Red Hat Advanced Cluster Management for Kubernetes 2.10

릴리스 노트

릴리스 노트

Last Updated: 2024-09-05

Red Hat Advanced Cluster Management for Kubernetes 2.10 릴리스 노트

릴리스 노트

법적 공지

초록

새로운 기능, 에라타 업데이트, 알려진 문제, 사용 중단 및 제거, GDPR 및 FIPS 준비 제품에 대한 제품 고려 사항에 대한 릴리스 노트에서 확인하십시오.

차례

1장. 릴리스 노트 **3**
1.1. RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES의 새로운 기능 3
1.2. 에라타 업데이트 6
1.3. 확인된 문제 8
1.4. 사용 중단 및 제거 47
1.5. GDPR 준비에 대한 RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES 플랫폼 고려 사항 51
1.6. FIPS 준비 60
1.7. 관찰 기능 지원 61

1장. 릴리스 노트

현재 릴리스에 대해 알아보십시오.

더 이상 사용되지 않음: Red Hat Advanced Cluster Management 2.7 및 이전 버전은 더 이상 지원되지 않습니다. 문서는 사용할 수 있지만 에라타 또는 기타 업데이트는 사용할 수 없습니다.

모범 사례: 최신 버전으로 업그레이드합니다.

- Red Hat Advanced Cluster Management for Kubernetes의 새로운 기능
- 에라타 업데이트
- 알려진 문제 및 제한 사항
- 사용 중단 및 제거
- GDPR 준비에 대한 Red Hat Advanced Cluster Management 고려 사항
- FIPS 준비
- 관찰 기능 지원

현재 지원되는 릴리스 중 하나 또는 제품 문서에 문제가 발생하는 경우 Red Hat 지원팀으로 이동하여 문제를 해결하거나 기술 자료 문서를 보거나 지원 팀과 연결하거나 케이스를 열 수 있습니다. 인증 정보를 사용하여 로그인해야 합니다. Red Hat 고객 포털 FAQ에서 고객 포털 설명서에 대해 자세히 알아볼 수도 있습니다.

이 문서는 문서의 구성 요소가 특정 버전의 OpenShift Container Platform에서만 생성되고 테스트되지 않는 한 가장 빨리 지원되는 Red Hat OpenShift Container Platform 버전을 참조합니다.

전체 지원 정보는 Red Hat Advanced Cluster Management for Kubernetes의 지원 매트릭스 및 라이프 사이클 및 업데이트 정책을 참조하십시오.

1.1. RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES의 새로운 기능

Red Hat Advanced Cluster Management for Kubernetes는 기본 제공 거버넌스, 클러스터 라이프사이클 관리 및 애플리케이션 라이프사이클 관리와 함께 관찰 기능을 통해 전체 Kubernetes 도메인에 대한 가시성을 제공합니다. 이번 릴리스에서는 더 많은 환경에서 클러스터 관리, 애플리케이션 GitOps 통합 등을 이동할 수 있습니다.

지원 매트릭스 에 액세스하여 허브 클러스터 및 관리형 클러스터 요구 사항 및 지원에 대해 알아보십시오.

중요: 일부 기능 및 구성 요소는 기술 프리뷰로 확인 및 릴리스됩니다.

- 클러스터
- 다중 클러스터 글로벌 허브
- 애플리케이션
- 가시성
- 거버넌스

- 백업 및 복원
- 네트워킹

1.1.1. Cluster

클러스터 라이프사이클 구성 요소 및 기능은 클러스터 플릿 관리를 개선하는 소프트웨어 운영자인 다중 클러스터 엔진 운영자 내에 있습니다. 멀티 클러스터 엔진 Operator는 클라우드 및 데이터 센터 전체에서 OpenShift Container Platform 및 Kubernetes 클러스터 라이프사이클 관리를 지원합니다. OpenShift Container Platform은 이 기술의 사전 요구 사항입니다.

- 다중 클러스터 엔진 Operator(클러스터)에 대한 문서는 제품 문서의 Cluster Lifecycle 섹션에서 확인할 수 있습니다.
- 클러스터 *라이프사이클 의 다중 클러스터 엔진 Operator 2.5의 새로운 기능* 보기.
- 클러스터 라이프사이클 개요에서 작업 및 지원 정보를 확인합니다 .

1.1.2. 다중 클러스터 글로벌 허브

Red Hat Advanced Cluster Management 백업 및 복원 기능과 함께 다중 클러스터 글로벌 허브를 사용할 수 있습니다. 이러한 기능을 통해 복구 솔루션 및 기본 리소스에 액세스할 수 있습니다. 자세한 내용은 Backup for multicluster global hub (기술 프리뷰) 를 참조하십시오.

기타 다중 클러스터 글로벌 허브 주제는 다중 클러스터 글로벌 허브 를 참조하십시오.

1.1.3. 애플리케이션

새 **.status.subscription** 필드를 사용하면 개별 패키지의 패키지 상태 대신 전체 서브스크립션 상태를 확인할 수 있습니다.

기타 애플리케이션 주제는 애플리케이션 관리를 참조하십시오.

1.1.4. 가시성

- 이제 허브 수집기 지표가 항상 수집되어 Red Hat Advanced Cluster Management Thanos 인스턴스로 전송됩니다. Observability를 활성화하면 서비스는 허브 클러스터의 **open-cluster-management-observability** 네임스페이스에서 **endpoint-operator** 및 **metrics-collector** Pod를 시작합니다. **MultiClusterObservability** Operator는 **endpoint-operator** 및 **metrics-collector** Pod를 시작하고 관리합니다. Observability 애드온은 더 이상 Pod를 제어하지 않습니다. 자세한 내용은 Observability 아키텍처를 참조하십시오.
- Grafana 대시보드를 사용하여 호스팅된 컨트롤 플레인 클러스터 용량 추정 및 기존 호스팅 컨트롤 플레인 리소스 사용률을 볼 수 있습니다. 호스팅된 컨트롤 플레인 관찰 기능은 클러스터 라이프사이클 또는 멀티 클러스터 엔진 Operator 및 Red Hat Advanced Cluster Management 통합에서 볼 수 있는 Red Hat Advanced Cluster Management 통합의 일부입니다.

Observability 서비스 소개 를 참조하십시오.

1.1.5. 거버넌스

- **기술 프리뷰** 를 사용하면 정책 준수 기록 API를 사용하여 허브 클러스터에 대한 규정 준수 기록 이벤트를 저장하고 쿼리할 수 있습니다. 정책 준수 기록 API(기술 프리뷰) 를 참조하십시오. API를 활성화하려면 정책 준수 기록(기술 프리뷰) 을 참조하십시오.

- 승인 이벤트를 관리하도록 Gatekeeper Operator webhook의 작업을 구성합니다. 자세한 내용은 Gatekeeper Operator 정책 관리를 참조하십시오.

- 정책 생성기를 활성화하여 Helm 차트를 처리하고 정책에 대한 설명을 추가합니다. **policyDefaults.policyLabels** 및 **policies.policyLabels** 선택적 사양 및 정책 생성기 구성 참조 테이블에 있는 추가 사양을 참조하십시오.

- **ConfigurationPolicy** 리소스에서 **recordDiff** 매개변수를 사용하여 **ConfigurationPolicy** 리소스에 대해 *diff 로깅* 을 활성화할 수 있습니다. 관리되는 클러스터의 **object-template** 과 오브젝트의 차이점은 관리 클러스터의 **config-policy-controller** Pod 내에 기록됩니다. 자세한 내용은 디버그 로그 구성을 참조하십시오.

- 정책 생성기를 활성화하여 Helm 차트를 처리하고 정책에 대한 설명을 추가합니다. 자세한 내용은 Policy Generator 구성 참조 표를 참조하십시오.

- 이제 거버넌스 프레임워크의 동시성을 구성할 수 있습니다. 자세한 내용은 정책 컨트롤러 고급 구성 을 참조하십시오.

- Gatekeeper Operator는 기본적으로 비활성화된 **auditFromCache** 감사 내의 사용자 정의 리소스 정의에 설정을 노출합니다. **auditFromCache** 를 활성화한 다음 동기화 세부 정보로 **config.gatekeeper.sh** 를 설정할 수 있습니다. 자세한 내용은 Gatekeeper Operator 정책 관리를 참조하십시오.

- **auditEventsInvolvedNamespace** 에서 생성할 네임스페이스 감사 이벤트를 관리하고, **admissionEventsInvolvedNamespace** 를 활성화하여 생성할 네임스페이스 승인 이벤트를 관리할 수 있습니다. Gatekeeper Operator 정책 관리를 참조하십시오.

- **기술 프리뷰:** Operator 정책 컨트롤러를 사용하여 클러스터 전체에서 OLM(Operator Lifecycle Manager) Operator를 모니터링하고 설치할 수 있습니다. 자세한 내용은 Operator 정책 컨트롤러 (기술 프리뷰) 를 참조하십시오.

- **배치** 리소스를 사용하여 정책을 배치할 위치를 정의합니다. 자세한 내용은 정책 개요 를 참조하십시오.

대시보드 및 정책 프레임워크에 대한 자세한 내용은 Governance 를 참조하십시오.

1.1.6. 백업 및 복원

- **backup-restore-enabled** 정책에는 **OADP 채널** 이라는 새 템플릿이 포함됩니다. **OADP-channel** 템플릿을 사용하여 백업을 방지하고 Operator가 잘못된 사용자 정의 리소스 정의로 실행되지 않도록 합니다. 자세한 내용은 백업 유효성 검사 또는 복원 구성을 참조하십시오.

- **MultiClusterHub** 에서 백업 구성 요소를 활성화하면 클러스터 백업 및 복원 Operator Helm 차트가 정책을 설치합니다. 새로운 **backup-restore-auto-import** 는 자동 관리 클러스터 가져오기 기능의 문제에 대해 알려줍니다. 자세한 내용은 백업 유효성 검사 또는 복원 구성을 참조하십시오.

허브 클러스터의 재해 복구 솔루션에 대한 자세한 내용은 백업 및 복원을 참조하십시오.

1.1.7. 네트워킹

- IBM Power Systems Virtual Server에 Submariner를 배포할 수 있습니다. 자세한 내용은 콘솔을 사용하여 Submariner 배포를 참조하십시오.

- **기술 프리뷰:** IBM Cloud에서 Red Hat OpenShift에 Submariner를 배포할 수도 있습니다. 자세한 내용은 콘솔을 사용하여 Submariner 배포를 참조하십시오.

네트워킹을 참조하십시오.

1.1.8. 이 릴리스에 대해 자세히 알아보기

- welcome에서 Red Hat Advanced Cluster Management for Kubernetes for Kubernetes에 대한 개요를 확인하십시오.
- Red Hat Advanced Cluster Management 릴리스 노트의 *알려진 문제 및 제한과* 같은 릴리스 노트를 참조하십시오.
- 제품의 주요 구성 요소에 대한 자세한 내용은 Multicluster 아키텍처 주제를 참조하십시오.
- Red Hat Advanced Cluster Management Troubleshooting 가이드의 지원 정보 및 자세한 내용을 참조하십시오.
- 오픈 커뮤니티의 상호 작용, 성장 및 기여를 위해 오픈 소스 오픈 *클러스터 관리* 리포지토리에 액세스합니다. 참여하려면 open-cluster-management.io 를 참조하십시오. 자세한 내용은 GitHub 리포지토리를 참조하십시오.

1.2. 에라타 업데이트

기본적으로 에라타 업데이트는 릴리스될 때 자동으로 적용됩니다. 자세한 내용은 릴리스가 릴리스될 때 여기에 게시됩니다.

중요: 참조를 위해 에라타 링크 및 Jira 번호가 콘텐츠에 추가되고 내부적으로 사용될 수 있습니다. 액세스가 필요한 링크는 사용자에게 제공되지 않을 수 있습니다.

업그레이드에 대한 자세한 내용은 Operator를 사용하여 업그레이드 를 참조하십시오.

1.2.1. 에라타 2.10.5

- 하나 이상의 제품 컨테이너 이미지에 대한 업데이트를 제공합니다.

1.2.2. Errata 2.10.4

- Red Hat Advanced Cluster Management for Kubernetes 버전 2.10을 사용하여 Red Hat OpenShift Container Platform 버전 4.16에 대한 완전 지원을 추가합니다.
- YAML 구분자를 추가하여 **Subscription** 및 **PlacementRule** YAML 콘텐츠를 구분합니다. 구분자가 없으면 콘텐츠가 잘못 구문 분석되었습니다. (ACM-12133)
- 서비스 계정에 대한 권한이 누락되어 **OperatorPolicy** 를 정책 종속성으로 지정하면 **governance-policy-framework** Pod가 충돌하는 문제가 해결되었습니다. (ACM-12436)
- 하나 이상의 제품 컨테이너 이미지에 대한 업데이트를 제공합니다.

1.2.3. Errata 2.10.3

- 정책을 클러스터의 오브젝트와 비교할 때 **ConfigurationPolicy** 컨트롤러에서 시험 실행 업데이트를 완료하지 못한 경우 오류를 보고하는 누락된 로그 메시지를 추가합니다. (ACM-10612)
- 삭제 후 정책이 빠르게 다시 생성되면 문제가 해결되어 관리 클러스터에서 규정 준수 상태가 채워지는 경우가 있습니다. (ACM-10664)

- 기본 로그 세부 정보 표시 설정으로 **governance-policy-framework** Pod에서 불필요한 로그가 표시되는 문제를 해결합니다. (ACM-10693)

- Gatekeeper Operator를 설치하거나 제거할 때 **governance-policy-framework** Pod를 다시 시작해야 하는 문제를 해결합니다. 이제 Pod를 다시 시작하지 않고 Gatekeeper와 Kubernetes 통합을 위한 Red Hat Advanced Cluster Management가 활성화되거나 비활성화됩니다. (ACM-10966)

- **MustOnlyHave** 규정 준수 유형의 **ConfigurationPolicy** 리소스가 정책 정의와 비교할 때 클러스터의 오브젝트에서 루트 수준 키를 인수하지 않은 버그가 수정되었습니다. (ACM-10877)

- 정책 생성기의 문제를 해결하여 **policyDefaults** 매개변수 섹션 외부에 존재하는 일부 배치 덮어쓰기가 기본값을 올바르게 재정의하지 않았습니다. (ACM-11075)

- 일부 클라우드 공급자에 의해 **application-manager** 라는 애플리케이션 애드온 서비스 계정이 프로비저닝되면 Red Hat Advanced Cluster Management **gitopsCluster** 컨트롤러가 Argo CD 푸시 모델에 대한 관리형 클러스터 시크릿을 자동으로 생성하지 못하는 문제를 해결합니다. (ACM-11149)

- **OperatorPolicy** 규정 준수 메시지에 동일한 메시지가 반복적으로 표시되지만 Operator 설치에 여러 오류로 실패한 경우 다른 순서가 있는 문제를 해결합니다. (ACM-11204)

- 하나 이상의 제품 컨테이너 이미지에 대한 업데이트를 제공합니다.

1.2.4. Errata 2.10.2

- **AddOnDeploymentConfig** 애드온을 업데이트 또는 삭제한 후 **multicluster-observability-controller** 가 조정되지 않은 문제를 해결합니다. (ACM-10406)

- **multicluster-observability-controller** 가 **AddOnDeploymentConfig** 애드온의 **nodePlacement** 필드에 설정된 구성으로 변경되지 않은 문제를 해결합니다. (ACM-10811)

- **multicluster-observability-controller** 에서 업그레이드 문제를 해결하여 **ServiceAccount** 를 지속적으로 업데이트했습니다. 연속 업데이트로 인해 여러 **Secret** 오브젝트가 시간이 지남에 따라 생성되었습니다. (ACM-10967)

- 하나 이상의 제품 컨테이너 이미지에 대한 업데이트를 제공합니다.

