



Red Hat OpenShift Service on AWS 4

トラブルシューティング

Red Hat OpenShift Service on AWS のサポートについて

Red Hat OpenShift Service on AWS 4 トラブルシューティング

Red Hat OpenShift Service on AWS のサポートについて

Enter your first name here. Enter your surname here.

Enter your organisation's name here. Enter your organisational division here.

Enter your email address here.

法律上の通知

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Troubleshooting.ent file |.

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

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

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

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

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

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

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

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

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

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

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

All other trademarks are the property of their respective owners.

概要

本書では、Red Hat OpenShift Service on AWS (ROSA) のサポートを得る方法を説明します。

目次

第1章 期限切れトークンのトラブルシューティング	3
1.1. 期限切れのオフラインアクセストークンのトラブルシューティング	3
第2章 インストールのトラブルシューティング	4
2.1. インストールのトラブルシューティング	4
2.1.1. インストールまたはアンインストールログの検査	4
2.1.2. STS を使用しないクラスターの AWS アカウントパーミッションの確認	4
2.1.3. AWS アカウントおよびクォータの確認	4
2.1.4. AWS 通知メール	4
第3章 IAM ロールのトラブルシューティング	6
3.1. OCM-ROLES および USER-ROLE の IAM リソースに関する問題の解決	6
3.1.1. OpenShift Cluster Manager ロールの作成	6
3.1.2. user-role IAM ロールの作成	8
3.1.3. AWS アカウントのリンク	9
3.1.4. 複数の AWS アカウントを Red Hat 組織に関連付ける	10
第4章 クラスターデプロイメントのトラブルシューティング	12
4.1. 失敗したクラスターに関する情報の取得	12
4.2. OSDCCSADMIN エラーのあるクラスターの作成に失敗する	12
4.3. ELASTIC LOAD BALANCER (ELB) のサービ出カルの作成	12
4.4. 削除できないクラスターの修復	13

第1章 期限切れトークンのトラブルシューティング

1.1. 期限切れのオフラインアクセストークンのトラブルシューティング

rosa CLI および `api.openshift.com` のオフラインアクセストークンの有効期限が切れると、エラーメッセージが表示されます。これは、`sso.redhat.com` がトークンが無効な場合に発生します。

出力例

```
Can't get tokens ....  
Can't get access tokens ....
```

手順

- 以下の URL で新たにオフラインアクセストークンを生成します。URL にアクセスするたびに、新しいオフラインアクセストークンが生成されます。
 - Red Hat OpenShift Service on AWS (ROSA):
<https://console.redhat.com/openshift/token/rosa>

第2章 インストールのトラブルシューティング

2.1. インストールのトラブルシューティング

2.1.1. インストールまたはアンインストールログの検査

インストールログを表示するには、以下を実行します。

- 以下のコマンドを実行し、**<cluster_name>** をクラスターの名前に置き換えます。

```
$ rosa logs install --cluster=<cluster_name>
```

- ログを確認するには、**--watch** フラグを追加します。

```
$ rosa logs install --cluster=<cluster_name> --watch
```

アンインストールログを表示するには、以下を実行します。

- 以下のコマンドを実行し、**<cluster_name>** をクラスターの名前に置き換えます。

```
$ rosa logs uninstall --cluster=<cluster_name>
```

- ログを確認するには、**--watch** フラグを追加します。

```
$ rosa logs uninstall --cluster=<cluster_name> --watch
```

2.1.2. STS を使用しないクラスターの AWS アカウントパーミッションの確認

以下のコマンドを実行して、AWS アカウントに適切なパーミッションがあることを確認します。このコマンドは、AWS Security Token Service(STS) を使用しないクラスターに対してのみパーミッションを検証します。

```
$ rosa verify permissions
```

エラーが発生した場合は、[SCP](#) が AWS アカウントに適用されていないことを二重に確認します。SCP を使用する必要がある場合は、必要最小限の SCP の詳細を [Red Hat Requirements for Customer Cloud Subscriptions](#) で確認してください。

2.1.3. AWS アカウントおよびクォータの確認

以下のコマンドを実行して、AWS アカウントに利用可能なクォータがあることを確認します。

```
$ rosa verify quota
```

AWS クォータはリージョンに基づいて変更されます。適切な AWS リージョンのクォータを確認してください。クォータを増やす必要がある場合は、[AWS コンソール](#) に移動し、失敗したサービスのクォータを増加することを要求します。

2.1.4. AWS 通知メール

クラスターの作成時に、Red Hat OpenShift Service on AWS サービスはサポートされるすべてのリージョンに小規模なインスタンスを作成します。チェックにより、使用される AWS アカウントがサポートされる各リージョンに確実にデプロイされます。

