



Red Hat Advanced Cluster Management for Kubernetes 2.8

문제 해결

문제 해결

법적 공지

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

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

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

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

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

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

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

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

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

All other trademarks are the property of their respective owners.

초록

클러스터의 문제 해결 주제 목록을 확인합니다. `must-gather` 명령을 사용하여 로그를 수집할 수도 있습니다.

차례

1장. 문제 해결	3
1.1. 문서화된 문제 해결	3
1.2. 문제를 해결하기 위해 MUST-GATHER 명령 실행	4
1.3. 설치 또는 보류 중 설치 상태 문제 해결	6
1.4. 재설치 실패 문제 해결	6
1.5. 오프라인 클러스터 문제 해결	7
1.6. 관리형 클러스터 가져오기 장애 문제 해결	8
1.7. 보류 중인 가져오기 상태로 클러스터 문제 해결	9
1.8. 이미 존재하는 클러스터 문제 해결 오류	9
1.9. VMWARE VSPHERE에서 클러스터 생성 문제 해결	10
1.10. 신뢰할 수 없는 권한 오류가 있는 RED HAT OPENSTACK PLATFORM에서 관리형 클러스터 생성 실패	13
1.11. OPENSIFT CONTAINER PLATFORM 버전 3.11 클러스터 가져오기 장애 문제 해결	14
1.12. 인증서 변경 후 가져온 클러스터 문제 해결	15
1.13. 클러스터를 삭제한 후 네임스페이스가 남아 있음	17
1.14. 클러스터를 가져올 때 AUTO-IMPORT-SECRET-EXISTS 오류	18
1.15. 클러스터 상태 변경 문제 해결	18
1.16. 보류 중 또는 실패 상태의 콘솔에서 클러스터 문제 해결	19
1.17. 애플리케이션 GIT 서버 연결 문제 해결	20
1.18. GRAFANA 문제 해결	22
1.19. 배치 규칙을 사용하여 선택하지 않은 로컬 클러스터 문제 해결	23
1.20. 애플리케이션 KUBERNETES 배포 버전 문제 해결	24
1.21. 성능 저하된 조건이 있는 KLUSTERLET 문제 해결	25
1.22. 오브젝트 스토리지 채널 보안 문제 해결	26
1.23. 가시성 문제 해결	27
1.24. OPENSIFT 모니터링 서비스 문제 해결	28
1.25. METRICS-COLLECTOR 문제 해결	28
1.26. POSTGRESQL 공유 메모리 오류 문제 해결	29
1.27. 설치 후 연결되지 않은 SUBMARINER 문제 해결	30
1.28. SUBMARINER 애드온 문제 해결	31
1.29. 오류와 함께 복원 상태 문제 해결	32
1.30. HUB 클러스터 백업을 복원할 때 일반 리소스가 제거됨	33
1.31. OADP 사용자 정의 리소스 정의 문제 해결	33
1.32. 여러 줄 YAML 구문 분석 문제 해결	34

1장. 문제 해결

문제 해결 가이드를 사용하기 전에 **oc adm must-gather** 명령을 실행하여 세부 정보를 수집하고, 로그를 수집하고, 문제 디버깅 단계를 수행할 수 있습니다. 자세한 내용은 [문제를 해결하려면 must-gather 명령 실행을 참조하십시오](#).

또한 역할 기반 액세스를 확인합니다. 자세한 내용은 [역할 기반 액세스 제어](#)를 참조하십시오.

1.1. 문서화된 문제 해결

Kubernetes용 Red Hat Advanced Cluster Management의 문제 해결 주제 목록을 확인합니다.

설치

설치 작업에 대한 기본 문서를 보려면 [설치 및 업그레이드](#)를 참조하십시오.

- [설치 또는 보류 중 설치 상태 문제 해결](#)
- [재설치 실패 문제 해결](#)

백업 및 복원

백업 및 복원에 대한 주요 문서를 보려면 [백업 및 복원](#)을 참조하십시오.

- [오류와 함께 복원 상태 문제 해결](#)
- [hub 클러스터 백업을 복원할 때 일반 리소스가 제거됨](#)
- [OADP 사용자 정의 정의 문제 해결](#)

클러스터 관리

클러스터 관리에 대한 기본 문서를 보려면 [다중 클러스터 엔진 Operator 클러스터 라이프사이클 개요](#) 를 참조하십시오.

- [오프라인 클러스터 문제 해결](#)
- [관리형 클러스터 가져오기 장애 문제 해결](#)
- [보류 중인 가져오기 상태로 클러스터 문제 해결](#)
- [인증서 변경 후 가져온 클러스터 문제 해결](#)
- [클러스터 상태 변경 문제 해결](#)
- [VMware vSphere에서 클러스터 생성 문제 해결](#)
- [보류 중 또는 실패 상태의 콘솔에서 클러스터 문제 해결](#)
- [OpenShift Container Platform 버전 3.11 클러스터 가져오기 장애 문제 해결](#)
- [성능 저하된 조건이 있는 Klusterlet 문제 해결](#)
- [오브젝트 스토리지 채널 보안 문제 해결](#)
- [클러스터를 삭제한 후 네임스페이스가 남아 있음](#)

- [클러스터를 가져올 때 Auto-import-secret-exists 오류](#)

애플리케이션 관리

애플리케이션 관리에 대한 주요 문서를 보려면 [애플리케이션 관리를 참조하십시오. .././html-single/applications](#)

- [애플리케이션 Kubernetes 배포 버전 문제 해결](#)
- [애플리케이션 Git 서버 연결 문제 해결](#)
- [선택하지 않은 로컬 클러스터 문제 해결](#)

거버넌스

- [여러 줄 YAML 구문 분석 문제 해결](#)

보안 가이드를 보려면 [위험 및 규정 준수를 참조하십시오.](#)

콘솔 관찰 기능

콘솔 관찰 기능에는 헤더 및 탐색 기능과 함께 검색 기능이 포함됩니다. 관찰 가이드를 보려면 [콘솔에서 관찰 기능을 참조하십시오.](#)

- [grafana 문제 해결](#)
- [가시성 문제 해결](#)
- [OpenShift 모니터링 서비스 문제 해결](#)
- [metrics-collector 문제 해결](#)
- [PostgreSQL 공유 메모리 오류 문제 해결](#)

Submariner 네트워킹 및 서비스 검색

이 섹션에는 Red Hat Advanced Cluster Management 또는 다중 클러스터 엔진 Operator에서 Submariner를 사용할 때 발생할 수 있는 Submariner 문제 해결 절차가 나열되어 있습니다. 일반적인 Submariner 문제 해결 정보는 Submariner 설명서의 [문제 해결](#)을 참조하십시오.

Submariner 네트워킹 서비스 및 서비스 검색에 대한 기본 문서를 보려면 [Submariner 다중 클러스터 네트워킹 및 서비스 검색](#)을 참조하십시오.

- [설치 후 연결되지 않는 Submariner 문제 해결 - 일반 정보](#)
- [Submariner 애드온 문제 해결](#)

1.2. 문제를 해결하기 위해 MUST-GATHER 명령 실행

문제 해결을 시작하려면 사용자가 **must-gather** 명령을 실행하여 문제를 디버깅할 수 있는 문제 해결 시나리오에 대해 알아보고 명령을 사용하여 시작하는 절차를 참조하십시오.

필수 액세스 권한: 클러스터 관리자

1.2.1. must-gather 시나리오

- **시나리오 1:** 문제 해결 방법에 대한 자세한 내용은 문서화된 문제 해결 섹션을 참조하십시오. 이 가이드는 제품의 주요 기능에 따라 구성됩니다. 이 시나리오에서는 가이드에서 해결 방법이 문서에 있는지 확인합니다. 예를 들어 클러스터 생성에 문제가 있는 경우 *클러스터 관리* 섹션에서 해결 방법을 찾을 수 있습니다.
- **시나리오 2:** 해결 단계에 문제가 문서화되지 않은 경우 **must-gather** 명령을 실행하고 출력을 사용하여 문제를 디버깅합니다.
- **시나리오 3:** **must-gather** 명령의 출력을 사용하여 문제를 디버깅할 수 없는 경우 Red Hat 지원과 출력을 공유하십시오.

1.2.2. must-gather 절차

must-gather 명령 사용을 시작하려면 다음 절차를 참조하십시오.

1. **must-gather** 명령에 대해 알아보고 Red Hat OpenShift Container Platform 설명서에서 [클러스터에 대한 데이터를 수집하는 데 필요한 사전 요구 사항을 설치합니다](#).
2. 클러스터에 로그인합니다. 데이터 및 디렉토리를 수집하는 데 사용되는 Kubernetes용 Red Hat Advanced Cluster Management를 추가합니다. 출력에 대한 이미지와 디렉토리를 삽입한 다음 명령을 실행합니다.

```
oc adm must-gather --image=registry.redhat.io/rhacm2/acm-must-gather-rhel8:v2.8 --dest-dir=<directory>
```

3. 일반적인 사용 사례의 경우 *허브* 클러스터에 로그인하는 동안 **must-gather** 를 실행해야 합니다. **참고:** 관리 클러스터를 확인하려면 **cluster-scoped-resources** 디렉터리에 있는 **gather-managed.log** 파일을 찾습니다.

```
<your-directory>/cluster-scoped-resources/gather-managed.log>
```

iPXCEED 및 AVAILABLE 열에 **True** 가 설정되지 않은 관리형 클러스터가 있는지 확인합니다. **True** 상태로 연결되지 않은 클러스터에서 **must-gather** 명령을 실행할 수 있습니다.

4. 지정된 디렉터리로 이동하여 다음 수준으로 구성된 출력을 확인합니다.
 - 두 개의 피어 수준: **cluster-scoped-resources** 및 **namespace** 리소스입니다.
 - 각 하위 수준: 클러스터 범위 및 네임스페이스 범위 리소스의 사용자 정의 리소스 정의의 API 그룹입니다.
 - 각각에 대한 다음 수준: YAML 파일은 종류 별로 정렬됩니다.

1.2.3. 연결이 끊긴 환경의 must-gather

연결이 끊긴 환경에서 **must-gather** 명령을 실행하려면 다음 단계를 완료합니다.

1. 연결이 끊긴 환경에서 Red Hat Operator 카탈로그 이미지를 미리 레지스트리에 미러링합니다. 자세한 내용은 [연결이 끊긴 네트워크에 설치를 참조하십시오](#).
2. 다음 명령을 실행하여 모든 정보를 수집합니다.

```
REGISTRY=<internal.repo.address:port>
IMAGE1=$REGISTRY/rhacm2/acm-must-gather-rhel8:v2.8
oc adm must-gather --image=$IMAGE1 --dest-dir=<directory>
```

현재 지원되는 릴리스 중 하나 또는 제품 설명서에 문제가 있는 경우 추가 문제를 해결하거나 지식베이스 문서를 보거나 [지원 팀에 연결하거나 케이스를 열 수 있는 Red Hat](#) 지원으로 이동하십시오. Red Hat 자격 증명을 사용하여 로그인해야 합니다.

1.3. 설치 또는 보류 중 설치 상태 문제 해결

Red Hat Advanced Cluster Management를 설치할 때 **MultiClusterHub** 는 설치 단계에서 남아 있거나 여러 Pod는 보류 중 상태를 유지합니다.

1.3.1. 증상: 보류 중 상태로 작동

MultiClusterHub를 설치한 후 10분 이상 경과한 **MultiClusterHub** 리소스 보고서 **ProgressDeadlineExceeded .components** 필드에서 하나 이상의 구성 요소가 전달됩니다. 클러스터의 리소스 제약 조건이 문제가 될 수 있습니다.

