

Sonatype Nexus Repository OSS on Amazon Web Services

部署手册

朱孟欣

魏昌昊

戴晓斌

鲁倩

版本：v1.0.1

最后更新时间: 2021 年 2 月



Copyright (c) 2021 by Amazon.com, Inc. or its affiliates.

目 录

背景.....	3
解决方案描述	3
使用场景	3
系统架构	3
架构图.....	3
Amazon VPC.....	4
Amazon EKS.....	4
Amazon EFS	4
Amazon S3	4
Amazon Certificate Manager (ACM).....	4
Amazon Route 53.....	5
部署说明	5
部署前提.....	5
快速部署	5
启动 CLOUDFORMATION 堆栈	5
指定堆栈详细信息.....	6
配置堆栈选项.....	8
审核堆栈.....	9
使用 NEXUS OSS	10
清理部署	11

背景

本部署指南详细描述了如何在云上使用 Amazon CloudFormation 模板部署

[Sonatype Nexus Repository OSS](#)，从而构建可自恢复、成本优化的架构。

解决方案描述

Nexus Repository OSS 的容器在 Amazon EKS 上部署和运行。为了确保系统可自恢复，Amazon EKS 部署在多个可用区，且使用 Amazon EFS 文件系统作为 Nexus Repository OSS 数据存储。

本解决方案使用 Amazon S3 作为 Nexus blob store 数据存储优化存储成本。此解决方案部署时需提供部署后 Nexus Repository OSS 自定义域名，以及该域名在 Route 53 的托管区域 ID。

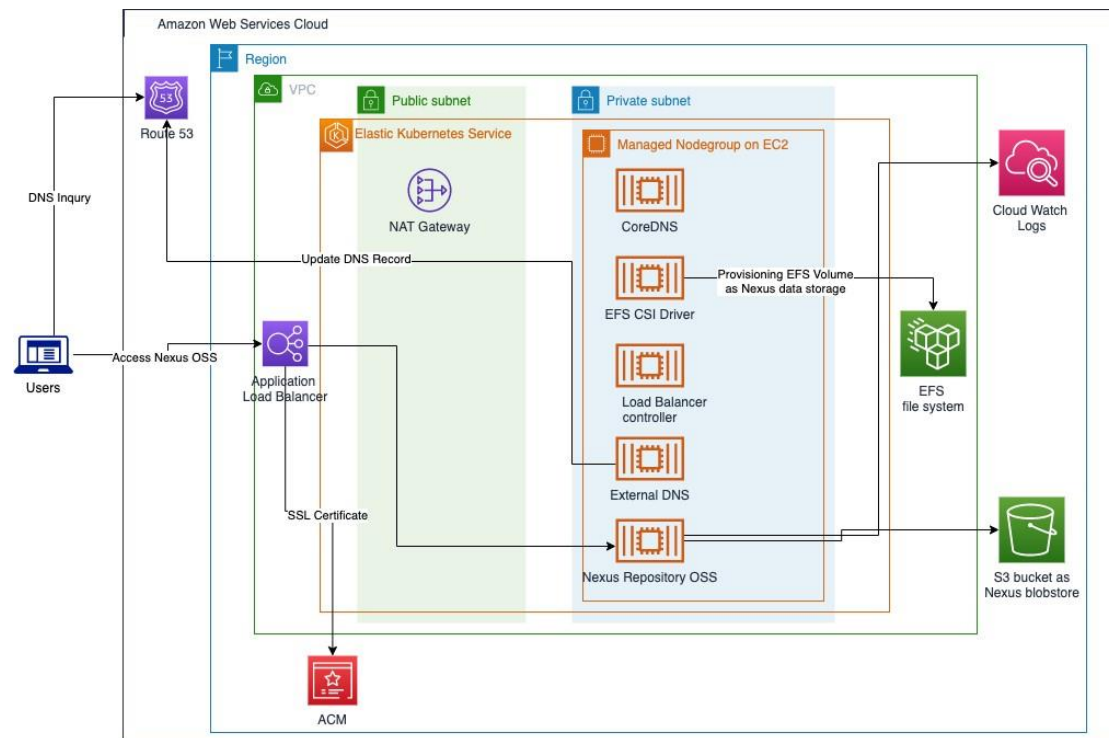
使用场景

此解决方案可以快速在 Amazon Web Services 账户的私有网络内部署基于 Nexus Repository OSS 的软件构件管理库，以便轻松安全地存储、发布和分享其软件开发过程中所使用的程序包。

