 나타냅니다.

1.2.6.2. Argo 애플리케이션은 3.x OpenShift Container Platform 관리 클러스터에 배포할 수 없습니다.

3.x의 **Argo ApplicationSet** 은 **Infrastructure.config.openshift.io API**를 사용할 수 없기 때문에 **3.x OpenShift Container Platform** 관리 클러스터에 배포할 수 없습니다.

1.2.6.3. multicluster_operators_subscription 이미지 변경 사항이 자동으로 적용되지 않음

klusterlet Operator가 이전에 처리했을 때 관리 클러스터에서 실행 중인 **application-manager** 애드온을 서브스크립션 운영자가 처리합니다. 서브스크립션 **Operator**는 **multicluster-hub** 를 관리하지 않으므로 **multicluster-hub** 이미지 매니페스트 **ConfigMap**의 **multicluster_operators_subscription** 이미지에 대한 변경 사항이 자동으로 적용되지 않습니다.

멀티**cluster -hub** 이미지 매니페스트 **ConfigMap**에서 다중**cluster_operators_subscription** 이미지를 변경하여 서브스크립션 운영자가 사용하는 이미지를 재정의하는 경우 관리 클러스터 의 **application-manager** 애드온은 서브스크립션 운영자 **Pod**가 다시 시작될 때까지 새 이미지를 사용하지 않습니다. **Pod**를 다시 시작해야 합니다.

1.2.6.4. 애플리케이션 토폴로지가 잘못된 애플리케이션을 표시

다른 **Gitops** 인스턴스에 동일한 이름의 **ApplicationSets** 가 생성된 경우 애플리케이션 토폴로지가 잘못된 애플리케이션을 표시합니다. **Gitops** 인스턴스가 여러 개 설치된 경우 각 **Gitops** 인스턴스에 이름이 동일한 **ApplicationSets** 가 있고 **ApplicationSets** 의 토폴로지가 올바르게 표시되지 않습니다. 이는 토폴로지가 생성된 **ApplicationSets** 의 네임스페이스를 구분하지 않기 때문입니다.

토폴로지를 올바르게 표시하려면 각 **Gitops** 인스턴스에서 다른 이름으로 **ApplicationSets** 를 생성해야 합니다.

1.2.6.5. 서브스크립션 관리자가 배포하지 않는 경우 정책 리소스가 배포되지 않음

policy.open-cluster-management.io/v1 리소스는 기본적으로 **Red Hat Advanced Cluster Management** 버전 **2.4**에 대해 애플리케이션 서브스크립션에 의해 더 이상 배포되지 않습니다.

서브스크립션 관리자는 이 기본 동작을 변경하기 위해 애플리케이션 서브스크립션을 배포해야 합니다.

자세한 내용은 서브스크립션 관리자로 허용 및 거부 목록 생성을 참조하십시오. 이전 **Red Hat Advanced Cluster Management** 버전의 기존 애플리케이션 서브스크립션에 의해 배포된 **policy.open-cluster-management.io/v1** 리소스는 남아 있지만 서브스크립션 관리자가 애플리케이션 서브스크립션을 배포하지 않는 한 소스 리포지토리와 조정되지 않습니다.

1.2.6.6. 애플리케이션 Ansible 후크 독립 실행형 모드

Ansible 후크 독립 실행형 모드는 지원되지 않습니다. 서브스크립션을 사용하여 허브 클러스터에 **Ansible** 후크를 배포하려면 다음 서브스크립션 **YAML**을 사용할 수 있습니다.

```
apiVersion: apps.open-cluster-management.io/v1
kind: Subscription
metadata:
  name: sub-rhacm-gitops-demo
  namespace: hello-openshift
annotations:
  apps.open-cluster-management.io/github-path: myapp
  apps.open-cluster-management.io/github-branch: master
spec:
  hooksecretref:
     name: toweraccess
  channel: rhacm-gitops-demo/ch-rhacm-gitops-demo
  placement:
    local: true
```

그러나 **spec.placement.local:true** 에 독립 실행형 모드에서 서브스크립션이 실행 중이므로 이 구성은 **Ansible** 인스턴스를 생성하지 않을 수 있습니다. 허브 모드에서 서브스크립션을 생성해야 합니다.

1. 로컬 클러스터에 배포하는 배치 규칙을 생성합니다. 다음 샘플을 참조하십시오.

```
apiVersion: apps.open-cluster-management.io/v1
kind: PlacementRule
metadata:
  name: <towhichcluster>
  namespace: hello-openshift
spec:
  clusterSelector:
    matchLabels:
      local-cluster: "true" #this points to your hub cluster
```

2. 서브스크립션에 해당 배치 규칙을 참조합니다. 다음을 참조하십시오.

```
apiVersion: apps.open-cluster-management.io/v1
kind: Subscription
metadata:
  name: sub-rhacm-gitops-demo
  namespace: hello-openshift
annotations:
  apps.open-cluster-management.io/github-path: myapp
  apps.open-cluster-management.io/github-branch: master
spec:
  hooksecretref:
     name: toweraccess
  channel: rhacm-gitops-demo/ch-rhacm-gitops-demo
  placement:
    placementRef:
      name: <towhichcluster>
      kind: PlacementRule
```

둘 다 적용한 후에는 허브 클러스터에서 생성된 **Ansible** 인스턴스가 표시되어야 합니다.

1.2.6.7. 애플리케이션 오류에 대한 역할 편집

편집기 역할에서 수행하는 사용자는 애플리케이션에 대한 읽기 또는 업데이트 권한만 있어야 하지만 잘못된 편집기는 애플리케이션을 생성하고 삭제 할 수도 있습니다. **OpenShift Container Platform Operator Lifecycle Manager** 기본 설정은 제품의 설정을 변경합니다. 문제를 해결하려면 다음 절차를 참조하십시오.

1. **oc edit clusterrole applications.app.k8s.io-v1beta2-edit -o yaml** 을 실행하여 애플리케

이션 편집 클러스터 역할을 엽니다.

2. 동사 목록에서 **create** 및 **delete** 를 제거합니다.

3. 변경 사항을 저장합니다.

1.2.6.8. 배치 규칙 오류에 대한 역할 편집

편집기 역할에서 수행하는 사용자는 배치 규칙에 대한 읽기 또는 업데이트 권한만 있어야 하지만 잘못된 편집기도 만들고 삭제 할 수 있습니다. **OpenShift Container Platform Operator Lifecycle Manager** 기본 설정은 제품의 설정을 변경합니다. 문제를 해결하려면 다음 절차를 참조하십시오.

1. **oc edit clusterrole placementrules.apps.open-cluster-management.io-v1-edit** 를 실행하여 애플리케이션 편집 클러스터 역할을 엽니다.

2. 동사 목록에서 **create** 및 **delete** 를 제거합니다.

3. 변경 사항을 저장합니다.

1.2.6.9. 업데이트된 배치 규칙 이후에 배포되지 않은 애플리케이션

배치 규칙 업데이트 후 애플리케이션이 배포되지 않는 경우 **klusterlet-addon-appmgr Pod**가 실행 중인지 확인합니다. **klusterlet-addon-appmgr** 은 끝점 클러스터에서 실행해야 하는 서브스크립션 컨테이너입니다.

oc get pods -n open-cluster-management-agent-addon 을 실행하여 확인할 수 있습니다.

콘솔에서 **kind:pod cluster:yourcluster** 를 검색하고 **klusterlet-addon-appmgr** 이 실행 중인지 확인할 수도 있습니다.

확인할 수 없는 경우 클러스터를 다시 가져온 후 다시 확인합니다.

1.2.6.10. 서브스크립션 Operator에서 SCC를 생성하지 않음

관리 SCC(보안 컨텍스트 제약 조건)의 Red Hat OpenShift Container Platform SCC 에 대해 알아보십시오. 관리 대상 클러스터에 필요한 추가 구성입니다.

배포마다 다른 보안 컨텍스트 및 다양한 서비스 계정이 있습니다. 서브스크립션 운영자는 SCC를 자동으로 생성할 수 없습니다. 관리자는 Pod에 대한 권한을 제어합니다. 기본이 아닌 네임스페이스에 Pod를 생성하기 위해 상대 서비스 계정에 적절한 권한을 활성화하려면 SCC(보안 컨텍스트 제약 조건) CR이 필요합니다.