1.2.5. Errata 2.10.1

- Red Hat Advanced Cluster Management for Kubernetes 백업 및 복구 기능을 사용하는 사용자에게 발생할 수 있는 문제를 수정하고 **cluster.open-cluster-management.io/backup: cluster-activation** 레이블을 사용하지 않고 **managedcluster** 네임스페이스를 백업합니다. 이로 인해 관리 클러스터 네임스페이스가 복원된 후 **Terminating** 상태로 유지되었습니다. (ACM-9780)

- **governance-policy-framework** Pod가 관리되는 클러스터에서 종료되는 동안 정책이 업데이트될 때 **취소된 컨텍스트** 메시지와 함께 정책을 일시적으로 설정할 수 있는 문제를 해결합니다. **(ACM-10402)**

- **일부 수정으로 인해 콘솔에서 정책 세부 정보를 새로 고치기 전에 새로 생성된 정책을 찾을 수 없는 것으로 표시되는 문제가 해결되었습니다. (ACM-10416)**

- 하나 이상의 제품 컨테이너 이미지에 대한 업데이트를 제공합니다.

1.3. 확인된 문제

애플리케이션 관리의 알려진 문제를 검토합니다. 다음 목록에는 이 릴리스에 대한 알려진 문제 또는 이전 릴리스에서 계속되는 알려진 문제가 포함되어 있습니다.

Red Hat OpenShift Container Platform 클러스터의 경우 **OpenShift Container Platform** 알려진 문제를 참조하십시오.

사용 중단 및 제거에 대한 자세한 내용은 사용 중단 및 제거를 참조하십시오.

클러스터 관리 또는 *클러스터 라이프사이클* 은 **Red Hat Advanced Cluster Management**를 사용하거나 사용하지 않고 멀티 클러스터 엔진 **Operator**에서 제공합니다. **Red Hat Advanced Cluster Management**에만 적용되는 클러스터 관리의 알려진 문제 및 제한 사항을 참조하십시오. 대부분의 클러스터 관리 알려진 문제는 클러스터 라이프 사이클의 알려진 문제의 클러스터 수명 문서에 있습니다.

- 설치 알려진 문제
- 비즈니스 연속성 알려진 문제
- 콘솔의 알려진 문제
- 애플리케이션 알려진 문제
- 관찰 가능성 알려진 문제
- 거버넌스 알려진 문제
- 네트워킹 알려진 문제

1.3.1. 설치 알려진 문제

설치 및 업그레이드에 대한 알려진 문제를 검토하십시오. 다음 목록에는 이 릴리스에 대한 알려진 문제 또는 이전 릴리스에서 계속되는 알려진 문제가 포함되어 있습니다.

Red Hat OpenShift Container Platform 클러스터의 경우 OpenShift Container Platform 알려진 문제를 참조하십시오.

사용 중단 및 제거에 대한 자세한 내용은 사용 중단 및 제거를 참조하십시오.

1.3.1.1. 업그레이드로 이전 버전을 설치 제거하고 다시 설치하면 실패할 수 있습니다.

OpenShift Container Platform에서 Red Hat Advanced Cluster Management를 설치 제거하면 나중에 이전 버전을 설치한 다음 업그레이드하려는 경우 문제가 발생할 수 있습니다. 예를 들어 OpenShift Container Platform에서 Red Hat Advanced Cluster Management를 설치 제거한 다음 이전 버전의 Red Hat Advanced Cluster Management를 설치하고 해당 버전을 업그레이드하면 업그레이드가 실패할 수 있습니다. StorageVersionMigration 사용자 정의 리소스가 제거되지 않은 경우 업그레이드가 실패합니다.

Red Hat Advanced Cluster Management를 설치 제거할 때 다시 설치하고 업그레이드하기 전에 이전 StorageVersionMigration 을 수동으로 제거해야 합니다.

예를 들어 이전 버전의 Red Hat Advanced Cluster Management를 사용하기 위해 OpenShift Container Platform에서 Red Hat Advanced Cluster Management 2.10을 제거하는 경우 StorageVersionMigration 리소스를 제거하지 않으면 업그레이드에 실패합니다.

1.3.1.2. ARM 통합 흐름을 사용한 인프라 Operator 오류

infrastructure-operator 를 설치할 때 ARM과 통합 흐름이 작동하지 않습니다. 이 문제를 해결하려면 ALLOW_CONVERGED_FLOW 를 false 로 설정합니다.

1. 다음 명령을 실행하여 ConfigMap 리소스를 생성합니다.

```
oc create -f
```

2. oc apply -f 를 실행하여 파일을 적용합니다. ALLOW_CONVERGED_FLOW 가 false 로 설정된 다음 파일 샘플을 참조하십시오.

```
apiVersion: v1
```

```
kind: ConfigMap
metadata:
  name: my-assisted-service-config
  namespace: assisted-installer
data:
  ALLOW_CONVERGED_FLOW: false
```

3. 다음 명령을 사용하여 **agentserviceconfig** 에 주석을 답니다.

```
oc annotate --overwrite AgentServiceConfig agent unsupported.agent-
install.openshift.io/assisted-service-configmap=my-assisted-service-config
```

문제가 해결되면 에이전트가 인벤토리에 나타납니다.

1.3.1.3. 에라타 릴리스로 업그레이드한 후에도 더 이상 사용되지 않는 리소스가 남아 있습니다.

2.4.x에서 **2.5.x**로 업그레이드한 후 **2.6.x**로 업그레이드한 후 관리 클러스터 네임스페이스에서 더 이상 사용되지 않는 리소스가 남아 있을 수 있습니다. 버전 **2.6.x**가 **2.4.x**에서 업그레이드된 경우 이러한 더 이상 사용되지 않는 리소스를 수동으로 삭제해야 합니다.

참고: 버전 **2.5.x**에서 버전 **2.6.x**로 업그레이드하기 전에 **30**분 이상 기다려야 합니다.

콘솔에서 삭제하거나 삭제하려는 리소스에 대해 다음 예와 유사한 명령을 실행할 수 있습니다.

```
oc delete -n <managed cluster namespace> managedclusteraddons.addon.open-cluster-
management.io <resource-name>
```

남아 있을 수 있는 더 이상 사용되지 않는 리소스 목록을 참조하십시오.

```
managedclusteraddons.addon.open-cluster-management.io:
policy-controller
manifestworks.work.open-cluster-management.io:
-klusterlet-addon-appmgr
-klusterlet-addon-certpolicyctrl
-klusterlet-addon-crds
-klusterlet-addon-iampolicyctrl
-klusterlet-addon-operator
-klusterlet-addon-policyctrl
-klusterlet-addon-workmgr
```

1.3.1.4. Red Hat Advanced Cluster Management를 업그레이드한 후 Pod가 백업되지 않을 수 있습니다.

Red Hat Advanced Cluster Management를 새 버전으로 업그레이드한 후 StatefulSet 에 속하는 몇 개의 Pod가 failed 상태로 남아 있을 수 있습니다. 이 infrequent 이벤트는 알려진 Kubernetes 문제로 인해 발생합니다.

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

1.3.1.5. OpenShift Container Platform 클러스터 업그레이드 실패 상태

OpenShift Container Platform 클러스터가 업그레이드 단계에 있으면 클러스터 pod가 다시 시작되고 1-5 분의 변형에 대한 업그레이드 실패 상태로 남아 있을 수 있습니다. 이 동작은 예상되는 후 몇 분 후에 해결됩니다.

1.3.1.6. MultiClusterEngine 버튼이 작동하지 않는 생성

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

MultiClusterEngine 필요

이 Operator를 사용하려면 MultiClusterEngine 인스턴스를 생성합니다.

팝업 창 메시지의 Create MultiClusterEngine 버튼이 작동하지 않을 수 있습니다. 이 문제를 해결하려면 Provided API 섹션의 MultiClusterEngine 타일에서 Create instance 를 선택합니다.

1.3.2. 비즈니스 연속성 알려진 문제

Red Hat Advanced Cluster Management for Kubernetes의 알려진 문제를 검토합니다. 다음 목록에는 이 릴리스에 대한 알려진 문제 또는 이전 릴리스에서 계속되는 알려진 문제가 포함되어 있습니다.

Red Hat OpenShift Container Platform 클러스터의 경우 OpenShift Container Platform 알려진 문제를 참조하십시오.

사용 중단 및 제거에 대한 자세한 내용은 사용 중단 및 제거를 참조하십시오.

1.3.2.1. 알려진 문제 백업 및 복원

사용 가능한 경우 해결 방법과 함께 알려진 문제 및 제한 사항이 여기에 나열되어 있습니다.

1.3.2.1.1. hub 클러스터 백업 및 복원 중에 *cluster-proxy-addon* 실패

Red Hat Advanced Cluster Management Hub 클러스터를 백업하고 제거하고 동일한 클러스터에 다시 설치한 다음 복원하면 **cluster-proxy-addon** 이 작동하지 않습니다. **Pod** 로그에서 다음 오류 메시지가 표시됩니다.

```
E0430 19:11:20.810624 1 clientset.go:188] "cannot connect once" err="rpc error: code = Unavailable desc = connection error: desc = \"transport: authentication handshake failed: tls: failed to verify certificate: x509: certificate signed by unknown authority\""
```

이 문제를 해결하려면 다음 단계를 완료합니다.

1. 다음 명령을 실행하여 **cluster-proxy-addon** 을 비활성화합니다.

```
oc patch mce multiclusterengine --type=merge -p '{"spec":{"overrides":{"components":[

{"name":"cluster-proxy-addon","enabled": false}
]}}}'
```

2. 다음 명령을 실행하여 **cluster-proxy-addon** 을 다시 설치합니다.

```
oc patch mce multiclusterengine --type=merge -p '{"spec":{"overrides":{"components":[

{"name":"cluster-proxy-addon","enabled": true}
]}}}'
```

1.3.2.1.2. *open-cluster-management-backup* 네임스페이스가 *Terminating* 상태로 유지됨

MultiClusterHub 리소스에서 **cluster-backup** 구성 요소가 비활성화되면 **Red Hat Advanced Cluster Management** 복원 작업에서 생성된 **Velero** 복원 리소스가 있는 경우 **open-cluster-management-backup** 네임스페이스가 **Terminating** 상태로 고정됩니다.

Terminating 상태는 **restores.velero.io/external-resources-finalizer** 에서 완료될 때까지 대기 중인 **Velero** 복원 리소스의 결과입니다. 이 문제를 해결하려면 다음 단계를 완료합니다.

1. **MultiClusterHub** 리소스에서 클러스터 백업 옵션을 비활성화하기 전에 모든 **Red Hat**

Advanced Cluster Management 복원 리소스를 삭제하고 Velero 복원이 정리될 때까지 기다립니다.

2. open-cluster-management-backup 네임스페이스가 이미 Terminating 상태에 있는 경우 모든 Velero 복원 리소스를 편집하고 종료자를 제거합니다.

3. Velero 리소스가 네임스페이스 및 리소스를 삭제할 수 있도록 허용합니다.

1.3.2.1.3. 관리 클러스터 백업에서 더 이상 베어 메탈 허브 리소스를 백업하지 않음

Red Hat Advanced Cluster Management 백업 및 복원 기능을 사용하여 베어 메탈 클러스터의 리소스를 백업하고 보조 허브 클러스터로 복원하는 경우 관리 클러스터는 기존 관리 클러스터를 삭제하는 노드에 다시 설치됩니다.

참고: 이는 제로 터치 프로비저닝을 사용하여 배포된 베어 메탈 클러스터에만 영향을 미칩니다. 즉, 베어 메탈 노드의 전원을 켜거나 끄고 부팅하기 위한 가상 미디어를 관리하는 BareMetalHost 리소스가 있습니다. 관리 클러스터 배포에 BareMetalHost 리소스를 사용하지 않은 경우 부정적인 영향을 미치지 않습니다.

이 문제를 해결하기 위해 기본 허브 클러스터의 BareMetalHost 리소스는 더 이상 관리 클러스터 백업과 함께 백업되지 않습니다.

다른 사용 사례가 있고 기본 허브 클러스터의 관리 BareMetalHost 리소스를 백업하려면 기본 허브 클러스터의 BareMetalHost 리소스에 다음 backup 레이블을 추가합니다. cluster.open-cluster-management.io/backup.

일반 리소스를 백업하는 데 이 백업 레이블을 사용하는 방법에 대한 자세한 내용은 백업되는 리소스 항목을 참조하십시오.

1.3.2.1.4. OADP 1.1.2 이상을 사용할 때 *BackupSchedule* 에서 *FailedValidation* 상태를 표시합니다.

Red Hat Advanced Cluster Management 백업 및 복원 구성 요소를 활성화하고 DataProtectionApplication 리소스를 성공적으로 생성하면 BackupStorageLocation 리소스가 Available. OADP 버전 1.1.2 이상을 사용하는 경우 BackupSchedule 리소스를 생성하고 상태는 FailedValidation:

```
oc get backupschedule -n open-cluster-management-backup
NAME PHASE MESSAGE
rosa-backup-schedule FailedValidation Backup storage location is not available. Check
```

velero.io.BackupStorageLocation and validate storage credentials.

이 오류는 **BackupStorageLocation** 리소스에서 **ownerReference** 에 대한 값이 누락되어 발생합니다. **DataProtectionApplication** 리소스의 값은 **ownerReference** 의 값으로 사용해야 합니다.

문제를 해결하려면 **ownerReference** 를 **BackupStorageLocation** 에 수동으로 추가합니다.

1. 다음 명령을 실행하여 **oadp-operator.v1.1.2** 파일을 엽니다.

```
oc edit csv -n open-cluster-management-backup oadp-operator.v1.1.2
```

2. **OADP Operator CSV**에서 **1** 을 **0** 으로 교체하여 **spec.deployments.label.spec.replicas** 값을 편집합니다.

3. 다음 예와 같이 **YAML** 스크립트의 **ownerReference** 주석을 패치합니다.

```
metadata:
resourceVersion: '273482'
name: dpa-sample-1
uid: 4701599a-cdf5-48ac-9264-695a95b935a0
namespace: open-cluster-management-backup
ownerReferences: <<

apiVersion: oadp.openshift.io/v1alpha1
blockOwnerDeletion: true
controller: true
kind: DataProtectionApplication
name: dpa-sample
uid: 52acd151-52fd-440a-a846-95a0d7368ff7
```

4. **spec.deployments.label.spec.replicas** 의 값을 다시 **1** 로 변경하여 새 설정으로 데이터 보호 애플리케이션 프로세스를 시작합니다.

1.3.2.1.5. Velero 복원 제한

새 허브 클러스터는 데이터가 복원된 새 허브 클러스터에 사용자가 생성한 리소스가 있는 경우 활성 허브 클러스터와 다른 구성을 가질 수 있습니다. 예를 들어 새 허브 클러스터에서 백업 데이터를 복원하기 전에 새 허브 클러스터에서 생성된 기존 정책이 포함될 수 있습니다.

Velero는 복원된 백업의 일부가 아닌 경우 기존 리소스를 건너뛰므로 새 **hub** 클러스터의 정책은 변

경되지 않고 유지되어 새 **hub** 클러스터와 활성 허브 클러스터 간에 다른 구성이 생성됩니다.

