Red Hat OpenShift Service on AWS 4

关于

AWS 上的 OpenShift Service 文档.

Last Updated: 2024-07-02

Red Hat OpenShift Service on AWS 4 关于

AWS 上的 OpenShift Service 文档.

法律通告

摘要

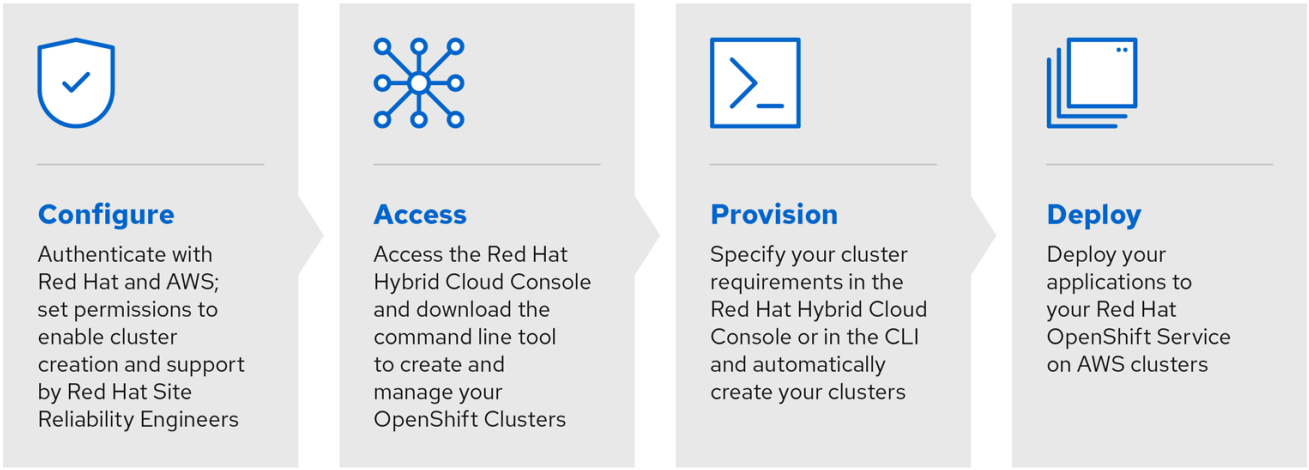
欢迎使用官方的 OpenShift Service on AWS 文档，您可以在其中了解 OpenShift Service on AWS 并开始了解其功能。

目录

第 1 章 RED HAT OPENSHIFT SERVICE ON AWS 4 文档

内容表

欢迎使用官方的 Red Hat OpenShift Service on AWS (ROSA)文档，您可以在其中了解 ROSA 并开始了解其功能。要了解 ROSA，使用 Red Hat OpenShift Cluster Manager 和命令行界面(CLI)工具(CLI)工具、使用体验以及与 Amazon Web Services (AWS)服务集成，从 ROSA 文档 开始。



要浏览 ROSA 文档，请使用左侧导航条。

第 2 章 使用 HCP 了解更多有关 ROSA 的信息

带有托管 control plane (HCP)的 Red Hat OpenShift Service on AWS (ROSA)提供了更低成本的解决方案，用于创建专注于效率的受管 ROSA 集群。您可以快速创建新集群并在几分钟内部署应用程序。

2.1. 使用 HCP 的 ROSA 的主要功能

- 使用 HCP 的 ROSA 至少需要两个节点，使其非常适合较小的项目，同时仍然能够扩展以支持更大的项目和企业。
- 底层 control plane 基础架构是完全管理的。control plane 组件（如 API 服务器和 etcd 数据库）托管在红帽拥有的 AWS 帐户中。
- 置备时间大约为 10 分钟。
- 客户可以单独升级 control plane 和机器池，这意味着它们在升级过程中不需要关闭整个集群。