系统架构

架构图

此解决方案可在由西云数据运营的 Amazon Web Services（宁夏）区域或由光环新网运营的 Amazon Web Services（北京）区域中部署。



组件

Amazon VPC

- 本解决方案使用 Amazon VPC，提供网络隔离、高可用的架构。

Amazon EKS

- 本解决方案使用 Amazon EKS，提供可自恢复的架构。

Amazon EFS

- 用于安全、高可用的存储 Nexus OSS 管理数据。

Amazon S3

- 用于安全、高可用、高持久、成本优化的存储软件构件。

Amazon Certificate Manager (ACM)

- 用于申请自定义的 SSL 证书。

Amazon Route 53

- 用于自定义域名解析及 ACM 证书创建时验证。

部署说明

部署前提

1. 部署使用的域名要通过 ICP 备案，且接入由西云数据运营的 Amazon Web Services（宁夏）区域或由光环新网运营的 Amazon Web Services（北京）区域。
2. 在 Route 53 中为该域名创建公开的托管区域。

快速部署

本文的步骤主要针对在运行在由西云数据运营的 Amazon Web Services（宁夏）区域或由光环新网运营的 Amazon Web Services（北京）区域中部署该解决方案，您可以使用以下链接快速启动一个 CloudFormation 堆栈来部署和管理整个方案：

启动 CloudFormation 堆栈

点击宁夏和北京区域链接，打开 Amazon Web Services 管理控制台（如果还没登录会先跳转到登录页面，登录后进入模板启动页面）。默认情况下，此模板在宁夏区域启动，您同时可以使用控制台右上方的区域选择链接，以在其他区域部署该方案。然后单击下面的按钮以启动 Amazon CloudFormation 模板。



CloudFormation > 堆栈 > 创建堆栈

第 1 步
指定模板

第 2 步
指定堆栈详细信息

第 3 步
配置堆栈选项

第 4 步
审核

创建堆栈

先决条件 - 准备模板

准备模板
每个堆栈都基于一个模板。模板是一个 JSON 或 YAML 文件，其中包含有关您希望在堆栈中包含的 AWS 资源的配置信息。

☒ 模板已就绪
 ☐ 使用示例模板
 ☐ 在设计器中创建模板

指定模板

模板是一个 JSON 或 YAML 文件，该文件描述了堆栈的资源 and 属性。

模板源
选择模板会生成一个 Amazon S3 URL，在那里它将被存储。

☒ Amazon S3 URL
 ☐ 上传模板文件

Amazon S3 URL

Amazon S3 模板 URL

S3 URL: 将在提供 URL 时生成 [在设计器中查看](#)

[取消](#)
[下一步](#)

指定堆栈详细信息

参数	默认值	用途
DomainName		Nexus OSS 自定义域名
NexusAdminInitPassword		Nexus OSS 初始的 admin 用户密码，密码需要满足如下要求， - 最少 8 个字符 - 至少包含一个大写字母，一个小写字母，一个数字 - 可以包含符号字符
R53HostedZoneId		自定义域名在 Route 53 中的托管区域 ID

CloudFormation > 堆栈 > 创建堆栈

第 1 步
指定模板

第 2 步
指定堆栈详细信息

第 3 步
配置堆栈选项

第 4 步
审核

指定堆栈详细信息

堆栈名称

堆栈名称

SonatypeNexus3

堆栈名称可以包含字母 (A-Z 和 a-z)、数字 (0-9) 和短划线 (-)。

参数

参数是在模板中定义的，并且允许您在创建或更新堆栈时输入自定义值。

DomainName

The domain name of Nexus OSS deployment, such as mydomain.com.

nexus.bjs.mydomain.com

NexusAdminInitPassword

The admin init password of Nexus3. - at least 8 characters - must contain at least 1 uppercase letter, 1 lowercase letter, and 1 number - Can contain special characters

R53HostedZoneId

The hosted zone ID of given domain name in Route 53.

z3

取消

上一步

下一步

点击【下一步】。

配置堆栈选项

保持默认值

第 1 步
指定模板

第 2 步
指定堆栈详细信息

第 3 步
配置堆栈选项

第 4 步
审核

配置堆栈选项

标签

您可以指定要应用于堆栈中资源的标签 (键值对)。每个堆栈最多可以添加 50 个唯一的标签。 [了解更多。](#)

键

值

移除

添加标签

权限

选择 IAM 角色可明确定义 CloudFormation 如何创建、修改或删除堆栈中的资源。如果您不选择角色，CloudFormation 会根据用户凭据使用权限。 [了解更多。](#)

IAM 角色 - 可选

选择 CloudFormation 用于在堆栈上执行的所有操作的 IAM 角色。

IAM 角色...

