Alibaba Cloud

Container Service User Guide

Document Version: 20220630

C-J Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

- You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloudauthorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
- 2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.
- 3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
- 4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).
- 5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud and/or its affiliates Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
- 6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
A Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
O Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
C) Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
? Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click Settings> Network> Set network type.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click OK.
Courier font	Courier font is used for commands	Run the cd /d C:/window command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	bae log listinstanceid Instance_ID
[] or [a b]	This format is used for an optional value, where only one item can be selected.	ipconfig [-all -t]
{} or {a b}	This format is used for a required value, where only one item can be selected.	switch {active stand}

Table of Contents

1.Workflow	09
2.Authorizations	10
2.1. Role authorization	10
2.2. Use sub-accounts	13
2.3. Create custom authorization policies	15
3.Clusters	19
3.1. Cluster introduction	19
3.2. Cluster lifecycle	19
3.3. Create a cluster	20
3.4. Cluster parameter configurations	25
3.5. Add an existing ECS instance	28
3.6. Manage cross-zone nodes	32
3.7. Bind and unbind a Server Load Balancer instance	34
3.8. Set the root domain name of a cluster	36
3.9. Download cluster certificate	38
3.10. Expand a cluster	39
3.11. Migrate a cluster	40
3.12. Search for a cluster	41
3.13. Delete a cluster	42
3.14. Clean up a cluster disk	42
3.15. Log on to image repository	43
3.16. Upgrade Agent	44
3.17. Upgrade Docker daemon	45
3.18. Upgrade system services	46
4.Nodes	48
4.1. Remove a node	48

4.2. Reset a node	48
4.3. View containers running on a node	50
4.4. Update a node certificate	51
5.Security groups	53
5.1. Container Service security group rules	53
5.2. Check a security group	55
5.3. Rebind a security group	56
6.Images and templates	57
6.1. View image list	57
6.2. View orchestration template list	57
6.3. Create an orchestration template	58
6.4. Update an orchestration template	59
6.5. Download an orchestration template	61
6.6. Delete an orchestration template	61
6.7. Save an orchestration template as a new one	62
7.Service orchestrations	64
7.1. Overview	64
7.2. Label description	65
7.3. probe	67
7.4. Rolling_updates	68
7.5. depends	70
7.6. scale	70
7.7. routing	71
7.8. lb	73
7.9. Log	75
7.10. Global	75
7.11. Service deployment constraints (affinity:service)	76
7.12. External	77

7.13. dns_options	77
7.14. oom_kill_disable	78
7.15. Variable substitution	78
7.16. Container rescheduling	78
7.17. High availability scheduling	79
7.18. Unsupported Docker Compose labels	79
8.Applications	81
8.1. Create an application	81
8.2. Application parameter configurations	87
8.3. Restrict container resources	91
8.4. High availability scheduling	92
8.5. Specified node scheduling	92
8.6. Schedule an application to specified nodes	93
8.7. View application details	95
8.8. Stop or activate an application	96
8.9. Change application configurations	97
8.10. Redeploy an application	98
8.11. Delete an application 10	00
8.12. Run offline tasks 10	00
8.13. Timing tasks 10	04
8.14. Default system application list10	06
9.Configurations 10	08
9.1. Create a configuration 10	08
9.2. Modify configurations 10	09
9.3. Implement multiple environments by using configurations 1	11
9.4. Delete a configuration 1	15
10.Services 17	16
10.1. Instructions 1	16

10.2. View service details	116
10.3. Activate or stop a service	117
10.4. Change service configurations	118
10.5. Reschedule a service	118
10.6. Delete a service	119
11.Networks	121
11.1. Container network interconnection	121
11.2. Use VPC in Container Service	123
12.Data volumes	129
12.1. Overview	129
12.2. Create an OSSFS data volume	129
12.3. Creating NAS data volumes	132
12.4. Create cloud disk data volumes	135
12.5. View and delete data volumes	137
12.6. Use third-party data volumes	138
12.7. FAQ	141
13.Logs	143
13.1. View logs	143
13.2. Enable Log Service	144
14.Monitoring	149
14.1. Container monitoring service	149
14.2. View monitoring information	150
14.3. Custom monitoring	152
14.4. Integrate with third-party monitoring solutions	154
14.5. Container auto scaling	157
14.6. Node auto scaling	163
14.7. Monitoring metrics	167

15.DevOps	173
15.1. Jenkins-based continuous delivery	
16.Service discovery and load balancing	173 182
16.1. Overview	182
16.2. Simple routing - supports HTTP and HTTPS	182
16.3. Simple routing - Configure domain names	187
16.4. Simple routing - Change HTTP to HTTPS	189
16.5. Simple routing - Force redirect from HTTP to HTTPS	194
16.6. Server Load Balancer routing	196
16.7. Service discovery between containers	201
16.8. Custom routing - simple sample	202
16.9. Custom routing - Supports TCP	214
16.10. Custom routing - supports multiple HTTPS certificates	217
17.Release policy	220
17.1. Introductions on release strategies	220
17.2. Blue-green release policy with simple routing	221
17.3. Blue-green release policy with Server Load Balancer routi	226

1.Workflow

The complete workflow for Container Service is as follows.



Step 1: Grant roles to an account.

For more information, see Role authorization.

Step 2: Create a cluster.

You can select the network environment of the cluster, and set the number of nodes and configurations for the cluster.

Step 3: Create an application by using an image or orchestration template.

Select an existing image or orchestration template, or create a new image or orchestration template.

If your application is composed of services supported by multiple images, create the application by using an orchestration template.

Step 4: Check the application status and the information of relevant services and containers after the deployment.

2.Authorizations 2.1. Role authorization

Grant the system default roles AliyunCSDefaultRole and AliyunCSClusterRole to the service account when you activate Container Service. Only after the roles are correctly granted, Container Service can normally call the services such as Elastic Compute Service (ECS), Object Storage Service (OSS), NAS, and Server Load Balancer (SLB), create clusters, and store logs.

Instructions

- If you have used Container Service before 15 January 2018, the system completes the role authorization by default. For more information about the permissions associated with each role, see the API documents of each product. If you used Container Service with a Resource Access Management (RAM) user before, upgrade the authorization policy for the RAM user. For more information, see 子账号策略升级.
- On 15 January 2018, Container Service is fully accessed to the cross-service authorization. New users who use the primary account can use Container Service only after having the cross-service authorization completed. If new users need to authorize RAM users to use Container Service, go to the RAM console to authorize the RAM users. For more information, see Use sub-accounts.

Procedure

1. If you have not granted the default roles to the service account correctly, the Cloud Resource Access Authorization page appears after you log on to the Container Service console. Click **Confirm Authorization Policy**.

25 needs your permission to access your cloud resources.
he system has created roles for the following user. These roles can be found below. CS. After authorization, CS will have access to your cloud resources.
AliyunCSDefaultRole
Description: The Container Service will use this role to access your resources in other services.
Permission Description: The policy for AliyunCSDefaultRole.
AliyunCSClusterRole
Description: The clusters of Container Service will use this role to access your resources in other services.
Permission Description: The policy for AliyunCSClusterRole.
Formation reactigates the policy of Allynica-calaborhous

? Note Container Service has configured the default role permissions. To modify the role permissions, go to the User Management page of the RAM console. Note that incorrect configurations might cause Container Service cannot obtain the required permissions.

2. After completing the authorization, refresh the Container Service console and then perform the operations.

To view the policy details of the roles AliyunCSDefaultRole and AliyunCSClusterRole, log on to the RAM console.

Default role permissions

For more information about permissions of each role, see the API documents of each product.

AliyunCSDefaultRole permissions

The default role AliyunCSDefault Role contains the following main permissions:

• ECS-related permissions

Action	Description
ecs:RunInstances	Query ECS instance information.
ecs:RenewInstance	Renew ECS instances.
ecs:Create*	Create ECS-related resources, such as instances and disks.
ecs:AllocatePublicIpAddress	Allocate public IP addresses.
ecs:AllocateEipAddress	Allocate Elastic IP (EIP) addresses.
ecs:Delete*	Delete ECS instances.
ecs:StartInstance	Start ECS-related resources.
ecs:StopInstance	Stop ECS instances.
ecs:RebootInstance	Restart ECS instances.
ecs:Describe*	Query ECS-related resources.
ecs:AuthorizeSecurityGroup	Configure inbound security group rules.
ecs:RevokeSecurityGroup	Revoke security group rules.
ecs:AuthorizeSecurityGroupEgress	Configure outbound security group rules.
ecs:AttachDisk	Add disks.
ecs:DetachDisk	Clean up disks.
ecs:AddTags	Add tags.
ecs:ReplaceSystemDisk	Change system disks of ECS instances.
ecs:ModifyInstanceAttribute	Modify ECS instance attributes.
ecs:JoinSecurityGroup	Add ECS instances to specified security groups.
ecs:LeaveSecurityGroup	Remove ECS instances from specified security groups.
ecs:UnassociateEipAddress	Unbind EIP addresses.
ecs:ReleaseEipAddress	Release EIP addresses.

• Virtual Private Cloud (VPC)-related permissions

Action	Description
vpc:Describe*	Query information of VPC-related resources.
vpc:DescribeVpcs	Query VPC information.
vpc:AllocateEipAddress	Allocate EIP addresses.
vpc:AssociateEipAddress	Associate with EIP addresses.
vpc:UnassociateEipAddress	Do not associate with EIP addresses.
vpc:ReleaseEipAddress	Release EIP addresses.
vpc:CreateRouteEntry	Create router interfaces.
vpc:DeleteRouteEntry	Delete router interfaces.

• SLB-related permissions

Action	Description
slb:Describe*	Query information related to Server Load Balancer.
slb:CreateLoadBalancer	Create Server Load Balancer instances.
slb:DeleteLoadBalancer	Delete Server Load Balancer instances.
slb:RemoveBackendServers	Unbind Server Load Balancer instances.
slb:StartLoadBalancerListener	Start specified listeners.
slb:StopLoadBalancerListener	Stop specified listeners.
slb:CreateLoadBalancerTCPListener	Create TCP-based listening rules for Server Load Balancer instances.
slb:AddBackendServers	Add backend servers.

AliyunCSClusterRole permissions

The default role AliyunCSClusterRole contains the following main permissions:

• OSS-related permissions

Action	Description
oss:PutObject	Upload files or folders.
oss:GetObject	Retrieve files or folders.
oss:ListObjects	Query file list information.

• NAS-related permissions

Action	Description
nas:Describe*	Return NAS-related information.
nas:CreateAccessRule	Create permission rules.

• SLB-related permissions

Action	Description
slb:Describe*	Query information related to Server Load Balancer.
slb:CreateLoadBalancer	Create Server Load Balancer instances.
slb:DeleteLoadBalancer	Delete Server Load Balancer instances.
slb:RemoveBackendServers	Unbind Server Load Balancer instances.
slb:StartLoadBalancerListener	Start specified listeners.
slb:StopLoadBalancerListener	Stop specified listeners.
slb:CreateLoadBalancerTCPListener	Create TCP-based listening rules for Server Load Balancer instances.
slb:AddBackendServers	Add backend servers.
slb:DeleteLoadBalancerListener	Delete listening rules of Server Load Balancer instances.
slb:CreateVServerGroup	Create VServer groups and add backend servers.
slb:ModifyVServerGroupBackendServers	Change backend servers in VServer groups.
slb:CreateLoadBalancerHTTPListener	Create HTTP-based listeners for Server Load Balancer instances.
slb:SetBackendServers	Configure backend servers and set the weight for a group of ECS instances at the Server Load Balancer instance backend.
slb:AddTags	Add tags for Server Load Balancer instances.

2.2. Use sub-accounts

Grant the sub-accounts the corresponding permissions before using the sub-accounts to log on to the Container Service console and perform the operations.

Step 1 Create sub-accounts and enable console logon

1. Log on to the RAM console.

- 2. Click Users in the left-side navigation pane. Click Create User in the upper-right corner.
- 3. Enter the username of the sub-account and then click OK.
- 4. On the User Management page, click Manage at the right of the created sub-account.
- 5. Click Enable Console Logon in the Web Console Logon Management section.
- 6. Enter the logon password in the appeared dialog box and click **OK**.

Step 2 Grant sub-accounts permissions to access Container Service

1. On the User Management page, click Authorize at the right of the created sub-account.

RAM	User Management	Create User CRefresh
Dashboard Users	User Name Search by User Name Search	
Groups	User Name/Display Name Description	Created At Actions
Policies	2 anglisen Progitised	2017-11-01 11:26:17 Manage Authorize Delete Join Group
Settings	Altaun 0557 Tolem Osmendan Itaan	2017-11-27 11:55:21 Manage Authorize Delete Join Group
	yangsun yangsun	2017-11-01 11:24:54 Manage Authorize Delete Join Group

2. Select the authorization policy and click 1 to add the policy to the Selected Authorization Policy Name.

Edit User-Level Authorization				×
Members added to this group have a group more than once.	II the perm	iissions of this gro	up. A member cannot be added to the sa	ime
Available Authorization Policy Names	Туре		Selected Authorization Policy Name	Туре
CS EcsRamRoleDocument		م •	AdministratorAccess Provides full acce	System
AliyunACSResourcesAccess_yangx aliyun container s	Custom	>	AliyunACSResourcesAccess_xingy aliyun container s	Custom
AliyunCSReadOnlyAccess Provides read-only	System	<		
AliyunCSFullAccess Provides full acce	System			
		-		
			ОК	Close

You can use the following system default authorization policies:

- AliyunCSFullAccess: Provides full access to Container Service.
- AliyunCSReadOnlyAccess: Provides read-only access to Container Service.

You can also create custom authorization policies as per your needs and grant the policies to the sub-accounts. For more information, see Create custom authorization policies.

Step 3 Log on to Container Service console with sub-accounts

Log on to the Container Service console with a sub-account.

If you have granted the AliyunCSDefaultRole and AliyunCSClusterRole roles to the main account, you can use the sub-account directly to log on to the Container Service console and perform the operations.

If you have not granted the AliyunCSDefaultRole or AliyunCSClusterRole roles to the main account before, click **Confirm Authorization Policy** in the appeared Cloud Resource Access Authorization page.



Then, refresh the Container Service console to perform the operations.

2.3. Create custom authorization policies

The authorization granularity of the system authorization policies provided by Container Service is coarse. If these authorization policies with coarse granularity cannot satisfy your requirements, create the custom authorization policies. For example, to control the permissions to a specific cluster, you must use the custom authorization policy to meet the requirements with fine granularity.

Create custom authorization policies

Get to know the basic structure and syntax of the authorization policy language before creating custom authorization policies. For more information, see Authorization policy language descriptions.

This document introduces how to grant Resource Access Management (RAM) users permissions to query, expand, and delete clusters.

Procedure

- 1. Log on to the RAM console with the primary account.
- 2. Click **Policies** in the left-side navigation pane. Click **Create Authorization Policy** in the upperright corner.
- 3. Select a template. Enter the authorization policy name and the policy content.

* Authorization Policy Name : Clusterpolicy Names must be 1-128 characters long. They may only contain the letters A-Z, numbers 0-9, and hyphens. Description : Policy Content : Policy Content : 1 { { "Statement"; [{ { "Action : ["Action : ["Action : ["Cs:Glet*", "Cs:GleCluster", "Cs:GleteCluster", "Cs:GleteCluster", "Cs:GleteCluster", "Resource": [] { ["acs:cs:*:*:cluster/cb2f4c [] {]] { [] [] [] [] [] [] []	ep 1: Select an authorizat	on policy Step 2: Edit permissions and submit. Policy creation compl
Name : Names must be 1-128 characters long. They may only contain the letters A-Z, numbers 0-9, and hyphens. Description : Policy Content : 1 2 *Cs:Get*, *Cs:Get*, *Cs:ScaleCluster*, *Cs:ScaleCluster*, *Resource*: [** </th <th>* Authorization Policy</th> <th>clusterpolicy</th>	* Authorization Policy	clusterpolicy
Description : Policy Content : $ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 7 \\ 8 \\ 9 \\ 10 \\ 7 \\ 8 \\ 9 \\ 10 \\ 7 \\ 8 \\ 9 \\ 10 \\ 7 \\ 8 \\ 9 \\ 10 \\ 7 \\ 8 \\ 9 \\ 10 \\ 7 \\ 8 \\ 9 \\ 10 \\ 7 \\ 8 \\ 9 \\ 10 \\ 7 \\ 8 \\ 9 \\ 10 \\ 7 \\ 8 \\ 9 \\ 10 \\ 7 \\ 8 \\ 9 \\ 10 \\ 7 \\ 8 \\ 9 \\ 10 \\ 7 \\ 8 \\ 9 \\ 10 \\ 7 \\ 8 \\ 9 \\ 10 \\ 7 \\ 8 \\ 10 \\ 7 \\ 8 \\ 10 \\ 7 \\ 8 \\ 10 \\ 7 \\ 8 \\ 10 \\ 7 \\ 8 \\ 10 \\ 7 \\ 8 \\ 10 \\ 7 \\ 8 \\ 10 \\ 7 \\ 8 \\ 10 \\ 7 \\ 8 \\ 10 \\ 7 \\ 8 \\ 10 \\ 7 \\ 8 \\ 10 \\ 7 \\ 8 \\ 10 \\ 7 \\ 8 \\ 10 \\ 7 \\ 8 \\ 10 \\ 7 \\ 8 \\ 10 \\ 7 \\ 8 \\ 10 \\ 7 \\ 10 \\ 10 \\ 7 \\ 8 \\ 10 \\ 7 \\ 10 \\ 10 \\ 7 \\ 10 \\ 10 \\ 7 \\ 10 \\ 10 \\ 10 \\ 7 \\ 10 \\ 10 \\ 10 \\ 10 \\ 10 \\ 10 \\ 10 \\ 10$	Name :	Names must be 1-128 characters long. They may only contain the letters A-Z, numbers 0-9, and hyphens.
Policy Content :	Description :	
	Policy Content :	1 { "Statement": [{ "Action": [4 "cs:Get*", "cs:ScaleCluster", 6 "cs:DeleteCluster", "getfect": "Allow", 7], "Effect": "Allow", 9 "cs:cs:*:*:cluster/cb2f4c "getfect": "1" 10 "acs:cs:*:*:cluster/cb2f4c "getfect": "1" 11] "Version": "1" 13 "Version": "1" Jetfect": "1" 14 Jetfect": "1" Jetfect": "1" Authorization Policy Format Jetfect": "1"
		Previous Create Authorization Policy

```
"Action": [
    "cs:Get*",
    "cs:ScaleCluster",
    "cs:DeleteCluster"
    "Effect": "Allow",
    "Resource": [
        "acs:cs:*:*:cluster/cluster ID"
"Version": "1"
```

Wherein:

• Action: Enter the permission that you want to grant.

Note All the Actions support wildcards.

- Resource supports the following configuration methods.
 - Grant permissions of a single cluster

```
"Resource": [
    "acs:cs:*:*:cluster/cluster ID"
```

• Grant permissions of multiple clusters

```
"Resource": [
    "acs:cs:*:*:cluster/cluster ID",
    "acs:cs:*:*:cluster/cluster ID"
```

• Grant permissions of all your clusters

```
"Resource": [
```

You must replace cluster ID with your actual cluster ID.

4. Click Create Authorization Policy after completing the configurations.

Container Service RAM action

Action	Description
CreateCluster	Create clusters.
AttachInstances	Add existing Elastic Compute Service (ECS) instances to clusters.
ScaleCluster	Expand clusters.
GetClusters	View cluster list.
GetClusterByld	View cluster details.
ModifyClusterName	Modify cluster names.
DeleteCluster	Delete clusters.
UpgradeClusterAgent	Upgrade cluster Agent.
GetClusterLogs	View cluster operation logs.
GetClusterEndpoint	View cluster access point.
GetClusterCerts	Download cluster certificate.
RevokeClusterCerts	Revoke cluster certificate.
BindSLB	Bind Server Load Balancer instances to clusters.
UnBindSLB	Unbind Server Load Balancer instances from clusters.
ReBindSecurityGroup	Rebind security groups to clusters.
CheckSecurityGroup	Check existing security group rules of clusters.
FixSecurityGroup	Fix cluster security group rules.
ResetClusterNode	Reset cluster nodes.

Action	Description
DeleteClusterNode	Delete cluster nodes.
CreateAutoScale	Create node auto scaling rules.
UpdateAutoScale	Update node auto scaling rules.
DeleteAutoScale	Delete node auto scaling rules.
GetClusterProjects	View applications in clusters.
CreateTriggerHook	Create triggers for applications.
GetTriggerHook	View application trigger list.
RevokeTriggerHook	Delete application triggers.
CreateClusterToken	Create tokens.

3.Clusters 3.1. Cluster introduction

A cluster is a collection of cloud resources that are required to run containers. It is associated with several Elastic Compute Service (ECS) nodes, Server Load Balancer, and other cloud resources.

Create a cluster

You can create a cluster by using the following methods:

Method 1: Create a cluster and several ECS instances.

You can directly create a cluster with several new ECS instances by using Container Service.

The ECS instances created using this method are all Pay-As-You-Go instances. If you want to use monthly or yearly subscription ECS instances, buy them separately and then follow **Method 2**.

Method 2: Create a zero-node cluster and add existing ECS instances to the cluster.

1. Create a zero-node cluster.

If you have purchased several ECS instances from the ECS service, create a zero-node cluster in Container Service. Method 1 except that you need to select Do not Add when creating the cluster to add existing ECS instances instead of creating some new ones.

The operations are the same as **Method 1** except that you need to select **Do not Add** when creating the cluster to add existing ECS instances instead of creating some new ones.

2. Add existing ECS instances.

You can add an existing ECS instance to Container Service in the following ways:

• Reset the image of the ECS instance and add the ECS instance to the cluster automatically.

As this method will reset the image and system disk of the ECS instance, proceed with caution. However, ECS instances added by using this method are cleaner.

• Run scripts on the ECS instance and manually add the ECS instance to the cluster.

This method is applicable to images that do not require a reset of the ECS instance.

Add an existing ECS instance.

Manage a cluster

You can search for, expand, connect to, clean up, or delete a cluster. For more information, see the following documents:

- Search for a cluster
- Expand a cluster
- Download cluster certificate
- Clean up a cluster disk
- Delete a cluster

3.2. Cluster lifecycle

A complete cluster lifecycle includes the following statuses.

Status	Description
inactive	The successfully created cluster does not contain any node.
initial	The cluster is applying for corresponding cloud resources.
running	The cluster successfully applied for the cloud resources.
updating	The cluster is upgrading the Agent.
scaling	Change the number of cluster nodes.
failed	The cluster application for cloud resources failed.
deleting	The cluster is being deleted.
delete_failed	The cluster failed to be deleted.
deleted (invisible to users)	The cluster is successfully deleted.

Cluster status flow



3.3. Create a cluster

You can specify the configurations and the number of Elastic Compute Service (ECS) instances when creating clusters. You can also create a zero-node cluster, and then bind it with other ECS instances.

? Note The zero-node cluster is in the Inactive status after the creation and is activated with the Running status after you add ECS instances to it. For how to add existing ECS instances to the cluster, see Add an existing ECS instance.

Instructions

Container Service performs the following operations when creating a cluster:

- Create a Server Load Balancer instance with 80:9080 configured as the listener if the Automatically Create Server Load Balancer check box is selected.
- Create a security group. The security group rules are as follows.

Virtual Private Cloud (VPC) inbound

<	alicloud-cs-auto-cr	reat 🐟 / vpc	-bp i will be jegel	0.8m6pubd0	Tutorial	C Back	k Add	Security Group Rules	Quickly Create Rules Ad	d ClassicLink Rule
Security Group R Instance List in S	Inbound Outbound								▲ Import Rules	± Export Rules
Network Interfac	Authorization Policy	Protocol Type	Port Range	Authorization Type	Authorization Object	Description	Priority	Creation time		Operation
	Allow	All	-1/-1	Address Field Access	172.22.0.0/16	-	100	2018-05-06 18:36:11	Modify Description	Clone Delete
	Allow	All ICMP	-1/-1	Address Field Access	0.0.0/0	-	100	2018-05-06 18:36:10	Modify Description	Clone Delete
	Allow	Custom TCP	80/80	Address Field Access	0.0.0/0	-	100	2018-05-06 18:36:09	Modify Description	Clone Delete
	Allow	Custom TCP	443/443	Address Field Access	0.0.0/0	-	100	2018-05-06 18:36:09	Modify Description	Clone Delete
=	Delete									

- Create a Resource Access Management (RAM) user if you have activated the RAM service.
- Create the ECS instances and distribute the Internet IP address to the ECS instances if you select Add in the Add Node field. (If the Network Type is VPC, distribute the Elastic IP (EIP) to the ECS instances and create the corresponding routing rules.)
- Use the configured Logon Password to configure the ECS instances.

Onte Container Service does not save this password.

• If the VPC node configuration fails, Container Service collects the standard output of the node creation and initialization. You can view the information in the cluster logs.

Limits

- Server Load Balancer instances created with clusters are only available in Pay-As-You-Go mode.
- By default, each account has a certain quota for the cloud resources they can create. The cluster fails to be created if the quota is exceeded. Make sure you have enough quota before creating the cluster. To increase your quota, open a ticket.
 - By default, each account can create at most five clusters in all regions and add up to 20 nodes to each cluster.
 - By default, each account can create at most 100 security groups.
 - By default, each account can create at most 60 Pay-As-You-Go Server Load Balancer instances.
 - By default, each account can create at most 20 EIPs.