AWS アカウントがサポートされるリージョンを1つも使用しないと、AWS が Your Request For Accessing AWS Resources Has Been Validated (AWS リソースへのアクセス要求が検証されました) という確認メールを1件以上送信する場合があります。通常、このメールの送信者は aws-verification@amazon.com です。

これは、Red Hat OpenShift Service on AWS サービスが AWS アカウント設定を検証する上で想定される動作です。

第3章 IAM ロールのトラブルシューティング

3.1. OCM-ROLES および USER-ROLE の IAM リソースに関する問題の解決

`rosa` CLI を使用してクラスターを作成しようとする、エラーが発生する場合があります。

出力例

```
E: Failed to create cluster: The sts_user_role is not linked to account '1oNI'. Please create a user role and link it to the account.
```

このエラーは、**user-role** IAM ロールが AWS アカウントにリンクされていないことを意味します。このエラーの原因として最も可能性が高いのは、Red Hat 組織の別のユーザーが **ocm-role** IAM ロールを作成したことです。**user-role** IAM ロールを作成する必要があります。



注記

あるユーザーが Red Hat アカウントにリンクされた **ocm-role** IAM リソースを設定した後、その Red Hat 組織でクラスターを作成するユーザーは、クラスターをプロビジョニングするために **user-role** IAM ロールが必要になります。

手順

- 次のコマンドを使用して、**ocm-role** および **user-role** の IAM ロールのステータスを評価します。

```
$ rosa list ocm-role
```

出力例

```
I: Fetching ocm roles
ROLE NAME                ROLE ARN                LINKED ADMIN
ManagedOpenShift-OCM-Role-1158  arn:aws:iam::2066:role/ManagedOpenShift-OCM-Role-1158  No    No
```

```
$ rosa list user-role
```

出力例

```
I: Fetching user roles
ROLE NAME                ROLE ARN                LINKED
ManagedOpenShift-User.osdocs-Role  arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role  Yes
```

これらのコマンドの結果を使用して、不足している IAM リソースを作成およびリンクできます。

3.1.1. OpenShift Cluster Manager ロールの作成

コマンドラインインターフェイス (CLI) を使用して、OpenShift Cluster Manager IAM ロールを作成します。

前提条件

- AWS アカウントがある。
- OpenShift Cluster Manager 組織で Red Hat 組織管理者特権があります。
- AWS アカウント全体のロールをインストールするために必要な権限がある。
- インストールホストに最新の AWS (**aws**) および ROSA (**rosa**) CLI をインストールして設定している。

手順

- 基本的な権限を持つ ocm-role IAM ロールを作成するには、次のコマンドを実行します。

```
$ rosa create ocm-role
```

- 管理者権限を持つ ocm-role IAM ロールを作成するには、次のコマンドを実行します。

```
$ rosa create ocm-role --admin
```

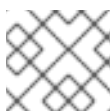
このコマンドを使用すると、特定の属性を指定してロールを作成できます。次の出力例は、選択された自動モードを示しています。これにより、**rosa** CLI で Operator のロールとポリシーを作成できます。詳細については、関連情報のアカウント全体のロールの作成方法を参照してください。

出力例

```
I: Creating ocm role
? Role prefix: ManagedOpenShift 1
? Enable admin capabilities for the OCM role (optional): No 2
? Permissions boundary ARN (optional): 3
? Role creation mode: auto 4
I: Creating role using 'arn:aws:iam::<ARN>:user/<UserName>'
? Create the 'ManagedOpenShift-OCM-Role-182' role? Yes 5
I: Created role 'ManagedOpenShift-OCM-Role-182' with ARN 'arn:aws:iam::
<ARN>:role/ManagedOpenShift-OCM-Role-182'
I: Linking OCM role
? OCM Role ARN: arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182 6
? Link the 'arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182' role with organization
'<AWS ARN'? Yes 7
I: Successfully linked role-arn 'arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182' with
organization account '<AWS ARN>'
```

1 作成されたすべての AWS リソースの接頭辞値。この例では、**ManagedOpenShift** がすべての AWS リソースを付加します。

2 このロールに追加の管理者権限を付与するかどうかを選択します。



注記

--admin オプションを使用した場合、このプロンプトは表示されません。

- 3 パーミッション境界を設定するためのポリシーの Amazon Resource Name (ARN)。
- 4 AWS ロールを作成する方法を選択します。**auto** を使用して、**rosa** CLI ツールはロールおよびポリシーを生成してリンクします。**auto** モードでは、AWS ロールを作成するためのいくつかの異なるプロンプトが表示されます。
- 5 auto メソッドは、接頭辞を使用して特定の **ocm-role** を作成するかどうかを尋ねます。
- 6 IAM ロールを OpenShift Cluster Manager に関連付けることを確認します。
- 7 作成したロールを AWS 組織にリンクします。