示例角色名称

移除

高级选项

您可以为堆栈设置附加选项，如通知选项和堆栈策略。 [了解更多。](#)

► 堆栈策略

定义要在堆栈更新期间保护以防止意外更新的资源。

► 回滚配置

指定在创建和更新堆栈时要监控的 CloudFormation 警报。如果操作违反了警报阈值，CloudFormation 会将其回滚。 [了解更多。](#)

► 通知选项

► 堆栈创建选项

取消 上一步 下一步

点击【下一步】。

审核堆栈

保持默认值，但请勾选如下图的确认选项。

堆栈创建选项

失败时回滚

已启用

超时

-

终止保护

已禁用

功能和转换

③ 转换可能需要访问功能

转换可能会添加 Identity and Access Management (IAM) 资源，这些资源可以为实体提供访问权限以便对您的 账户做出更改。如果转换添加 IAM 资源，您必须确认其容量以创建或更新它们。确认您想要创建或更新 IAM 资源，并且它们具有所需的最低权限。此外，如果它们具有自定义名称，请检查这些名称在您的 账户里是唯一的。 [了解更多](#)。

☒ 我确认， CloudFormation 可能创建 IAM 资源。

☒ 我确认， CloudFormation 可能创建具有自定义名称的 IAM 资源。

☒ 我确认， CloudFormation 可能需要以下功能: CAPABILITY_AUTO_EXPAND

取消

上一步

创建更改集

创建堆栈

点击【创建堆栈】。

等待大概 40 分钟，堆栈创建完成。

本解决方案创建了一个专用的 S3 存储桶用于高持久、高可用、低成本保存构件或软件包。您可以从堆栈输出中查看该 S3 存储桶名称，如下图，

NexusT2

删除

更新

堆栈操作

创建堆栈

堆栈信息

事件

资源

输出

参数

模板

更改集

输出 (3)

搜索输出

键	值	描述	导出名称
NexusClusterConfigCommand940654AB	aws eks update-kubeconfig --name NexusCluster2168A4B1-8534ec397a714bfd94086e85f6b6d0af --region cn-north-1 --role-arn arn:aws-cn:iam::[redacted]:role/NexusT2-AdminRole38563C57-1BOYEUPW7B5FL	-	-
NexusClusterGetTokenCommand68FC21D1	aws eks get-token --cluster-name NexusCluster2168A4B1-8534ec397a714bfd94086e85f6b6d0af --region cn-north-1 --role-arn arn:aws-cn:iam::[redacted]:role/NexusT2-AdminRole38563C57-1BOYEUPW7B5FL	-	-
nexus3s3bucketblobstore	nexus2-nexus3blobstore0[redacted]ok	S3 Bucket created for Nexus3 S3 Blobstore	-

Page 9 of 12

亚马逊

amazon web services

西云数据运营宁夏区域

光环新网运营北京区域

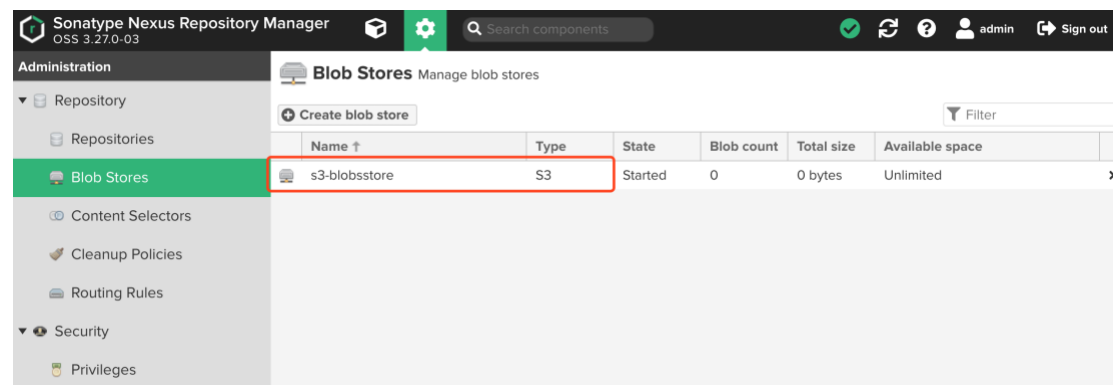
此外，Nexus Repository OSS 部署在 Amazon EKS 集群中，您可以通过输出查看如何使用 Amazon Web Services CLI 工具获取 EKS 集群访问 token 或者更新 kubeconfig 配置文件。请查阅[文档](#)了解更多 EKS 配置信息。