Procedure

- 1. Log on to the Container Service console.
- 2. Click Swarm > Clusters in the left-side navigation pane. Click Create Cluster in the upper-right corner.

Container Service	Cluster List. You can create up to 5 clusters and can add up to 20 nodes in each cluster. Refresh Create Cluster •
Overview	2. O Create cluster O How to add existing ECS instances O Cross-zone node management. O Log Service integration O Connect to cluster through Docker Client
Applications	Name *
Services	Cluster Name/ID Cluster Type Region Network Type Cluster Status Node Status • Number of Nodes Time Created Docker Version Action
Clusters 2	You currently do not have any clusters. You can Create Cluster
Nodes	
Networks	

- 3. Complete the following configurations.
 - **Cluster Name**: Enter the name of the cluster. It can be 1–63 characters long and contain numbers, Chinese characters, English letters, and hyphens (-).

(?) Note The cluster name must be unique under the same account and the same region.

- **Region**: Select the region in which the cluster is to be deployed.
- **Zone**: Select the zone for the cluster.

? Note You can select the region and zone according to the distribution of your servers.

* Cluster Name:								
	The cluster name	e should be 1-63 c	haracters long, a	nd can contain nu	umbers, Chinese	characters, Englis	h letters and hyp	hens.
Region:	China North 1	China North 2	China East 1	China East 2	China South 1	Asia Pacific NE 1	US West 1	Asia Pacific SE 1
	(Qingdao)	(Beijing)	(Hangzhou)	(Shanghai)	(Shenzhen)	(Tokyo)	(Silicon Valley)	(Singapore)
	Asia Pacific SE 2	Asia Pacific SE 3	EU Central 1	US East 1		China North 3		
	(Sydney)	(Kuala Lumpur)	(Frankfurt)	(Virginia)	Hong Kong	(Zhangjiakou)		
Zone:	East China 1 Zo	ne G 🛛 👻						

4. Select the network type of the cluster. Currently, Container Service only supports VPC.

Complete the corresponding configurations.

Network Type:	VPC				
	vpc-bp/w99wppd11ml*	vsw-bpt/hathditionsgil 👻			
Initial CIDR Block	172.20.0.0/16	Existing CIDR Block of Container Service ⑦			
Ci Vi - - - Si	Can not be same as the CIDR used by the VPC. Can not be modified after creation. /alid value: · 192.168.0.0/16 · 172.19-30.0.0/16 · 10.0.0.0/16 System reserved private network address: 172.16/17/18/31.0.0/16 Maximum number of boots allowed in the cluster, 256				

VPC enables you to build an isolated network environment based on Alibaba Cloud. You can have full control over your own virtual network, including a free IP address range, Classless Inter-Domain Routing (CIDR) block division, and the configurations of route table and gateway.

Specify a VPC, a VSwitchld, and the initial CIDR block of containers (the subnet CIDR block to which the Docker containers belong. For ease of IP management, containers of different virtual machines belong to different CIDR blocks, and container subnet CIDR block cannot conflict with virtual machine CIDR block). We recommend that you build your own VPC/VSwitchld for the cluster to prevent issues such as network conflicts.

5. Select whether or not to add nodes.

You can create a cluster with several new ECS instances, or create a zero-node cluster and then add existing ECS instances to the cluster. For how to add existing ECS instances to the cluster, see Add an existing ECS instance.

$\circ \ \text{Add}$

a. Select the operating system for the node.

CentO	ating System: CentOS	7.4 64bit 🔹
-------	----------------------	-------------

Currently, Ubuntu 14.04/16.04 64bit and CentOS 7.4 64bit are supported.

b. Configure the ECS instance specifications.

	Instance General	Generation III Generation IV ②
		The series III use Intel Broadwell CPU , DDR4 memory, default is I/O optimization instance, high frequency and frequency in the two CPU with a variety of memory ratio, can provide users with better performance and more choices.
	Instance Family:	Type gn5 Enhanced sn1ne Enhanced sn2ne Enhanced se1ne
	I/O Optimized:	IO optimized
		instance
lode	Instance Type:	8-core, 60GB (ecs.gn5 *
Add N		More instance type, please contact customer service
	Instance Quantit	0 5set(s) 10set(s) 20set(s) 2 set(s) \$
		Each cluster can contain up to 20 ECS instances.
	System Disk Typ	Ultra Cloud Disk SSD Cloud Disk
	Data Disk Type:	Ultra Cloud Disk SSD Cloud Disk
	Attach Data Disk	Attach Data Disk
	Login:	Password Key Pair
	* Logon Passwo	0
		The password should be 8-30 characters long and contain three types of characters (uppercase/lowercase letters, numbers and special characters).

You can select the generation, family, type, and quantity of the instance, disk type and capacity (the ECS instance has a 20 GB system disk by default), and logon password. Container Service uses the configured **Logon Password** to configure the ECS instances when creating the cluster, but does not save this password.

? Note

- The data disk is mounted to the /var/lib/docker directory and used for the storage of Docker images and containers if you select the Attach Data Disk check box.
- In terms of performance and management, we recommend that you mount an independent data disk to the host and manage the persistent data of containers by using Docker volumes.

• Do not Add

You can click **Add Existing Instance** to add existing ECS instances to the cluster, or click Add Existing Instances on the Cluster List page to add existing ECS instances to the cluster after the cluster is created. For more information, see Add an existing ECS instance.

6. Select whether or not to configure public EIP.

If you select VPC as the network type, Container Service configures an EIP for each ECS instance in the VPC environment by default. If this is not required, select the **Do not Configure Public EIP** check box and then configure the SNAT gateway.

? Note You can apply for up to 20 EIPs per account. To use VPC and create EIP automatically when creating a cluster, the cluster fails to be created if the number of EIPs under your account reaches its quota.

EIP:	Do not Configure Public EIP
	You must configure the SNAT (refer to the following documents) if a public EIP is not configured. Failure in configuring the SNAT will cause the VPC unable to access the public network. This will affect cluster creation and application deployment. Documents for reference: Configuring SNAT for Linux in a VPC environment to use a server proxy with EIP to access the Internet without a public network ECS instance

7. Select whether or not to create a Server Load Balancer instance.

Server Load Balancer:	✓ Automatically Create Server Load Balancer	
	A public network Server Load Balancer instance is created by default while a cluster is created. The billing method is Pay-As-You-Go.	

The Automatically Create Server Load Balancer check box is selected by default. With this check box selected, a Server Load Balancer instance is created after the cluster is created. You can access the container applications in the cluster by means of this Server Load Balancer instance. The created Server Load Balancer instance is in the Pay-As-You-Go mode.

8. Select whether or not to install cloud monitoring plug-in on your ECS instances.

To view the monitoring information of the created ECS instances in the CloudMonitor console, select the Install cloud monitoring plug-in on your ECS check box.

Monitoring Plug-in: Install cloud monitoring plug-in on your	ECS.
Installing a cloud monitoring plug-in on the CloudMonitor console	e node allows you to view the monitoring information of the created ECS instance in the

9. You can select to add the IP addresses of the ECS instances to the RDS instance whitelist.

Adding the IP addresses of the ECS instances to the RDS instance whitelist facilitates the ECS instances to access the RDS instances.

? Note

- We recommend that you configure the RDS Whitelist when **Add** is selected for Add Node.
- If **Do not Add** is selected for Add Node and you want to configure the RDS Whitelist, add the existing ECS instances on the Create Cluster page. The RDS Whitelist cannot be configured if you create a zero-node cluster and add existing ECS instances after the cluster creation.
- The ECS instance must be in the same region as the RDS instance so that the IP address of the ECS instance can be added to the RDS instance whitelist.
- i. Click Select RDS Instances. The Add to RDS instance whitelist dialog box appears.

RDS Whitelist : Select RDS Instances

ii. Select the RDS instances and then click OK.

Add t	to RDS instance whitelist			×
	InstanceId	Instance engine version	ZoneId	Network
	rm-1udal1k7o8p2yvkv0	MySQL 5.6	cn-hangzhou-b	VPC
	rm-1ud0rifgodbkvmwf9	MySQL 5.7	cn-hangzhou-b	VPC
				OK Cancel

10. Click Create Cluster.

After the cluster is successfully created, you can configure the ECS instance or Server Load Balancer instance in the corresponding console.

Subsequent operations

On the **Cluster List** page, you can click **View Logs** at the right of the cluster to view the creation process logs of the cluster.

Container Service	Cluster List			You can	reate up to 5	clusters ar	nd can add up	to 20 nodes in each clu	ister. Refr	resh C	reate Cluster	•
Overview	Help: ${\mathscr S}$ Create cluster ${\mathscr S}$ How to add e	isting ECS inst	ances 🔗 Cross-z	one node management 🔗 L	og Service in	tegration	🖉 Connect to	cluster through Docker	Client			
Applications	Name *											
Services	Cluster Name/ID	Cluster Type	Region	Network Type	Cluster Status	Node Status 🕜	Number of Nodes	Time Created	Docker Version		Ad	ion
Clusters		Alihaha		VPC						Managa	View Logs	٦.
Nodes	test <1:071732830846486736#5736#5787077488	Cloud Cluster	China East 1 (Hangzhou)	vpc- bp t wik2wjrgz0t Imdpubd0	Running	Healthy C	2	05/06/2018,18:36:09	17.06.2- ce	Manage	Dele Monitor Mo	ste re •

You can create applications in the created cluster. For more information, see Create an application.

3.4. Cluster parameter configurations

This document aims to help you understand what the parameters on the page mean when you create a cluster. Then, you can configure the parameters smoothly. For some parameters, some documents are provided for your reference.

Cluster Name

> Document Version: 20220630

Configure the cluster name.

- The name can be 1-63 characters long and contain numbers, Chinese characters, English letters, and hyphens (-), but cannot start with a hyphen (-).
- You can modify the cluster name on the Cluster List page after creating the cluster.

Region and Zone

Container Service authorizes to create the region and zone of the Elastic Compute Service (ECS) instances. Currently, the regions and zones supported by Container Service belong to the subset of ECS product. For more information, see Regions and zones.

Network Type

Select VPC as the network type of the ECS instances. Alibaba Cloud Virtual Private Cloud (VPC) allows you to create a custom VPC. Layer-2 logical isolation exists between different VPCs. You can plan the Classless Inter-Domain Routing (CIDR) block of each cluster flexibly. VPC is applicable to a scenario with large-scale container clusters and provides higher security and flexibility. To better guarantee the system security and the support of hybrid cloud business, Container Service does not support creating clusters whose network type is classic network or with non-I/O optimized instance since January 1, 2018.

Initial CIDR Block of Container Service

Configure this parameter only when you select VPC. When planning the CIDR block, make sure the container initial CIDR block does not overlap with the VPC CIDR block.

- You can only specify one CIDR block for each VPC. 172.16.0.0/12 is the default VPC CIDR block.
- Specify the corresponding container CIRD block when creating a Container Service cluster. Currently, Container Service supports the following container CIDR blocks: 192.168.1.0/24 and 172.[16-31]. 1.0/24

Add Node

Container Service has two ways to add nodes: create nodes and add existing nodes. If you select Add, Container Service is authorized to automatically create ECS instances when the cluster is created and automatically add the created ECS instances to the created cluster. If you select Do not Add, the existing ECS instances are added to the cluster. You can add the existing ECS instances on the Create Cluster page directly or create a zero-node cluster and then add the existing ECS instances on the Cluster List page. For more information, see Add an existing ECS instance.

Node Type

The node type is Pay-As-You-Go by default. After creating the ECS instances, you can go to the ECS console to change the Pay-As-You-Go ECS instances to monthly or yearly subscription ECS instances.

Operating System

Select the operating system installed in the ECS instances. We recommend that you use Ubuntu 14.04 64 bit and CentOS 7.4 64 bit.

Instance Generation and Instance Family

Different instance generations correspond to different instance families. ECS instances provide you with corresponding computing capabilities based on the instance specifications. ECS instances can be divided into many generations and families according to the business scenarios and usage scenarios. For the specific scenarios for each instance generation and family, see Instance family.

Instance Type

ECS instance type defines two basic attributes: the CPU configuration and memory configuration of the instance. However, ECS instances can determine the specific service pattern of an instance only by working together with the disk, image, and network type.

Instance Quantity

The number of the ECS instances to be created. The number of ECS instances in one cluster cannot exceed 20. To enhance the cluster availability, we do not recommend that you create a cluster with one node. 2 sets is the default value in the console.

System Disk Type

Select the cloud disk type of the installation system. Select Ultra Cloud Disk or SSD Cloud Disk according to your requirements on the system performance of the ECS instances. For the performance indicator comparison between these two types of cloud disks, see EBS performance.

Data disk configurations

Select the type of the data disk that is to be mounted to the container. Select the **Attach Data Disk** check box and select the data disk capacity. The data disk is mounted to the */var/lib/docker* directory of the container to store the image data and container data.

Logon Password and Confirm Password

Enter and confirm the logon password of the ECS instances. The password is 8–30 characters long and must contain uppercase letters/lowercase letters, numbers, and special characters at the same time. This password is required when you log on to the ECS console or log on to the ECS instance by using SSH.

? Note

- Container Service uses this password to configure the ECS instances when creating the cluster, but does not save this password.
- Keep this password properly for the initialization usage.

EIP

The Elastic IP (EIP) is used to access the Internet. By default, Container Service retains the EIP. If you select to not retain the EIP, the cluster releases the EIP after the instance initialization. You can access the Internet by using the What is NAT Gateway? on your own.

Server Load Balancer

An Internet Server Load Balancer instance is created by default if a cluster is created. The billing method is Pay-As-You-Go. The created Server Load Balancer instance is used to distribute the traffic to control the services and implement the service high availability.

Monitoring Plug-in

Select the check box to install the cloud monitoring plug-in on the ECS instances. Then, the operating system-level performance indicators of the ECS instances in the cluster can be monitored.

RDS Whitelist

You can select to add the IP addresses of the created nodes to the RDS instance whitelist, which facilitates the ECS instances to access the RDS instances.

- We recommend that you configure the RDS Whitelist when Add is selected for Add Node.
- If **Do not Add** is selected for Add Node and you want to configure the RDS Whitelist, add the existing ECS instances on the Create Cluster page. The RDS Whitelist cannot be configured if you create a zero-node cluster and add existing ECS instances after the cluster creation.
- The ECS instance must be in the same region as the RDS instance so that the IP address of the ECS instance can be added to the RDS instance whitelist.

Security Group

Container Service configures the default security group and only sets the inbound security group rules. You can configure the security group according to your business scenarios after the cluster is created successfully. For more information, see Container Service security group rules

- Ports 443 and 80 can be opened or closed as per your needs.
- We recommend that you retain the ICMP rules for communication between nodes and the convenience of troubleshooting. Some tools also depend on ICMP.
- Make sure you open all the ports you need. Otherwise, some services become inaccessible. The port that is accessed by using Server Load Balancer is not required to be opened.

3.5. Add an existing ECS instance

You can add a purchased Elastic Compute Service (ECS) instance to a specified cluster.

Note At most 20 ECS instances can be added to a cluster by default. To add more ECS instances, open a ticket.

You can add an existing ECS instance in the following ways:

- Add ECS instances automatically: The image and system disk of the ECS instance are reset by using this method. You can add one or more ECS instances to the cluster at a time.
- Add the ECS instance manually: Manually add the ECS instance by running scripts on the ECS instance. You can only add one ECS instance to the cluster at a time.

Prerequisites

If you have not created a cluster before, create a cluster first.

Instructions

- The ECS instance to be added must be in the same region and use the same network type (Virtual Private Cloud (VPC)) as the cluster.
- When adding an existing ECS instance, make sure that your ECS instance has an Elastic IP (EIP) for the network type VPC, or the corresponding VPC has configured the NAT gateway. In short, make sure the corresponding node can access public network normally. Otherwise, the ECS instance fails to be added.
- The ECS instance to be added must be under the same account as the cluster.
- If you select to manually add the ECS instance, note that:

 If you have already installed Docker on your ECS instance, the ECS instance may fail to be added. We recommend that you uninstall Docker and remove the Docker folders before adding the ECS instance by running the following command:

```
Ubuntu: apt-get remove -y docker-engine , rm -fr /etc/docker/ /var/lib/docker /etc/def
ault/docker
```

CentOS: yum remove -y docker-engine , rm -fr /etc/docker /var/lib/docker

• Container Service nodes have special requirements for the operating system of the ECS instance. We recommend that you use Ubuntu 14.04/16.04 or CentOS 7 as the operating system. We have strictly tested the stability and compatibility of these operating systems.

Procedure

- 1. Log on to the Container Service console.
- 2. Click Swarm > Clusters in the left-side navigation pane.
- 3. Click **More** at the right of the cluster that you want to add ECS instances and then select **Add Existing Instances** from the drop-down list.



4. Add ECS instances.

The ECS instances displayed are filtered and synchronized from your ECS instance list according to the region and network type defined by the cluster.

Add the ECS instances in the following ways:

• Add ECS instances automatically.

(?) Note As this method will reset the image and system disk of the ECS instance, proceed with caution. Create a snapshot to back up your data before adding the ECS instance. For information about how to create a snapshot, see Create a snapshot of a disk.

a. Select the ECS instances you want to add to the cluster and click **Next Step**.

You can add one or more ECS instances at a time.

- b. Configure the instance information. Click **Next Step** and then click **Confirm** in the confirmation dialog box.
- c. Click Finish.
- Manually add the ECS instance by running scripts on the ECS instance.
 - a. Select Manually Add. Select an ECS instance, and then click Next Step.

You can only add one ECS instance at a time.

- b. Confirm the instance information and click **Next Step**.
- c. The scripts unique to this ECS instance are displayed. Click **log on to the ECS instance xxxxxx**.

	Select Existing ECS Instance(s)	>	Enter Instance Information	Added Successfully	
\bigotimes	Token generated. Please log on to the	and execute	the following command:		
	curl -is http://ali				
	3ace8e4678953d192 -				
	Go and execute this command	acaminat			

d. The VNC connection password is displayed in the dialog box. Copy the password and click **Close**.

VNC Con	nection Password	×
	VNC Connection Password:	
	Warning! The VNC connection password is viewable only once. Ensure you record this password and keep it in a secure location for subsequent login attempts.	
	Close	

e. In the dialog box, enter the VNC connection password and click OK.

Enter VNC Password	×
*Please enter VNC password:	
	OK Cancel

f. Enter the logon account (root) and password of the ECS instance, and press Enter to log on to the ECS instance.

Send Remote Command+	Successfully connected to the instance.	Note: A black screen indicates that the system is in sleep mode. Press any key to activate the system.	Input Commands	Modify Management Terminal Password
	Ukanta 16.04.2 LTS [Zhp Instants] Basants: Balcanet to Ukanta 16.04.2 LTS (ORDA-Laux 4. - Bacanetal Laux: https://stanta.com - Baypert: - Baypert: - Baypert: - Baypert: - Baypert: - Baypert: - Come to Allbaba Cloud Elartic Concentra - Capital	ttyl 4.0-02-generic x00_04) con con Ange rvice †		

g. Click **Input Commands**. Paste the preceding scripts into the dialog box, click **OK** and press Enter.

>	py Commands
	Copy and paste content into the text box. Up to 2000 characters are allowed. Non-standard keyboard characters are not supported.
	* Commands Content: curl -Ls http://aliyuncontainerservice.oss-cn- hangzhou.aliyuncs.com/17.03.1-ce/attachNodeScript sudo -H bash -s instance-id i-
C	

The system runs the scripts. Wait until the scripts are successfully run. A success message is displayed. The ECS instance is successfully added.

发送远程命令+	成功连接到实例-bp	提示:如果出现持续展屏。	说明系统处于休眠状态,	按任意键可以激活。	复制命令蜡入:	修改远程连接密码
	The following NED packages will be installed: and the set of the	158 kB) 1 may be dengerous.				
	Ideable for final integer "registrep-internet" angent weights and the integer integers and the integers and the integers weights and the integers and the integers and the integers and the integers weights and the integers and the integers and the integers and the integers weights and the integers and the integers and the integers and the integers weights and the integers and the integers and the integers and the integers weights and the integers and the integers and the integers and the integers weights and the integers and the	9–30ba363' locally nmel-agent:0.9–30ba36 t nay be dangerous. ad' locally ent:0.9–979afad				

Related operation

You can modify the VNC connection password of the ECS instance in the remote terminal connection page. Click **Modify Management Terminal Password**, enter the new password and click **OK** in the dialog box.

Modify Managemer	nt Terminal Password	×
Note: The modified V console.	NC password will not take effect until the instance is restarted at the	
*Please enter a new		
password:	Password character limit is 6 characters. Only uppercase letters, lowercase letters, and numbers are supported.	
*Confirm the new password:	•••••	
	ОК Салсе	el

3.6. Manage cross-zone nodes

To enhance the high availability of applications, you can distribute multiple nodes in different zones when creating a cluster.

You can create a cluster with one node or a zero-node cluster. Then, add nodes of different zones by expanding the cluster or adding existing Elastic Compute Service (ECS) instances.

? Note

- Nodes added by expanding the cluster are Pay-As-You-Go ECS instances.
- Nodes added by adding existing ECS instances can be Pay-As-You-Go ECS instances or monthly/yearly subscription ECS instances.

Add nodes of different zones by expanding the cluster

Procedure

- 1. Log on to the Container Service console.
- 2. Click Swarm > Clusters in the left-side navigation pane.
- 3. ClickMore at the right of the cluster that you want to expand and then select > Expand . As shown in the following figure.

Container Service	Cluster List			You can	create up to	5 clusters a	nd can add uj	to 40 nodes in each cl	uster. Refr	resh Create C	Cluster 👻
Overview	Hep: & Create cluster & How to add	existing ECS in:	stances 🔗 Cross-	zone node management 🔗	Log Service in	ntegration	🖉 Connect b	o cluster through Docker	Client		
Applications	Name *										
Services	Cluster Name/ID	Cluster Type	Region (All) +	Network Type	Cluster Status	Node Status 🕐	Number of Nodes	Time Created	Docker Version		Action
Nodes Networks	test c36634da0194645454c0t3c0d6c3ba404408	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc- boll w Köndingell 1 fm Constraint	Running	Healthy C	2	05/19/2018,20:33:11	17.06.2- ce	Manage 3	v Logs Delete or More
Data Volumes										Upgrade Agent Upgrade Docke	e ar
Configurations ···· • Images and Tem									•	Upgrade Syster	m Service
Docker Images										Add Existing In	nstances
Solutions										Create Applicat	ion

4. The Expand page appears. Configure the specifications of the new nodes.

You can create nodes of different zones by setting Zone.

	Cluster Name:	test
Cluster	Region:	China East 1 (Hangzhou)
	Zone:	East China 1 Zone G 🛛 🝷

- 5. Click **Expand** to add the new nodes to the cluster.
- 6. Repeat the preceding steps to create and add nodes of different zones to the cluster.

Add nodes of different zones by adding existing ECS instances

Prerequisites

To add nodes by using this method, purchase ECS instances from the ECS purchase page first, and select different zones for them during the purchase.

Procedure

- 1. Log on to the Container Service console.
- 2. Click Swarm > Clusters in the left-side navigation pane.
- 3. ClickMore at the right of the cluster that you want to add existing ECS instances and then select > Add Existing Instances . As shown in the following figure.

Container Service	Cluster List			You can	create up to	5 clusters a	nd can add u	o to 40 nodes in each cl	uster. Refi	resh Create Cluster -
Overview	Help: & Create cluster & How to add	existing ECS ins	stances 🔗 Cross-	zone node management 🔗	Log Service in	ntegration	🖉 Connect t	o cluster through Docker	Client	
Applications	Name *									
Services	Cluster Name/ID	Cluster Time	Pogion (All) -	Network Time	Cluster	Node Status 🙆	Number of	Time Created	Docker	â ction
Clusters 2	Cluster Warney 10	cluster type	Kegion (All) *	Network Type	Sulus	saus 🕡	noues	Time created	Version	Action
Nodes	test c35634dx8944c494c83cdbx484488	Alibaba Cloud Cluster	China East 1 (Hangzhou)	vpc-	Running	Healthy	2	05/19/2018,20:33:11	17.06.2- ce	Manage View Logs Delete
Networks				COLUMPS REPORT OF CONCERN						Upgrade Agent
Data Volumes										Upgrade Docker 3
Configurations =										Upgrade System Service
 Images and Tem 										Expand
Docker Images									4	Add Existing Instances
Orchestration T										Create Application
Solutions										

4. Select ECS instances of different zones and add them manually or automatically to the cluster.

For more information, see Add an existing ECS instance.

Sele	ct Existing ECS Instance(s)	Ente	er Instance Information	>	Added Successfully
Adding Method:					
Automatically Add Add	Manually Add				
Adding an existing ECS in:	stance to the Container Service will change t	the instance system disk. The di	isk ID will change and the prev	vious system disk will be relea	sed.
Note: 1. Your previous system the disk list and click "M 2. To retain enough sna 3. Back up data before p	I disk's user snapshots will be retained. Auto lodify Attributes" to view and modify attribut pshot quota for the periodic automatic snap performing this operation to avoid data loss.	matic snapshots will be retained e values. shot policy, you can delete unwa	d or deleted according to the s anted user and automatic snaj	etting of the "Delete automati pshots.	c snapshots when releasing disk" option. You can go to
Select Existing ECS Insta	ance(s):				
Instance ID	ter the instance ID for exact search.	Search			
Instance ID	Instance Name	IP Address	Zone	Network Type	Instance Type

5. Repeat the preceding steps to add ECS instances of different zones to the cluster.

3.7. Bind and unbind a Server Load Balancer instance

You can automatically create a Pay-As-You-Go Server Load Balancer instance when creating a cluster, or bind a monthly/yearly subscription or Pay-As-You-Go Server Load Balancer instance to a cluster after creating the cluster.