이 제한을 해결하기 위해 클러스터 백업 및 복원 **Operator**는 복원 후 작업을 실행하여 **restore.cluster.open-cluster-management.io** 리소스가 생성되면 사용자가 생성한 리소스 또는 다른 복원 작업을 정리합니다.

자세한 내용은 백업 설치 및 복원 연산자 항목을 참조하십시오.

1.3.2.1.6. 수동 구성에서는 관리되는 클러스터를 표시하지 않음

관리형 클러스터는 패시브 허브 클러스터에서 활성화 데이터가 복원된 경우에만 표시됩니다.

1.3.2.1.7. 복원되지 않은 관리형 클러스터 리소스

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

복원된 클러스터에서 **local-cluster** 리소스와 관련된 구성 변경 사항을 수동으로 적용해야 합니다. 백업 설치 및 복원 **Operator** 항목에서 *새 허브 클러스터 준비*를 참조하십시오.

1.3.2.1.8. 복원된 Hive 관리 클러스터에서 새 허브 클러스터와 연결하지 못할 수 있습니다.

새 허브 클러스터에서 **Hive** 관리 클러스터에 대한 변경되거나 교체된 **CA**(인증 기관)의 백업을 복원하면 관리 클러스터가 새 허브 클러스터에 연결되지 않습니다. 백업과 함께 사용할 수 있는 이 관리형 클러스터의 **admin kubeconfig** 시크릿이 더 이상 유효하지 않기 때문에 연결이 실패합니다.

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

1.3.2.1.9. 가져온 관리 클러스터에 *Pending 가져오기* 상태가 표시됨

기본 허브 클러스터에서 수동으로 가져온 관리형 클러스터에는 수동 허브 클러스터에서 활성화 데이터가 복원될 때 **Pending** 가져오기 상태가 표시됩니다. 자세한 내용은 관리형 서비스 계정을 사용하여 클러스터 연결을 참조하십시오.

1.3.2.1.10. hub 클러스터를 복원한 후 *appliedmanifestwork* 가 관리 클러스터에서 제거되지 않음

새 허브 클러스터에서 허브 클러스터 데이터를 복원하면 고정된 클러스터 세트가 아닌 애플리케이션 서브스크립션에 대한 배치 규칙이 있는 관리 클러스터에서 **applymanifestwork** 가 제거되지 않습니다.

고정된 클러스터 세트가 아닌 애플리케이션 서브스크립션에 대한 배치 규칙의 다음 예를 참조하십시오.

```
spec:
  clusterReplicas: 1
  clusterSelector:
    matchLabels:
      environment: dev
```

결과적으로 관리 클러스터가 복원된 허브 클러스터에서 분리되면 애플리케이션이 분리됩니다.

문제를 방지하려면 배치 규칙에 고정 클러스터 세트를 지정합니다. 다음 예제를 참조하십시오.

```
spec:
  clusterSelector:
    matchLabels:
      environment: dev
```

다음 명령을 실행하여 나머지 **appliedmanifestwork** 를 수동으로 삭제할 수도 있습니다.

```
oc delete appliedmanifestwork <the-left-appliedmanifestwork-name>
```

1.3.2.1.11. *appliedmanifestwork* 가 제거되지 않고 사양에서 *agentID* 가 누락되어 있습니다.

Red Hat Advanced Cluster Management 2.6을 기본 허브 클러스터로 사용하지만 복원 허브 클러스터가 **2.7** 이상 버전 **2.7** 이상이면 **2.7** 릴리스에 이 필드가 도입되므로 **agentID** 가 **appliedmanifestworks** 사양에 누락되어 있습니다. 이로 인해 관리 클러스터의 기본 허브에 대한 추가 적용된**manifestworks** 가 생성됩니다.

이 문제를 방지하려면 기본 허브 클러스터를 **Red Hat Advanced Cluster Management 2.7**로 업그레이드한 다음 새 **hub** 클러스터에서 백업을 복원합니다.

각 **appliedmanifestwork** 에 대해 **spec.agentID** 를 수동으로 설정하여 관리 클러스터를 수정합니다.

1. 다음 명령을 실행하여 **agentID** 를 가져옵니다.

```
oc get klusterlet klusterlet -o jsonpath='{.metadata.uid}'
```

2. 다음 명령을 실행하여 각 **appliedmanifestwork** 에 **spec.agentID** 를 설정합니다.

```
oc patch appliedmanifestwork <appliedmanifestwork_name> --type=merge -p '{"spec": {"agentID": "'$AGENT_ID'"}}'
```

1.3.2.1.12. *managed-serviceaccount* 애드온 상태가 *알 수 없음*표시

새 허브 클러스터의 **Kubernetes Operator** 리소스에 대해 다중 클러스터 엔진에서 활성화하지 않고 관리형 서비스 계정을 사용하는 경우 관리형 클러스터 **appliedmanifestwork addon-serviceaccount-deploy** 가 가져온 관리 클러스터에서 제거됩니다.

관리 클러스터는 여전히 새 **hub** 클러스터로 가져오지만 **managed-serviceaccount** 애드온 상태가 표시됩니다.

다중 클러스터 엔진 **Operator** 리소스에서 **Managed Service** 계정을 활성화한 후 **managed-serviceaccount** 애드온을 복구할 수 있습니다. 관리형 서비스 계정을 활성화하는 방법을 알아보려면 자동 가져오기 활성화를 참조하십시오.

1.3.3. 콘솔의 알려진 문제

콘솔의 알려진 문제를 검토합니다. 다음 목록에는 이 릴리스에 대한 알려진 문제 또는 이전 릴리스에서 계속되는 알려진 문제가 포함되어 있습니다.

Red Hat OpenShift Container Platform 클러스터의 경우 **OpenShift Container Platform** 알려진 문제를 참조하십시오.

사용 중단 및 제거에 대한 자세한 내용은 사용 중단 및 제거를 참조하십시오.

1.3.3.1. 콘솔에서 OpenShift Dedicated를 업그레이드할 수 없음

콘솔에서 **OpenShift Dedicated** 클러스터에 대한 업그레이드를 요청할 수 있지만 **openshift** 클러스터 이외의 클러스터 오류 메시지와 함께 업그레이드할 수 없습니다. 현재는 해결방법이 없습니다.

1.3.3.2. Search PostgreSQL pod가 CrashLoopBackoff 상태입니다.

search-postgres Pod는 CrashLoopBackoff 상태입니다. Red Hat Advanced Cluster Management가 hugepages 매개변수가 활성화된 노드가 있는 클러스터에 배포하고 search-postgres Pod가 이러한 노드에서 예약되는 경우 Pod가 시작되지 않습니다.

search-postgres Pod의 메모리를 늘리려면 다음 단계를 완료합니다.

1. 다음 명령을 사용하여 search-operator Pod를 일시 중지합니다.

```
oc annotate search search-v2-operator search-pause=true
```

2. hugepages 매개변수 제한으로 search-postgres 배포를 업데이트합니다. 다음 명령을 실행하여 hugepages 매개변수를 512Mi 로 설정합니다.

```
oc patch deployment search-postgres --type json -p '[{"op": "add", "path":
"/spec/template/spec/containers/0/resources/limits/hugepages-2Mi", "value":"512Mi"}]'
```

3. Pod의 메모리 사용량을 확인하기 전에 search-postgres 포드가 Running 상태인지 확인합니다. 다음 명령을 실행합니다.

```
oc get pod <your-postgres-pod-name>  -o jsonpath="Status: {.status.phase}"
```

4. 다음 명령을 실행하여 search-postgres Pod의 메모리 사용량을 확인합니다.

```
oc get pod <your-postgres-pod-name> -o
jsonpath='{.spec.containers[0].resources.limits.hugepages-2Mi}'
```

다음 값이 512Mi 로 표시됩니다.

1.3.3.3. 클러스터 세트의 네임스페이스 바인딩을 편집할 수 없음

admin 역할 또는 bind 역할을 사용하여 클러스터 세트의 네임스페이스 바인딩을 편집하면 다음 메시지와 유사한 오류가 발생할 수 있습니다.

ResourceError: managedclustersetbindings.cluster.open-cluster-management.io "<cluster-set>" is forbidden: User "<user>" cannot create/delete resource "managedclustersetbindings" in

API group "cluster.open-cluster-management.io".

이 문제를 해결하려면 바인딩하려는 네임스페이스에서 ManagedClusterSetBinding 리소스를 생성하거나 삭제할 수 있는 권한도 있어야 합니다. 역할 바인딩을 사용하면 클러스터 세트를 네임스페이스로 바인딩할 수 있습니다.

1.3.3.4. 호스팅된 컨트롤 플레인 클러스터를 프로비저닝한 후 수평 스크롤이 작동하지 않음

호스팅된 컨트롤 플레인 클러스터를 프로비저닝한 후 ClusterVersionUpgradeable 매개변수가 너무 길면 Red Hat Advanced Cluster Management 콘솔의 클러스터 개요에서 수평으로 스크롤하지 못할 수 있습니다. 결과적으로 숨겨진 데이터를 볼 수 없습니다.

이 문제를 해결하려면 브라우저 확대 컨트롤을 사용하여 축소하거나, Red Hat Advanced Cluster Management 콘솔 창을 늘리거나, 텍스트를 복사하여 다른 위치에 붙여넣습니다.

1.3.3.5. *EditApplicationSet* 확장 기능 반복

여러 레이블 표현식을 추가하거나 ApplicationSet 에 대한 클러스터 선택기를 입력하려고 하면 다음 메시지가 반복적으로 표시될 수 있습니다. "Expand to enter expression". 이 문제에도 클러스터 선택을 입력할 수 있습니다.

1.3.4. 애플리케이션 알려진 문제 및 제한 사항

애플리케이션 관리의 알려진 문제를 검토합니다. 다음 목록에는 이 릴리스에 대한 알려진 문제 또는 이전 릴리스에서 계속되는 알려진 문제가 포함되어 있습니다.

Red Hat OpenShift Container Platform 클러스터의 경우 OpenShift Container Platform 알려진 문제를 참조하십시오.

사용 중단 및 제거에 대한 자세한 내용은 사용 중단 및 제거를 참조하십시오.

애플리케이션 라이프사이클 구성 요소의 알려진 문제는 다음과 같습니다.

1.3.4.1. 서브스크립션 배포 OpenShift Container Platform 3.11의 애플리케이션 토폴로지 오류

참고: Red Hat Advanced Cluster Management 지원 (OpenShift Container Platform 3.11은 더 이상 사용되지 않음)

OpenShift Container Platform 3.11 클러스터를 대상으로 하는 서브스크립션 애플리케이션을 생성하면 **Kubernetes**의 결함으로 인해 애플리케이션 토폴로지가 **ReplicaSet** 및 **Pod** 리소스에 대해 잘못 표시됩니다. 이 결함은 **pod-template-hash** 가 **ReplicaSet** 또는 **Pod** 리소스 이름의 해시와 일치하지 않는 위치입니다. 이후 **Kubernetes** 버전이 수정되었지만 **OpenShift Container Platform 3.11**은 수정되지 않습니다. 자세한 내용은 **Kubernetes** 버그 참조를 참조하십시오.

이 버그로 인해 토폴로지가 리소스 상태를 반영하지 않을 수 있습니다. 예를 들어 **Pod** 및 **replicaset** 은 반영되지 않지만 해당 리소스가 있습니다.

- **Pod** 에 대한 다음 관리 클러스터 명령 및 출력을 참조하십시오.

```
oc get pod -n test-helloworld
```

```
NAME                                READY   STATUS    RESTARTS   AGE
helloworld-app-deploy-596765ff66-ndrv8   1/1     Running   0          20m
```

- **replicaset** 은 다음 관리 클러스터 명령 및 출력을 참조하십시오.

```
oc get replicaset -n test-helloworld
```

```
NAME                          DESIRED   CURRENT   READY   AGE
helloworld-app-deploy-596765ff66   1         1         1       20m
```

1.3.4.2. OpenShift Container Platform 3.11 관리 클러스터에 대한 애플리케이션 Kubernetes Lease API 누락

애플리케이션 애드온 구성 요소는 **OpenShift Container Platform 3.11** 사용자에게 누락된 ***Kubernetes Lease API*** ,**leases.coordination.k8s.io** 를 사용합니다. **Kubernetes Lease API**는 **Kubernetes 1.14**에서 도입되었지만 **OpenShift Container Platform 3.11** 번들의 **Kubernetes** 버전 **1.11** 입니다.

이 문제를 해결하려면 다음 **Kubernetes Lease API CustomResourceDefinition** 을 **OpenShift Container Platform 3.11** 관리형 클러스터에 수동으로 적용합니다.

```
apiVersion: apiextensions.k8s.io/v1beta1
kind: CustomResourceDefinition
metadata:
  name: leases.coordination.k8s.io
spec:
  group: coordination.k8s.io
```

```
  names:
    kind: Lease
    listKind: LeaseList
    plural: leases
    singular: lease
    shortNames:
    - ls
  scope: Namespaced
  versions:
  - name: v1
    served: true    storage: true    schema:
      openAPIV3Schema:
        description: Lease defines a lease concept.
        type: object
        properties:
          apiVersion:
            type: string
          kind:
            type: string
          metadata:
            type: object
          spec:
            type: object
            properties:
              acquireTime:
                format: date-time
                type: string
              holderIdentity:
                type: string
              leaseDurationSeconds:
                format: int64
                type: integer
              leaseTransitions:
                format: int64
                type: integer
              renewTime:
                format: date-time
                type: string
            required:
            - holderIdentity
            - leaseDurationSeconds
            - renewTime
        required:
        - kind
        - metadata
        - spec
  additionalPrinterColumns:
  - JSONPath: .metadata.creationTimestamp
    name: Age
    type: date
  subresources:
    status: {}
```

참고: Red Hat Advanced Cluster Management 지원 (OpenShift Container Platform 3.11은 더 이상 사용되지 않음)

1.3.4.3. 서비스 계정에 자동 보안이 없습니다

Red Hat OpenShift Container Platform 4.15에서 **IBM VMware** 및 **Bare Metal**과 같은 일부 클라우드 공급자가 프로비저닝한 서비스 계정을 생성하면 계정이 자동으로 시크릿을 생성하지 않습니다. 따라서 **Red Hat Advanced Cluster Management gitopsCluster** 컨트롤러가 **Argo CD** 푸시 모델에 대한 관리 클러스터 시크릿을 생성하지 못합니다.

이 문제는 **AWS**에서 프로비저닝한 **Red Hat OpenShift Container Platform 4.15**에서는 발생하지 않습니다. 그러나 다른 클라우드 공급자가 프로비저닝한 **Red Hat OpenShift Container Platform 4.15**에서 문제가 발생할 수 있습니다. 이 문제는 **Red Hat Advanced Cluster Management 2.10.3** 및 **Red Hat Advanced Cluster Management 2.9.4**에서 제공됩니다.

이 문제를 해결하려면 시크릿을 수동으로 생성하여 서비스 계정 **open-cluster-management-agent-addon/application-manager** 에 연결해야 합니다. 이렇게 하려면 다음 단계를 완료합니다.