네임스페이스에서 SCC CR을 수동으로 생성하려면 다음을 완료합니다.

1. 배포에 정의된 서비스 계정을 찾습니다. 예를 들어 다음 nginx 배포를 참조하십시오.

```
nginx-ingress-52edb
nginx-ingress-52edb-backend
```

2. 네임스페이스에서 SCC CR을 생성하여 서비스 계정 또는 계정에 필요한 권한을 할당합니다. kind: SecurityContextConstraints 가 추가되는 다음 예제를 참조하십시오.

```
apiVersion: security.openshift.io/v1
defaultAddCapabilities:
kind: SecurityContextConstraints
metadata:
  name: ingress-nginx
  namespace: ns-sub-1
priority: null
readOnlyRootFilesystem: false
requiredDropCapabilities:
fsGroup:
  type: RunAsAny
runAsUser:
  type: RunAsAny
seLinuxContext:
  type: RunAsAny
users:
- system:serviceaccount:my-operator:nginx-ingress-52edb
- system:serviceaccount:my-operator:nginx-ingress-52edb-backend
```

1.2.6.11. 애플리케이션 채널에는 고유한 네임스페이스가 필요합니다.

동일한 네임스페이스에 둘 이상의 채널을 생성하면 허브 클러스터에 오류가 발생할 수 있습니다.

예를 들어, 설치 프로그램에서 Helm 유형 채널로 네임스페이스 charts-v1 을 사용하므로 charts-v1 에서 추가 채널을 생성하지 마십시오. 고유한 네임스페이스에서 채널을 생성해야 합니다. 모든 채널에는

다른 GitHub 채널과 네임스페이스를 공유할 수 있는 GitHub 채널을 제외한 개별 네임스페이스가 필요합니다.

1.2.6.12. Ansible Automation Platform 작업 실패

호환되지 않는 옵션을 선택하면 Ansible 작업이 실행되지 않습니다. Ansible Automation Platform은 -cluster-scoped 채널 옵션을 선택한 경우에만 작동합니다. 이는 Ansible 작업을 수행해야 하는 모든 구성 요소에 영향을 미칩니다.

1.2.6.13. Ansible Automation Platform Operator는 프록시 외부에서 Ansible Tower에 액세스

AAP(Ansible Automation Platform) Operator는 프록시 사용 OpenShift Container Platform 클러스터 외부에서 Ansible Tower에 액세스할 수 없습니다. 문제를 해결하려면 프록시 내에 Ansible Tower를 설치할 수 있습니다. Ansible Tower에서 제공하는 설치 단계를 참조하십시오.

1.2.6.14. 버전 2.4에서 Helm Argo 애플리케이션을 편집할 때 템플릿 정보가 표시되지 않습니다.

Helm Argo 애플리케이션이 생성되고 편집되면 YAML 파일이 올바르면 템플릿 정보가 비어 있습니다. 에라타 2.4.1로 업그레이드하여 오류를 수정합니다.

1.2.6.15. 애플리케이션 이름 요구사항

애플리케이션 이름은 37자를 초과할 수 없습니다. 문자가 이 양을 초과하면 애플리케이션 배포에 다음 오류가 표시됩니다.

```
status:
  phase: PropagationFailed
  reason: 'Deployable.apps.open-cluster-management.io "_long_lengthy_name_" is invalid:
metadata.labels: Invalid value: "_long_lengthy_name_": must be no more than 63
characters/n'
```

1.2.6.16. 애플리케이션 콘솔 테이블 제한 사항

콘솔의 다양한 *애플리케이션* 테이블에 대한 다음 제한 사항을 참조하십시오.

- *개요* 페이지의 *애플리케이션* 테이블과 *고급 구성* 페이지의 *서브스크립션* 표에서 *클러스터* 열에 애플리케이션 리소스가 배포된 클러스터 수가 표시됩니다. 애플리케이션은 로컬 클러스터의 리소스로 정의되므로 실제 애플리케이션 리소스가 로컬 클러스터에 배포되었는지 여부에 관계없이 로컬 클러스터는 검색 결과에 포함됩니다.
-

서브스크립션 의 고급 구성 표에서 애플리케이션 열에는 해당 서브스크립션을 사용하는 총 애플리케이션 수가 표시되지만 서브스크립션이 하위 애플리케이션을 배포하면 검색 결과에도 포함됩니다.

- *채널 의 고급 구성* 표에서 서브스크립션 열에는 해당 채널을 사용하는 로컬 클러스터의 총 서브스크립션 수가 표시되지만 검색 결과에 포함된 다른 서브스크립션에서 배포한 서브스크립션은 포함되지 않습니다.

1.2.6.17. 애플리케이션 콘솔 토폴로지 필터링 없음

애플리케이션의 콘솔 및 토폴로지 가 2.5에 대한 변경 사항입니다. 콘솔 토폴로지 페이지에서 필터링 기능이 없습니다.

1.2.6.18. ApplicationSet 리소스는 토폴로지에서 상태를 표시하지 않음

ApplicationSet YAML에 정의된 네임스페이스와 다른 네임스페이스에 리소스를 배포하는 ApplicationSet 애플리케이션을 생성하면 리소스 상태가 토폴로지에 표시되지 않습니다.

1.2.6.19. 오브젝트 스토리지 애플리케이션에서 허용 및 거부 목록이 작동하지 않음

개체 스토리지 애플리케이션 서브스크립션에서는 허용 및 거부 목록 기능이 작동하지 않습니다.

1.2.6.20. ApplicationSet 마법사가 경로를 자동으로 가져오지 않음

이전에 생성된 ApplicationSet 과 동일한 URL 및 분기를 사용하여 새 ApplicationSet 을 생성하면 ApplicationSet 마법사에서 경로를 자동으로 가져오지 않습니다.

문제를 해결하려면 경로 필드에 수동으로 경로 를 입력합니다.

1.2.7. 거버넌스 알려진 문제

1.2.7.1. Red Hat Advanced Cluster Management에서 로그아웃할 수 없음

외부 ID 공급자를 사용하여 Red Hat Advanced Cluster Management에 로그인하면 Red Hat Advanced Cluster Management에서 로그아웃하지 못할 수 있습니다. 이는 Red Hat Advanced Cluster Management를 사용하고 IBM Cloud 및 Keycloak과 함께 ID 공급자로 설치된 경우 발생합니다.

Red Hat Advanced Cluster Management에서 로그아웃하기 전에 외부 ID 공급자에서 로그아웃해야

합니다.

1.2.7.2. 게이트 키퍼 Operator 설치에 실패

Red Hat OpenShift Container Platform 버전 4.9에 게이트 키 연산자를 설치하면 설치에 실패합니다. OpenShift Container Platform을 버전 4.9.0.로 업그레이드하기 전에 gatekeeper Operator를 버전 0.2.0으로 업그레이드해야 합니다. 자세한 내용은 게이트 키퍼(upgrading gatekeeper) 및 게이트키퍼 (Gatekeeper) 운영자 를 참조하십시오.

1.2.7.3. 네임스페이스가 종료 상태가 될 때 불만되는 구성 정책

complianceType 매개변수에 대해 mustnothave 로 구성된 구성 정책이 있고 remediationAction 매개변수에 적용하는 경우 Kubernetes API에 대한 삭제 요청이 수행된 후 정책이 준수로 나열됩니다. 따라서 정책이 규정 준수로 나열되는 동안 Kubernetes 오브젝트를 Terminating 상태로 유지할 수 있습니다.

1.2.7.4. 정책을 통해 배포된 Operator는 ARM을 지원하지 않습니다.

ARM 환경에 설치하는 것은 지원되지만 정책을 사용하여 배포된 Operator는 ARM 환경을 지원하지 않을 수 있습니다. Operator를 설치하는 다음 정책은 ARM 환경을 지원하지 않습니다.

- Quay Container Security Operator에 대한 Red Hat Advanced Cluster Management 정책
- Compliance Operator에 대한 Red Hat Advanced Cluster Management 정책

1.2.7.5. 정책 템플릿 문제

구성 정책에 대한 정책 템플릿을 편집할 때 다음 문제가 발생할 수 있습니다.

- 구성 정책의 이름을 새 이름으로 바꾸면 이전 이름으로 구성 정책의 사본이 유지됩니다.
- hub 클러스터의 정책에서 구성 정책을 제거하면 구성 정책이 관리 클러스터에 남아 있지만 해당 상태는 제공되지 않습니다. 이 문제를 해결하려면 정책을 비활성화하고 다시 활성화합니다. 전체 정책을 삭제할 수도 있습니다.