使用 Nexus OSS

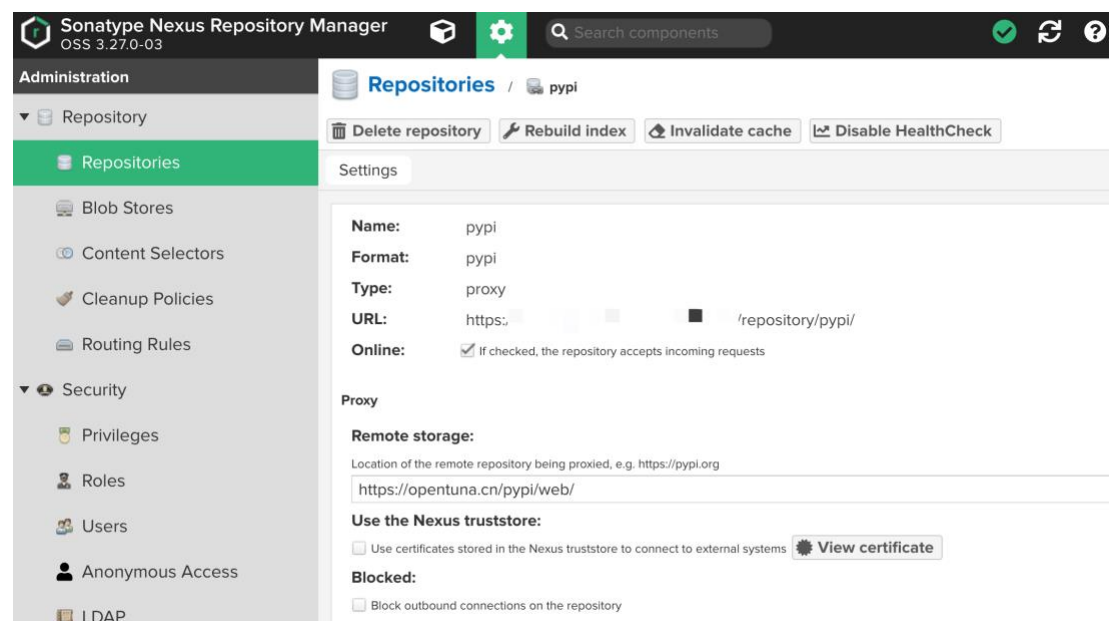
在浏览器的地址栏输入部署 Nexus Repository OSS 时输入的自定义域名，如上面定义的 `nexus.bjs.mydomain.com`。

使用用户名 `admin` 和部署时输入的初始密码登录 Nexus Repository OSS。为了系统安全，请及时修改管理员初始密码为符合企业安全规范的强密码。

访问 Nexus Repository OSS 设置，打开 **Repository – Blob Stores**，您可以看到本方案创建的 S3 存储桶已经被配置为一个名为 `s3-blobstore` 的 blob store。

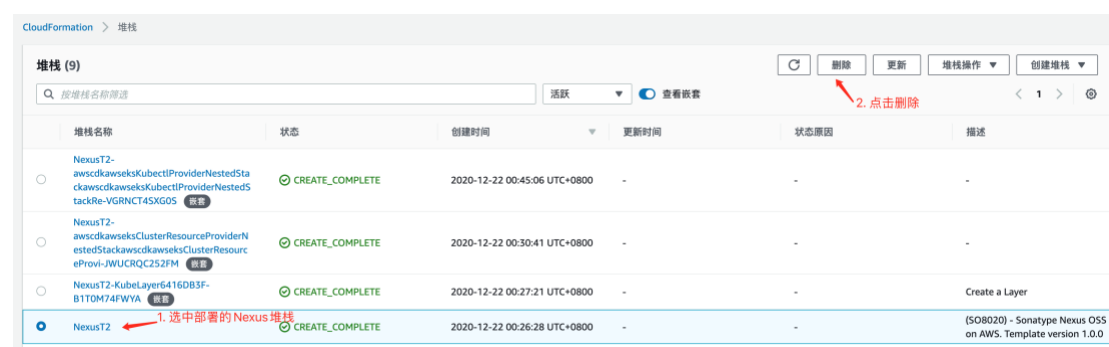


创建 Nexus Repository OSS 支持软件库，例如，代理模式下的 pypi 仓库，



清理部署

打开亚马逊云科技控制台，进入 CloudFormation 堆栈列表页面，选中您之前部署的堆栈名称，点击删除按钮。Nexus Repository OSS 解决方案部署的资源将会被删除。



请注意：本解决方案创建了一个 EFS 文件系统（以 *Nexus3FileSystem* 命名）存储 Nexus repository OSS 配置数据和一个 S3 存储桶（桶名称包含 *nexus3blobstore-*）用于存储构件数据。因为 EFS 文件系统和 S3 存储桶保存

了您的数据，删除本解决方案的时候，他们并不会被自动删除。如果您不再需要这些数据，请您通过控制台或 API 删除他们。