MultiClusterHub 가 설치된 네임스페이스에서 Pod를 확인합니다. **보류 중** 상태가 다음과 유사한 것으로 표시될 수 있습니다.

```
reason: Unschedulable
message: '0/6 nodes are available: 3 Insufficient cpu, 3 node(s) had taint {node-role.kubernetes.io/master:
}, that the pod didn't tolerate.'
```

이 경우 작업자 노드 리소스가 클러스터에 부족하여 제품을 실행할 수 없습니다.

1.3.2. 문제 해결: 작업자 노드 크기 조정

이 문제가 발생하면 더 큰 작업자 노드로 클러스터를 업데이트해야 합니다. 클러스터 [크기 조정](#)에 대한 지침은 클러스터 스케일링을 참조하십시오.

1.4. 재설치 실패 문제 해결

Kubernetes용 Red Hat Advanced Cluster Management를 다시 설치할 때 Pod가 시작되지 않습니다.

1.4.1. 증상: 재설치 실패

Red Hat Advanced Cluster Management를 설치한 후 Pod가 시작되지 않으면 이전에 Red Hat Advanced Cluster Management가 설치되어 있고 일부 항목이 제거된 것은 아닙니다.

이 경우 설치 프로세스를 완료한 후 Pod가 시작되지 않습니다.

1.4.2. 문제 해결: 재설치 실패

이 문제가 있는 경우 다음 단계를 완료합니다.

1. 설치 제거 프로세스를 실행하여 설치 제거의 단계에 따라 현재 구성 요소를 제거합니다.
[../html-single/install#uninstalling](#)
2. Helm 설치 지침에 따라 Helm CLI 바이너리 버전 3.2.0 이상을 설치합니다.
<https://helm.sh/docs/intro/install/>

3. Red Hat OpenShift Container Platform CLI가 **oc** 명령을 실행하도록 구성되어 있는지 확인합니다. **oc** 명령을 구성하는 방법에 대한 자세한 내용은 OpenShift Container Platform 설명서에서 OpenShift [CLI 시작하기](#) 를 참조하십시오.
4. 다음 스크립트를 파일에 복사합니다.

```
#!/bin/bash
ACM_NAMESPACE=<namespace>
oc delete mch --all -n $ACM_NAMESPACE
helm ls --namespace $ACM_NAMESPACE | cut -f 1 | tail -n +2 | xargs -n 1 helm delete --namespace $ACM_NAMESPACE
oc delete apiservice v1beta1.webhook.certmanager.k8s.io v1.admission.cluster.open-cluster-management.io v1.admission.work.open-cluster-management.io
oc delete clusterimageset --all
oc delete configmap -n $ACM_NAMESPACE cert-manager-controller cert-manager-cainjector-leader-election cert-manager-cainjector-leader-election-core
oc delete consolelink acm-console-link
oc delete crd klusterletaddonconfigs.agent.open-cluster-management.io placementbindings.policy.open-cluster-management.io policies.policy.open-cluster-management.io userpreferences.console.open-cluster-management.io searchservices.search.acm.com discoveredclusters.discovery.open-cluster-management.io discoveryconfigs.discovery.open-cluster-management.io
oc delete mutatingwebhookconfiguration cert-manager-webhook cert-manager-webhook-v1alpha1 ocm-mutating-webhook managedclustermutators.admission.cluster.open-cluster-management.io
oc delete oauthclient multicloudingress
oc delete rolebinding -n kube-system cert-manager-webhook-webhook-authentication-reader
oc delete scc kui-proxy-scc
oc delete validatingwebhookconfiguration cert-manager-webhook cert-manager-webhook-v1alpha1 channels.apps.open.cluster.management.webhook.validator application-webhook-validator multiclusterhub-operator-validating-webhook ocm-validating-webhook
```

스크립트의 **<namespace>** 를 Red Hat Advanced Cluster Management가 설치된 네임스페이스 이름으로 바꿉니다. 네임스페이스가 정리되고 삭제되므로 올바른 네임스페이스를 지정해야 합니다.

5. 스크립트를 실행하여 이전 설치에서 아티팩트를 제거합니다.
6. 설치를 실행합니다. [온라인에 연결된 동안 설치](#) 를 참조하십시오.

1.5. 오프라인 클러스터 문제 해결

오프라인 상태를 표시하는 클러스터의 일반적인 원인은 몇 가지 있습니다.

1.5.1. 증상: 클러스터 상태가 오프라인입니다.

클러스터 생성 절차를 완료한 후에는 Red Hat Advanced Cluster Management 콘솔에서 액세스할 수 없으며 **오프라인** 상태의 상태가 표시됩니다.

1.5.2. 문제 해결: 클러스터 상태가 오프라인 상태임

1. 관리 클러스터를 사용할 수 있는지 확인합니다. Red Hat Advanced Cluster Management 콘솔의 *Clusters* 영역에서 이를 확인할 수 있습니다. 사용할 수 없는 경우 관리 클러스터를 다시 시작해 봅니다.

2. 관리형 클러스터 상태가 여전히 오프라인인 경우 다음 단계를 완료합니다.
 - a. hub 클러스터에서 `oc get managedcluster <cluster_name> -o yaml` 명령을 실행합니다. `<cluster_name>`을 클러스터 이름으로 바꿉니다.
 - b. `status.conditions` 섹션을 찾습니다.
 - c. `type: ManagedClusterConditionAvailable`의 메시지를 확인하고 문제를 해결합니다.

1.6. 관리형 클러스터 가져오기 장애 문제 해결

클러스터 가져오기에 실패하는 경우 클러스터 가져오기에 실패한 이유를 확인하기 위해 몇 가지 단계를 수행할 수 있습니다.

1.6.1. 증상: 가져온 클러스터를 사용할 수 없음

클러스터 가져오기 절차를 완료한 후에는 Kubernetes 콘솔용 Red Hat Advanced Cluster Management에서 액세스할 수 없습니다.

1.6.2. 문제 해결: Imported cluster not available

가져오기를 시도한 후 가져온 클러스터를 사용할 수 없는 몇 가지 이유가 있을 수 있습니다. 클러스터 가져오기에 실패한 경우 가져오기 실패 이유를 찾을 때까지 다음 단계를 완료합니다.

1. Red Hat Advanced Cluster Management hub 클러스터에서 다음 명령을 실행하여 Red Hat Advanced Cluster Management 가져오기 컨트롤러가 실행 중인지 확인합니다.

```
kubectl -n multicluster-engine get pods -l app=managedcluster-import-controller-v2
```

실행 중인 포드 두 개가 표시되어야 합니다. Pod 중 하나가 실행되고 있지 않은 경우 다음 명령을 실행하여 로그를 확인하여 이유를 확인합니다.

```
kubectl -n multicluster-engine logs -l app=managedcluster-import-controller-v2 --tail=-1
```

2. Red Hat Advanced Cluster Management hub 클러스터에서 다음 명령을 실행하여 Red Hat Advanced Cluster Management 가져오기 컨트롤러에서 관리 클러스터 가져오기 시크릿이 성공적으로 생성되었는지 확인합니다.

```
kubectl -n <managed_cluster_name> get secrets <managed_cluster_name>-import
```

가져오기 보안이 없는 경우 다음 명령을 실행하여 가져오기 컨트롤러의 로그 항목을 보고 생성되지 않은 이유를 확인합니다.

```
kubectl -n multicluster-engine logs -l app=managedcluster-import-controller-v2 --tail=-1 | grep importconfig-controller
```

3. Red Hat Advanced Cluster Management hub 클러스터에서 관리 클러스터가 로컬 클러스터 되거나 Hive에 의해 프로비저닝되거나 자동 가져오기 보안이 있는 경우 다음 명령을 실행하여 관리 클러스터의 가져오기 상태를 확인합니다.

```
kubectl get managedcluster <managed_cluster_name> -o=jsonpath='{range .status.conditions[*]}.type{"\t"}{.status}"{"\t"}{.message}"{"\n"}{end}' | grep ManagedClusterImportSucceeded
```

ManagedClusterImportSucceeded 조건이 **true** 가 아닌 경우 명령 결과는 실패 이유를 나타냅니다.

4. 성능 저하된 상태의 관리형 클러스터의 **Klusterlet** 상태를 확인합니다. **Klusterlet**이 성능 저하된 이유를 찾으려면 성능이 저하된 조건을 가진 **Klusterlet** 문제 해결을 참조하십시오.

1.7. 보류 중인 가져오기 상태로 클러스터 문제 해결

클러스터 콘솔에서 **보류 중 가져오기**가 계속되는 경우 절차에 따라 문제를 해결합니다.

1.7.1. 증상: 보류 중인 가져오기 상태가 있는 클러스터

Red Hat Advanced Cluster Management 콘솔을 사용하여 클러스터를 가져온 후 클러스터는 **보류 중 가져오기** 상태와 함께 콘솔에 나타납니다.

1.7.2. 문제 확인: 가져오기 상태가 보류 중인 클러스터

1. 문제가 있는 Kubernetes Pod 이름을 보려면 관리형 클러스터에서 다음 명령을 실행합니다.

```
kubectl get pod -n open-cluster-management-agent | grep klusterlet-registration-agent
```

2. 관리형 클러스터에서 다음 명령을 실행하여 오류에 대한 로그 항목을 찾습니다.

```
kubectl logs <registration_agent_pod> -n open-cluster-management-agent
```

registration_agent_pod 를 1단계에서 확인한 Pod 이름으로 교체합니다.

3. 네트워킹 연결 문제가 있음을 나타내는 텍스트에 대해 반환된 결과를 검색합니다. 예에는 다음이 포함됩니다. 이러한 호스트는 없습니다.

1.7.3. 문제 해결: 가져오기 상태가 보류 중인 클러스터

1. hub 클러스터에 다음 명령을 입력하여 문제가 있는 포트 번호를 검색합니다.

```
oc get infrastructure cluster -o yaml | grep apiServerURL
```

2. 관리 클러스터의 호스트 이름을 확인하고 호스트 및 포트에 대한 아웃바운드 연결이 발생하는지 확인합니다.

관리형 클러스터에서 통신을 설정할 수 없는 경우 클러스터 가져오기가 완료되지 않습니다. 관리 클러스터의 클러스터 상태는 *Pending import* 입니다.

1.8. 이미 존재하는 클러스터 문제 해결 오류

OpenShift Container Platform 클러스터를 Red Hat Advanced Cluster Management **MultiClusterHub** 로 가져올 수 없고 **AlreadyExists** 오류가 발생하면 절차를 수행하여 문제를 해결합니다.

1.8.1. 증상: OpenShift Container Platform 클러스터를 가져올 때 **Already exists** 오류 로그

Red Hat Advanced Cluster Management **MultiClusterHub** 로 OpenShift Container Platform 클러스터를 가져올 때 오류 로그가 표시됩니다.

error log:

Warning: apiextensions.k8s.io/v1beta1 CustomResourceDefinition is deprecated in v1.16+, unavailable in v1.22+; use apiextensions.k8s.io/v1 CustomResourceDefinition

Error from server (AlreadyExists): error when creating "STDIN":

customresourcedefinitions.apiextensions.k8s.io "klusterlets.operator.open-cluster-management.io" already exists

The cluster cannot be imported because its Klusterlet CRD already exists.

Either the cluster was already imported, or it was not detached completely during a previous detach process.

Detach the existing cluster before trying the import again."