1.2.8. 알려진 문제 백업 및 복원

1.2.8.1. IBM Power 및 IBM Z에서는 백업 및 복원 기능이 작동하지 않습니다.

hub 클러스터의 백업 및 복원 기능에는 **OADP(Data Protection) Operator**가 필요합니다. **OADP Operator**는 **IBM Power** 또는 **IBM Z** 아키텍처에서는 사용할 수 없습니다.

1.2.8.2. 백업 충돌 방지

허브 클러스터가 수동에서 기본 클러스터 및 백업으로 변경되면 다른 클러스터에서 동일한 스토리지 위치에서 데이터를 백업할 수 있습니다. 이로 인해 백업 충돌이 발생할 수 있습니다. 즉, 최신 백업이 수동 허브 클러스터에서 생성됩니다.

패시브 허브 클러스터는 **hub** 클러스터에서 **BackupSchedule.cluster.open-cluster-management.io** 리소스가 활성화되어 있기 때문에 백업을 생성하지만 허브 클러스터가 더 이상 기본 허브 클러스터가 아니기 때문에 백업 데이터를 더 이상 기록해서는 안 됩니다. 다음 명령을 실행하여 백업 충돌이 있는지 확인합니다.

```
oc get backupschedule -A
```

다음 상태가 표시될 수 있습니다.

```
NAMESPACE       NAME              PHASE           MESSAGE
openshift-adp   schedule-hub-1    BackupCollision   Backup acm-resources-schedule-20220301234625, from cluster with id [be97a9eb-60b8-4511-805c-298e7c0898b3] is using the same storage location. This is a backup collision with current cluster [1f30bfe5-0588-441c-889e-eaf0ae55f941] backup. Review and resolve the collision then create a new BackupSchedule resource to  resume backups from this cluster.
```

BackupSchedule.cluster.open-cluster-management.io 리소스 상태를 **BackupCollision** 로 설정하여 백업 충돌을 방지합니다. **BackupSchedule** 리소스에서 생성한 **Schedule.velero.io** 리소스는 자동으로 삭제됩니다.

백업 충돌은 **hub-backup-pod** 정책으로 보고됩니다. 관리자는 어떤 **hub** 클러스터가 데이터를 스토리지 위치에 쓰는지 확인해야 합니다. 그런 다음 **Passive hub** 클러스터에서 **BackupSchedule.cluster.open-cluster-management.io** 리소스를 제거하고 기본 허브 클러스터에서 새 **BackupSchedule.cluster.open-cluster-management.io** 리소스를 다시 생성하여 백업을 다시 시작합니다.

자세한 내용은 **Cluster Backup and restore operator** 에서 참조하십시오.

1.2.8.3. Velero 복원 제한 사항

다음 복원 제한 사항을 확인합니다.

- 새 **hub** 클러스터는 초기 허브 클러스터에서 백업 데이터를 복원하기 전에 새 허브 클러스터에 기존 정책이 있을 때 데이터가 복원되는 초기 허브 클러스터와 동일하지 않습니다. 백업 리소스와 함께 사용할 수 없는 정책이므로 새 허브 클러스터에서 이 정책이 실행되고 있지 않아야 합니다.

- **Velero**는 기존 리소스를 건너뛰므로 새 허브 클러스터의 정책은 변경되지 않습니다. 따라서 이 정책은 초기 허브 클러스터에서 백업된 정책과 동일하지 않습니다.

- 사용자가 새 허브 클러스터에 백업을 다시 적용할 때 새 **hub** 클러스터는 활성 허브 클러스터와 다른 구성을 갖습니다. 이전 복원의 **hub** 클러스터에 기존 정책이 있으므로 다시 복원되지 않습니다. 백업에 예상 업데이트가 포함되어 있어도 정책 콘텐츠는 새 허브 클러스터에서 **Velero**에 의해 업데이트되지 않습니다.

앞서 언급한 제한 사항을 해결하기 위해 **restore.cluster.open-cluster-management.io** 리소스를 생성할 때 클러스터 백업 및 복원 **Operator**는 **Velero** 복원이 시작되기 전에 **hub** 클러스터를 정리하여 복원을 준비하는 일련의 단계를 실행합니다. 자세한 내용은 복원 전에 허브 클러스터 정리를 참조하십시오.

1.2.8.4. 가져온 관리 클러스터가 표시되지 않습니다.

기본 허브 클러스터에서 수동으로 가져온 관리형 클러스터는 수동 허브 클러스터에서 활성화 데이터가 복원되는 경우에만 표시됩니다.

1.2.8.5. 클러스터 백업 및 복원 업그레이드 제한

enableClusterBackup 매개변수를 **true** 로 설정하여 클러스터를 **2.4**에서 **2.5**로 업그레이드하는 경우 다음 메시지가 표시됩니다.

> *When upgrading from version 2.4 to 2.5, cluster backup must be disabled*

클러스터를 업그레이드하기 전에 **enableClusterBackup** 매개변수를 **false** 로 설정하여 클러스터 백업 및 복원을 비활성화합니다. **MultiClusterHub** 리소스의 **components** 섹션은 다음 **YAML** 파일과 유사합니다.

업그레이드가 완료되면 백업 및 복원 구성 요소를 다시 활성화할 수 있습니다. 다음 샘플을 확인합니다.

```
overrides:
    components:
      - enabled: true
        name: multiclusterhub-repo
      - enabled: true
        name: search
      - enabled: true
        name: management-ingress
      - enabled: true
        name: console
      - enabled: true
        name: insights
      - enabled: true
        name: grc
      - enabled: true
        name: cluster-lifecycle
      - enabled: true
        name: volsync
      - enabled: true
        name: multicluster-engine
      - enabled: false
        name: cluster-proxy-addon
      - enabled: true <<<<<<<<
        name: cluster-backup
  separateCertificateManagement: false
```

OADP를 수동으로 설치한 경우 업그레이드하기 전에 OADP를 수동으로 제거해야 합니다. 업그레이드가 완료되고 백업 및 복원이 다시 활성화되면 OADP가 자동으로 설치됩니다.

1.2.8.6. 관리 클러스터 리소스가 복원되지 않음

로컬 클러스터 관리 클러스터 리소스의 설정을 복원하고 새 허브 클러스터에서 로컬 클러스터 데이터를 덮어쓰면 설정이 잘못 구성됩니다. 리소스에 클러스터 URL 세부 정보와 같은 로컬 클러스터 특정 정보가 포함되어 있기 때문에 이전 허브 클러스터 local- cluster 의 콘텐츠가 백업되지 않습니다.

복원된 클러스터에서 로컬 클러스터 리소스와 관련된 구성 변경 사항을 수동으로 적용해야 합니다. 자세한 내용은 새 허브 클러스터 준비를 참조하십시오.

1.2.8.7. prepareForBackup은 Velero 일정이 처음 생성될 때만 호출됩니다.

prepareForBackup 함수에 정의된 레이블은 스케줄 생성 후 생성된 리소스에 추가되지 않습니다. 이는 백업이 시작되기 전에 레이블이 지정되는 Red Hat OpenShift 시크릿의 Hive 및 Infrastructure Operator에 영향을 미칩니다.

영향을 받는 리소스 목록을 확인합니다.

- clusterDeployments 에서 사용하고 클러스터 클레임에 의해 생성된 보안
- 클러스터 풀 시크릿
- 레이블 agent-install.openshift.io/watch 및 environment.metal3.io라벨이 있는 시크릿

BackupSchedule,veleroSchedule 또는 veleroTTL 값을 업데이트하여 새 일정 세트를 시작합니다. 그런 다음 생성된 백업을 복원에 사용합니다. 이 백업은 백업의 최신 리소스에 레이블을 지정하도록 정의됩니다.

1.2.8.8. 복원된 Hive 관리형 클러스터가 새 hub 클러스터와 연결되지 않을 수 있습니다.

Hive 관리 클러스터에 대해 변경되거나 순환된 인증 기관(CA)의 백업을 복원하면 새 허브 클러스터에서 관리 클러스터가 새 허브 클러스터에 연결되지 않습니다. 이 관리된 클러스터에 대한 admin kubeconfig 시크릿은 더 이상 백업과 함께 사용할 수 없으므로 연결에 실패합니다.