2.2. 使用 HCP 的 ROSA 入门

使用以下部分查找内容以帮助您了解和使用 HCP 的 ROSA。

2.2.1. 架构

使用 HCP 了解 ROSA	使用 HCP 部署计划 ROSA	其他资源
架构概述	备份和恢复	带有 HCP 生命周期的 ROSA
使用 HCP 架构的 ROSA		使用 HCP 服务定义的 ROSA
		获取支持

2.2.2. Cluster Administrator

使用 HCP 了解 ROSA	使用 HCP 部署 ROSA	使用 HCP 管理 ROSA	其他资源
使用 HCP 架构的 ROSA	使用 HCP 安装 ROSA	日志记录	获得支持
OpenShift 互动学习门户	Storage	监控概述	带有 HCP 生命周期的 ROSA
	备份和恢复		
	升级		

2.2.3. 开发者

了解使用 HCP 的 ROSA 中的应用程序开发	部署应用程序	其他资源
Red Hat Developers 网站	构建应用程序概述	获取支持
Red Hat OpenShift Dev Spaces（以前称为 Red Hat CodeReady Workspaces）	Operator 概述	
	镜像	
	以开发者为中心的 CLI	

第 3 章 使用 HCP 的 AWS STS 和 ROSA 解释

带有托管 control plane (HCP)的 Red Hat OpenShift Service on AWS (ROSA)使用 AWS (Amazon Web Services)安全令牌服务(STS)用于 AWS Identity Access Management (IAM)获取必要的凭证，以便与 AWS 帐户中的资源交互。

3.1. AWS STS 凭证方法

作为使用 HCP 的 ROSA 的一部分，红帽必须被授予在 AWS 帐户中管理基础架构资源所需的权限。使用 HCP 的 ROSA 授予集群自动化软件有限、对 AWS 帐户中资源的短期访问权限。

STS 方法使用预定义的角色和策略为 IAM 角色授予临时的、具有最低权限的权限。在请求后，凭据通常会在一小时后过期。过期后，AWS 不再识别它们，不再从 API 请求访问它们。如需更多信息，请参阅 AWS 文档。

必须为使用 HCP 集群的每个 ROSA 创建 AWS IAM STS 角色。ROSA 命令行界面(CLI) (**rosa**)管理 STS 角色，并帮助您为每个角色附加 ROSA 特定 AWS 管理的策略。CLI 提供了用于创建角色、附加 AWS 管理的策略的命令和文件，以及允许 CLI 自动创建角色并附加策略的选项。

3.2. AWS STS 安全

AWS STS 的安全功能包括：

- 用户提前创建的明确和有限的策略集合。
    - 用户可以查看平台所需的每个请求权限。
- 该服务不能在这些权限之外执行任何操作。
- 不需要轮转或撤销凭证。每当服务需要执行某个操作时，它会获取以一小时或更少形式过期的凭证。
- 凭证过期会降低凭证泄漏和重复使用的风险。

使用 HCP 的 ROSA 将集群软件组件具有短期安全凭证授予特定和隔离的 IAM 角色。凭证与特定于每个组件的 IAM 角色关联，并发出 AWS API 调用的集群。此方法与云服务资源管理中最低特权和安全实践的原则一致。

3.3. 使用 HCP 的 ROSA 组件

- **AWS 基础架构** - 集群所需的基础架构，包括 Amazon EC2 实例、Amazon EBS 存储和网络组件。如需有关云资源配置的更多信息，请参阅 AWS 计算类型，以查看计算节点的支持的实例类型 和 置备的 AWS 基础架构。
- **AWS STS** - 授予短期动态令牌的方法，为用户提供与 AWS 帐户资源临时交互所需的权限。
- **OpenID Connect (OIDC)** - 集群 Operator 与 AWS 进行身份验证的机制，通过信任策略假设集群角色，并从 AWS IAM STS 获取临时凭证来发出所需的 API 调用。
- **角色和策略** - ROSA 与 HCP 使用的角色和策略可以划分成集群范围的角色和 Operator 角色和策略。
  策略决定了每个角色允许的操作。如需有关信任策略的更多详情，请参阅使用 STS 的 ROSA 集群以及 ROSA IAM 角色资源 的更多详情，请参阅关于 IAM 资源。
    - 集群范围的角色有：