Container Service supports binding an Internet Server Load Balancer instance, a VPC Server Load Balancer instance, or an intranet Server Load Balancer instance in a classic network to a cluster.

Limits

- You can only bind a Server Load Balancer instance to a cluster of the same region.
- You can only bind a Server Load Balancer instance to a cluster created by the same account.
- A VPC cluster can bind an Internet Server Load Balancer instance or a VPC Server Load Balancer instance.
- One cluster can only bind one Server Load Balancer instance.
- Two clusters cannot share one Server Load Balancer instance.

Prerequisites

You have created a Server Load Balancer instance in the Server Load Balancer console and configured the TCP 9080 port for the instance to listen to backend servers.

Bind a Server Load Balancer instance

- 1. Log on to the Container Service console.
- 2. Click **Manage** at the right of the cluster that you want to bind a Server Load Balancer instance. The cluster details page appears.



3. Click Load Balancer Settings in the left-side navigation pane > and then click Bind Server Load Balancer.

<	Custerswarmmode-cluster	Refresh
Basic Information		
Load Balancer Setti	Server Load Balancer Settings Set Domain Name	
User Tags	No Server Load Balancer is bound to your cluster.	
Image List	Bind Server Load Balancer	
Container List	2	
Events	_	
Node Scaling		
Secrets		

4. Select the Server Load Balancer instance that you want to bind to the cluster from the Server Load Balancer ID list and click **OK**.

? Note If the selected Server Load Balancer instance has been bound to a backend server, the system will prompt you that "This Server Load Balancer instance is already bound to a backend server". You need to select another Server Load Balancer instance that has not been bound to any backend server.

Rebind a Server Load Balancer instance

You can change the Server Load Balancer instance bound to your cluster per your needs.

- 1. Log on to the Container Service console.
- 2. Click Clusters in the left-side navigation pane.
- 3. Click **Manage** at the right of the cluster that you want to re-bind a Server Load Balancer instance. The cluster details page appears.

Container Service	Cluster List			You car	n create up to 5	clusters and can	add up to 20 nodes i	n each cluster. Sub	account Authorization	Refre	hCreat	Cluster
Overview	Help: Ø Create cluster Ø How to ad	d existing ECS Instances	& Cross-zone node man	agement 🔗 Log Service integr	ration 🔗 Conn	ect to cluster thro	ugh Docker Client					
Applications	Name 🔻											
Services	Cluster Name/ID	Cluster Type	Region	Network Type	Cluster Status	Node Status 📀	Number of Nodes	Time Created	Docker Version			Action
Clusters Nodes	swarmmode-cluster c9b0ccb95e9cd4134babe12fd04c8a1ba swarm mode	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc-bp15p1sjmx3fg7p5u7edy	Running	Healthy C	2	2017-09-16 14:27:5	5 17.06.1-ce	Manage	View Logs Monitor	Delete More -
Networks Data Volumes	swarmcluster cfe91179222fa486a8b8fcced671676a6	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc-bp15p1sjmx3fg7p5u7edy	Running	Healthy C	2	2017-09-16 14:27:1	5 17.06.1-ce	Manage	View Logs Monitor	Delete More
Configurations									2			
Images and Templ												
Operation Logs												
Getting Started												

4. Click Load Balancer Settings in the left-side navigation pane, > and click Re-bind Server Load Balancer.



5. Select the Server Load Balancer instance that you want to bind to the cluster from the Server Load Balancer ID list and click **OK**.

Unbind a Server Load Balancer instance

You can unbind a Server Load Balancer instance in the Container Service console if the instance is not required.

- 1. Log on to the Container Service console.
- 2. Click Clusters in the left-side navigation pane.
- 3. Click **Manage** at the right of the cluster that you want to unbind a Server Load Balancer instance. The cluster details page appears.

Container Service	Cluster List			You car	reate up to 5	clusters and can a	add up to 20 nodes i	n each cluster. Sub	account Authorization	Refres	Create	Cluster
Overview	Help: Ø Create cluster Ø How to add	existing ECS instances	& Cross-zone node mana	agement 🔗 Log Service integr	ation 🔗 Conn	act to cluster thro	ugh Docker Client					
Applications	Name 🔻											
Services	Cluster Name/ID	Cluster Type	Region	Network Type	Cluster Status	Node Status 🔞	Number of Nodes	Time Created	Docker Version			Action
Clusters Nodes	swarmmode-cluster c9b0ccb95e9cd4134babe12fd04c8a1ba swarm mode	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc-bp15p1sjmx3fg7p5u7edy	Running	Healthy C	2	2017-09-16 14:27:50	5 17.06.1-ce	Manage	View Logs Monitor	Delete More -
Networks Data Volumes	swarmcluster cfe91179222fa486a8b8fcced671676a6	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc-bp15p1sjmx3fg7p5u7edy	Running	Healthy C	2	2017-09-16 14:27:1	5 17.06.1-ce	Manage	View Logs Monitor	Delete More •
Configurations									2			
 Images and Templ 												
Operation Logs												
Getting Started												

4. Click Load Balancer Settings in the left-side navigation pane, > and click Unbind Server Load Balancer.

<	Ouster swarmmode-duster	Refresh
Basic Information		
Load Balancer Setti	Server Load dalancer settings Set Lomain Name	
User Tags	Server Load Balancer ID: Ib-lud	
Image List		
Container List	Re-bind Server Load Balancer Unbind Server Load Balancer	
Events	2	
Node Scaling		
Secrets		

3.8. Set the root domain name of a cluster

Context

When you Create an Nginx webserver from an image and configure the web routing rules, you are only required to enter the domain name prefix nginx. Then, you can obtain the domain name in the format of \$cluster_id.\$region_id.alicontainer.com. You can replace this domain name by setting a root domain name (51111.com is used in this example) of the cluster. When you redeploy the application nginx , the domain name changes from nginx.cd5b226071936493b89e75bbe8841664c.cn-hangzhou.alicontainer.com to nginx.51111.com , which makes it convenient for you to access the cluster applications with your own root domain name.

Note To guarantee the normal operation of the following example, upgrade the Agent to the latest version first.

Procedure

- 1. Bind a Server Load Balancer instance.
 - i. Log on to the Container Service console.
 - ii. Log on to the Container Service console.
 - iii. Click **Clusters** in the left-side navigation pane.
iv. Click Manage at the right of the cluster (routing-test-online in this example) that you want to configure.

Container Service	Cluster list				You	can create up to 100 c	lusters and may add up to 2000 n	odes in each cluster	Subaccount authorization	Refresh	Create	e cluster
Overview												
Applications	Helper: Create cluster How to add existing ECS ins	tances Multiple zones node manage	ement Log service integ	ration Connect to	duster through Docker o	lient						
Services	Name											
Clusters 1	Name/ID	Region	Network type	Status	Node status 🔞	No. of nodes	Time Created	Docker version				Action
Nodes	routing-test-online ccc8ab7a5bb48445682ae20c74dbb0363	China North 2(Beljing)	Classic network	Ready	Healthy C	1	2016-10-14 15:43:01	1.11.2.1	2	Manage	Logs Monitor	Delete More •
 Images and Templates 	11013hz caf9b682bdc4241449c3d02193a0f419f	China East 1(Hangzhou)	Classic network	Faled®	No node status	2	2016-10-13 17:14:58	1.11.2.1		Manage	Logs Monitor	Delete More +
Docker Images Application templates	i10136j cx5a4e674a60e4247a459681c55189b5e	China North 2(Beljing)	Classic network	Faled®	No node status	2	2016-10-13 14:44:26	1.11.2.1		Manage	Logs Monitor	Delete More +
Get Started												

v. Click Load Balancer Settings in the left-side navigation pane.

If no Server Load Balancer instance is bound to this cluster, log on to the Server Load Balancer console and create a Server Load Balancer instance. Then, return to this page and bind the instance to this cluster.

? Note For more information about how to bind and unbind a Server Load Balancer instance to and from a cluster and the limits in Container Service, see Bind and unbind a Server Load Balancer instance.

<	Cluster:test
Basic Information	
Load Balancer Se	Server Load Balancer Settings Set Domain Name
User Tags	Server Load Balancer ID: Ib-Latition to immun
Image List	
Container List	Re-bind Server Load Balancer Unbind Server Load Balancer
Events	
Node Scaling	

- 2. Set the domain name.
 - i. Click the Set Domain Name tab and enter the root domain name you bought in the Domain Name field. In this example, 51 ili.com is entered.

Server Load Balancer Settings	Set Domain Name
Domain Name:	51ili.com
	Set Cancel

- ii. Click Set .
- 3. Resolve the domain name to the bound Server Load Balancer instance.
 - i. Log on to the Server Load Balancer console. Click Instances in the left-side navigation pane, and then click the ID of the Server Load Balancer instance bound to the cluster routing-testonline.

ii. View the instance details. Find the instance IP address.

acs-slb-c9b105e434 tReturn to Server Load Balancer List	Restrictions and Notes
Basic Information	^
Server Load Balancer ID: Balancer and Balancer ID: Balanc	Status: Status
Server Load Balancer Name: 201-00-000-000-000-000-000-000-000-000-0	Region: China East 1 (Hangzhou)
Instance IP Type: Public IP	Zone: cn-hangzhou-f(Master)/cn-hangzhou-e(Slave)
Network Type: Classic Network	
Billing Information	Billing Details Release
Billing Method: Pay by Traffic	Created At: 2017-11-27 09:15:59
Instance IP Address: 47.47.41.157(Public IP)	Automatic Release Time: -

- iii. Log on to the Alibaba Cloud DNS console and add record A to resolve *.51ili.com to the Server Load Balancer VIP address.
- 4. Redeploy the nginx application.
 - i. Click Redeploy at the right of nginx. The service access endpoint of the application nginx is changed.

The access endpoint before setting the root domain name.

The access endpoint after setting the root domain name.

ii. Access the latest access endpoint http://nginx.51ili.com.

3.9. Download cluster certificate

Context

With the downloaded certificate, you can connect to the endpoint exposed from the cluster by using Docker Swarm API or Docker client. For more information, see Connect to a cluster by using Docker tools.

- 1. Obtain the access address.
 - i. Log on to the Container Service console.
 - ii. Log on to the Container Service console.
 - iii. Click **Clusters** in the left-side navigation pane. On the Cluster List page, click **Manage** at the right of a cluster.

Container Service	L Cluster List			Yo	u can create	up to 5 cluste	rs and can add	up to 10 nodes in each o	luster. Refr	esh Crea	te Cluster 🚽
Overview	Help: & Create cluster & How to add	existing ECS instar	ices 🔗 Cross-zone i	node management 🔗 Log	Service integr	ration 🔗 Cor	nnect to cluster	through Docker Client			
Applications	Name 🔻										
Services	Cluster Name/ID	Cluster Type	Region (All) -	Network Type	Cluster Status	Node Status 🕜	Number of Nodes	Time Created	Docker Version	3	Action
Nodes Networks	test-swarm cx13aLac205erC4880408013aBbc8204e	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc- bol kil?v=kontigenueved	Running	Healthy C	1	05/21/2018,10:29:11	17.06.2- ce	Manage Mo	View Logs Delete nitor More +

iv. The cluster details page is displayed, showing the cluster connection information.

	Connection Information
To	access and manage clusters, certificates granted by Albaba Cloud are required. Each cluster has its own certificate. If you have not yet downloaded the certificate for the current cluster, click Download Certificate Revoke Downloaded Certificate
Cl	ister Access Point:
	tcp://master4g5.cs-cn-hangzhou.aliyun.com:21003
Us	er Guide:
	Configure Environment Variable (Linux or Mac):
	export DOCKER_TLS_VERIFY='1" export DOCKER_HOST="tcp://master4g5.cs-cn-hangzhou.aliyun.com:21003" #Set the current path as the storage path for the cluster certificate file. export DOCKER_CERT_PATH="\$PHD"
No	tice:
	1. The certificate allows secure access to the container cluster. Please keep it secure. Each cluster certificate is unique. You must configure the correct certificate in order to use Docker Clent or Docker Compose to access the cluster.
	2. If your downloaded certificate is accidentally leaked, you can revoke it and download a new one.

2. Download and save the TLS certificate.

Configure a TLS certificate before you use the preceding access address to access the Docker cluster.

Click **Download Certificate** in the cluster details page to download the TLS certificate. The certFiles.zip file is downloaded. certificate. The certFiles.zip file is downloaded. In the following example, the downloaded certificate is saved to the *~/.acs/certs/ClusterName/* directory. ClusterName indicates the name of your cluster. You can save the certificate to a different directory, but we recommend using the *~/.acs/certs/ClusterName/* directory for easy management.

```
mkdir ~/.acs/certs/ClusterName/ #Replace ClusterName with your cluster name
cd ~/.acs/certs/ClusterName/
cp /path/to/certFiles.zip .
unzip certFiles.zip
```

The certFiles.zip file contains ca.pem, cert.pem, and key.pem.

3.10. Expand a cluster

Prerequisites

A cluster can contain up to 20 nodes.

Context

You can expand your cluster according to your business needs.

Note Elastic Compute Service (ECS) instances added by expanding the cluster are Pay-As-You-Go instances.

- 1. Log on to the Container Service console.
- 2. Click **Clusters** in the left-side navigation pane.
- 3. On the Cluster List page, click **More** at the right of the cluster that you want to expand and then select **Expand** from the list.

Container Service	Cluster List		Y	'ou can create up to 5 clusters	and can ad	ld up to 20 no	des in each clust	er. Subaccount	Authorization	Refresh	Create Cluster
Overview Applications Services	Help: Create cluster How to add ext	sting ECS instance	s Cross-zone node r	nanagement Log Service int	egration (Connect to clus	ter through Do	ker Client			
Clusters	Cluster Name/ID	Cluster Type	Region	Network Type	Cluster Status	Node Status 🔞	Number of Nodes	Time Created	Docker Version		Action
Data Volumes	routing-test-online ccf530ee2b1c1400e96425b05846fa35c	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc- bp1659u1p811058ea3npd	Ready	Healthy 🕽	1	2017-03-31 22:32:40	17.03.1-ce	Manage	2 Delete More-
Images and Temp Operation Logs									Update F Upgrade	AM Authorizat	tion Information
Getting Started									Upgrade Upgrade	Docker System Servic	e
									Add Exist Create A	ting Instances pplication	

4. In the displayed dialog box, configure the specifications of the new node.

You can select the number and the specifications of the ECS instances you are about to add to the cluster.

5. Click Expand.

3.11. Migrate a cluster

For a Swarm cluster created earlier, you can guarantee the performance and stability of the cluster by migrating the cluster.

Context

- The latest time for migrating a cluster is displayed through SMS, station message, or email. Complete the Swarm cluster migration before the latest time. The system automatically migrates the cluster if you do not migrate the cluster before the latest time.
- Cluster migration rebuilds connections from cluster nodes to the container server without affecting applications deployed in the cluster, nor adding or modifying any data. Make sure that you perform this operation during the low peak period of your business because unpredictable risks might still exist throughout the migration process.

Procedure

- 1. Log on to the Container Service console.
- 2. Under the Swarm menu, click Clusters.
- 3. Click **Cluster Migration** in the action column at the right of the cluster to be migrated.

 Alibaba Cloud Cluster	US Western 1 (Silicon Valley)	VPC	Running	Healthy 🕽	2	08/21/2018,21:46:39	17.06.2- ce	Manage View Logs Delete Monitor Cluster Migration More -
Alibaba Cloud Cluster	US Western 1 (Silicon Valley)	VPC	Running	Healthy 🕽	2	08/21/2018,21:46:32	17.06.2- ce	Manage View Logs Delete Monitor More →

4. Click OK in the Prompt dialog box.

? Note During cluster migration:

- Information query, deployment, upgrade, and other operations cannot be performed in the console.
- The cluster cannot be connected to through the cluster access point API.
- The data and application status in the cluster remain unchanged. Applications deployed on the cluster are still accessible.
- The migration process takes about three minutes.

On the Cluster List page, Migrating is displayed in the Cluster Status column.

	Alibaba Cloud Cluster	US Western 1 (Silicon Valley)	VPC	Higrating	Healthy	2	08/21/2018,21:46:47	17.06.2- ce	Manage View Logs Delete Monitor More ▼
and the production of the	Alibaba Cloud Cluster	US Western 1 (Silicon Valley)	VPC	Running	Healthy 🕽	2	08/21/2018,21:46:39	17.06.2- ce	Manage View Logs Delete Monitor More ▼

Result

After cluster migration is completed, on the **Cluster List** page, **Running** is displayed in the **Cluster Status** column.

? Note

- The cluster ID, access point address, and other attributes remain unchanged.
- Please be sure to confirm that your business is running properly.
- During the migration process, if you have any questions, please open a ticket in which you include the cluster ID and state whether your deployed applications are normal.

-	Alibaba Cloud Cluster	US Western 1 (Silicon Valley)	VPC	Running	Healthy 🕽	2	08/21/2018,21:46:47	17.06.2- ce	Manage View Logs Delete Monitor More▼
1000 00 00 00 da	Alibaba Cloud Cluster	US Western 1 (Silicon Valley)	VPC	Running	Healthy 🕽	2	08/21/2018,21:46:39	17.06.2- ce	Manage View Logs Delete Monitor More ▼

3.12. Search for a cluster

- 1. Log on to the Container Service console.
- 2. Click Swarm > Clusters in the left-side navigation pane.
- 3. Enter the cluster name or keywords of the cluster name in the search box. Clusters with the keywords in their names are displayed. As shown in the following figure.



Cluster List		Y	ou can create up to 5 clusters	er. Subaccount A	Authorization	Refresh	Create Cluster			
Help: Create cluster How to add ex	isting ECS instance	s Cross-zone node m	nanagement Log Service int	egration C	onnect to clus	ter through Dock	ker Client			
Name ROUT]									
Cluster Name/ID	Cluster Type	Region	Network Type	Cluster Status	Node Status 🕜	Number of Nodes	Time Created	Docker Version		Action
routing-test-online ccf530ee2b1c1400e96425b05846fa35c	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc- bp1659u1p811058ea3npd	Ready	Healthy 🕽	1	2017-03-31 22:32:40	17.03.1-ce	Manage	View Logs Delete Monitor More+

3.13. Delete a cluster

Context

You can delete clusters from Container Service. Deleting the cluster also deletes its associated Elastic Compute Service (ECS) instances, Server Load Balancer instance, and other cloud resources, so proceed with caution.

Procedure

- 1. Log on to the Container Service console.
- 2. Click Swarm > Clusters in the left-side navigation pane.
- 3. Click **Delete** at the right of the cluster you are about to delete.

Container Service	Cluster List		Y	ou can create up to 5 clusters	and can ad	d up to 20 noc	les in each cluste	r- Subaccount A	uthorization	Refresh	Create Cluster
Overview Applications	Help: Create cluster How to add exit	sting ECS instances	Cross-zone node m	nanagement Log Service int	egration C	onnect to clus	ter through Dock	er Client			
Services	Name 💌]									
Clusters	Cluster Name/ID	Cluster Type	Region	Network Type	Cluster Status	Node Status 🕜	Number of Nodes	Time Created	Docker Version		Action
Nodes Data Volumes Configurations	routing-test-online ccf530ee2b1c1400e96425b05846fa35c	Albaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc- bp1659u1p811058ea3npd	Ready	Healthy 🕽	1	2017-03-31 22:32:40	17.03.1-ce	Manage	Logs Delete Monitor More+
 Images and Temp Operation Logs Ξ 											
Cotting Started											

4. In the displayed window, select whether or not to keep the Server Load Balancer instance and click OK.

3.14. Clean up a cluster disk

Context

Cleaning up disk clears the dirty data on each server in your cluster. Dirty data is limited to:

- Docker images downloaded locally but not used.
- Volume directory once attached to a container but not cleaned up after the destruction of the container.

- 1. Log on to the Container Service console.
- 2. Click Clusters in the left-side navigation pane.
- 3. On the Cluster List page, click **Manage** at the right of the cluster that you want to clean up the disk.

1	Container Service	Cluster List		Y	You can create up to 5 clusters and can add up to 20 nodes in each cluster.					Subaccount Authorization Refresh		
	Overview											
	Applications	Help: Create cluster How to add exi	sting ECS instances	Cross-zone node n	nanagement Log Service int	egration (Connect to clus	ter through Dock	er Client			
	Services	Name 💌]									
	Clusters 1	Cluster Name/ID	Cluster Type	Region	Network Type	Cluster Status	Node Status 🕜	Number of Nodes	Time Created	Docker Version		Action
	Nodes Data Volumes Configurations	routing-test-online ccf530ee2b1c1400e96425b05846fa35c	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc- bp1659u1p811058ea3npd	Ready	Healthy 🕽	1	2017-03-31 22:32:40	17.03.1-ce	Manage	View Logs Delete Monitor More+
•	Images and Temp											
	Operation Logs											
	Getting Started											

4. Click Clear Disk on the cluster details page.

Basic Information				Upgrade Agent	Upgrade System Service	Clear Disk
Cluster ID: ccf	VPC	Running	Region: China East 1 (Hangzhou)	Number of I	Nodes 1 Expand Add Existi	ng Instances
Security Group ID: sg-bp						

3.15. Log on to image repository

Prerequisites

- Prepare an available image repository. Use the Docker Hub official service in this example, which requires you to register a Docker ID and build an available repository in it.
- Configure the independent logon password for the repository. In this example, log on to the Container Registry console to configure or modify the repository logon password. Note that you are configuring the password when you modify the repository logon password for the first time.

Context

You can log on to the image repository in a cluster to provide the related cluster logon information, which facilitates you to manage clusters by using cluster management tools.

Procedure

- 1. Log on to the Container Service console.
- 2. Click Clusters in the left-side navigation pane.
- 3. Click Manage at the right of the cluster you want to configure.

Container Service	Cluster List				You can crea	ite up to 5 clu	sters and can a	dd up to 20 nodes in	n each cluster.	Refresh Create Cluster
Overview	Help: & Create cluster & How to add	existing ECS instar	nces 🔗 Cross-zone n	ode management 🔗 Log S	ervice integra	ation 🔗 Conr	nect to cluster t	nrough Docker Clier	it	
Services	Cluster Name/ID	Cluster Type	Region	Network Type	Cluster Status	Node Status ⊘	Number of Nodes	Time Created	Docker Version	Action
Nodes Networks	swarmmode-test	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc- bpdreijut Ligaal-Repert 754	Running	Healthy 🕽	1	2018-01-11 17:14:16	17.06.2-ce	Manage View Logs Delete Monitor More-
Data Volumes Configurations	test -060305984/35473655-4408356042732	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc- hptwgicttgaeHenwm7bi	Running	Healthy $oldsymbol{2}$	2	2018-01-10 09:28:17	17.06.2-ce	Manage View Logs Delete Monitor More +

4. Click Log on to Hub.

Cluster:test				Enable Log Service	Log on to Hub	Refresh
Basic Information			Upgrad	e Agent Upgrade	System Service	Clear Disk
Cluster ID: c3d0305804c50-071d05c44052d0042f12	VPC	Running	Region: China East 1 (Hangzhou)	Number of Nodes	s 2 Expand Add Existing	g Instances
Security Group ID: ag-bot Jerigner-glids fund Check Security	Group Rebind					

5. Configure the parameters in the displayed dialog box.

Log on to Hub			×
Repository Domain Name	registry.cn-hangzhou.aliyuncs.com		
Username* :	Querent Opper.		
Password* :	•••••		
	The user's account password will be encrypted		
Email :			
		ОК	Cancel

- Repository Domain Name: Enter the hub domain name of the image repository. Take the image address registry.cn-hangzhou.aliyuncs.com/acs/agent:0.8 as an example. The repository domain name is registry.cn-hangzhou.aliyuncs.com
- Username: Enter the username of the image repository. In this example, enter the Docker ID registered in Docker Hub.
- Password: Enter the independent logon password of the image repository. In this example, enter the logon password set when you registered in Docker Hub. Registry's login password is set and modified on the container mirroring Service's console.
- Email: Enter the email set when you registered the image repository. In this example, enter the email set when you registered in Docker Hub.
- 6. Click OK. You have successfully logged on to the image repository if no error message appears.

3.16. Upgrade Agent

Context

(?) Note Your applications are not affected during the upgrade, but you can neither manage the cluster by using the Web interface, nor use Docker client to connect to the cluster access port for about 2 minutes.

The Agent of Container Service, which is installed on each server in the cluster, receives commands issued by the Container Service control system.

New functions are regularly added to Container Service. If you need the latest functions, upgrade the Agent of the cluster.

- 1. Log on to the Container Service console.
- 2. Click Clusters in the left-side navigation pane.
- 3. On the Cluster List page, click More at the right of the cluster that you want to upgrade the Agent > and then select Upgrade Agent from the list .