새 허브 클러스터에서 관리 클러스터의 복원된 admin kubeconfig 시크릿을 수동으로 업데이트해야 합니다.

1.2.9. Submariner 알려진 문제

1.2.9.1. Submariner는 현재 OpenShift SDN을 CNI 네트워크 공급자로만 지원

OpenShiftSDN만 CNI 네트워크 공급자로 지원됩니다. OVN은 현재 지원되지 않습니다.

1.2.9.2. Submariner는 일부 Red Hat Enterprise Linux 노드를 작업자 노드로 지원하지 않습니다.

4.18.0-359.el8.x86_64 및 4.18.0-372.11.1.el8_6.x86_64 사이의 커널 버전을 사용하는 Red Hat Enterprise Linux 작업자 노드를 포함하는 클러스터에 Submariner를 배포하는 경우 애플리케이션 워크로드가 원격 클러스터와 통신하지 못합니다.

1.2.9.3. Submariner는 Red Hat Advanced Cluster Management에서 관리할 수 있는 모든 인프라 공급자를 지원하지 않습니다.

Submariner는 Red Hat Advanced Cluster Management에서 관리할 수 있는 모든 인프라 공급업체에서 지원되지 않습니다. 지원되는 공급자 목록은 Red Hat Advanced Cluster Management 지원 매트

릭스 를 참조하십시오.

1.2.9.4. Submariner는 Red Hat Advanced Cluster Management 콘솔을 통해 Red Hat OpenStack Platform 인프라 준비를 지원하지 않습니다.

Red Hat OpenStack 클러스터에 대한 자동 클라우드 준비는 제품 인타이틀먼트 단축(product-title-short} 콘솔)의 Submariner에서 지원되지 않습니다. Red Hat Advanced Cluster Management API를 사용하여 클라우드를 수동으로 준비할 수 있습니다.

1.2.9.5. Submariner는 Globalnet을 통해 헤드리스 서비스를 지원하지 않습니다.

Submariner는 Globalnet을 통해 헤드리스 서비스를 지원합니다. 그러나 clusterset.local 도메인 이름을 사용하여 동일한 클러스터에 상주하는 클라이언트에서 내보낸 헤드리스 서비스에 액세스하면 헤드리스 서비스와 연결된 globalIP 가 클러스터에서 라우팅할 수 없는 클라이언트로 반환됩니다.

cluster.local 도메인 이름을 사용하여 로컬 헤드리스 서비스에 액세스할 수 있습니다.

1.2.9.6. Submariner는 에어캐지드 클러스터를 지원하지 않습니다.

Submariner는 Air-gapped 환경에서 프로비저닝된 클러스터에 대해 검증되지 않습니다.

1.2.9.7. 수많은 게이트웨이를 배포할 수 없음

여러 게이트웨이를 배포할 수 없습니다.

1.2.9.8. NAT가 활성화된 경우 Submariner는 VXLAN을 지원하지 않습니다.

VXLAN 배선 드라이버를 사용하는 Submariner는 현재 NAT 이외의 배포에서만 지원됩니다.

1.2.9.9. 글로벌net 제한 사항

Globalnet은 Red Hat OpenShift Data Foundation 재해 복구 솔루션에서는 지원되지 않습니다. 지역 재해 복구 시나리오에 각 클러스터에서 클러스터 및 서비스 네트워크에 대해 겹치지 않은 개인 IP 주소 범위를 사용해야 합니다.

1.3. 에라타 업데이트

기본적으로 에라타 업데이트는 릴리스될 때 자동으로 적용됩니다. 자세한 내용은 Operator를 사용하여 업그레이드를 참조하십시오.

중요: 참조를 위해 에라타 링크 및 GitHub 번호가 콘텐츠에 추가되어 내부적으로 사용될 수 있습니다. 액세스 권한이 필요한 링크는 사용자가 사용할 수 없습니다.

FIPS 알림: spec.ingress.sslCiphers 에서 자체 암호를 지정하지 않으면 multiclusterhub-operator 에서 기본 암호 목록을 제공합니다. 2.4의 경우 이 목록에는 FIPS에서 승인하지 않은 두 개의 암호가 포함되어 있습니다. 버전 2.4.x 또는 이전 버전에서 업그레이드하고 FIPS 준수를 원하는 경우 다중 클러스터 허브 리소스에서 다음 두 암호를 제거하십시오. ECDHE-ECDSA-CHACHA20-POLY1305 및 ECDHE-RSA-CHACHA20-POLY1305.

1.3.1. 에라타 2.5.9

- 하나 이상의 제품 컨테이너 이미지 및 보안 수정 사항에 대한 업데이트를 제공합니다.

1.3.2. 에라타 2.5.8

- must-gather 명령에서 Red Hat OpenShift Container Platform 버전 번호를 수집합니다. (ACM-2857)
- MEMCACHED 인덱스의 max_item_size 설정이 모든 MEMCACHED 클라이언트를 변경하지 않도록 하는 문제를 해결합니다. (ACM-4683)
- 이름에 점이 있는 정책 상태가 이제 더 빨리 업데이트됩니다. (ACM-4736)

1.3.3. 에라타 2.5.7

- 콘솔에서 Edit time window 링크를 수정합니다. 이제 링크가 올바른 편집 페이지가 열립니다. (ACM-2647)
- 애플리케이션을 생성할 때 토폴로지 노드가 애플리케이션 콘솔에 표시되도록 하는 문제를 해결합니다. (ACM-3340)

1.3.4. 에라타 2.5.6

- 하나 이상의 제품 컨테이너 이미지 및 보안 수정 사항에 대한 업데이트를 제공합니다.

1.3.5. 에라타 2.5.5

- 특정 키와 값이 있는 사용자 정의 라벨을 정책에 추가할 때 모든 정책에 서비스 거부를 유발하는 문제를 해결합니다.

1.3.6. 에라타 2.5.4

- 하나 이상의 제품 컨테이너 이미지 및 보안 수정 사항에 대한 업데이트를 제공합니다.

1.3.7. 에라타 2.5.3

- 지원되지 않는 **--validate-cluster-security** 플래그를 **HypershiftDeployment** 컨트롤러 인수로 사용할 때 권한 문제를 해결합니다. (Bugzilla 2109544)

- 관리 클러스터의 동시 동기화 요청을 방지하기 위해 검색 집계기 논리를 업데이트합니다. (Bugzilla 2092863)

- 하나 이상의 제품 컨테이너 이미지 및 보안 수정 사항에 대한 업데이트를 제공합니다.

1.3.8. 에라타 2.5.2

- **Red Hat Advanced Cluster Management** 버전 2.5.2부터 이후 **Red Hat Advanced Cluster Management** 버전 2.5.x는 **Red Hat OpenShift Container Platform** 버전 4.11에서 지원됩니다.

- **Kubernetes operator** 버전 2.0.2용 멀티 클러스터 엔진부터 이후의 **Kubernetes Operator** 버전 2.0.x용 다중 클러스터 엔진은 **Red Hat OpenShift Container Platform** 버전 4.11에서 지원됩니다.

- **Submariner Globalnet**이 온-프레미스 및 퍼블릭 클러스터에서 연결되지 않은 **MTU** 문제를 해결합니다. (Bugzilla 2074547)

- 설치 후 **management-ingress** 포드가 시작되지 않도록 하는 문제를 해결합니다. (Bugzilla 2082254)

- 대문자가 포함된 라벨이 있는 **ClusterClaim** 을 생성할 때 관리 클러스터 로그에서 오류가 발생한 버그를 수정합니다. (Bugzilla 2095481)

- **Red Hat OpenShift Container Platform**에 설치할 때 **MultiClusterHub** 가 설치 단계에서 중단될 수 있는 문제를 해결합니다. (Bugzilla 2099503)

- 관리 클러스터에서 더 많은 지표를 수집할 수 있도록 사용자 정의 지표 허용 목록에 있는 사용자 지정 지표의 제한을 늘립니다. (Bugzilla 2099808)

- 콘솔에서 정책의 메모리 값을 업데이트한 후 강제 적용 하도록 설정된 **LimitRange** 정책을 유발하는 버그가 수정되어 있습니다. (Bugzilla 2100036)

- 서브스크립션 애플리케이션과 함께 **app-of-apps** 패턴을 사용할 때 다음 오류가 발생한 문제를 해결하십시오. 이 애플리케이션에는 서브스크립션 일치 선택기 **(spec.selector.matchExpressions)**가 없습니다. (BugzillaECDHE1577)

- **Red Hat Advanced Cluster Management** 클러스터 백업 및 복원 **Operator**를 사용하여 **Hub** 클러스터를 복구한 후 "알려되지 않은" 상태로 클러스터가 남아 있는 문제를 해결합니다. (BugzillaECDHE3653).