- ManagedOpenShift-Installer-Role
- ManagedOpenShift-Worker-Role
- ManagedOpenShift-Support-Role

- 帐户范围的 AWS 管理的策略有：
  - ROSAInstallerPolicy
  - ROSAWorkerInstancePolicy
  - ROSASRESupportPolicy
  - ROSAIngressOperatorPolicy
  - ROSAAmazonEBSCSIDriverOperatorPolicy
  - ROSACloudNetworkConfigOperatorPolicy
  - ROSAControlPlaneOperatorPolicy
  - ROSAImageRegistryOperatorPolicy
  - ROSAKMSProviderPolicy
  - ROSAKubeControllerPolicy
  - ROSAManageSubscription
  - ROSANodePoolManagementPolicy

注意

集群 Operator 角色使用某些策略，如下所列。Operator 角色在第二个步骤中创建，因为它们依赖于现有集群名称，且无法与集群范围的角色同时创建。

- Operator 角色是：
  - <operator_role_prefix>-openshift-cluster-csi-drivers-ebs-cloud-credentials
  - <operator_role_prefix>-openshift-cloud-network-config-controller-cloud-credentials
  - <operator_role_prefix>-openshift-machine-api-aws-cloud-credentials
  - <operator_role_prefix>-openshift-cloud-credential-operator-cloud-credentials
  - <operator_role_prefix>-openshift-image-registry-installer-cloud-credentials
  - <operator_role_prefix>-openshift-ingress-operator-cloud-credentials
- 为每个集群范围的角色和每个 Operator 角色创建信任策略。

3.4. 使用 HCP 集群部署 ROSA

按照以下步骤使用 HCP 集群部署 ROSA：

1. 您可以创建集群范围的角色。
2. 您可以创建 Operator 角色。
3. 红帽使用 AWS STS 将所需的权限发送到 AWS，以允许 AWS 创建并附加对应的 AWS 管理的 Operator 策略。
4. 您可以创建 OIDC 供应商。
5. 已创建集群。

