将ECS实例自动加入和移出Redis实例白名单

更新时间：2020-10-23 13:05:16

[**本页目录**](javascript:void(0))

* [前提条件](https://help.aliyun.com/document_detail/102410.html?spm=a2c4g.11186623.6.651.32be4f86IH84dl#h2-url-1)
* [背景信息](https://help.aliyun.com/document_detail/102410.html?spm=a2c4g.11186623.6.651.32be4f86IH84dl#h2-url-2)
* [操作步骤](https://help.aliyun.com/document_detail/102410.html?spm=a2c4g.11186623.6.651.32be4f86IH84dl#title-iic-9l4-btc)
* [步骤一：对RAM角色授予OOS服务权限](https://help.aliyun.com/document_detail/102410.html?spm=a2c4g.11186623.6.651.32be4f86IH84dl#title-upg-xh0-yuk)
* [步骤二：为扩容活动创建生命周期挂钩并触发扩容](https://help.aliyun.com/document_detail/102410.html?spm=a2c4g.11186623.6.651.32be4f86IH84dl#title-tbv-evs-i9i)
* [步骤三：查看Redis实例白名单](https://help.aliyun.com/document_detail/102410.html?spm=a2c4g.11186623.6.651.32be4f86IH84dl#title-w8b-5ug-owj)
* [（可选）步骤四：查看OOS执行情况](https://help.aliyun.com/document_detail/102410.html?spm=a2c4g.11186623.6.651.32be4f86IH84dl#title-rpg-821-wo6)
* [常见问题](https://help.aliyun.com/document_detail/102410.html?spm=a2c4g.11186623.6.651.32be4f86IH84dl#d7e149)

本教程介绍如何使用弹性伸缩生命周期挂钩挂起ECS实例，并结合运维编排服务OOS的模板，实现将ECS实例自动加入和移出Redis实例白名单。

**前提条件**

* 使用本教程进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成[账号注册](https://account.aliyun.com/register/register.htm?)。
* 已创建伸缩组，且伸缩组处于启用状态。
* 已创建Redis实例。
* 已为OOS服务创建RAM角色，具体操作请参见[为OOS服务设置RAM权限](https://help.aliyun.com/document_detail/120810.html)。

**说明** 本教程中使用默认的RAM角色OOSServiceRole，您也可以使用其他自定义的RAM角色，但需要保证RAM角色拥有执行OOS模板所需的权限。

**背景信息**

伸缩组支持关联负载均衡实例和RDS实例，但是暂时不能关联Redis实例。如果您有业务数据存储在Redis实例上，手动配置ECS实例加入或移出Redis实例白名单，操作效率较低。您可以通过生命周期挂钩和OOS模板将ECS实例自动加入和移出Redis实例白名单。

**操作步骤**

本教程以OOS公共模板ACS-ESS-LifeCycleModifyRedisIPWhitelist为例，实现在扩容时将ECS实例加入Redis实例白名单。步骤如下：

* [步骤一：对RAM角色授予OOS服务权限](https://help.aliyun.com/document_detail/102410.html?spm=a2c4g.11186623.6.651.32be4f86IH84dl#section-xm3-ezf-7ac)
* [步骤二：为扩容活动创建生命周期挂钩并触发扩容](https://help.aliyun.com/document_detail/102410.html?spm=a2c4g.11186623.6.651.32be4f86IH84dl#section-d01-6z7-54c)
* [步骤三：查看Redis实例白名单](https://help.aliyun.com/document_detail/102410.html?spm=a2c4g.11186623.6.651.32be4f86IH84dl#section-4zh-mic-anv)
* [（可选）步骤四：查看OOS执行情况](https://help.aliyun.com/document_detail/102410.html?spm=a2c4g.11186623.6.651.32be4f86IH84dl#section-zqx-4mp-kce)

**说明** 如果需要在缩容时将ECS实例移出Redis实例白名单，创建适用于弹性收缩活动的生命周期挂钩并触发缩容即可。

**步骤一：对RAM角色授予OOS服务权限**

您需要拥有OOS的执行权限才能执行OOS的模板。执行ACS-ESS-LifeCycleModifyRedisIPWhitelist中定义的运维操作时涉及云服务器ECS、弹性伸缩、云数据库Redis的资源。