1. 관리 클러스터에 로그인합니다.
2. 다음 시크릿 템플릿을 실행하여 시크릿을 생성합니다.

```
apiVersion: v1
kind: Secret
metadata:
  name: application-manager-dockercfg
  namespace: open-cluster-management-agent-addon
  annotations:
    kubernetes.io/service-account.name: application-manager
    openshift.io/token-secret.name: application-manager-dockercfg
    openshift.io/token-secret.value: application-manager-dockercfg
type: kubernetes.io/service-account-token
```

3. 다음 명령을 실행하여 생성된 시크릿에서 토큰을 검색합니다.

```
% oc get secrets -n open-cluster-management-agent-addon application-manager-
dockercfg -o yaml
data:
  token: <token1>
```

4. 다음 명령을 실행하여 **data.token** 을 디코딩합니다.

```
echo <token1 copied from data.token> |base64 -d
```

5. 다음 명령을 실행하여 생성된 시크릿 주석으로 토큰을 업데이트합니다.

```
% oc edit secrets -n open-cluster-management-agent-addon application-manager-
dockercfg
metadata:
 annotations:
  openshift.io/token-secret.value: <paste the decoded token>
```

6. 다음 명령을 실행하여 수정된 시크릿을 서비스 계정에 연결합니다.

```
% oc edit sa -n open-cluster-management-agent-addon application-manager
....
secrets:
- name: application-manager-dockercfg
```

보안을 성공적으로 생성하고 서비스 계정에 연결했는지 확인하려면 다음 단계를 완료합니다.

1. **hub** 클러스터의 클러스터 네임스페이스로 이동합니다.

2. 다음 명령을 실행하여 클러스터 시크릿이 생성되었는지 확인합니다.

```
% oc get secrets -n perf5 perf5-cluster-secret
NAME                TYPE    DATA   AGE
perf5-cluster-secret   Opaque   3     7m40s
```

1.3.4.4. *PlacementRule* 을 사용하여 서브스크립션 애플리케이션을 편집해도 편집기에 서브스크립션 YAML이 표시되지 않습니다.

PlacementRule 리소스를 참조하는 서브스크립션 애플리케이션을 생성하면 서브스크립션 **YAML**이 콘솔의 **YAML** 편집기에 표시되지 않습니다. 터미널을 사용하여 서브스크립션 **YAML** 파일을 편집합니다.

1.3.4.5. 시크릿 종속 항목이 있는 Helm 차트는 Red Hat Advanced Cluster Management 서브스크립션을 통해 배포할 수 없습니다

Helm 차트를 사용하여 **Kubernetes** 보안에 개인 정보 데이터를 정의하고 **Helm** 차트의 **value.yaml** 파일 내에서 이 시크릿을 참조할 수 있습니다.

사용자 이름과 암호는 참조된 **Kubernetes** 시크릿 리소스 **dbsecret** 에서 제공합니다. 예를 들어 다음 샘플 **value.yaml** 파일을 참조하십시오.

```
credentials:
  secretName: dbsecret
  usernameSecretKey: username
  passwordSecretKey: password
```

보안 종속 항목이 있는 **Helm** 차트는 **Helm** 바이너리 **CLI**에서만 지원됩니다. **Operator SDK Helm** 라이브러리에서는 지원되지 않습니다. **Red Hat Advanced Cluster Management** 서브스크립션 컨트롤러는 **Operator SDK Helm** 라이브러리를 적용하여 **Helm** 차트를 설치하고 업그레이드합니다. 따라서 **Red Hat Advanced Cluster Management** 서브스크립션은 시크릿 종속성을 사용하여 **Helm** 차트를 배포할 수 없습니다.

1.3.4.6. Argo CD 푸시 모델의 클러스터 시크릿 생성은 지원되지 않습니다.

OpenShift Container Platform 3.11 관리 클러스터의 **Argo CD Push** 모델에 대해 사용자 지정 클러스터 시크릿을 생성할 수 없습니다. 이는 **OpenShift Container Platform 3.11** 관리 클러스터에서 관리 서비스 계정 애드온이 지원되지 않기 때문에 발생합니다.

1.3.4.7. Argo CD pull model ApplicationSet 애플리케이션에 대해 토폴로지가 올바르게 표시되지 않음

Argo CD 가져오기 모델을 사용하여 **ApplicationSet** 애플리케이션을 배포하고 애플리케이션 리소스 이름이 사용자 지정되면 각 클러스터에 따라 리소스 이름이 다르게 표시될 수 있습니다. 이 경우 토폴로지에서 애플리케이션을 올바르게 표시하지 않습니다.

1.3.4.8. 로컬 클러스터는 가져오기 모델을 위한 관리형 클러스터로 제외됨

허브 클러스터 애플리케이션 세트는 대상 관리 클러스터에 배포되지만 관리 허브 클러스터인 로컬 클러스터는 대상 관리 클러스터로 제외됩니다.

결과적으로 **Argo CD** 애플리케이션이 **Argo CD** 풀 모델을 통해 로컬 클러스터에 전파되면 로컬 클러스터 **Argo CD** 애플리케이션이 **Argo CD ApplicationSet** 리소스의 배치 결정에서 제거되더라도 로컬 클러스터 **Argo CD** 애플리케이션이 정리되지 않습니다.

이 문제를 해결하고 로컬 클러스터 **Argo CD** 애플리케이션을 정리하려면 로컬 클러스터 **Argo CD** 애플리케이션에서 **skip-reconcile** 주석을 제거합니다. 다음 주석을 참조하십시오.

```
annotations:
   argocd.argoproj.io/skip-reconcile: "true"
```

또한 Argo CD 콘솔의 애플리케이션 섹션에서 가져오기 모델 Argo CD 애플리케이션을 수동으로 새로 고침하면 새로 고침이 처리되지 않으며 Argo CD 콘솔의 REFRESH 버튼이 비활성화됩니다.

이 문제를 해결하려면 Argo CD 애플리케이션에서 새로 고침 주석을 제거합니다. 다음 주석을 참조하십시오.

```
annotations:
  argocd.argoproj.io/refresh: normal
```

1.3.4.9. Argo CD 컨트롤러 및 전파 컨트롤러가 동시에 조정될 수 있습니다.

Argo CD 컨트롤러와 전파 컨트롤러는 모두 동일한 애플리케이션 리소스에서 조정할 수 있으며 관리형 클러스터에서 애플리케이션 배포 인스턴스가 중복되지만 다른 배포 모델에서 발생할 수 있습니다.

가져오기 모델을 사용하여 애플리케이션을 배포하기 위해 Argo CD 컨트롤러는 Argo CD argocd.argoproj.io/skip-reconcile 주석이 ApplicationSet 의 template 섹션에 추가되면 Argo CD 컨트롤러에서 이러한 애플리케이션 리소스를 무시합니다.

argocd.argoproj.io/skip-reconcile 주석은 GitOps Operator 버전 1.9.0 이상에서만 사용할 수 있습니다. 충돌을 방지하려면 허브 클러스터 및 모든 관리 클러스터가 가져오기 모델을 구현하기 전에 GitOps Operator 버전 1.9.0으로 업그레이드할 때까지 기다립니다.

1.3.4.10. 리소스가 배포되지 않음

MulticlusterApplicationSetReport 에 나열된 모든 리소스는 실제로 관리 클러스터에 배포됩니다. 리소스를 배포하지 못하면 리소스가 리소스 목록에 포함되지 않지만 원인은 오류 메시지에 나열됩니다.

1.3.4.11. 리소스 할당에 몇 분이 걸릴 수 있습니다.

수백 개의 관리형 클러스터에 배포된 관리 클러스터 및 Argo CD 애플리케이션 세트가 있는 대규모 환경의 경우 허브 클러스터에서 Argo CD 애플리케이션 생성에 몇 분이 걸릴 수 있습니다. 다음 예제 파일에 표시되므로 애플리케이션 세트의 clusterDecisionResource 생성기에서 requeueAfterSeconds 를 0 으로 설정할 수 있습니다.

```
apiVersion: argoproj.io/v1alpha1
kind: ApplicationSet
metadata:
  name: cm-allclusters-app-set
  namespace: openshift-gitops
spec:
```

```
generators:
- clusterDecisionResource:
    configMapRef: ocm-placement-generator
    labelSelector:
      matchLabels:
        cluster.open-cluster-management.io/placement: app-placement
    requeueAfterSeconds: 0
```

1.3.4.12. 애플리케이션 ObjectBucket 채널 유형에서 허용 및 거부 목록을 사용할 수 없습니다

subscription-admin 역할에 **ObjectBucket** 채널 유형의 허용 및 거부 목록을 지정할 수 없습니다. 다른 채널 유형에서 서브스크립션의 허용 및 거부 목록은 배포할 수 있는 **Kubernetes** 리소스와 배포해서는 안 되는 **Kubernetes** 리소스를 나타냅니다.

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

Infrastructure.config.openshift.io API는 **3.x**에서 사용할 수 없으므로 콘솔의 **Argo ApplicationSet**은 **3.x OpenShift Container Platform** 관리 클러스터에 배포할 수 없습니다.

1.3.4.13. multicluster_operators_subscription 이미지에 대한 변경 사항은 자동으로 적용되지 않습니다.

관리 클러스터에서 실행 중인 **application-manager** 애드온은 이전에 **klusterlet Operator**가 처리한 경우 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.

multicluster-hub 이미지 매니페스트 **ConfigMap**에서 **multicluster_operators_subscription** 이미지를 변경하여 서브스크립션 **Operator**에서 사용하는 이미지를 재정의하는 경우 관리 클러스터의 **application-manager** 애드온은 서브스크립션 **Operator pod**가 다시 시작될 때까지 새 이미지를 사용하지 않습니다. **Pod**를 다시 시작해야 합니다.

1.3.4.14. 서브스크립션 관리자가 배포하지 않는 한 정책 리소스가 배포되지 않음

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

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

자세한 내용은 서브스크립션 관리자로서 허용 및 거부 목록 생성 을 참조하십시오. 이전 **Red Hat**

Advanced Cluster Management 버전에서 기존 애플리케이션 서브스크립션에 의해 배포된 policy.open-cluster-management.io/v1 리소스는 서브스크립션 관리자가 애플리케이션 서브스크립션을 배포하지 않는 한 소스 리포지토리와 더 이상 조정되지 않습니다.

1.3.4.15. 애플리케이션 Ansible 후크 독립 실행형 모드

Ansible 후크 독립 실행형 모드는 지원되지 않습니다. 서브스크립션과 함께 허브 클러스터에 Ansible 후크를 배포하려면 다음 서브스크립션 YAML을 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 실행되는 서브스크립션이 있으므로 이 구성은 Ansible 인스턴스를 생성하지 않을 수 있습니다. 허브 모드에서 서브스크립션을 생성해야 합니다.

1. local-cluster 에 배포하는 배치 규칙을 생성합니다. local-cluster: "true" 가 허브 클러스터를 참조하는 다음 샘플을 참조하십시오.

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

2. 서브스크립션의 배치 규칙을 참조합니다. 다음 샘플을 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 적용하면 **hub** 클러스터에 생성된 **Ansible** 인스턴스가 표시됩니다.

1.3.4.16. 업데이트된 배치 규칙 후 애플리케이션이 배포되지 않음

배치 규칙을 업데이트한 후 애플리케이션이 배포되지 않은 경우 **application-manager** 포드가 실행 중인지 확인합니다. **application-manager** 는 관리 클러스터에서 실행해야 하는 서브스크립션 컨테이너입니다.

oc get pods -n open-cluster-management-agent-addon |grep application-manager 를 실행하여 확인할 수 있습니다.

콘솔에서 **kind:pod cluster:yourcluster** 를 검색하고 **application-manager** 가 실행 중인지 확인할 수도 있습니다.

확인할 수 없는 경우 클러스터를 다시 가져오고 다시 확인합니다.

1.3.4.17. 서브스크립션 Operator에서 SCC를 생성하지 않음

관리형 클러스터에 필요한 추가 구성인 **SCC(보안 컨텍스트 제약 조건)** 관리에서 **Red Hat OpenShift Container Platform SCC**에 대해 알아봅니다.

배포마다 보안 컨텍스트와 서비스 계정이 다릅니다. 서브스크립션 **Operator**는 **SCC CR**을 자동으로 생성할 수 없습니다. 관리자는 **Pod**에 대한 권한을 제어합니다. 상대 서비스 계정에 적절한 권한을 활성화하려면 기본이 아닌 네임스페이스에서 **Pod**를 생성하려면 **SCC(보안 컨텍스트 제약 조건) CR**이 필요합니다. 네임스페이스에서 **SCC CR**을 수동으로 생성하려면 다음 단계를 완료합니다.

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

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

2. 네임스페이스에 **SCC CR**을 생성하여 서비스 계정 또는 계정에 필요한 권한을 할당합니다. **kind: SecurityContextConstraints** 가 추가된 예제는 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
```

1.3.4.18. 애플리케이션 채널에는 고유한 네임스페이스가 필요합니다.

동일한 네임스페이스에 두 개 이상의 채널을 생성하면 **hub** 클러스터에 오류가 발생할 수 있습니다.

예를 들어, 네임스페이스 **charts-v1** 은 설치 프로그램에서 **Helm** 유형 채널로 사용하므로 **charts-v1** 에 추가 채널을 생성하지 마십시오. 고유한 네임스페이스에 채널을 생성해야 합니다. 모든 채널에는 다른 **GitHub** 채널과 네임스페이스를 공유할 수 있는 **GitHub** 채널을 제외한 개별 네임스페이스가 필요합니다.

1.3.4.19. Ansible Automation Platform 작업 실패

호환되지 않는 옵션을 선택할 때 **Ansible** 작업이 실행되지 않습니다. **Ansible Automation Platform** 은 **-cluster** 범위의 채널 옵션이 선택된 경우에만 작동합니다. 이는 **Ansible** 작업을 수행해야 하는 모든 구성 요소에 영향을 미칩니다.

1.3.4.20. Ansible Automation Platform Operator가 프록시 외부에서 Ansible Automation Platform에 액세스

Red Hat Ansible Automation Platform Operator는 프록시 지원 **OpenShift Container Platform** 클러스터 외부에서 **Ansible Automation Platform**에 액세스할 수 없습니다. 해결하려면 프록시에 **Ansible**

Automation Platform을 설치할 수 있습니다. **Ansible Automation Platform**에서 제공하는 설치 단계를 참조하십시오.

1.3.4.21. 애플리케이션 이름 요구사항

애플리케이션 이름은 **37**자를 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'
```

1.3.4.22. 애플리케이션 콘솔 테이블 제한 사항

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

- *개요* 페이지의 *애플리케이션* 표와 *고급 구성* 페이지의 *서브스크립션* 표에서 ***Clusters*** 열에 애플리케이션 리소스가 배포되는 클러스터 수가 표시됩니다. 애플리케이션은 로컬 클러스터의 리소스로 정의되므로 실제 애플리케이션 리소스가 로컬 클러스터에 배포되었는지 여부에 관계없이 로컬 클러스터는 검색 결과에 포함됩니다.
- *서브스크립션 고급 구성* 표의 애플리케이션 *열에* 는 해당 서브스크립션을 사용하는 총 애플리케이션 수가 표시되지만 서브스크립션이 하위 애플리케이션을 배포하는 경우 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.

1.3.4.23. 애플리케이션 콘솔 토폴로지 필터링 없음

2.10에 대한 *애플리케이션* 변경에 대한 *콘솔* 및 *토폴로지*. 콘솔 토폴로지 페이지의 필터링 기능은 없습니다.

1.3.4.24. 오브젝트 스토리지 애플리케이션에서 허용 및 거부 목록이 작동하지 않음

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

1.3.5. 관찰 가능성 알려진 문제

Red Hat Advanced Cluster Management for Kubernetes의 알려진 문제를 검토합니다. 다음 목록에는 이 릴리스에 대한 알려진 문제 또는 이전 릴리스에서 계속되는 알려진 문제가 포함되어 있습니다.