Container Service

Container Service	Cluster List		Ye	ou can create up to 5 clusters	and can add	d up to 20 nod	es in each cluster	Subaccount A	uthorization	Refresh	Create Cluster
Overview Applications	Help: Create cluster How to add exit	sting ECS instances	Cross-zone node	management Log Service in	tegration	Connect to clu	ster through Doc	ker Client			
Services	Name 💌										
Clusters	Cluster Name/ID	Cluster Type	Region	Network Type	Cluster Status	Node Status ⊘	Number of Nodes	Time Created	Docker Version		Action
Data Volumes	routing-test-online ccf530ee2b1c1400e96425b05846fa35c	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc- bp1659u1p811058ea3npd	Ready	Healthy 🕄	1	2000-01-01 08:00:00	17.03.1-ce	Manage	Anne More -
 Images and Temp Operation Logs Ξ 								3	Update R Upgrade / Upgrade I	AM Authorizat Agent Docker	tion Information
Getting Started									Upgrade S Expand	System Servic	e
									Add Existi	ng Instances	
									Create Ap	plication	

4. Click **OK** in the displayed dialog box.

3.17. Upgrade Docker daemon

Context

Standard Docker daemon is installed on each server in the cluster to manage containers.

- ? Note
 - The cluster Docker daemon upgrade requires that the machine is able to access the Internet to download necessary software packages.
 - The cluster Docker daemon upgrade may fail. To guarantee your data security, we recommend that you back up snapshots before upgrading Docker daemon.
 - During the cluster Docker daemon upgrade, the services deployed on the cluster are interrupted and you cannot perform operations on the cluster and applications. Make appropriate arrangements before the upgrade. The upgrade lasts 3–30 minutes. The cluster status changes to Running after the upgrade.

You can view the Docker version of the cluster on the Cluster List page.

Container Service	Cluster List			Ye	ou can create	up to 5 cluste	rs and can add	up to 10 nodes in each	cluster. Re	efresh Create Cluster -
Kubernetes Swarm										
Overview	Help: & Create cluster & How to add	existing ECS instar	nces 🔗 Cross-zone i	node management 🔗 Log	Service integ	ration 8 Co	nnect to cluster	through Docker Client		
Applications	Name 🔻									
Services	Charles Marsa (75)	Charles Trees	Desire (AID	Natural Taxa	Cluster	Node	Number of	Two Guebal	Docker	A stress
Clusters	Cluster Name/ID	Cluster Type	Region (All) +	Network Type	Status	Status 🔮	NODES	Time Created	version	Action
Nodes Networks	test-swarm control or forbert (Hand H) are control to the	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC MIC- bot kathyr Hannigan urydd	Running	Healthy \mathfrak{C}	1	05/21/2018,10:29:11	17.06.2- ce	Manage View Logs Delete Monitor More -

- 1. Log on to the Container Service console.
- 2. Under Swarm, click Clusters in the left-side navigation pane.
- 3. On the Cluster List page, click **Upgrade** in the Docker Version column, or click**More > Upgrade Docker** at the right of the cluster.

Container Service	Cluster List		u can create up to 5 clusters	rs and can add up to 20 nodes in each cluster. Subaccour				uthorization	Refresh	Create Cluster	
Overview Applications Services	Help: Create cluster How to add existing ECS instances Cross-zone node management Log Service integration Connect to cluster through Docker Client Name 💌										
Clusters	Cluster Name/ID	Cluster Type	Region	Network Type	Cluster Status	Node Status 🞯	Number of Nodes	Time Created	Docker Version		Action
Nodes Data Volumes	routing-test-online ccf530ee2b1c1400e96425b05846fa35c	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc- bp1659u1p811058ea3npd	Ready	Healthy 🕽	1	2000-01-01 08:00:00	17.03.1-ce	Manage	Momeor More-
Images and Temp Operation Logs Ξ								3	Update R Upgrade	AM Authorizat Agent Docker	ion Information
Getting Started									Upgrade Expand	System Servic	e
									Add Exist Create Ap	ing Instances oplication	

- 4. On the Upgrade Docker page, click **Upgrade Agent** to upgrade the Agent first if your Agent is not in the latest version.
- 5. If your Agent is in the latest version, upgrade Docker daemon

in the following ways:

• Upgrade Directly

Click Upgrade Directly to enter the Docker Engine upgrade process.

• Back up Snapshot before Upgrade

We recommend that you back up the snapshots before upgrading Docker daemon. In this way, you can recover Docker daemon by using the snapshots if an error occurs during the upgrade process.

Click **Back up Snapshot before Upgrade**, and then the system calls the Elastic Compute Service (ECS) API to take snapshots of the cluster nodes.

Backing up snapshots may take some time. Wait until the snapshots are backed up, and then the system automatically enters the Docker Engine upgrade process.

If the snapshots failed to be backed up, you can click **Continue** or **Quit**. Click **Continue** to enter the Docker Engine upgrade process, or click **Quit** to give up the upgrade.

What's next

Return to the **Cluster List** page and you can see that the cluster you upgraded the Docker daemon is in the Docker-Engine is upgrading status. This may take a while as container data will be backed up during the upgrade of the Docker Engine.

3.18. Upgrade system services

Context

The system services of a cluster, including Log Service acslogging , Simple Routing Service acsrouting , Monitor Service acsmonitoring, and Volume Service acsvolumedriver , are used to deal with general services necessary for applications. This document introduces how to upgrade these system services.

Note During the upgrade of the cluster system services, your applications or services may be temporarily inaccessible or abnormal, so proceed with caution. We recommend that you upgrade the system services when the access traffic is low or at the maintenance time.

Procedure

- 1. Log on to the Container Service console.
- 2. Under Swarm, click **Clusters** in the left-side navigation pane.
- 3. On the Cluster List page, click **More** at the right of the cluster whose system services you want to upgrade and then select **Upgrade System Service** from the drop-down list. As shown in the following figure.

Container Service	Cluster List	Cluster List You can create up to 5 clusters and can add up to 20 nodes in each cluster. Subaccount										Create Cluster
Overview												
Applications	Help: Create cluster How to add ex	isting ECS instan	ces Cross-zone n	ode management Log Servi	ce integratio	on Connect	to cluster thro	ugh Docker Clier	nt			
Services	Name 💌											
Clusters	Cluster Name/ID	Cluster Type	Region	Network Type	Cluster Status	Node Status 🕜	Number of Nodes	Time Created	Do Ve	cker		Action
Nodes	VPC										Manage	Logs
Data Volumes	routing-test-online ccf530ee2b1c1400e96425b05846fa35c	Alibaba Cloud Cluster	China East 1 (Hangzhou)	vpc- bp1659u1p811058ea3npd	Ready	Healthy 🕽	1	2000-01-01 08:00:00	17 ce	.03.1-	-	2 Delete Monitor More -
Configurations										Update R	AM Authorizat	ion Information
Images and Templates										Upgrade	Agent	
Operation Logs										Upgrade	Docker	_
Getting Started									3	Upgrade	System Servic	e
										Expand		
										Add Exist	ing Instances	
										Create A	pplication	

4. The Upgrade System Service dialog box opens. Select the system services you want to upgrade and click **Upgrade**.

For example, select **Simple Routing Service** (corresponding to acsrouting; note that the upgrade will temporarily affect your access to applications) and **Volume Service** (corresponding to acsvolumedriver; note that the upgrade might temporarily affect the functions of your associated applications).

Click **Applications** in the left-side navigation pane and select the cluster from the Cluster dropdown list. You can see the system services are being upgraded.

After the upgrade, the affected services and applications resume normal functioning.

4.Nodes 4.1. Remove a node

Context

You can remove nodes from a cluster. Deleting a node removes the machine from the cluster. The machine information of the removed node cannot be viewed in the node list.

? Note

- Back up the data before removing a node.
- Deleting the node only removes the Elastic Compute Service (ECS) instance from the cluster. The ECS instance is not released. To release the ECS instance, go to the ECS console and manually release the instance.

Procedure

- 1. Log on to the Container Service console.
- 2. Click Nodes in the left-side navigation pane.
- 3. Select the cluster where the node you want to remove resides from the Cluster list.
- 4. Click Moreat the right of the node you want to remove and then > select Remove from the list .

Container	Service	Node List									F	efresh
Kubernetes	Swarm											
Overview		Help: 🖉 Postpay instanc	te to Prepay									
Application	5	Cluster: swarm-test •	2									
Services		IP Address	Instance Type	Instance ID/Name	Status	Number of Containers	Configuration	Operating System	Docker Version	Agent		3
Clusters			Alibaba Cloud Node	2012	Normal	16	CPU:2core(s) Memory:3.859 GB	Ubuntu 16.04.3 LTS	17.06.2-ce	0.10-98812ae	Monitor	More -
Nodes	U									4	Remove Upgrade D] Docker

5. In the displayed confirmation dialog box, click Confirm.

4.2. Reset a node

Context

You can reset a node in a cluster. The system disk of the corresponding machine (the reset node) is replaced and the data stored in the system disk is lost. The reset machine is re-added to the cluster.

? Note

- Resetting an Elastic Compute Service (ECS) instance changes the ECS system disk. The disk ID is changed and the previous system disk is released.
- The reset ECS instance is restored to the status when it was added to the cluster.
- All data is cleaned up when resetting the node.
- Back up your data before resetting the node to avoid data loss.

Procedure

- 1. Log on to the Container Service console.
- 2. Click Nodes in the left-side navigation pane.
- 3. Select the cluster where the node you want to reset resides from the Cluster list.
- 4. Select the cluster where you want to reset the nodes.Click More at the right of the node you want to > reset and then select Reset from the list .

Container	Service	Node List									R	efresh
Kubernetes	Swarm											
Overview		Help: 🖉 Postpay instant	ce to Prepay									
Applications		Cluster: swarm-test	2									
Services		IP Address	Instance Type	Instance ID/Name	Status	Number of Containers	Configuration	Operating System	Docker Version	Agent		3
Clusters		-	Alibaba Cloud Node	212 ISSN	Normal	16	CPU:2core(s) Memory:3.859 GB	Ubuntu 16.04.3 LTS	17.06.2-ce	0.10-98812ae	Monitor	More -
Nodes	1									4	Reset	_
Networks											Upgrade D	ocker

5. In the confirmation window, enter the instance logon password, and click Confirm. In the pop-up confirmation dialog box, fill in the login password for the instance and click OK.

Reset		\times
Instance ID :	i-bp1iv5vwf06ovxvyt5ub	
Instance Name :	ce33a1ac76fbe414883418910abbd214e-node1	
* Operating System :	Ubuntu 16.04 64bit Currently, only Ubuntu and CentOS operating systems are supported.	
Login :	Password O Key Pair	
* Password :	••••••• The password should be 8–30 characters long and contain three types of characters (uppercase/lowercase letters, numbers, and special characters). Slash (\) and quotation mark (") are not supported.	
* Confirm Password :	••••••	
Reminder :	 When resetting an ECS instance, a new system disk is attached. The disk ID will change and the previous system disk will be released. 1. The reset ECS nodes will restore to the status when they were added to the cluster. 2. When resetting the node, all data will be erased. 3. Please back up data before performing this operation to avoid data loss. 	
	Confirm	Cancel

4.3. View containers running on a node

Context

You can view containers running on a node on the Node List page.

- 1. Log on to the Container Service console.
- 2. Click Swarm > **Nodes** in the left-side navigation pane.
- 3. On the Node List page, select a cluster from the Cluster drop-down list.
- 4. Click the node ID.

Container Service	Node List									Refr	fresh
Kubernetes Swarm	Help: 🖉 Postpay instan	ce to Prepay									
Applications	Cluster: swarm-test	. 2									
Services	IP Address	Instance Type	Instance ID/Name	Status	Number of Containers	Configuration	Operating System	Docker Version	Agent		Action
Clusters	3 (eip)	Alibaba Cloud Node		Normal	7	CPU:2core(s) Memory:3.702 GB	CentOS Linux 7 (Core)	17.06.2-ce	0.10-98812ae	Monitor !	More 🕶

You can see the list of containers running on the node.

<	Node:17							
Container List								
Node Monitoring	Instance ID: i-bp1bn8 Lab Instance Name: c9b0 co	bels: om.docker.swarm.task: om.docker.swarm.task:	Status: Norr	mal		Region: China East 1 (Hangzhou)		Cluster: swarmmode-cluster
	Name/ID e8	om.docker.swarm.node.id;js8gmwj3misc9vec 874b2lz om.docker.stack.namespace:acslogging	P	Port	Container IP		Node IP	Action
	acs-agent () ali system co	liyun.addon:acslogging om.docker.compose.project:acslogging om.docker.swarm.service.name:acslogging_lo			172.1		172.	Monitor Logs
	acslogging_logsp 0 gs default dk	ispout om.docker.swarm.task.id:izp2ab29r7e6hplv23 kq40en			acslo		172.	Monitor Logs Web Terminal
	acslogging_logta default	om.docker.swarm.service.id:9bagrz3bz1hdw7 z53swkifvx liyun.cap.oom_kill_disable:true			172.1		172.	Monitor Logs Web Terminal
Ξ	acsmonitoring_ac pc default	om.ookker.swarm.task.name:acsioggnig_jogs out.js8ghfwj5m1sc9vete874b2lz.izp2ab29r7e hplv23dkq40en liuun sewice irtactonoing. kospout			172.1		172.	Monitor Logs Web Terminal
	acsrouting_routi	running registry-vpc.cn sha256:4c6242345	8	80/tcp	10.25 Ingre multi acsro		172.	Monitor Logs Web Terminal
	acsvolumedriver	running registry-vpc.cn sha256:4030f33dc			172.1		172.	Monitor Logs
	tunnel-agent () system	running registry-vpc.cn sha256:644001fe1			172.1		172.	Monitor Logs

What's next

In the list, you can view the labels, images, the image SHA256 values, logs, and monitoring information of containers and perform operations on containers, including starting and stopping containers, deleting containers, and operating on containers on a remote terminal.

4.4. Update a node certificate

You can update a node certificate of a Swarm cluster to avoid node certificate expiration.

Prerequisites

- 1. You have created a swarm cluster, see Create a cluster.
- 2. Updating a node certificate reboots the node Docker Daemon. Make sure that containers on the node are all configured to restart automatically.

(?) Note You can configure a container restart policy when creating an application. When you create an application by using an image, select the **Always** check box for **Restart**. When you create an application by using a template, configure a container restart policy in the template restart: always.

3. If a node certificate expires within 60 days, a prompt is displayed. You must timely update the node certificate.

Context

Each cluster node has a certificate used to access system control services. Each issued certificate has a valid period. When the valid period of a certificate is about to expire, you must manually renew the certificate. Otherwise, the service of the node is affected.

Procedure

> Document Version: 20220630

- 1. Log on to the Container Service console.
- 2. Under the Swarm menu, click **Nodes** in the left-side navigation pane. The certificate expiration information of each cluster node is displayed.

? Note The certificate expiration time is displayed in the status column only if the node certificate expires within 60 days.

3. Select a node in the node list, and click **More > Update Certificate** on the right to reissue the node certificate.

? Note We recommend that you upgrade the cluster agent to the latest version before updating the node certificate.

- 4. (Optional)If the system prompts you to upgrade the cluster agent after you click Update Certificate, the current cluster agent does not support this feature. You need to upgrade the cluster agent to the new version first, see Upgrade Agent. If no prompt is displayed, go to the next step.
- 5. If no prompt is displayed or the cluster agent is updated, click **Update Certificate**. Confirm updating information and then update the node cluster certificate.

? Note

- When the node certificate update is completed, the Docker Daemon node is automatically restarted about 1 minute later.
- To guarantee that containers on the node can automatically restart, make sure that an automatic restart policy is configured.
- 6. After the cluster node certificate is updated, the node certificate information is no longer displayed.

5.Security groups 5.1. Container Service security group rules

View security group rules

Procedure

- 1. Log on to the Container Service console.
- 2. Click Clusters in the left-side navigation pane.
- 3. On the Cluster List page, click Manage at the right of a cluster.

Container Service	Cluster List						You can o	reate up to 5 clusters and car	add up to 20 nodes in each du	ster. Refresh	Create Ch	ister -
Overview	Help: ${\mathscr O}$ Create cluster ${\mathscr O}$ How to add existing	ECS instances 🖉 Cross-20	ne node management 🖉 Log Ser	vice integration & Connect to cluster (through Docker Client							
Applications	Name *											
Services	Cluster Name/ID	Cluster Type	Region	Network Type	Cluster Status	Node Status 🙆	Number of Nodes	Time Created	Docker Version			Action
Clusters 1 Nodes	testsafe-vpc	Albaba Cloud Cluster	China East 1 (Hangzhou)	VPC	Running	Healthy C	1	2017-09-04 15:47:52	17.03.1-ce	Manage	View Logs Monitor	Delete More +
Networks Data Volumes	test-safe 🖌	Alfaba Cloud Cluster	China East 1 (Hangzhou)	Classic Network	Running	Healthy C	1	2017-09-04 15:19:34	17.03.1-ce 2	Manage	View Logs Monitor	Delete More +

4. Click the security group ID to jump to the details page of this security group on the Elastic Compute Service (ECS) console.

<	Cluster:test-safe				Enable Log Service	Log on to Hub	Refresh
Basic Information	Danis Teformation				There is seen a later of the	Cartan Carta	dura piuli
Load Balancer Se	basic Information				Upgrade Agent Upgrade	System Service	Clear Disk
Courd Data i Cer De	Cluster ID:	Classic Network	Running	Region: China East 1 (Hangzhou)	Number of Nodes 1	Expand Add Existin	g Instances
User Tags	Security Group ID: Check Security Group Rebind						
Image List							

5. Click Security Group Rules in the left-side navigation pane. You can view the security group rules.

<	alicloud-cs-auto-cre	eat 🔹 /					Tutorial	C Back Add Security Group Rules	s Quickly Create Rules Add ClassicLink Rule
Instance List in S	Inbound Outbound								
Scenty Group Ic	Authorization Policy	Protocol Type	Port Range	Authorization Type	Authorization Object	Description	Priority	Creation time	Operation
	Allow	All	-1/-1	Address Field Access	172.18.0.0/16		1	2017-09-04 15:48:03	Modify Description Clone Delete
	Allow	All ICMP	-1/-1	Address Field Access	0.0.0/0	1.0	1	2017-09-04 15:48:02	Modify Description Clone Delete
	Allow	Custom TCP	80/80	Address Field Access	0.0.0.0/0		1	2017-09-04 15:48:01	Modify Description Clone Delete
	Allow	Custom TCP	443/443	Address Field Access	0.0.0/0		1	2017-09-04 15:48:01	Modify Description Clone Delete
=	Allow	Custom TCP	22/22	Address Field Access	0.0.0.0/0		1	2017-09-04 15:48:00	Modify Description Clone Delete

Security group rules

For the Container Service clusters created after February 28, 2017, the security groups created by default have been reinforced. Alibaba Cloud Container Service only sets the inbound security group rules. Container Service only supports creating clusters in the VPC environment since January 1, 2018. The opening rules of VPC clusters are as follows.

Virtual Private Cloud (VPC) security group:

<	alicloud-cs-auto-crea	at 🐟 /					Tutorial	C Back Add Security Group Rules	Quickly Create Rules Add ClassicLink Rule
Instance List in S	Inbound Outbound								
Security Group R	Authorization Policy	Protocol Type	Port Range	Authorization Type	Authorization Object	Description	Priority	Creation time	Operation
	Allow	All	-1/-1	Address Field Access	172.18.0.0/16		1	2017-09-04 15:48:03	Modify Description Clone Delete
	Allow	All ICMP	-1/-1	Address Field Access	0.0.0.0/0	-	1	2017-09-04 15:48:02	Modify Description Clone Delete
	Allow	Custom TCP	80/80	Address Field Access	0.0.0/0	-	1	2017-09-04 15:48:01	Modify Description Clone Delete
	Allow	Custom TCP	443/443	Address Field Access	0.0.0.0/0		1	2017-09-04 15:48:01	Modify Description Clone Delete
Ξ	Allow	Custom TCP	22/22	Address Field Access	0.0.0.0/0	-	1	2017-09-04 15:48:00	Modify Description Clone Delete

? Note

- Ports 443 and 80 are opened by default for the convenience of your business Web services. You can open or close the ports per your needs.
- We recommend that you retain the ICMP rules for communication between nodes and the convenience of troubleshooting. Some tools also depend on ICMP.
- The VPC security group sets the basic address of the container network segment as the Authorization Object. In this example, it is 172.20.0.0/16. This is related to the initial ClasslessInter-Domain Routing (CIDR) block of Container Service that you set when creating the VPC cluster (for details, see Create a cluster). The Authorization Object ensures the communication between containers.

For the clusters created before February 28, 2017, the security group rules are loose. Take the classic network security group rules as an example.

sg,	, aliclo ± 5	ecurity Group List			Tutorial C Refresh	Back	Add Security Group Rules
Intranet Inbound In	ntranet Outbound Internet Inbound	Internet Outbound					
Note: When you add ingre the IPv4 address; for exam	ass rules for intranet side Classic Security-gr nple: 10.x.y.z/32. Tutorial	oup, we recommend that	specify another security group as s	ource; or you can use an individual IPv4 add	ress to make your host more se	ecure. You m	ust use the /32 prefix after
Authorization Policy	Protocol Type	Port Range	Authorization Type	Authorization Object	Priority		Operation
Allow	All	-1/-1	Address Field Access	0.0.0/0	1		Clone Delete
Allow	Custom TCP		Address Field Access	0.0.0.0/0	1	1 Clone	
Allow	Custom TCP		Address Field Access	0.0.0/0	1		Clone Delete
sg-	/ aliclo ±s	ecurity Group List			Tutorial C Refresh	Back	Add Security Group Rules
Intranet Inbound In	ntranet Outbound Internet Inbound	Internet Outbound					
Authorization Policy	Protocol Type	Port Range	Authorization Type	Authorization Object	Priority		Operation
Allow	Custom TCP 237		Address Field Access	0.0.0.0/0	1		Clone Delete
Allow	All -1/-1		Address Field Access	0.0.0.0/0	1		Clone Delete
Allow	Custom TCP 22/22		Address Field Access	0.0.0/0	1		Clone Delete

To tighten the rules, refer to the configurations of the security groups created after February 28, 2017 and make the following changes by using **Add Security Group Rules** and **Delete** in the preceding figure:

- Add a rule in the intranet inbound and Internet inbound, with Allow selected as the Authorization Policy and All ICMP selected as the Protocol Type.
- To directly access ports 80, 443, or other ports of the virtual machine (VM), add the intranet and Internet rules to open these ports.

(?) Note Make sure you open all the ports you need. Otherwise, some services will become inaccessible. Do not open ports accessed by using Server Load Balancer instances.

• Delete the Internet inbound rules and intranet inbound rules with -1/-1 as the port range and 0. 0.0.0 as the address range.

Security configuration principles

• Each cluster has one security group.

Every Container Service cluster manages one security group. You can configure rules for this security group.

• Minimal permission principle.

To ensure the security of your cluster, we recommend that the security group opens the minimal permissions to the external.

• Security groups created by Container Service add some default rules.

For easier operations on ECS instances, security groups created by Container Service add some default rules, for example, ports 80 and 443 are opened. Delete the rules if you don't need them.

- Try to communicate by using the container intranet and do not expose communications to the host machine.
- When authorizing ECS instances outside the security group to access the security group, authorize a security group, instead of an individual IP address.

To authorize ECS instances outside the security group to access the current security group, create a new security group, add these ECS instances to the new security group, and then authorize the new security group to access the current security group.

• Open the container network segment at the VPC intranet outbound/inbound.

Otherwise, the network between containers is disconnected.

5.2. Check a security group

Context

You can check whether the cluster security group rules are safe or not in the Container Service console.

Procedure

- 1. Log on to the Container Service console.
- 2. Click Swarm > Clusters in the left-side navigation pane.
- 3. Click Manage at the right of a cluster.

Container	Service	Cluster List				You can create up to 5 clusters and can add up to 10 nodes in each cluster. Refresh Create Cluster -						•	
Kubernetes	Swarm	Help: Ø Create cluster Ø H	ow to add existing ECS i	nstances 🔗 Cro	ss-zone node management		integration	S Connect	to cluster through Dock	er Client			
Applications	5	Name 🔻											
Services		Cluster Name/ID	Cluster Type	Region (All) 👻	Network Type	Cluster Status	Node Status 🕜	Number of Nodes	Time Created	Docker Version		А	Action
Clusters	1	test-safe	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc-	Running	Healthy	1	05/21/2018,10:29:11	17.06.2- C0	Mar	nage View Log De 2 Monitor M	ıs lete lore ↓
Networks													

4. Click Check Security Group. Then, the system checks the status of the cluster security group.

Cluster:swarmcluster					Log on to Hub Refresh
Basic Information				Upgrade Agent Upgrad	de System Service Clear Disk
Cluster ID: cfe91	VPC	Running	Region: China East 1 (Hangzhou)	Number of Nodes 2	Expand Add Existing Instances
Security Group ID: sg-bp1 Check Security Group Rebind					

If the security group rules are normal, the Confirm Checking Security Group dialog box opens. Click **Cancel**.

Confirm Checking Security Group	×
Your security group rule is safe.	
	Cancel

If your security group rules contain risks, a dialog box opens, listing the security group rules with risks. Click **Repair**. Then, the system deletes security group rules with risks and creates new security group rules.

5.3. Rebind a security group

Context

You can rebind a security group to your cluster in the Container Service console. The system re-creates a security group, binds this new security group to your cluster, and adds the nodes in your cluster to this new security group.

Procedure

- 1. Log on to the Container Service console.
- 2. Click **Clusters** in the left-side navigation pane.
- 3. On the Cluster List page, click Manage at the right of a cluster.