- 지정되지 않은 경우 **NodePool.Release.Image** 의 기본값을 **HostedClusterSpec.Release.Image** 에 지정된 릴리스 이미지로 설정합니다. (Bugzilla 2105436)

- **SSH**를 사용하여 비공개 호스팅 **Git** 서버에 연결된 애플리케이션 서브스크립션이 실패하는 문제를 해결합니다. 수정을 통해 개인 호스팅 **Git** 서버에 **SSH** 연결을 수행할 수 있습니다. (Bugzilla 2105885)

- 콘솔을 사용하여 정책을 삭제할 때 관련 **PolicyAutomation** 및 **AnsibleJob** 오브젝트가 제거되지 않도록 하는 버그를 수정합니다. (Bugzilla 2116060)

1.3.9. 에라타 2.5.1

- 관리 클러스터에 배포된 일부 애플리케이션을 제거한 버그를 수정합니다. (Bugzilla 2101453)

- 개요 페이지에서 콘솔 오류를 해결합니다. 그러면 백엔드 서비스를 사용할 수 없습니다. (Bugzilla 2096389)

- 정책 애드온의 비정상적인 상태 또는 실패로 클러스터 애드온 콘솔 문제를 해결합니다. (Bugzilla 2088270)

1.4. 중단 및 제거

제품의 일부가 더 이상 사용되지 않거나 Kubernetes용 Red Hat Advanced Cluster Management에서 제거된 경우를 알아봅니다. 현재 릴리스 및 두 개의 이전 릴리스에 대한 표에 표시되는 권장 동작 및 세부 사항의 대체 작업을 고려하십시오.

중요:

- Red Hat Advanced Cluster Management 2.4 및 이전 버전은 제거되어 더 이상 지원되지 않습니다. 이 문서는 사용 가능한 상태로 남아 있을 수 있지만 에라타 또는 기타 사용 가능한 업데이트없이 더 이상 사용되지 않습니다.

- Red Hat Advanced Cluster Management의 최신 버전으로 업그레이드하는 것이 좋습니다.

1.4.1. API 사용 중단 및 제거

Red Hat Advanced Cluster Management는 API에 대한 Kubernetes 사용 중단 지침을 따릅니다. 해당 정책에 대한 자세한 내용은 Kubernetes 사용 중단 정책을 참조하십시오. Red Hat Advanced Cluster Management API는 더 이상 사용되지 않거나 다음 타임라인 외부에서만 제거됩니다.

- 모든 V1 API는 일반적으로 12 개월 또는 3 개의 릴리스에서 사용할 수 있으며 지원됩니다. V1 API는 제거되지 않지만 해당 시간 제한 외부에서 더 이상 사용되지 않을 수 있습니다.

- 모든 베타 API는 일반적으로 9 개월 또는 3 개의 릴리스에서 사용할 수 있습니다. 베타 API는 해당 시간 제한 외부에서 제거되지 않습니다.

- 모든 alpha API는 지원되지 않아도 되지만 사용자에게 도움이 되는 경우 더 이상 사용되지 않거나 제거될 수 있습니다.

1.4.1.1. API 사용 중단

제품 또는 카테고리	영향을 받는 항목	버전	권장 작업	자세한 내용 및 링크
검색	DiscoveredCluster 및 DiscoveryConfig **v1alpha1** API는 더 이상 사용되지 않습니다. Discovery API가 **V1** 로 업그레이드 되었습니다.	2.5	**V1** 을 사용하십시오.	없음
배치	**v1alpha1** 은 더 이상 사용되지 않기 때문에 v1alpha1 API가 **v1beta1** 로 업그레이드됩니다.	2.5	**v1beta1** 을 사용합니다.	**배치** API **v1alpha1** 의 **spec.prioritizerPolicy.configurations.name** 필드가 제거되었습니다. **v1beta1** 에서 **spec.prioritizerPolicy.configurations.scoreCoordinate.builtIn** 을 사용합니다.
PlacementDecisions	**v1alpha1** 은 더 이상 사용되지 않기 때문에 v1alpha1 API가 **v1beta1** 로 업그레이드됩니다.	2.5	**v1beta1** 을 사용합니다.	없음
애플리케이션	**v1alpha1** API가 완전히 제거됩니다. GitOps 클러스터 API가 **V1beta1** 로 업그레이드됩니다.	2.5	**V1beta1** 을 사용합니다.	없음
애플리케이션	**deployables.apps.open-cluster-management.io**	2.5	없음	배포 가능한 API는 업그레이드 경로에 대해서만 남아 있습니다. 배포 가능한 CR 생성, 업데이트 또는 삭제는 조정되지 않습니다.

제품 또는 카테고리	영향을 받는 항목	버전	권장 작업	자세한 내용 및 링크
CertPolicyController	**v1** API는 더 이상 사용되지 않습니다.	2.5	이 API를 사용하지 마십시오.	CertPolicyController.agent.open-cluster-management.io
ApplicationManager	**v1** API는 더 이상 사용되지 않습니다.	2.5	이 API를 사용하지 마십시오.	ApplicationManager.agent.open-cluster-management.io
IAMPolicyController	**v1** API는 더 이상 사용되지 않습니다.	2.5	이 API를 사용하지 마십시오.	IAMPolicyController.agent.open-cluster-management.io
PolicyController	**v1** API는 더 이상 사용되지 않습니다.	2.5	이 API를 사용하지 마십시오.	PolicyController.agent.open-cluster-management.io
SearchCollector	**v1** API는 더 이상 사용되지 않습니다.	2.5	이 API를 사용하지 마십시오.	SearchCollector.agent.open-cluster-management.io
WorkManager	**v1** API는 더 이상 사용되지 않습니다.	2.5	이 API를 사용하지 마십시오.	WorkManager.agent.open-cluster-management.io
ManagedClusterSets	**v1alpha1** 은 더 이상 사용되지 않기 때문에 v1alpha1 API가 **v1beta1** 로 업그레이드됩니다.	2.4	**v1beta1** 을 사용합니다.	없음
ManagedClusterSetBindings	**v1alpha1** 은 더 이상 사용되지 않기 때문에 v1alpha1 API가 **v1beta1** 로 업그레이드됩니다.	2.4	**v1beta1** 을 사용합니다.	없음

1.4.2. Red Hat Advanced Cluster Management 사용 중단

더 이상 사용되지 않는 구성 요소, 기능 또는 서비스가 지원되지만 더 이상 사용하지 않으며 향후 릴리스에서 더 이상 사용되지 않을 수 있습니다. 권장 동작 의 대체 작업과 다음 표에 제공된 세부 사항을 고려하십시오.

제품 또는 카테고리	영향을 받는 항목	버전	권장 작업	자세한 내용 및 링크
클러스터	베어 메탈 자산을 사용한 클러스터 생성	2.5	콘솔을 사용하여 인프라 환경 생성	더 이상 사용되지 않는 영역에 대해 베어 메탈 자산 생성 및 수정 및 베어 메탈에 클러스터 생성을 참조하십시오. 절차 프로세스를 위해 온-프레미스 환경에서 클러스터 만들기 를 참조하십시오.
애드온 operator	기본 제공 관리형 클러스터 애드온 설치	2.5	없음	없음
가시성	**data.custom_rules.yaml.groups.rules** is deprecated	2.5	**data.custom_rules.yaml.groups.recording_rules** 를 사용합니다.	관찰 기능을 사용자 지정 할 수 있습니다.
설치 프로그램	**enableClusterProxyAddon** 및 **operator.open-cluster-management.io_multiclusterhubs_crd.yaml**에서 **ClusterBackup** 필드를 활성화합니다.	2.5	없음	설치 구성을 위한 고급 구성을 참조하십시오.
klusterlet operator	**릴리스-2.4**,**릴리스-2.3** 채널에 업데이트가 수신되지 않음	2.3 이상	Red Hat OpenShift 전용 클러스터를 가져오고 관리하려면 업데이트를 받으려면 2.5로 업그레이드해야 합니다.	Operator 를 사용하여 업그레이드를 참조하십시오.
애플리케이션	보안 관리	2.4	대신 시크릿에 정책 허브 템플릿을 사용합니다.	보안 정책 관리를 참조하십시오.
거버넌스 콘솔	**pod-security-policy**	2.4	없음	없음

제품 또는 카테고리	영향을 받는 항목	버전	권장 작업	자세한 내용 및 링크
설치 프로그램	**operator.open-cluster-management.io_multiclusterhubs_crd.yaml**에서 cert-manager 설정을 분리합니다.	2.3	없음	없음
거버넌스	사용자 정의 정책 컨트롤러	2.3	없음	없음

1.4.3. 제거

제거된 항목은 일반적으로 이전 릴리스에서 더 이상 사용되지 않으며 제품에서 더 이상 사용할 수 없는 기능입니다. 제거된 함수에 대안을 사용해야 합니다. 권장 동작 의 대체 작업과 다음 표에 제공된 세부 사항을 고려하십시오.