1. 登录[RAM控制台](https://ram.console.aliyun.com/)。
2. 在左侧导航栏，单击**RAM角色管理**。
3. 创建权限策略。
   1. 在左侧导航栏，单击**权限管理 > 权限策略管理**。
   2. 在页面左上角，单击**创建权限策略**。
   3. 在**新建自定义权限策略**页面，指定权限配置，然后单击**确定**。

本教程中使用的配置如下表所示，未提及的配置保持默认即可。

| **配置项** | **说明** |
| --- | --- |
| **策略名称** | 填写ESSHookPolicyForRedisWhitelist。 |
| **配置模式** | 选择**脚本配置**。 |
| **策略内容** | 输入以下内容：  {  "Version": "1",  "Statement": [  {  "Action": [  "ecs:DescribeInstances"  ],  "Resource": "\*",  "Effect": "Allow"  },  {  "Action": [  "kvstore:ModifySecurityIps"  ],  "Resource": "\*",  "Effect": "Allow"  },  {  "Action": [  "ess:CompleteLifecycleAction"  ],  "Resource": "\*",  "Effect": "Allow"  }  ]  } |

1. 为OOSServiceRole授予权限策略。
   1. 在左侧导航栏，单击**RAM角色管理**。
   2. 找到OOSServiceRole，在**操作**区域，单击**添加权限**。

为OOS服务扮演的RAM角色OOSServiceRole添加权限即可完成授权。

* 1. 在**添加权限**页面，指定权限配置，然后单击**确定**。

本教程中使用的配置如下表所示，未提及的配置保持默认即可。

| **配置项** | **说明** |
| --- | --- |
| **授权范围** | 选择**云帐号全部资源**。 |
| **选择权限** | 添加自定义策略ESSHookPolicyForRedisWhitelist。 |

**步骤二：为扩容活动创建生命周期挂钩并触发扩容**

在创建生命周期挂钩时选择通知方式为OOS模板并设置相关参数，即可在触发扩容活动时将ECS实例自动加入Redis实例白名单。

1. 登录[弹性伸缩控制台](https://essnew.console.aliyun.com/)。
2. 在左侧导航栏中，单击**伸缩组管理**。
3. 在顶部菜单栏处，选择地域。
4. 找到待操作的伸缩组，选择一种方式打开伸缩组详情页面。
   * 在**伸缩组名称/ID**区域，单击伸缩组ID。
   * 在**操作**区域，单击**查看详情**。
5. 为扩容活动创建生命周期挂钩。
   * 在页面上方，单击**生命周期挂钩**页签。
   * 单击**创建生命周期挂钩**。
   * 指定生命周期挂钩配置，然后单击**确认**。

本教程中使用的配置如下表所示，未提及的配置保持默认即可。

| **配置项** | **说明** |
| --- | --- |
| **名称** | 输入ESSHookForAddRedisWhitelist。 |
| **适用的伸缩活动类型** | 选择**弹性扩张活动**。 |
| **超时时间** | 输入适当的超时时间，例如300秒。  **说明** 超时时间即用于执行自定义操作的时间，若超时时间过短，可能导致自定义操作失败，请评估自定义操作耗时并设置适当的超时时间。 |
| **执行策略** | 选择**继续**。 |
| **通知方式** | 模板配置如下：   * + - 通知方式：选择**OOS模板**。     - OOS模板类型：选择**公共模板**。     - 公共模板：选择ACS-ESS-LifeCycleModifyRedisIPWhitelist。   ACS-ESS-LifeCycleModifyRedisIPWhitelist的执行参数配置如下：   * + - **Redis实例ID**：输入Redis实例的ID。     - **修改IP白名单的方式**：选择Append，对应弹性扩张活动，将ECS实例加入Redis实例白名单。     - **执行使用到的权限的来源**：选择OOSServiceRole，步骤一中已为RAM角色OOSServiceRole添加操作ECS、弹性伸缩、Redis资源的权限，OOS服务扮演该RAM角色即可拥有相关权限。 |

