

Try ROSA

2025-05-09

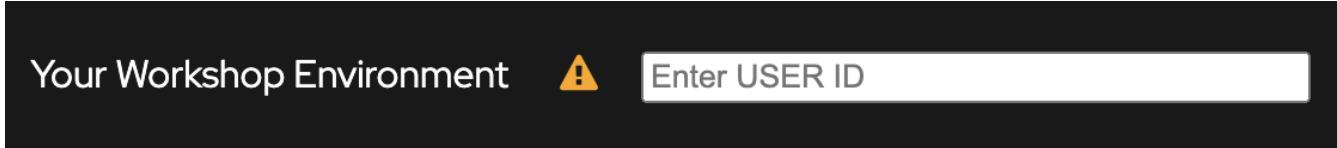
ROSA ရွှေးချေးဆိပ်အမြတ်အမာန်

0. ワークショップ

:imagesdir::../assets/images :sectnums: :sectnumlevels: 4

概要

ワークショップ環境Enter User IDを入力する必要がありますIDは: user1になります



OK UserID HTTP USERID=user1



ROSA API URL AWS URL

3. 各種環境のURLとログイン方法	
ROSA コンソール	https://console-openshift-console.apps.rosa.keomizorosa.guj9.p3.openshiftapps.com
ROSA API	https://api.keomizorosa.guj9.p3.openshiftapps.com:443
OpenShift コンソール（オンプレ環境想定）	https://console-openshift-console.apps.aaa
AWS コンソール	https://714932348383.signin.aws.amazon.com/console
Gitリポジトリ	ワークショップの共有メモを参照してください

OpenShift CLI

OpenShift Container Platform https://docs.redhat.com/ja/documentation/openshift_container_platform/4.18/html/cli_tools/openshift-cli-oc#cli-installing-cli_cli-developer-commands

OpenShift Container Platform <https://console-openshift-console.apps.rosa.%SUBDOMAIN%/command-line-tools>

skopeo 乽乿

<https://www.redhat.com/ja/topics/containers/what-is-skopeo> 乽乿

乽乿URL

ROSA 乽	https://console-openshift-console.apps.rosa.%SUBDOMAIN%
ROSA API	https://api.%SUBDOMAIN%:443
OpenShift 乽	https://console-openshift-console.apps.xxx
AWS 乽	https://%AWSACCOUNTID%.signin.aws.amazon.com/console
Git 乽	乽

OpenShift 乽

1. OpenShift 乽
2. 乽users-htpasswd乽
3. 乽%USERID% openshift 乽

OpenShift 乽

OpenShift 乽Pod 乽

1. ROSA 乽> _
2. 乽CreateProject 乽%USERID%-term
3. 乽Start 乽

乽OpenShift CLI 乽

1. OpenShift API 乽

```
oc login -u %USERID% -p openshift https://api.%SUBDOMAIN%:443
```

1. ROSA HCP

:imagesdir::../assets/images :experimental: :source-highlighter: highlightjs

ROS

ROS

▶ <https://www.youtube.com/watch?v=hTFk8inWe90> (*YouTube video*)

ROS

ROSA Red Hat AWS Red Hat AWS Security Token Service (STS) ROSA HCP

- STS ROSA AWS
- STS ROSA IAM
- AWS

ROSA HCP AWS Red Hat

AWS ROSA HCP ROSA Classic HCP 2 ROSA HCP

ROSA の前提条件を確認する [Info](#)

このページでは、アカウントが Red Hat OpenShift Service on AWS (ROSA) クラスターを作成するための前提条件を満たしているかどうかを確認します。

ROSA の有効化 [Info](#)

ROSA は AWS と Red Hat が共同で管理します。Red Hat との接続を作成するには、ROSA を有効にします。この接続は、計測と請求に必要です。

 ROSA を有効にすると、次の 2 種類のクラスターを作成できます。

- ROSA Classic: AWS アカウントでホストされるクラスターコントロールプレーンインフラストラクチャ。
- ROSA HCP (ROSA とホスト型コントロールプレーン (HCP)): Red Hat が所有する AWS アカウントでホストされるクラスターコントロールプレーンインフラストラクチャ。ROSA HCP は現在プレビュー段階であり、本番環境のワークロードには使用しないでください。ROSA HCP のレビューに関する用語については、次の「トライアルとレビュー」を参照してください。

クラスターを作成するときに、どのコントロールプレーンモデルを使用するかを選択します。[詳細](#) 

 ROSA HCP と ROSA Classic はすでに有効になっています。

最終チェック日: December 09, 2023 at 05:06 (UTC)

▶ AWS Organizations の管理者: 組織全体で ROSA Classic を有効にする

AWS CLI の構成ファイル (`~/.aws/credentials`) に記載されています

- `aws_access_key_id`
- `aws_secret_key`

構成ファイル (`~/.aws/config`) に記載されています

```
$ cat ~/.aws/config
[default]
region = us-east-2
```

AWS API の構成 (AWS CLI) に記載されています

```
$ aws sts get-caller-identity
{
    "UserId": "AIDXXXXXXXXXXXXXX",
    "Account": "XXXXXX",
    "Arn": "arn:aws:iam::XXXXXX:user/testuser01"
}
```

AWSとRed Hatの連携を開始する

```
$ aws iam create-service-linked-role --aws-service-name "elasticloadbalancing.amazonaws.com"
```



AWSとRed Hatの連携を開始する
AWS Service Role for Elastic Load Balancing

AWSとRed Hatの連携を開始する
AWSとRed Hatの連携を開始する

Service Quotas [Info](#)

ROSAを使用するには、クォータを増やす必要がある場合があります。

☑ クォータは ROSA の要件を満たしています。

最終チェック日: December 09, 2023 at 05:06 (UTC)

ELB サービスにリンクされたロール [Info](#)

ROSAは、Elastic Load Balancing (ELB) サービスにリンクされたロールを使用して、ユーザーに代わって AWS のサービスを呼び出します。アカウントにこのロールがない場合は、ロールが作成されます。

☑ AWS Service Role for Elastic Load Balancing はすでに存在します。

[ロールの表示](#)

最終チェック日: December 09, 2023 at 05:06 (UTC)

次のステップ

Red Hatに進むを選択して、これらの前提条件のステップを完了します。

- AWSとRed Hatアカウントのリンク | [Info](#)
- AWSアカウント全体のロールの作成 | [Info](#)

完了したら、Red Hatコンソールでクラスターを作成できます。

[キャンセル](#)

[Red Hatに進む](#)

Red Hat

Red Hat

I have read and agreed to the terms and conditions

Red Hat Hybrid Cloud Console

Services ▾ Search for services Preview off ⚙ ⓘ Hirofumi Kojima ▾

connect

Complete your account connection

Red Hat account number 13 [REDACTED]

AWS account ID 92 [REDACTED]

Subscription(s) Red Hat OpenShift Service on AWS with Hosted Control Plane

Terms and conditions *

United States (English) ▾

I have read and agreed to the [terms and conditions](#).

Connect accounts Cancel

Red Hat Hybrid Cloud Console

Congratulations, your Red Hat and AWS accounts are linked
Welcome to the Red Hat Hybrid Cloud Console. If you cannot access production tools for a subscription that you have purchased, please wait 5 minutes and confirm your subscription at subscription inventory. Here you can configure or manage Red Hat OpenShift Cluster Manager.

ROSA CLI Red Hat Hybrid Cloud Console PATH



```
$ chmod +x rosa
$ sudo mv rosa /usr/local/bin/
$ rosa version
1.2.31
```

ROSA CLI Red Hat Hybrid Cloud Console PATH URL

```
$ rosa login
To login to your Red Hat account, get an offline access token at
https://console.redhat.com/openshift/token/rosa
? Copy the token and paste it here: *****
I: Logged in as '<Red Hat Hybrid Cloud Console>' on 'https://api.openshift.com'
```

Red Hat Hybrid Cloud Console AWS Red

Hat Hybrid Cloud Console AWS Account ID ARN

```
$ rosa whoami
AWS Account ID: XXXXXXXXXXXX
AWS Default Region: us-east-2
AWS ARN: arn:aws:iam::XXXXXXXXXX:user/testuser01
```

OCM API:	https://api.openshift.com
OCM Account ID:	XXXXXXXXXX
OCM Account Name:	Hiforumi Kojima
OCM Account Username:	<Red Hat ユーザー名>
OCM Account Email:	hkojima@redhat.com
OCM Organization ID:	XXXXXXXXXX
OCM Organization Name:	Hiforumi Kojima
OCM Organization External ID:	XXXXXXXXXX

ROSA CLIのインストールOpenShift CLI (oc) のインストールLinuxのopenshift-client.tarの展開

```
$ rosa download openshift-client
$ tar xvf openshift-client-linux.tar.gz
$ sudo mv oc /usr/local/bin/
$ rosa verify openshift-client
I: Verifying whether OpenShift command-line tool is available...
I: Current OpenShift Client Version: 4.14.5
```

ROSA HCPのインストールAWS VPC・IAMの設定

ROSA HCPのインストールAWS VPCのAWSのVPCのTerraformのVPCのTerraformのVPCのAWSのAWSのIDの設定

```
$ git clone https://github.com/openshift-cs/terraform-vpc-example
$ cd terraform-vpc-example
$ terraform init

$ terraform plan -out rosa.tfplan -var region=us-east-2
$ terraform apply rosa.tfplan
```

AWSのVPCのSingleAZとMultiAZの設定

HCPのVPCのAZのterraform plan

```
$ terraform plan -out rosa.tfplan -var region=us-east-2 \
-var single_az_only=false \
-var 'subnet_azs=["use2-az1", "use2-az2", "use2-az3"]'
```

AWS VPCのSUBNET_IDSterraform outputのIDのHCPのexportのSUBNET_IDSの設定

```
$ export SUBNET_IDS=$(terraform output -raw cluster-subnets-string)
$ echo $SUBNET_IDS
```

subnet-0fb4f75f448b5499c, subnet-0087cb7bb3f628793

AWS IAMとROSA CLIによるAWSアカウントの構成

```
$ rosa create account-roles --mode auto --hosted-cp --yes
I: Logged in as '<Red Hat OpenShift>' on 'https://api.openshift.com'
I: Validating AWS credentials...
I: AWS credentials are valid!
I: Validating AWS quota...
I: AWS quota ok. If cluster installation fails, validate actual AWS resource usage
against https://docs.openshift.com/rosa/roса_getting_started/roса-required-aws-
service-quotas.html
I: Verifying whether OpenShift command-line tool is available...
I: Current OpenShift Client Version: 4.14.5
I: Creating account roles
I: Creating hosted CP account roles using 'arn:aws:iam::XXXXXXXXXX:user/testuser01'
I: Created role 'ManagedOpenShift-HCP-ROSA-Installer-Role' with ARN
'arn:aws:iam::XXXXXXXXXX:role/ManagedOpenShift-HCP-ROSA-Installer-Role'
I: Created role 'ManagedOpenShift-HCP-ROSA-Support-Role' with ARN
'arn:aws:iam::XXXXXXXXXX:role/ManagedOpenShift-HCP-ROSA-Support-Role'
I: Created role 'ManagedOpenShift-HCP-ROSA-Worker-Role' with ARN
'arn:aws:iam::XXXXXXXXXX:role/ManagedOpenShift-HCP-ROSA-Worker-Role'
I: To create an OIDC Config, run the following command:
    rosa create oidc-config
```

AWSとROSA CLIによるAWSアカウントの構成

IAM > ロール

ロール (19) 情報

IAM ロールは、短期間有効な認証情報を持つアクセス権を持つアカウント作成できるアイデンティティです。信頼するエンティティにロールを委任することもできます。

ロール名	信頼されたエンティティ	最後のアクティビティ
ManagedOpenShift-HCP-ROSA-Installer-Role	アカウント: 71XXXXXX	-
ManagedOpenShift-HCP-ROSA-Support-Role	アカウント: 71XXXXXX	-
ManagedOpenShift-HCP-ROSA-Worker-Role	AWS のサービス: ec2	-

ROSA HCPによるOperatorのIAMとOpenID Connectの構成

```
$ rosa create oidc-config --mode auto --yes
I: Setting up managed OIDC configuration
I: To create Operator Roles for this OIDC Configuration, run the following command and
remember to replace <user-defined> with a prefix of your choice:
    rosa create operator-roles --prefix <user-defined> --oidc-config-id
280rqooan3kqqn4o1us1ip073fsrkfm8
If you are going to create a Hosted Control Plane cluster please include '--hosted-cp'
I: Creating OIDC provider using 'arn:aws:iam::XXXXXXXXXX:user/testuser01'
I: Created OIDC provider with ARN 'arn:aws:iam::XXXXXXXXXX:oidc-provider/rh-oidc.s3.us-
```

east-1.amazonaws.com/280rqooan3kqqn4o1us1ip073fsrkfm8'

ROSA CLIROSACLIHCPROSAHCPIAMROSAIAM2ROSAHCP

- 账户角色(account roles): Red Hat SRE
- 操作员角色(operator roles): OpenShift Operator AWS IAM ROSA HCP

ROSACLI IAM ROSAHCP IAM ROSAHCP AWS IAM ROSA HCP

ROSA HCPROSAHCP

ROSA HCPROSAHCPversion OpenShiftOpenShiftdry-run
ROSACLI ROSAHCP ROSA HCP m5.xlarge



SingleAZ/MultiAZ ROSA HCP

--oidc-config-id ROSA rosa create oidc-config oidc-config-id
(:0ikrpt0nv000c000trn00renuakl0mn) ROSA

```
export OIDC_CONFIG_ID=oidc config id
export CLUSTER_NAME=AWS Orgnization ROSA
$ rosa create cluster --cluster-name=$CLUSTER_NAME --mode=auto --yes --hosted-cp \
--oidc-config-id $OIDC_CONFIG_ID \
--subnet-ids=$SUBNET_IDS --region=us-east-2 \
--compute-machine-type m5.xlarge --version 4.14.2
```

ROSA HCPROSAHCP2ROSAHCP500ROSAHCPSingleAZ, MultiAZ

MultiAZ SingleAZ ROSA rosa create cluster subnet-ids
MultiAZ/SingleAZ

AWS EC2 c5.xlarge(4vCPU/RAM8GiB) ROSA HCP
EC2 m5.xlarge(4vCPU/RAM16GiB) ROSA HCP
(: --compute-machine-type c5.xlarge) (: --replicas 3)

ROSACLI ROSAHCP ROSA HCP

```
export OIDC_CONFIG_ID=oidc config id
export CLUSTER_NAME=AWS Orgnization ROSA
$ rosa create cluster --cluster-name=$CLUSTER_NAME --mode=auto --hosted-cp \
```

```
--subnet-ids=$SUBNET_IDS --region=us-east-2 --version 4.18.10

I: Using 'XXXXXXXXXX' as billing account
I: To use a different billing account, add --billing-account xxxxxxxxxxxx to previous
command
I: Using arn:aws:iam::XXXXXXXXXX:role/ManagedOpenShift-HCP-ROSA-Installer-Role for the
Installer role
I: Using arn:aws:iam::XXXXXXXXXX:role/ManagedOpenShift-HCP-ROSA-Worker-Role for the
Worker role
I: Using arn:aws:iam::XXXXXXXXXX:role/ManagedOpenShift-HCP-ROSA-Support-Role for the
Support role

? OIDC Configuration ID: $OIDC_CONFIG_ID | https://rh-oidc.s3.us-east-
1.amazonaws.com/280rqooan3kqqn4o1us1ip073fsrkfm8
? Tags (optional):
? AWS region: us-east-2
? PrivateLink cluster: No
? Machine CIDR: 10.0.0.0/16
? Service CIDR: 172.30.0.0/16
? Pod CIDR: 10.128.0.0/14
? Enable Customer Managed key: No
? Compute nodes instance type: [Use arrows to move, type to filter, ? for more help]
  m5dn.metal
  m5.metal
  m5n.metal
> m5.xlarge
  m5zn.metal
  m6a.12xlarge
  m6a.16xlarge
? Compute nodes instance type: m5.xlarge
? Enable autoscaling: No
? Compute nodes: 2
? Host prefix: 23
? Enable FIPS support: No
? Encrypt etcd data: No
? Disable Workload monitoring: No
? Use cluster-wide proxy: No
? Additional trust bundle file path (optional):
? Enable audit log forwarding to AWS CloudWatch: No

I: Creating cluster 'hcp-01'
I: To create this cluster again in the future, you can run:
  rosa create cluster --cluster-name hcp-01 --mode auto --role-arn
  arn:aws:iam::XXXXXXXXXX:role/ManagedOpenShift-HCP-ROSA-Installer-Role --support-role
  -arn arn:aws:iam::XXXXXXXXXX:role/ManagedOpenShift-HCP-ROSA-Support-Role --worker-iam
  -role arn:aws:iam::XXXXXXXXXX:role/ManagedOpenShift-HCP-ROSA-Worker-Role --operator
  -roles-prefix hcp-01-g8r1 --oidc-config-id 280rqooan3kqqn4o1us1ip073fsrkfm8 --region
  us-east-2 --version 4.14.2 --replicas 2 --compute-machine-type m5.xlarge --machine
  -cidr 10.0.0.0/16 --service-cidr 172.30.0.0/16 --pod-cidr 10.128.0.0/14 --host-prefix
  23 --subnet-ids subnet-0fb4f75f448b5499c,subnet-0087cb7bb3f628793 --hosted-cp
I: To view a list of clusters and their status, run 'rosa list clusters'
```

I: Cluster 'hcp-01' has been created.

I: Once the cluster is installed you will need to add an Identity Provider before you can login into the cluster. See 'rosa create idp --help' for more information.