Red Hat OpenShift Container Platform 클러스터의 경우 OpenShift Container Platform 알려진 문제를 참조하십시오.

사용 중단 및 제거에 대한 자세한 내용은 사용 중단 및 제거를 참조하십시오.

1.3.5.1. 구성 기본값

MultiClusterObservability 는 이전 버전의 Cluster Monitoring Operator를 사용합니다. 이전 버전에서는 cluster-monitoring-config 구성 맵이 관찰 기능 내의 다른 구성으로 업데이트되지 않도록 합니다. 그런 다음 구성이 기본값으로 재설정됩니다.

1.3.5.2. 복원된 허브 클러스터의 Observatorium API 게이트웨이 Pod에 오래된 테넌트 데이터가 있을 수 있습니다.

복원된 허브 클러스터의 Observatorium API 게이트웨이 Pod에는 Kubernetes 제한으로 인해 백업 후 오래된 테넌트 데이터가 포함될 수 있습니다. 제한에 대한 자세한 내용은 마운트된 ConfigMaps가 자동으로 업데이트 되는 것을 참조하십시오.

결과적으로 Observatorium API 및 Thanos 게이트웨이는 수집기에서 메트릭을 거부하고 Red Hat Advanced Cluster Management Grafana 대시보드는 데이터를 표시하지 않습니다.

Observatorium API 게이트웨이 Pod 로그에서 다음 오류를 참조하십시오.

```
level=error name=observatorium caller=logchannel.go:129 msg="failed to forward metrics"
returncode="500 Internal Server Error" response="no matching hashring to handle tenant\n"
```

Thanos는 다음 오류와 함께 Pod 로그를 수신합니다.

```
caller=handler.go:551 level=error component=receive component=receive-handler tenant=xxxx
err="no matching hashring to handle tenant" msg="internal server error"
```

이 문제를 해결하려면 다음 절차를 참조하십시오.

1. **observability-observatorium-api** 배포 인스턴스를 **N** 에서 **0** 으로 축소합니다.

2. **observability-observatorium-api** 배포 인스턴스를 **0** 에서 **N** 으로 확장합니다.

참고: 기본적으로 **N = 2** 이지만 일부 사용자 지정 구성 환경에서는 **2** 보다 클 수 있습니다.

이렇게 하면 올바른 테넌트 정보를 사용하여 모든 **Observatorium API** 게이트웨이 **Pod**가 다시 시작되고 수집기의 데이터가 **5-10**분 내에 **Grafana**에 표시되기 시작합니다.

1.3.5.3. *openshift-monitoring* 네임스페이스에서 *PrometheusRules* 및 *ServiceMonitor* 를 추가할 수 있는 권한

Red Hat Advanced Cluster Management 2.9부터는 정의된 **Red Hat Advanced Cluster Management Hub** 클러스터 네임스페이스에 라벨을 사용해야 합니다. 레이블 **openshift.io/cluster-monitoring: "true"** 로 인해 **Cluster Monitoring Operator**가 메트릭의 네임스페이스를 스크랩합니다.

Red Hat Advanced Cluster Management 2.9가 배포되거나 설치가 **2.9**로 업그레이드되면 **Red Hat Advanced Cluster Management Observability ServiceMonitor** 및 **PrometheusRule** 리소스가 더 이상 **openshift-monitoring** 네임스페이스에 표시되지 않습니다.

1.3.5.4. 프록시 설정 지원 부족

observability 애드온의 **additional AlertManagerConfig** 리소스는 프록시 설정을 지원하지 않습니다. 관찰 기능 경고 전달 기능을 비활성화해야 합니다.

경고 전달을 비활성화하려면 다음 단계를 완료합니다.

1. **MultiClusterObservability** 리소스로 이동합니다.

2. **mco-disabling-alerting** 매개변수 값을 **true**로 업데이트합니다.

자체 서명된 **CA** 인증서가 있는 **HTTPS** 프록시는 지원되지 않습니다.

1.3.5.5. 서비스 수준 개요 대시보드에서 로컬 클러스터 중복

다양한 허브 클러스터에서 동일한 S3 스토리지를 사용하여 Red Hat Advanced Cluster Management 관찰 기능을 배포할 때 *Kubernetes/Service -Level Overview/API Server 대시보드 내에서 중복 로컬 클러스터*를 감지하고 표시할 수 있습니다. 중복 클러스터는 다음 패널의 결과에 영향을 미칩니다. *상위 클러스터*,*SLO*를 *초과한 클러스터 수*, *SLO*를 *충족하는* 클러스터 수 local-cluster는 공유 S3 스토리지와 연결된 고유한 클러스터입니다. 여러 로컬 클러스터 가 대시보드 내에 표시되지 않도록 하려면 각 고유한 허브 클러스터가 허브 클러스터에 특별히 S3 버킷을 사용하여 관찰 기능을 배포하는 것이 좋습니다.

1.3.5.6. 관찰 기능 끝점 Operator가 이미지를 가져오지 못했습니다

MultiClusterObservability CustomResource(CR)에 배포할 풀 시크릿을 생성하고 open-cluster-management-observability 네임스페이스에 pull-secret이 없는 경우 observability 엔드포인트 Operator가 실패합니다. 새 클러스터를 가져오거나 Red Hat Advanced Cluster Management를 사용하여 생성된 Hive 클러스터를 가져오는 경우 관리 클러스터에서 풀 이미지 시크릿을 수동으로 생성해야 합니다.

자세한 내용은 관찰 기능 활성화를 참조하십시오.

1.3.5.7. ROKS 클러스터의 데이터가 없습니다

Red Hat Advanced Cluster Management observability는 기본 제공 대시보드 내의 일부 패널에 있는 ROKS 클러스터의 데이터를 표시하지 않습니다. 이는 ROKS가 관리하는 서버에서 API 서버 메트릭을 노출하지 않기 때문입니다. 다음 Grafana 대시보드에는 ROKS 클러스터를 지원하지 않는 패널이 포함되어 있습니다. Kubernetes/API 서버,Kubernetes/Compute Resources/Workload,Kubernetes/Compute Resources/Namespace(Workload)

1.3.5.8. ROKS 클러스터에서 etcd 데이터가 없습니다

ROKS 클러스터의 경우 Red Hat Advanced Cluster Management observability는 대시보드의 *etcd* 패널에 데이터를 표시하지 않습니다.

1.3.5.9. 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 새로고침하고 **hub** 클러스터에 로그인되어 있는지 확인합니다.

- ***rbac-query-proxy* Pod**에서 오류가 발생했습니다.

managedcluster 리소스에 대한 무단 액세스로 인해 클러스터 또는 프로젝트를 쿼리할 때 다음 오류가 발생할 수 있습니다.

프로젝트 또는 클러스터를 찾을 수 없음

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

1.3.5.10. 관리 클러스터에서 Prometheus 데이터 손실

기본적으로 **OpenShift**의 **Prometheus**는 임시 스토리지를 사용합니다. **Prometheus**는 재시작할 때마다 모든 메트릭 데이터를 손실됩니다.

Red Hat Advanced Cluster Management에서 관리하는 **OpenShift Container Platform** 관리 클러스터에서 관찰 기능이 활성화되거나 비활성화되면 **observability** 엔드포인트 **Operator**는 로컬 **Prometheus**를 자동으로 재시작하는 **alertmanager** 구성을 추가하여 **cluster-monitoring-config ConfigMap** 을 업데이트합니다.

1.3.5.11. 주문 외부 샘플을 수집하는 동안 오류 발생

관찰 기능 수신 **Pod**는 다음 오류 메시지를 보고합니다.

> Error on ingesting out-of-order samples

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

문제는 시계열 간격이 30초와 같은 더 낮은 값으로 설정된 경우에만 발견됩니다. 이 문제는 메트릭 컬렉션 간격이 기본값인 300초로 설정된 경우 표시되지 않습니다.

1.3.5.12. 업그레이드 후 Grafana 배포 실패

이전 버전의 2.6에서 배포한 grafana-dev 인스턴스가 있고 환경을 2.6로 업그레이드하는 경우 grafana-dev 가 작동하지 않습니다. 다음 명령을 실행하여 기존 grafana-dev 인스턴스를 삭제해야 합니다.

```
./setup-grafana-dev.sh --clean
```

다음 명령을 사용하여 인스턴스를 다시 생성합니다.

```
./setup-grafana-dev.sh --deploy
```

1.3.5.13. *klusterlet-addon-search* Pod 실패

메모리 제한에 도달하여 klusterlet-addon-search Pod가 실패합니다. 관리 클러스터에서 klusterlet-addon-search 배포를 사용자 정의하여 메모리 요청 및 제한을 업데이트해야 합니다. hub 클러스터에서 search-collector 라는 ManagedclusterAddon 사용자 정의 리소스를 편집합니다. search-collector 에 다음 주석을 추가하고 addon.open-cluster-management.io/search_memory_request=512Mi 및 addon.open-cluster-management.io/search_memory_limit=1024Mi 를 업데이트합니다.

예를 들어 foobar 라는 관리 클러스터가 있는 경우 다음 명령을 실행하여 메모리 요청을 512Mi 로 변경하고 메모리 제한을 1024Mi 로 변경합니다.

```
oc annotate managedclusteraddon search-collector -n foobar \
addon.open-cluster-management.io/search_memory_request=512Mi \
addon.open-cluster-management.io/search_memory_limit=1024Mi
```

1.3.5.14. *disableHubSelfManagement* 를 활성화하면 Grafana 대시보드의 빈 목록

mulitclusterengine 사용자 정의 리소스에서 disableHubSelfManagement 매개변수가 true 로 설정된 경우 Grafana 대시보드에 빈 레이블 목록이 표시됩니다. 레이블 목록을 보려면 매개변수를 false 로 설정하거나 매개변수를 제거해야 합니다. 자세한 내용은 disableHubSelfManagement 를 참조하십시오.

1.3.5.14.1. 엔드포인트 URL에는 FQDN(정규화된 도메인 이름)이 있을 수 없습니다.

endpoint 매개변수에 FQDN 또는 프로토콜을 사용하면 관찰 기능 Pod가 활성화되지 않습니다. 다음과 같은 오류 메시지가 표시됩니다.

Endpoint url cannot have fully qualified paths

프로토콜 없이 **URL**을 입력합니다. 끝점 값은 보안에 대해 다음 **URL**과 유사해야 합니다.

endpoint: example.com:443

1.3.5.14.2. Grafana 다운 샘플링 데이터 불일치

이전 데이터를 쿼리하려고 하면 계산된 단계 값과 다운샘플링된 데이터 사이에 불일치가 있으면 결과가 비어 있습니다. 예를 들어 계산된 단계 값이 **5m** 이고 다운샘플링된 데이터가 **1**시간 간격인 경우 **Grafana**에서 데이터가 표시되지 않습니다.

이 불일치는 **URL** 쿼리 매개변수가 **Thanos** 쿼리 프런트 엔드 데이터 소스를 통해 전달되어야 하기 때문에 발생합니다. 이후 데이터가 누락될 때 **URL** 쿼리는 다른 다운스트림 수준에 대한 추가 쿼리를 수행할 수 있습니다.

Thanos Query 프런트 엔드 데이터 소스 구성을 수동으로 업데이트해야 합니다. 다음 단계를 완료합니다.

1. 쿼리 프런트 엔드 데이터 소스로 이동합니다.
2. 쿼리 매개변수를 업데이트하려면 ***Misc*** 섹션을 클릭합니다.
3. *사용자 정의 쿼리 매개변수* 필드에서 **max_source_resolution=auto** 를 선택합니다.
4. 데이터가 표시되는지 확인하려면 **Grafana** 페이지를 새로 고칩니다.

쿼리 데이터는 **Grafana** 대시보드에서 표시됩니다.

1.3.5.15. 메트릭 수집기에서 프록시 구성을 감지하지 않음

addonDeploymentConfig 를 사용하여 구성한 관리 클러스터의 프록시 구성은 메트릭 수집기에서 탐지되지 않습니다. 이 문제를 해결하려면 관리 클러스터 **ManifestWork** 를 제거하여 프록시를 활성화할 수 있습니다. **ManifestWork** 를 제거하면 **addonDeploymentConfig** 의 변경 사항을 적용해야 합니다.

1.3.5.16. 사용자 정의 CA 번들이 있는 HTTPS 프록시는 지원되지 않습니다.

사용자 정의 CA 번들이 필요한 경우 관리 클러스터의 프록시 구성이 작동하지 않습니다.

1.3.6. 거버넌스 알려진 문제

Governance의 알려진 문제를 검토합니다. 다음 목록에는 이 릴리스에 대한 알려진 문제 또는 이전 릴리스에서 계속되는 알려진 문제가 포함되어 있습니다.

Red Hat OpenShift Container Platform 클러스터의 경우 OpenShift Container Platform 알려진 문제를 참조하십시오.

사용 중단 및 제거에 대한 자세한 내용은 사용 중단 및 제거를 참조하십시오.

1.3.6.1. OpenShift Container Platform 3.11에서는 컨테이너 보안 Operator를 사용할 수 없습니다.

OpenShift Container Platform 3.11에서는 컨테이너 보안 Operator를 사용할 수 없습니다. 따라서 ImageManifestVuln 정책 정책에서 policy-imagemanifestvuln-sub 의 정책 템플릿을 사용하여 OpenShift Container Platform 3.11 클러스터에 적용할 수 없습니다.

ImageManifestVuln 정책을 적용하려고 하면 다음 위반 메시지가 표시됩니다.

> violation - couldn't find mapping resource with kind Subscription, please check if you have CRD deployed.

1.3.6.2. 구성 요소가 비활성화되면 거버넌스 리소스가 제대로 정리되지 않음

거버넌스 리소스가 제대로 정리되지 않습니다. 구성 요소가 false 로 설정되거나 MultiClusterHub Operator에서 비활성화되면 거버넌스 구성 요소가 제거되어 관리하는 추가 기능을 정리할 수 있습니다.

1.3.6.3. Red Hat Advanced Cluster Management에서 로그아웃할 수 없음

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

Red Hat Advanced Cluster Management에서 로그아웃하기 전에 외부 ID 공급자에서 로그아웃해야

합니다.

1.3.6.4. 네임스페이스가 *Terminating* 상태인 경우 구성 정책의 불만 사항

complianceType 매개변수에 대해 **mustnothave** 를 사용하여 구성된 구성 정책이 있고 **remediationAction** 매개변수에 대한 적용이 **Kubernetes API**에 대한 삭제 요청이 수행될 때 정책을 준수하도록 나열됩니다. 따라서 정책이 준수로 나열되는 동안 **Kubernetes** 오브젝트는 **Terminating** 상태로 고정될 수 있습니다.

1.3.6.5. 정책과 함께 배포된 Operator는 ARM을 지원하지 않습니다.

ARM 환경에 설치할 수 있지만 정책과 함께 배포된 **Operator**는 **ARM** 환경을 지원하지 않을 수 있습니다. **Operator**를 설치하는 다음 정책은 **ARM** 환경을 지원하지 않습니다.