1.8.2. 문제 확인: OpenShift Container Platform 클러스터를 가져올 때 준비됨

다음 명령을 실행하여 새 Red Hat Advanced Cluster Management **MultiClusterHub** 로 가져올 클러스터에 Red Hat Advanced Cluster Management 관련 리소스가 있는지 확인합니다.

```
oc get all -n open-cluster-management-agent
oc get all -n open-cluster-management-agent-addon
```

1.8.3. 문제 해결: OpenShift Container Platform 클러스터를 가져올 때 Already exists

다음 명령을 실행하여 기존 리소스를 제거합니다.

```
oc delete namespaces open-cluster-management-agent open-cluster-management-agent-addon --wait=false
oc get crds | grep open-cluster-management.io | awk '{print $1}' | xargs oc delete crds --wait=false
oc get crds | grep open-cluster-management.io | awk '{print $1}' | xargs oc patch crds --type=merge -p '{"metadata":{"finalizers": []}}'
```

1.9. VMWARE VSPHERE에서 클러스터 생성 문제 해결

VMware vSphere에서 Red Hat OpenShift Container Platform 클러스터를 생성할 때 문제가 발생하는 경우 다음 문제 해결 정보를 참조하십시오.

참고: 경우에 따라 VMware vSphere에서 클러스터 생성 프로세스가 실패하면 해당 링크가 로그를 볼 수 없습니다. 이 경우 **hive-controllers** Pod의 로그를 확인하여 문제를 식별할 수 있습니다. **hive-controllers** 로그는 **hive** 네임스페이스에 있습니다.

1.9.1. 인증서 IP SAN 오류와 함께 관리형 클러스터 생성 실패

1.9.1.1. 증상: 관리형 클러스터 생성 실패 인증서 IP SAN 오류

VMware vSphere에 새 Red Hat OpenShift Container Platform 클러스터를 생성하면 클러스터가 인증서 IP SAN 오류를 나타내는 오류 메시지와 함께 실패합니다.

1.9.1.2. 문제 확인: 관리형 클러스터 생성 실패 인증서 IP SAN 오류 발생

관리 클러스터의 배포가 실패하고 배포 로그에 다음 오류를 반환합니다.

```
time="2020-08-07T15:27:55Z" level=error msg="Error: error setting up new vSphere SOAP client: Post https://147.1.1.1/sdk: x509: cannot validate certificate for xx.xx.xx.xx because it doesn't contain any IP SANs"
```

```
time="2020-08-07T15:27:55Z" level=error
```

1.9.1.3. 문제 해결: 관리형 클러스터 생성 실패 인증서 IP SAN 오류 발생

자격 증명의 IP 주소 대신 VMware vCenter 서버 정규화된 호스트 이름을 사용합니다. IP SAN을 포함하도록 VMware vCenter CA 인증서를 업데이트할 수도 있습니다.

1.9.2. 알 수 없는 인증 기관과 함께 관리되는 클러스터 생성 실패

1.9.2.1. 증상: 관리형 클러스터 생성이 알 수 없는 인증 기관과 함께 실패합니다.

VMware vSphere에 새 Red Hat OpenShift Container Platform 클러스터를 생성하면 인증서가 알 수 없는 기관에서 서명되므로 클러스터가 실패합니다.

1.9.2.2. 문제 확인: 관리형 클러스터 생성이 알 수 없는 인증 기관과 함께 실패했습니다.

관리 클러스터의 배포가 실패하고 배포 로그에 다음 오류를 반환합니다.

```
Error: error setting up new vSphere SOAP client: Post https://vspherehost.com/sdk: x509: certificate signed by unknown authority"
```

1.9.2.3. 문제 해결: 관리형 클러스터 생성이 알 수 없는 인증 기관과 함께 실패했습니다.

인증 정보를 생성할 때 인증 기관에서 올바른 인증서를 입력했는지 확인합니다.

1.9.3. 만료된 인증서로 관리되는 클러스터 생성 실패

1.9.3.1. 증상: 관리형 클러스터 생성 실패 **with expired certificate**

VMware vSphere에 새 Red Hat OpenShift Container Platform 클러스터를 생성하면 인증서가 만료되었거나 아직 유효하지 않기 때문에 클러스터가 실패합니다.

1.9.3.2. 문제 확인: 관리형 클러스터 생성이 만료된 인증서로 실패했습니다.

관리 클러스터의 배포가 실패하고 배포 로그에 다음 오류를 반환합니다.

```
x509: certificate has expired or is not yet valid
```

1.9.3.3. 문제 해결: **Managed cluster creation fails with expired certificate**

ESXi 호스트의 시간이 동기화되었는지 확인합니다.

1.9.4. 관리형 클러스터 생성이 실패하여 태그 지정에 대한 권한이 부족함

1.9.4.1. 증상: 관리형 클러스터 생성이 실패하고 태그 지정에 필요한 권한이 충분하지 않음

VMware vSphere에 새 Red Hat OpenShift Container Platform 클러스터를 생성하면 태그 지정에 사용할 수 있는 권한이 부족하기 때문에 클러스터가 실패합니다.

1.9.4.2. 문제 확인: 관리형 클러스터 생성 실패와 태그 지정에 대한 권한이 충분하지 않음

관리 클러스터의 배포가 실패하고 배포 로그에 다음 오류를 반환합니다.

```
time="2020-08-07T19:41:58Z" level=debug msg="vsphere_tag_category.category: Creating..."
time="2020-08-07T19:41:58Z" level=error
time="2020-08-07T19:41:58Z" level=error msg="Error: could not create category: POST
https://vspherehost.com/rest/com/vmware/cis/tagging/category: 403 Forbidden"
time="2020-08-07T19:41:58Z" level=error
time="2020-08-07T19:41:58Z" level=error msg=" on ../tmp/openshift-install-436877649/main.tf line
54, in resource \"vsphere_tag_category\" \"category\":"
time="2020-08-07T19:41:58Z" level=error msg=" 54: resource \"vsphere_tag_category\" \"category\"
{"
```

1.9.4.3. 문제 해결: 관리형 클러스터 생성 실패와 태그 지정에 대한 권한이 충분하지 않음

VMware vCenter 필수 계정 권한이 올바른지 확인합니다. 자세한 내용은 [이미지 레지스트리](#) 를 참조하십시오.

1.9.5. 잘못된 dnsVIP로 관리되는 클러스터 생성 실패

1.9.5.1. 증상: 관리형 클러스터 생성 실패와 함께 잘못된 dnsVIP

VMware vSphere에 새 Red Hat OpenShift Container Platform 클러스터를 생성하면 유효하지 않은 dnsVIP가 있기 때문에 클러스터가 실패합니다.

1.9.5.2. 문제 확인: 관리형 클러스터 생성 실패 잘못된 dnsVIP

VMware vSphere를 사용하여 새 관리 클러스터를 배포하려고 할 때 다음 메시지가 표시되면 VMware Installer Provisioned Infrastructure (IPI)를 지원하지 않는 이전 OpenShift Container Platform 릴리스 이미지가 있기 때문입니다.

```
failed to fetch Master Machines: failed to load asset \\\\"Install Config\\\": invalid \\\\\"install-
config.yaml\\\" file: platform.vsphere.dnsVIP: Invalid value: \\\\\"\\\": \\\\\"\\\" is not a valid IP
```

1.9.5.3. 문제 해결: Managed 클러스터 생성 실패 잘못된 dnsVIP

최신 버전의 OpenShift Container Platform에서 VMware Installer Provisioned Infrastructure를 지원하는 릴리스 이미지를 선택합니다.

1.9.6. 잘못된 네트워크 유형으로 관리 클러스터 생성 실패

1.9.6.1. 증상: 관리형 클러스터 생성이 잘못된 네트워크 유형과 함께 실패합니다.

VMware vSphere에서 새 Red Hat OpenShift Container Platform 클러스터를 생성하면 잘못된 네트워크 유형이 지정되어 있기 때문에 클러스터가 실패합니다.

1.9.6.2. 문제 확인: 관리형 클러스터 생성 실패 잘못된 네트워크 유형

VMware vSphere를 사용하여 새 관리 클러스터를 배포하려고 할 때 다음 메시지가 표시되면 VMware Installer Provisioned Infrastructure (IPI)를 지원하지 않는 이전 OpenShift Container Platform 이미지가 있기 때문입니다.

```
time="2020-08-11T14:31:38-04:00" level=debug msg="vsphereprivate_import_ova.import:
```



```

Creating...
time="2020-08-11T14:31:39-04:00" level=error
time="2020-08-11T14:31:39-04:00" level=error msg="Error: rpc error: code = Unavailable desc = transport is closing"
time="2020-08-11T14:31:39-04:00" level=error
time="2020-08-11T14:31:39-04:00" level=error
time="2020-08-11T14:31:39-04:00" level=fatal msg="failed to fetch Cluster: failed to generate asset \"Cluster\": failed to create cluster: failed to apply Terraform: failed to complete the change"

```

1.9.6.3. 문제 해결: 관리형 클러스터 생성 실패 잘못된 네트워크 유형

지정된 VMware 클러스터에 유효한 VMware vSphere 네트워크 유형을 선택합니다.

1.9.7. 관리 클러스터 생성 실패 오류 처리 디스크 변경

1.9.7.1. 증상: 디스크 처리 디스크 변경으로 인해 VMware vSphere 관리 클러스터 추가 실패

VMware vSphere에 새 Red Hat OpenShift Container Platform 클러스터를 생성하면 디스크 변경 처리 시 오류가 있기 때문에 클러스터가 실패합니다.

1.9.7.2. 문제 확인: 오류 처리 디스크 변경으로 인해 VMware vSphere 관리 클러스터 추가 실패

다음과 유사한 메시지가 로그에 표시됩니다.

```

ERROR
ERROR Error: error reconfiguring virtual machine: error processing disk changes post-clone: disk.0: ServerFaultCode: NoPermission: RESOURCE (vm-71:2000), ACTION (queryAssociatedProfile): RESOURCE (vm-71), ACTION (PolicyIDByVirtualDisk)

```

1.9.7.3. 문제 해결: 오류 처리 디스크 변경으로 인해 VMware vSphere 관리 클러스터 추가 실패

VMware vSphere 클라이언트를 사용하여 *프로필 중심 스토리지 권한에 대한 모든 권한을* 사용자에게 부여합니다.

1.10. 신뢰할 수 없는 권한 오류가 있는 RED HAT OPENSTACK PLATFORM에서 관리형 클러스터 생성 실패

Red Hat OpenStack Platform에서 Red Hat OpenShift Container Platform 클러스터를 생성할 때 문제가 발생하는 경우 다음 문제 해결 정보를 참조하여 문제를 해결하는지 확인하십시오.

1.10.1. 증상: 관리형 클러스터 생성이 권한 없는 오류와 함께 실패합니다.

자체 서명된 인증서를 사용하여 Red Hat OpenStack Platform에 새 Red Hat OpenShift Container Platform 클러스터를 생성한 후 신뢰할 수 없는 권한 오류를 나타내는 오류 메시지와 함께 클러스터가 실패합니다.

1.10.2. 문제 확인: Managed cluster creation failed with unknown authority error

관리 클러스터의 배포에 실패하고 다음 오류 메시지를 반환합니다.

X509: 알 수 없는 기관에서 서명한 인증서

1.10.3. 문제 해결: Managed cluster creation fails with unknown authority error

다음 파일이 올바르게 구성되었는지 확인합니다.