Name: hcp-01
ID: 280scqkn8ocjoochasq423tg4donvpaq
External ID: 56549c55-3d86-4ba3-b163-4ca5abf67c59
Control Plane: ROSA Service Hosted
OpenShift Version: 4.14.2
Channel Group: stable
DNS: Not ready
AWS Account: XXXXXXXXX
AWS Billing Account: XXXXXXXXX
API URL:
Console URL:
Region: us-east-2
Availability:
- Control Plane: MultiAZ
- Data Plane: SingleAZ
Nodes:
- Compute (desired): 2
- Compute (current): 0
Network:
- Type: OVNKubernetes
- Service CIDR: 172.30.0.0/16
- Machine CIDR: 10.0.0.0/16
- Pod CIDR: 10.128.0.0/14
- Host Prefix: /23
Workload Monitoring: Enabled
Ec2 Metadata Http Tokens: optional
STS Role ARN: arn:aws:iam::XXXXXXXXXX:role/ManagedOpenShift-HCP-ROSA-
Installer-Role
Support Role ARN: arn:aws:iam::XXXXXXXXXX:role/ManagedOpenShift-HCP-ROSA-
Support-Role
Instance IAM Roles:
- Worker: arn:aws:iam::XXXXXXXXXX:role/ManagedOpenShift-HCP-ROSA-
Worker-Role
Operator IAM Roles:
- arn:aws:iam::XXXXXXXXXX:role/hcp-01-g8r1-kube-system-capa-controller-manager
- arn:aws:iam::XXXXXXXXXX:role/hcp-01-g8r1-kube-system-control-plane-operator
- arn:aws:iam::XXXXXXXXXX:role/hcp-01-g8r1-kube-system-kms-provider
- arn:aws:iam::XXXXXXXXXX:role/hcp-01-g8r1-openshift-cluster-csi-drivers-ebs-cloud-
credentials
- arn:aws:iam::XXXXXXXXXX:role/hcp-01-g8r1-openshift-cloud-network-config-controller-
cloud-cred
- arn:aws:iam::XXXXXXXXXX:role/hcp-01-g8r1-openshift-image-registry-installer-cloud-
credentials
- arn:aws:iam::XXXXXXXXXX:role/hcp-01-g8r1-openshift-ingress-operator-cloud-
credentials
- arn:aws:iam::XXXXXXXXXX:role/hcp-01-g8r1-kube-system-kube-controller-manager
Managed Policies: Yes

```

State: waiting (Waiting for user action)
Private: No
Created: Dec 9 2023 07:17:00 UTC
Details Page: https://console.redhat.com/openshift/details/s/2ZI0eJctRNzSZe58wMQFmAl2Sd
OIDC Endpoint URL: https://rh-oidc.s3.us-east-1.amazonaws.com/280rqooan3kqqn4o1us1ip073fsrkfm8 (Managed)
Audit Log Forwarding: disabled

I: Preparing to create operator roles.
I: Creating roles using 'arn:aws:iam::XXXXXXXXXX:user/testuser01'
I: Created role 'hcp-01-g8r1-openshift-cloud-network-config-controller-cloud-cred' with ARN 'arn:aws:iam::XXXXXXXXXX:role/hcp-01-g8r1-openshift-cloud-network-config-controller-cloud-cred'
I: Created role 'hcp-01-g8r1-kube-system-capa-controller-manager' with ARN 'arn:aws:iam::XXXXXXXXXX:role/hcp-01-g8r1-kube-system-capa-controller-manager'
I: Created role 'hcp-01-g8r1-kube-system-control-plane-operator' with ARN 'arn:aws:iam::XXXXXXXXXX:role/hcp-01-g8r1-kube-system-control-plane-operator'
I: Created role 'hcp-01-g8r1-kube-system-kms-provider' with ARN 'arn:aws:iam::XXXXXXXXXX:role/hcp-01-g8r1-kube-system-kms-provider'
I: Created role 'hcp-01-g8r1-kube-system-kube-controller-manager' with ARN 'arn:aws:iam::XXXXXXXXXX:role/hcp-01-g8r1-kube-system-kube-controller-manager'
I: Created role 'hcp-01-g8r1-openshift-image-registry-installer-cloud-credentials' with ARN 'arn:aws:iam::XXXXXXXXXX:role/hcp-01-g8r1-openshift-image-registry-installer-cloud-credentials'
I: Created role 'hcp-01-g8r1-openshift-ingress-operator-cloud-credentials' with ARN 'arn:aws:iam::XXXXXXXXXX:role/hcp-01-g8r1-openshift-ingress-operator-cloud-credentials'
I: Created role 'hcp-01-g8r1-openshift-cluster-csi-drivers-ebs-cloud-credentials' with ARN 'arn:aws:iam::XXXXXXXXXX:role/hcp-01-g8r1-openshift-cluster-csi-drivers-ebs-cloud-credentials'

I: Preparing to create OIDC Provider.
I: OIDC provider already exists.
I: To determine when your cluster is Ready, run 'rosa describe cluster -c hcp-01'.
I: To watch your cluster installation logs, run 'rosa logs install -c hcp-01 --watch'.

```

STATE: installing (ready) 10 minutes

```
$ rosa list cluster
ID          NAME      STATE   TOPOLOGY
280scqkn8ocjochasq423tg4donvpaq  hcp-01  ready  Hosted CP
```

Red Hat SRE AWS AWS

rosa list machinepool REPLICAS

```
$ rosa list machinepool -c $CLUSTER_NAME
ID      AUTOSCALING  REPLICAS  INSTANCE TYPE  LABELS    TAINTS    AVAILABILITY ZONE
SUBNET           VERSION  AUTOREPAIR
```

workers No	2/2	m5.xlarge	us-east-2a
subnet-0087cb7bb3f628793	4.14.2	Yes	

ROSA HCP OpenShift Cluster Manager (OCM) SingleAZ(2) MultiAZ(2+3) MultiAZ



OCM OpenShift Cluster Manager Red Hat OpenShift Hybrid Console

OCM

Clusters > hcp-01

hcp-01

Open console

Actions ▾



Overview Access control Add-ons Cluster history Networking Machine pools Support Settings

Add machine pool

Machine pool	Instance type	Availability zones	Node count	Autoscaling	Version
--------------	---------------	--------------------	------------	-------------	---------

workers	m5.xlarge	us-east-2a	2	Disabled	4.14.2
---------	-----------	------------	---	----------	--------

Subnets

subnet-0087cb7bb3f628793

Feedback

Clusters > hcp-multiaz-02

hcp-multiaz-02

Open console

Actions ▾



Overview Access control Add-ons Cluster history Networking Machine pools Support Settings

Add machine pool

Machine pool	Instance type	Availability zones	Node count	Autoscaling	Version
--------------	---------------	--------------------	------------	-------------	---------

workers-0	c5.xlarge	us-east-2b	1	Disabled	4.14.2
-----------	-----------	------------	---	----------	--------

workers-1	c5.xlarge	us-east-2a	1	Disabled	4.14.2
-----------	-----------	------------	---	----------	--------

Feedback

hcp-multiaz-01[Open console](#)

Actions ▾


[Overview](#) [Access control](#) [Add-ons](#) [Cluster history](#) [Networking](#) [Machine pools](#) [Support](#) [Settings](#)
[Add machine pool](#)

Machine pool	Instance type	Availability zones	Node count	Autoscaling	Version	⋮
workers-0	c5.xlarge	us-east-2c	1	Disabled	4.14.2	⋮
workers-1	c5.xlarge	us-east-2b	1	Disabled	4.14.2	⋮
workers-2	c5.xlarge	us-east-2a	1	Disabled	4.14.2	⋮

[Feedback](#)

MultiAZ 2 MultiAZ 3 ROSA HCP workers-2
 1 1 OpenShift Monitoring Prometheus Pod oc (OpenShift CLI) cluster-admin Prometheus
 Pod Prometheus Pod OpenShift k8s Prometheus

```
$ oc get prometheus -n openshift-monitoring
NAME      VERSION   DESIRED   READY   RECONCILED   AVAILABLE   AGE
k8s      2.53.1     2          2        True        True        17m
```

```
$ oc delete pvc -n openshift-monitoring \
prometheus-data-prometheus-k8s-0 \
prometheus-data-prometheus-k8s-1
```

```
$ oc delete pod -n openshift-monitoring \
prometheus-k8s-0 \
prometheus-k8s-1
```

ROSA HCP

ROSA HCP rosa create admin

```
$ rosa create admin --cluster $CLUSTER_NAME
```

I: Admin account has been added to cluster 'hcp-01'.

I: Please securely store this generated password. If you lose this password you can delete and recreate the cluster admin user.

I: To login, run the following command:

```
oc login https://api.hcp-01.240p.p3.openshiftapps.com:443 --username cluster-admin  
--password XXXXX-XXXXX-XXXXX-XXXX
```

I: It may take several minutes for this access to become active.

ROSA

HCP

URL rosa create admin (cluster-admin)
ROSA

```
$ rosa describe cluster -c hcp-01 |grep Console  
Console URL: https://console-openshift-console.apps.rosa.hcp-  
01.240p.p3.openshiftapps.com
```

ROSA

HCP

ROSA

HCP

- GitHub 用 GitHub Enterprise
- GitLab
- Google
- LDAP
- OpenID Connect
- htpasswd

htpasswd

cluster-admin

ROSA

htpasswd testuser1 ~ testuser100 ROSA HCP
users.htpasswd ROSA HCP

```
$ htpasswd -cb users.htpasswd testuser1 <password>  
$ for i in {2..100}; do htpasswd -b users.htpasswd testuser$i <password>; done
```

```
$ rosa create idp --type=htpasswd --name=testuser-htpasswd01 --cluster=$CLUSTER_NAME  
--from-file=users.htpasswd  
I: Configuring IDP for cluster 'hcp-01'  
I: Identity Provider 'testuser-htpasswd01' has been created.  
It may take several minutes for this access to become active.  
To add cluster administrators, see 'rosa grant user --help'.
```

I: To log in to the console, open <https://console-openshift-console.apps.rosa.hcp-01.240p.p3.openshiftapps.com> and click on 'testuser-htpasswd01'.

rosa create idp htpasswd users.htpasswd testuserX
ROSA

ROSA HCPのロールを管理するための rosa grant user (grant) と rosa revoke user (revoke) のコマンド

```
$ rosa grant user cluster-admin --user <ユーザー名> --cluster <ROSA HCP名>
$ rosa revoke user cluster-admin --user <ユーザー名> --cluster <ROSA HCP名>
```

ROSA HCPの操作

ROSA HCPの操作 rosa delete cluster で ROSA HCPを削除する rosa list cluster で ROSA HCPをリストする rosa operator-roles で ROSA HCPの操作ロールを削除する rosa delete operator-roles で ROSA HCPの操作ロールを削除する

OpenID Connect(OIDC)認証による ROSA HCPの認証方法 ROSA HCPの認証方法 OpenID Connect認証による認証方法



OpenID Connect認証による認証方法

ROSA HCPの認証方法

HCPの認証方法 ROSA HCPの認証方法

```
$ rosa list cluster
ID           NAME   STATE  TOPOLOGY
280scqkn8ocjoochasq423tg4donvpaq  hcp-01  ready  Hosted CP
```

```
$ rosa delete cluster -c hcp-01 --yes
...<snip>...
```

I: Once the cluster is uninstalled use the following commands to remove the above aws resources.

```
rosa delete operator-roles --prefix hcp-01-g8r1
rosa delete oidc-provider --oidc-config-id 280rqooan3kqqn4o1us1ip073fsrkfm8
I: To watch your cluster uninstallation logs, run 'rosa logs uninstall -c rosa-hcp-01
--watch'
```

```
$ rosa delete operator-roles --prefix hcp-01-g8r1 --mode auto --yes
```

2. ROSA で開発環境構築

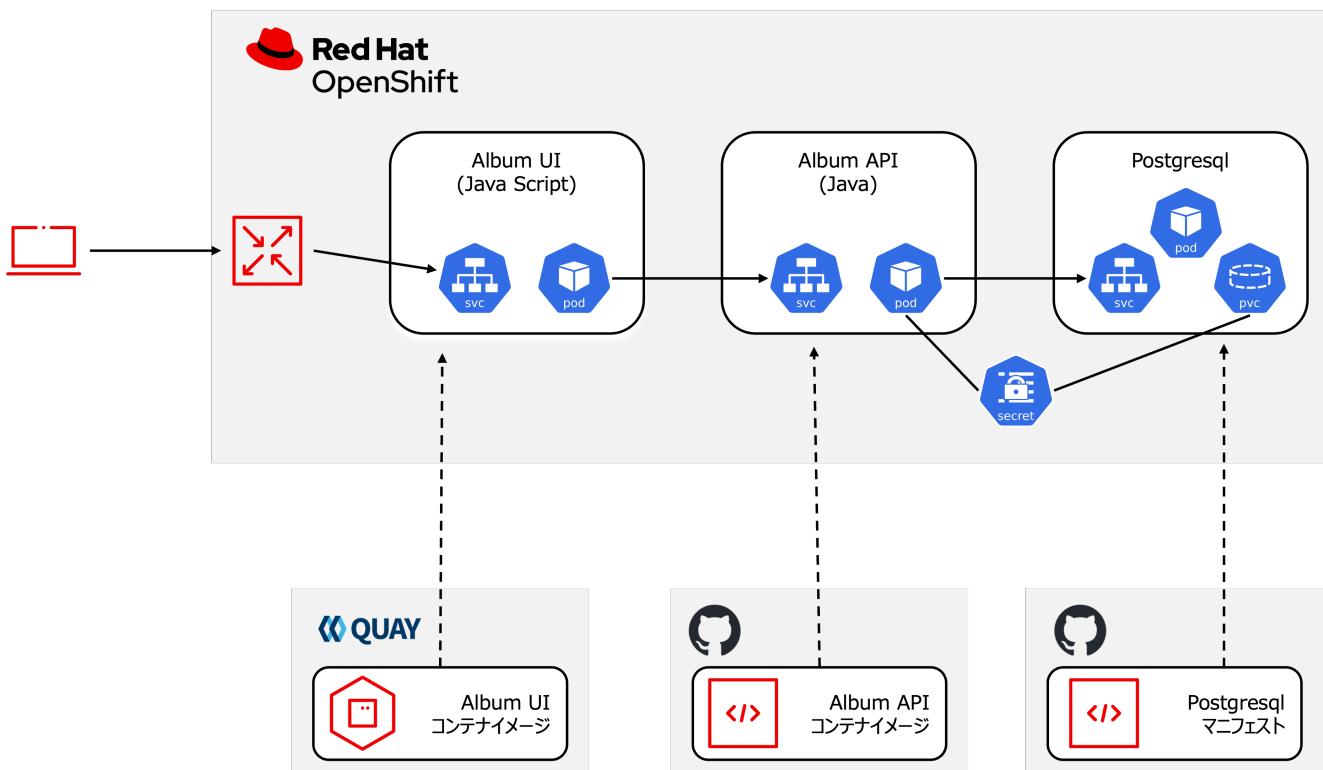
:imagesdir::../assets/images :sectnums: :sectnumlevels: 4

概要

Album UI (album-ui) と Album API (album-api) の 2 つのコンテナイメージを Red Hat OpenShift 上にデプロイする。データベース PostgreSQL を Red Hat OpenShift 上に接続する。

Red Hat OpenShift は Git と連携するため、OpenShift で開発環境を構築する。OpenShift は YAML ファイルで構成される。OpenShift では、YAML ファイルを用いて各コンポーネントを定義する。

構成図



Postgresql の構成

Postgresql のマニフェストを GitHub 上に配置する。Secret を用いて接続情報を管理する。

```
oc new-project %USERID%-app  
oc apply -f https://raw.githubusercontent.com/akubicharm/containerapps-albumapi-java/main/openshift/postgresql/postgresql.yaml
```

Postgresql の状態を確認する。Pod が Running で OK である。

```
oc get secret  
oc get pvc  
oc get deployment
```

```
oc get pods
```

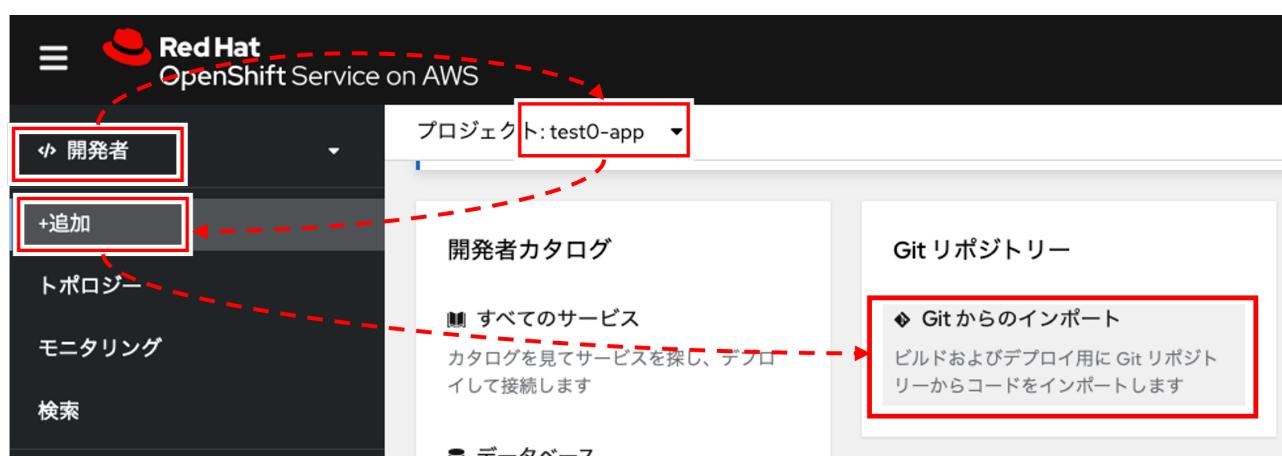
```
oc get pods -w
```

Album API プロジェクト作成

Album API プロジェクトを Git リポジトリからインポートする手順

Album API プロジェクトを作成する手順 Postgresql データベース用 Secret (postgresql) を作成する手順

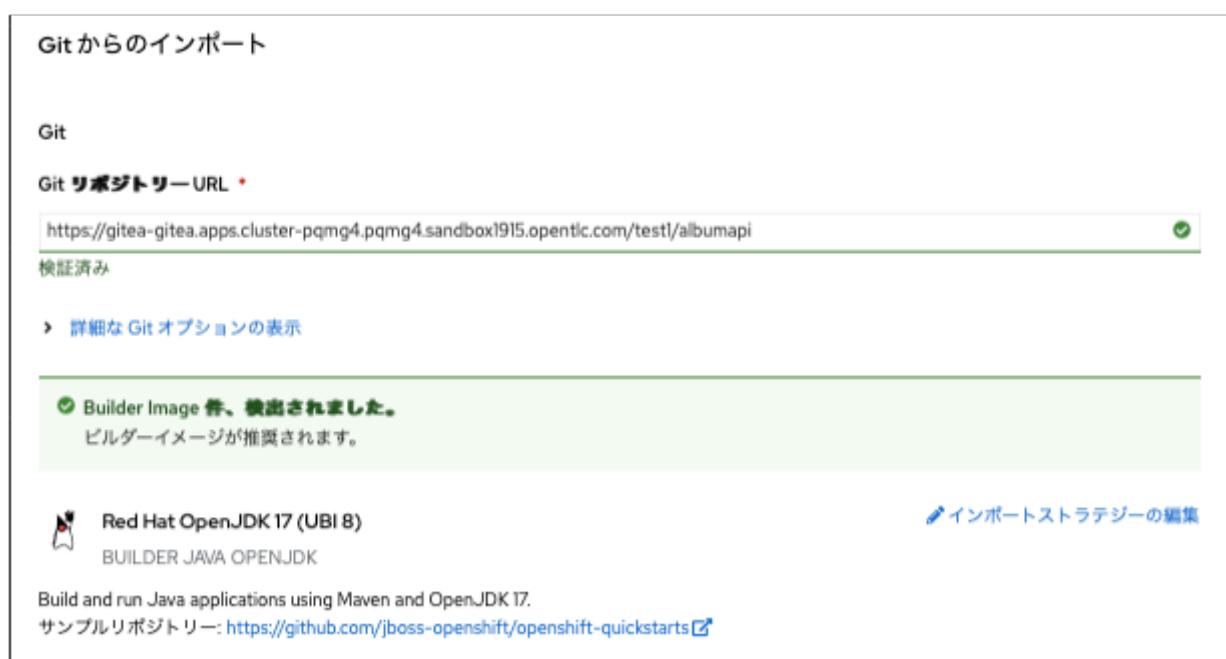
1. プロジェクト作成
2. データベース + PostgreSQL
3. プロジェクトを Git リポジトリ - Git リポジトリ接続