在集群创建过程中，ROSA CLI 会为您创建所需的 JSON 文件，并输出您需要的命令。如果需要，ROSA CLI 也可以为您运行命令。

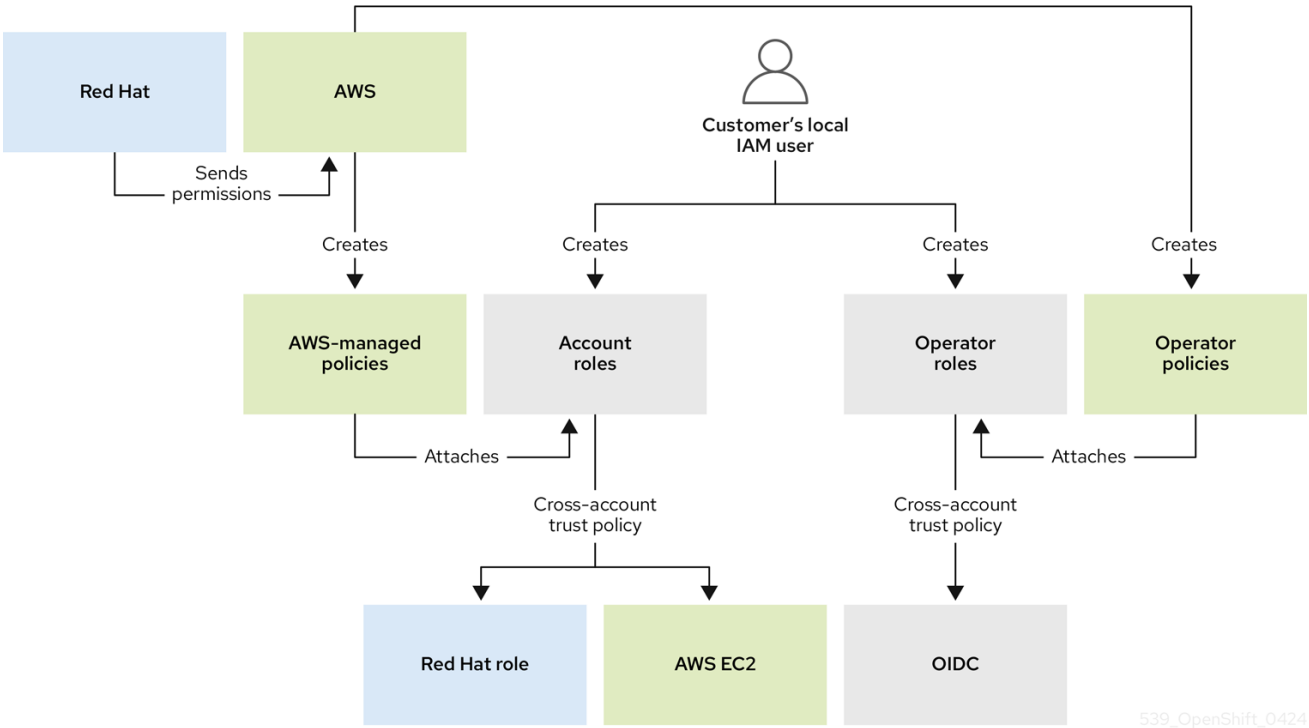
ROSA CLI 可以自动为您创建角色，也可以使用 **--mode manual** 或 **--mode auto** 标志手动创建角色。有关部署的详情，请参阅使用自定义创建集群。

3.5. 使用 HCP 工作流的 ROSA

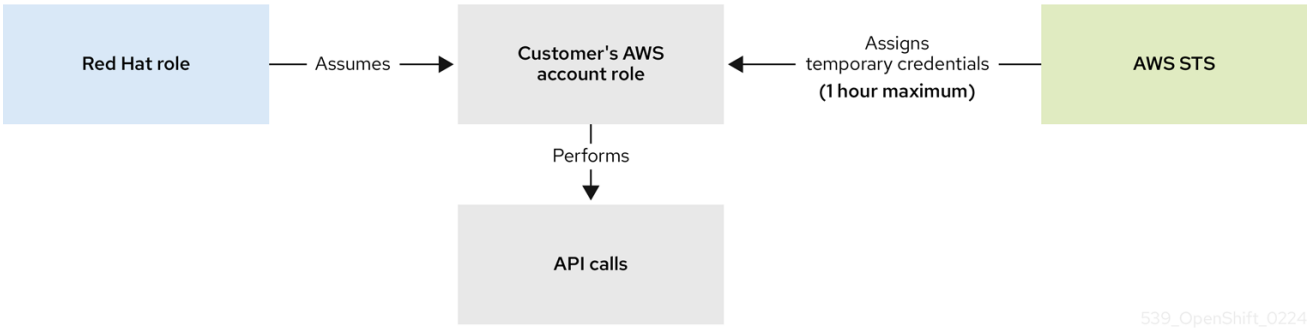
用户创建所需的集群范围的角色。在创建角色时，会创建一个信任策略，称为跨帐户信任策略，该策略允许红帽拥有的角色假定角色。还会为 EC2 服务创建信任策略，它允许 EC2 实例上的工作负载假定角色和获取凭据。AWS 为每个角色分配对应的权限策略。

创建集群范围的角色和策略后，用户可以创建集群。启动集群创建后，用户会创建 Operator 角色，以便集群 Operator 可以发出 AWS API 调用。然后，这些角色被分配给之前创建的相应权限策略，以及带有 OIDC 供应商的信任策略。Operator 角色与集群范围的角色不同，它们最终代表需要访问 AWS 资源的 pod。因为用户无法将 IAM 角色附加到 pod，所以它们必须使用 OIDC 供应商创建信任策略，以便 Operator，因此 pod 可以访问它们所需的角色。