제품 또는 카테고리	영향을 받는 항목	버전	권장 작업	자세한 내용 및 링크
애플리케이션	배포 가능한 컨트롤러	2.5	없음	배포 가능한 컨트롤러가 제거되었습니다.
Red Hat Advanced Cluster Management 콘솔	비주얼 웹 터미널 (기술 프리뷰)	2.4	대신 터미널 사용	없음
애플리케이션	단일 ArgoCD 가져오기 모드: 허브 클러스터의 하나의 ArgoCD 서버로 가져온 시크릿입니다.	2.3	클러스터 보안을 여러 ArgoCD 서버로 가져올 수 있습니다.	없음
애플리케이션	argocd 클러스터 통합: **spec.applicationManager.argocdCluster**	2.3	GitOps 클러스터를 생성하고 사용자 정의 리소스를 배치하여 관리 클러스터를 등록합니다.	관리형 클러스터에서 GitOps 구성
거버넌스	cert-manager 내부 인증서 관리	2.3	작업이 필요하지 않음	없음

1.5. RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES 플랫폼 고려 사항

1.5.1. notice

이 문서는 일반 데이터 보호 규정 (ECDHE) 준비에 도움이 되도록 작성되었습니다. 이 제품은 사용자가 구성할 수 있는 Red Hat Advanced Cluster Management for Kubernetes 플랫폼의 기능과 제품 사용의 측면에 대한 정보를 제공합니다. 이 기능은 귀하의 organization with help your enterprise readiness를 참조하십시오. 클라이언트가 선택하고 구성할 수 있는 다양한 방법과 제품이 타사 클러스터 및 시스템과 함께 사용할 수 있는 다양한 방법으로 인해 이 정보는 포괄적인 목록이 아닙니다.

고객은 유럽 연합 일반 데이터 보호 규정을 포함하여 다양한 법률 및 규정을 준수할 책임이 있습니다. 고객은 고객의 비즈니스에 영향을 미칠 수 있는 모든 관련 법률 및 규정의 식별 및 해석과 고객이 이러한 법률 및 규정을 준수하기 위해 취해야 할 모든 조치에 대한 조언을 얻을 책임이 있습니다.

여기에 설명된 제품, 서비스 및 기타 기능은 모든 클라이언트 상황에 적합하지 않으며 가용성을 제한할 수 있습니다. Red Hat은 법률, 회계 또는 감사 조언을 제공하거나 서비스 또는 제품이 고객이 법률 또는 규정을 준수하도록 보장한다는 것을 보증하지 않습니다.

1.5.2. 목차

- *개인 정보의 사용을 제한할 수 있는 기능*
- *부록*

1.5.3. GDPR

***general Data Protection regulations regulations (ECDHE)**는 유럽 연합 (EU)에 의해 채택되었으며 2018 년 5 월 25 일부터 적용됩니다.*

1.5.3.1. #177이 중요한 이유는 무엇입니까?

***hieradata**는 개인의 개인 데이터를 처리하기 위해 보다 강력한 데이터 보호 규제 프레임워크를 설정합니다. **iPXE**는 다음을 제공합니다.*

- *개인에 대한 새롭고 향상된 권한*
- *개인 데이터에 대한 광범위한 정의*
- *프로세서에 대한 새로운 의무*
- *비준수에 대한 상당한 금융 수익의 가능성이 있습니다.*
- *필수 데이터 위반 알림*

1.5.3.2. journalctl에 대해 자세히 알아보기

- ***EU#177** 정보 포털*
- ***Red Hat journalctl** 웹 사이트*

1.5.4. journalctl에 대한 제품 구성

다음 섹션에서는 **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼 내에서 데이터 관리의 측면을 설명하고 **client**에 대한 **requirements** 요구 사항을 지원하는 기능에 대한 정보를 제공합니다.

1.5.5. 데이터 라이프 사이클

Red Hat Advanced Cluster Management for Kubernetes는 컨테이너화된 온프레미스 애플리케이션을 개발하고 관리하기 위한 애플리케이션 플랫폼입니다. 컨테이너 오케스트레이터 **Kubernetes**, 클러스터 라이프사이클, 애플리케이션 라이프사이클 및 보안 프레임워크(정부, 위험 및 규정 준수)가 포함된 컨테이너를 관리하기 위한 통합 환경입니다.

따라서 **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼은 플랫폼 구성 및 관리와 관련된 기술 데이터를 주로 처리하며, 그 중 일부는**ECDHE**의 대상이 될 수 있습니다. **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼은 플랫폼을 관리하는 사용자에 대한 정보도 처리합니다. 이 데이터는 **10.0.0.1** 요구 사항 충족을 담당하는 고객의 인식을 위해 이 문서 전체에 설명되어 있습니다.

이 데이터는 구성 파일이나 데이터베이스에 있는 로컬 또는 원격 파일 시스템의 플랫폼에서 유지됩니다. **Kubernetes** 플랫폼용 **Red Hat Advanced Cluster Management**에서 실행되도록 개발된 애플리케이션은 **journalctl**에 따라 다른 형태의 개인 데이터를 처리할 수 있습니다. 플랫폼 데이터를 보호하고 관리하는 데 사용되는 메커니즘은 플랫폼에서 실행되는 애플리케이션에서도 사용할 수 있습니다. **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼에서 실행되는 애플리케이션에 의해 수집된 개인 데이터를 관리하고 보호하는 데 추가 메커니즘이 필요할 수 있습니다.

Kubernetes 플랫폼용 **Red Hat Advanced Cluster Management** 및 해당 데이터 흐름을 가장 잘 이해하려면 **Kubernetes, Docker** 및 **Operator**의 작동 방식을 이해해야 합니다. 이러한 오픈 소스 구성 요소는 **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼의 핵심입니다. **Kubernetes** 배포를 사용하여 **Docker** 이미지를 참조하는 **Operator**에 빌드된 애플리케이션 인스턴스를 배치합니다. **Operator**에는 애플리케이션에 대한 세부 정보가 포함되어 있으며 **Docker** 이미지에는 애플리케이션이 실행해야 하는 모든 소프트웨어 패키지가 포함되어 있습니다.

1.5.5.1. Red Hat Advanced Cluster Management for Kubernetes 플랫폼을 통한 데이터 흐름

Red Hat Advanced Cluster Management for Kubernetes는 관리자 **ID** 및 암호, 서비스 사용자 **ID** 및 암호, **IP** 주소 및 **Kubernetes** 노드 이름과 같은 개인 데이터로 간주할 수 있는 몇 가지 기술 데이터를 다룹니다. **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼은 플랫폼을 관리하는 사용자에 대한 정보도 처리합니다. 플랫폼에서 실행되는 애플리케이션은 플랫폼에 알 수 없는 다른 범주의 개인 데이터를 도입할 수 있습니다.

이 기술 데이터가 수집/생성, 저장, 액세스, 보안, 기록 및 삭제된 방법에 대한 정보는 이 문서의 뒷부분에서 설명합니다.

1.5.5.2. 온라인 연락처를 위해 사용되는 개인 데이터

고객은 주로 다음과 같은 다양한 방법으로 온라인 댓글/수증/요청을 제출할 수 있습니다.