4. Git リポジトリ URL の確認

<https://gitea-gitea.apps.cluster-pqmg4.pqmg4.sandbox1915.opentlc.com/%USERID%/albumapi>

5. Builder Image として OpenJDK17 を選択



6. 亂子 albumapi 亂子
7. Deployment 亂子
8. >
 - spring_datasource◦
 - ◦: **spring_profile_active**
 - ◦: **postgresql**
 - JDBC URL◦
 - ◦+ConfigMap◦
 - ◦◦ **POSTGRESQL_URL**
 - ◦◦◦ **postgresql**
 - ◦◦◦: **database-url**
 - DB◦
 - ◦+ConfigMap◦
 - ◦◦ **POSTGRESQL_USER**
 - ◦◦◦ **postgresql**
 - ◦◦◦: **database-user**
 - DB◦
 - ◦+ConfigMap◦
 - ◦◦ **POSTGRESQL_PASSWORD**
 - ◦◦◦ **postgresql**
 - ◦◦◦: **database-password**
9. 亂子 8080 亂子
10. route 亂子

環境変数 (Runtime のみ)

名前	値
POSTGRES_URL	postgresql database-url
POSTGRES_USER	postgresql database-user
POSTGRES_PASSWORD	postgresql database-password
spring_profiles_active	postgresql

[+ 値の追加](#) [+ ConfigMap またはシークレットから追加](#)

詳細オプション

ターゲットポート

8080 [×](#)

トラフィックのターゲットポート。

route の作成
パブリック URL でコンポーネントを公開します

[▶ 詳細なルーティングオプションの表示](#)

名前をクリックして、ヘルスチェック、スケーリング、リソース制限、ラベル の詳細オプションにアクセスします。

[作成](#) [キャンセル](#)



route
route

REST API の構造

album-api URL

1. URL
2. URL の URL https://albumapi-%USERID%-app.apps.rosa.%SUBDOMAIN%/
Please visit /albums to see a list of albums. /albums URL
3. JSON

```
[  
 {  
   "id": 1,  
   "title": "OpenShift Virtualization\u30d5\u30a1\u30d5\u30a1\u30a4\u30a2\u30a4\u30a4\u30a1\u30a4\u30a2",  
   "artist": "\u30d5 \u30a1/\u30d5 \u30a4",  
   "price": 3080,  
   "book_url": "https://book.impress.co.jp/books/1124101080",  
   "image_url": "https://img.ips.co.jp/ij/24/1124101080/1124101080-520x.jpg"  
 },  
 {
```

```

    "id": 2,
    "title": "Ansible",
    "artist": "",
    "price": 3960,
    "book_url": "https://www.shuwasystem.co.jp/book/9784798068725.html",
    "image_url": "https://www.shuwasystem.co.jp/images/book/647676.jpg"
},
{
    "id": 3,
    "title": "OpenShift",
    "artist": "",
    "price": 4180,
    "book_url": "https://www.shoieisha.co.jp/book/detail/9784798172552",
    "image_url": "https://www.seshop.com/static/images/product/24696/L.png"
},
{
    "id": 4,
    "title": "Podman",
    "artist": "Daniel Walsh",
    "price": 4180,
    "book_url": "https://www.shuwasystem.co.jp/book/9784798070209.html",
    "image_url": "https://www.shuwasystem.co.jp/images/book/633833.jpg"
},
{
    "id": 5,
    "title": "Red Hat Enterprise Linux",
    "artist": "",
    "price": 4950,
    "book_url": "https://info.nikkeibp.co.jp/media/LIN/atcl/books/082200035/",
    "image_url": "https://cdn-
info.nikkeibp.co.jp/media/LIN/atcl/books/082200035/top.jpg?__scale=w:250,h:322&_sh=099
0b30450"
},
{
    "id": 6,
    "title": "Quarkus in Action (Free eBook Edition)",
    "artist": "Martin Stefanko/Jan Martiska",
    "price": 0,
    "book_url": "https://developers.redhat.com/e-books/quarkus-
action?extIdCarryOver=true&sc_cid=701f2000001Css5AAC",
    "image_url":
"https://developers.redhat.com/sites/default/files/styles/cheat_sheet_feature/public/E-
book%20cover%20graphic_Quarkus%20in%20Action.jpg.webp?itok=xZlT_iv4"
}
]

```

Album UI 介绍

Album UI (album-ui) 介绍

1. プロジェクトリスト

2. プロジェクト+ダッシュボード

3. プロジェクト詳細



4. URL: quay.io/keomizo_redhat/albumui-nodejs を選択

URLを選択

イメージのデプロイ

イメージ

イメージストリームまたはイメージレジストリーから既存のイメージをデプロイします。

外部レジストリーからのイメージ名

quay.io/keomizo_redhat/albumui-nodejs



検証済み

プライベートリポジトリからイメージをデプロイするには、イメージレジストリーの認証情報を使用して [イメージのフルシークレットを作成する](#) 必要があります。

非セキュアなレジストリーからのイメージの許可

5. Deploymentを選択

6. 端末番号 8080 を選択

7. route を選択

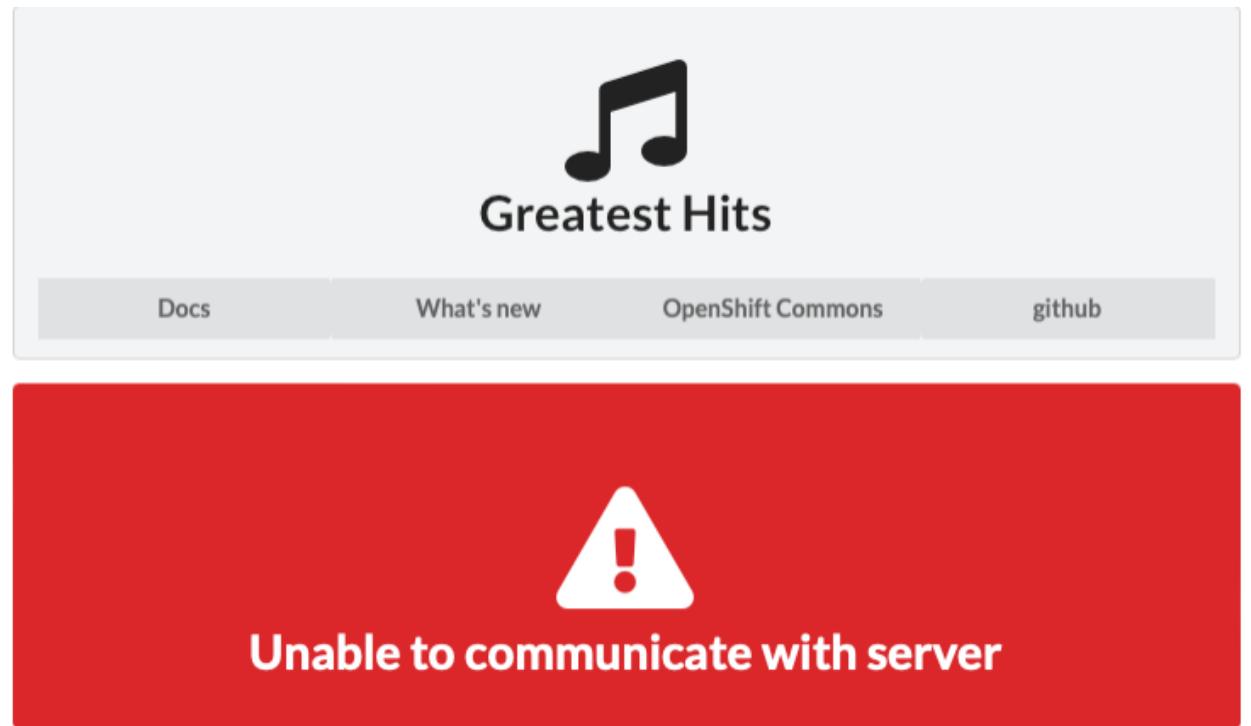
8. ダッシュボード

9. OK

10. URLを選択 URL: <https://albumui-nodejs-%USERID%-app.apps.rosa.%SUBDOMAIN%/>



11. ❌Unable to communicate with serverUnable to communicate with server



Album UI □ Album API □□□

Album UI URL API_BASE_URL

UI URL API_BASE_URL

1. Pod Deployment env
2. Configmap Pod

UI URL API_BASE_URL

UI URL API_BASE_URL

Deployment API_BASE_URL

1. Pod(D)album-ui
2. Pane Deployment
3. URL

UI	API_BASE_URL
	http://albumapi:8080

4. Deployment

Deployment Pod Pod

5. album-apiの実行

The screenshot shows the homepage of the Greatest Hits website. At the top, there is a large musical note icon and the text "Greatest Hits". Below the header, there is a navigation bar with links to "Docs", "What's new", "OpenShift Commons", and "github". The main content area displays two book covers. The first book, "OpenShift Virtualization サーバ仮想化 実践ガイド", has a blue cover with the OpenShift logo and the title in white. The second book, "実践 ANSIBLE", has a red cover featuring a golden robot-like character holding a tablet.

OpenShift Virtualization サーバ仮想化 実践ガイド
石川 純平/大村 真樹 3080

実践 ANSIBLE
八木澤健人/吳理沙/小野天平/長嶺精彦/山中裕史 3960

Configmapの作成

1. Configmapの作成

2. Configmapの確認

名前	albumui-config
名前	API_BASE_URL
値	http://albumapi:8080

3. Configmapの登録

4. Deploymentの登録

5. Configmapの登録

名前	API_BASE_URL の値
名前	ConfigMap albumui-config

□□□□□

API_BASE_URL

6. Deployment Pod Pod

Deployment Pod Pod

7. album-api

The screenshot shows the homepage of the Greatest Hits website, featuring a large musical note icon and the text "Greatest Hits". Below the header is a navigation bar with links to "Docs", "What's new", "OpenShift Commons", and "github". The main content area displays two book recommendations:

OpenShift Virtualization サーバ仮想化実践ガイド
石川 純平/大村 真樹 3080
The cover features the OpenShift logo and the title "OpenShift Virtualization サーバ仮想化 実践ガイド". It also includes a subtitle "コンテナと仮想マシンの共存と運用管理".

インフラの構成管理と自動化のための実践Ansible
八木澤健人/吳理沙/小野天平/長嶺精彦/山中裕史 3960
The cover features a yellow robot-like character holding a tablet. The title "実践ANSIBLE" is prominently displayed.

YAML Configmap



```
apiVersion: v1
kind: ConfigMap
metadata:
  name: albumui-config
  namespace: %USERID%-app
data:
  API_BASE_URL: http://albumapi:8080
  immutable: false
```

3. Skopeo

:imagesdir:../assets/images :sectnums: :sectnumlevels: 4

OpenShift

s2i(Source)

to

Image)

OpenShift → OpenShift

Skopeo

Skopeo → OSS → Red Hat → Enterprise

Linux → OSS → Red Hat → Enterprise

<https://www.redhat.com/ja/topics/containers/what-is-skopeo>

skopeo 介绍

RHEL → Github → <https://github.com/containers/skopeo/blob/main/install.md>

skopeo cli 介绍

skopeo → OpenShift → AWS ECR

OpenShift

OpenShift → cluster-admin

cluster-admin
cluster-admin

```
oc patch configs.imageregistry.operator.openshift.io/cluster --patch
'{"spec": {"defaultRoute": true}}' --type=merge
```

i

cluster-admin

```
export TOKEN=$(oc whoami -t)
export ROUTE=$(oc get route -n openshift-image-registry -o
jsonpath='{.items[0].spec.host}')
curl -k -H "Authorization: Bearer $TOKEN" "https://$ROUTE/v2/_catalog"
| jq
```

URL

```
default-route-openshift-image-registry.apps.rosa.%SUBDOMAIN%
```

ECR Token

Amazon ECR တွင် token အတွက်အကျဉ်းမှုများ

AWS CLI အသေဆိပ်အတွက်အကျဉ်းမှုများ



```
aws ecr get-login-password --region us-east-2
```

OpenShift Token

OpenShift တွင် token အတွက်အကျဉ်းမှုများ skopeo အသေဆိပ်အတွက် OpenShift CLI အသေဆိပ်အကျဉ်းမှုများ

```
oc login https://api.%SUBDOMAIN%:443 -u %USERID% -p openshift
```

OpenShift တွင် token အတွက်အကျဉ်းမှုများ



1. OpenShift တွင် token အတွက်အကျဉ်းမှုများ
2. AWS CLI အသေဆိပ်အတွက်
3. Docker တွင် token အတွက်အကျဉ်းမှုများ
4. %USERID% မှ openshift တွင် token အတွက်အကျဉ်းမှုများ
5. Display Token အတွက်

Skopeo အသေဆိပ်အကျဉ်းမှုများ

1. ECR token

```
export ECR_TOKEN=[ECR TOKEN]
```

```
skopeo login --tls-verify=false -u AWS -p $ECR_TOKEN %AWSACCOUNTID%.dkr.ecr.us-east-2.amazonaws.com
```

1. OpenShift တွင် token အတွက်အကျဉ်းမှုများ

```
oc login https://api.%SUBDOMAIN%:443 -u %USERID% -p {password}
export TOKEN=$(oc whoami -t)
skopeo login --tls-verify=false -u %USERID% -p $TOKEN default-route-openshift-
image-registry.apps.rosa.%SUBDOMAIN%
```

2. OpenShift 从本地仓库拉取 ECR 镜像

```
skopeo copy docker://default-route-openshift-image-  
registry.apps.rosa.%SUBDOMAIN%/%USERID%-app/albumui-nodejs  
docker://%AWSACCOUNTID%.dkr.ecr.us-east-2.amazonaws.com/%USERID%/albumui:latest
```

通过命令行输入凭证 credential 从本地仓库拉取镜像

```
oc login https://api.%SUBDOMAIN%:443 -u %USERID% -p {password}  
export TOKEN=$(oc whoami -t)  
export ECR_TOKEN=[ECR凭证]  
skopeo copy --src-creds %USERID%:$TOKEN docker://default-route-openshift-image-  
registry.apps.rosa.%SUBDOMAIN%/%USERID%-app/albumui --dest-creds AWS:$ECR_TOKEN  
docker://%AWSACCOUNTID%.dkr.ecr.us-east-2.amazonaws.com/albumui:latest
```

(通过命令行 ECR 从本地仓库拉取镜像)

Private 从 ECR 仓库拉取镜像到本地仓库，OpenShift 从本地仓库拉取镜像

OpenShift 本地仓库

CLI 通过 OpenShift 本地仓库

ECR 本地 Image Pull Secret

1. OpenShift 本地仓库
2. ECR 本地仓库 Pull Secret

```
oc create secret docker-registry ecr-secret --  
docker-server=%AWSACCOUNTID%.dkr.ecr.us-east-2.amazonaws.com --docker-user  
name=AWS --docker-password=$(aws ecr get-login-password)
```

OpenShift GUI 本地 Manifest 本地仓库拉取镜像

本地仓库拉取镜像 (GUI 方式)

1. 登录 OpenShift GUI
2. 新建+本地仓库
3. 本地仓库拉取镜像
4. 本地仓库拉取镜像 ECR URI

%AWSACCOUNTID%.dkr.ecr.us-east-2.amazonaws.com/album/albumui:latest

5. 本地仓库拉取镜像

Manifest

1. Deployment

```
oc create deployment albumui --image=%AWSACCOUNTID%.dkr.ecr.us-east-2.amazonaws.com/album/albumui:latest --dry-run=client -o yaml > deployment-albumui.yaml  
oc apply -f deployment-albumui.yaml
```

2. Service

```
oc create service clusterip albumui --tcp=8080 --dry-run=client -o yaml > service-albumui.yaml  
oc apply -f service-albumui.yaml
```

3. Route

```
oc create route edge albumui --service=albumui --port 8080 --dry-run=client -o yaml > route-albumui.yaml  
oc apply -f route-albumui.yaml
```

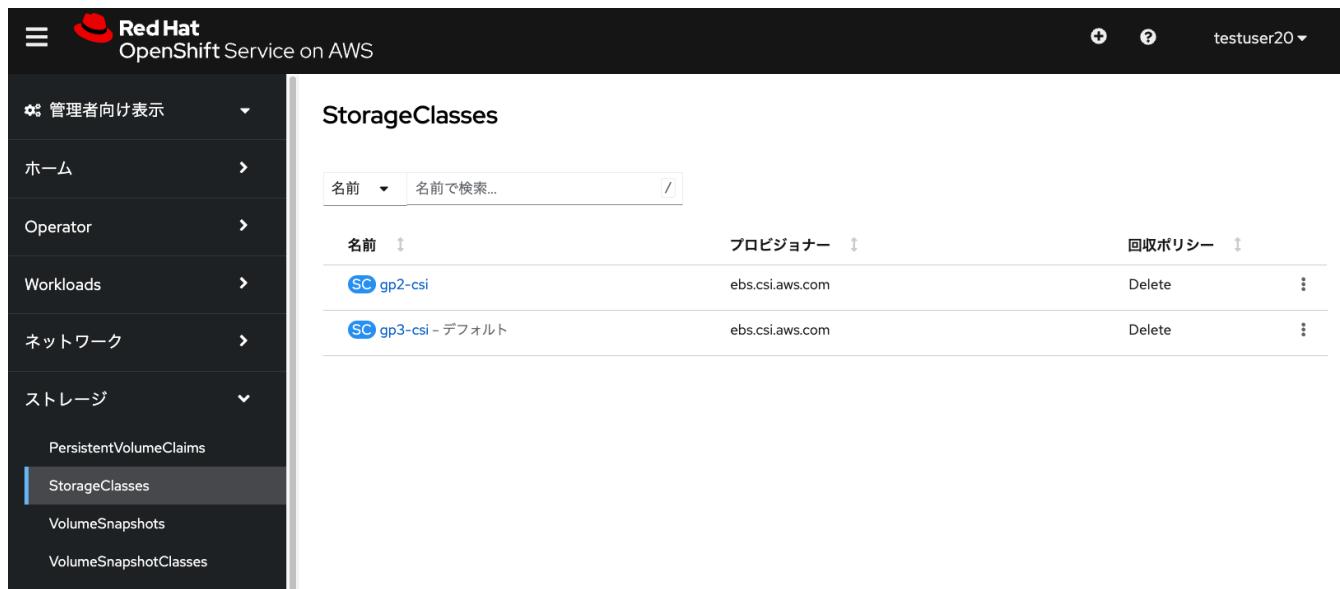
4. Amazon EBS

Amazon EBS

Amazon EBSはAmazon Elastic Block Storeの略称で、Amazonが提供するストレージサービスです。

Persistent Volume Claim (PVC)