1. **clouds.yaml** 파일은 **cacert** 매개변수에 **ca.crt** 파일의 경로를 지정해야 합니다. **cacert** 매개변수는 ignition shim을 생성할 때 OpenShift 설치 프로그램에 전달됩니다. 다음 예제를 참조하십시오.

```
clouds:
  openstack:
    cacert: "/etc/pki/ca-trust/source/anchors/ca.crt"
```

2. **certificatesSecretRef** parameter는 **ca.crt** 파일과 일치하는 파일 이름이 있는 보안을 참조해야 합니다. 다음 예제를 참조하십시오.

```
spec:
  baseDomain: dev09.red-chesterfield.com
  clusterName: txue-osspoke
  platform:
    openstack:
      cloud: openstack
      credentialsSecretRef:
        name: txue-osspoke-openstack-creds
      certificatesSecretRef:
        name: txue-osspoke-openstack-certificatebundle
```

일치하는 파일 이름으로 보안을 생성하려면 다음 명령을 실행합니다.

```
oc create secret generic txue-osspoke-openstack-certificatebundle --from-file=ca.crt=ca.crt.pem -n $CLUSTERNAME
```

3. **ca.crt** 파일의 크기는 63000바이트 미만이어야 합니다.

1.11. OPENSIFT CONTAINER PLATFORM 버전 3.11 클러스터 가져오기 장애 문제 해결

1.11.1. 증상: OpenShift Container Platform 버전 3.11 클러스터 가져오기 실패

Red Hat OpenShift Container Platform 버전 3.11 클러스터를 가져오려고 하면 가져오기에 실패하고 다음 콘텐츠와 유사한 로그 메시지가 표시됩니다.

```
customresourcedefinition.apiextensions.k8s.io/klusterlets.operator.open-cluster-management.io
configured
clusterrole.rbac.authorization.k8s.io/klusterlet configured
clusterrole.rbac.authorization.k8s.io/open-cluster-management:klusterlet-admin-aggregate-clusterrole
configured
clusterrolebinding.rbac.authorization.k8s.io/klusterlet configured
namespace/open-cluster-management-agent configured
secret/open-cluster-management-image-pull-credentials unchanged
serviceaccount/klusterlet configured
deployment.apps/klusterlet unchanged
klusterlet.operator.open-cluster-management.io/klusterlet configured
Error from server (BadRequest): error when creating "STDIN": Secret in version "v1" cannot be
handled as a Secret:
```

```
v1.Secret.ObjectMeta:
v1.ObjectMeta.TypeMeta: Kind: Data: decode base64: illegal base64 data at input byte 1313, error
found in #10 byte of ...|dhruy45="}, "kind": "..., bigger context
...|tye56u56u568yu07i67i67i67o556574i"}, "kind": "Secret", "metadata": {"annotations": {"kube|...
```

1.11.2. 문제 확인: OpenShift Container Platform 버전 3.11 클러스터 가져오기 실패

이는 **kubectl** 명령줄 도구의 설치된 버전이 1.11 또는 이전 버전이므로 종종 발생합니다. 다음 명령을 실행하여 실행 중인 **kubectl** 명령줄 도구 버전을 확인합니다.

```
kubectl version
```

반환된 데이터에 버전 1.11 또는 이전 버전이 나열된 경우 *문제 해결 방법 (OpenShift Container Platform 버전 3.11 클러스터 가져오기 실패)*을 완료합니다.

1.11.3. 문제 해결: OpenShift Container Platform 버전 3.11 클러스터 가져오기 실패

다음 절차 중 하나를 완료하여 이 문제를 해결할 수 있습니다.

- **kubectl** 명령줄 도구의 최신 버전을 설치합니다.
 1. Kubernetes 문서에서 [Install and Set Up kubectl](#) 툴의 최신 버전을 다운로드합니다.
 2. **kubectl** 툴을 업그레이드한 후 클러스터를 다시 가져옵니다.
- 가져오기 명령이 포함된 파일을 실행합니다.
 1. [CLI를 사용하여 관리 클러스터 가져오기](#) 절차를 시작합니다.
 2. 클러스터를 가져올 명령을 생성할 때 **import.yaml** 이라는 YAML 파일에 해당 명령을 복사합니다.
 3. 다음 명령을 실행하여 파일에서 클러스터를 다시 가져옵니다.

```
oc apply -f import.yaml
```

1.12. 인증서 변경 후 가져온 클러스터 문제 해결

사용자 정의 **apiserver** 인증서 설치가 지원되지만 인증서 정보를 변경하기 전에 가져온 하나 이상의 클러스터는 **오프라인** 상태입니다.

1.12.1. 증상: 인증서 변경 후 오프라인 클러스터

인증서 보안 업데이트 절차를 완료한 후 온라인 클러스터 중 하나 이상에 이제 콘솔에 **오프라인** 상태가 표시됩니다.

1.12.2. 문제 확인: 인증서 변경 후 오프라인 클러스터

사용자 정의 API 서버 인증서에 대한 정보를 업데이트한 후 새 인증서를 가져 와서 실행 중인 클러스터는 이제 **오프라인** 상태가 됩니다.

인증서가 문제가 있음을 나타내는 오류는 오프라인 관리 클러스터의 **open-cluster-management-agent** 네임스페이스에 있는 Pod 로그에서 확인할 수 있습니다. 다음 예제는 로그에 표시되는 오류와 유사합니다.

다음 **work-agent** 로그를 참조하십시오.

```
E0917 03:04:05.874759    1 manifestwork_controller.go:179] Reconcile work test-1-klusterlet-
addon-workmgr fails with err: Failed to update work status with err Get "https://api.aaa-
ocp.dev02.location.com:6443/apis/cluster.management.io/v1/namespaces/test-1/manifestworks/test-
1-klusterlet-addon-workmgr": x509: certificate signed by unknown authority
E0917 03:04:05.874887    1 base_controller.go:231] "ManifestWorkAgent" controller failed to sync
"test-1-klusterlet-addon-workmgr", err: Failed to update work status with err Get "api.aaa-
ocp.dev02.location.com:6443/apis/cluster.management.io/v1/namespaces/test-1/manifestworks/test-
1-klusterlet-addon-workmgr": x509: certificate signed by unknown authority
E0917 03:04:37.245859    1 reflector.go:127] k8s.io/client-go@v0.19.0/tools/cache/reflector.go:156:
Failed to watch *v1.ManifestWork: failed to list *v1.ManifestWork: Get "api.aaa-
ocp.dev02.location.com:6443/apis/cluster.management.io/v1/namespaces/test-1/manifestworks?
resourceVersion=607424": x509: certificate signed by unknown authority
```

다음 **registration-agent** 로그를 참조하십시오.

```
I0917 02:27:41.525026    1 event.go:282] Event(v1.ObjectReference{Kind:"Namespace",
Namespace:"open-cluster-management-agent", Name:"open-cluster-management-agent", UID:"",
APIVersion:"v1", ResourceVersion:"", FieldPath:""}): type: 'Normal' reason:
'ManagedClusterAvailableConditionUpdated' update managed cluster "test-1" available condition to
"True", due to "Managed cluster is available"
E0917 02:58:26.315984    1 reflector.go:127] k8s.io/client-go@v0.19.0/tools/cache/reflector.go:156:
Failed to watch *v1beta1.CertificateSigningRequest: Get "https://api.aaa-
ocp.dev02.location.com:6443/apis/cluster.management.io/v1/managedclusters?
allowWatchBookmarks=true&fieldSelector=metadata.name%3Dtest-
1&resourceVersion=607408&timeout=9m33s&timeoutSeconds=573&watch=true": x509: certificate
signed by unknown authority
E0917 02:58:26.598343    1 reflector.go:127] k8s.io/client-go@v0.19.0/tools/cache/reflector.go:156:
Failed to watch *v1.ManagedCluster: Get "https://api.aaa-
ocp.dev02.location.com:6443/apis/cluster.management.io/v1/managedclusters?
allowWatchBookmarks=true&fieldSelector=metadata.name%3Dtest-
1&resourceVersion=607408&timeout=9m33s&timeoutSeconds=573&watch=true": x509: certificate
signed by unknown authority
E0917 02:58:27.613963    1 reflector.go:127] k8s.io/client-go@v0.19.0/tools/cache/reflector.go:156:
Failed to watch *v1.ManagedCluster: failed to list *v1.ManagedCluster: Get "https://api.aaa-
ocp.dev02.location.com:6443/apis/cluster.management.io/v1/managedclusters?
allowWatchBookmarks=true&fieldSelector=metadata.name%3Dtest-
1&resourceVersion=607408&timeout=9m33s&timeoutSeconds=573&watch=true": x509: certificate
signed by unknown authority
```

1.12.3. 문제 해결: 인증서 변경 후 오프라인 클러스터

관리 클러스터가 로컬 클러스터 이거나 Red Hat Advanced Cluster Management for Kubernetes를 사용하여 관리되는 클러스터를 생성한 경우 관리 클러스터를 다시 가져오는 데 10분 이상 기다려야 합니다.

관리형 클러스터를 즉시 다시 가져오려면 hub 클러스터에서 관리형 클러스터 가져오기 보안을 삭제하고 Red Hat Advanced Cluster Management를 사용하여 다시 가져올 수 있습니다. 다음 명령을 실행합니다.

```
oc delete secret -n <cluster_name> <cluster_name>-import
```

& **<cluster_name>** 을 가져올 관리형 클러스터 이름으로 바꿉니다.

Red Hat Advanced Cluster Management를 사용하여 가져온 관리형 클러스터를 다시 가져오려면 다음 단계를 완료하여 관리 클러스터를 다시 가져옵니다.

1. hub 클러스터에서 다음 명령을 실행하여 관리형 클러스터 가져오기 보안을 다시 생성합니다.

```
oc delete secret -n <cluster_name> <cluster_name>-import
```

<cluster_name >을 가져올 관리형 클러스터 이름으로 바꿉니다.

2. hub 클러스터에서 다음 명령을 실행하여 관리 대상 클러스터 가져오기 보안을 YAML 파일에 노출합니다.

```
oc get secret -n <cluster_name> <cluster_name>-import -ojsonpath='{.data.import\.yaml}' | base64 --decode > import.yaml
```

<cluster_name >을 가져올 관리형 클러스터 이름으로 바꿉니다.

3. 관리형 클러스터에서 다음 명령을 실행하여 **import.yaml** 파일을 적용합니다.

```
oc apply -f import.yaml
```

참고: 이전 단계에서는 관리 대상 클러스터를 hub 클러스터에서 분리하지 않습니다. 이 단계는 새 인증서 정보를 포함하여 관리형 클러스터의 현재 설정으로 필요한 매니페스트를 업데이트합니다.

1.13. 클러스터를 삭제한 후 네임스페이스가 남아 있음

관리형 클러스터를 제거하면 일반적으로 네임스페이스가 클러스터 제거 프로세스의 일부로 제거됩니다. 드문 경우지만 네임스페이스는 일부 아티팩트와 함께 남아 있습니다. 이 경우 네임스페이스를 수동으로 제거해야 합니다.

1.13.1. 증상: 클러스터를 삭제한 후에도 네임스페이스가 유지됩니다.

관리형 클러스터를 제거하면 네임스페이스가 제거되지 않습니다.

1.13.2. 문제 해결: 클러스터를 삭제한 후에도 네임스페이스가 유지됩니다.

네임스페이스를 수동으로 제거하려면 다음 단계를 완료합니다.

1. 다음 명령을 실행하여 <cluster_name> 네임스페이스에 남아 있는 리소스 목록을 생성합니다.

```
oc api-resources --verbs=list --namespaced -o name | grep -E '^secrets|^serviceaccounts|^managedclusteraddons|^roles|^rolebindings|^manifestworks|^lease|^managedclusterinfo|^appliedmanifestworks|^clusteroauths' | xargs -n 1 oc get --show-kind -ignore-not-found -n <cluster_name>
```

cluster_name 을 삭제하려는 클러스터의 네임스페이스 이름으로 바꿉니다.