- ***Slack** 채널이 있는 경우 공개 **Slack** 커뮤니티*
- *제품 문서에 대한 공개 댓글 또는 티켓*
- *<기술 커뮤니티의 대중의 대화>*

*일반적으로 고객 이름과 이메일 주소만 사용하여 연락처 주제의 개인 답변을 제공하며 개인 데이터 사용은 **Red Hat** 온라인 개인 정보 취급 방침 을 준수합니다.*

1.5.6. 데이터 수집

***Red Hat Advanced Cluster Management for Kubernetes** 플랫폼은 민감한 개인 데이터를 수집하지 않습니다. 관리자 **ID** 및 암호, 서비스 사용자 **ID** 및 암호, **IP** 주소 및 **Kubernetes** 노드 이름과 같은 기술 데이터를 생성하고 관리하며, 이는 개인 데이터로 간주될 수 있습니다. **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼은 플랫폼을 관리하는 사용자에 대한 정보도 처리합니다. 이러한 모든 정보는 역할 기반 액세스 제어가 있는 관리 콘솔을 통해 또는 **Kubernetes** 플랫폼 용 **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼 노드에 로그인하더라도 시스템 관리자만 액세스할 수 있습니다.*

***Red Hat Advanced Cluster Management for Kubernetes** 플랫폼에서 실행되는 애플리케이션은 개인 데이터를 수집할 수 있습니다.*

*컨테이너화된 애플리케이션을 실행하는 **Kubernetes** 플랫폼용 **Red Hat Advanced Cluster Management**의 사용 및 **journalctl** 요구 사항을 충족할 때, 다음과 같은 애플리케이션에서 수집한 개인 데이터 유형 및 해당 데이터를 관리하는 방법을 고려해야 합니다.*

- *애플리케이션이 전달될 때 데이터가 어떻게 보호되고 있습니까? 전송 중에 데이터가 암호화됩니까?*
- *데이터가 애플리케이션에 의해 어떻게 저장됩니까? 데이터가 유휴 상태에서 암호화됩니까?*
- *수집 및 저장되는 애플리케이션에 액세스하는 데 사용되는 자격 증명은 무엇입니까?*

- 애플리케이션에서 수집 및 저장된 데이터 소스에 액세스하는 데 사용하는 자격 증명은 무엇입니까?

- 필요에 따라 애플리케이션에서 수집한 데이터는 어떻게 제거됩니까?

이는 **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼에서 수집하는 데이터 유형의 최종 목록이 아닙니다. 이는 고려해야 할 예로 제공됩니다. 데이터 유형에 대한 질문이 있는 경우 **Red Hat**에 문의하십시오.

1.5.7. 데이터 스토리지

Red Hat Advanced Cluster Management for Kubernetes 플랫폼은 로컬 또는 원격 파일 시스템에 구성 파일 또는 데이터베이스에 있는 상태 저장 저장소의 플랫폼 구성 및 관리와 관련된 기술 데이터를 유지합니다. 모든 데이터를 안전하게 보호해야합니다. **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼은 **dm-crypt** 를 사용하는 상태 저장 저장소의 데이터 암호화를 지원합니다.

다음 항목에서는 **data**가 저장된 영역을 강조 표시합니다.이 항목은 **10.0.0.1**에 대해 고려해야 할 수 있습니다.

- 플랫폼 구성 데이터: **Kubernetes** 플랫폼 구성용 **Red Hat Advanced Cluster Management**는 일반 설정, **Kubernetes**, 로그, 네트워크, **Docker** 및 기타 설정에 대한 속성으로 구성 **YAML** 파일을 업데이트하여 사용자 지정할 수 있습니다. 이 데이터는 하나 이상의 노드를 배포하기 위해 **Kubernetes** 플랫폼 설치 관리자의 **Red Hat Advanced Cluster Management**로 사용됩니다. 속성에는 부트스트랩에 사용되는 관리자 **ID** 및 암호도 포함됩니다.

- **Kubernetes** 구성 데이터: **Kubernetes** 클러스터 상태 데이터는 분산 키-값 저장소인 **etcd**에 저장됩니다.

- 사용자 **ID** 및 암호를 포함한 사용자 인증 데이터: 사용자 **ID** 및 암호 관리는 클라이언트 엔터프라이즈 **LDAP** 디렉터리를 통해 처리됩니다. **LDAP**에서 정의된 사용자 및 그룹은 **Kubernetes** 플랫폼 팀용 **Red Hat Advanced Cluster Management**에 추가하고 액세스 역할을 할당할 수 있습니다. **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼은 **LDAP**의 이메일 주소와 사용자 **ID**를 저장하지만 암호는 저장하지 않습니다. **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼은 그룹 이름을 저장하고 로그인하면 사용자가 속한 사용 가능한 그룹을 캐시합니다. 그룹 멤버십은 장기적인 방식으로 유지되지 않습니다. 엔터프라이즈 **LDAP**에 남아 있는 사용자 및 그룹 데이터 보안을 고려해야 합니다. **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼에는 엔터프라이즈 디렉터리와 상호 작용하고 액세스 토큰을 유지보수하는 인증 서비스인 **OIDC(Open ID Connect)**도 포함되어 있습니다. 이 서비스는 **ETCD**를 백업 저장소로 사용합니다.

- *사용자 ID 및 암호를 포함한 서비스 인증 데이터: 구성 요소 간 액세스를 위해 Kubernetes 플랫폼 구성 요소에 사용되는 Red Hat Advanced Cluster Management에서 사용하는 자격 증명은 Kubernetes Secrets로 정의됩니다. 모든 Kubernetes 리소스 정의는 etcd 키-값 데이터 저장소에 유지됩니다. 초기 인증 정보 값은 플랫폼 구성 데이터에 Kubernetes Secret 구성 YAML 파일로 정의됩니다. 자세한 내용은 Kubernetes 문서의 시크릿 을 참조하십시오.*

1.5.8. 데이터 액세스

Kubernetes 플랫폼용 Red Hat Advanced Cluster Management 데이터는 다음과 같은 정의된 제품 인터페이스를 통해 액세스할 수 있습니다.

- *웹 사용자 인터페이스(콘솔)*
- *Kubernetes kubectl CLI*
- *Red Hat Advanced Cluster Management for Kubernetes CLI*
- *oc CLI*

이러한 인터페이스는 Red Hat Advanced Cluster Management for Kubernetes 클러스터를 관리할 수 있도록 설계되었습니다. Red Hat Advanced Cluster Management for Kubernetes에 대한 관리 액세스는 안전하게 보호할 수 있으며 요청이 수행될 때 세 가지 논리, 즉 인증, 역할 매핑 및 권한 부여가 수행됩니다.

1.5.8.1. 인증

Red Hat Advanced Cluster Management for Kubernetes 플랫폼 인증 관리자는 콘솔에서 사용자 자격 증명을 수락하고 인증 정보를 백엔드 OIDC 공급자로 전달합니다. 이 공급자는 엔터프라이즈 디렉터리에 대한 사용자 자격 증명을 검증합니다. 그러면 OIDC 공급자는 JSON 웹 토큰(JWT)의 콘텐츠와 함께 인증 관리자에 대한 인증 쿠키(auth-cookie)를 반환합니다. JWT 토큰은 인증 요청 시 그룹 멤버십 외에도 사용자 ID 및 이메일 주소와 같은 정보를 유지합니다. 이 인증 쿠키는 다시 콘솔로 전송됩니다. 세션 중에 쿠키가 새로 고쳐집니다. 콘솔에서 로그아웃하거나 웹 브라우저를 종료한 후 12시간 동안 유효합니다.

콘솔에서 생성된 모든 후속 인증 요청에 대해 프런트 엔드 NGINX 서버는 요청에서 사용 가능한 인증 쿠키를 디코딩하고 인증 관리자를 호출하여 요청의 유효성을 검사합니다.

Red Hat Advanced Cluster Management for Kubernetes 플랫폼 CLI에서 로그인할 자격 증명을

제공해야 합니다.

kubectl 및 oc CLI에는 클러스터에 액세스하기 위해 인증 정보가 필요합니다. 이러한 인증 정보는 관리 콘솔에서 얻을 수 있으며 12시간 후에 만료됩니다. 서비스 계정을 통한 액세스가 지원됩니다.