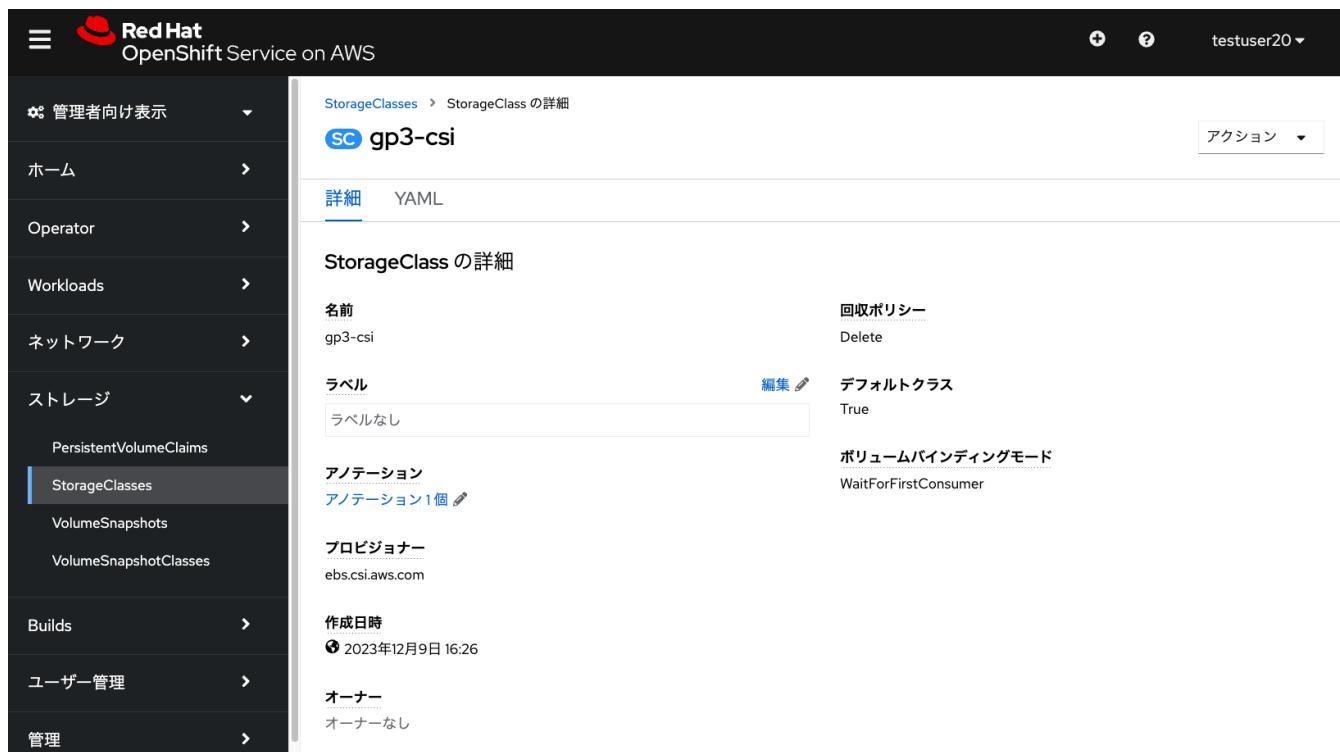
ROSAではAmazon Elastic Block Store (EBS) を使用するためには、Amazon EBS(gp2, gp3)を用意する必要があります。



The screenshot shows the Red Hat OpenShift Service on AWS interface. The left sidebar is collapsed. The main area displays a table titled "StorageClasses". The table has three columns: "名前" (Name), "プロビジョナー" (Provisioner), and "回収ポリシー" (Reclaim Policy). There are two entries:

名前	プロビジョナー	回収ポリシー
SC gp2-csi	ebs.csi.aws.com	Delete
SC gp3-csi - デフォルト	ebs.csi.aws.com	Delete

Amazon EBS(gp3)を用意する手順は、以下の通りです。



The screenshot shows the detailed view of a StorageClass named "gp3-csi". The left sidebar is collapsed. The top navigation bar shows the path "StorageClasses > StorageClass の詳細". The main area is titled "StorageClass の詳細" and contains the following information:

名前	回収ポリシー
gp3-csi	Delete

Below this, there are sections for "ラベル" (Labels), "アノテーション" (Annotations), "プロビジョナー" (Provisioner), "作成日時" (Created At), and "オーナー" (Owner).

gp3 PersistentVolumeClaim (PersistentVolumeClaim, PVC) を作成

The screenshot shows the Red Hat OpenShift Service on AWS interface. The left sidebar has a 'PersistentVolumeClaims' section selected under 'Storage'. The main area is titled 'PersistentVolumeClaim の作成' (Create PersistentVolumeClaim). It shows the following configuration:

- StorageClass:** gp3-csi
- PersistentVolumeClaim 名:** test-pvc-20
- アクセスモード:** 単一ユーザー (RWO) (selected)
- サイズ:** 1 GiB
- ポリュームモード:** ファイルシステム (selected)

At the bottom are '作成' (Create) and 'キャンセル' (Cancel) buttons.

PVC1 PVC1 PVC1 PVC1

gp3 WaitForFirstConsumer
Pod Pending Immediate PVC

The screenshot shows the Red Hat OpenShift Service on AWS web interface. The left sidebar has a 'PersistentVolumeClaims' section selected under 'Storage'. The main content area shows a PersistentVolumeClaim named 'test-pvc-20' in the 'test-project20' namespace. The 'Pending' status is indicated. The 'Details' tab is selected, showing fields like Name (test-pvc-20), Namespace (test-project20), Labels (ラベルなし), Annotations (アノテーションなし), and Creation Time (2023年12月10日 13:04). Other tabs include 'YAML', 'Events', and 'VolumeSnapshots'.

PVCとPod

PodとPersistentVolumeClaimのYAMLを比較してみる

PodとKubernetes/OpenShiftの構成要素
 ポッドYAML構成要素の構造(OpenShift/CentOS等の)は
 ポッドの構成要素と構造が似ています。
 PodとPersistentVolumeClaimの構成要素は1つPodと1つPersistentVolumeClaimです。

構成要素を比較する+構成要素を比較するYAMLを比較してみる

```
apiVersion: v1
kind: Pod
metadata:
  name: test-ebs
  namespace: %USERID%-app
spec:
  volumes:
    - name: ebs-storage-vol
```

```

persistentVolumeClaim:
  claimName: test-pvc-20
containers:
- name: test-ebs
  image: centos:latest
  command: [ "/bin/bash", "-c", "--" ]
  args: [ "while true; do touch /mnt/ebs-data/verify-ebs && echo 'hello ebs' && sleep 30; done;" ]
  volumeMounts:
    - mountPath: "/mnt/ebs-data"
      name: ebs-storage-vol
securityContext:
  allowPrivilegeEscalation: false
  seccompProfile:
    type: RuntimeDefault

```

test-ebsのPodを確認するPodの状態を確認するPod名はtest-pvc-20でPVC名はtest-pvc-20であることを確認する

PVC	Status	PersistentVolumes	Capacity
test-pvc-20	Bound	pvc-5269c4d8-b835-4295-a184-f13c7lddb620	1 GiB

Podの状態を確認する

行	ログ
1	hello ebs
2	hello ebs
3	hello ebs
4	hello ebs
5	hello ebs
6	hello ebs
7	hello ebs
8	hello ebs

[詳細](#) [Metrics](#) [YAML](#) [環境](#) [ログ](#) [イベント](#) [ターミナル](#)

接続中 test-ebs

[+] 拡張

```
sh-4.4$ df -h | grep ebs
/dev/nvme2n1      974M   24K  958M   1% /mnt/ebs-data
sh-4.4$ mount | grep ebs
/dev/nvme2n1 on /mnt/ebs-data type ext4 (rw,relatime,seclabel)
sh-4.4$
sh-4.4$
sh-4.4$ echo test > /mnt/ebs-data/testfile
sh-4.4$ ls -lh /mnt/ebs-data/
total 20K
drwxrws---. 2 root          1000800000 16K Dec 10 04:08 lost+found
-rw-r--r--. 1 1000800000 1000800000     5 Dec 10 04:16 testfile
-rw-r--r--. 1 1000800000 1000800000     0 Dec 10 04:16 verify-ebs
sh-4.4$ █
```

Podのターミナルでecho命令を実行した結果、/mnt/ebs-dataディレクトリにtestfileが作成された。Pod内から直接EBS volumesにアクセスできる。

Pod → Pod → Podの構造で、Pod2はPod1のサブポッドである。

Amazon EBS → Pod → Podの構造で、Pod2はPod1のサブポッドである。



Amazon

EBS → PVC → 1 → Pod → Pod

...

1 → EBS → PVC → 39 → Pod → Pod

...

Amazon EFS Container Storage Interface(CSI. Kubernetes用のAPI)を介してAWS EFS CSI Driver OperatorがEBS volumesをマウントする。

ROSA HCPがAWS STSを介してAmazon EFSをマウントするIAMロールを付与する。

Red Hat
OpenShift Service on AWS

プロジェクト:すべてのプロジェクト ▾

OperatorHub

Kubernetes コミュニティーより Red Hat パートナーの Operator をご覧ください。商用ソフトウェアの購入は、[Red Hat Marketplace](#) をご利用ください。開発者向けにオプションのアドオンおよび共有サービスを提供するには、クラスターに Operator をインストールしてください。Operator の機能は、インストール後に、セルフサービス機能が提供される [開発者カタログ](#) に表示されます。

すべての項目

すべての項目

検索: EFS CSI

1項目

AI/Machine Learning

Application Runtime

Big Data

Cloud Provider

Database

Developer Tools

Development Tools

Drivers and plugins

Integration & Delivery

Logging & Tracing

Red Hat

AWS EFS CSI Driver Operator

Red Hat による提供

Install and configure AWS EFS CSI driver.

OperatorHub インストール済みの Operator Workloads ネットワーク ストレージ Builds

5. ROSAの構成

ロギング

ROSAnetでロギングを構成するには、ROSAnetのOpenShiftクラスタにAmazon CloudWatch Logsを構成する必要があります。

Loki Logging構成



ROSAnetでロギングを構成するには、ROSAnetのOpenShiftクラスタにAmazon CloudWatch Logsを構成する必要があります。

ROSAnetでロギングを構成するには、ROSAnetのOpenShiftクラスタにAmazon CloudWatch Logsを構成する必要があります。

1. Lokiを構成するためのAmazon S3とAWS STSのIAMロールを取得します。

2. Amazon S3のロールを構成します。

3. ROSAnetのOpenShiftクラスタにAmazon S3とAWS STSのIAMロールを割り当てます。

ROSAnetでロギングを構成するには、ROSAnetのOpenShiftクラスタにAmazon CloudWatch Logsを構成する必要があります。

Amazon S3とAWS STSのIAM構成

AWSアカウントのAWS CLIとAmazon S3のAWS IAMとAWS STSのIAMを構成します。IAMポリシーを構成するには、AWSマネジメントコンソールを使用します。

ROSAnetでロギングを構成するには、Amazon S3 Full Access IAMポリシーを構成する必要があります。

rosa-hcp-s3-role 情報 削除

Allows S3 to call AWS services on your behalf.

概要 編集

作成日: March 22, 2025, 22:16 (UTC+09:00)

最後のアクティビティ: 39 分前

ARN: arn:aws:iam:█████████████████████████████████████:role/rosa-hcp-s3-role

最大セッション時間: 1 時間

許可 信頼関係 タグ 最終アクセス日時 セッションを取り消す

許可ポリシー (1) 情報 削除 許可を追加

最大 10 個の管理ポリシーを添付できます。

絞り込み タイプ: すべてのタイプ

検索	ポリシー名	タイプ	アタッチされたエンティティ
	AmazonS3FullAccess	AWS 管理	2

rosa-hcp-s3-role 情報

Allows S3 to call AWS services on your behalf.

削除

概要

編集

作成日

March 22, 2025, 22:16 (UTC+09:00)

ARN

arn:aws:iam:XXXXXXXXXX:role/rosa-hcp-s3-role

最後のアクティビティ

40 分前

最大セッション時間

1 時間

許可

信頼関係

タグ

最終アクセス日時

セッションを取り消す

信頼されたエンティティ

信頼ポリシーを編集

指定された条件でこのロールを引き受けることができるエンティティ。

```
1 [ {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Effect": "Allow",  
6             "Principal": {  
7                 "Federated": "arn:aws:iam:XXXXXXXXXX:oidc-provider/oidc.op1.openshiftapps.com/289dfjXXXXXXXXXX"  
8             },  
9             "Action": "sts:AssumeRoleWithWebIdentity",  
10            "Condition": {  
11                "StringEquals": {  
12                    "oidc.op1.openshiftapps.com/289dfjXXXXXXXXXX:sub": "system:serviceaccount:openshift-logging:logging-loki"  
13                }  
14            }  
15        }  
16    ]  
17 }]
```

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "Federated": "arn:aws:iam::<AWS_ACCOUNT_ID>:oidc-provider/<AWS_IAM_ID_PROVIDER_ID>"  
            },  
            "Action": "sts:AssumeRoleWithWebIdentity",  
            "Condition": {  
                "StringEquals": {  
                    "<AWS_IAM_ID_PROVIDER_ID>:sub": "system:serviceaccount:openshift-logging:logging-loki"  
                }  
            }  
        }  
    ]  
}
```

AWS IAM IDXXXXXXXXXX OpenShift ROSAopenshift-logging logging-lokiAmazon S3

Loki

Operator LokiStackOpenShift Amazon S3



ROSAXXXXXX

rosa

list

oidc-provider

ROSAXXXXXXAWS

IAM

IDXXXXXXXXXX oidc.op1.openshiftapps.com/289dfjXXXXXX AWS IAM

ID₁XXXXXXXXXXXXID₂XXXXXX

```
$ rosa list oidc-provider
I: Fetching OIDC providers
OIDC PROVIDER ARN
Cluster ID      In Use
arn:aws:iam::<AWS_ACCOUNT_ID>:oidc-provider/oidc.op1.openshiftapps.com/289dfjXXXXXX
2el3cammYYYYYY Yes
```

IAM₁XXXXXXARN₂XXXXXX

Amazon S3₁XXXXXX

AWS₁XXXXXXAWS CLI₂ Amazon S3₃XXXXXX

```
aws s3api create-bucket \
--bucket amzn-s3-demo-bucket1$(uuidgen | tr -d - | tr '[[:upper:]]' '[[:lower:]]' ) \
--region us-east-2 \
--create-bucket-configuration LocationConstraint=us-east-2
```

AWS₁XXXXXXROSAROSA HCP₂XXXXXX

XXXXXX

OpenShift Logging₁XXXXXXOperator₂XXXXXX

OpenShift Logging₁XXXXXXOperator₂XXXXXX(cluster-admin₃XXXXXX)XXXXXX

OperatorHub₁Red Hat OpenShift Logging Operator₂XXXXXX 1XXXXXX
XXXXXXOperator₁vector₂Loki₃CloudWatch₄XXXXXX

The screenshot shows the Red Hat OpenShift Service on AWS web interface. The left sidebar has a navigation menu with items like '管理者向け表示', 'ホーム', 'Operator', 'OperatorHub' (which is selected), 'インストール済みの Operator', 'Workloads', 'ネットワーク', 'ストレージ', 'Builds', and 'モニタリング'. The main content area has a header 'プロジェクト: test-project20'. Below it, there's a section titled 'OperatorHub' with a sub-section 'すべての項目'. A search bar at the top right of this section contains the text 'openshift logging'. A single search result is shown: 'Red Hat OpenShift Logging' by Red Hat, Inc. The result card includes a Red Hat logo, the operator name, and a brief description: 'The Red Hat OpenShift Logging Operator for OCP provides a means for configuring and...'.

Operator のインストール

更新チャネルのいずれかにサブスクライブして Operator をインストールし、Operator を最新の状態に保ちます。ストラテジーでは手動または自動の更新のいずれかを決定します。

更新チャネル * ②

stable-6.2

バージョン *

6.2.1

インストールモード *

- クラスターのすべての namespace (デフォルト)
Operator はすべての namespace で利用可能になります。
- クラスターの特定の namespace
Operator は単一の namespace でのみ利用可能になります。

インストール済みの namespace *

- Operator 推奨の namespace: PR openshift-logging
- namespace の選択

⚠ namespace はすでに存在します

namespace `openshift-logging` はすでに存在し、使用されます。他のユーザーはこの namespace にすでにアクセスできます。



CLF Cluster Log Forwarder ① 必須

ClusterLogForwarder is an API to configure forwarding logs.

You configure forwarding by specifying a list of `pipelines`, which forward from a set of named inputs to a set of named outputs.

LFME Log File Metric Exporter

A Log File Metric Exporter instance. LogFileMetricExporter is the Schema for the logFileMetricExporters API

更新の承認 * ②

- 自動
- 手動

インストール

キャンセル

OperatorHub Cluster Observability Operator リソース ディレクティブ モニタリング ネットワーク リソース ディレクティブ モニタリング ネットワーク

The screenshot shows the Red Hat OpenShift Service on AWS OperatorHub interface. The left sidebar has a navigation menu with items like Home, Operator, Workloads, Network, Storage, Builds, Monitoring, Compute, User Management, and Management. The 'Operator' item is currently selected. The main content area has a search bar at the top with the placeholder 'プロジェクト: すべてのプロジェクト'. Below it, there's a search result for 'Cluster observ' with one item shown:

すべての項目	すべての項目
AI/Machine Learning	Cluster observ
Application Runtime	1項目
Big Data	
Cloud Provider	
Database	
Developer Tools	
Development Tools	
Drivers and plugins	
Integration & Delivery	
Logging & Tracing	
Modernization & Migration	
Monitoring	
Networking	
OpenShift Optional	
Openshift Optional	
Other	
Security	

The result is a card for the 'Cluster Observability Operator' provided by Red Hat, with a brief description: 'A Go based Kubernetes operator to setup and manage highly available Monitoring Stack using...'

Operator のインストール

更新チャネルのいずれかにサブスクライブして Operator をインストールし、Operator を最新の状態に保ちます。ストラテジーでは手動または自動の更新のいずれかを決定します。

更新チャネル* ⑦

stable

バージョン*

1.1.1

インストールモード*

- クラスターのすべての namespace (デフォルト)
Operator はすべての namespace で利用可能になります。
- クラスターの特定の namespace
このモードはこの Operator ではサポートされません

インストール済みの namespace*

- Operator 推奨の namespace: PR openshift-cluster-observability-operator
- namespace の選択

⚠ namespace はすでに存在します

namespace openshift-cluster-observability-operator はすでに存在し、使用されます。他のユーザーはこの namespace にすでにアクセスできます。

更新の承認* ⑦

- 自動
- 手動



提供される API



PodMonitor defines monitoring for a set of pods



Probe defines monitoring for a set of static targets or ingresses



PrometheusRule defines recording and alerting rules for a Prometheus instance



ServiceMonitor defines monitoring for a set of services

OperatorHub に Loki Operator が登録されています。Community Loki Operator は Red Hat 提供の Loki Operator です。ARN は IAM によって定義されています。ARN は ARN によって定義されています。Operator は ARN によって定義されています。Operator は Loki によって定義されています。

Red Hat OpenShift Service on AWS

プロジェクト:すべてのプロジェクト

OperatorHub

Kubernetes ユニティーや Red Hat パートナーの Operator をご覧ください。商用ソフトウェアの購入は、Red Hat Marketplace をご利用ください。開発者向けにオプションのアドオンおよび共有サービスを提供するには、クラスターに Operator をインストールしてください。Operator の機能は、インストール後に、セルフサービス機能が提供される 開発者カタログ に表示されます。

すべての項目 検索: Loki Operator 1項目

Loki Operator
Red Hat による提供

The Loki Operator for OCP provides a means for configuring and managing a Loki stack for...

ソース

- Red Hat (1)
- Certified (0)

STS モードのクラスター

このクラスターは、AWS Security Token Service を使用してクラウド API をアクセスします。この Operator でクラウド API を使用して直接必要なアクションを実行するには、インストール時に(ポリシーが割り当てられた)ロール ARN を指定する必要があります。アップグレード前に、次のバージョンで必要なバーミッシュンをロールに適切に割り当てるための手順を実行する必要があるため、手動サブスクリプションを強く推奨します。詳細は、Operator の説明を参照してください。

ロール ARN * ①
arn:aws:iam::<AWS_ACCOUNT_ID>:role/<AWS_IAM_ROLE_NAME>

更新チャネル * ②
stable-6.2

バージョン *
6.2.0

インストールモード *
 クラスターのすべての namespace (デフォルト)
 クラスターの特定の namespace
このモードはこの Operator ではサポートされません

インストール済みの namespace *
 Operator 推奨の namespace: **openshift-operators-redhat**
 namespace の選択

namespace はすでに存在します
namespace **openshift-operators-redhat** はすでに存在し、使用されます。他のユーザーはこの namespace にすでにアクセスできます。

更新の承認 * ③
 自動
 手動

インストール キャンセル

ローカルストア

Loki

S3 (Amazon Simple Storage Service) ID + OpenShift + rosa-hcp-test-bucket-00001 us-

east-1 ロギング