- Quay Container Security Operator를 위한 Red Hat Advanced Cluster Management 정책
- Compliance Operator를 위한 Red Hat Advanced Cluster Management 정책

1.3.6.6. ConfigurationPolicy 사용자 정의 리소스 정의는 종료 중 상태로 유지됨

KlusterletAddonConfig 에서 정책 컨트롤러를 비활성화하거나 클러스터를 분리하여 관리 클러스터에서 **config-policy-controller** 애드온을 제거하면 **ConfigurationPolicy** 사용자 정의 리소스 정의가 종료 상태가 될 수 있습니다. **ConfigurationPolicy** 사용자 정의 리소스 정의가 종료 상태에 있는 경우 나중에 애드온을 다시 설치하는 경우 새 정책이 클러스터에 추가되지 않을 수 있습니다. 다음과 같은 오류도 표시될 수 있습니다.

```
template-error; Failed to create policy template: create not allowed while custom resource definition is terminating
```

다음 명령을 사용하여 사용자 정의 리소스 정의가 고정되었는지 확인합니다.

```
oc get crd configurationpolicies.policy.open-cluster-management.io -o=jsonpath='{.metadata.deletionTimestamp}'
```

삭제 타임스탬프가 리소스에 있으면 사용자 정의 리소스 정의가 고정됩니다. 이 문제를 해결하려면 클러스터에 남아 있는 구성 정책에서 모든 종료자를 제거합니다. 관리 클러스터에서 다음 명령을 사용하고 **< cluster-namespace >**를 관리 클러스터 네임스페이스로 바꿉니다.

```
oc get configurationpolicy -n <cluster-namespace> -o name | xargs oc patch -n <cluster-namespace>
--type=merge -p '{"metadata":{"finalizers": []}}'
```

구성 정책 리소스는 클러스터에서 자동으로 제거되고 사용자 정의 리소스 정의는 종료 상태를 종료합니다. 애드온을 이미 다시 설치한 경우 삭제 타임스탬프 없이 사용자 정의 리소스 정의가 자동으로 다시 생성됩니다.

1.3.6.7. 기존 구성 정책을 수정할 때 *pruneObjectBehavior* 가 작동하지 않음

기존 구성 정책을 수정하면 **pruneObjectBehavior** 가 작동하지 않습니다. **pruneObjectBehavior** 가 작동하지 않는 이유는 다음과 같습니다.

- 구성 정책에서 **pruneObjectBehavior** 를 **DeleteAll** 또는 **DeleteIfCreated** 로 설정하면 수정 전에 생성된 이전 리소스가 올바르게 정리되지 않습니다. 구성 정책을 삭제할 때 정책 생성 및 정책 업데이트의 새 리소스만 추적 및 삭제됩니다.

- **pruneObjectBehavior** 를 **None** 으로 설정하거나 매개변수 값을 설정하지 않으면 관리 클러스터에서 이전 오브젝트가 의도치 않게 삭제될 수 있습니다. 특히 사용자가 템플릿에서 이름,네임스페이스,종류 또는 **apiversion** 을 변경할 때 발생합니다. **object-templates-raw** 또는 **namespaceSelector** 매개변수가 변경될 때 매개변수 필드를 동적으로 변경할 수 있습니다.

1.3.6.8. 정책 상태가 적용될 때 반복된 업데이트 표시

정책이 **remediationAction: enforce and is repeatedly updated**로 설정된 경우 **Red Hat Advanced Cluster Management** 콘솔에는 성공적인 업데이트로 인해 반복된 위반이 표시됩니다. 오류에 대한 다음 두 가지 원인 및 해결 방법을 참조하십시오.

- 다른 컨트롤러 또는 프로세스는 다른 값으로 오브젝트를 업데이트하는 중입니다.

  이 문제를 해결하려면 정책을 비활성화하고 정책의 **objectDefinition** 과 관리 클러스터의 개체 간의 차이점을 비교합니다. 값이 다르면 다른 컨트롤러 또는 프로세스가 업데이트될 수 있습니다. 오브젝트의 메타데이터 를 확인하여 값이 다른 이유를 식별하는 데 도움이 됩니다.

- 정책을 적용할 때 **Kubernetes**에서 오브젝트를 처리하므로 **ConfigurationPolicy** 의 오브젝트**Definition** 이 일치하지 않습니다.

  이 문제를 해결하려면 정책을 비활성화하고 정책의 **objectDefinition** 과 관리 클러스터의 개체 간의 차이점을 비교합니다. 키가 다르거나 누락된 경우 **Kubernetes**는 기본값 또는 빈 값이 포함된 키 제거와 같이 오브젝트에 적용하기 전에 키를 처리했을 수 있습니다.

1.3.6.9. OpenShift Container Platform 4.12 이상에서 지원되지 않는 Pod 보안 정책

Pod 보안 정책 지원은 **OpenShift Container Platform 4.12** 이상 및 **Kubernetes v1.25** 이상에서 제거됩니다. **PodSecurityPolicy** 리소스를 적용하면 다음과 같은 비호환 메시지가 표시될 수 있습니다.

> violation - couldn't find mapping resource with kind PodSecurityPolicy, please check if you have CRD deployed

1.3.6.10. 중복 정책 템플릿 이름에서 불일치 결과 생성

동일한 정책 템플릿 이름으로 정책을 생성하면 탐지되지 않은 결과가 표시되지만 원인을 모를 수 있습니다. 예를 들어 **create-pod** 라는 여러 구성 정책으로 정책을 정의하면 일관되지 않은 결과가 발생합니다. 모범 사례: 정책 템플릿에 중복 이름을 사용하지 마십시오.

1.3.6.11. 비활성화된 경우 거버넌스 배포가 오류 없이 종료되지 않음

MultiClusterHub 오브젝트에서 거버넌스 배포를 비활성화하면 오류 없이 배포가 정리되지 않습니다. 배포도 정리되도록 거버넌스를 비활성화하려면 다음 단계를 완료합니다.

1. 관리 클러스터의 **KlusterletAddonConfig** 에서 **policyController** 를 비활성화합니다. 모든 관리 클러스터에 이 작업을 수행하는 경우 다음 명령을 실행합니다.

```
for CLUSTER in $(oc get managedclusters -o jsonpath='{.items[].metadata.name}'); do
  oc patch -n ${CLUSTER} klusterletaddonconfig ${CLUSTER} --type=merge --
patch='{"spec":{"policyController":{"enabled":false}}}'
done
```

2. 로컬 클러스터만 해당: 로컬 클러스터의 **ManifestWork** 를 삭제하고 로컬 클러스터의 **governance-policy-framework-uninstall Pod**가 **CrashLoopBackOff** 에 있는 경우 **ManagedClusterAddon** 에서 종료자를 제거합니다. 다음 명령을 실행합니다.

```
oc delete manifestwork -n local-cluster -l open-cluster-management.io/addon-
name=governance-policy-framework
oc patch managedclusteraddon -n local-cluster governance-policy-framework --
type=merge --patch='{"metadata":{"finalizers":[]}}'
```

3. **MultiClusterHub** 오브젝트에서 **spec.overrides** 섹션의 **grc** 요소를 **false** 로 설정하여 필요한 경우 거버넌스를 전역적으로 비활성화합니다. 다음 명령을 실행합니다.

```
oc edit multiclusterhub <name> -n <namespace>
```

4.

로컬 클러스터 전용: 로컬 클러스터 정책이 있는 경우 다음 명령을 실행하여 정책을 삭제할 수 있습니다.

```
oc delete policies -n local-cluster --all
```

5. KlusterletAddonConfig 에서 거버넌스를 다시 활성화하려면 MultiClusterHub 의 spec.overrides 섹션의 grc 요소를 다시 활성화합니다. 다음 명령을 실행합니다.

```
for CLUSTER in $(oc get managedclusters -o jsonpath='{.items[].metadata.name}'); do
  oc patch -n ${CLUSTER} klusterletaddonconfig ${CLUSTER} --type=merge --
patch='{"spec":{"policyController":{"enabled":true}}}'
done
```

6. 배포에 실패한 경우 governance-policy-addon-controller 에 오래된 리스를 가질 수 있습니다. 다음 명령을 사용하여 리스를 삭제합니다.

```
oc delete lease governance-policy-addon-controller-lock -n <namespace>
```

1.3.6.12. 데이터베이스 및 정책 준수 기록 API 중단

데이터베이스 및 정책 준수 기록 API 중단에 대한 복원력이 기본 제공되어 있지만 관리 클러스터에서 기록할 수 없는 규정 준수 이벤트는 성공적으로 기록될 때까지 메모리에 대기열에 추가됩니다. 즉, 관리 클러스터의 중단 및 governance-policy-framework Pod가 다시 시작되면 대기 중인 모든 규정 준수 이벤트가 손실됩니다.

데이터베이스 중단 중에 새 정책을 생성하거나 업데이트하는 경우 데이터베이스 ID에 대한 정책 매핑은 업데이트할 수 없으므로 이 새 정책에 대해 전송된 규정 준수 이벤트를 기록할 수 없습니다. 데이터베이스가 다시 온라인 상태가 되면 매핑이 자동으로 업데이트되고 해당 정책에서 향후 규정 준수 이벤트가 기록됩니다.

1.3.6.13. PostgreSQL 데이터 손실

최신 데이터 없이 백업 복원과 같은 PostgreSQL 서버에 데이터 손실이 있는 경우 Red Hat Advanced Cluster Management Hub 클러스터의 거버넌스 정책 전파기를 다시 시작하여 정책의 매핑을 데이터베이스 ID로 업데이트해야 합니다. 거버넌스 정책 전파를 다시 시작할 때까지 데이터베이스에 존재한 정책과 관련된 새로운 규정 준수 이벤트가 더 이상 기록되지 않습니다.

거버넌스 정책 전파기를 다시 시작하려면 Red Hat Advanced Cluster Management Hub 클러스터에서 다음 명령을 실행합니다.

```
oc -n open-cluster-management rollout restart deployment/grc-policy-propagator
```

1.3.7. 네트워킹에 대한 알려진 문제

Submariner에 대한 알려진 문제를 검토합니다. 다음 목록에는 이 릴리스에 대한 알려진 문제 또는 이전 릴리스에서 계속되는 알려진 문제가 포함되어 있습니다.

Red Hat OpenShift Container Platform 클러스터의 경우 OpenShift Container Platform 알려진 문제를 참조하십시오.

사용 중단 및 제거에 대한 자세한 내용은 사용 중단 및 제거를 참조하십시오.

1.3.7.1. Submariner 알려진 문제

네트워킹 기능을 사용하는 동안 발생할 수 있는 다음과 같은 알려진 문제 및 제한 사항을 참조하십시오.

1.3.7.1.1. *ClusterManagementAddon* submariner 애드온 없음

버전 2.8 이하의 경우 Red Hat Advanced Cluster Management를 설치할 때 Operator Lifecycle Manager와 함께 하위marine r-addon 구성 요소도 배포합니다. MultiClusterHub 사용자 정의 리소스를 생성하지 않은 경우 submariner-addon Pod에서 오류를 보내 Operator가 설치되지 않습니다.

ClusterManagementAddon 사용자 정의 리소스 정의가 누락되어 있기 때문에 다음 알림이 발생합니다.

> graceful termination failed, controllers failed with error: the server could not find the requested resource (post clustermanagementaddons.addon.open-cluster-management.io)

ClusterManagementAddon 리소스는 cluster-manager 배포에 의해 생성되지만 클러스터에 MultiClusterEngine 구성 요소가 설치되면 이 배포를 사용할 수 있습니다.

MultiClusterHub 사용자 정의 리소스가 생성될 때 클러스터에서 이미 사용할 수 있는 MultiClusterEngine 리소스가 없는 경우 MultiClusterHub Operator는 MultiClusterEngine 인스턴스를 배포하고 필요한 Operator를 이전 오류를 해결합니다.

1.3.7.1.2. 관리 클러스터를 가져올 때 Submariner 애드온 리소스가 제대로 정리되지 않음

MCH(MultiClusterHub) Operator 내에서 하위marine r-addon 구성 요소가 false 로 설정된 경우 관리 클러스터 리소스에 대해 하위marine r-addon 종료자가 제대로 정리되지 않습니다. 종료자가 올바르

게 정리되지 않았으므로 hub 클러스터 내에서 하위mariner-addon 구성 요소가 비활성화되지 않습니다.

1.3.7.1.3. Red Hat Advanced Cluster Management에서 관리할 수 있는 일부 인프라 공급자가 지원되는 것은 아닙니다.

Submariner는 Red Hat Advanced Cluster Management에서 관리할 수 있는 모든 인프라 공급자에서 지원되지 않습니다. 지원되는 공급자 목록은 Red Hat Advanced Cluster Management 지원 매트릭스 를 참조하십시오.

1.3.7.1.4. Submariner 설치 계획 제한

Submariner 설치 계획은 전체 설치 계획 설정을 따르지 않습니다. 따라서 운영자 관리 화면에서는 Submariner 설치 계획을 제어할 수 없습니다. 기본적으로 Submariner 설치 계획이 자동으로 적용되며 Submariner 애드온은 설치된 Red Hat Advanced Cluster Management 버전에 해당하는 사용 가능한 최신 버전으로 항상 업데이트됩니다. 이 동작을 변경하려면 사용자 지정된 Submariner 서브스크립션을 사용해야 합니다.

1.3.7.1.5. 제한된 헤드리스 서비스 지원

Globalnet을 사용할 때 선택기가 없는 헤드리스 서비스에 대해서는 서비스 검색이 지원되지 않습니다.

1.3.7.1.6. NAT가 활성화되면 VXLAN을 사용하는 배포는 지원되지 않습니다.

NAT 이외의 배포만 VXLAN 케이블 드라이버를 사용하여 Submariner 배포를 지원합니다.

1.3.7.1.7. OVN Kubernetes에는 OCP 4.11 이상이 필요합니다.

OVN Kubernetes CNI 네트워크를 사용하는 경우 Red Hat OpenShift 4.11 이상이 필요합니다.

1.3.7.1.8. 자체 서명된 인증서로 인해 브로커에 연결하지 못할 수 있습니다.

브로커의 자체 서명된 인증서로 인해 결합된 클러스터가 브로커에 연결되지 않을 수 있습니다. 인증서 유효성 검사 오류와 함께 연결에 실패합니다. 관련 SubmarinerConfig 오브젝트에서 InsecureBrokerConnection 을 true 로 설정하여 브로커 인증서 검증을 비활성화할 수 있습니다. 다음 예제를 참조하십시오.

```
apiVersion: submarineraddon.open-cluster-management.io/v1alpha1
kind: SubmarinerConfig
metadata:
  name: submariner
```

```
    namespace: <managed-cluster-namespace>
  spec:
    insecureBrokerConnection: true
```

1.3.7.1.9. Submariner는 OpenShift SDN 또는 OVN Kubernetes만 지원

Submariner는 OpenShift SDN 또는 OVN-Kubernetes CNI(Container Network Interface) 네트워크 공급자를 사용하는 Red Hat OpenShift Container Platform 클러스터만 지원합니다.

1.3.7.1.10. Microsoft Azure 클러스터에 대한 명령 제한

하위ctl 진단 방화벽 간 클러스터 간 명령은 Microsoft Azure 클러스터에서 작동하지 않습니다.

1.3.7.1.11. 사용자 정의 *CatalogSource* 또는 *Subscription*에서 자동 업그레이드가 작동하지 않음

Submariner는 Red Hat Advanced Cluster Management for Kubernetes가 업그레이드되면 자동으로 업그레이드됩니다. 사용자 정의 CatalogSource 또는 Subscription 을 사용하는 경우 자동 업그레이드가 실패할 수 있습니다.

관리 클러스터에 Submariner를 설치할 때 자동 업그레이드가 작동하려면 각 관리 클러스터의 SubmarinerConfig 사용자 정의 리소스에서 spec.subscriptionConfig.channel 필드를 stable-0.15 로 설정해야 합니다.