1. 触发扩容。

本教程中以手动执行伸缩规则为例，您也可以通过定时任务、报警任务等方式触发扩容。

**说明** 手动执行伸缩规则触发扩缩容时，生命周期挂钩会生效，但手动添加或移出已有ECS实例时，生命周期挂钩不会生效。

* + 在页面上方，单击**伸缩规则**页签。
  + 单击**创建伸缩规则**。
  + 设置伸缩规则的属性，然后单击**确认**。

本教程中使用的配置如下表所示，未提及的配置保持默认即可。

| **配置项** | **说明** |
| --- | --- |
| **规则名称** | 输入Add1。 |
| **伸缩规则类型** | 选择**简单规则**。 |
| **执行的操作** | 设置为增加1台。 |

* + 在**伸缩规则**页面，找到新建的伸缩规则Add1，在**操作**区域，单击**执行**。
  + 单击**确定**。

执行伸缩规则后自动创建1台ECS实例，由于伸缩组内已创建生命周期挂钩ESSHookForAddRedisWhitelist，ECS实例会被挂起，同时自动通知OOS服务执行ACS-ESS-LifeCycleModifyRedisIPWhitelist中定义的运维操作。

**步骤三：查看Redis实例白名单**

1. 登录[云数据库Redis版管理控制台](https://kvstore.console.aliyun.com/)。
2. 在左侧导航栏，单击**实例列表**。
3. 找到Redis实例，在**实例ID/名称**区域，单击实例ID。
4. 在左侧导航栏，单击**白名单设置**。

如下图所示，Redis实例白名单中加入了新建ECS实例的私有IP，符合使用公共模板ACS-ESS-LifeCycleModifyRedisIPWhitelist的预期。[](https://static-aliyun-doc.oss-cn-hangzhou.aliyuncs.com/assets/img/zh-CN/6394129951/p139207.png)

如果成功创建了ECS实例，但是新建ECS实例的私有IP并没有加入Redis实例白名单，请前往OOS控制台查看运维任务执行情况，具体步骤请参见[（可选）步骤四：查看OOS执行情况](https://help.aliyun.com/document_detail/102410.html?spm=a2c4g.11186623.6.651.32be4f86IH84dl#section-zqx-4mp-kce)。

**（可选）步骤四：查看OOS执行情况**

1. 登录[OOS管理控制台](https://oos.console.aliyun.com/)。
2. 在左侧导航栏，单击**执行管理**。
3. 按开始时间找到执行，然后在**操作**区域，单击**详情**。
4. 单击**高级视图**。

**执行结果**页签中显示执行状态。[](https://static-aliyun-doc.oss-cn-hangzhou.aliyuncs.com/assets/img/zh-CN/6394129951/p139215.png)

如果执行失败，**执行结果**页签中也会显示相关的报错信息。[](https://static-aliyun-doc.oss-cn-hangzhou.aliyuncs.com/assets/img/zh-CN/6394129951/p139210.png)

**常见问题**

如果运维任务执行失败，请根据执行结果中的报错信息排查原因。常见的报错信息及解决方案如下：

* 报错信息：Forbidden.Unauthorized message: A required authorization for the specified action is not supplied.

解决方案：请检查是否为RAM角色OOSServiceRole添加了相应的权限，例如步骤一中的示例权限。您需要为RAM角色添加操作权限，确保OOS服务能够操作OOS模版中涉及的资源。

* 报错信息：Forbidden.RAM message: User not authorized to operate on the specified resource, or this API doesn't support RAM.

解决方案：请检查是否为RAM角色OOSServiceRole添加了相应的权限，例如步骤一中的示例权限。您需要为RAM角色添加操作权限，确保OOS服务能够操作OOS模版中涉及的资源。

* 报错信息：LifecycleHookIdAndLifecycleActionToken.Invalid message: The specified lifecycleActionToken and lifecycleActionId you provided does not match any in process lifecycle action.

解决方案：请评估生命周期挂钩的超时时间，确保在超时时间内可以执行完OOS模板中定义的运维任务。