3.1.2. user-role IAM ロールの作成

コマンドラインインターフェイス (CLI) を使用して、OpenShift Cluster Manager IAM ロールを作成できます。

前提条件

- AWS アカウントがある。
- インストールホストに最新の AWS (**aws**) および ROSA (**rosa**) CLI をインストールして設定している。

手順

- 基本的な権限を持つ ocm-role IAM ロールを作成するには、次のコマンドを実行します。

```
$ rosa create user-role
```

このコマンドを使用すると、特定の属性を指定してロールを作成できます。次の出力例は、選択された自動モードを示しています。これにより、**rosa** CLI で Operator のロールとポリシーを作成できます。詳細は、関連情報の自動および手動のデプロイメントモードについてを参照してください。

出力例

```
I: Creating User role
? Role prefix: ManagedOpenShift 1
? Permissions boundary ARN (optional): 2
? Role creation mode: auto 3
I: Creating ocm user role using 'arn:aws:iam::2066:user'
? Create the 'ManagedOpenShift-User.osdocs-Role' role? Yes 4
I: Created role 'ManagedOpenShift-User.osdocs-Role' with ARN
'arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role'
I: Linking User role
? User Role ARN: arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role
? Link the 'arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role' role with account '1AGE'?
Yes 5
I: Successfully linked role ARN 'arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role' with
account '1AGE'
```

- 1 作成されたすべての AWS リソースの接頭辞値。この例では、**ManagedOpenShift** がすべての AWS リソースを付加します。
- 2 パーミッション境界を設定するためのポリシーの Amazon Resource Name (ARN)。
- 3 AWS ロールを作成する方法を選択します。**auto** を使用して、**rosa** CLI ツールは AQS アカウントを生成してリンクします。**auto** モードでは、AWS ロールを作成するためのいくつかの異なるプロンプトが表示されます。
- 4 **auto** メソッドは、接頭辞を使用して特定の **user-role** を作成するかどうかを尋ねます。
- 5 作成したロールを AWS 組織にリンクします。

3.1.3. AWS アカウントのリンク

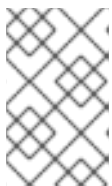
rosa CLI を使用して AWS アカウントをリンクします。

前提条件

- AWS アカウントがある。
- [OpenShift Cluster Manager Hybrid Cloud Console](#) を使用してクラスターを作成している。
- AWS アカウント全体のロールをインストールするために必要な権限がある。詳細については、このセクションのその他のリソースを参照してください。
- インストールホストに最新の AWS (**aws**) および ROSA (**rosa**) CLI をインストールして設定している。
- **ocm-role** および **user-role** IAM ロールを作成している。

手順

1. CLI から、Amazon Resource Name (ARN) を使用して、**ocm-role** リソースを Red Hat 組織にリンクします。



注記

rosa link コマンドを実行するには、Red Hat Organization Administrator (組織管理者権限) が必要です。**ocm-role** リソースを AWS アカウントにリンクすると、組織内のすべてのユーザーに表示されます。

```
$ rosa link ocm-role --role-arn <arn>
```

出力例

```
I: Linking OCM role
? Link the '<AWS ACCOUNT ID>' role with organization '<ORG ID>'? Yes
I: Successfully linked role-arn '<AWS ACCOUNT ID>' with organization account '<ORG ID>'
```

2. CLI から、Amazon Resource Name (ARN) を使用して、**user-role** リソースを Red Hat ユーザーアカウントにリンクします。

```
$ rosa link user-role --role-arn <arn>
```

出力例

```
I: Linking User role
? Link the 'arn:aws:iam:::role/ManagedOpenShift-User-Role-125' role with
organization '<AWS ID>'? Yes
I: Successfully linked role-arn 'arn:aws:iam:::role/ManagedOpenShift-User-Role-125'
with organization account '<AWS ID>'
```

3.1.4. 複数の AWS アカウントを Red Hat 組織に関連付ける

複数の AWS アカウントを Red Hat 組織に関連付けることができます。複数のアカウントを関連付けると、Red Hat 組織の関連付けられた AWS アカウントのいずれかに Red Hat OpenShift Service on AWS (ROSA) クラスターを作成できます。

この機能を使用すると、リージョンにバインドされた環境として複数の AWS プロファイルを使用することにより、さまざまな AWS リージョンにクラスターを作成できます。

前提条件

- AWS アカウントがある。
- [OpenShift Cluster Manager Hybrid Cloud Console](#) を使用してクラスターを作成している。
- AWS アカウント全体のロールをインストールするために必要な権限がある。
- インストールホストに最新の AWS (**aws**) および ROSA (**rosa**) CLI をインストールして設定している。
- **ocm-role** および **user-role** IAM ロールを作成している。