```
apiVersion: v1
kind: Secret
metadata:
  name: logging-loki-s3
  namespace: openshift-logging
stringData:
  bucketnames: rosa-hcp-test-bucket-000001
  region: us-east-1
```

The screenshot shows the Red Hat OpenShift Service on AWS web interface. The left sidebar lists various project components like Home, Operator, Workloads, Network, Storage, Builds, Monitoring, Compute, User Management, and Management. The main area is titled 'YAML のインポート' (Import YAML) and contains a code editor with the following YAML configuration:

```
1 apiVersion: v1
2 kind: Secret
3 metadata:
4   name: logging-loki-s3
5   namespace: openshift-logging
6 stringData:
7   bucketnames: rosa-hcp-test-bucket-000001
8   region: us-east-1
```

At the bottom of the code editor, there are two buttons: '作成' (Create) and 'キャンセル' (Cancel). The 'Create' button is highlighted with a red box.

openshift-logging

OpenShift プロジェクトで Loki を構成するための YAML 定義を示す。OpenShift と連携して、YAML で構成可能。

プロジェクト名: openshift-logging

ロギング名: logging-loki-s3

サイズ: 1x.demo

LokiStack

LokiStack の構成を示す。



1x.demo ロギング用 LokiStack の構成

```
apiVersion: loki.grafana.com/v1
kind: LokiStack
metadata:
  name: logging-loki
  namespace: openshift-logging
spec:
  managementState: Managed
  size: 1x.demo
  storage:
```

```

schemas:
- effectiveDate: '2024-10-01'
  version: v13
secret:
  name: logging-loki-s3
  type: s3
storageClassName: gp3-csi
tenants:
  mode: openshift-logging

```

The screenshot shows the Red Hat OpenShift Service on AWS interface. The left sidebar contains navigation links for Home, Operator, Workloads, Network, Storage, Builds, Monitoring, Compute, User Management, and Management. The main area is titled "YAML のインポート" (Import YAML) and displays a code editor with the following YAML configuration:

```

1  apiVersion: loki.grafana.com/v1
2  kind: LokiStack
3  metadata:
4    name: logging-loki
5    namespace: openshift-logging
6  spec:
7    managementState: Managed
8    size: 1x.demo
9    storage:
10      schemas:
11        - effectiveDate: '2024-10-01'
12        | version: v13
13      secret:
14        name: logging-loki-s3
15        type: s3
16      storageClassName: gp3-csi
17      tenants:
18        mode: openshift-logging

```

Below the code editor are two buttons: "作成" (Create) and "キャンセル" (Cancel). The top right corner shows the user is logged in as "cluster-admin".

UIPlugin ローカルストア OpenShift ローカルストア LokiStack ログ

```

apiVersion: observability.openshift.io/v1alpha1
kind: UIPlugin
metadata:
  name: logging
spec:
  type: Logging
  logging:
    lokiStack:
      name: logging-loki

```

The screenshot shows the Red Hat OpenShift Service on AWS UI. On the left is a sidebar with navigation links: ホーム, Operator, Workloads, ネットワーク, ストレージ, Builds, モニタリング, コンピュート, ユーザー管理, and 管理. The main area has a title 'YAML のインポート' and a note: 'YAML または JSON ファイルをエディターにドラッグアンドドロップするか、手動でファイルを入力し、---を使用してそれぞれの定義を分離します。'. A code editor window displays the following YAML configuration:

```
1 apiVersion: observability.openshift.io/v1alpha1
2 kind: UIPlugin
3 metadata:
4   name: logging
5 spec:
6   type: Logging
7   logging:
8     lokiStack:
9       name: logging-loki
```

At the bottom are '作成' and 'キャンセル' buttons, and a small icon in the bottom right corner.

The screenshot shows the Red Hat OpenShift Service on AWS UI. The sidebar includes 'Logs' under the 'Logs' section. The main area is titled 'Logs' and contains a search bar with 'Content' and 'Severity' dropdowns, and buttons for 'Export as CSV', 'Explain Log Volume', and 'Run Query'. A dropdown menu for 'application' is open, showing options: application (selected), infrastructure, and audit. Below the search bar is a table with columns 'Date' and 'Message'. A message at the bottom says '⚠ No datapoints found'. At the top right are buttons for 'Show Histogram', 'Last 1 hour', 'Refresh off', and a refresh icon.

Logs

Logs

collector

LokiStack

```

oc create sa collector -n openshift-logging
oc adm policy add-cluster-role-to-user logging-collector-logs-writer -z collector -n
openshift-logging
oc adm policy add-cluster-role-to-user collect-application-logs -z collector -n
openshift-logging
oc adm policy add-cluster-role-to-user collect-audit-logs -z collector -n openshift-
logging
oc adm policy add-cluster-role-to-user collect-infrastructure-logs -z collector -n
openshift-logging

```

OpenShiftコンソール(**cluster-admin** ユーザー)のOpenShift Web Terminal

The screenshot shows the OpenShift Web Terminal interface. On the left, there's a sidebar with navigation links: '管理者向け表示', 'ホーム', 'Operator', 'Workloads', and 'ネットワーク'. The main area is titled 'Logs' and contains a search bar with 'Content' and 'Severity' dropdowns, and buttons for 'Export as CSV', 'Explain Log Volume', 'Run Query', 'Show Resources', 'Show Stats', and 'Show Query'. Below the search bar is a table with columns 'Date' and 'Message'. A yellow warning icon indicates 'No datapoints found'. At the bottom of the terminal window, there's a command-line interface (CLI) window titled 'ターミナル1' showing the output of the command 'oc create sa collector -n openshift-logging'.

```

Welcome to the OpenShift Web Terminal. Type "help" for a list of installed CLI tools.
bash-5.1 ~ $ oc whoami
cluster-admin
bash-5.1 ~ $
bash-5.1 ~ $ oc create sa collector -n openshift-logging
oc adm policy add-cluster-role-to-user logging-collector-logs-writer -z collector -n openshift-logging
oc adm policy add-cluster-role-to-user collect-application-logs -z collector -n openshift-logging
oc adm policy add-cluster-role-to-user collect-audit-logs -z collector -n openshift-logging
oc adm policy add-cluster-role-to-user collect-infrastructure-logs -z collector -n openshift-logging
error: failed to create serviceaccount: serviceaccounts "collector" already exists
clusterrole.rbac.authorization.k8s.io/logging-collector-logs-writer added: "collector"
clusterrole.rbac.authorization.k8s.io/collect-application-logs added: "collector"
clusterrole.rbac.authorization.k8s.io/collect-audit-logs added: "collector"
clusterrole.rbac.authorization.k8s.io/collect-infrastructure-logs added: "collector"
bash-5.1 ~ $
bash-5.1 ~ $ 

```

vectorのLokiStackを定義するYAMLをOpenShiftコンソールに貼り付けます。

- vector: **collector**
- LokiStack: **logging-loki**

```

apiVersion: observability.openshift.io/v1
kind: ClusterLogForwarder
metadata:
  name: collector
  namespace: openshift-logging
spec:
  serviceAccount:
    name: collector
  outputs:
  - name: default-lokistack
    type: lokiStack
    lokiStack:
      authentication:

```

```

token:
  from: serviceAccount
target:
  name: logging-loki
  namespace: openshift-logging
tls:
  ca:
    key: service-ca.crt
    configMapName: openshift-service-ca.crt
pipelines:
- name: default-logstore
  inputRefs:
    - application
    - infrastructure
    - audit
  outputRefs:
    - default-lokistack

```

YAML のインポート

YAML または JSON ファイルをエディターにドラッグアンドドロップするか、手動でファイルを入力し、 を使用してそれぞれの定義を分離します。

```

1  apiVersion: observability.openshift.io/v1
2  kind: ClusterLogForwarder
3  metadata:
4    name: collector
5    namespace: openshift-logging
6  spec:
7    serviceAccount:
8      name: collector
9    outputs:
10   - name: default-lokistack
11     type: lokiStack
12     lokiStack:
13       authentication:
14         token:
15           from: serviceAccount
16         target:
17           name: logging-loki
18           namespace: openshift-logging
19       tls:
20         ca:
21           key: service-ca.crt
22           configMapName: openshift-service-ca.crt
23     pipelines:
24   - name: default-logstore
25     inputRefs:
26       - application
27       - infrastructure
28       - audit
29     outputRefs:
30       - default-lokistack

```

作成 キャンセル

YAML の inputRefs: について

- **application**

標準出力と標準エラー出力 (stdout/stderr) がロギングされる仕組みです。通常はコンソール出力

- **infrastructure** : ROSA が実行する環境 (openshift-* , kube-*)

OpenShift のインフラストラクチャ (コンポーネント) が監視される仕組みです。

- **audit** : 安全性監査 (auditd) が実行される仕組みです。

audit.log (/var/log/audit/audit.log) が監視される仕組みです。OpenShift Logging

OperatorによるRed Hat SRE 1による ROSA の構成

Red Hat SRE 1による ROSA の構成では、
collector-* Pod (vector) が openshift-logging リソースを監視する
collector-* Pod が openshift-logging リソースを監視する LokiStack が構成される。

The screenshot shows the Red Hat OpenShift Service on AWS console. The left sidebar is collapsed. The top navigation bar shows the Red Hat logo, the service name, and a user dropdown for 'cluster-admin'. The main content area has a header 'Pods' with a 'Pod の作成' button. A filter bar at the top of the table includes '名前' and '名前で検索...' fields. The table lists the following pods:

名前	ステータス	準備完了	再起動回数	オーナー	メモリー	CPU	作成済み
collector-tc9vx	Running	1/1	0	DS collector	296.8 MiB	0.008 コア	2025年5月1日 18:49
collector-v9rb	Running	1/1	0	DS collector	254.6 MiB	0.008 コア	2025年5月1日 18:49
logging-loki-ingester-0	Running	1/1	0	SS logging-loki-ingester	242.1 MiB	0.005 コア	2025年5月1日 18:28
logging-loki-querier-57dc8f449f-wx2wb	Running	1/1	0	RS logging-loki-querier-57dc8f449f	88.3 MiB	0.004 コア	2025年5月1日 18:28
logging-loki-distributor-864b7cbf46-6ml5w	Running	1/1	0	RS logging-loki-distributor-864b7cbf46	73.7 MiB	0.005 コア	2025年5月1日 18:28
cluster-logging-operator-7975f465bc-mszbv	Running	1/1	0	RS cluster-logging-operator-7975f465bc	64.6 MiB	0.002 コア	2025年5月1日 17:29
logging-loki-gateway-669f67d57f-gmhmm	Running	2/2	0	RS logging-loki-gateway-669f67d57f	59.2 MiB	0.003 コア	2025年5月1日 18:28
logging-loki-gateway-669f67d57f-8qh4l	Running	2/2	0	RS logging-loki-gateway-669f67d57f	56.7 MiB	0.006 コア	2025年5月1日 18:28

6. OpenShiftの監視とログ

監視とログ

OpenShiftの監視とログについて

OpenShiftの監視とログ

OpenShiftの監視とログについて(この)→Logs

cluster-admin

The screenshot shows the Red Hat OpenShift Service on AWS console interface. The left sidebar has a dark theme with white text. The 'Logs' option under the 'Workloads' section is highlighted with a blue bar. The main content area is titled 'Logs' and shows a table of log entries. The table has columns for 'Date' and 'Message'. The 'Message' column contains log lines like:

- I0501 09:58:34.97518 1
9.0.12:36194: write: co
- I0501 09:58:34.764197 1
8.0.12:48578: write: co
- I0501 09:58:34.455099 1
8.0.12:50474: write: cc
- :fffff:10.129.0.2 - - [
- <134>May 1 09:58:33 haproxy[1]: 10.129.0.73:53678 [01/May/2025:09:58:33.945] local_apiserver remote_apiserver/controlplane 1/2/20 21207 -- 37/37/36/36/0 0/0
- <134>May 1 09:58:33 haproxy[1]: 10.129.0.73:53244 [01/May/2025:09:58:33.668] local_apiserver remote_apiserver/controlplane 1/6/293 96632 -- 38/38/37/37/0 0/0
- <134>May 1 09:58:33 haproxy[1]: 10.129.0.73:53206 [01/May/2025:09:58:33.665] local_apiserver remote_apiserver/controlplane 1/5/291 10094 -- 39/39/38/38/0 0/0
- time="2025-05-01T09:58:33.761456452" level=info msg=“response.go.version=“go1.22.12 (Red Hat 1.22.12-2.el9_5) X:strictfp psruntime” http.request.host=“10.129.0.28:5000” http.request.id=8218e628-a14d-4f5c-9274-58bfede127d3 http.request.method=GET http.request.remoteaddr=“10.129.0.2:34570” http.request.uri=/healthz http.request.useragent=kube-probe/1.31 http.response.duration=“29.661μs” http.response.status=200 http.response.written=0
- time="2025-05-01T09:58:33.7585410962" level=info msg=“response.go.version=“go1.22.12 (Red Hat 1.22.12-2.el9_5) X:strictfp psruntime” http.request.host=“10.129.0.28:5000” http.request.id=2659e2d1-4d0f-432a-a663-708583db5be0 http.request.method=GET http.request.remoteaddr=“10.129.0.2:34552” http.request.uri=/healthz http.request.useragent=kube-probe/1.31 http.response.duration=“40.226μs” http.response.status=200 http.response.written=0
- <134>May 1 09:58:33 haproxy[1]: 10.129.0.73:52878 [01/May/2025:09:58:32.927] local_apiserver remote_apiserver/controlplane 1/3/827 2071761 -- 37/37/36/36/0 0/0

監視とログ(OpenShiftコンソール)の監視とログ

監視とログ

Podの監視とログ

Red Hat OpenShift Service on AWS

プロジェクト: test-project20

Pods > Pod の詳細

nodejs-ex-git-5bf8c9db55-7jpth Running

アクション

詳細 メトリクス YAML 環境 ログ イベント ターミナル Aggregated Logs

ログのストリーミング中です... nodejs-ex-git 現在のログ Search

ログ全体を表示 行の折り返し Raw ダウンロード 拡張

13 行

```

2 DEV_MODE=false
3 NODE_ENV=production
4 DEBUG_PORT=5858
5 Launching via npm...
6 npm info using npm@10.8.2
7 npm info using node@v20.18.2
8
9 > nodejs-rest-http-crude@4.0.0 start
10 > node .
11
12 {"level":30,"time":1746100131307,"pid":12,"hostname":"nodejs-ex-git-5bf8c9db55-7jpth","msg":"Listening on port 8080"}
13 {"level":50,"time":1746100131312,"pid":12,"hostname":"nodejs-ex-git-5bf8c9db55-7jpth","err":{"type":"AggregateError","message":"","cause":[{"type":"SyntaxError","message":"Unexpected identifier"}]}}

```

OpenShift Service on AWS のモニタリング機能を確認する

Red Hat OpenShift Service on AWS

プロジェクト: test-project20

モニタリング

イベント Dashboard Logs Metrics アラート サイレンス

Show Histogram Last 1 hour Refresh off Show Query

Content Search by Content Severity Show Resources Show Stats Export as CSV Explain Log Volume

Run Query

Namespaces test-project20 Clear all filters

Date ↓ Message ↑

Forbidden

Missing permissions to get logs

Make sure you have the required role to get application logs in this namespace.

Ask your administrator to grant you this role:

```

apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: view-application-logs
  namespace: <project-name>
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-logging-application-view
subjects:
- kind: User
  name: <testuser>
  apiGroup: rbac.authorization.k8s.io

```

OpenShift Service on AWS のモニタリング機能を確認する

OpenShift Service on AWS + YAML + YAML + YAML + view-application-logs
RoleBinding + %USERID% - app

OpenShift

%USERID%

OpenShift

%USERID%

OpenShift

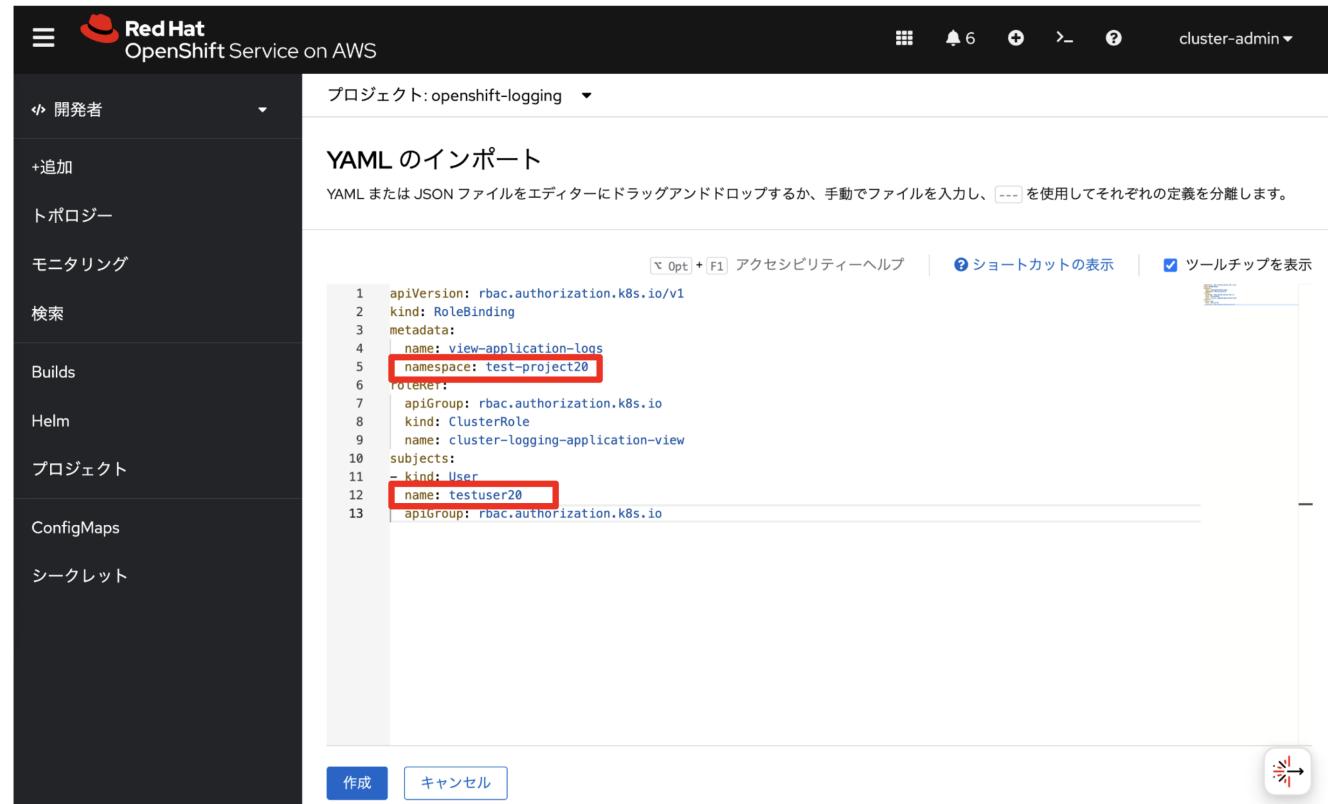
%USERID% - app

OpenShift RBAC 実践



The screenshot shows the OpenShift YAML editor interface. At the top, there are tabs for "YAML" and "Subject.kind.name". The "Subject.kind.name" tab is active, showing the role name "cluster-logging-application-view". Below the tabs, the YAML code for a RoleBinding is displayed:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: view-application-logs
  namespace: %USERID%-app
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-logging-application-view
subjects:
- kind: User
  name: %USERID%
  apiGroup: rbac.authorization.k8s.io
```



The screenshot shows the Red Hat OpenShift Service on AWS web interface. The left sidebar includes options like "開発者", "+追加", "トポロジー", "モニタリング", "検索", "Builds", "Helm", "プロジェクト", "ConfigMaps", and "シークレット". The main area is titled "YAML のインポート" and shows a YAML editor with the following code:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: view-application-logs
  namespace: test-project20
  rotoken:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-logging-application-view
subjects:
- kind: User
  name: testuser20
  apiGroup: rbac.authorization.k8s.io
```

Two specific lines in the YAML code are highlighted with red boxes: "namespace: test-project20" and "name: testuser20". At the bottom of the editor, there are "作成" (Create) and "キャンセル" (Cancel) buttons.

RoleBinding

Red Hat OpenShift Service on AWS

%USERID%

Red Hat OpenShift Service on AWS

The screenshot shows the Red Hat OpenShift Service on AWS web interface. The left sidebar is collapsed, showing '開発者' (Developer) and 'モニタリング' (Monitoring). Under Monitoring, there are sections for 'Builds', 'Helm', 'プロジェクト' (Project), 'ConfigMaps', 'シークレット' (Secrets), and 'Logs'. The 'Logs' section is currently selected and highlighted in blue.

The main content area is titled 'モニタリング' (Monitoring) and has tabs for 'Events', 'Dashboard', 'Logs' (which is active), 'Metrics', 'Alerts', and 'Sentinels'. Below the tabs is a search bar with filters for 'Content' (Search by Content) and 'Severity' (Show Resources, Show Stats, Export as CSV, Explain Log Volume, Show Query). A 'Run Query' button is also present.

The log table has columns for 'Date' (sorted descending) and 'Message'. It lists several log entries from May 1, 2025, at 20:48:51.313 to May 1, 2025, at 20:48:51.059. One entry shows a detailed stack trace of an AggregateError due to ECONNREFUSED during network connections.

```

{
  "level": 50,
  "time": "2025-05-01T11:48:51.059Z",
  "pid": 12,
  "hostname": "ip-10-0-0-244.us-east-2.compute.internal",
  "kubernetes": {
    "annotations": "[{"k8s.v1.annov.org/pod-networks": "[]"}]",
    "node": "ip-10-0-0-244.us-east-2.compute.internal"
  }
}

```

日付を選択する場合は、日付を指定して検索できます。日付範囲を指定して検索する場合は、日付範囲を指定して検索できます。

7. モニタリング

概要

ROSANerdHatSREがRed Hat OpenShift Service on AWS上にPrometheusを構成する手順

ROSANerdHatSREがRed Hat OpenShift Service on AWS上にPrometheusを構成する手順

- ROSAモニタリング (Platform monitoring)
- ユーザ定義プロジェクトモニタリング (User-defined projects monitoring)

ROSANerdHatSREがRed Hat OpenShift Service on AWS上にPrometheusを構成する手順



ROSANerdHatSREがRed Hat OpenShift Service on AWS上にPrometheusを構成する手順



ROSANerdHatSREがRed Hat OpenShift Service on AWS上にPrometheusを構成する手順

名前	表示名	ステータス	リクエスター	メモリー	CPU	作成済み
PR openshift-monitoring	表示名なし	Active	リクエスターなし	-	-	2023年12月9日 16:26
PR openshift-user-workload-monitoring	表示名なし	Active	リクエスターなし	4,094.6 MiB	0.149 コア	2023年12月9日 16:25
PR openshift-customer-monitoring	表示名なし	Active	リクエスターなし	743.9 MiB	0.057 コア	2023年12月9日 16:25

ROSANerdHatSREがRed Hat OpenShift Service on AWS上にPrometheusを構成する手順



openshift-monitoring

Red

Hat

SRE

openshift-monitoring

openshift-monitoring

Red Hat OpenShift Service on AWS

プロジェクト: openshift-monitoring

Pods

Pod の作成

名前	ステータス	準備完了	再起動回数	オーナー	メモリー	CPU	作成済み
Prometheus-k8s-1	Running	6/6	0	SS prometheus-k8s	1,402.5 MiB	0.049 コア	2023年12月9日 16:50
Prometheus-k8s-0	Running	6/6	0	SS prometheus-k8s	1,379.6 MiB	0.051 コア	2023年12月9日 16:50
Thanos-querier-845f7548df-k8bln	Running	6/6	0	RS thanos-querier-845f7548df	171.5 MiB	0.006 コア	2023年12月9日 16:49
Thanos-querier-845f7548df-t2zq8	Running	6/6	0	RS thanos-querier-845f7548df	168.7 MiB	0.006 コア	2023年12月9日 16:49
Alertmanager-main-0	Running	6/6	0	SS alertmanager-main	154.1 MiB	0.003 コア	2023年12月9日 16:50
Alertmanager-main-1	Running	6/6	0	SS alertmanager-main	143.8 MiB	0.003 コア	2023年12月9日 16:50
Kube-state-metrics-5cd69bf5d-tfgl5	Running	3/3	0	RS kube-state-metrics-5cd69bf5d	109.3 MiB	0.002 コア	2023年12月9日 16:49

ROSA

Red

Hat

SRE

ROSA

Red Hat OpenShift Service on AWS

プロジェクト: openshift-monitoring

PersistentVolumeClaims

PersistentVolumeClaim の作成

名前	ステータス	PersistentVolumes	容量	使用済み	StorageClass
PVC prometheus-data-prometheus-k8s-0	Bound	PV pvc-28626527-d9f0-4bdd-8a29-a239272fcf18	100 GiB	1.14 GiB	SC gp3-csi
PVC prometheus-data-prometheus-k8s-1	Bound	PV pvc-a99c7f9e-9459-4386-88bd-22555673609d	100 GiB	1.13 GiB	SC gp3-csi

PersistentVolume

PersistentVolume

Pod

openshift-user-workload-monitoring

Pod

Kubernetes nodeSelector

Pod

名前	ステータス	準備完了	再起動回数	オーナー	メモリー	CPU	作成済み
Prometheus-user-workload-1	Running	6/6	0	SS prometheus-user-workload	220.7 MiB	0.025 コア	2023年12月9日 16:49
Prometheus-user-workload-0	Running	6/6	0	SS prometheus-user-workload	211.3 MiB	0.026 コア	2023年12月9日 16:49
Thanos-ruler-user-workload-1	Running	4/4	0	SS thanos-ruler-user-workload	123.9 MiB	0.003 コア	2023年12月9日 16:49
Thanos-ruler-user-workload-0	Running	4/4	0	SS thanos-ruler-user-workload	116.5 MiB	0.003 コア	2023年12月9日 16:49
Prometheus-operator-74ccdc5c-g7zr6	Running	2/2	0	RS prometheus-operator-74ccdc5c	74.6 MiB	0.001 コア	2023年12月9日 16:49



ROSA HCPの構築 rosa create cluster のHCPの構築を手順通り実行する
monitoring でPodの監視機能を有効にする

監視対象としてPodを登録する

監視対象としてPodを登録する

監視対象としてPodを登録する

openshift-user-workload-

monitoring でPodを登録する

user-workload-monitoring-config

監視対象としてPodを登録する

監視対象としてPodを登録する

監視対象としてPodを登録する



KubernetesのConfigMapを用いて監視機能を有効にする

OpenShiftのConfigMapを用いて監視機能を有効にする → Workloads → ConfigMaps

ConfigMapを用いて監視機能を有効にする OpenShift CLI(oc)を用いて監視機能を有効にする



監視対象としてPodを登録する

```

kind: ConfigMap
apiVersion: v1
metadata:
  name: user-workload-monitoring-config
  namespace: openshift-user-workload-monitoring
data:
  config.yaml: |
    prometheus:
      retention: 30d
      volumeClaimTemplate:
        spec:
          resources:
            requests:
              storage: 200Gi
  
```

8. ROSAのモニタリング

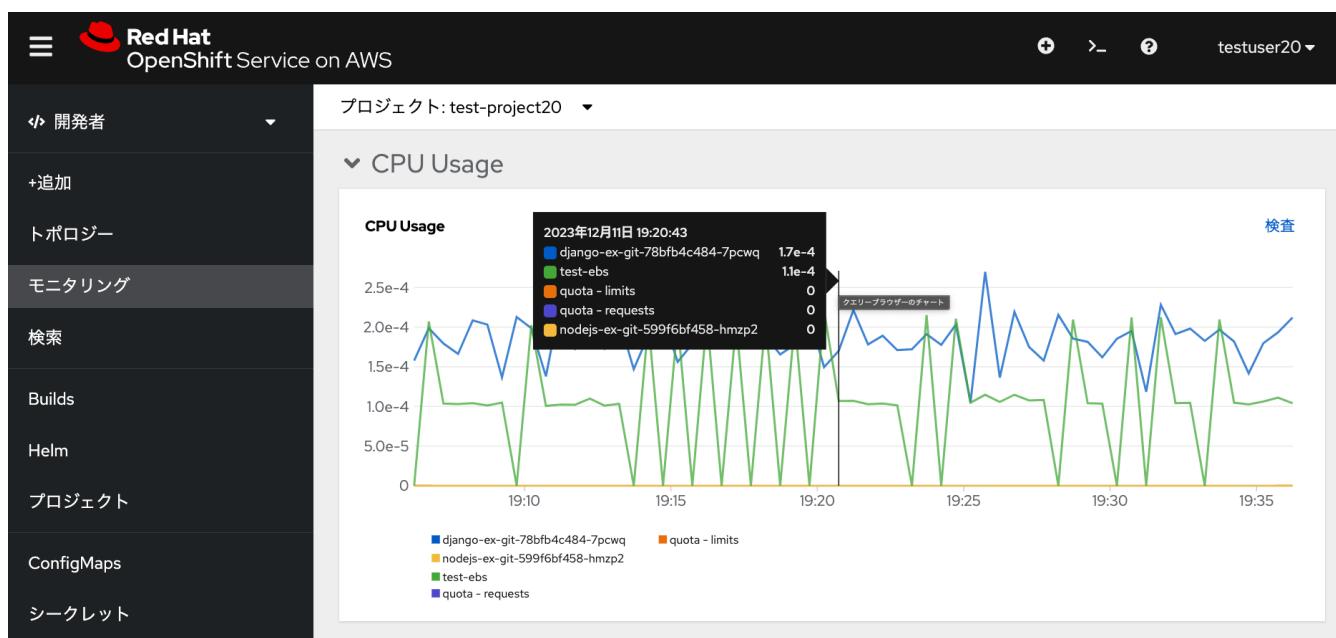
モニタリング

ROSAnetでモニタリング機能を実装するには、OpenShift Service on AWS (openshift-monitoring) を利用する。

モニタリング構成

ROSAnetでモニタリング構成 (openshift-monitoring) を実装する。

モニタリング構成 (openshift-monitoring) の構成は、OpenShift Service on AWS (openshift-monitoring) の CPU 使用率 / リソース使用量 / リクエスト数 / ファイル IO 使用量を監視する。



ROSAnetでモニタリング機能を実装するには、OpenShift Service on AWS (openshift-monitoring) を利用する。

モニタリング

[ダッシュボード](#) Metrics アラート Silences イベント

ダッシュボード

Kubernetes / Compute Resources / Namespace (Pods) ▾

時間の範囲

最後の 30 分 ▾

更新間隔

30 秒 ▾

CPU Utilisation
(from requests)

検
査

52.72%

CPU Utilisation
(from limits)

検
査

-

Memory Utilisation
(from requests)

検
査

119.94%

Memory Utilisation
(from limits)

検
査

-

▼ CPU Usage

CPU Usage

検査



PodのCPU使用率を示す(左)と、(右)のCPU使用率

PodのCPU使用率を示す(左)と、(右)のCPU使用率を示す。CPU/メモリの監視

KubernetesのPodのCPU使用率

監視するCPU使用率を示す(左)と、(右)のCPU使用率

監視するCPU使用率を示す(左)と、(右)のCPU使用率

監視するPodのCPU使用率

監視するCPU使用率を示す(左)と、(右)のCPU使用率

監視するKubernetesのCPU使用率

Metrics

Metrics

Metrics(CPU 使用率)

Prometheus(PromQL)

モニタリング

ダッシュボード Metrics イベント

CPU 使用量

PromQL の非表示

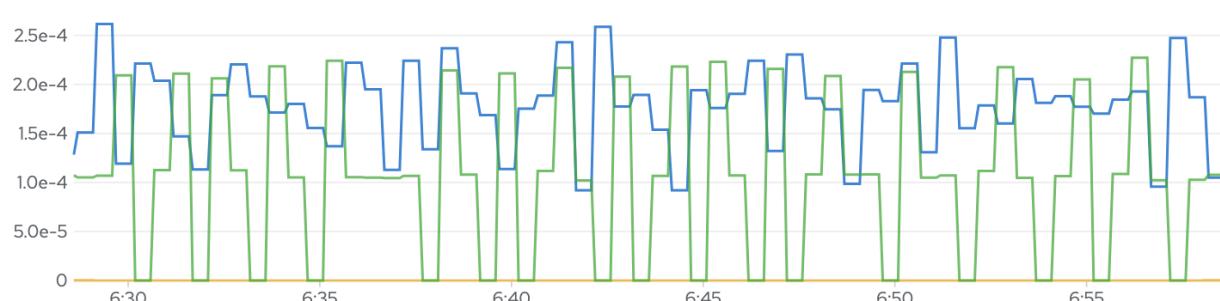
sum(node_namespace_pod_container:container_cpu_usage_seconds_total:sum_irate{namespace='test-project20'}) by (pod)



30m

ズームのリセット

□ スタック



すべて選択解除

pod

値

pod	値
django-ex-git-78bfb4c484-7pcwq	0.0001049666666668376
nodejs-ex-git-599f6bf458-hmzp2	0
test-ebs	0.00010786666666670422

CPU Usage

OpenShift データリザーバーによって Pod の PVC が割り当てられ、(割り当て) リソースがモニタリングされています。

OpenShift データリザーバーによって etcd モニタリングされています。

OpenShift 3 データリザーバーによって etcd モニタリングされています。



API Server Operator モニタリングされています。モニタリングイベント。event-ttl
モニタリングイベント。Operator モニタリングされています。OpenShift データリザーバー モニタリングされています。

Red Hat
OpenShift Service on AWS

☰ 開発者 プロジェクト: test-project20 ▾

+追加 モニタリング ダッシュボード Metrics イベント

トポロジー リソース すべて /

検索 名前またはメッセージ... /

リソース すべて X X

Builds

Helm

プロジェクト

ConfigMaps

シークレット

モニタリング

検索

イベントをストリーミング中...

PVC test-pvc-01 persistentvolume-controller からの生成 NS test-project20 2023年12月11日 19:56 直近の 0 分に 4 回

waiting for first consumer to be created before binding

古いイベントは保存されません。

The screenshot shows the Red Hat OpenShift Service on AWS web interface. The left sidebar has a dark theme with white text. The main area is titled 'モニタリング' (Monitoring) with tabs for 'ダッシュボード' (Dashboard), 'Metrics', and 'イベント' (Events). The 'イベント' tab is selected. A search bar at the top right includes filters for 'リソース' (Resource) set to 'すべて' (All), 'すべて' (All), and a date range from '直近の 0 分' (Last 0 minutes) to '4 回' (4 times). Below the search is a message 'イベントをストリーミング中...' (Streaming events). A single event card is shown: 'PVC test-pvc-01 persistentvolume-controller からの生成' (Created by persistentvolume-controller) in the 'NS test-project20' namespace on '2023年12月11日 19:56' (December 11, 2023, 19:56). The event details are 'waiting for first consumer to be created before binding'. At the bottom of the event list, it says '古いイベントは保存されません。' (Older events are not saved).

9. ROSA

ROS

ROS

ROS

ROS
ROS

openshift-user-workload-monitoring
user-workload-monitoring-config
(ConfigMap) 3 alertmanager: ...



ROS