Container	Service	Cluster List				You can create up to 5 clusters and can add up to 10 nodes in each cluster				ach cluster.	Refresh	Create Cluster	•
Kubernetes	Swarm												
Overview		Help: Ø Create cluster	How to add existing ECS inst	ances 🔗 Cro	ss-zone node management	S Log Service	e integration	S Connect	to cluster through Dock	er Client			
Applications		Name 🔻											
Services		Cluster Name/ID	Cluster Type F	Region (All) 👻	Network Type	Cluster Status	Node Status 🕜	Number of Nodes	Time Created	Docker Version			Action
Clusters	1	test-safe	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc-	Running	Healthy C	1	05/21/2018,10:29:11	17.06.2- Ce	Μ	anage View La 2 Monitor	ogs Delete More▼
Networks												_	

4. Click Rebind.

Cluster:swarmcluster					Log on to Hub	Refresh
Basic Information				Upgrade Agent Upgrad	e System Service	Clear Disk
Cluster ID: cfe91	VPC	Running	Region: China East 1 (Hangzhou)	Number of Nodes 2	Expand Add Existin	ng Instances
Security Group ID: sg-bp1 Check Security Group						

5. The Rebind Security Group dialog box opens. Click **Confirm**.

Rebind Se	ecurity Group	\times
0	Rebinding security group will create and bind a new security group for your cluster. Are you sure you want to rebind a new security group?	
	Confirm Cancel	

6.Images and templates 6.1. View image list

Procedure

- 1. Log on to the Container Service console.
- 2. In the left-side navigation pane, click **Images and Templates > Docker Images** .You can view the image category.
 - Popular: Some common images recommended by Container Service.
 - Official: Official images provided by Docker Hub.

Container	Service	Image List Popular Offic	ial	
Kubernetes	Swarm			
Overview Applications	5	€ mongolDB	mongo Type:fuklic Source:DOCICER_HUB ★797 MongoDB document databases provide high availability and easy scalability.	Create Application →
Services Clusters Nodes		MySQL.	mysql Type:Public Source:DOCICER_HUB ★1243 MySQL is a widely used, open-source relational database management system (RDBMS).	Create Application +
Networks Data Volum	nes	NGINX	nginx Type:Public Source:DOCIER_HUB ★1169 Official build of Nginx.	Create Application →
Configuratio	ons d Templates		php Type:Public Source:DOCIGR_HUB ★381 While designed for web development, the PHP scripting language also provides general-purpose use.	Create Application ->

6.2. View orchestration template list

Procedure

- 1. Log on to the Container Service console.
- 2. In the left-side navigation pane, click > Images and Templates > Orchestration Templates .

You can view the template category, or search for specific templates according to the keywords of template name, description, and image information.

- Sample: Common orchestration templates recommended by Container Service.
- My Orchestrations: The orchestration templates you created.

Container Service	Orches	tration List Sample My Orchestrations		Search Create
Overview Applications	¢00	gitlab Details V1	Service:Image postgreed: registry.cn-hangzhou.aliyuncs.com/acs-sample/postgreed-sameersbn:9.4-24 qittab : registry.cn-hangzhou.aliyuncs.com/acs-sample/gittab-sameersbn:3atest redis : registry.cn-hangzhou.aliyuncs.com/acs-sample/redis-sameersbn:3atest	Create Application ->
Clusters Nodes Networks Data Volu	0°0	jenkins Details VI	Service:Image service:Tragetory.cm-hangzhou.aliyuncs.com/acs-sample/jenkins-2.60.3 slave-gbas: registry.aliyuncs.com/acs-sample/jenkins-slave-dind-gbang slave-gbas: registry.aliyuncs.com/acs-sample/jenkins-slave-dind-gbas slave-phas: registry.aliyuncs.com/acs-sample/jenkins-slave-dind-ordels slave-phas: registry.aliyuncs.com/acs-sample/jenkins-slave-dind-ordels slave-phas: registry.aliyuncs.com/acs-sample/jenkins-slave-dind-orbup slave-phas: registry.aliyuncs.com/acs-sample/jenkins-slave-dind-ophp	Create Application →
Configurations Timages and Tem Docker Images Orchestration T	₽ °	jstorm Details VI	Service:Image zkt : mesoscioud/zookeeper:3.4.8-ubuntu zk2 : mesoscioud/zookeeper:3.4.8-ubuntu zk3 : mesoscioud/zookeeper:3.4.8-ubuntu mittus : registry:d=naptou.aliyuncs.com/jstorm-docker/jstorm supervisor : registry:.cn-hangzhou.aliyuncs.com/jstorm-docker/jstorm	Create Application ->
Solutions Operation Logs Getting Started	0 00	Redis-cluster-with-Sentinel Details V1	Service:Image master : redis:3 slave : redis:3 sentinel : registry.allyuncs.com/acs-sample/redis-sentinel:3	Create Application →

6.3. Create an orchestration template

Procedure

- 1. Log on to the Container Service console.
- 2. In the left-side navigation pane, click Orchestration TemplatesImages and Templates > > Orchestration Templates .
- 3. Click Create in the upper right corner.

Container Service	Orchestration List Sample My Orchestrations		Search Create
Overview Applications	OO gitlab Details VI	Service:Image postgresq1 : registry.cn-hangzhou.aliyuncs.com/acs-sample/postgresql-sameersbn:9. 4-24 gitab : registry.cn-hangzhou.aliyuncs.com/acs-sample/gitab-sameersbn:latest redis : registry.cn-hangzhou.aliyuncs.com/acs-sample/redis-sameersbn:latest	Create Application ->
Clusters Nodes Networks	O jenkins Details VI	Service:Image jerkins : registry.cn-hangzhou.aliyuncs.com/acs-sample/jenkins:2.60.3 slave-golang : registry.aliyuncs.com/acs-sample/jenkins-slave-dind-golang slave-apva : registry.aliyuncs.com/acs-sample/jenkins-slave-dind-dava slave-option : registry.aliyuncs.com/acs-sample/jenkins-slave-dind-nodejs slave-option : registry.aliyuncs.com/acs-sample/jenkins-slave-dind-option slave-option : registry.aliyuncs.com/acs-sample/jenkins-slave-dind-option	Create Application +
Data Volumes Configurations • Images and Templates	1 Details VI	Service:Image zk1 : mesoscloud/zookeeper:3.4.8-ubuntu zk2 : mesoscloud/zookeeper:3.4.8-ubuntu zk3 : mesoscloud/zookeeper:3.4.8-ubuntu nimbus : registry.cn-hangzhou.aliyuncs.com/jstorm-docker/jstorm supervisor : registry.cn-hangzhou.aliyuncs.com/jstorm-docker/jstorm	Create Application +
Docker Images Orchestration Templa	2 0 Redis-cluster-with-Sentinel Details	Service:Image master : redis:3 slave : redis:3 sentinel : registry.allyuncs.com/acs-sample/redis-sentinel:3	Create Application +

- 4. On the **Create Orchestration** page, complete the following configurations:
 - Name: Enter a name for the template.
 - **Description**: Enter the information about this template.
 - Content : The yml file of Docker Compose. For more information, see Compose file details.

*Name:	test	
	The name should be 1-64 characters long, and can contain numbers, Engli	sh letters, Chinese characters and hyphens.
Description:		
Content:	1 newServiceBlock1510281361729:	Service(s) Contained
	3 restart: always 4 cepose: 5 - 80/tcp 6 labels: 7 aliyun.scale: '1' 8	Service Name: newServiceBlock1510281361 Image: nginclatest Add Service
	You can use an orchestration template to define and deploy a multi-contain	ner application. The Docker Compose format is supported. For more
	A LLC	

The services contained in the orchestration template are displayed on the right side. To modify a service, click **Edit**. The Create Service dialog box opens. Modify the configurations and then click OK. To delete a service, click **Delete**.

To add another service to the orchestration template, click Add Service. The **Create Service** dialog box opens. Select an image and complete the other configurations. Click OK.

Create Service

 \times

Scale:	1				
Port Mapping:	Host Port		Container Port	Put	lish Protocol
	Host Port		Container Port	V	-
Environment:	Variable Name	١	/ariable Value		
[Name		/alue		
Data Volume:	Host Path or Data Volu Name	ume	Container Path		Permission
	Host Path or Data Volu	ıme M	Container Path		Read/Wri
Web Routing:	Container Port	[Domain Name:		
	Container Port		Domain name: For examp	le: http:/	/[domain name]
1	Note: All domain names	for a	port must be entered in	one enti	γ.
Restart:	Z				

5. Click **Create Orchestration** to create the orchestration template.

What's next

You can view your created orchestration templates under **My Orchestrations** on the **Orchestration** List page.

Orchestration	n List Sample	My Orchestrations		Search	Create
Øo	test Details V1	Service:Image newServiceBlock1510281361724ginx:latest	Create Appl	cation →	

Click **Details** to view the detailed information of the orchestration template or click **Create Application** to create an application by using this orchestration template.

6.4. Update an orchestration template

Context

You can only edit **orchestration templates** displayed under **My Orchestrations** on the Orchestration List page. To edit templates displayed under **Sample**, save the sample template as **your own template** and then edit it. For how to save an orchestration template as a new one, see Save an orchestration template as a new one.

Procedure

- 1. Log on to the Container Service console.
- 2. n the left-side navigation pane, click **Images and Templates > > Orchestration Templates**.
- 3. Click the **My Orchest rations** tab and then click **Details** of the orchestration template you want to update.

Container Service	Orchestration List Sample	My Orchestrations	3				Search	Create
Kubernetes Swarm			-					
Overview	Øo test			Service: Image nginx: nginx:latest	(reate Application →		
Applications								
Services	4							
Clusters								
Nodes								
Networks								
Images and Templates								
Docker Images 2								
Orchestration Templa								

4. Click Edit in the upper-right corner.

Orchestration:test • Back to Orchestration List	Edit	Delete	Download	Save As	Create Application
1 - hewServiceBlock15102B1361729: 2 image: rnginx:latest' 3 restart: always 4 - expose: 5 - 80/tcp 6 - labels: 7 aliyun.scale: '1'					

5. Edit the template content.

To modify a service, you can modify the content in the template directly or click **Edit** to modify the configurations in the appeared **Create Service** dialog box.

To add another service to the orchestration template, click Add Service. The Create Service dialog box appears. Select an image and complete the other configurations. Click OK. You can modify the content in the template directly or click **Delete** to delete the service.

Orchestratic	t. Back to Orchestration List	Cancel Save
Name:	test The name should be 1-64 characters long, and can contain numbers, English letters, Chinese characters and hyphens.	
Description:		
Template:	1 - hexServiceBlock1510281361729: 2 image: 'nginx:Latest' 3 restart: always 4 expose: 5 - 80/tcp 6 - Labels: 7 aliyun.scale: '1'	Service (s) Contained Service Name: newServiceBlock1510281361 Image: nginx:latest Edit Delete Add Service

6. Click Save in the upper-right corner to save the modifications.

6.5. Download an orchestration template

Procedure

- 1. Log on to the Container Service console.
- 2. In the left-side navigation pane, click Images and Templates > > Orchestration Templates .
- 3. Click **Details** of the orchestration template you want to download.

Container Service	Orchestration List Sample My Orchestrations	Search	Create
Kubernetes Swarm			
Overview Applications	GO gitlab Details VI	Service: Image podgracej: registry.cn-hangzhou.aliyuncs.com/acs-sample/podgracej.sameersbn:34-24 gdtab: registry.cn-hangzhou.aliyuncs.com/acs-sample/redis-sameersbn:latest redis: registry.cn-hangzhou.aliyuncs.com/acs-sample/redis-sameersbn:latest	on →
Services Clusters Nodes Networks	CO CO Detatis VI	Service: Image jeritize: registry.cn-hangzhou.alivuncs.com/acs-sample/jeritize:2.66.3 stave-golanz: registry.alivuncs.com/acs-sample/jeritize-iave-dind-golang stave-golanz: registry.alivuncs.com/acs-sample/jeritize-iave-dind-dolang stave-golanz: registry.alivuncs.com/acs-sample/jeritize-iave-dind-dolang stave-golanz: registry.alivuncs.com/acs-sample/jeritize-iave-dind-dolang stave-golanz: registry.alivuncs.com/acs-sample/jeritize-iave-dind-dolang stave-golanz: registry.alivuncs.com/acs-sample/jeritize-iave-dind-dolang stave-golanz: registry.alivuncs.com/acs-sample/jeritize-iave-dind-dolang	on →
Data Volumes Configurations I I Images and Templates	QO jstorm Details VI	Service: Image ktc: mesoclout/zookesper:3.4.8-ubuntu ktc: mesoclout/zookesper:3.4.8-ubuntu ninbus: registry-ch-hangthou.aluvuncs.com/jstorm-docker/jstorm supervisor: registry-cn-hangthou.aluvuncs.com/jstorm-docker/jstorm	on →
Docker Images 2 Orchestration Templa	Redis-cluster-with-Sentinel	Service: Image master: redie:3 slave: redie:3 sertifiel: redie:3 sertifiel: redie:3	on →

4. Click **Download** in the upper right corner to download the template file with the suffix yml.



6.6. Delete an orchestration template

Context

Orchestration List page.
Orchestration List page.

- 1. Log on to the Container Service console.
- 2. In the left-side navigation pane, click Images and Templates > Images and Templates > >

Orchestration Templates .

3. Click the **My Orchest rations** tab and then click **Details** of the orchestration template you want to delete.

Container	Service	Orchestration List	Sample My Orchestrations	3		Search Create
Kubernetes	Swarm					
Overview		00	test	Service: Image	Create Application ->	
Applications		₩O	Details V1	nginx: nginx:latest	Create Hyprication **	
Services			4			
Clusters						
Nodes						
Networks						
Data Volume	85					
Configuratio	ns 🚺					
 Images and 	Templates					
Docker Im	ages 2					

4. Click **Delete** in the upper right corner.

Orchestration:test t Back to Orchestration List	Edit	Delete	Download	Save As	Create Application
1 - hewServiceBlock510201361729: 2 inage: 'ngink:latest' 3 restart: abways 4 expose: 5 - 50/tcp 6 - labels: 7 aliyun.scale: '1'					

5. Click **OK** in the confirmation dialog box.

6.7. Save an orchestration template as a new one

You can save an orchestration template under Sample or My Orchestrations on the Orchestration List page as a new one.

Procedure

- 1. Log on to the Container Service console.
- 2. In the left-side navigation pane, clickImages and Templates > Orchestration Templates .
- 3. Click the Sample tab or the My Orchestrations tab, and then click **Details** of the orchestration template you want to save as a new one.

Container Service	Orchestration List Sample My Orchestrations	Sec	rch Create
Kubernetes Swarm			
Overview Applications	CO gitlab Details	Service: Image postgread; registry.cn-hangzhou.aliy.uncs.com/acs-sample/gotagresql-sameersbn:9.4-24 grabit: registry.cn-hangzhou.aliy.uncs.com/acs-sample/gotab-sameersbn:latest redis: registry.cn-hangzhou.aliy.uncs.com/acs-sample/redis-sameersbn:latest	pplication 🔶
Services Clusters Nodes Networks	3 O jenkins Detais	Service: Image jenkins: registry.cn-hangzhou.aliyu.ncs.com/acs-sample/jenkins:2.60.3 diave-dpian; registry.aliyu.ncs.com/acs-sample/jenkins-slave-dind-oplang diave-dpian; registry.aliyu.ncs.com/acs-sample/jenkins-slave-dind-solari diave-dpian; registry.aliyu.ncs.com/acs-sample/jenkins-slave-di	oplication →
Data Volumes Configurations 1 Images and Templates	O jstorm Details	Service: Image 241: mesoscioud/zookesper:3.4.8-ubuntu 242: mesoscioud/zookesper:3.4.8-ubuntu 243: mesoscioud/zookesper:3.4.8-ubuntu 243: mesoscioud/zookesper:3.4.8-ubuntu 249: mesoscioud/zookesper:3.4.	oplication →
Docker Images 2 Orchestration Templa	Redis-cluster-with-Sentinel	Service: Image master: redis:3 slave: redis:3 sertimel: registry.allyuncs.com/acs-sample/redis-sertimel:3	oplication →

4. Click Save As in the upper right corner.

Orchestration:gitlab t Back to Orchestration List	Download	Save As	Create Application
<pre>1 postgresql: 2 inage: registry.cn-hangzhou.aliyuncs.com/acs-sample/postgresql-sameersbn:9.4-24 3 environment: 4 - DB_USER-gitlab 5 - DB_PASS-password 6 - DB_NMWT=gitlabhg_production 7 - DB_EXTENSION+pg_trgm 8 - labels:</pre>			*

5. The Save Template As dialog box opens. Enter a name for the new template in the Name field and then click **OK**.

Save Template As			\times
Name:	gitlab-for-test		
		ОК	Cancel

The new orchest ration template is displayed under **My Orchest ration** on the **Orchest ration List** page.

Orchestr	ration List Sample My Orchestrations				Search	Create
Ø 0	gitlab-for-test Details Vi	Service:[mage postgresql : registry.cn-hangzhou.allyuncs.com/acs-sample/postgr gitlab : registry.cn-hangzhou.allyuncs.com/acs-sample/gitlab- redis : registry.cn-hangzhou.allyuncs.com/acs-sample/redis-s	resql-sameersbn:9.4-24 .sameersbn:latest sameersbn:latest	Cre	eate Application	→

7.Service orchestrations 7.1. Overview

Container Service supports describing multi-container applications by using the Docker Compose orchestration template.

The orchestration template allows you to describe an integrated application. The application can be composed of several services. For example, a portal application is composed of an Nginx service, a Web service, and a database service.

A service may have several containers. Make sure all of the containers have the same configurations. For example, the Web service in the preceding application can start two or more containers based on the traffic.

Capability

Container Service supports automatically deploying and managing an application by using the orchestration template.

The labels used by the orchestration template are compatible with most of the labels in Docker Compose V1 and V2. For information about specific compatible labels, see Label description.

The orchestration template also supports the template formats of Compose V1 and V2. For more information, see Docker Compose V1 and Docker Compose V2.

Container Service also provides many extension capabilities based on the community version:

- Unlike the community version of Docker Compose and Swarm, Alibaba Cloud Container Service supports cross-node container link. So you can directly deploy the application described by Docker Compose template to the distributed cluster to provide high availability and scalability.
- Container Service, based on the description in the Compose template of community version, also provides extensions to simplify the deployment, operation, and maintenance of Web and microservice applications. For more information, see Label description.

Example

The following is a WordPress application. It includes the Web service provided by WordPress image and the db service provided by MySQL image.

```
web:
 image: wordpress:4.2
 ports:
   - "80"
 environment:
   - WORDPRESS AUTH KEY=changeme
   - WORDPRESS SECURE AUTH KEY=changeme
   - WORDPRESS LOGGED IN KEY=changeme
   - WORDPRESS NONCE KEY=changeme
   - WORDPRESS AUTH SALT=changeme
   - WORDPRESS SECURE AUTH SALT=changeme
   - WORDPRESS LOGGED IN SALT=changeme
    - WORDPRESS NONCE SALT=changeme
 restart: always
 links:
   - db:mysql
 labels:
   aliyun.log store wordpress: stdout
   aliyun.probe.url: http://container/license.txt
   aliyun.probe.initial delay seconds: "10"
   aliyun.routing.port 80: wordpress; http://www.example.com; https://www.nice.com
   aliyun.scale: "3"
db:
 image: mysql:5.6
 environment:
   MYSQL ROOT PASSWORD: password
 restart: always
 labels:
   aliyun.log store mysql: stdout
```

7.2. Label description

The labels used by the Container Service orchestration template are compatible with most of the labels implemented in Docker Compose V1 and V2. Many extension capabilities are provided based on the community version.

Labels with extension capabilities

Container Service extends the deployment and lifecycle management capabilities for orchestration templates, and all the extension capabilities are described under labels and used as sub-labels.

Label	Description				
probe	Sets the health check of a service.				
Rolling_updates	Sets the rolling update of a service.				
parallelism	Sets how many containers that rolling_updates can concurrently update at a time. Note: This label must be used with rolling_updates .				

Label	Description
depends	Sets the dependencies of a service.
scale	Sets the number of containers for a service to scale horizontally.
routing	Sets the access domain name of a service.
routing.session_sticky	Sets whether or not routing keeps session sticky (namely, session persistence) during the routing request. Note: This label must be used with routing.
lb	Exposes the service port to the Internet or intranet by customizing Alibaba Cloud Server Load Balancer NAT mapping.
Log	Integrates with Alibaba Cloud Log Service to collect container logs and send the logs to Log Service.
Global	Sets the service as a global service.

Labels with function enhancement

Container Service provides the Service deployment constraints (affinity:service) label to set the deployment constraints for a service.

Additionally supported labels

Label	Description
External	Sets a service to directly link to an external address.
dns_options	Sets the DNS options. The semantics of this label is the same as that ofdns-opt parameter in the docker run command.
oom_kill_disable	Sets whether or not to prohibit OOM Killer. The semantics of this label is the same as that of oom-kill-disable parameter in the docker run command.

Variable substitution

Container Service supports the parameterized Docker Compose template. The template can include the environment variables as parameters. When the template is deployed, you are prompted to enter the parameter values, and the template variables are substituted during the deployment.

For more information, see Variable substitution.

Container rescheduling

Container Service supports rescheduling Docker containers. When a node is invalid, the container can be automatically scheduled to another available node for operation.

For more information, see Container rescheduling.

High availability scheduling

To make the application have higher availability, Container Service supports scheduling containers of the same service in different zones. When a zone malfunctions, the application can still provide services.

For more information, see High availability scheduling.

Unsupported Docker Compose labels

Currently, Container Service does not support some Docker Compose labels. For more information, see Unsupported Docker Compose labels.

7.3. probe

Set the health check of a service.

- Check the health by using URLs. HTTP and TCP protocols are supported.
- Check the health by using shell scripts.

The health check is initiated from the container host. At regular intervals (two seconds by default), a request is sent to the container or the shell script commands are run on the container.

The health check is successful if the following criteria are met: The HTTP request returns the code 2XX/3XX. The TCP port can establish a link. The shell scripts return the value 0.

Descriptions of the fields used for check:

- aliyun.probe.url : The URL requested by HTTP and TCP. You only need to add the word container , without entering your domain name or IP address. The URL is used for the health check after being resolved into the corresponding IP address of the container. The service passes the health check when 2XX or 3XX is returned.
 - For example, the container provides the HTTP service by using the port 8080 and provides /ping as the URL for the health check. The URL format for the probe is http://container:8080/ping. Container Service automatically requests to check the URL returned results by using HTTP GET. The health check is successful if 2XX or 3XX is returned.
 - For example, MySQL container monitors port 3306. The URL format for the probe is tcp://contai ner:3306 . The service checks whether the container opens the port 3306 or not. If yes, the health check is successful.
- aligun.probe.cmd : The shell command, /check.sh , is run during the health check. Container Service regularly runs this command within the container. If the shell scripts return the value 0, the health check is successful.
- aliyun.probe.timeout_seconds : The timeout for health check.
- aligun.probe.initial_delay_seconds : The number of seconds delayed to start the health check after the start of the container.

? Note

- A service can only contain either aliyun.probe.url Or aliyun.probe.cmd.
- If both <u>aligun.probe.url</u> and <u>aligun.probe.cmd</u> are not contained in the service, by default, the container is healthy and other <u>aligun.probe.xxx</u> labels are ignored.

Example:

Use URL to check whether or not the container is healthy.

```
os:
  image: my_nginx
  labels:
    aliyun.probe.url: http://container/ping
    aliyun.probe.timeout_seconds: "10"
    aliyun.probe.initial_delay_seconds: "3"
```

Use shell scripts to check whether or not the container is healthy.

```
os:
  image: my_app
  labels:
    aliyun.probe.cmd: health_check.sh
    aliyun.probe.initial delay seconds: "3"
```

7.4. Rolling_updates

During a service update, if the service includes more than one container (defined by the scale label), the (N+1)th container is updated after the Nth container is successfully updated. In this way, the service downtime is minimized.

Example:

Deploy the WordPress service.Specify to deploy 2 containers by using the scale label. Use the rolling updates label to minimize the service downtime for WordPress.

```
web:
 image: wordpress
 ports:
   - 80
 restart: always
 links:
   - 'db:mysql'
 labels:
   aliyun.logs: /var/log
   aliyun.routing.port 80: http://wordpress
   aliyun.rolling updates: 'true'
   aliyun.scale: '2'
db:
 image: mariadb
 environment:
   MYSQL_ROOT_PASSWORD: example
 restart: always
 labels:
   aliyun.logs: /var/log/mysql
```

parallelism

The parallelism label defines how many containers that rolling_updates can concurrently update at a time.

Onte This label must be used with the rolling_update label.

parallelism value:

- The default value is 1, namely, updating one container at a time.
- When the value is greater than 1, during rolling_updates , a certain number (defined by the par allelism label) of containers are concurrently updated at a time to realize the batch update.
- When the value is invalid, the default value 1 is used.

? Note To ensure that at least one container is providing service, we recommend that the defined parallelism value is less than the number of containers in the service.

Example:

Deploy the Nginx service. Specify to deploy 3 containers by using the scale label. Use the rolling_updates label and parallelism label to define that 2 containers are updated in batch at a time.

```
web:
    image: nginx:latest
    restart: always
    environment:
        - "reschedule:on-node-failure"
    ports:
        - 80
    labels:
        aliyun.scale: "4"
        aliyun.scale: "4"
        aliyun.rolling_updates: 'true'
        aliyun.rolling_updates.parallelism: "2"
```

7.5. depends

Set the dependencies of a service.

After setting the dependencies of a service, Container Service can control the start sequence of containers, starting the containers one by one.