1.3.7.1.12. Submariner는 IPsec 지원 OVN-Kubernetes 배포와 충돌

IPsec 지원 OVN-Kubernetes 배포에서 생성된 IPsec 터널은 Submariner에서 생성한 IPsec 터널과 충돌할 수 있습니다. Submariner와 함께 IPsec 모드에서 OVN-Kubernetes를 사용하지 마십시오.

1.3.7.1.13. *ManageClusterSet*에서 *ManagedCluster* 를 제거하기 전에 Submariner 제거

ClusterSet에서 클러스터를 제거하거나 클러스터를 다른 ClusterSet 로 이동하는 경우 Submariner 설치가 더 이상 유효하지 않습니다.

ManageClusterSet 에서 ManagedCluster 를 이동하거나 제거하기 전에 Submariner를 제거해야 합니다. Submariner를 제거하지 않으면 더 이상 Submariner를 제거하거나 다시 설치할 수 없으며 Submariner가 ManagedCluster 에서 작동하지 않습니다.

1.3.7.1.14. OpenShift Container Platform 4.15 이상을 사용하는 VMware vSphere에서 Submariner 설치에 실패합니다.

허브 클러스터에서 관리 클러스터에 대한 브로커 시크릿이 누락되어 OpenShift Container Platform 4.15 이상을 실행하는 VMware vSphere에서 Submariner 애드온 설치가 실패합니다. 하위marine r-addon Pod만 관리 클러스터의 submariner-operator 네임스페이스에 생성되고 콘솔에 레이블이 지정되지 않은 게이트웨이가 표시됩니다.

ClusterSet 브로커 네임스페이스의 각 관리 클러스터에 대해 수동으로 시크릿을 생성하여 문제를 해결할 수 있습니다. 보안을 수동으로 생성하려면 다음 단계를 완료합니다.

1. hub 클러스터에 로그인합니다.
2. YAML 파일을 생성하고 다음 템플릿을 추가합니다. 필요한 경우 값을 바꿉니다.

```
apiVersion: v1
kind: Secret
metadata:
  name: <ManagedClusterName>-broker
  namespace: <ClustersetName>-broker
  annotations:
    kubernetes.io/service-account.name: <ManagedClusterName>
type: kubernetes.io/service-account-token
```

3. 다음 명령을 실행하여 YAML 파일을 적용합니다.

```
oc apply
```

1.3.8. 다중 클러스터 글로벌 허브 Operator의 알려진 문제

multicluster 글로벌 허브 Operator의 알려진 문제를 검토합니다. 다음 목록에는 이 릴리스에 대한 알려진 문제 또는 이전 릴리스에서 계속되는 알려진 문제가 포함되어 있습니다. OpenShift Container Platform 클러스터의 경우 OpenShift Container Platform 알려진 문제를 참조하십시오.

1.3.8.1. 다중 클러스터 글로벌 허브 Grafana 콘솔은 FIPS 지원 환경에서 열 수 없습니다.

FIPS가 활성화된 최신 OpenShift Container Platform 환경에서 다중 클러스터 글로벌 허브가 실행 중인 경우 잘못된 oauth-proxy 이미지로 인해 Grafana 콘솔에 액세스할 수 없습니다. Red Hat Advanced Cluster Management 2.10.x는 최신 OpenShift Container Platform 버전을 지원하므로 Red Hat Advanced Cluster Management 2.10.x에서 oauth-proxy 이미지를 가져올 수 있습니다.

Grafana 콘솔에 액세스하려면 Red Hat Advanced Cluster Management 번들 이미지로 oauth-proxy 이미지를 수동으로 업데이트합니다. oauth-proxy 이미지를 업데이트하려면 다음 단계를 완료합니

다.

1. 다음 명령을 실행하여 **mch-image-manifest-xxx** 에서 올바른 **oauth-proxy** 이미지를 가져옵니다. **& lt;.data.oauth_proxy_latestocp >**를 **OpenShift Container Platform** 버전으로 교체합니다.

```
oc get cm -n open-cluster-management mch-image-manifest-xxx -ojsonpath=
<.data.oauth_proxy_latestocp>
```

2. 다음 명령을 실행하여 **multicluster global hub clusterserviceversion (CSV)**의 배포 이미지를 올바른 이미지로 업데이트합니다.

```
oc edit csv multicluster-global-hub-operator-rh.v1.1.x -n multicluster-global-hub
```

3. **RELATED_IMAGE_OAUTH_PROXY** 값을 찾아 **1**단계에서 받은 출력으로 바꿉니다.

1.3.8.2. Kafka Operator가 다시 시작됨

FIPS(Federal Information Processing Standard) 환경에서 **Kafka Operator**는 **OOM(**메모리 부족**)** 상태로 인해 다시 시작됩니다. 이 문제를 해결하려면 리소스 제한을 **512M** 이상으로 설정합니다. 이 제한을 설정하는 방법에 대한 자세한 단계는 **amq stream doc** 를 참조하십시오.

1.3.8.3. 알려진 문제 백업 및 복원

원래 다중 클러스터 글로벌 허브 클러스터가 충돌하면 다중 클러스터 글로벌 허브가 생성된 이벤트 및 **cron** 작업이 손실됩니다. 새 다중 클러스터 글로벌 허브 클러스터를 복원하더라도 이벤트 및 **cron** 작업이 복원되지 않습니다. 이 문제를 해결하려면 **cron** 작업을 수동으로 실행할 수 있습니다. **https://access.redhat.com/documentation/en-us/red_hat_advanced_cluster_management_for_kubernetes/2.9/html/multicluster_global_hub/multicluster-global-hub#global-hub-compliance-manual**

1.3.8.4. 관리되는 클러스터 디스플레이는 표시되지만 계산되지 않음

성공적으로 생성되지 않은 관리 클러스터입니다. 즉 **clusterclaim id.k8s.io** 는 관리 클러스터에 존재하지 않으며 정책 준수 대시보드에 포함되지 않지만 정책 콘솔에 표시됩니다.

1.3.8.5. OpenShift Container Platform 4.13 하이퍼링크에 다중 클러스터 글로벌 허브가 설치되어 있으면 홈으로 리디렉션될 수 있습니다.

다중 클러스터 글로벌 허브 **Operator**가 **OpenShift Container Platform 4.13**에 설치된 경우 관리 클

러스터 목록에 연결되는 모든 하이퍼링크와 대시보드의 세부 페이지가 **Red Hat Advanced Cluster Management** 홈페이지로 리디렉션될 수 있습니다.

대상 페이지로 수동으로 이동해야 합니다.

1.3.8.6. 표준 그룹 필터는 새 페이지로 전달할 수 없습니다.

Global Hub Policy Group Compliancy Overview Hub Dashboard에서 **View Offending Policies for standard group** 을 클릭하여 하나의 데이터 포인트를 확인할 수 있지만 이 링크를 클릭하면 표준 그룹 필터가 새 페이지로 이동할 수 없습니다.

이는 클러스터 그룹 호환 개요에도 문제가 있습니다.

1.3.8.7. OpenShift Container Platform 3.11 클러스터 *Observability* 페이지로 리디렉션할 수 없습니다

관리형 허브 클러스터에서 **OpenShift Container Platform 3.11** 클러스터(더 이상 사용되지 않음)를 관리 클러스터로 가져오는 경우 **Global Hub >** 개요 대시보드의 ***Observability*** 페이지로 리디렉션할 수 없습니다.

대상 페이지로 수동으로 이동해야 합니다.

1.4. 사용 중단 및 제거

Red Hat Advanced Cluster Management for Kubernetes에서 제품의 일부가 더 이상 사용되지 않거나 제거되는지 알아보십시오. 현재 릴리스와 두 개의 이전 릴리스의 테이블에 표시되는 *권장 작업* 및 세부 사항의 대체 작업을 고려하십시오.

더 이상 사용되지 않음: **Red Hat Advanced Cluster Management 2.7** 및 이전 버전은 더 이상 지원되지 않습니다. 문서는 사용할 수 있지만 에라타 또는 기타 업데이트는 사용할 수 없습니다.

모범 사례: 최신 버전으로 업그레이드합니다.

1.4.1. API 사용 중단 및 제거

Red Hat Advanced Cluster Management는 **API**에 대한 **Kubernetes** 사용 중단 지침을 따릅니다. 해당 정책에 대한 자세한 내용은 **Kubernetes** 사용 중단 정책을 참조하십시오. **Red Hat Advanced Cluster**

Management API는 다음 타임라인 외부에서 더 이상 사용되지 않거나 제거됩니다.

- 모든 **V1 API**는 일반적으로 **12**개월 또는 **3**개의 릴리스에서 더 큰 릴리스에서 일반적으로 사용할 수 있습니다. **V1 API**는 제거되지 않지만 시간 제한 외부에서 더 이상 사용되지 않을 수 있습니다.
- 모든 베타 **API**는 일반적으로 **9** 개월 또는 세 번 릴리스에서 사용할 수 있습니다. 베타 **API**는 해당 시간 제한 외부에서 제거되지 않습니다.
- 모든 알파 **API**는 지원되지 않아도 되지만 사용자에게 도움이 되는 경우 더 이상 사용되지 않거나 제거될 수 있습니다.

1.4.1.1. API 제거

제품 또는 카테고리	영향을 받는 항목	버전	권장 작업	자세한 내용 및 링크
ManagedClusterSets	**v1beta1** API가 제거되었습니다.	2.9	대신 **v1beta2** 를 사용합니다.	ManagedClusterSets.cluster.open-cluster-management.io
ManagedClusterSetBindings	**v1beta1** API가 제거되었습니다.	2.9	대신 **v1beta2** 를 사용합니다.	ManagedClusterSetBindings.cluster.open-cluster-management.io
HypershiftDeployment	**HypershiftDeployment** API가 제거되었습니다.	2.7	이 API를 사용하지 마십시오.	
BareMetalAssets	**v1alpha1** API가 제거되었습니다.	2.7	이 API를 사용하지 마십시오.	Baremetalassets.inventory.open-cluster-management.io
배치	**v1alpha1** API가 제거되었습니다.	2.7	대신 **v1beta1** 을 사용합니다.	Placements.cluster.open-cluster-management.io
PlacementDecisions	**v1alpha1** API가 제거되었습니다.	2.7	대신 **v1beta1** 을 사용합니다.	PlacementDecisions.cluster.open-cluster-management.io

제품 또는 카테고리	영향을 받는 항목	버전	권장 작업	자세한 내용 및 링크
ClusterManagementAddOn	**addOnConfiguration** 필드는 **ClusterManagementAddOn** 사양에서 더 이상 사용되지 않습니다.	2.7	**supportedConfigs** 필드를 사용합니다.	없음
ManagedClusterAddOn	**addOnConfiguration** 필드는 **ManagedClusterAddOn** 사양에서 더 이상 사용되지 않습니다.	2.7	**supportedConfigs** 필드를 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 않는 것은 권장되지 않으며 향후 릴리스에서 더 이상 사용되지 않을 수 있습니다. *권장*** **작업 및 다음 표에 제공되는 세부 사항의 대체 작업을 고려하십시오.**

제품 또는 카테고리	영향을 받는 항목	버전	권장 작업	자세한 내용 및 링크
OpenShift Container Platform 3.11에서 지원되는 기능	다양한 구성 요소	2.9	없음	라이프 사이클 정책
거버넌스	IAM 정책 컨트롤러	2.9	없음	
거버넌스	컨테이너 보안 Operator	OpenShift Container Platform 3.11	없음	OpenShift Container Platform 3.11에서는 컨테이너 보안 Operator를 사용할 수 없습니다.

제품 또는 카테고리	영향을 받는 항목	버전	권장 작업	자세한 내용 및 링크
설치 프로그램	**operator.open-cluster-management.io_multiclusterhubs_crd.yaml** 의 **Ingress.sslCiphers** 필드	2.9	없음	설치 구성은 고급 구성 을 참조하십시오. Red Hat Advanced Cluster Management for Kubernetes 버전 및 원래 **spec.ingress.sslCiphers** 필드가 정의된 **MultiClusterHub** 사용자 정의 리소스가 있는 경우 이 필드는 계속 인식되지만 더 이상 사용되지 않으며 적용되지 않습니다.
애플리케이션 및 관리	**PlacementRule**	2.8	**PlacementRule** 을 사용할 수 있는 배치를 사용하십시오.	**PlacementRule** 은 계속 사용할 수 있지만 지원되지 않으며 콘솔은 기본적으로 **배치를** 표시합니다.
설치 프로그램	**operator.open-cluster-management.io_multiclusterhubs_crd.yaml**의 **customCAConfigmap** 필드	2.7	없음	설치 구성은 고급 구성 을 참조하십시오.

1.4.3. 제거

삭제된 **항목은 일반적으로 이전 릴리스에서 더 이상 사용되지 않으며 제품에서 더 이상 사용할 수 없는 기능입니다. 제거된 함수에 대한 대안을 사용해야 합니다.** ***권장*** **작업 및 다음 표에 제공되는 세부 사항의 대체 작업을 고려하십시오.**

제품 또는 카테고리	영향을 받는 항목	버전	권장 작업	자세한 내용 및 링크

제품 또는 카테고리	영향을 받는 항목	버전	권장 작업	자세한 내용 및 링크
검색	**SearchCustomizations.open-cluster-management.io** 사용자 정의 리소스 정의가 제거됩니다.	2.7	**search.open-cluster-management.io/v1alpha1** 을 사용하여 검색을 사용자 지정합니다.	없음
검색	RedisGraph는 내부 데이터베이스로 PostgreSQL으로 교체되었습니다.	2.7	변경이 필요하지 않습니다.	PostgreSQL을 내부 데이터베이스로 사용하여 검색 구성 요소가 다시 구현됩니다.
콘솔	독립 실행형 웹 콘솔	2.7	통합 웹 콘솔을 사용합니다.	자세한 내용은 콘솔 액세스를 참조하십시오.

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

1.5.1. 알림

이 문서는 일반 데이터 보호 규정 (GDPR) 준비에 대한 준비를 돕기 위한 것입니다. 사용자가 구성할 수 있는 Kubernetes 플랫폼용 Red Hat Advanced Cluster Management의 기능과 제품 사용 측면과 GDPR 준비에 도움이 되도록 고려해야 하는 정보를 제공합니다. 클라이언트가 기능을 선택하고 구성할 수 있는 다양한 방법과 제품이 자체적으로 및 타사 클러스터 및 시스템과 함께 사용할 수 있는 다양한 방식으로 인해 이 정보가 완전한 목록이 아닙니다.

고객은 유럽 연합 일반 데이터 보호 규정을 포함한 다양한 법률 및 규정을 자체 준수하도록 할 책임이 있습니다. 고객은 고객의 비즈니스에 영향을 미칠 수 있는 관련 법률 및 규정의 식별 및 해석 및 고객이 이러한 법률 및 규정을 준수하기 위해 취해야 할 모든 조치를 취할 책임이 있습니다.

본원에서 설명된 제품, 서비스 및 기타 기능은 모든 클라이언트 상황에 적합하지 않으며 가용성이 제한될 수 있습니다. Red Hat은 법적, 회계 또는 감사 조언을 제공하거나, 서비스 또는 제품이 고객이 법률 또는 규정을 준수하도록 보장할 것을 보증하지 않습니다.

1.5.2. 목차

- GDPR
- GDPR의 제품 구성
- 데이터 라이프 사이클
- 데이터 수집
- 데이터 스토리지
- 데이터 액세스
- 데이터 처리
- 데이터 삭제
- 개인 데이터 사용 제한 기능
- 부록

1.5.3. GDPR

GDPR(General Data Protection Regulation)은 유럽 연합("EU")에 의해 채택되었으며 2018년 5월 25일부터 적용됩니다.