2. 다음 명령을 입력하여 목록을 편집하여 삭제 상태가 아닌 목록에서 식별된 각 리소스를 **삭제**합니다.

```
oc edit <resource_kind> <resource_name> -n <namespace>
```

resource_kind 를 리소스 종류로 교체합니다. **resource_name** 을 리소스 이름으로 교체합니다. **namespace** 를 리소스의 네임스페이스 이름으로 바꿉니다.

3. 메타데이터의 **에서** 종료자 속성을 찾습니다.
4. vi editor **dd** 명령을 사용하여 비Kubernetes 종료자를 삭제합니다.
5. 목록을 저장하고 **:wq** 명령을 입력하여 **vi** 편집기를 종료합니다.
6. 다음 명령을 입력하여 네임스페이스를 삭제합니다.

```
oc delete ns <cluster-name>
```

cluster-name 을 삭제하려는 네임스페이스의 이름으로 바꿉니다.

1.14. 클러스터를 가져올 때 **AUTO-IMPORT-SECRET-EXISTS** 오류

자동 가져오기 시크릿을 읽는 오류 메시지와 함께 클러스터 가져오기가 실패합니다.

1.14.1. 증상: 클러스터를 가져올 때 자동 가져오기 시크릿이 존재하는 경우 오류

관리를 위해 하이브 클러스터를 가져오는 경우 **자동 가져오기-비밀번호 오류**가 이미 존재합니다.

1.14.2. 문제 해결: 클러스터를 가져올 때 자동 가져오기-**secret-exists** 오류

이 문제는 이전에 Red Hat Advanced Cluster Management에서 관리하던 클러스터를 가져오려고 할 때 발생합니다. 이 경우 클러스터를 다시 가져오려고 할 때 보안이 충돌합니다.

이 문제를 해결하려면 다음 단계를 완료하십시오.

1. 기존 **auto-import-secret** 을 수동으로 삭제하려면 hub 클러스터에서 다음 명령을 실행합니다.

```
oc delete secret auto-import-secret -n <cluster-namespace>
```

cluster-namespace 를 클러스터 네임스페이스로 교체합니다.

2. 대상 관리 클러스터를 허브 클러스터로 가져오는 절차를 사용하여 클러스터를 다시 가져옵니다.

클러스터를 가져옵니다.

1.15. 클러스터 상태 변경 문제 해결

환경 또는 클러스터를 수동으로 변경하지 않고 관리형 클러스터의 상태가 **오프라인** 과 **사용 가능** 간에 전환됩니다.

1.15.1. 증상: 클러스터 상태가 오프라인에서 사용 가능으로 변경됩니다.

관리 클러스터를 hub 클러스터에 연결하는 네트워크가 불안정할 때 **오프라인** 과 **사용 가능한** 허브 클러스터 사이클에 의해 보고되는 관리 클러스터의 상태가 설정됩니다.

허브 클러스터와 관리형 클러스터 간의 연결은 **leaseDurationSeconds** 간격 값에 유효한 리스를 통해 유지 관리됩니다. **leaseDurationSeconds** 값의 5번 연속 시도 내에서 리스를 검증하지 않으면 클러스터가 **오프라인**으로 표시됩니다.

예를 들어, 리스 **DurationSeconds** 간격이 **60초** 인 5분 후에 클러스터가 **오프라인** 상태로 표시됩니다. 이 구성은 연결 문제 또는 대기 시간과 같은 이유로 부적절하여 불안정성을 유발할 수 있습니다.

1.15.2. 문제 해결: 클러스터 상태가 오프라인에서 사용 가능으로 변경

5개의 검증 시도는 기본값이며 변경할 수 없지만 **leaseDurationSeconds** 간격을 변경할 수 있습니다.

클러스터를 **오프라인**으로 표시할 시간(분)을 확인한 다음 해당 값을 60으로 곱하여 초로 변환합니다. 그런 다음 기본 5개의 시도로 나눕니다. 그 결과 **리스DurationSeconds** 값이 됩니다.

1. 다음 명령을 입력하여 hub 클러스터에서 **ManagedCluster** 사양을 편집하지만 **cluster-name** 을 관리 클러스터 이름으로 교체합니다.

```
oc edit managedcluster <cluster-name>
```

2. 다음 샘플 YAML에 표시된 대로 **ManagedCluster** 사양에서 **leaseDurationSeconds** 값을 늘립니다.

```
apiVersion: cluster.open-cluster-management.io/v1
kind: ManagedCluster
metadata:
  name: <cluster-name>
spec:
  hubAcceptsClient: true
  leaseDurationSeconds: 60
```

3. 파일을 저장하고 적용합니다.

1.16. 보류 중 또는 실패 상태의 콘솔에서 클러스터 문제 해결

생성한 클러스터의 **보류 중** 상태 또는 **실패** 상태를 확인하는 경우 절차에 따라 문제를 해결합니다.

1.16.1. 증상: 보류 중 또는 실패한 상태의 콘솔에서 클러스터

Kubernetes 콘솔용 Red Hat Advanced Cluster Management for Kubernetes 콘솔을 사용하여 새 클러스터를 생성한 후 클러스터는 *Pending* 상태로 전환되지 않거나 **실패** 상태를 표시하지 않습니다.

1.16.2. 문제 확인: 보류 중 또는 실패 상태의 콘솔에서 클러스터

클러스터에 *Failed* 상태가 표시되면 클러스터의 세부 정보 페이지로 이동하여 제공된 로그 링크를 따릅니다. 로그를 찾을 수 없거나 클러스터에서 *Pending* 상태를 표시하는 경우 다음 절차에 따라 로그를 확인합니다.

- 절차 1

1. hub 클러스터에서 다음 명령을 실행하여 새 클러스터의 네임스페이스에서 생성된 Kubernetes 포드의 이름을 확인합니다.

```
oc get pod -n <new_cluster_name>
```

new_cluster_name 을 생성한 클러스터 이름으로 교체합니다.

2. 이름에 **provision** 문자열이 포함된 Pod가 나열되지 않은 경우 2 절차로 계속 진행합니다. 제목에 **프로비저닝** 이 있는 Pod가 있는 경우 hub 클러스터에서 다음 명령을 실행하여 해당 Pod의 로그를 확인합니다.

```
oc logs <new_cluster_name_provision_pod_name> -n <new_cluster_name> -c hive
```

`new_cluster_name_provision_pod_name` 을 생성한 클러스터의 이름으로 교체한 다음 `provision` 가 포함된 Pod 이름으로 교체합니다.

3. 로그에서 문제의 원인을 설명할 수 있는 오류를 검색합니다.

- 절차 2

이름에 `provision` 가 있는 Pod가 없는 경우 프로세스의 앞부분에서 문제가 발생했습니다. 로그를 확인하려면 다음 절차를 완료합니다.

1. hub 클러스터에서 다음 명령을 실행합니다.

```
oc describe clusterdeployments -n <new_cluster_name>
```

`new_cluster_name` 을 생성한 클러스터 이름으로 교체합니다. 클러스터 설치 로그에 대한 자세한 내용은 Red Hat OpenShift 문서의 [설치 로그 수집](#) 을 참조하십시오.

2. 리소스의 `Status.Conditions.Message` 및 `Status.Conditions.Reason` 항목에 문제에 대한 추가 정보가 있는지 확인합니다.

1.16.3. 문제 해결: 보류 중 또는 실패한 상태의 콘솔의 클러스터

로그에서 오류를 확인한 후 클러스터를 삭제하고 다시 생성하기 전에 오류를 해결하는 방법을 확인합니다.

다음 예제에서는 지원되지 않는 영역을 선택하는 경우 가능한 로그 오류와 이를 해결하는 데 필요한 작업을 제공합니다.

```
No subnets provided for zones
```

클러스터를 생성할 때 지원되지 않는 리전 내에서 하나 이상의 영역을 선택했습니다. 클러스터를 다시 생성하여 문제를 해결할 때 다음 작업 중 하나를 완료합니다.

- 리전 내에서 다른 영역을 선택합니다.
- 다른 영역이 나열된 경우 지원을 제공하지 않는 영역을 생략합니다.
- 클러스터의 다른 리전을 선택합니다.

로그에서 문제를 확인한 후 클러스터를 제거하고 다시 생성합니다.

[클러스터 생성](#) 에 대한 자세한 내용은 클러스터 생성을 참조하십시오.

1.17. 애플리케이션 GIT 서버 연결 문제 해결

`open-cluster-management` 네임스페이스의 로그에 Git 리포지토리를 복제하지 못했습니다.

1.17.1. 증상: Git 서버 연결

`open-cluster-management` 네임스페이스의 서브스크립션 컨트롤러 Pod `다중cluster-hub-subscription-<random-characters>` 의 로그는 Git 리포지토리를 복제하지 못함을 나타냅니다. 알 수 없는 기관 오류로 서명된 `x509: 인증서` 또는 `10.0.0.1 Gateway` 오류가 표시됩니다.

1.17.2. 문제 해결: Git 서버 연결

중요: 이전 버전을 사용하는 경우 업그레이드합니다.

1. `apps.open-cluster-management.io_channels_crd.yaml` 을 동일한 파일 이름으로 저장합니다.
2. Red Hat Advanced Cluster Management 클러스터에서 다음 명령을 실행하여 파일을 적용합니다.

```
oc apply -f apps.open-cluster-management.io_channels_crd.yaml
```

3. **open-cluster-management** 네임스페이스에서 **advanced-cluster-management.<version, example 2.5.0>** CSV를 편집하고 다음 명령을 실행하고 편집합니다.

```
oc edit csv advanced-cluster-management.<version, example 2.5.0> -n open-cluster-management
```

다음 컨테이너를 찾습니다.

- **multicluster-operators-standalone-subscription**

- **multicluster-operators-hub-subscription**

컨테이너 이미지를 사용하려는 컨테이너로 교체합니다.

```
quay.io/open-cluster-management/multicluster-operators-subscription:<your image tag>
```

이번 업데이트에서는 **open-cluster-management** 네임스페이스에서 다음 Pod를 다시 생성합니다.

- **multicluster-operators-standalone-subscription-<random-characters>**

- **multicluster-operators-hub-subscription-<random-characters>**

4. 새 포드가 새 docker 이미지로 실행되고 있는지 확인합니다. 다음 명령을 실행한 다음 새 docker 이미지를 찾습니다.

```
oc get pod multicluster-operators-standalone-subscription-<random-characters> -n open-cluster-management -o yaml
oc get pod multicluster-operators-hub-subscription-<random-characters> -n open-cluster-management -o yaml
```

5. 관리 클러스터에서 이미지를 업데이트합니다.

hub 클러스터에서 다음 명령을 실행하여 **multicluster_operators_subscription** 키의 이미지 값을 사용하려는 이미지로 업데이트합니다.

```
oc edit configmap -n open-cluster-management mch-image-manifest-<version, example 2.5.0>
...
data:
  multicluster_operators_subscription: <your image with tag>
```

6. 기존 **multicluster-operators-hub-subscription** Pod를 다시 시작합니다.

```
oc delete pods -n open-cluster-management multicluster-operators-hub-subscription--<random-characters>
```

이렇게 하면 관리 클러스터에서 **open-cluster-management-agent-addon** 네임스페이스에서 **application-manager-`<random-characters>`** Pod가 다시 생성됩니다.