Example:

```
Note Separate dependencies by using a comma (,).
```

```
web:
image: wordpress:4.2
ports:
    - 80
links:
    - db:mysql
labels:
    aliyun.depends: db,redis
db:
image: mysql
environment:
    - MYSQL_ROOT_PASSWORD=password
redis:
image: redis
```

7.6. scale

Set the number of containers for a service to scale horizontally.

Currently, Docker Compose can only start one container in each service. To expand the number of containers, manually set the number after the container is started.

```
You can use the scale label to scale as the container is started.
```

Moreover, after a container is deleted, you can redeploy the application by completing the following steps: Log on to the Container Service console. Click **Applications** in the left-side navigation pane. Click **Redeploy** at the right of the application you want to redeploy. Then, Container Service restarts the container or creates a new container to restore the number of containers to the specified quantity.

Example:

```
web:
    image: wordpress:4.2
    ports:
        - 80
    links:
        -db: mysql
    labels:
        aliyun. scale: "3"
db:
    image: mysql
    environment:
        - MYSQL_ROOT_PASSWORD=password
```

7.7. routing

The routing label configures the access domain name of a service.

Format:

aliyun.routing.port_\$container_port: [http://]\$domain|\$domain_prefix[:\$context_path]

Field description:

- \$container port : container port. Note: This is not the host port.
- \$domain : domain name. Enter a domain name.
- \$domain_prefix : domain name prefix. If you enter a domain name prefix, Container Service
 provides you with a test domain name and the domain name suffix is .<cluster_id>.<region_id>.a
 licontainer.com .
- \$context_path : requested service path. You can select services according to the requested path.

Domain name selection:

- If the HTTP protocol is used to expose the service, you can use the internal domain name (the top-level domain is alicontainer.com) provided by Container Service for testing, or use your own domain name.
- If the HTTPS protocol is used, you can use only your own domain name. For example, www.example.c
 om . You must modify the DNS settings to assign the domain name to the Server Load Balancer service provided by the container cluster.

Format requirements of the label statement:

- Container Service allocates a subdomain name to each cluster, and you only need to provide the domain name prefix to bind the internal domain name. The domain name prefix only indicates a domain name level and cannot be separated with periods (.).
- If you do not specify scheme , the HTTP protocol is used by default.
- The length of the domain name cannot exceed 128 characters. The length of the context root cannot exceed 128 characters.
- When you bind multiple domain names to the service, use semicolons (;) to separate them.
- A backend service can have multiple ports. These ports are exposed by the container. A port can only

be assigned one label. Therefore, a service with multiple ports must be assigned multiple labels.

Example:

Use the routing label.

Bind the internal domain name wordpress.<cluster_id>.<region_id>.alicontainer.com provided by Container Service and your own domain name http://wp.sample.com/context to port 80 of the Web service.

```
web:
image: wordpress:4.2
links:
   - db:mysql
labels:
   aliyun.routing.port_80: wordpress;http://wp.sample.com/context
db:
   image: mysql
environment:
   - MYSQL ROOT PASSWORD=password
```

The internal domain name that you finally get is wordpress.cd3dfe269056e4543acbec5e19b01c074.cn-beijing.alicontainer.com .

After starting the Web service, you can access the corresponding Web services by using the URL:

http://wordpress.cd3dfe269056e4543acbec5e19b01c074.cn-beijing.alicontainer.com

Of http://wp.sample.com/context .

To support the HTTPS service, upload the HTTPS certificate by using the Server Load Balancer console on the Alibaba Cloud website, and then bind the corresponding cluster to access the Server Load Balancer terminal.

routing.session_sticky

By using this feature, you can determine whether to maintain session sticky (session persistence) when you set the routing for a routing request. With session persistence, during the session, each request is routed to the same backend container instead of being randomly routed to different containers.

```
? Note
```

- The setting takes effect only when you have configured aligun.routing.port_\$contaienr port .
- Simple routing session persistence is based on the Cookie mechanism. By default, the maximum expiration time of Cookie is 8 hours and the idle expiration time is 30 minutes.
- Simple routing session persistence is enabled by default.

The setting methods are as follows:

Enable session persistence

aliyun.routing.session_sticky: true

• Disable session persistence

```
aliyun.routing.session_sticky: false
```
Example of a template orchestration file:

```
web:
    image: wordpress:4.2
    links:
        - db:mysql
    labels:
        aliyun.routing.port_80: wordpress;http://wp.sample.com/context
        aliyun.routing.session_sticky: true
db:
    image: mysql
    environment:
        - MYSQL_ROOT_PASSWORD=password
```

7.8. lb

Expose the service port to the Internet or intranet by customizing Alibaba Cloud Server Load Balancer NAT mapping. The Agent must be upgraded to the latest version to support this extension capability label.

The label format is as follows. Variables with s are placeholders.

```
aliyun.lb.port_$container_port:$scheme://$[slb_name|slb_id]:$slb_front_port
```

Example:

```
web:
 image: wordpress:4.2
 ports:
   - 7777:80
   - 9999:9999
   - 8080:8080
   - 53:53/udp
 links:
   - db:mysql
 labels:
   aliyun.lb.port 80: http://slb example name:8080
   aliyun.lb.port 9999: tcp://slb example name:9999
   Aliyun. lb. port 8very: https: // FIG: 80
   Aliyun. lb. port 53: UDP: // FIG: 53
db:
 image: mysql
 environment:
    - MYSQL_ROOT_PASSWORD=password
```

To better use the custom Server Load Balancer 1b label, you must understand three ports used in a routing request: the Server Load Balancer frontend port, the Server Load Balancer backend port (namely, the Elastic Compute Service (ECS) instance port), and the container port. Take the first 1b label aligun.lb.port 80 as an example. From left to right, The Server Load Balancer backend port is the ECS instance port, which can be obtained from host and container port mapping of the ports label. The container port 80 corresponds to the host port port 80 in the key indicates the port to be exposed by the container, and port 8080 indicates the frontend port to be exposed by Server Load Balancer. The Server Load Balancer backend port is the ECS instance port, which can be obtained from host and container port mapping of the ports label. The container port 80 corresponds to the host port 7777. So the backend port forwarded by Server Load Balancer is 7777. The first lb label indicates that a request sent to the Web service: First enters port 8080 of the Server Load Balancer frontend. Then, is forwarded to port 7777 of the backend ECS instance. Enters port 80 of the container according to the port mapping of ports. Finally, is submitted to the WordPress process in the container to provide the service. The other three lb labels also apply to the preceding explanation. All the Server Load Balancer instances configured by the lb label do not go through the routing service built in the cluster, and you control the request routing by yourself.

Format requirements of the label statement:

- The Server Load Balancer instance can be specified by using its name or ID.
- The Server Load Balancer instance name is limited to 1-80 characters, including letters, numbers, hyphens (-), forward slashes (/), periods (.), and underscores (_).
- The container port is limited to 1-65535.
- The Server Load Balancer front end port is limited to 1-65535.

Limits on deploying services with custom Server Load Balancer NAT mapping:

- You must create a Server Load Balancer instance, name it, and create the corresponding listening port. Then, provide the mapping container port scontainer_port, the used protocol scheme (possible values include tcp, http, https, udp, and the Server Load Balancer instance name sslb_name or sslb_id by using extension labels, and specify the frontend port sslb_fr ont_port of the Server Load Balancer instance.
- You must specify the host and container port mapping of the service port to be exposed and then use the standard Dockerfile label ports to specify the port mapping. to specify the port mapping. You must specify the host port and this port cannot conflict with the host port mapped by other services. Server Load Balancer uses the host port to bind the backend ECS instance.
- A service can only use one or more Server Load Balancer instances to expose the service port. Services cannot share and use the same Server Load Balancer instance because they are distributed in different ECS instance backends.
- When using the lb label to configure Server Load Balancer routing, the default Server Load Balancer instance cannot be used.
- The host that has the service with Server Load Balancer NAT mapping deployed uses the same host and container port mapping. Therefore, these services only have one instance on each ECS.
- The supported Server Load Balancer protocol *\$scheme* includes tcp, http, https, and udp.
- You must create a listening port in the Alibaba Cloud Server Load Balancer console.
- Log on to the Server Load Balancer console to modify the configurations for the Server Load Balancer instance used in Container Service, such as bandwidth limitation.

- The value of the lb label is that you do not need to bind the backend ECS instance of Server Load Balancer by yourself. After configuring the corresponding labels, the backend is bound automatically. instance of Server Load Balancer by yourself. After configuring the corresponding labels, the backend is bound automatically. Therefore, except for binding the Server Load Balancer backend, you must set and modify the Server Load Balancer instances in the Alibaba Cloud Server Load Balancer console.
- Container Service helps you generate a Resource Access Management (RAM) sub-account (you are required to activate RAM). This account has some Server Load Balancer permissions, but does not have the permission to create or delete Server Load Balancer instances. Use this account to help you manage the Server Load Balancer instances used in Container Service, for example, binding some nodes in the cluster as the service backend.
- In the whole lifecycle of the service, the 1b label always works unless the service is deleted or the service is redeployed after 1b label is deleted. Meanwhile, the Server Load Balancer instances configured in the 1b label cannot be mixed.

7.9. Log

Container Service, integrated with Alibaba Cloud Log Service, collects container logs and sends the logs to Alibaba Cloud Log Service.

Example:

```
mysql:
   image: mysql
   ports:
      - 80
   labels:
       aliyun.scale: "1"
   environment:
       - MYSQL ROOT PASSWORD=password
wordpress:
   image: registry.aliyuncs.com/jiangjizhong/wordpress
   ports:
       - 80
   labels:
        aliyun.routing.port 80: wordpress-with-log
        aliyun.log store dbstdout: stdout #Note here
    links:
        - mysql
```

For more information, see Enable Log Service.

7.10. Global

Set the service as a global service.

Some services need to be deployed to every node, such as monitoring and logging services. When a node is created, these services are deployed to the node.

A service is deployed to each node of the cluster if the service is set as global . When a node is created or added in the cluster, a container instance is automatically deployed to the node.

```
monitor:
    image: sample
        labels:
        aliyun.global: true
```

7.11. Service deployment constraints (affinity:service)

Set the deployment constraints for a service.

Container Service supports the container deployment constraints compatible with Docker Swarm. You can control the deployment of a container with the Docker Swarm filters.

But the community version of Docker Compose does not have relevant capabilities to control the direct deployment constraint for a service.

In Container Service, you can add affinity: service in environment to constrain the affinity between services so as to control the service deployment policy. Container Service supports soft affinity and hard affinity between services.

Example:

In this example, affinity:service!=db is the deployment constraint for the web service. In this way, the web service is always deployed to nodes where the db service is not deployed. Therefore, when a node is invalid, the service availability is enhanced. When your cluster has only one node, as hard anti-affinity is specified, the deployment will fail because it cannot meet the specified mandatory constraints.

```
web:
 image: registry.aliyuncs.com/acs-sample/wordpress:4.5
 ports:
   - '80'
 environment:
   - affinity:service! =db
 restart: always
 links:
   - 'db:mysql'
 labels:
   aliyun.logs: /var/log
   aliyun.probe.url: http://container/license.txt
   aliyun.probe.initial delay seconds: '10'
   aliyun.routing.port 80: http://wordpress
   aliyun.scale: '2'
db:
 image: registry.aliyuncs.com/acs-sample/mysql:5.7
 environment:
   MYSQL ROOT PASSWORD: password
 restart: always
 labels:
   aliyun.logs: /var/log/mysql
```

7.12. External

Set a service to directly link to an external address.

In the extension field, the following fields can be used:

- host : Set the domain name of the link.
- ports : Set the port of the link.

Example:

Directly start a MySQL container without using the external label.

```
web:
    image: wordpress:4.2
    ports:
        - 80
    links:
        - db:mysql
db:
    image: 10.32.161.160:5000/mysql
    environment:
        - MYSQL_ROOT_PASSWORD=password
```

Use the external label to describe an RDS service that is not deployed in the cluster and provide the service to the WordPress deployed in the cluster for use.

```
wordpress:
image: wordpress:4.2
ports:
    - 80
links:
    - db:mysql
environment:
    - WORDPRESS_DB_USER=cloud
    - WORDPRESS_DB_PASSWORD=MYPASSWORD
    - WORDPRESS_DB_NAME=wordpress
db:
external:
    host: rdsxxxx.mysql.rds.aliyuncs.com
    ports:
        - 3306
```

7.13. dns_options

Set the DNS options. The function of this label is the same as that of --dns-opt in the docker run command.

```
wordpress:
  image: wordpress:4.2
  dns_options:
    - "use-vc"
```

7.14. oom_kill_disable

Set whether or not to prohibit OOM Killer. The function of this label is the same as that of --oom-killdisable in the docker run command.

```
wordpress:
  image: wordpress:4.2
  oom-kill-disable: true
```

7.15. Variable substitution

Container Service supports the parameterized Docker Compose template. The template can include the environment variables as parameters. When the template is deployed, you are prompted to enter the parameter values, and the template variables are substituted during the deployment.

For example, you can define the parameter POSTGRES_VERSION.

```
db:
    image: "postgres:${POSTGRES VERSION}"
```

When the preceding Compose template is deployed, Container Service prompts you to enter the value of the POSTGRES_VERSION parameter, such as 9.3. Container Service substitutes the variable of the Compose template with this parameter value. In this example, a postgres:9.3 container is deployed.

Container Service is fully compatible with Docker Compose syntax, and you can use either \$VARIABLE or \${VARIABLE} syntax in the template.

In the Compose template, you can use store strings containing s. In this way, Container Service will not erroneously treat such a string as the parameter.

For more information on the variable substitution supported in the Compose template, see Variable substitution.

7.16. Container rescheduling

Container Service supports rescheduling Docker containers. When a node is invalid, the container can be automatically scheduled to other available node for operation.

By default, container rescheduling is disabled. If needed, you can enable the container rescheduling.

Container Service provides a container rescheduling policy that is compatible with Docker Swarm. You can enable container rescheduling by using environment variable or label.

Environment variable:

```
redis:
    image: redis
    environment:
        - reschedule:on-node-failure
```

Label:

```
web:
  image: nginx
  restart: always
  environment:
    - aaaaa=aaaaa
  labels:
    aliyun.scale: "3"
    com.docker.swarm.reschedule-policies: "[\"on-node-failure\"]"
```

Note If you re-schedule the container, You need to restore the Persistence State required for the docker container, you need to work with docker file volumes that support data migration or sharing.

7.17. High availability scheduling

To make the application have higher availability, Container Service supports scheduling containers of the same service in different zones. When a zone malfunctions, the application can still provide services.

You can specify the zone selection in the orchestration file by using the environment variables in the following formats:

• availability:az==3

The service must be distributed in at least three zones. The container creation fails if less than three zones are in the current cluster, or the service cannot be distributed in three zones because of limited machine resources.

• availability:az==~3

Try to distribute the service in three zones. Container can still be created even if the condition cannot be met.

In the following example, the service must be distributed in at least two zones.

```
nnn:
expose:
    - 443/tcp
    - 80/tcp
image: 'nginx:latest'
environment:
    - 'availability:az==2'
labels:
    aliyun.scale: '8'
restart: always
volumes:
    - /var/cache/nginx
```

7.18. Unsupported Docker Compose labels

Label	Description		
build	This label is used to build container images by using the Dockerfile and other files in the current directory. Currently Container Service does not provide the function to build images. We recommend that you separate the building and deployment operations. You can use image repository to build the image from the code source, or push the image built locally to the image repository. You can use the image label in the orchestration template to refer to the image in the image repository).		
dockerfile	The same as build .		
env_file	Currently Container Service does not support specifying environment variables in files. You can add environment variables by using the environment label.		
mac_address	Currently the setting of Mac address is not supported.		
detach	All the images in Container Service are enabled in the detach mode, and the attach mode is not allowed.		
stdin_open	The same as detach .		
tty	The same as detach .		
extends	Not supported.		
networks	The network in Compose file format of version 2 version 2. See Cross-host interconnected container network for network management and service discovery for Container Service. allows the service container to start in the custom network, and the containers in Container Service are all in the same cross-host interconnected container network. Therefore, Container Service does not support using the networks label in Compose file format of version 2. See Container network interconnection for network management and service discovery for Container Service.		

8.Applications 8.1. Create an application

Context

Limit s

Swarm clusters only support the compose V1 and compose V2 orchestration templates. The system reports an error if you select to use the compose V3 template.

Onte In the orchestration template list, compose V3 templates are marked with composev3.

Procedure

- 1. Log on to the Container Service console.
- 2. Click Applications in the left-side navigation pane.
- 3. Click Create Application in the upper-right corner.

Container Service - Swarn	n	Container Servic 1. Starting from 2. Starting from	e will end technical support fo July 1, 2019, users cannot on December 31, 2019, technica	or Swarm by the end of 2019. ' eate Swarm clusters in the con I support services for Swarm c	We recommend that you migrate isole. If you want to create Swar lusters will end. You cannot mar	e to Kubernetes in advance. The detailed support so m clusters after this date, submit a ticket. hage Swarm clusters in the console. Documents rela	hedule is as follows: ted to Swarm will be removed from the Alibaba	a
Overview		Cloud official we For more inform	bsite. You can still use APIs b ation about migrating to Kube	o manage Swarm clusters. ernetes, see the document (En	glish version will be available so	on). If you encounter any problems, please contact	Technical Support.	
Applications 1	L	Application List					Refrash Create App	lication
Services	Ŀ							
Clusters	Ŀ	Help: 🖉 Create a	n application 🔗 Change app	lication configurations 🔗 Sir	nple route blue-green release pol	licy 🔗 Container auto scaling	4	
Nodes	L	Cluster: test 🔻	Hide System Applications				Name 🔻	
		Name	Status	Services	Time Created 🔺	Time Updated 🔺		Action
Networks	-							_

- 4. Complete the basic information for the application you are about to create.
 - **Name**: Enter the name of the application. It can be 1–64 characters long and contain numbers, English letters, and hyphens (-), but cannot start with a hyphen (-).
 - Version: Enter the version of the application. By default, 1.0 is entered.
 - **Cluster**: Select the cluster on which the application is to be deployed.
 - Update: The update method of the application. Select Standard Release or Blue-Green Release. For more information, see Introductions on release strategies.
 - **Description**: Enter the information of the application. This field is optional. The entered description cannot exceed 1024 characters, and is displayed on the **Application List** page.
 - **Pull Docker Image**: With this check box selected, Container Service pulls the latest Docker image from the repository to deploy the application, even when the image tag does not change.

To improve efficiency, Container Service caches the image. When deploying an application, Container Service uses the cached image instead of pulling the image from the repository if the image tag is the same as that of the local cache. Therefore, if you modify your codes and image but do not modify the image tag for the convenience of upper business, Container Service uses the old image cached locally to deploy the application. With this check box selected, Container Service ignores the cached image and re-pulls the image from the repository when deploying the application to make sure the latest image and codes are always used.

Create Application	n					
Help: Ø Restrict o	container resources 🔗 High availability sch	neduling 🔗 Create a Ngin	x webserver from an image	S Create WordPress by	using an application templa	te 🔗 Orchestration template
description 🔗 Lab	el description					
	Basic Information		Configuration	>		Done
Name:	test					
	The name should be 1-64 characters long	, and can contain numbers,	, English letters and hyphens	, but cannot start with a l	iyphen.	
Version:	10					
Verbion.	10					
Cluster:	tect	T				
	con					
Update:	Standard Release	Ŧ				
Description:						
	Pull Docker Image ()					
					Create with Image	Create with Orchestration Template

5. Click Create with Image.

Click Create with Image. Set the following parameters according to your requirements.

i. In the General section:

	Image Name: Private registry entry supported		Image Version:	
		Select image		Select image version
eneral	Scale:	1	Network Mode:	Default 🔻
Ğ	Restart:	✓ Always		

Set the Image Name and Image Version.

You can select an image provided by Container Service or enter your image address in the format of domainname/namespace/imagename:tag. To select an image, click Select image, select the image, and then click OK. By default, the Container Service uses the latest image version. To use another version of the image, click Select image version, and then click OK.

- Set the number of containers (Scale).
- Select the Network Mode of the application. Currently, Container Service supports two
 network modes: Default and host. The Default mode is the bridge network mode. The host
 network mode allows containers to use the network stacks of Elastic Compute Service (ECS)
 instances. For more information, see Docker container networking.
- Set the Restart field.

The Always check box is selected by default. With the check box selected, the containers are restarted regardless of the exit status code. Docker daemon restarts the containers unlimitedly. Whatever the container status is, the container tries to be restarted when daemon is started.

When the check box is not selected, the restart policy becomes no, indicating containers are not restarted automatically on exit.

ii. In the Container section:

	Command:				
	Entrypoint:				
ontainer	CPU Limit:			Memory Limit:	MB
0	Capabilites:	ADD	DROP		
	Container Config:	🗆 stdin 🗖 tty			

Set the startup command (Command and Entrypoint) of the container. If configured, the image default configurations are overwritten.

Command is used to specify the startup command of the container main process. For more information, see Command.

Entrypoint is used to specify the container startup process and parameter. Used together with command, the cmd contents can be passed to Entrypoint as parameters. For more information, see Entrypoint.

• Set the resource limits (CPU Limit and Memory Limit) of the container.

Set the resource limit for the CPU and memory to be used by the container. For more information, see Restrict container resources.

Set the Capabilities.

For how to add or drop Linux related privileges for the container, see Capabilities.

• Set the Container Config.

iii. In the Network section:

	Port Mapping:	• Add domain names to services exposed to the public network
etwork	Web Routing:	• Expose HTTP services through acsrouting
Z	Load Balancer:	Expose services using custom Server Load Balancer

• Set the **Port Mapping**. Specify the port mapping for the host and the container, and select TCP or UDP as the protocol.

The port mapping is used for the routing between container and host, and is the precondition of Web Routing and Load Balancer. The container provides external services by means of the configured port mapping.

Set the Web Routing. The cluster automatically creates the acsrouting application, including the routing service, and provides the simple routing function. A routing service instance is deployed on each node. In a node, the acsrouting_routing_index container implements the routing forward in the cluster to route the HTTP or HTTPS service. For more information, see Simple routing - supports HTTP and HTTPS.

(?) Note When exposing the HTTP/HTTPS services, you can use the overlay network or Virtual Private Cloud (VPC) to directly access the container port, without configuring the specific host port.

Set the Load Balancer. Configure the port mapping before configuring the mapping of container_port \$scheme://\$[slb_name|slb_id]:\$slb_front_port . For how to use the Server Load Balancer label, see lb.

When configuring this parameter, control the routing access path on your own, including the routing mapping of Server Load Balancer front end port > backend host port > container port.

iv. Set the Data Volume.

	Data Volume:	• Use third-party data volumes			
		Host Path or Data Volume Name	Container Path	Permission	
Volume		e.g. /path or name	e.g. /path	/ RW	•
	volumes_from:				

- Create a data volume. Enter the host path or data volume name, the container path, and select RW or RO as the data volume permission. For more information, see volume.
- Configure the volumes_from field. Enter the name and permission parameter of another service or container, such as service_name:ro. If no access permission is specified, RW is the default permission. For more information, see volumes_from. After the configuration, the container is authorized to use volumes of another service or container.

v. Set the Environment variables.

Formats such as array, dictionary, and boolean are supported. For more information, see Environment variables.

vi. Set the container Labels.

For the extension labels supported by Container Service, see Label description.

vii. In the Deploy section:

	Smooth	\square Enable @ Note: This only takes effect when used with health check [probe label].
	Upgrade:	
Deploy	Across Multiple Zones:	◯ Ensure ◯ Try best
	Auto Scaling:	Enable Note: Before using auto scaling, upgrade the cluster Agent to the latest version.

• Set whether to enable Smooth Upgrade for containers.

For more information, see Rolling_updates.

• Set the Across Multiple Zones settings for containers.

Select **Ensure** to deploy containers in two zones. The container creation fails if less than two zones are in the current cluster, or the containers cannot be deployed in two zones because of limited machine resources. Select **Try best** to try to deploy containers in two zones. The container can still be created even if this condition is not met.

If this parameter is not configured, Container Service deploys the containers in one zone by default. For more information, see High availability scheduling.

• Set whether or enable the container Auto Scaling.

For more information, see Container auto scaling.

- viii. Click Create at the right of the page after completing the settings.
- 6. Click Create with Orchestration Template.

Create Application * Back to Application List				
Help: \mathscr{D} Restrict container resources \mathscr{D} High availability scheduling Label description	\mathscr{S} Create a Nginx webserver from an image	${\mathscr S}$ Create WordPress by using an application templa	ate $ \mathscr{O} $ Orchestration template description	8
Basic Information	Configuration		Done	
1			Add Service	
You can use an orchestration template to define and deploy a multi- to https://docs.docker.com/compose/	container application. The Docker Compose form	nat is supported. For more information, refer		
Use Existing Orchestration Template		Sav	re Template Prev Create and Dep	loy

i. Click Use Existing Orchestration Template or write a new template by yourself.

The contents of the orchestration template comply with the Docker Compose format.

- ii. Click Select next to the template after clicking Use Existing Orchestration Template.
- iii. Edit the orchestration template.

Edit the orchestration template according to your requirements. Make modifications in the template directly, or click **Edit** to modify the service or **Delete** to delete the service.



Click Add Service to add another service to this orchestration template. Select the image and configure the parameters. Then, click OK.