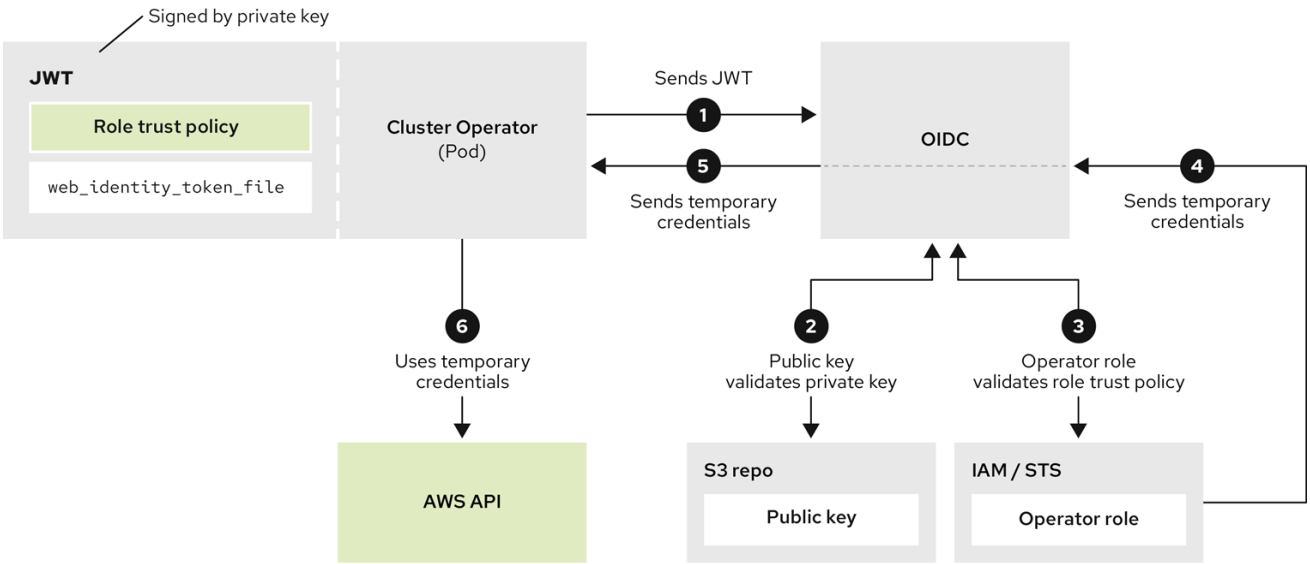
用户将角色分配给对应的策略权限后，最后一步是创建 OIDC 供应商。



当需要新角色时，当前使用红帽角色的工作负载将假定 AWS 帐户中的角色，从 AWS STS 获取临时凭证，并开始使用所假定角色的权限策略允许的用户 AWS 帐户中的 API 调用执行操作。凭据是临时的，最长持续时间为一小时。



Operator 使用以下流程获取必要的凭证来执行其任务。每个 Operator 都会被分配一个 Operator 角色、权限策略和带有 OIDC 供应商的信任策略。Operator 将通过将包含角色和令牌文件的 JSON Web 令牌(**web_identity_token_file**)传递给 OIDC 供应商来假定角色，然后使用公钥验证签名密钥。公钥是在集群创建过程中创建的，并存储在 S3 存储桶中。然后，Operator 会确认签名令牌文件中的主题与角色信任策略中的角色匹配，以确保 OIDC 供应商只能获取允许的角色。然后，OIDC 供应商会向 Operator 返回临时凭证，以便 Operator 可以发出 AWS API 调用。有关可视化表示，请查看以下图：



第 4 章 法律通知