1.5.8.2. 역할 매핑

Red Hat Advanced Cluster Management for Kubernetes 플랫폼은 RBAC(역할 기반 액세스 제어)를 지원합니다. 역할 매핑 단계에서 인증 단계에서 제공되는 사용자 이름은 사용자 또는 그룹 역할에 매핑됩니다. 역할은 인증된 사용자가 수행할 수 있는 관리 활동을 승인할 때 사용됩니다.

1.5.8.3. 권한 부여

Red Hat Advanced Cluster Management for Kubernetes 플랫폼 역할은 클러스터 구성 작업, 카탈로그 및 Helm 리소스, Kubernetes 리소스에 대한 액세스를 제어합니다. Cluster Administrator, Administrator, Operator, Editor, Viewer를 포함한 여러 IAM(Identity and Access Management) 역할이 제공됩니다. 팀에 추가할 때 역할이 사용자 또는 사용자 그룹에 할당됩니다. 리소스에 대한 팀 액세스는 네임스페이스를 통해 제어할 수 있습니다.

1.5.8.4. Pod 보안

Pod 보안 정책은 Pod에서 수행할 수 있는 작업 또는 액세스할 수 있는 작업에 대한 클러스터 수준 제어를 설정하는 데 사용됩니다.

1.5.9. 데이터 처리

Kubernetes용 Red Hat Advanced Cluster Management 사용자는 시스템 구성을 통해 구성 및 관리와 관련된 기술 데이터를 처리하고 보호하는 방식을 제어할 수 있습니다.

RBAC(역할 기반 액세스 제어)는 사용자가 액세스할 수 있는 데이터 및 기능을 제어합니다.

Data-in-transit 은 TLS 를 사용하여 보호됩니다. HTTPS (TLS 기본)는 사용자 클라이언트와 백엔드 서비스 간의 보안 데이터 전송에 사용됩니다. 사용자는 설치 중에 사용할 루트 인증서를 지정할 수 있습니다.

data-at-rest 보호는 dm-crypt 를 사용하여 데이터를 암호화하는 방식으로 지원됩니다.

Kubernetes 플랫폼용 Red Hat Advanced Cluster Management for Kubernetes 플랫폼 기술 데이터를 관리하고 보호하는 데 사용되는 동일한 플랫폼 메커니즘을 사용하여 사용자 개발 또는 사용자 제공 애플리케이션의 개인 데이터를 관리하고 보호할 수 있습니다. 클라이언트는 추가 제어를 구현하기 위해 자체 기능을 개발할 수 있습니다.

1.5.10. 데이터 삭제

Red Hat Advanced Cluster Management for Kubernetes 플랫폼은 명령으로 생성되거나 제품에 의해 수집된 데이터를 삭제하기 위한 명령, API(애플리케이션 프로그래밍 인터페이스) 및 사용자 인터페이스 작업을 제공합니다. 이러한 기능을 통해 사용자는 서비스 사용자 ID 및 암호, IP 주소, Kubernetes 노드 이름 또는 기타 플랫폼 구성 데이터와 같은 기술 데이터를 삭제할 수 있습니다.

데이터 삭제 지원을 위해 고려해야 할 Kubernetes 플랫폼용 Red Hat Advanced Cluster Management 영역:

- 플랫폼 구성과 관련된 모든 기술 데이터는 관리 콘솔 또는 Kubernetes kubectl API를 통해 삭제할 수 있습니다.

계정 데이터 삭제 지원을 위해 고려해야 할 Red Hat Advanced Cluster Management for Kubernetes 플랫폼 영역입니다.

- 플랫폼 구성과 관련된 모든 기술 데이터는 Kubernetes용 Red Hat Advanced Cluster Management 또는 Kubernetes kubectl API를 통해 삭제할 수 있습니다.

엔터프라이즈 LDAP 디렉터리를 통해 관리되는 사용자 ID 및 암호 데이터를 제거하는 기능은 Kubernetes용 Red Hat Advanced Cluster Management와 함께 사용되는 LDAP 제품에서 제공합니다.

1.5.11. 개인 정보의 사용을 제한할 수 있는 기능

이 문서에 요약된 기능을 사용하여 Red Hat Advanced Cluster Management for Kubernetes 플랫폼을 사용하면 최종 사용자가 개인 데이터로 간주되는 플랫폼 내의 모든 기술 데이터 사용을 제한할 수 있습니다.

journalctl에 따라 사용자는 처리에 액세스, 수정 및 제한할 수 있는 권한이 있습니다. 다음을 제어하려면 이 문서의 다른 섹션을 참조하십시오.

- 액세스 권한

- *Red Hat Advanced Cluster Management for Kubernetes 플랫폼 관리자는 Kubernetes 플랫폼용 Red Hat Advanced Cluster Management 기능을 사용하여 개인 데이터에 액세스할 수 있습니다.*

- *Red Hat Advanced Cluster Management for Kubernetes 플랫폼 관리자는 Red Hat Advanced Cluster Management for Kubernetes 플랫폼 기능을 사용하여 Red Hat Advanced Cluster Management for Kubernetes 플랫폼의 개별 데이터에 대한 개인 정보를 제공할 수 있습니다.*

- *변경할 수 있는 권한*

  - *Red Hat Advanced Cluster Management for Kubernetes 플랫폼 관리자는 Kubernetes 플랫폼용 Red Hat Advanced Cluster Management 기능을 사용하여 사용자가 데이터를 수정하거나 수정할 수 있습니다.*

  - *Red Hat Advanced Cluster Management for Kubernetes 플랫폼 관리자는 Kubernetes 플랫폼용 Red Hat Advanced Cluster Management 기능을 사용하여 개인의 데이터를 수정할 수 있습니다.*

- *처리를 제한할 수 있는 권한*

  - *Red Hat Advanced Cluster Management for Kubernetes 플랫폼 관리자는 Kubernetes 플랫폼용 Red Hat Advanced Cluster Management 기능을 사용하여 개인의 데이터 처리를 중지할 수 있습니다.*

1.5.12. 부록

Red Hat Advanced Cluster Management for Kubernetes는 관리자 ID 및 암호, 서비스 사용자 ID 및 암호, IP 주소 및 Kubernetes 노드 이름과 같은 개인 데이터로 간주할 수 있는 몇 가지 기술 데이터를 다룹니다. Red Hat Advanced Cluster Management for Kubernetes 플랫폼은 플랫폼을 관리하는 사용자에 대한 정보도 처리합니다. 플랫폼에서 실행되는 애플리케이션은 플랫폼에 알 수 없는 다른 범주의 개인 데이터를 도입할 수 있습니다.

이 부록에는 플랫폼 서비스에서 기록한 데이터에 대한 세부 정보가 포함되어 있습니다.

1.6. FIPS 준비

Red Hat Advanced Cluster Management for Kubernetes를 위한 **FIPS** 준비 완료 **Red Hat Advanced Cluster Management**는 동일한 도구를 사용하여 암호화 호출이 **Red Hat OpenShift Container Platform**에서 사용하는 **RHEL(Red Hat Enterprise Linux)** 인증 암호화 모듈에 전달되도록 합니다. **OpenShift FIPS** 지원에 대한 자세한 내용은 **FIPS** 암호화 지원을 참조하십시오.

1.6.1. 제한

Red Hat Advanced Cluster Management 및 **FIPS**를 통해 다음과 같은 제한 사항을 확인하십시오.

- **Red Hat OpenShift Container Platform**은 **x86_64** 아키텍처에서만 **FIPS**를 지원합니다.
- **Integrity Shield**는 **FIPS**가 준비되지 않은 기술 프리뷰 구성 요소입니다.
- 검색 및 관찰 기능 구성 요소에서 사용하는 **PVC(**영구 볼륨 클레임**)** 및 **S3** 스토리지는 제공된 스토리지를 구성할 때 암호화해야 합니다. **Red Hat Advanced Cluster Management**는 스토리지 암호화를 제공하지 않으며 **OpenShift Container Platform** 설명서, **FIPS** 암호화 지원을 참조하십시오.
- **Red Hat Advanced Cluster Management** 콘솔을 사용하여 관리형 클러스터를 프로비저닝하는 경우 관리형 클러스터 생성의 **Cluster details** 섹션에서 다음 확인란을 선택하여 **FIPS** 표준을 활성화합니다.

> *FIPS with information text: Use the Federal Information Processing Standards (FIPS) modules provided with Red Hat Enterprise Linux CoreOS instead of the default Kubernetes cryptography suite file before you deploy the new managed cluster.*