T N	Distance in the second			
Image Name:	Private registry entr Se	elect image		
Image Versior	n: Se	elect image version		
Scale:	1			
Port Mapping:	Host Port	Container Port	Publish Protocol	Actio
	Host Port	Container Port	¥ 🛛	Add
Environment:	Variable Name	Variable Value		Actio
	Name	Value		Add
Data Volume:	Host Path or Data Volun Name	ne Container Path	Permission	Actio
	Host Path or Data Volum	ne I Container Path	Read/Writ 🔻	Add
Web Routing:	Container Port	Domain Name:		Actio
	Container Port	Domain name: For example:	http://[domain nam	Add
I	Note: All domain names f	or a port must be entered in on	ie entry.	
Restart:	2			

iv. Click Create and Deploy after completing the settings.

8.2. Application parameter configurations

This document aims to help you understand what the parameters on the page mean when you create a swarm application by using an image. Then, you can configure the parameters smoothly. For some parameters, some documents are provided for your reference.

Image Name

- Select an existing image in the image list.
- Enter the image address directly. Take the image address of a Docker Hub user's WordPress container as an example. registry.cn-hangzhou.aliyuncs.com/acs-sample/wordpress:4.6 is a complete image address composed of domain name, namespace, image name, and label. For more information about the image address, see Basic concepts of images.

Image Version

You can specify the image version, namely, the image tag, after selecting an existing image in the image list. If not specified, the latest version is used by default.

Scale

Configure the number of containers. Multiple containers can enhance application availability efficiently.

Network Mode

Select Default or host.

- **Default**: Namely, the bridge network mode. By connecting to the default bridge docker0, this mode assigns an independent network namespace for each container. You can see that eth0 is created in the container by using this configuration.
- Host: The network stack information that allows containers to use host. Containers created in this mode can view all the network devices on the host and have the full access permission to these devices.

For more information about Docker container network, see Docker container networking.

Restart

Specify the restart policy for the container. For more information, see restart.

- With this check box cleared, the system does not restart the container under any circumstances.
- With this check box selected, the system tries to restart the container until the specified container is running normally.

Command

Configure the command that is run by default after the container is started and configure the corresponding parameters. We recommend that you use the Exec format. The command is run if the container is started and docker run does not specify other commands. For more information, see command.

The default command specified by command is ignored if docker run specifies other commands.

Command has three formats:

- Exec format: CMD ["executable", "param1", "param2"] . This is the recommended format of command.
- CMD ["param1", "param2"] : Use together with entrypoint command that is in the Exec format to provide the additional parameters.
- Shell format: CMD command param1 param2 .

Entrypoint

The execution command to start containers. Entrypoint command can run the containers in the form of applications or services.

Entrypoint seems similar to CMD, both of which can specify the command to be run and the corresponding parameters. The difference is that entrypoint is not ignored and must be run, even if other commands are specified when running docker run.

Entrypoint has two formats:

```
• Exec format: ENTRYPOINT ["executable", "param1", "param2"] . This is the recommended format
```

of entrypoint.

• Shellformat: ENTRYPOINT command param1 param2 .

CPU Limit and Memory Limit

CPU 100 indicates one core and the unit of memory is the MB. You can configure the CPU limit and memory limit for a container, which facilitates your resource planning. The corresponding compose labels are mem_limit and cpu_shares. For more information, see Restrict container resources.

Capabilities

By default, the root permission in Docker containers has strict limits. With the Linux kernel capabilities, related permissions can be granted to the containers. For the parameters used to grant permissions to the containers, see Runtime privilege and Linux capabilities.

The related parameter commands are as follows:

- ADD field: Corresponds to the parameter -cap-add: Add Linux capabilities . Enter the Capability Key that containers can add in this field to add the permission to containers.
- DROP field: Corresponds to the parameter -cap-drop: Drop Linux capabilities . Enter the Capability Key that containers already have by default in this field to delete this permission from containers.

Container Config

Select the stdin check box to enable standard input for containers. Select the tty check box to assign an virtual terminal to send signals to the containers. These two options are usually used together, which indicates to bind the terminal (tty) to the container standard input (stdin). For example, an interactive program obtains standard input from you and then displays the obtained standard input in the terminal.

Port Mapping

Specify the port mapping between host and container, and select TCP or UDP as the protocol. Port mapping is used for the routing between container and host and implements the access to the container from outside.

Port mapping is the prerequisite for the configurations of simple routing and Server Load Balancer routing. The container provides external services by using the configured port mapping.

Web Routing

After a cluster is created in Container Service, the acsrouting application, including the routing service (namely, routing), is created automatically to provide the simple routing function. Each node has a service deployed. In a node, the acsrouting_routing_index container implements the routing forward in the cluster to route the HTTP services or HTTPS services. For more information, see Simple routing - supports HTTP and HTTPS.

Note When exposing HTTP/HTTPS services, the specific host port can be unconfigured. The container port can be accessed directly by using the overlay network or Virtual Private Cloud (VPC).

Load Balancer

Control the routing access path on your own when configuring this parameter, including the routing mapping of Server Load Balancer frontend port > backend host port > container port.

Configure the port mapping in advance. Then, configure the mapping of container_port and \$scheme://\$[slb_name|slb_id]:\$slb_front_port. For more information about the Server Load Balancer labels, see lb.

Data Volume

We recommend that you use data volumes to store the persistent data generated by containers, which is more secure, and easier to manage, back up, and migrate. For more information, see Use volumes.

- Select to create a data volume. Enter the host path or data volume name, the container path, and select RW or RO as the data volume permission.
- Enter the name and permission parameters of another service or container in the volumes_from field. For example, service_name:ro. If the access permission is not specified, the default permission is RW. For more information, see volume compose. After the configuration, containers can be granted to use the data volumes of another service or container.

Environment

Environment variables support the input form of key-value pairs and the formats such as array, dictionary, and boolean. For more information, see environment-variables.

You can configure the relevant environment variables for Docker containers. Environment variables can be used as flags and represent some parameters of environment deployment. You can also use environment variables to pass configurations and build automated deployment scripts.

Labels

Label applies metadata to Docker objects and can be used to build images, record license information, and describe the relationship among containers, data volumes, and network to implement powerful features.

Labels support the input form of key-value pairs and are stored in the format of strings. You can specify multiple labels for containers. The Docker native labels and Label description are supported.

Smooth Upgrade

Select whether or not to **enable** the smooth upgrade. Enabling smooth upgrade is equivalent to adding the label <code>rolling_update=true</code>. Use together with the label probe to make sure the containers can be updated successfully. For more information, seeprobe and Rolling_updates.

Across Multiple Zones

Select Ensure or Try best.

Select **Ensure** to deploy containers in two different zones. With this option selected, the container creation fails if the current cluster does not have two zones or the containers cannot be distributed in two zones because of limited machine resources.

You can also select Try best. Then, Container Service tries to deploy the containers in two different zones. Container can still be created even if the condition cannot be met.

If this parameter is not configured, Container Service deploys the containers in one zone by default. For more information, see High availability scheduling.

Auto Scaling

To meet the demands of applications under different loads, Container Service supports auto scaling for the service, which automatically adjusts the number of containers according to the container resource usage in the service.

For more information, see Container auto scaling.

8.3. Restrict container resources

One advantage of Docker containers is that they allow you to restrict resources, such as CPU, memory, and I/O performance. In swarm clusters, you can restrict the resources for applications.

You can restrict container resources in the Container Service console by setting interface parameters or configuring settings in orchestration templates.

Interface parameters

You can **restrict resources** Change application configurations when Create an application or changing the service configurations.

In swarm clusters, a single CPU core is equivalent to 100 CPUs. The unit of memory is MB.

50	Memory Limit:	512	МВ
----	---------------	-----	----

Orchestration templates

In orchestration templates, you can use the mem_limit and cpu_shares labels to set CPU limit and memory limit.

CPU limit

A single CPU core is equivalent to 100 CPUs. If your machine is configured with 4 cores, the total number of available CPU resources is 400. In orchestration templates, you can use the cpu_shares label to specify CPU limit. cpu_shares: 50 indicates 0.5 core.

Memory limit

You can use the mem_limit label to restrict memory usage. The unit is the byte and the minimum memory is 4 MB. If you set the memory limit and a container applies for a memory that exceeds the limit, the container is stopped because of OOM.

The following orchestration template demonstrates how to restrict CPU and memory.

```
nl:
expose:
    - 443/tcp
    - 80/tcp
image: 'nginx:latest'
cpu_shares: 50 #0.5 core
mem_limit: 536870912 #512MB
labels:
    aliyun.scale: '1'
restart: always
volumes:
    - /var/cache/nginx
```

Resource scheduling

To ensure that containers can obtain sufficient specified resources, such as 0.5 CPU core and 512 MB of memory in the preceding example, Container Service reserves resources for containers. For example, a 4-core machine can schedule up to eight cpu_shares=50 containers. If you create containers without specifying the cpu_shares and mem_limit labels, Container Service does not reserve resources for such containers by default.

Other resource limits

For other resource limits, see Docker Compose instructions.

8.4. High availability scheduling

To make the application have higher availability, Container Service supports scheduling containers of the same service in different zones. When a zone malfunctions, the application can still provide services.

You can specify the zone selection in the orchestration file by using the environment variables in the following formats:

- availability:az==3 : The service must be distributed in at least three zones. The container creation fails if less than three zones are in the current cluster, or the service cannot be distributed in three zones because of limited machine resources.
- availability:az==~3 : Try to distribute the service in three zones. Container can still be created even if the condition cannot be met.

Note The deployment constraint only works for newly created containers. It does not work when containers created in the past change the configurations.

In the following example, the service must be distributed in at least two zones.

```
nnn:
expose:
    - 443/tcp
    - 80/tcp
image: 'nginx:latest'
environment:
    - 'availability:az==2'
labels:
    aliyun.scale: '8'Aliyun. Scale: '8'
restart: always
volumes:
    - /var/cache/nginx-/Var/Cache/nginx
```

8.5. Specified node scheduling

To deploy a service to a specified node, you can use the constraint keyword.

Note The deployment constraint only works for newly created containers. It does not work when existing containers change the configurations.

In the following example, the service is deployed to node1.

```
web:
    image: 'nginx:latest'
    restart: always
    environment:
        - 'constraint:aliyun.node_index==1'
    ports:
        - 80
    labels:
        aliyun.scale: 2
```

Container Service supports the following expressions:

Expression	Description:
constraint:aliyun.node_index==1	Deploy the service to node1.
constraint:aliyun.node_index! =1	Do not deploy the service to node1.
constraint:aliyun.node_index==(1 2 3)	Deploy the service to node1, node2, or node3.
constraint:aliyun.node_index! =(1 2 3)	Deploy the service to a machine other than node1, node2, and node3.
affinity:image==~redis	Try to deploy the service to a machine with a Redis image. The image full name is supported. For example,Supports filling the full name of the mirror, such registry.cn- hangzhou.aliyuncs.com/xxx/xxx 。
affinity:service! =~redis	Try not to deploy the service to a machine with a Redis service. For more information, see Service deployment constraints (affinity:service).

8.6. Schedule an application to specified nodes

To deploy an application to specified nodes, we recommend that you use user tags and the constraint keyword to make the deployment configurations.

? Note

- The deployment constraint only works for newly created containers. It does not work when existing containers change the configurations.
- After you use a user tag to deploy an application, deleting the user tag does not affect the deployed application, but will affect the next deployment of the application. Proceed with caution when deleting user tags.

Procedure

- 1. Add user tags for nodes.
 - i. Log on to the Container Service console.
 - ii. Click Swarm > **Clusters** in the left-side navigation pane.
 - iii. Click Manage at the right of the cluster.

Container Service	Cluster List		Yo	u can create up to 5 clusters	and can add	l up to 20 node:	s in each cluster.	Subaccount A	uthorization	Refresh	Create Cluster
Overview Applications	Help: Create cluster How to add exist	ing ECS instances	Cross-zone node n	nanagement Log Service int	tegration	Connect to clust	er through Doc	ker Client			
Services	Name 💌										
Clusters 1	Cluster Name/ID	Cluster Type	Region	Network Type	Cluster Status	Node Status	Number of Nodes	Time Created	Docker Version 2		Action
Data Volumes Configurations	test c9d5b559d38ee4138b62a682c8166779a	Albaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc- bp1659u1p811058ea3npd	Ready	No node status 😋	2	2017-04-01 09:44:19	17.03.1-ce	Manage	View Logs Delete Monitor More+
 Images and Temp Operation Logs Ξ 	routing-test-online ccf530ee2b1c1400e96425b05846fa35c	Albaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc- bp1659u1p811058ea3npd	Ready	Healthy 🕽	1	2017-03-31 22:32:40	17.03.1-ce	Manage	View Logs Delete Monitor More+
Getting Started											

- iv. Click User Tags in the left-side navigation pane.
- v. Select the nodes that you want to deploy the application and then click Add Tag.

<	Cluster:test
Basic Information	2 stance ID/Name
User Tags	Heri Nomeskavilgen: del Seria 1901 (1911)
List Commer List	Hopi7manthlu44holom Studie City of Ci
Events Node Scaling	Delete Tag Add Tag

vi. Enter your tag key and tag value, and then click **OK** to add user tags for the selected nodes.

AddTags		\times
Tags :	group:1	
	ОК	Close

2. Create an application by clicking Create with Orchestration Template. Configure the constrai

nt keyword in the template.

For information about how to create an application, see Create an application.

```
environment:
    - constraint:group==1 #Indicates to deploy the application on all the nodes with the
"group:1" tag
```

Delete a user tag

- 1. Log on to the Container Service console.
- 2. Click Swarm > Clusters in the left-side navigation pane.
- 3. Click Manage at the right of the cluster.

Container Service	Cluster List		Yo	u can create up to 5 clusters	and can add	d up to 20 node:	s in each cluster.	Subaccount Au	thorization	Refresh	Create Cluster
Overview	Help: Create cluster How to add exist	ing ECS instances	Cross-zone node r	nanagement Log Service int	egration	Connect to clust	er through Dock	ker Client			
Services	Name										
Clusters 1	Cluster Name/ID	Cluster Type	Region	Network Type	Cluster Status	Node Status Ø	Number of Nodes	Time Created	Docker Version 2		Action
Data Volumes	test c9d5b559d38ee4138b62a682c8166779a	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc- bp1659u1p811058ea3npd	Ready	No node status 🛢	2	2017-04-01 09:44:19	17.03.1-ce	Manage	View Logs Delete Monitor More≁
 Images and Temp Operation Logs 	routing-test-online ccf530ee2b1c1400e96425b05846fa35c	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc- bp1659u1p811058ea3npd	Ready	Healthy 🗢	1	2017-03-31 22:32:40	17.03.1-ce	Manage	View Logs Delete Monitor More+
Getting Started											

- 4. Click User Tags in the left-side navigation pane.
- 5. Select the nodes that you want to delete the user tags and then click Delete Tag.

<	Clusteritest	Refresh
Basic Information		
Load Balancer Set	User Tags	
User Tags	Portan (group:1	
Container List	Pop1. group:1	
Events Node Scaling	Delete Tag Add Tag	

6. The confirmation dialog box appears. Click OK.



8.7. View application details

Procedure

- 1. Log on to the Container Service console.
- 2. Click **Applications** in the left-side navigation pane.
- 3. Select the cluster in which the application you want to view resides from the Cluster list.
- 4. Click the application name.

Container Service	Application List						Refresh Create Application		
Kubernetes Swarm	Help: & Create 2 lication & C	hange application configura	itions 🔗 Simple route b	lue-green release policy 🔗 C	Container auto scaling		Application list updated. \times		
Applications 1	Cluster: 🔹 test-swarm 💌 🗹 Hide S	Cluster: test-swarm 🔹 🗹 Hide System Applications 🔲 Hide Offline Applications 🔛 Hide Online Applications 🔍 Name 💌							
Services	Name Description	Status	Container Status	Time Created 🔺	Time Updated 🔺		Action		
Clusters	wordpress-test	Ready	Ready:1 Stop:0	06/15/2018,14:34:17	06/15/2018,14:34:17	Stop Up	date Delete Redeploy Events		

5. Click the Services tab to view the services of the application.

Services	Containers	Logs	Events	Routes			
Name	Application	Status	Cont	ainer Status	Image		Action
db	test	Ready	Read Stop:	y:1	registry.aliyuncs.com/acs-sample/mysql:5.7	Stop Restart	Reschedule Update Delete Events
web	test	Ready	Read Stop:	y:3	registry.aliyuncs.com/acs-sample/wordpress:4.5	Stop Restart	Reschedule Update Delete Events

6. Click the **Containers** tab to view the containers of the application.

				Routes	ogs Events	ers Lo	Services Contain
Action	Node IP	Container IP	Port	Image	Health Check	Status	Name/ID
Delete Stop Monitor Logs Web Terminal	172.16.33.	172.18.7.4	3306/tcp	al registry.aliyunc sha256:ec7e75e52		running	test_db_1 () c1421187a96e6659
Delete Stop Monitor Logs Web Terminal	172.16.33.	172.18.6.5	172.16.33.29:32769- >80/tcp	registry.aliyunc sha256:592af506c	Normal	running	test_web_1 () 46453dfc49d9e056

7. Click the Logs tab to view the logs of the application.

Services Containers Logs Events	Routes
Entries Per Container: 100items •	Filter by Container Name: All Filter by Start Time: Download Logs
test_web_1 2017-11-14T08:23:02.2090798 test_web_1 2017-11-14T08:23:05.4046282 test_web_1 2017-11-14T08:23:08.6335903 test_web_1 2017-11-14T08:23:12.9051066 test_web_1 2017-11-14T08:23:16.0845859 test_web_1 2017-11-14T08:23:19.2589918 test_web_1 2017-11-14T08:23:22.4481633	<pre>552 172.17.0.1 - [14/Nov/2017:16:23:02 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" "Go-http-client/1.1" 1072 172.17.0.1 - [14/Nov/2017:16:23:08 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" "Go-http-client/1.1" 1022 172.17.0.1 - [14/Nov/2017:16:23:12 +0800] "GET /license.txt HTTP/1.1" 200 7603 "- "Go-http-client/1.1" 1032 172.17.0.1 - [14/Nov/2017:16:23:12 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" "Go-http-client/1.1" 1032 172.17.0.1 - [14/Nov/2017:16:23:12 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" "Go-http-client/1.1" 1032 172.17.0.1 - [14/Nov/2017:16:23:14 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" "Go-http-client/1.1" 1052 172.17.0.1 - [14/Nov/2017:16:23:19 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" "Go-http-client/1.1" 1052 172.17.0.1 - [14/Nov/2017:16:23:22 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" "Go-http-client/1.1" 1052 172.17.0.1 - [14/Nov/2017:16:23:22 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" "Go-http-client/1.1" 1052 172.17.0.1 - [14/Nov/2017:16:23:22 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" "Go-http-client/1.1" 1052 172.17.0.1 - [14/Nov/2017:16:23:22 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" "Go-http-client/1.1" 1052 172.17.0.1 - [14/Nov/2017:16:23:22 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" "Go-http-client/1.1" 1052 172.17.0.1 - [14/Nov/2017:16:23:22 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" "Go-http-client/1.1" 1052 172.17.0.1 - [14/Nov/2017:16:23:22 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" "Go-http-client/1.1" 1052 172.17.0.1 - [14/Nov/2017:16:23:22 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" "Go-http-client/1.1" 1052 172.17.0.1 - [14/Nov/2017:16:23:22 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" "Go-http-client/1.1" 1052 172.17.0.1 - [14/Nov/2017:16:23:22 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" "Go-http-client/1.1" 1052 172.17.0.1 - [14/Nov/2017:16:23:22 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" "Go-http-client/1.1"</pre>

8. Click the **Events** tab to view the events of the application.

Services	Containers	Logs	Events	Routes
© 2017-11-14	4 15:55:11			
Create servic	ce test_web cor	npleted.		
C 2017-11-14	4 15:55:11			
Activate cont	tainer test_web	_3 succee	ded.	
C 2017-11-14	4 15:55:11			
Create applic	cation test com	pleted.		

9. Click the **Routes** tab to view the route address of the application.

Services	Containers	Logs	Events	Routes
Route Addres	SS			
wordpress.c8	8b2da019b32e48	Bedb11213	17a9c02d81.0	cn-hangzhou.

8.8. Stop or activate an application

Context

Procedure

- 1. Log on to the Container Service console.
- 2. Click Swarm > **Applications** in the left-side navigation pane.
- 3. Select the cluster in which the application you want to stop or activate resides from the Cluster drop-down list.
- 4. Activate or stop the application according to the status.

Click Activate at the right of the application that you want to activate.

Container Service	Application List						Refresh	Create Application	
Overview	Help: 🖉 Create an appli	cation & Change application co	nfigurations 🔗 Simpl	le route blue-green rele	ase policy 🔗 Container auto	scaling			
Applications	Cluster: test-swarm 🔻	Suster: test-swarm 🔻 🗷 Hide System Applications 🗉 Hide Offline Applications 📾 Hide Online Applications 🛛 Name 🔻							
Services	Name	Description	Status	Container Status	Time Created 🔺	Time Updated 🔺		Action	
Clusters Nodes	nginx		Stopped	Ready:0 Stop:1	06/06/2018,15:52:54	06/06/2018,19:10:39	Activate	Update Delete Redeploy Events	

Click **Stop** at the right of the application that you want to stop.

Container Service	Application List	oplication List								
Overview	Help: 🖉 Create an ap	Help: Ø Create an application 🖉 Change application configurations 🖉 Simple route blue-green release policy 🖉 Container auto scaling								
Applications	Cluster: test-swarm v 🕷 Hide System Applications 🗉 Hide Offline Applications 📾 Hide Online Applications 🛛 Name v							Q X		
Services	Name	Description	Status	Container Status	Time Created 🔺	Time Updated 🔺		Action		
Clusters Nodes	nginx		Ready	Ready:1 Stop:0	06/06/2018,15:52:54	06/06/2018,19:41:00	Stop	Update Delete Redeploy Events		

5. In the displayed dialog box, click OK.

8.9. Change application configurations

Procedure

- 1. Log on to the Container Service console.
- 2. Click **Applications** in the left-side navigation pane.
- 3. Select the cluster where the application you want to change configurations resides from the Cluster list.
- 4. Click **Update** at the right of the application you want to change configurations.

Container	Service	Application List						Refresh Create Application
Kubernetes	Swarm							Application list under all a
Overview		Help: Ø' Creat	tion & Change application co	onfigurations & Simple rou	te blue-green release policy	Ontainer auto scaling		Application ist updated.
Applications	- 1	Cluster: test-swarm 🔻	Hide System Applications	Hide Offline Applications	Hide Online Application	s	Name 🔻	Q
Services		Name Description	Status	Container Status	Time Created 🔺	Time Updated 🔺		Action
Clusters		test	Ready	Ready:1 Stop:0	06/15/2018,14:45:37	06/15/2018,14:45:37	Stop	Update Delete Redeploy Events
Nodes								

5. The Change Configuration dialog box opens. Modify the configurations.

Note You must update the **Version**. Otherwise, the **OK** button is not available.

• \: By default, to avoid losing the container data in the local data volume on the current machine, Container Service restarts the container or recreates a container on the current machine when you change the application configurations. To schedule the container to another machine, turn on the Force Reschedule switch. Then, Container Service schedules the container to another machine according to your scheduling settings in the Template.

Note After scheduling the container to another machine by turning on the Force Reschedule switch, the container data in the local data volume on the former machine are lost. So proceed with caution. So proceed with caution.

• Use Existing Orchestration Template: Click Use Existing Orchestration Template to select a template to change the application configurations. A confirmation dialog box opens. Click Confirm.

Note The new template will overwrite the current template. Click OK in the Change Configuration dialog box.

hange Configura	tion	
Name:	test	
*Version:	1.0 Note: The version of the application must be changed; otherwise, the "OK" button is not available.	
Description:		
Use Latest Image:	Force O C Reschedule :	
Release Mode:	Blue-Green Release 🔻 🕖	
Template:	<pre>1 / web: 2 image: registry.aliyuncs.com/acs-sample/wordpress:4.5 3 ports: 4 - '80' 5 environment: 6 WORDPRESS_AUTH_KEY: changeme 7 WORDPRESS_SECURE_AUTH_KEY: changeme 8 WORDPRESS_LOGGED_IN_KEY: changeme 9 WORDPRESS_LOGGED_IN_KEY: changeme 10 WORDPRESS_LOGGED_IN_SALT: changeme 11 WORDPRESS_SECURE_AUTH_SALT: changeme 12 WORDPRESS_SECURE_AUTH_SALT: changeme 13 WORDPRESS_NONCE_SALT: changeme 14 WORDPRESS_NONCE_AA: changeme 15 restart: always 16 links: 17 - 'db:mysql'</pre>	
	Use Existing Orchestration Template Label description	
	OK Ca	incel

What's next

If the application is not updated after you change the configurations, you can redeploy the application to apply the configuration modifications. For more information, see Redeploy an application.

8.10. Redeploy an application

You can redeploy an application after deploying it, if necessary. Redeploying an application re-pulls the image used by the application. Therefore, if you update the application image after deploying the application, redeployment will use the updated image to deploy the application.

? Note Redeployment does not update the data volume, which means the old data volume of the host is still used. Therefore, if you mount a data volume to the host and change the configurations of the data volume in the new image, the new configurations will not take effect after the redeployment.

You must redeploy an application in the following situations:

- You update the image after deploying the application and want to deploy the application according to the updated image.
- You stop or delete some containers and want to activate or recreate those containers. During the redeployment, Container Service activates the stopped containers and recreates the deleted containers.