1.5.3.1. GDPR이 중요한 이유는 무엇입니까?

GDPR은 개인의 개인 데이터를 처리하기 위한 더 강력한 데이터 보호 규제 프레임워크를 설정합니다. GDPR은 다음과 같은 기능을 제공합니다.

- 개인을 위한 새롭고 향상된 권리
- 개인 데이터에 대한 광범위한 정의
- 프로세서에 대한 새로운 의무
- 비준수에 대한 상당한 금융 연금의 가능성이 있습니다.
- 강제 데이터 유출 알림

1.5.3.2. GDPR에 대해 자세히 알아보기

- EU GDPR 정보 포털
- Red Hat GDPR 웹 사이트

1.5.4. GDPR의 제품 구성

다음 섹션에서는 **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼 내에서 데이터 관리의 측면을 설명하고 **GDPR** 요구 사항이 있는 클라이언트를 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(**governance, risk, compliance**)를 포함하는 컨테이너를 관리하기 위한 통합 환경입니다.

따라서 **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼은 주로 플랫폼의 구성 및 관리와 관련된 기술 데이터를 처리하며 그 중 일부는 **GDPR**의 적용을 받을 수 있습니다. **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼은 플랫폼을 관리하는 사용자에 대한 정보도 처리합니다. 이 데이터는 **GDPR** 요구 사항 충족을 담당하는 고객의 인식을 위해 이 문서 전체에서 설명되어 있습니다.

이 데이터는 구성 파일 또는 데이터베이스로 로컬 또는 원격 파일 시스템의 플랫폼에서 유지됩니다. **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼에서 실행되도록 개발된 애플리케이션은 **GDPR**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 애플리케이션에서 수집한 개인 데이터를 관리하고 보호하려면 추가 메커니즘이 필요할 수 있습니다.

Kubernetes 플랫폼 및 해당 데이터 흐름에 대한 **Red Hat Advanced Cluster Management**를 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 실행하는 데 필요한 모든 소프트웨어 패키지가 포함되어 있습니다.

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

플랫폼으로서 **Red Hat Advanced Cluster Management for Kubernetes**는 관리자 사용자 **ID** 및 암호, 서비스 사용자 **ID** 및 암호, **IP** 주소 및 **Kubernetes** 노드 이름과 같이 개인 데이터로 간주할 수 있는 여러 기술 데이터 카테고리를 처리합니다. **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼은 플랫폼을 관리하는 사용자에 대한 정보도 처리합니다. 플랫폼에서 실행되는 애플리케이션에서는 플랫폼에 알려지지 않은 다른 개인 데이터 범주가 도입될 수 있습니다.

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

1.5.5.2. 온라인 연락처에 사용되는 개인정보

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

- **Slack** 채널이 있는 경우 공개 **Slack** 커뮤니티
- 제품 설명서의 공개 의견 또는 티켓
- 기술 커뮤니티의 공개 대화

일반적으로 고객 이름과 이메일 주소만 사용되며, 연락처에 대한 개인 응답을 활성화하는 데 사용되며, 개인 데이터 사용은 **Red Hat** 온라인 개인정보처리방침 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 관리합니다. 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 콘솔 또는 **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼 노드에 로그인하는 경우에도 시스템 관리자를 통해서만 시스템 관리자가 액세스할 수 있습니다.

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

컨테이너화된 애플리케이션을 실행하는 **Kubernetes** 플랫폼에 대한 **Red Hat Advanced Cluster Management** 사용 및 **GDPR** 요구 사항을 충족할 필요가 있는 경우, 애플리케이션에 의해 수집된 개인정보 유형과 해당 데이터 관리 방법의 측면을 고려해야 합니다.

- 데이터가 애플리케이션에 전달될 때 그리고 애플리케이션에서 전달될 때 데이터가 어떻게 보호됩니까? 전송 중 데이터가 암호화되어 있습니까?
- 애플리케이션이 데이터를 어떻게 저장합니까? 데이터가 미사용 상태에서 암호화됩니까?
- 수집 및 저장된 애플리케이션에 액세스하는 데 사용되는 인증 정보는 어떻게 됩니까?
- 애플리케이션에서 수집 및 저장된 데이터 소스에 액세스하는 데 사용되는 인증 정보는 어떻게 됩니까?
- 필요에 따라 애플리케이션에서 수집한 데이터는 어떻게 제거됩니까?

이는 **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼에서 수집한 데이터 유형에 대한 명확한 목록은 아닙니다. 이는 고려 사항에 대한 예가 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 시스템의 상태 저장 저장소에 있는 플랫폼 구성 및 관리와 관련된 기술 데이터를 구성 파일 또는 데이터베이스로 유

지합니다. 미사용 모든 데이터를 보호하려면 고려해야 합니다. **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼은 **dm-crypt** 를 사용하는 상태 저장 저장소의 미사용 데이터 암호화를 지원합니다.

다음 항목은 데이터가 저장된 영역을 강조하며, 이는 **GDPR**에 대해 고려할 수 있습니다.

- 플랫폼 구성 데이터: **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼 구성은 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 프로그램의 **Red Hat Advanced Cluster Management**에 대한 입력으로 사용됩니다. 속성에는 부트스트랩에 사용되는 관리자 사용자 **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**에 정의된 사용자 및 그룹은 **Kubernetes** 플랫폼 팀의 **Red Hat Advanced Cluster Management**에 추가되고 액세스 역할이 할당될 수 있습니다. **Kubernetes**용 **Red Hat Advanced Cluster Management** 플랫폼은 **LDAP**의 이메일 주소와 사용자 **ID**를 저장하지만 암호를 저장하지 않습니다. **Kubernetes**용 **Red Hat Advanced Cluster Management** 플랫폼은 그룹 이름과 로그인 시 사용자가 속한 사용 가능한 그룹을 캐시합니다. 그룹 멤버십은 장기적인 방식으로 유지되지 않습니다. 엔터프라이즈 **LDAP**에서 미사용 사용자 및 그룹 데이터 보안을 고려해야 합니다. **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼에는 엔터프라이즈 디렉터리와 상호 작용하고 액세스 토큰을 유지 관리하는 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 **Red Hat Advanced Cluster Management**에서 사용하는 인증 정보는 **Kubernetes** 시크릿으로 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

Red Hat Advanced Cluster Management for Kubernetes 플랫폼 데이터는 다음과 같이 정의된 제품 인터페이스 세트를 통해 액세스할 수 있습니다.

- 웹 사용자 인터페이스(컨트롤러)

- Kubernetes kubectl CLI
- Red Hat Advanced Cluster Management for Kubernetes CLI
- oc CLI

이러한 인터페이스는 Kubernetes 클러스터용 Red Hat Advanced Cluster Management를 관리할 수 있도록 설계되었습니다. Kubernetes용 Red Hat Advanced Cluster Management에 대한 관리 액세스 권한을 보호할 수 있으며, 요청이 생성되면 논리 3단계(인증, 역할 매핑 및 권한 부여)가 포함됩니다.

1.5.8.1. 인증

Red Hat Advanced Cluster Management for Kubernetes 플랫폼 인증 관리자는 콘솔에서 사용자 인증 정보를 수락하고 엔터프라이즈 디렉터리에 대해 사용자 인증 정보를 검증하는 백엔드 OIDC 공급자로 인증 정보를 전달합니다. 그런 다음 OIDC 공급자는 JSON 웹 토큰(JWT)의 콘텐츠가 포함된 인증쿠키(인증 쿠키)를 인증 관리자에게 반환합니다. JWT 토큰은 인증 요청 시 그룹 멤버십 외에 사용자 ID 및 이메일 주소와 같은 정보를 유지합니다. 그런 다음 이 인증 쿠키가 콘솔로 다시 전송됩니다. 세션 중에 쿠키가 새로 고쳐집니다. 콘솔에서 로그아웃하거나 웹 브라우저를 종료한 후 12시간 동안 유효합니다.

콘솔에서 수행된 모든 후속 인증 요청에 대해 프런트 엔드 NGINX 서버는 요청에서 사용 가능한 인증 쿠키를 디코딩하고 인증 관리자를 호출하여 요청을 검증합니다.

Kubernetes 플랫폼 CLI용 Red Hat Advanced Cluster Management를 사용하려면 사용자가 로그인할 수 있는 인증 정보를 제공해야 합니다.

kubectl 및 oc CLI도 클러스터에 액세스하기 위해 인증 정보가 필요합니다. 이러한 인증 정보는 관리 콘솔에서 가져와 12 시간 후에 만료될 수 있습니다. 서비스 계정을 통한 액세스가 지원됩니다.

1.5.8.2. 역할 매핑

Red Hat Advanced Cluster Management for Kubernetes 플랫폼은 역할 기반 액세스 제어(RBAC)를 지원합니다. 역할 매핑 단계에서는 인증 단계에서 제공되는 사용자 이름이 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, 카탈

로그 및 Helm 리소스 및 Kubernetes 리소스에 대한 액세스를 제어합니다. 클러스터 관리자, 관리자, Operator, 편집기, 뷰어를 포함하여 여러 IAM(Identity and Access Management) 역할이 제공됩니다. 팀에 추가할 때 사용자 또는 사용자 그룹에 역할이 할당됩니다. 리소스에 대한 팀 액세스는 네임스페이스를 통해 제어할 수 있습니다.

1.5.8.4. Pod 보안

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

1.5.9. 데이터 처리

Red Hat Advanced Cluster Management for Kubernetes 사용자는 구성 및 관리와 관련된 기술 데이터를 처리하고 시스템 구성을 통해 보호하는 방법을 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 안전한 데이터 전송에 사용됩니다. 사용자는 설치 중에 사용할 root 인증서를 지정할 수 있습니다.

data-at-rest 보호는 dm-crypt 를 사용하여 데이터를 암호화하여 지원합니다.

이러한 플랫폼 메커니즘은 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. 고객은 추가 제어를 구현하기 위해 자체 기능을 개발할 수 있습니다.

1.5.10. 데이터 삭제

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

데이터 삭제를 지원하기 위해 고려해야 하는 Red Hat Advanced Cluster Management for Kubernetes 플랫폼의 영역:

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

계정 데이터 삭제를 지원하기 위해 고려해야 하는 **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼의 영역:

- 플랫폼 구성과 관련된 모든 기술 데이터는 **Red Hat Advanced Cluster Management for Kubernetes** 또는 **Kubernetes kubectl API**를 통해 삭제할 수 있습니다.

엔터프라이즈 **LDAP** 디렉터리를 통해 관리되는 사용자 **ID** 및 암호 데이터를 제거하는 기능은 **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼과 함께 사용되는 **LDAP** 제품을 통해 제공됩니다.

1.5.11. 개인 데이터 사용 제한 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.

GDPR 하에 사용자는 처리에 액세스, 수정 및 제한할 수 있는 권한이 있습니다. 이 문서의 다른 섹션을 참조하여 다음을 제어하십시오.

- 액세스 권한
  - **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼 관리자는 **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼 기능을 사용하여 개인에게 데이터에 대한 액세스를 제공할 수 있습니다.
  - **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼 관리자는 **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼 기능을 사용하여 개인에 대한 **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼에 대한 개인 정보를 제공할 수 있습니다.
- 수정 권한
  - **Red Hat Advanced Cluster Management for Kubernetes** 플랫폼 관리자는 **Red Hat**

Advanced Cluster Management for Kubernetes 플랫폼 기능을 사용하여 데이터를 수정하거나 수정할 수 있습니다.

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

- 처리를 제한할 수 있는 권한
  - Red Hat Advanced Cluster Management for Kubernetes 플랫폼 관리자는 Red Hat Advanced Cluster Management for Kubernetes 플랫폼 기능을 사용하여 개별 데이터 처리를 중지할 수 있습니다.

1.5.12. 부록

플랫폼으로서 Red Hat Advanced Cluster Management for Kubernetes는 관리자 사용자 ID 및 암호, 서비스 사용자 ID 및 암호, IP 주소 및 Kubernetes 노드 이름과 같이 개인 데이터로 간주할 수 있는 여러 기술 데이터 카테고리를 처리합니다. Red Hat Advanced Cluster Management for Kubernetes 플랫폼은 플랫폼을 관리하는 사용자에 대한 정보도 처리합니다. 플랫폼에서 실행되는 애플리케이션에서는 플랫폼에 알려지지 않은 다른 범주의 개인 데이터가 도입될 수 있습니다.

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

1.6. FIPS 준비

Red Hat Advanced Cluster Management for Kubernetes는 FIPS용으로 설계되었습니다. FIPS 모드에서 Red Hat OpenShift Container Platform을 실행하는 경우 OpenShift Container Platform은 OpenShift Container Platform에서 지원하는 아키텍처에서만 FIPS 검증에 제출된 Red Hat Enterprise Linux 암호화 라이브러리를 사용합니다. NIST 검증 프로그램에 대한 자세한 내용은 암호화 모듈 유효성 검사 프로그램을 참조하십시오. 검증을 위해 제출된 RHEL 암호화 라이브러리의 개별 버전에 대한 최신 NIST 상태는 규정 준수 활동 및 정부 표준을 참조하십시오.

FIPS가 활성화된 클러스터를 관리하려면 FIPS 모드에서 작동하도록 구성된 OpenShift Container Platform 클러스터에 Red Hat Advanced Cluster Management를 설치해야 합니다. 허브 클러스터에서 생성된 암호화가 관리 클러스터에서 사용되므로 허브 클러스터는 FIPS 모드에 있어야 합니다.

관리 클러스터에서 FIPS 모드를 활성화하려면 OpenShift Container Platform 관리 클러스터를 프로비저닝할 때 fips: true 를 설정합니다. 클러스터를 프로비저닝한 후에는 FIPS를 활성화할 수 없습니다. 자

세한 내용은 **OpenShift Container Platform** 설명서를 참조하십시오. 클러스터에 대한 추가 보안이 필요하십니까?

1.6.1. 제한

Red Hat Advanced Cluster Management 및 **FIPS**에서 다음 제한 사항을 읽으십시오.

- 제공된 스토리지를 구성할 때 검색 및 관찰 구성 요소에서 사용하는 **PVC**(영구 볼륨 클레임) 및 **S3** 스토리지는 암호화해야 합니다. **Red Hat Advanced Cluster Management**는 스토리지 암호화를 제공하지 않습니다. **OpenShift Container Platform** 설명서, 영구 스토리지 구성을 참조하십시오.

- **Red Hat Advanced Cluster Management** 콘솔을 사용하여 관리형 클러스터를 프로비저닝하는 경우 관리 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.

1.7. 관찰 기능 지원

- **Red Hat Advanced Cluster Management**는 **Red Hat OpenShift Data Foundation** (이전의 **Red Hat OpenShift Container Platform**)에서 테스트 및 완벽하게 지원합니다.

- **Red Hat Advanced Cluster Management**는 **S3 API**와 호환되는 사용자 제공 타사 오브젝트 스토리지에서 다중 클러스터 관찰 기능 **Operator**의 기능을 지원합니다. 관찰 기능 서비스는 **Thanos**에서 지원되는 안정적인 오브젝트 저장소를 사용합니다.

- **Red Hat Advanced Cluster Management** 지원팀에는 근본 원인을 파악하기 위한 적절한 노력이 포함됩니다. 지원 티켓을 열고 근본 원인은 사용자가 제공한 **S3** 호환 오브젝트 스토리지인 경우 고객 지원 채널을 사용하여 문제를 열어야 합니다.