手順

追加の AWS アカウントを関連付けるには、最初にローカル AWS 設定でプロファイルを作成します。次に、追加の AWS アカウントに **ocm-role**、**user**、および **account** のロールを作成して、アカウントを Red Hat 組織に関連付けます。

追加のリージョンでロールを作成するには、**rosa create** コマンドの実行時に **--profile <aws-profile>** パラメーターを指定し、**<aws_profile>** を追加のアカウントプロファイル名に置き換えます。

- OpenShift Cluster Manager ロールを作成するときに AWS アカウントプロファイルを指定するには、以下を実行します。

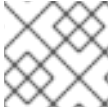
```
$ rosa create --profile <aws_profile> ocm-role
```

- ユーザーロールを作成するときに AWS アカウントプロファイルを指定するには、以下を実行します。

```
$ rosa create --profile <aws_profile> user-role
```

- アカウントロールを作成するときに AWS アカウントプロファイルを指定するには、以下を実行します。

```
$ rosa create --profile <aws_profile> account-roles
```



注記

プロファイルを指定しない場合は、デフォルトの AWS プロファイルが使用されます。

第4章 クラスターデプロイメントのトラブルシューティング

本書では、クラスターデプロイメントエラーのトラブルシューティング方法を説明します。

4.1. 失敗したクラスターに関する情報の取得

クラスターのデプロイメントに失敗すると、クラスターはエラー状態になります。

手順

以下のコマンドを実行してさらに多くの情報を取得します。

```
$ rosa describe cluster -c <my_cluster_name> --debug
```

4.2. OSDCCSADMIN エラーのあるクラスターの作成に失敗する

クラスター作成アクションが失敗すると、以下のエラーメッセージが表示されることがあります。

出力例

```
Failed to create cluster: Unable to create cluster spec: Failed to get access keys for user 'osdCcsAdmin': NoSuchEntity: The user with name osdCcsAdmin cannot be found.
```

手順

この問題を修正するには、以下を実行します。

1. スタックを削除します。

```
$ rosa init --delete
```

2. アカウントを再初期化します。

```
$ rosa init
```

4.3. ELASTIC LOAD BALANCER (ELB) のサービ出カルの作成

AWS アカウントにロードバランサーを作成していない場合は、Elastic Load Balancer (ELB) のサービ出カルがまだ存在しない可能性があります。以下のエラーが表示される場合があります。

```
Error: Error creating network Load Balancer: AccessDenied: User: arn:aws:sts::xxxxxxxxxxxx:assumed-role/ManagedOpenShift-Installer-Role/xxxxxxxxxxxxxxxxxxxx is not authorized to perform: iam:CreateServiceLinkedRole on resource: arn:aws:iam::xxxxxxxxxxxx:role/aws-service-role/elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing"
```

手順

この問題を解決するには、ロールが AWS アカウントに存在することを確認します。設定されていない場合は、以下のコマンドでこのロールを作成します。


```
aws iam get-role --role-name "AWSServiceRoleForElasticLoadBalancing" || aws iam create-service-linked-role --aws-service-name "elasticloadbalancing.amazonaws.com"
```



注記

このコマンドは、アカウントごとに1回のみ実行する必要があります。

4.4. 削除できないクラスターの修復

特定のケースで、クラスターを削除しようとする、[OpenShift Cluster Manager Hybrid Cloud Console](#)に次のエラーが表示されます。

```
Error deleting cluster
CLUSTERS-MGMT-400: Failed to delete cluster <hash>: sts_user_role is not linked to your account. sts_ocm_role is linked to your organization <org number> which requires sts_user_role to be linked to your Red Hat account <account ID>.Please create a user role and link it to the account: User Account <account ID> is not authorized to perform STS cluster operations
```

```
Operation ID: b0572d6e-fe54-499b-8c97-46bf6890011c
```

CLI からクラスターを削除しようとする、次のエラーが表示されます。

```
E: Failed to delete cluster <hash>: sts_user_role is not linked to your account. sts_ocm_role is linked to your organization <org_number> which requires sts_user_role to be linked to your Red Hat account <account_id>.Please create a user role and link it to the account: User Account <account ID> is not authorized to perform STS cluster operations
```

このエラーは、**user-role** がリンク解除または削除されたときに発生します。

手順

1. 次のコマンドを実行して、**user-role** IAM リソースを作成します。

```
$ rosa create user-role
```

2. ロールが作成されたことを確認したら、クラスターを削除できます。以下で、ロールが作成され、リンクされたことを確認します。

```
I: Successfully linked role ARN <user role ARN> with account <account ID>
```