7. 새 포트가 새 docker 이미지로 실행되고 있는지 확인합니다.
8. 콘솔 또는 CLI를 통해 애플리케이션을 생성할 때 채널 사양에 'insecureSkipVerify: true'를 수동으로 추가합니다. 다음 예제를 참조하십시오.

```
apiVersion: apps.open-cluster-management.io/v1
kind: Channel
metadata:
labels:
  name: sample-channel
  namespace: sample
spec:
  type: GitHub
  pathname: <Git URL>
  insecureSkipVerify: true
```

1.18. GRAFANA 문제 해결

Grafana 탐색기에서 시간이 많이 소요되는 메트릭을 쿼리하면 **게이트웨이 시간 초과** 오류가 발생할 수 있습니다.

1.18.1. 증상: Grafana Explorer 게이트웨이 시간 제한

Grafana explorer에서 시간이 많이 걸리는 메트릭을 쿼리할 때 **게이트웨이 시간 제한** 오류가 발생하면 **open-cluster-management-observability** 네임스페이스의 Grafana로 인해 시간 초과가 발생할 수 있습니다.

1.18.2. 문제 해결: Grafana 구성

이 문제가 있는 경우 다음 단계를 완료합니다.

1. Grafana의 기본 구성에 예상 시간 제한 설정이 있는지 확인합니다.

- a. Grafana의 기본 시간 초과 설정을 확인하려면 다음 명령을 실행합니다.

```
oc get secret grafana-config -n open-cluster-management-observability -o jsonpath="{.data.grafana\.ini}" | base64 -d | grep dataproxy -A 4
```

다음과 같은 시간 초과 설정이 표시되어야 합니다.

```
[dataproxy]
timeout = 300
dial_timeout = 30
keep_alive_seconds = 300
```

- b. Grafana의 기본 데이터 소스 쿼리 시간 제한을 확인하려면 다음 명령을 실행합니다.

```
oc get secret/grafana-datasources -n open-cluster-management-observability -o jsonpath="{.data.datasources\.yaml}" | base64 -d | grep queryTimeout
```

다음과 같은 시간 초과 설정이 표시되어야 합니다.

```
queryTimeout: 300s
```

- Grafana의 기본 구성에 예상 시간 제한 설정이 있는 경우 다음 명령을 실행하여 **open-cluster-management-observability** 네임스페이스에서 Grafana를 구성할 수 있습니다.

```
oc annotate route grafana -n open-cluster-management-observability --overwrite
haproxy.router.openshift.io/timeout=300s
```

Grafana 페이지를 새로 고치고 메트릭을 다시 쿼리합니다. **게이트웨이 시간 초과** 오류가 더 이상 표시되지 않습니다.

1.19. 배치 규칙을 사용하여 선택하지 않은 로컬 클러스터 문제 해결

관리형 클러스터는 배치 규칙을 사용하여 선택되지만, 관리되는 허브 클러스터인 **local-cluster** 는 선택되지 않습니다. 배치 규칙 사용자에게 **local-cluster** 네임스페이스에서 **managedcluster** 리소스를 가져올 수 있는 권한이 부여되지 않습니다.

1.19.1. 증상: 관리형 클러스터로 선택되지 않은 로컬 클러스터 문제 해결

모든 관리형 클러스터는 배치 규칙을 사용하여 선택되지만 **local-cluster** 는 선택되지 않습니다. 배치 규칙 사용자에게 **local-cluster** 네임스페이스에서 **managedcluster** 리소스를 가져올 수 있는 권한이 부여되지 않습니다.

1.19.2. 문제 해결: 관리형 클러스터로 선택되지 않은 로컬 클러스터 문제 해결

이 문제를 해결하려면 **local-cluster** 네임스페이스에 **managedcluster** 관리 권한을 부여해야 합니다. 다음 단계를 완료합니다.

- 관리형 클러스터 목록에 로컬 클러스터 목록이 포함되어 있고 배치 규칙 결정 목록에 로컬 클러스터가 표시되지 않는지 확인합니다. 다음 명령을 실행하고 결과를 봅니다.

```
% oc get managedclusters
```

로컬 클러스터가 참여한 샘플 출력에서는 **PlacementRule** 의 YAML에 포함되지 않습니다.

```
NAME          HUB ACCEPTED  MANAGED CLUSTER URLS  JOINED  AVAILABLE
AGE
local-cluster true          True  True    56d
cluster1     true          True  True    16h
```

```
apiVersion: apps.open-cluster-management.io/v1
kind: PlacementRule
metadata:
  name: all-ready-clusters
  namespace: default
spec:
  clusterSelector: {}
status:
  decisions:
  - clusterName: cluster1
    clusterNamespace: cluster1
```

2. YAML 파일에서 역할을 생성하여 **local-cluster** 네임스페이스에 **managedcluster** 관리 권한을 부여합니다. 다음 예제를 참조하십시오.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: managedcluster-admin-user-zisis
  namespace: local-cluster
rules:
- apiGroups:
  - cluster.open-cluster-management.io
  resources:
  - managedclusters
  verbs:
  - get
```

3. **RoleBinding** 리소스를 생성하여 **local-cluster** 네임스페이스에 대한 배치 규칙 사용자에게 액세스 권한을 부여합니다. 다음 예제를 참조하십시오.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: managedcluster-admin-user-zisis
  namespace: local-cluster
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: managedcluster-admin-user-zisis
  namespace: local-cluster
subjects:
- kind: User
  name: zisis
  apiGroup: rbac.authorization.k8s.io
```

1.20. 애플리케이션 KUBERNETES 배포 버전 문제 해결

더 이상 사용되지 않는 Kubernetes **apiVersion** 이 있는 관리 클러스터는 지원되지 않을 수 있습니다. 더 이상 사용되지 않는 API 버전에 대한 자세한 내용은 [Kubernetes 문제](#)를 참조하십시오.

1.20.1. 증상: 애플리케이션 배포 버전

Subscription YAML 파일에서 하나 이상의 애플리케이션 리소스에서 더 이상 사용되지 않는 API를 사용하는 경우 다음 오류와 유사한 오류가 발생할 수 있습니다.

```
failed to install release: unable to build kubernetes objects from release manifest: unable to recognize
"": no matches for
kind "Deployment" in version "extensions/v1beta1"
```

또는 인스턴스에 **old.yaml** 이라는 YAML 파일에 새 Kubernetes API 버전이 있는 경우 다음과 같은 오류가 발생할 수 있습니다.

```
error: unable to recognize "old.yaml": no matches for kind "Deployment" in version
"deployment/v1beta1"
```

1.20.2. 문제 해결: 애플리케이션 배포 버전

1. 리소스에서 **apiVersion** 을 업데이트합니다. 예를 들어 서브스크립션 YAML 파일에 *Deployment* 종류 오류가 표시되면 **extensions/v1beta1** 에서 **apps/v1** 으로 **apiVersion** 을 업데이트해야 합니다.
다음 예제를 참조하십시오.

```
apiVersion: apps/v1
kind: Deployment
```

2. 관리형 클러스터에서 다음 명령을 실행하여 사용 가능한 버전을 확인합니다.

```
kubectl explain <resource>
```

3. **VERSION** 이 있는지 확인합니다.

1.21. 성능 저하된 조건이 있는 KLUSTRERLET 문제 해결

Klusterlet 성능 저하 조건은 관리 클러스터에서 Klusterlet 에이전트의 상태를 진단하는 데 도움이 될 수 있습니다. Klusterlet이 성능 저하 상태에 있는 경우 관리 클러스터의 Klusterlet 에이전트에 문제를 해결해야 하는 오류가 있을 수 있습니다. **True** 로 설정된 Klusterlet 성능 저하 상태에 대한 다음 정보를 참조하십시오.

1.21.1. 증상: Klusterlet이 성능 저하 상태에 있습니다.

관리되는 클러스터에 Klusterlet을 배포한 후 **KlusterletRegistrationDegraded** 또는 **KlusterletWorkDegraded** 조건이 *True* 임을 표시합니다.

1.21.2. 문제 확인: Klusterlet이 성능 저하된 상태에 있습니다.

1. 관리 클러스터에서 다음 명령을 실행하여 Klusterlet 상태를 확인합니다.

```
kubectl get klusterlets klusterlet -oyaml
```

2. **KlusterletRegistrationDegraded** 또는 **KlusterletWorkDegraded** 를 확인하여 조건이 **True** 로 설정되어 있는지 확인하십시오. 나열된 성능이 저하된 조건에 대해 문제를 해결하도록 진행합니다.

1.21.3. 문제 해결: Klusterlet이 성능 저하 상태에 있습니다.

다음 성능 저하 상태 목록과 이러한 문제를 해결하는 방법을 참조하십시오.

- 상태가 *True*인 **KlusterletRegistrationDegraded** 조건이 *True* 이고 조건 이유인 경우 *BootstrapSecretMissing*, **open-cluster-management-agent** 네임스페이스에서 부트스트랩 시크릿을 생성해야 합니다.
- **KlusterletRegistrationDegraded** 조건이 *True* 로 표시되고 조건 이유가 *BootstrapSecretError* 또는 *BootstrapSecretUnauthorized* 인 경우 현재 부트스트랩 시크릿이 유효하지 않습니다. 현재 부트스트랩 보안을 삭제하고 **open-cluster-management-agent** 네임스페이스에서 유효한 부트스트랩 보안을 다시 생성합니다.
- **KlusterletRegistrationDegraded** 및 **KlusterletWorkDegraded** 가 *True* 로 표시되고 조건 이유는 *HubKubeConfigSecretMissing* 이므로 Klusterlet을 삭제하고 다시 생성합니다.

- **KlusterletRegistrationDegraded** 및 **KlusterletWorkDegraded** 가 *True* 로 표시되고 조건 이유는 *ClusterNameMissing*, *HubConfigMissing*, *HubConfigSecretError*, *HubConfigSecretUnauthorized*, **open-cluster-management-agent** 네임스페이스에서 hub cluster kubeconfig 시크릿을 삭제합니다. 등록 에이전트는 새 허브 클러스터 kubeconfig 보안을 가져오기 위해 다시 부트스트랩합니다.
- **KlusterletRegistrationDegraded** 에 *True* 가 표시되고 조건 이유가 *GetRegistrationDeploymentFailed* 또는 *UnavailableRegistrationPod* 인 경우 상태 메시지를 확인하여 문제 세부 정보를 가져오고 해결하려고 할 수 있습니다.
- **KlusterletWorkDegraded** 에 *True* 가 표시되고 조건 이유가 *GetWorkDeploymentFailed* ,또는 *UnavailableWorkPod* 인 경우 상태 메시지를 확인하여 문제 세부 정보를 가져오고 해결하려고 할 수 있습니다.

1.22. 오브젝트 스토리지 채널 보안 문제 해결

SecretAccessKey 를 변경하면 오브젝트 스토리지 채널의 서브스크립션이 업데이트된 보안을 자동으로 가져올 수 없으며 오류가 표시됩니다.

1.22.1. 증상: 오브젝트 스토리지 채널 시크릿

오브젝트 스토리지 채널의 서브스크립션은 업데이트된 보안을 자동으로 가져올 수 없습니다. 이렇게 하면 서브스크립션 운영자가 리소스를 조정하고 오브젝트 스토리지에서 관리 클러스터에 리소스를 배포할 수 없습니다.

1.22.2. 문제 해결: 오브젝트 스토리지 채널 시크릿

보안을 생성하려면 인증 정보를 수동으로 입력한 다음 채널 내의 시크릿을 참조해야 합니다.