```
kind: ConfigMap
apiVersion: v1
metadata:
  name: user-workload-monitoring-config
  namespace: openshift-user-workload-monitoring
data:
  config.yaml: |
    prometheus:
      retention: 30d
      volumeClaimTemplate:
        spec:
          resources:
            requests:
              storage: 200Gi
    alertmanager:
      enabled: true
      enableAlertmanagerConfig: true
```

ROS

Prometheus
ROS

OpenShift Web +



OpenShift YAML/JSON Pod



YAML ファイルを用いて Prometheus の監視対象となる OpenShift アプリケーションを定義します。Prometheus の監視対象となる OpenShift アプリケーションは、OpenShift の Service です。

```
---
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    app: prometheus-example-app
    name: prometheus-example-app
    namespace: %USERID%-app
spec:
  replicas: 2
  selector:
    matchLabels:
      app: prometheus-example-app
  template:
    metadata:
      labels:
        app: prometheus-example-app
    spec:
      containers:
        - image: quay.io;brancz/prometheus-example-app:v0.2.0
          imagePullPolicy: IfNotPresent
          name: prometheus-example-app
---
apiVersion: v1
kind: Service
metadata:
  labels:
    app: prometheus-example-app
    name: prometheus-example-app
    namespace: %USERID%-app
spec:
  ports:
    - port: 8080
      protocol: TCP
      targetPort: 8080
      name: web
```

```
selector:  
  app: prometheus-example-app  
type: ClusterIP
```

プロジェクト: test-project20 ▾

YAML のインポート

Drag and drop YAML or JSON files into the editor, or manually enter files and use `---` to separate each definition.

Esc Opt + F1

```
1  ---  
2  apiVersion: apps/v1  
3  kind: Deployment  
4  metadata:  
5    labels:  
6      app: prometheus-example-app  
7      name: prometheus-example-app  
8  spec:  
9    replicas: 2  
10   selector:  
11     matchLabels:  
12       app: prometheus-example-app  
13   template:  
14     metadata:  
15       labels:  
16         app: prometheus-example-app  
17     spec:  
18       containers:  
19         - image: quay.io;brancz/prometheus-example-app:v0.2.0  
20           imagePullPolicy: IfNotPresent  
21           name: prometheus-example-app  
22 ---  
23   apiVersion: v1  
24   kind: Service  
25   metadata:  
26     labels:  
27       app: prometheus-example-app  
28       name: prometheus-example-app  
29   spec:  
30     ports:  
31       - port: 8080  
32         protocol: TCP  
33         targetPort: 8080  
34       name: web  
35     selector:  
36       app: prometheus-example-app  
37     type: ClusterIP
```

作成

キャンセル

ServiceMonitor

prometheus-example-app Service

Kubernetes

ServiceMonitorのOpenShiftのリソースを監視するための権限を付与する
cluster-admin

YAMLでServiceMonitorを定義する
+ServiceMonitorを30s毎に監視する
selector: app: prometheus-example-app Serviceを監視する



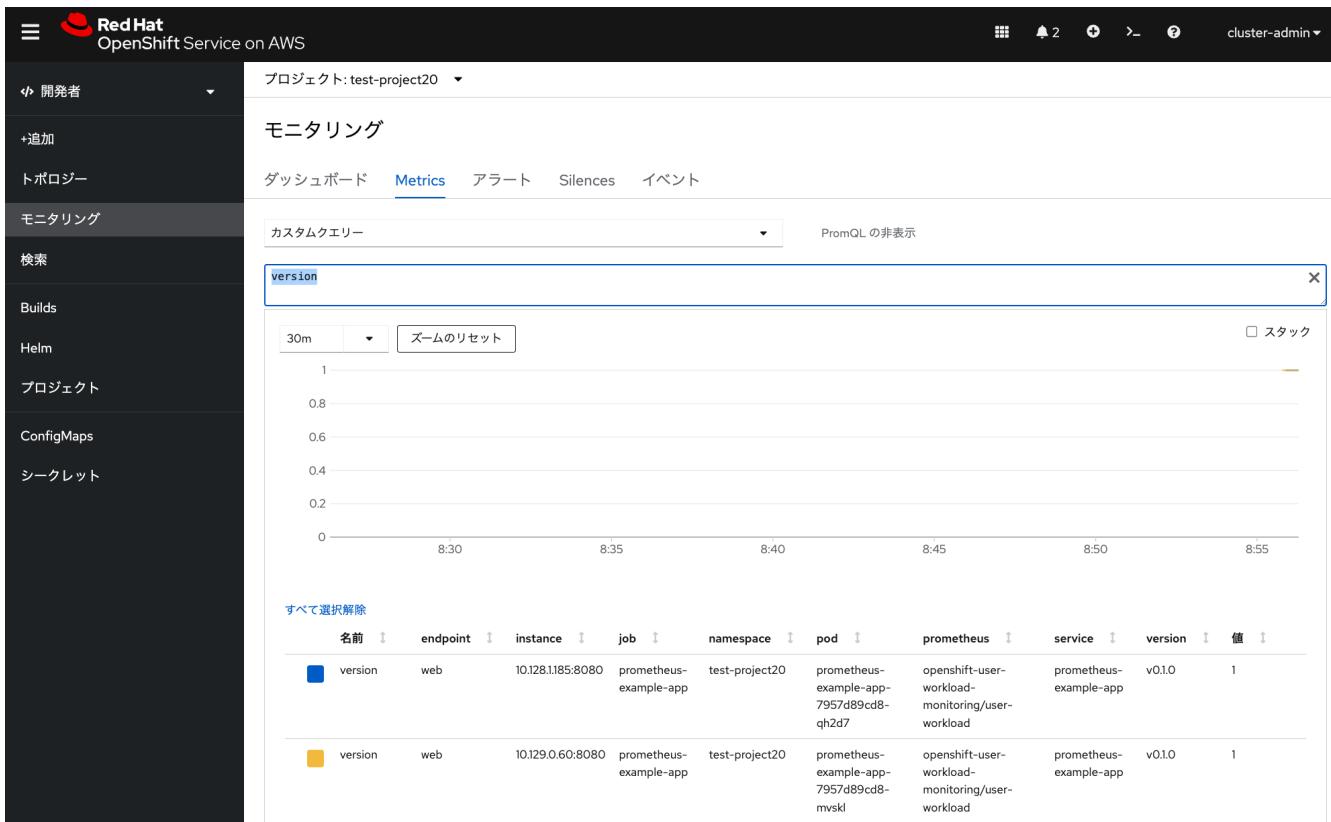
prometheus-example-app Service ServiceMonitor

```
apiVersion: monitoring.coreos.com/v1
kind: ServiceMonitor
metadata:
  labels:
    k8s-app: prometheus-example-monitor
  name: prometheus-example-monitor
  namespace: %USERID%-app
spec:
  endpoints:
  - interval: 30s
    port: web
    scheme: http
    path: /metrics
  selector:
    matchLabels:
      app: prometheus-example-app
```

Metricsを監視する

Metricsを監視する

Metricsを監視するversion Enter



OpenShift Metrics

OpenShift Metrics は、Kubernetes の Pod と Service に対する Prometheus Rule を構成するための YAML ファイルを生成します。

Pod が version < 2 の場合に alert が発火する Prometheus Rule を生成します。

最初の Pod が version < 1 の場合に alert が発火する Prometheus Rule を生成します。

Pod が version < 1 の場合に alert が発火する Prometheus Rule を生成します。

for: 30s



PrometheusRule は ServiceMonitor によって監視される Service に対して適用されます。YAML ファイルを確認してみましょう。

```

apiVersion: monitoring.coreos.com/v1
kind: PrometheusRule
metadata:
  name: example-alert
  namespace: %USERID%-app
spec:
  groups:
  - name: prometheus-example-app-down
    rules:
    - alert: PrometheusExampleAppDown
      annotations:
        description: One or more example pods down.
        summary: Example Pods Down.
      expr: sum(version) < 2 or absent(version)
      for: 30s
  
```

```
labels:  
  severity: warning
```


-----3-----

The screenshot shows the Red Hat OpenShift Service on AWS interface. The left sidebar is dark with white text and icons. The main area has a light background. A prominent alert is displayed at the top: "AR PrometheusExampleAppDown" with a yellow warning icon. Below it, the "アラートルールの詳細" (Alert Rule Details) section shows the rule configuration. The "式" (Query) field contains the Prometheus query: `sum(version{namespace="test-project20"}) < 2 or absent(version{namespace="test-project20"})`. The "アクティブなアラート" (Active Alerts) section shows a graph from 8:40 to 9:05. A single data point is highlighted at 8:51:45 with the value 1, corresponding to the alert rule. The graph has a y-axis from 0 to 1 and an x-axis from 8:40 to 9:05. A tooltip for this point says "2023年12月12日 8:51:45 [namespace='test-project20'] 1". A button "ズームのリセット" (Reset Zoom) is visible above the graph.

----- prometheus-example-app -----
-----1-----Pod-----1-----

The screenshot shows the Red Hat OpenShift Service on AWS interface. The left sidebar is dark with white text and icons. The main area has a light background. On the left, there's a list of application icons: nodejs-ex-git-app, terminal-5dbcrrk, and promet...le-app. The "promet...le-app" icon is highlighted with a dashed border. On the right, a detailed view for "D prometheus-example-app" is shown. It includes a "ヘルスチェック" (Health Check) section with a note about the container not running normally. Below it are tabs for "詳細" (Details), "リソース" (Resources), and "モニタリング" (Monitoring). A large circular icon indicates "2 Pods". A red box highlights the "2 Pods" text and a red arrow points to the "2" in the circle. The "名前" (Name) field is "prometheus-example-app" and the "更新ストラテジー" (Update Strategy) is "RollingUpdate".

One or more example pods down

The screenshot shows the Red Hat OpenShift Service on AWS web interface. The left sidebar is dark with white text, listing options like '開発者', '+追加', 'トポロジー', 'モニタリング' (selected), '検索', 'Builds', 'Helm', 'プロジェクト', 'ConfigMaps', and 'シークレット'. The main area has a light background. At the top, it says 'プロジェクト: test-project20'. Below that is a navigation bar with tabs: 'ダッシュボード', 'Metrics', 'アラート' (selected), 'Silences', and 'イベント'. Underneath is a search bar with a dropdown labeled 'フィルター' and a search input field containing '/'. A table lists an alert: 'PrometheusExampleAppDown' (severity: 警告, status: 実行中, notification switch is on). A note below the table says 'One or more example pods down.'



OFF

CLI

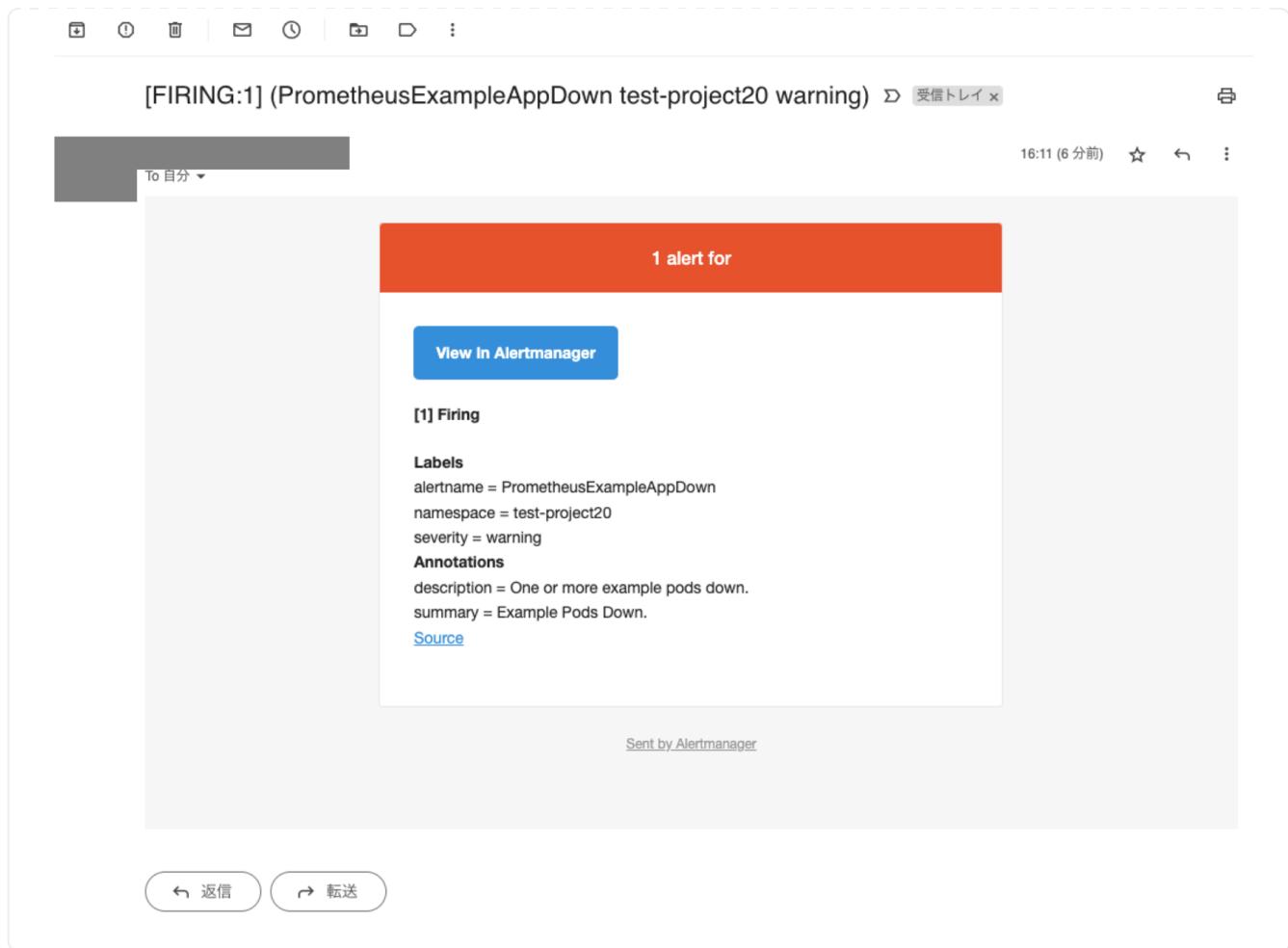
OFF

Pod2 (Pod) は OFF

ROSAとOpenShiftの連携方法

- PagerDuty
- Webhook
- Email
- Slack

GmailとOpenShiftの連携方法



返信

転送

10. ROSA Machinepool

Machinepool

Machinepool(マシンプール)とは?

Machinepool

Machinepool(CPUリソース)を管理する

ROSA

CLI(rosaコマンド)でMachinepoolを操作する

ROSAでMachinepoolを操作する

Machinepoolを操作する

Machinepool rosa list machinepool を実行する



Machinepoolを表示する -c ROSAで rosa list cluster
Machinepoolを表示する ROSAで rosa list machinepool hcp-01

```
$ rosa list cluster
ID           NAME      STATE   TOPOLOGY
280scqkn8ocjochasq423tg4donvpaq  hcp-01  ready  Hosted CP

$ rosa list machinepool -c hcp-01
ID      AUTOSCALING  REPLICAS  INSTANCE TYPE  LABELS      TAINTS      AVAILABILITY ZONE
SUBNET          VERSION    AUTOREPAIR
workers No      2/2        m5.xlarge
subnet-0087cb7bb3f628793  4.14.2  Yes          us-east-2a
```

AWS EC2リソース(インスタンスm5.xlarge)をMachinepoolに登録する



Machinepoolを登録する ROSA HCPで rosa create machinepool

Machinepoolを登録する rosa create machinepool



ROSAsでMachinepoolを登録する ROSAで rosa create machinepool

```
$ rosa create machinepool -c hcp-01
```

I: Enabling interactive mode

? Machine pool name: mp20

? OpenShift version: [Use arrows to move, type to filter, ? for more help]

> 4.14.2

4.14.1

4.14.0

? OpenShift version: 4.14.2

```
? Select subnet for a hosted machine pool: Yes
? Subnet ID: subnet-0087cb7bb3f628793 ('hcp-cluster01-vpc-private-use2-az1','vpc-
0727149c80d7f166f','us-east-2a', Owner ID: '999417968296')
? Enable autoscaling: No
? Replicas: 1
? Labels (optional):
? Taints (optional):
I: Fetching instance types
? Instance type: m5.xlarge
? Autorepair: Yes
I: Machine pool 'mp20' created successfully on hosted cluster 'hcp-01'
I: To view all machine pools, run 'rosa list machinepools -c hcp-01'
```

ROSA HCP
ROSACLOUD 4.14.2
ROSACLOUD

Subnet ID
HCP
ROSACLOUD HCP
ROSACLOUD VPC
ROSACLOUD

Replicas
Autorepair



2023-12-01 ROSA HCP EC2

rosa list machinepool
EC2 5~10

```
$ rosa list machinepool -c hcp-01
```

ID	AUTOSCALING	REPLICAS	INSTANCE TYPE	LABELS	TAINTS	AVAILABILITY ZONE
SUBNET		VERSION	AUTOREPAIR			
mp20	No	1/1	m5.xlarge			us-east-2a
subnet-0087cb7bb3f628793		4.14.2	Yes			
workers	No	2/2	m5.xlarge			us-east-2a
subnet-0087cb7bb3f628793		4.14.2	Yes			

ROSA
cluster-admin
ROSACLOUD → Node

mp20 マシンプールを編集する rosa edit machinepool マシンプール名 リピカス 0
マシンプール名は0に設定され ROSAマシンプールNode数が1に設定されました

```
$ rosa edit machinepool mp20 -c hcp-01 --replicas 0
I: Updated machine pool 'mp20' on cluster 'hcp-01'
```

```
$ rosa list machinepool -c hcp-01
ID      AUTOSCALING  REPLICAS  INSTANCE TYPE  LABELS      TAINTS      AVAILABILITY ZONE
SUBNET          VERSION  AUTOREPAIR
mp20      No        0/0       m5.xlarge
subnet-0087cb7bb3f628793 4.14.2 Yes
workers  No        2/2       m5.xlarge
subnet-0087cb7bb3f628793 4.14.2 Yes
```

マシンプール

Machinepoolは複数のマシンを構成するための構造です
マシンプールは複数のPodを構成するための構造で(CPU等)を定義します
マシンプールは複数のPodを構成するための構造で

マシンプールは複数のマシンを構成するための構造で ROSAマシンプールを構成します

マシンプール mp20 マシンプール名 rosa edit machinepool マシンプール名
マシンプール名は1に設定され2に設定されました

```
$ :マシンプール
$ rosa edit machinepool mp20 -c hcp-01 --enable-autoscaling=true
? Min replicas: 1
? Max replicas: 2
I: Updated machine pool 'mp20' on hosted cluster 'hcp-01'
```