1. 서브스크립션 CR에 주석을 달아 서브스크립션 Operator에 단일 조정을 생성합니다. 다음 데이터 사양을 참조하십시오.

```
apiVersion: apps.open-cluster-management.io/v1
kind: Channel
metadata:
  name: deva
  namespace: ch-obj
  labels:
    name: obj-sub
spec:
  type: ObjectBucket
  pathname: http://ec2-100-26-232-156.compute-1.amazonaws.com:9000/deva
  sourceNamespaces:
    - default
  secretRef:
    name: dev
---
```

```
apiVersion: v1
kind: Secret
metadata:
  name: dev
  namespace: ch-obj
  labels:
    name: obj-sub
```

```
data:
  AccessKeyID: YWRtaW4=
  SecretAccessKey: cGFzc3dvcmRhZG1pbG==
```

- 테스트를 위해 **oc annotate** 를 실행합니다.

```
oc annotate appsub -n <subscription-namespace> <subscription-name> test=true
```

명령을 실행한 후 애플리케이션 콘솔로 이동하여 리소스가 관리 클러스터에 배포되었는지 확인할 수 있습니다. 또는 관리 클러스터에 로그인하여 지정된 네임스페이스에서 애플리케이션 리소스가 생성되었는지 확인할 수 있습니다.

1.23. 가시성 문제 해결

Observability 구성 요소를 설치한 후 구성 요소가 고착되어 **Installing** 상태가 표시됩니다.

1.23.1. 증상: MultiClusterObservability 리소스 상태가 중단됨

설치 후 Observability 상태가 Installing 상태에 있고 Observability CRD(사용자 정의 리소스 정의)를 생성하는 경우 **spec:storageConfig:storageClass** 매개변수에 정의된 값이 없을 수 있습니다. 또는 observability 구성 요소가 기본 **storageClass** 를 자동으로 검색하지만 스토리지 값이 없는 경우 구성 요소는 설치 상태와 함께 남아 있습니다.

1.23.2. 문제 해결: MultiClusterObservability 리소스 상태 정지

이 문제가 있는 경우 다음 단계를 완료합니다.

- 관찰 기능 구성 요소가 설치되었는지 확인합니다.
 - multicluster-observability-operator** 가 있는지 확인하려면 다음 명령을 실행합니다.

```
kubectl get pods -n open-cluster-management|grep observability
```

- 적절한 CRD가 있는지 확인하려면 다음 명령을 실행합니다.

```
kubectl get crd|grep observ
```

구성 요소를 활성화하기 전에 다음 CRD를 표시해야 합니다.

```
multiclusterobservabilities.observability.open-cluster-management.io
observabilityaddons.observability.open-cluster-management.io
observatoria.core.observatorium.io
```

- 베어 메탈 클러스터에 대한 자체 storageClass를 생성하는 경우 **NFS를 사용하여 영구 스토리지를 참조하십시오.**
- 관찰 기능 구성 요소가 기본 storageClass를 찾을 수 있도록 **multicluster-observability-operator** 사용자 정의 리소스 정의에서 **storageClass** 매개변수를 업데이트합니다. 매개변수는 다음 값과 유사합니다.

```
storageclass.kubernetes.io/is-default-class: "true"
```

설치가 완료되면 observability 구성 요소 상태가 *Ready* 상태로 업데이트됩니다. 설치가 완료되지 않으면 *Fail* 상태가 표시됩니다.

1.24. OPENSIFT 모니터링 서비스 문제 해결

관리형 클러스터의 관찰 가능 서비스는 OpenShift Container Platform 모니터링 스택에서 메트릭을 스크랩해야 합니다. OpenShift Container Platform 모니터링 스택이 준비되지 않은 경우 **metrics-collector** 가 설치되지 않습니다.

1.24.1. 증상: OpenShift 모니터링 서비스가 준비되지 않음

endpoint-observability-operator-x Pod는 **openshift-monitoring** 네임스페이스에서 **prometheus-k8s** 서비스를 사용할 수 있는지 확인합니다. **openshift-monitoring** 네임스페이스에 서비스가 없으면 **metrics-collector** 가 배포되지 않습니다. **prometheus** 리소스를 가져오는 데 실패 라는 오류 메시지가 표시될 수 있습니다.

1.24.2. 문제 해결: OpenShift 모니터링 서비스가 준비되지 않음

이 문제가 있는 경우 다음 단계를 완료합니다.

1. OpenShift Container Platform 클러스터에 로그인합니다.
2. **openshift-monitoring** 네임스페이스에 액세스하여 **prometheus-k8s** 서비스를 사용할 수 있는지 확인합니다.
3. 관리 클러스터의 **open-cluster-management-addon-observability** 네임스페이스에서 **endpoint-observability-operator-x** Pod를 재시작합니다.

1.25. METRICS-COLLECTOR 문제 해결

관리 클러스터에서 **observability-client-ca-certificate** 시크릿이 새로 교체되지 않으면 내부 서버 오류가 발생할 수 있습니다.

1.25.1. 증상: metrics-collector에서 observability-client-ca-certificate를 확인할 수 없음

메트릭을 사용할 수 없는 관리형 클러스터가 있을 수 있습니다. 이 경우 **metrics-collector** 배포에서 다음 오류가 발생할 수 있습니다.

```
error: response status code is 500 Internal Server Error, response body is x509: certificate signed by unknown authority (possibly because of "crypto/rsa: verification error" while trying to verify candidate authority certificate "observability-client-ca-certificate")
```

1.25.2. 문제 해결: metrics-collector에서 observability-client-ca-certificate를 확인할 수 없음

이 문제가 있는 경우 다음 단계를 완료합니다.

1. 관리형 클러스터에 로그인합니다.
2. **open-cluster-management-addon-observability** 네임스페이스에 있는 **observability-open-cluster-management.io-observability-signer-client-cert** 라는 시크릿을 삭제합니다. 다음 명령을 실행합니다.


```
oc delete secret observability-controller-open-cluster-management.io-observability-signer-client-cert -n open-cluster-management-addon-observability
```

참고: **observability-controller-open-cluster-management.io-observability-signer-client-cert** 는 새 인증서를 사용하여 자동으로 다시 생성됩니다.

metrics-collector 배포가 다시 생성되고 **observability-controller-open-cluster-management.io-observability-signer-client-cert** 시크릿이 업데이트되었습니다.

1.26. POSTGRESQL 공유 메모리 오류 문제 해결

대규모 환경이 있는 경우 검색 결과에 영향을 미치는 PostgreSQL 공유 메모리 오류와 애플리케이션의 토 폴로지 보기가 발생할 수 있습니다.

1.26.1. 증상: PostgreSQL 공유 메모리 오류

search-api 로그에 다음과 같은 오류 메시지가 표시됩니다. **ERROR: could not resize shared memory segment "/PostgreSQL.1083654800" to 25031264 bytes: No space left on device (SQLSTATE 53100)**

1.26.2. 문제 해결: PostgreSQL 공유 메모리 오류

문제를 해결하려면 **search-postgres** ConfigMap에 있는 PostgreSQL 리소스를 업데이트합니다. 리소스를 업데이트하려면 다음 단계를 완료합니다.

1. 다음 명령을 실행하여 **open-cluster-management** 프로젝트로 전환합니다.

```
oc project open-cluster-management
```

2. **search-postgres** Pod 메모리를 늘립니다. 다음 명령을 수행하면 메모리를 **16Gi** 로 늘립니다.

```
oc patch search -n open-cluster-management search-v2-operator --type json -p [{"op": "add", "path": "/spec/deployments/database/resources", "value": {"limits": {"memory": "16Gi"}, "requests": {"memory": "32Mi", "cpu": "25m"}}}]
```

3. 다음 명령을 실행하여 검색 Operator가 변경 사항을 덮어쓰지 않도록 합니다.

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

4. 다음 명령을 실행하여 **search-postgres** YAML 파일에서 리소스를 업데이트합니다.

```
oc edit cm search-postgres -n open-cluster-management
```

리소스를 늘리려면 다음 예제를 참조하십시오.

```
postgresql.conf: |-
work_mem = '128MB' # Higher values allocate more memory
max_parallel_workers_per_gather = '0' # Disables parallel queries
shared_buffers = '1GB' # Higher values allocate more memory
```

종료하기 전에 변경 사항을 저장해야 합니다.

5. 다음 명령을 실행하여 **postgres** 및 **api** pod를 다시 시작합니다.

```
oc delete pod search-postgres-xyz search-api-xzy
```

6. 변경 사항을 확인하려면 **search-postgres** YAML 파일을 열고 다음 명령을 실행하여 **postgresql.conf:** 에 대한 변경 사항이 있는지 확인합니다.

```
oc get cm search-postgres -n open-cluster-management -o yaml
```

환경 변수 추가에 대한 자세한 내용은 [사용자 정의 및 구성 검색](#)을 참조하십시오.

1.27. 설치 후 연결되지 않은 SUBMARINER 문제 해결

구성 후 Submariner가 올바르게 실행되지 않는 경우 다음 단계를 완료하여 문제를 진단합니다.

1.27.1. 증상: 설치 후 Submariner가 연결되지 않음

Submariner 네트워크는 설치 후 통신하지 않습니다.

1.27.2. 문제 확인: 설치 후 연결되지 않는 Submariner

Submariner를 배포한 후 네트워크 연결이 설정되지 않은 경우 문제 해결 단계를 시작합니다. Submariner를 배포할 때 프로세스가 완료될 때까지 몇 분이 걸릴 수 있습니다.

1.27.3. 문제 해결: 설치 후 연결할 수 없음

배포 후 Submariner가 올바르게 실행되지 않으면 다음 단계를 완료합니다.

1. 다음 요구 사항을 확인하여 Submariner의 구성 요소가 올바르게 배포되었는지 확인합니다.
 - **submariner-addon** Pod는 hub 클러스터의 **open-cluster-management** 네임스페이스에서 실행됩니다.
 - 다음 Pod는 각 관리 클러스터의 **submariner-operator** 네임스페이스에서 실행됩니다.
 - submariner-addon
 - submariner-gateway
 - submariner-routeagent
 - submariner-operator
 - Submariner-globalnet (ClusterSet에서 Globalnet이 활성화된 경우에만)
 - submariner-lighthouse-agent
 - submariner-lighthouse-coresdns
 - Submariner-networkplugin-syncer (지정 CNI 값이 **OVNKubernetes**인 경우에만)
 - submariner-metrics-proxy
2. **subctl diagnose all** 명령을 실행하여 **submariner-addon** Pod를 제외하고 필요한 Pod의 상태를 확인합니다.
3. **must-gather** 명령을 실행하여 디버깅 문제를 해결하는 데 도움이 되는 로그를 수집합니다.

1.28. SUBMARINER 애드온 문제 해결

클러스터 세트의 클러스터에 Submariner 애드온을 추가하면 *연결 상태, 에이전트 상태 및 게이트웨이 노드의 상태가 클러스터에 예기치 않은 상태가 표시됩니다.*

1.28.1. 증상: Submariner 추가 기능 상태가 저하됨

클러스터 세트의 클러스터에 Submariner 추가 기능을 추가하면 클러스터의 *게이트웨이 노드, 에이전트 상태 및 연결 상태가 표시됩니다.*

- 라벨이 지정된 게이트웨이 노드
 - **progressing**: 게이트웨이 노드에 레이블을 지정하는 프로세스입니다.
 - **nodes not labeled**: 게이트웨이 노드에 레이블이 지정되지 않았습니다. 레이블을 지정할 프로세스가 완료되지 않았기 때문일 수 있습니다.
 - **nodes not labeled**: 다른 프로세스가 완료될 때까지 대기 중이므로 게이트웨이 노드에 아직 레이블이 지정되지 않았습니다.
 - 노드 레이블: 게이트웨이 노드에 레이블이 지정되어 있습니다.
- 에이전트 상태
 - 진행 중: Submariner 에이전트 설치가 시작되었습니다.
 - 성능이 저하됨: Submariner 에이전트가 아직 진행 중이므로 올바르게 실행되지 않을 수 있습니다.
- 연결 상태
 - progressing: Submariner 애드온을 사용하여 연결을 설정하는 프로세스입니다.
 - Degraded: 연결이 준비되지 않았습니다. 애드온을 방금 설치한 경우 프로세스가 계속 진행 중일 수 있습니다. 연결이 이미 설정된 후 실행 중인 경우 두 클러스터가 서로 연결이 끊어졌습니다. 클러스터가 여러 개 있는 경우 클러스터 중 연결이 끊어진 경우 모든 클러스터에 **Degraded** 상태가 표시됩니다.