```
$ :マシンプール
$ rosa edit machinepool mp20 -c hcp-01 --enable-autoscaling=false
```

? Replicas: 1

I: Updated machine pool 'mp20' on hosted cluster 'hcp-01'

Machinepool
OpenShift Cluster Manager (OCM)
Enable autoscaling



OpenShift Cluster Manager (OCM)

The screenshot shows the OCM interface for the hcp-01 cluster. The left sidebar has links for OpenShift, Overview, Dashboard, Clusters (which is selected), Learning Resources, Releases, Developer Sandbox, and Downloads. The main content area shows the hcp-01 cluster details with tabs for Overview, Access control, Add-ons, Cluster history, Networking, Machine pools (selected), Support, and Settings. Below these tabs is a table with two rows of machine pool data. A modal window titled "Add machine pool" is open at the top. The table columns are: Machine pool, Instance type, Availability zo..., Node count, Autoscaling, and Version. The first row shows "mp20" as the machine pool, "m5.xlarge" as the instance type, "us-east-2a" as the availability zone, "1" as the node count, "Disabled" as the autoscaling status, and "4.14.2" as the version. The second row shows "workers" as the machine pool, "m5.xlarge" as the instance type, "us-east-2a" as the availability zone, "2" as the node count, "Disabled" as the autoscaling status, and "4.14.2" as the version. To the right of the table, there is a context menu with options "Edit" and "Delete".

Machine pool	Instance type	Availability zo...	Node count	Autoscaling	Version
mp20	m5.xlarge	us-east-2a	1	Disabled	4.14.2
workers	m5.xlarge	us-east-2a	2	Disabled	4.14.2

Edit machine pool

X

Machine pool

mp20



Scaling

Enable autoscaling ?

Autoscaling automatically adds and removes worker (compute) nodes from the cluster based on resource requirements.

Minimum nodes count * ?

- 1 +

Maximum nodes count * ?

- 2 +

› Edit node labels and taints

Save

Cancel

Machinepool

rosa

delete

machinepool

Machinepool

Pod



rosa delete machinepool Machinepool

```
$ rosa delete machinepool mp20 -c hcp-01
```

? Are you sure you want to delete machine pool 'mp20' on hosted cluster 'hcp-01'? Yes
I: Successfully deleted machine pool 'mp20' from hosted cluster 'hcp-01'

Machinepool

Machinepool

Machinepool

Machinepool

```
$ rosa edit machinepool mp20 -c hcp-01 --enable-autoscaling=true
```

```
? Min replicas: 1
? Max replicas: 2
I: Updated machine pool 'mp20' on hosted cluster 'hcp-01'
```

Machinepoolの設定を確認するには、ROSAのコンソールを開いて

Node → Node Pool を選択します。

hypershift.openshift.io/nodePool=<ROSAの名前>-<Machinepool名>

hypershift.openshift.io/nodePool=hcp-01-mp20 の URL を開くと、機械プールの詳細が表示されます。

rosa create machinepool で Machinepool を作成する方法です。
labels=key1=value1,key2=value2,...
key=value でラベルを定義できます。2023年12月現在 rosa edit machinepool で Machinepool を編集できます。

YAML 形式で機械プールを定義する方法です。

YAML 形式

busybox

Pod 15 個

nodeSelector

Pod 15 個

key: value でラベルを定義する方法です。(例: hcp-01-mp20)

value でラベルの値を定義する方法です。

CPU でラベルを定義する方法です。Pod 15 個

```
apiVersion: batch/v1
kind: Job
metadata:
  generateName: work-queue-
spec:
  template:
    spec:
```

```

nodeSelector:
  hypershift.openshift.io/nodePool: "hcp-01-mp20"
containers:
- name: work
  image: busybox
  command: ["sleep", "360"]
resources:
  requests:
    memory: 500Mi
    cpu: 500m
restartPolicy: Never
backoffLimit: 4
completions: 15
parallelism: 15

```

OpenShiftのJobを手動で作成する方法 JobのYAML定義を入力して作成します。

The screenshot shows the Red Hat OpenShift Service on AWS web interface. The left sidebar navigation includes 'Projects' (selected), 'Home', 'Operator', 'Workloads' (selected), 'Pods', 'Deployments', 'DeploymentConfigs', 'StatefulSets', 'シークレット', 'ConfigMaps', 'CronJobs', 'Jobs' (selected), 'DaemonSets', 'ReplicaSet', 'ReplicationControllers', and 'HorizontalPodAutoscalers'. The main content area is titled 'Job の作成' and displays the YAML code for the Job:

```

1  apiVersion: batch/v1
2  kind: Job
3  metadata:
4    generateName: work-queue-
5  spec:
6    template:
7      spec:
8        nodeSelector:
9          hypershift.openshift.io/nodePool: "hcp-01-mp20"
10         containers:
11           - name: work
12             image: busybox
13             command: ["sleep", "360"]
14             resources:
15               requests:
16                 memory: 500Mi
17                 cpu: 500m
18             restartPolicy: Never
19   backoffLimit: 4
20   completions: 15
21   parallelism: 15

```

Below the code editor are three buttons: '作成' (Create), 'キャンセル' (Cancel), and 'ダウンロード' (Download).

Podを起動するためのYAML定義を入力して作成します。
Podを起動するためのMachinepoolを起動します。
Podを起動するためのMachinepoolを起動します。

ip-10-0-0-48.XXX
ip-10-0-0-138.XXX

プロジェクト: test-project20

Jobs > Job の詳細

J work-queue-stk94 In progress

アクション

名前	ステータス	準備完了	再起動回数	ノード	メモリー	CPU	作成済み
P work-queue-stk94-2rhq5	Running	1/1	0	N ip-10-0-0-138.us-east-2.compute.internal	0.6 MiB	-	2023年12月12日 19:11
P work-queue-stk94-dmkjg	Running	1/1	0	N ip-10-0-0-138.us-east-2.compute.internal	0.6 MiB	-	2023年12月12日 19:11
P work-queue-stk94-gg8v2	Running	1/1	0	N ip-10-0-0-138.us-east-2.compute.internal	0.6 MiB	-	2023年12月12日 19:11
P work-queue-stk94-rmcz4	Running	1/1	0	N ip-10-0-0-138.us-east-2.compute.internal	0.6 MiB	-	2023年12月12日 19:11
P work-queue-stk94-vpfps	Running	1/1	0	N ip-10-0-0-138.us-east-2.compute.internal	0.6 MiB	-	2023年12月12日 19:11
P work-queue-stk94-xt5lt	Running	1/1	0	N ip-10-0-0-138.us-east-2.compute.internal	0.7 MiB	-	2023年12月12日 19:11
P work-queue-stk94-6dqjx	Completed	0/1	0	N ip-10-0-0-48.us-east-2.compute.internal	-	-	2023年12月12日 19:11
P work-queue-stk94-44nk6	Completed	0/1	0	N ip-10-0-0-48.us-east-2.compute.internal	-	-	2023年12月12日 19:11
P work-queue-stk94-dvsqb	Completed	0/1	0	N ip-10-0-0-48.us-east-2.compute.internal	-	-	2023年12月12日 19:11
P work-queue-stk94-hbk85	Completed	0/1	0	N ip-10-0-0-48.us-east-2.compute.internal	-	-	2023年12月12日 19:11

ROSASの仕組みを理解するため、Red Hat OpenShift Service on AWS (ROSA) の UI を見ています。ROSASは、Red Hat OpenShift Service on AWS (ROSA) の一部で、AWS Lambda と連携して実行環境を自動的に用意する機能です。

m5.xlargeマシンプールで実行されるJobの状況を確認します。

15個のJobが実行され、15個のPodが作成されました。

- 実行時間: 15分

- 実行時間: 10分

ROSASは、Red Hat OpenShift Service on AWS (ROSA) の一部で、AWS Lambda と連携して実行環境を自動的に用意する機能です。ROSASは、Red Hat OpenShift Service on AWS (ROSA) の一部で、AWS Lambda と連携して実行環境を自動的に用意する機能です。

プロジェクト: test-project20

Jobs

名前 ラベル 完了 タイプ

J work-queue-stk94 batch.kubernetes... =e819f58f-3c6b-448c-contr... =e819f58f-3c6b-448c-job-name=work-queue-stk94 15 of 15 固定の完了数

並列処理の編集

PodDisruptionBudget の追加

ラベルの編集

アノテーションの編集

Job の編集

Job の削除

Machinepool删除 rosa delete machinepool

```
$ rosa delete machinepool mp20 -c hcp-01
```

```
? Are you sure you want to delete machine pool 'mp20' on hosted cluster 'hcp-01'? Yes  
I: Successfully deleted machine pool 'mp20' from hosted cluster 'hcp-01'
```

11. ROSA HCP

ROS

ROSA HCP

ROSA HCP
Machinepool SingleAZ/MultiAZ

OCM ROSA CLI



ROS

ROSA

CLI

OCM

OpenShift Cluster Manager (OCM) ROSA HCP
OpenShift Web CLI(oc) OCM ROSA
CLI

OCM ROSA HCP Settings Update

hcp-01[Open console](#)

Actions ▾


[Overview](#) [Access control](#) [Add-ons](#) [Cluster history](#) [Networking](#) [Machine pools](#) [Support](#) [Settings](#)
Update strategy

Note: In the event of [Critical security concerns](#) (CVEs) that significantly impact the security or stability of the cluster, updates may be automatically scheduled by Red Hat SRE to the latest z-stream version not impacted by the CVE within 2 business days after customer notifications.

 Recurring updates

The cluster control plan will be automatically updated based on your preferred day and start time when new patch updates ([z-stream](#)) are available. When a new minor version is available, you'll be notified and must manually allow the cluster to update to the next minor version. The worker nodes will need to be manually updated.

 Individual updates

Schedule each update individually. Take into consideration end of life dates from the [lifecycle policy](#) when planning updates.

Node draining

You may set a grace period for how long pod disruption budget-protected workloads will be respected during updates. After this grace period, any workloads protected by pod disruption budgets that have not been successfully drained from a node will be forcibly evicted.

Grace period

▼
[Save](#)[Cancel](#)**Update status**

Update available

4.14.2

4.14.5

[Update](#)
✉ Feedback


Update strategy Recurring updates (4.14.5) z-stream (4.14.5) ROSA HCP

(4.15-4.16) OCM

OCM

Update strategy

Note: In the event of [Critical security concerns](#) (CVEs) that significantly impact the security or stability of the cluster, updates may be automatically scheduled by Red Hat SRE to the latest z-stream version not impacted by the CVE within 2 business days after customer notifications.

Recurring updates

The cluster control plan will be automatically updated based on your preferred day and start time when new patch updates ([z-stream](#)) are available. When a new minor version is available, you'll be notified and must manually allow the cluster to update to the next minor version. The worker nodes will need to be manually updated.

i For recurring updates, the control plane will be updated when a new version becomes available at least 2 days prior to your selected start time. Worker nodes will need to be manually updated.

Select a day and start time

Saturday

02:00 UTC

Individual updates

Schedule each update individually. Take into consideration end of life dates from the [lifecycle policy](#) when planning updates.

PreviousNext

1 Select version

2 Schedule update

3 Confirmation

Select version

4.14.5

★ Recommended

The latest on your current minor version.

[View release notes](#)

Next

Back

Cancel

Update
5
time

now

ROSA

HCP

a different

Schedule

time

Next

- 1 Select version
- 2 Schedule update
- 3 Confirmation

Schedule update

Update now (update will begin within the next hour)

Schedule a different time

2023-12-13



12:00



UTC 13 Dec 2023 03:00 UTC

[Next](#)

[Back](#)

[Cancel](#)

Confirm Update

- 1 Select version
- 2 Schedule update
- 3 Confirmation

Confirmation of your update

Version 4.14.2 → 4.14.5

Scheduled UTC 13 Dec 2023 03:00 UTC

Local time Wed Dec 13 2023 12:00:00 GMT+0900 (日本標準時)

Confirm update

Back

Cancel

確認する場合は「確認する」をクリックして下さい。キャンセルする場合は「キャンセル」をクリックして下さい。

Clusters > hcp-01

hcp-01

Open console

Actions ▾



Overview

Access control

Add-ons

Cluster history

Networking

Machine pools

Support

Settings

Update strategy

Note: In the event of [Critical security concerns](#) (CVEs) that significantly impact the security or stability of the cluster, updates may be automatically scheduled by Red Hat SRE to the latest z-stream version not impacted by the CVE within 2 business days after customer notifications.

Recurring updates

The cluster control plan will be automatically updated based on your preferred day and start time when new patch updates ([z-stream](#)) are available. When a new minor version is available, you'll be notified and must manually allow the cluster to update to the next minor version. The worker nodes will need to be manually updated.

Update status

Update available



Cancel this update

Cancel update

X

This update to version 4.14.5 is scheduled for 13 Dec 2023 03:00 UTC.

[Cancel this update](#)

[Close](#)

ROSA HCP Machinepool 15

OCM

ROSA HCP Machinepool Machinepool Machinepool

OCM Machinepool Machinepool Machinepool
OCM Machinepool 5 ROSA CLI

Clusters > hcp-01

hcp-01

[Open console](#)

Actions ▾



Overview Access control Add-ons Cluster history Networking Machine pools Support Settings

⚠️ Update available for Machine pools

You can update all worker nodes to the current control plane version (4.14.2), or use the CLI to update a specific version. [Learn more about updates](#)

[Update all Machine pools now](#)

[Add machine pool](#)

Machine pool	Instance type	Availability zones	Node count	Autoscaling	Version
--------------	---------------	--------------------	------------	-------------	---------

mp01	c5.xlarge	us-east-2a	1	Disabled	4.14.0 Update ⌂
------	-----------	------------	---	----------	---------------------------------

Subnets

subnet-0087cb7bb3f628793

workers	m5.xlarge	us-east-2a	2	Disabled	4.14.2
---------	-----------	------------	---	----------	--------

Labels

testkey01 = testvalue01

Subnets

subnet-0087cb7bb3f628793



Update machine pool

x

Update machine pool mp01 to version 4.14.2?

Update machine pool

Cancel

Clusters > hcp-01

hcp-01

Open console

Actions ▾



Overview Access control Add-ons Cluster history Networking Machine pools Support Settings

Add machine pool

Machine pool	Instance type	Availability zones	Node count	Autoscale
--------------	---------------	--------------------	------------	-----------

▼ mp01	c5.xlarge	us-east-2a	1	Disabled	4.14.0 ?	⋮
--------	-----------	------------	---	----------	--------------------------	---

Subnets

subnet-0087cb7bb3f628793

▼ workers	m5.xlarge	us-east-2a	2	Disabled	4.14.2	⋮
-----------	-----------	------------	---	----------	--------	---

Labels

testkey01 = testvalue01

Subnets

subnet-0087cb7bb3f628793

Feedback

Machinepool

Machinepool

Machinepool

Machinepool

Machinepool

Machinepool

Machinepool

Machinepool



ROSA

Kubernetes

Lab

Pod

Machinepool



ROSA

HCP

MachinePool

Podの状態を監視する(cordon/uncordon) Podを削除する(drain)

クラスタの構成要素を監視する(監視対象の追加/削除)

ROSA CLIの操作

OCMによるROSA

CLIによるROSA

HCPによる

クラウドプロバイダによる

```
$ rosa list upgrade cluster -c hcp-01
VERSION NOTES
4.14.5 recommended
```

クラウドプロバイダによる操作 2023年12月13日23時(UTC) rosa upgrade cluster によるROSA OperatorによるIAMによる操作

```
$ rosa upgrade cluster -c hcp-01 --control-plane \
--schedule-date 2023-12-13 --schedule-time 23:00 \
--version 4.14.5 --mode auto --yes
```

```
I: Ensuring account and operator role policies for cluster
'280scqkn8ocjoochasq423tg4donvpaq' are compatible with upgrade.
I: Account roles with the prefix 'ManagedOpenShift' have attached managed policies.
I: Cluster 'hcp-01' operator roles have attached managed policies. An upgrade isn't
needed
I: Account and operator roles for cluster 'hcp-01' are compatible with upgrade
I: Upgrade successfully scheduled for cluster 'hcp-01'
```

クラウドプロバイダによる操作

```
$ rosa list upgrade cluster -c hcp-01
VERSION NOTES
4.14.5 recommended - scheduled for 2023-12-13 23:00 UTC
```

rosa delete upgrade による操作 2023年12月13日23時(UTC) rosa delete upgradeによる操作

```
$ rosa delete upgrade cluster -c hcp-01
? Are you sure you want to cancel scheduled upgrade on cluster 'hcp-01'? Yes
I: Successfully canceled scheduled upgrade on cluster 'hcp-01'
```

```
$ rosa list upgrade cluster -c hcp-01
VERSION NOTES
4.14.5 recommended
```

ROSA CLI

Machinepool
version
OpenShift
version
Instance type
m5.xlarge
c5.xlarge

```
$ rosa create machinepool -c hcp-01

I: Enabling interactive mode
? Machine pool name: mp20
? OpenShift version: [Use arrows to move, type to filter, ? for more help]
  4.14.2
  4.14.1
> 4.14.0
? OpenShift version: 4.14.0
? Select subnet for a hosted machine pool: No
? AWS availability zone: us-east-2a
? Enable autoscaling: No
? Replicas: 1
? Labels (optional):
? Taints (optional):
I: Fetching instance types
? Instance type: c5.xlarge
? Autorepair: Yes
I: Machine pool 'mp20' created successfully on hosted cluster 'hcp-01'
I: To view all machine pools, run 'rosa list machinepools -c hcp-01'
```

rosa list machinepool 机器池 ROSA → Node
Machinepool

rosa list upgrade 机器池
Machinepool 4.14.1 → 4.14.2

```
$ rosa list upgrade -c hcp-01 --machinepool mp20
VERSION NOTES
4.14.2 recommended
4.14.1
```

Machinepool
rosa upgrade machinepool interactive
UTC 9

```
$ rosa upgrade machinepool mp20 -c hcp-01 --interactive

I: Interactive mode enabled.
Any optional fields can be left empty and a default will be selected.
? Enable automatic upgrades: No
? Please input desired date in format yyyy-mm-dd: 2023-12-13
? Please input desired UTC time in format HH:mm: 23:00
? Machine pool version: 4.14.1
```

```
? Are you sure you want to upgrade machine pool 'mp20' to version '4.14.1'? Yes  
I: Upgrade successfully scheduled for the machine pool 'mp20' on cluster 'hcp-01'
```

Machinepool ROSA
Machinepool

Machinepool rosa delete upgrade

```
$ rosa delete upgrade -c hcp-01 --machinepool mp20 --yes  
I: Successfully canceled scheduled upgrade for machine pool 'mp20' for cluster 'hcp-01'
```

Machinepool rosa delete machinepool

```
$ rosa delete machinepool mp20 -c hcp-01 --yes  
I: Successfully deleted machine pool 'mp20' from hosted cluster 'hcp-01'
```