연결된 클러스터와 연결이 끊긴 클러스터도 표시합니다.

1.28.2. 문제 해결: Submariner 추가 기능 상태가 저하됨

- 성능이 저하된 상태는 프로세스가 완료되면 종종 자체적으로 확인됩니다. 표의 상태를 클릭하여 프로세스의 현재 단계를 확인할 수 있습니다. 해당 정보를 사용하여 프로세스가 완료되었는지 여부와 다른 문제 해결 단계를 수행해야 하는지 확인할 수 있습니다.
- 자체적으로 해결되지 않는 문제의 경우 다음 단계를 완료하여 문제를 해결합니다.
 1. 다음 조건이 있는 경우 **subctl** 유틸리티와 함께 **진단** 명령을 사용하여 Submariner 연결에서 일부 테스트를 실행할 수 있습니다.
 - a. **에이전트 상태** 또는 **연결 상태가 Degraded** 상태입니다. **진단** 명령은 문제에 대한 자세한 분석을 제공합니다.
 - b. 모든 것이 콘솔에서 녹색이지만 네트워킹 연결이 올바르게 작동하지 않습니다. **진단** 명령은 콘솔 외부에 다른 연결 또는 배포 문제가 없는지 확인하는 데 도움이 됩니다. 배포 후 문제를 확인하기 위해 **진단** 명령을 실행하는 것이 좋습니다.

명령을 실행하는 방법에 대한 자세한 내용은 Submariner의 [진단](#) 을 참조하십시오.

2. **연결 상태로** 문제가 계속되는 경우 **subctl** 유틸리티 도구의 **진단** 명령을 실행하여 두 Submariner 클러스터 간 연결에 대한 자세한 상태를 얻을 수 있습니다. 명령의 형식은 다음과 같습니다.

```
subctl diagnose all --kubeconfig <path-to-kubeconfig-file>
```

path-to-kubeconfig-file 을 **kubeconfig** 파일의 경로로 바꿉니다. 명령에 대한 자세한 내용은 Submariner 설명서의 [진단](#) 을 참조하십시오.

3. 방화벽 설정을 확인합니다. 연결에 문제가 발생하여 클러스터가 통신하지 못하는 방화벽 권한 문제로 인해 발생하는 경우가 있습니다. 이로 인해 **연결 상태**가 **degraded**으로 표시될 수 있습니다. 다음 명령을 실행하여 방화벽 문제를 확인합니다.

```
subctl diagnose firewall inter-cluster <path-to-local-kubeconfig> <path-to-remote-cluster-kubeconfig>
```

path-to-local-kubeconfig 를 클러스터 중 하나의 **kubeconfig** 파일 경로로 바꿉니다.

path-to-remote-kubeconfig 를 다른 클러스터의 **kubeconfig** 파일 경로로 교체합니다. **verify** 명령을 **subctl** 유틸리티 도구로 실행하여 두 개의 Submariner 클러스터 간 연결을 테스트할 수 있습니다. 명령의 기본 형식은 다음과 같습니다.

4. **연결 상태로** 문제가 계속되는 경우 **subctl** 유틸리티 도구로 **verify** 명령을 실행하여 두 Submariner 클러스터 간 연결을 테스트할 수 있습니다. 명령의 기본 형식은 다음과 같습니다.

```
subctl verify --kubeccontexts <cluster1>,<cluster2> [flags]
```

cluster1 및 **cluster2** 를 테스트 중인 클러스터 이름으로 교체합니다. 명령에 대한 자세한 내용은 Submariner 설명서에서 [확인하십시오](#).

5. 문제 해결 단계에서 문제를 해결한 후 **benchmark** 명령을 **subctl** 툴과 함께 사용하여 추가 진단을 실행할 때 비교할 기반을 설정합니다. 명령의 옵션에 대한 자세한 내용은 Submariner 설명서에서 [벤치마크](#) 를 참조하십시오.

1.29. 오류와 함께 복원 상태 문제 해결

백업을 복원하면 리소스가 올바르게 복원되지만 Red Hat Advanced Cluster Management 복원 리소스에 **FinishedWithErrors** 상태가 표시됩니다.

1.29.1. 증상: 복원 상태 해결이 오류와 함께 완료됩니다.

Red Hat Advanced Cluster Management에는 **FinishedWithErrors** 상태 및 Red Hat Advanced Cluster Management 복원에서 생성한 Velero 복원 리소스가 **PartiallyFailed** 상태가 표시됩니다.

1.29.2. 문제 해결: 복원 상태 해결 상태 완료 오류

비어 있는 백업에서 복원하는 경우 **FinishedWithErrors** 상태를 무시해도 됩니다.

Red Hat Advanced Cluster Management for Kubernetes restore에는 모든 Velero 복원 리소스에 대한 누적 상태가 표시됩니다. 한 상태가 **PartiallyFailed** 이고 다른 상태가 **Completed** 이면 표시되는 누적 상태는 하나 이상의 문제가 있음을 알리는 것입니다.

문제를 해결하려면 **PartiallyFailed** 상태의 모든 개별 Velero 복원 리소스의 상태를 확인하고 자세한 내용은 로그를 확인합니다. **DownloadRequest** 사용자 정의 리소스를 사용하여 오브젝트 스토리지에서 로그를 직접 가져오거나 OADP Operator에서 다운로드할 수 있습니다.

콘솔에서 **DownloadRequest** 를 생성하려면 다음 단계를 완료합니다.

1. **Operators > 설치된 Operators & gt; Create DownloadRequest** 로 이동합니다.
2. **Kind** 로 **BackupLog** 를 선택하고 콘솔 지침에 따라 **DownloadRequest** 생성을 완료합니다.

1.30. HUB 클러스터 백업을 복원할 때 일반 리소스가 제거됨

hub 클러스터 백업을 복원하고 **Restore.cluster.open-cluster-management.io** 리소스에서 생성한 **cleanupBeforeRestore:CleanupRestored** paramater를 사용하면 **acm-resources-generic-schedule** 백업에 의해 생성된 리소스가 제거될 수 있습니다.

1.30.1. 증상: 허브 클러스터 백업을 복원할 때 일반 리소스가 제거됩니다.

acm-resources-generic-schedule 백업에 백업된 리소스는 복원된 허브 클러스터에 표시되지 않습니다. 백업 Operator 로그를 확인하는 경우 다음과 유사한 메시지가 표시됩니다.

```
_2023-06-08T13:42:48.066572033Z 2023-06-08T13:42:48.066Z INFO Deleting resource
DRPlacementControl [c1-helloworld-placement-1-drpc.c1-helloworld] {"controller": "restore",
"controllerGroup": "cluster.open-cluster-management.io", "controllerKind": "Restore", "restore":
{"name":"restore-acm","namespace":"open-cluster-management-backup"}}
```

1.30.2. 문제 해결: 허브 클러스터 백업을 복원할 때 일반 리소스가 제거됩니다.

다음 조건이 발생하면 리소스가 제거됩니다.

- Secret 또는 ConfigMap 리소스 유형과 **cluster.open-cluster-management.io/backup** 레이블과 일치하지 않는 **acm-resources-generic-schedule** 백업에서 지원하는 리소스가 있습니다.
- **Restore.cluster.open-cluster-management.io** 리소스를 사용하는 복원을 실행하고 **cleanupBeforeRestore:** 값을 **cleanup Restored** 로 설정합니다.
- 최신 Red Hat Advanced Cluster Management 백업 세트에는 **acm-resources-schedule** 백업이 포함되어 있지 않으므로 이전 버전의 백업이 선택됩니다. 결과적으로 **acm-resources-schedule** 백업에는 **acm-resources-generic-schedule** 백업과 다른 타임스탬프가 있습니다. 복원 후 작업 중에 **cleanRestore** 옵션이 처리되면 **acm-resources-schedule** 백업과 동일한 타임스탬프가 없기 때문에 모든 일반 리소스가 정리됩니다. 문제를 해결하려면 복원 작업을 다시 실행하고 **cleanupBeforeRestore:** 값을 **None** 으로 설정합니다.

1.31. OADP 사용자 정의 리소스 정의 문제 해결

MultiClusterHub 리소스는 **cluster-backup** 플래그가 **false** 로 설정된 경우에도 백업 및 복원 구성 요소에서 제공하고 지원하는 리소스로 Velero 및 OADP 사용자 정의 리소스 정의를 덮어씁니다.

1.31.1. 증상: OADP 사용자 정의 리소스 정의

OADP Operator를 수동으로 설치하려고 하면 설치 버전에서 백업 및 복원 구성 요소가 설치한 것과 동일한 사용자 정의 리소스 정의를 사용하지 않는 경우 설치에 실패합니다.

1.31.2. 문제 해결: OADP 사용자 정의 리소스 정의

이 문제를 임시로 해결하기 위해 테스트 환경에서 **MultiClusterHub** 조정을 일시 중지할 수 있습니다. OADP Operator를 수동으로 설치하기 전에 다음 명령을 실행하여 **MultiClusterHub**가 OADP Operator 버전에서 설치한 사용자 정의 리소스 정의를 업데이트하지 못하도록 합니다.

```
oc annotate mch multiclusterhub -n open-cluster-management mch-pause=true
```

1.32. 여러 줄 YAML 구문 분석 문제 해결

fromSecret 함수를 사용하여 **Secret** 리소스의 콘텐츠를 **Route** 리소스에 추가하려는 경우 콘텐츠가 잘못 표시됩니다.

1.32.1. 증상: 여러 줄 YAML 구문 분석 문제 해결

관리형 클러스터 및 허브 클러스터가 동일한 클러스터인 경우 인증서 데이터를 다시 적용하기 때문에 콘텐츠가 템플릿 JSON 문자열로 구문 분석되지 않습니다. 다음과 같은 오류 메시지가 표시될 수 있습니다.

```
message: >-
  [spec.tls.caCertificate: Invalid value: "redacted ca certificate
  data": failed to parse CA certificate: data does not contain any
  valid RSA or ECDSA certificates, spec.tls.certificate: Invalid
  value: "redacted certificate data": data does not contain any valid
  RSA or ECDSA certificates, spec.tls.key: Invalid value: "": no key specified]
```

1.32.2. 문제 해결: 여러 줄 YAML 구문 분석 문제 해결

hub 클러스터 및 관리 클러스터를 **Secret 값에서** 검색하도록 인증서 정책을 구성합니다. **autoindent** 함수를 사용하여 다음 콘텐츠로 인증서 정책을 업데이트합니다.

```
    tls:
      certificate: |
        {{ print "{{hub fromSecret \"open-cluster-management\" \"minio-cert\" \"tls.crt\" hub}}" |
base64dec | autoindent }}
```