Procedure

- 1. Log on to the Container Service console.
- 2. Click Swarm > **Applications** in the left-side navigation pane.
- 3. Select the cluster where the application you want to redeploy resides from the Cluster drop-down list.
- 4. Click **Redeploy** at the right of the application you want to redeploy.

Container	Service	Application	List						Refresh	Create Application
Kubernetes Overview	Swarm	Help: & Cre	at 2 plication	& Change application o						
Applications	1	Cluster: tes	t-swarm 🔻 🗹 H	ide System Applications	Hide Offline Applications	Hide Online Applications		Name 🔻		Q X
Services		Name	Description	Status	Container Status	Time Created 🔺	Time Updated 🔺			3 Action
Clusters		nginx-test		Ready	Ready:1 Stop:0	06/15/2018,14:54:41	06/15/2018,14:54:41	Stop	Update Dele	te Redeploy Events

5. A confirmation dialog box appears. Click OK.

Check whether the redeployment succeeds

To confirm whether the redeployment is successful or not, view the image sha256 to check whether the container image after the redeployment is the latest one.

- 1. Log on to the Container Service console.
- 2. Click Swarm > **Applications** in the left-side navigation pane.
- 3. Select the cluster where the redeployed application resides from the Cluster drop-down list.
- 4. Click the application name.

Container Service	Application List					Refresh	Create Application
Kubernetes Swarm	Help: & Creat 2 pplication	& Change application cor					
Applications 1	Cluster: test-swarm 🔻	Hide System Applications	Hide Offline Applications	Hide Online Applications		Name 🔻	Q X
Services	Name Description	Status	Container Status	Time Created 🔺	Time Updated 🔺		Action
Clusters	nginx-test 3	Ready	Ready:1 Stop:0	06/15/2018,14:54:41	06/15/2018,14:54:41	Stop Update	Delete Redeploy Events

5. Click the Containers tab to view the image sha256.

The redeployment is successful if the container image is the latest one.

Services	Containers	Logs	Events	Routes					
Name/ID		Status	Healt	h Check	Image	Port	Container IP	Node IP	Action
nginx_ngin 486ab82dc	x_1 ⓓ :d5efb32	running	Norm	al	nginx:latest sha256:5e69fe4b3 <	ha256:5e69fe4	lb3c310ea B	172.	Delete Stop Monitor Logs Web Terminal

8.11. Delete an application

Context

You can delete applications that will not be used.

Procedure

- 1. Log on to the Container Service console.
- 2. Click **Applications** in the left-side navigation pane.
- 3. Select the cluster where the application you want to delete resides from the Cluster list.
- 4. Click **Delete** at the right of the application you want to delete.

Container	Service	Application List	Application List							
Kubernetes	Swarm	Help: @ Creat 2 holicat	on A Change application of	infigurations 🔊 Simple rou	ite blue-areen release noticu	& Container auto scaling		Applicat	tion list updated	1. ×
Overview						Container dato scannig				
Applications		Cluster: test-swarm •	Hide System Applications	Hide Offline Applications	Hide Unline Application:	5	Name V		L L	×
Services		Name Description	Status	Container Status	Time Created 🔺	Time Updated 🔺			3	Action
Clusters		test	Ready	Ready:1 Stop:0	06/15/2018,15:10:59	06/15/2018,15:10:59	Stop	Update D	elete Red	eploy Events

5. A confirmation dialog box opens. Click OK.

Select the **Remove the Data Volumes (volume)** check box to delete all the data volumes related to this application. The named data volumes cannot be deleted.



8.12. Run offline tasks

Container Service abstracts the basic model of offline computing and provides the offline computing function based on Docker containers.

The core functions include:

- Job orchestration
- Job scheduling and lifecycle management

• Integration of storage and other functions

Basic concepts

The following table compares the concepts of offline applications with those of online applications.

Concept	Offline application	Online application
Container	Task execution unit	Service execution unit
Operation history	Execution history of tasks that encountered an error and were re-executed	None
Service (Task)	A special function that can be divided into several containers for execution	A group of containers with the same functions
Application (Job)	A combination of several tasks	A combination of several services

In a word, an offline job contains several tasks. Each task can be executed by several containers. Each container can have multiple operation histories. By contrast, an online application contains several services and each service can be provided by several containers simultaneously.

Docker Compose-based job orchestration

Similar to online applications, Docker Compose can be used to describe and orchestrate jobs. Docker Compose supports the vast majority of Docker functions, such as:

- CPU, memory, and other resource limits
- Dat a volumes
- Environment variables and labels
- Network models and port exposure

In addition, Alibaba Cloud Container Service has expanded the following functions:

- Container quantity: The number of containers that each task is divided into.
- Number of retries: The number of retries made by each container.
- Remove containers: Whether or not to delete a container after it has completed its run. You can select the following policies: remove-finished (deletes the container after it completes its run), remove-failed (deletes the container that fails the run), remove-all (deletes all of the containers), and remove-none (does not delete any container).
- DAG model task dependencies: Tasks in a job can have dependencies between each other. Tasks that others depend on are executed first.

The following is an example of offline job Docker Compose.

```
version: "2"
labels:
 aliyun.project type: "batch"
services:
  s1:
   image: registry.aliyuncs.com/jimmycmh/testret:latest
   restart: no
   cpu shares: 10
   mem limit: 10000000
   labels:
     aliyun.scale: "10"
     aliyun.retry count: "20"
     aliyun.remove containers: "remove-all"
  s2:
   image: registry.aliyuncs.com/jimmycmh/testret:latest
    cpu shares: 50
   mem limit: 10000000
   labels:
     aliyun.scale: "4"
     aliyun.retry_count: "20"
     aliyun.remove containers: "remove-finished"
     aliyun.depends: "s1"
```

Note:

- Only Docker Compose 2.0 is supported.
- Add the label aligun.project_type: "batch" at the job level. If this label is not added or its value is not batch , the application is considered as an online application.
- Any value of restart will be changed to no .
- Use the aligun.depends label to specify dependencies. A task can depend on several other tasks. Separate the tasks by using commas (,).
- The default value of aligun.retry_count is 3.
- The default value of aligun.remove_containers is remove-finished .

Job lifecycle management

The container status is determined by the container running and exit status. The task status is determined by the statuses of all the containers in the task. The job status is determined by the statuses of all the tasks in the job.

Container status

- Running: The container is running.
- Finished: The container exits and ExitCode==0 .
- Failed: The container exits and ExitCode!=0.

Task status

- Running: A container is running.
- Finished: All containers are finished.
- Failed: The number of failures of a container exceeds the set value.

Job status

- Running: A task is running.
- Finished: All tasks are finished.
- Failed: A task failed.

The preceding statuses can all be retrieved by means of API to facilitate automated Operation and Maintenance(O&M).

Shared storage

Data is shared and exchanged between containers and tasks. Shared storage can be used to resolve this issue. For example, when running an MR job on Hadoop, HDFS is used for data exchange. In Container Service, two types of shared storage can be used. Their features and application scenarios are compared as follows:

Storage	Advantages	Disadvantages	Scope
OSSFS data volumes	Cross-host sharing.	Low read/write and ls performance. Modifying a file causes the file to be overwritten.	Shared configuration files. Attachment upload.
NAS data volumes	Cross-host sharing; On- demand capacity expansion; high performance, high reliability; high Mount speed	Slightly higher cost	Heavy lo applications that need to share data, such as file servers, etc; heavy lo applications that require rapid migration, such as databases, etc.
A third-party storage integrated by you, such as Portworx	Virtualize the cloud disks in the cluster into a large shared disk. High performance. Snapshots, multiple copies.	Certain O&M capabilities are required.	I/O-intensive applications that need data sharing, such as file servers. I/O- intensive applications that need fast migration, such as databases.

For more information about how to use the data volumes, see the following documents:

- Create an OSSFS data volume
- Creating NAS data volumes
- Use OSSFS data volumes to share WordPress attachments

Integrate with Log Service and CloudMonitor

Log and monitoring are important tools used to analyze offline jobs. Alibaba Cloud Container Service integrates with the CloudMonitor function. Adding a label in the orchestration template can collect CPU, memory, and other data of containers to CloudMonitor. For more information, see the following documents:

- Enable Log Service
- Container monitoring service

Procedure

1. Log on to the Container Service console and create a cluster.

For more information, see Create a cluster.

- 2. Click **Applications** in the left-side navigation pane and then click **Create Application** in the upper-right corner.
- 3. Complete the basic information for the application and then click **Create with Orchestration Template**.
- 4. Use the preceding orchestration template and then click Create and Deploy.
- 5. On the **Application List** page, click the application name to view the application running status.

8.13. Timing tasks

Having a timing task is a common requirement. Generally, select one or more machines and realize the timing tasks by using crontab. However, for large-scale or a large number of timing tasks, this method has many limits such as:

- Low reliability. If one machine goes down, all the timing tasks on this machine cannot be executed.
- No scheduling function. Loads among machines might not be balanced.
- No retry mechanism. Tasks might fail to be run.
- Cannot run large-scale distributed tasks.

On the basis of the offline tasks, Container Service provides the function of timing tasks, with which you can solve the preceding problems by some simple descriptions. For more information on offline tasks, see Run offline tasks.

Note You can only use this function if you have upgraded your Agent since October 25th,
 2016 or the cluster is newly created.

Timing task description based on Docker Compose

The same as offline tasks, timing tasks are also based on Docker Compose. You can realize the timing function by adding the aligun.schedule label in the orchestration template. The following example shows.

? Note When you create or update a timing task, the system will not pull the latest image. This is because using the latest image will make the same task use different images at different time, which might cause your troubleshooting complicated. We recommend that you update your timing task image by updating the image tag.

Container Service

```
version: "2"
labels:
    aliyun.project_type: "batch"
    aliyun.schedule: "0-59/30 * * * * *"
services:
    sl:
    image: registry.aliyuncs.com/jimmycmh/busybox:latest
    labels:
        aliyun.scale: "5"
        aliyun.scale: "5"
        aliyun.retry_count: "3"
        aliyun.remove_containers: "remove-all"
        command: date
```

Note:

- aligun.schedule: "0-59/30 * * * * * " indicates running this task every 30 seconds. The format of schedule is the same as that of crontab (but note that the format of schedule is second minute hour day month week, and that of crontab on Linux is minute hour day month week) and uses Beijing time.
- The timing function is only applicable to offline tasks. Therefore, the system automatically adds the aliyun.project_type: "batch" label after you add the aliyun.schedule label. So the aliyun .project_type: "batch" label in the preceding example can be omitted.
- In addition, all the functions in offline tasks can still be used in timing tasks (for example, scale, retry_count, remove_containers). For the specific meanings of these labels, see Run offline tasks.

Execution process

After a timing task is created, the application is in the status of Waiting. When the specified time of the task is reached, the task is started. The subsequent status changes are the same as the offline applications. The application status repeats this process when the next execution time is reached.

For the same timing task, only a single instance can be executed at a time. If the task execution time is longer than the task execution period (for example, the execution time of the preceding task is longer than 30s), the next execution enters the execution queue. When the length of the execution queue is greater than 3, this execution will be discarded.

You can click the History tab on the application details page to view the execution history and results. Only the last 10 items of execution history are kept in the list.

Services	Containers	Logs	Events	Routes	History]	
Name	S	Status:				Start	Finished
test	•	Comple	te			2017-12-11 19:06:30	2017-12-11 19:06:40
test	•	Comple	te			2017-12-11 19:07:00	2017-12-11 19:07:10
test	•	Comple	te			2017-12-11 19:07:30	2017-12-11 19:07:40
test	•	Comple	te			2017-12-11 19:08:00	2017-12-11 19:08:10
test	•	Comple	te			2017-12-11 19:08:30	2017-12-11 19:08:41
test	•	Comple	te			2017-12-11 19:09:00	2017-12-11 19:09:10
test	•	Comple	te			2017-12-11 19:09:30	2017-12-11 19:09:40
test	•	Comple	te			2017-12-11 19:10:00	2017-12-11 19:10:10
test	•	Comple	te			2017-12-11 19:10:30	2017-12-11 19:10:40
test		Comple	te			2017-12-11 19:11:00	2017-12-11 19:11:10

High availability

The timing task controller adopts the master-slave mode. The control function is switched to the slave controller when the master controller malfunctions.

If the task execution time is in the master-slave switch period, the task will be executed until the switch is completed. If the task needs to be run for several times in the master-slave switch period, the task will be executed only once after the switch is completed. Therefore, to ensure that the task is not lost, do not design tasks with a repetition period less than one minute.

8.14. Default system application list

Application name	Chinese name	Services contained	Brief introduction
acsrouting	acsrouting	routing	Provides the request routing service with layer-7 protocol, which consists of Server Load Balancer and an HAProxy container. After the domain name is correctly configured, the request can be sent to the specified container.
acslogging	acslogging	logtail, logspout	Integrates with Alibaba Cloud Log Service to upload the logs printed by applications in containers to Alibaba Cloud Log Service for storage, facilitating you to query and analyze the logs. For how to use acsmonitoring, see Enable Log Service.
acsmonitoring	Monitoring service	acs-monitoring-agent	Integrates with Alibaba Cloud CloudMonitor and currently popular third- party open-sourced monitoring frameworks, facilitating you to query the monitoring information and configure the monitoring alarms. For how to use acsmonitoring, see Container monitoring service.

Application name	Chinese name	Services contained	Brief introduction
acsvolumedriver	Data volume	volumedriver	Integrates with Alibaba Cloud CloudMonitor and currently popular third- party open-sourced monitoring frameworks, facilitating you to query the monitoring information and configure the monitoring alarms. For how to use acsmonitoring, see Container monitoring service.

9.Configurations 9.1. Create a configuration

Context

Container Service supports creating configurations and transmitting the configurations by configuring the parameters, which facilitates you to manage multiple container environment variables.

Limit s

- You can only select a region of an existing cluster when creating a configuration.
- The configuration creation fails and the system reports an error if clusters in the selected region do not have any nodes.
- You cannot view the configurations in a region on the Configuration File List page if clusters in the region are all deleted or do not have any nodes. You can view the configurations in the region on the Configuration File List page when a cluster in the region contains nodes.

Procedure

- 1. Log on to the Container Service console.
- 2. Click Swarm > Configurations in the left-side navigation pane.
- 3. Select the region where you want to create a configuration from the Region drop-down list and then click **Create** in the upper-right corner.

Container Service		Configuration File List Refresh		Create	ſ
Kubernetes	Swarm			3	
Overview		Region: China East 1 (Hangzhou) 🔻 2			
Applications					
Services		Configuration File Name Description		Operation	
Clusters		CONCOURSE_EXTERNAL_URL Dele	ite	Modify	
Nodes		Note: If the selected region contains no cluster, the configuration files of this region will not be displayed; these files will be displayed once a cluster is created under this region. The maximum number of allowed is 50.	configur	ation files	
Networks					
Data Volum	es				
Configuratio	ins 1				

- 4. Enter the configuration file information and click OK.
 - File Name: It can contain 1-32 characters.
 - **Description**: It can contain up to 128 characters.
 - **Configuration**: You can add up to 50 configurations in a region. Enter the **Variable Name** and **Variable Value**, and then click **Add** on the right.

You can also click **Edit JSON File**. The JSON Format dialog box appears. Enter the configurations in the dialog box and click **OK**.
Configuration File				
	* File Name:	test	and the set of the DD shares to	
	Description:	The configuration file	name should contain 1 to 32 characte	15.
		The description can c	ontain up to 128 characters.	
	Configuration:	Edit JSON File		
		Variable Name	Variable Value	Action
		scale_number	3	Edit Delete
		parallelism_number	1	Add
		The variable key shou to 128 characters. Th value cannot be empl	uld contain 1 to 32 characters; the varia le variable value must be unique. The v ty.	able value should contain 1 variable name and variable
			OK Cancel	

In this example, the variables <code>scale_number</code> and <code>parallelism_number</code> are set, which are used to pass the parameters of the Alibaba Cloud extension labels <code>scale</code> and <code>rolling_updates</code> respectively.

9.2. Modify configurations

Context

You can modify the configurations of a configuration file.

Onte Modifying the configuration file affects applications that use this file.

Procedure

- 1. Log on to the Container Service console.
- 2. Click Swarm > Configurations in the left-side navigation pane.
- 3. On the Configuration File List page, select a region from the Region drop-down list.
- 4. Click Modify at the right of the configuration that you want to modify.

Container	Service	Configuration File List	Refresh Create
Kubernetes	Swarm		
Overview		Region: China East 1 (Hangzhou) 🔻	
Applications		Configuration File Name Description	00.3
Services			Delay I Martin
Clusters		rest_cound	Delete
Nodes		Note: If the selected region contains no cluster, the configuration files of this region will not be displayed; these files will be displayed once a cluster is created under this region. The maxin allowed is 50.	um number of configuration files
Networks			
Data Volum	es		
Configuratio	ns 🚺		

5. Click **Confirm** in the displayed dialog box.

Confirm	ation ×
0	Modifying the configuration file will affect applications associated wi th this file. Do you want to continue?
	Confirm Cancel

- 6. Modify the configurations.
 - Click Edit at the right of the configuration you want to modify. Update the configuration and then click Save.
 - You can also click Edit JSON File. Click OK after making the modifications.

Configuration File			
* File Name:	size		
Description:			
	The description can a	contain up to 130 characters	
Configuration:	Edit JSON File	ontain up to 128 characters.	
	Variable Name	Variable Value	Action
	size	2	Edit Delete
	Name	Value	Add
	The variable key sho to 128 characters. Th value cannot be emp	uld contain 1 to 32 characters; the variable variable value must be unique. The var ty.	le value should contain 1 iable name and variable
		OK Cancel	

7. After modifying the configurations, click **OK**.

9.3. Implement multiple environments by using configurations

An application consists of codes and configurations. After an application is containerized, the configurations are usually transmitted by using container environment variables to deploy multiple applications using the same image and different configurations.

Limits

- When associating a configuration file with an application, make sure the configuration file is in the same region as the application.
- Currently, associating a configuration file when creating an application is only available when you create the application by using an orchestration template.

Create an application

- 1. Log on to the Container Service console.
- 2. Under Swarm, click **Configurations** in the left-side navigation pane. Select the region in which you want to create a configuration from the Region list and click **Create**.

Container Service	Configuration File List	Refresh Create
Overview		3
Applications	Report: China Last 1 (Hangdrou)	
Services	Configuration File Name Description	Operation
Clusters	Note: If the selected region contains no cluster, the configuration files of this region will not be displayed; these files will be displayed once a cluster is created under this region. The maximum number of configuration files allowed is 50.	
Nodes		
Networks		
Data Volumes		
Configurations		
 Images and Templates 		
Operation Logs		
Getting Started		

- 3. Complete the settings and then click **OK**.
 - File Name: It can contain 1-32 characters.
 - **Description**: It can contain up to 128 characters.
 - **Configuration**: You can add up to 50 configurations in a region.

In this example, the size variable is set.

* File Name:	test-group				
	The configuration file nan	ne should contain 1 to 32 characters.			
Description:	test group				
	The description can conta	in up to 128 characters.			
Configuration:	Edit JSON File				
	Variable Name	Variable Value	Action		
	size	2	Edit Delete		
	Name	Value	Add		
The variable key should contain 1 to 32 characters; the variable value should contain 1 to 128 characters. The variable value must be unique. The variable name and variable value cannot be empty.					
		OK Cancel			

- 4. Under Swarm, click **Applications** in the left-side navigation pane. Select the cluster in the same region as the created configuration from the Cluster list and click **Create Application**.
- 5. Enter the basic information of the application and click **Create with Orchestration Template**.
- 6. Enter the following orchestration template and then click Create and Deploy.

Wherein, size is a dynamic variable and will be overwritten by the value in the configuration.



7. The dialog box appears. Select the configuration file to be associated with from the **Associated Configuration File** drop-down list. Click Replace Variable and click **OK**.

Template Parameter X							
	Associated Configu	ration File:					
	Parameter	Value	Contrast				
	size		Miss				
	Description: Same The selected values are the sam Diff The selected values are different Miss The selected	ed configuration file contains this variable and e. configuration file contains this variable but th t. d configuration file does not contain this varial	the variable e variable ble.				
		Replace Variable OK	Cancel				

Update an application

If you associated a configuration file when creating an application, you can update the application by modifying the configuration file and redeploying the application.

- 1. Log on to the Container Service console.
- 2. Under Swarm, click **Configurations** in the left-side navigation pane. Select the region in which the configuration you want to modify resides from the Region list, and click **Modify** at the right of the configuration.

Overview	Region: China East 1 (Hangzhou) 🔻		
Applications		2	
Services	Configuration File Name	Description	3 Operation
Clusters	test-group	test group	Delete Modify
Nodes	Note: If the selected region contains no cluster	; the configuration files of this region will not be displayed; these files will be displayed once a cluster is creat	ated under this region. The maximum number of configuration
Networks	Tiles allowed is 50.		
Data Volu			
Configurations =			

- 3. Click **Confirm** in the displayed dialog box.
- 4. Click Edit (changes to Save after you click it) at the right of the variable you want to modify. Modify the variable value. Click Save and then click OK.

* File Name:	test- group		
Description:	test group		
	The description can cor	ntain up to 128 characters.	
Configuration:	Edit JSON File		
	Variable Name	Variable Value	Action
	size	3	Save Delete
	Name	Value	Add
	The variable key should to 128 characters. The value cannot be empty.	l contain 1 to 32 characters; the variable value should variable value must be unique. The variable name and	contain 1 variable
		OK Cancel	

5. Under Swarm, click **Applications** in the left-side navigation pane. Select the cluster in the same region as the created configuration, and then click **Redeploy** at the right of the application.

Container Service	Application List					Re	fresh	Create Application
Overview	Helper: Create application Change a	application configuration Simple route blue	-green release policy Container auto	scaling				
Applications	Custer: test 💽 🕅 Hide system applications 🛙 Hide offine applications							
Clusters	Name Description	Status	Container status	Time Created 🔺	Time Updated 🔺			3 Action
Nodes	test	Ready	Ready:2 Stop:0	2016-12-29 19:08:08	2016-12-29 19:29:57	Stop Update	Delete	Redeploy Events

After the application is updated, the number of containers changes to three.

Cluster:	test 💌 🗹 Hide syst	em applications 🔲 Hide offine application	B Hide online applications			Name 💌
Name	Description	Status	Container status	Time Created 🔺	Time Updated 🔺	Action
test		Ready	Ready:3 Stop:0	2016-12-29 19:08:08	2016-12-29 20:05:47	Stop Update Delete Redeploy Events

Trigger an update

If you associated a configuration file when creating an application, you can redeploy the application by using the redeployment trigger.

- 1. Log on to the Container Service console.
- 2. Under Swarm, click **Configurations** in the left-side navigation pane. Select the region in which the configuration you want to modify resides from the Region list, and click **Modify** at the right of the configuration.

Overview	Region: China East 1 (Hangzhou) 🔻		
Applications			
Services	Configuration File Name	Description	3 Operation
Clusters	test-group	test group	Delete Modify
Nodes	Note: If the selected region contains no cluster, the	configuration files of this region will not be displayed; these files will be displayed once a cluster is o	reated under this region. The maximum number of configuration
Networks	files allowed is 50.		
Data Volu			
Configurations			

- 3. Click **Confirm** in the displayed dialog box.
- 4. Click Edit (changes to Save after you click it) at the right of the variable you want to modify. Modify the variable value. Click Save and then click OK.

* File Name:	test- group		
Description:	test group		
	The description can conta	ain up to 128 characters.	/2
Configuration:	Edit JSON File		
	Variable Name	Variable Value	Action
	size	3	Save Delete
	Name	Value	Add
	The variable key should on to 128 characters. The variable value cannot be empty.	contain 1 to 32 characters; the variable value should c ariable value must be unique. The variable name and	ontain 1 variable
		OK Cancel	

5. Create a redeployment trigger.

For how to create a trigger, see Triggers.

Trigger 1	frigger 1. You can only have one of each trogger type®										^
Trigger link ((move mouse ov	er to copy)					Secret (move mouse over to copy)	Туре	Action		
https://und	efined/hook/trigg	ger?triggerUr	-Y2IwMm	NjZmI5YjU5M	IzQ5YWVhNDU4ZGMwYmE4MGQw		Redeploy	Delete trig	iger		
Services	Containers	Routes	Logs	Events							
Name	Application Status Container status Image								Action		
busybox	ox test Ready Ready:3 busybocitest				Stop Restart	Resched	ule Updat Delete Ev	te i vents			

6. Initiate the redeployment trigger.

curl	"https://cs.console.aliyun.com/hook/trigger?triggerUrl=Y2ViZDhkZTIwZGMyMjRmOTM4NDI
zMTgv	wMzI3NmIwM2IxfHRlc3QtZ3JvdXB8c2NhbGluZ3wxOXZwYzNmOXFiNTcwfA==&secret=46624237677565
4951	546d6451656a7a66e7f5b61db6885f8d15aa64826672c2"

After the application is updated, the number of containers changes to three.

Cluster:	test 💌 🗹 Hide sy	stem applications 🔲 Hide offi	ne applications 🔲 Hide online applications			Name 💌
Name	Description	Status	Container status	Time Created 🗢	Time Updated 🔺	Action
test		Ready	Ready:3 Stop:0	2016-12-29 19:08:08	2016-12-29 20:05:47	Stop Update Delete Redeploy Events

9.4. Delete a configuration

Context

You can delete a configuration that is no longer in use.

Procedure

- 1. Log on to the Container Service console.
- 2. Click **Configuration**s in the left-side navigation pane.
- 3. On the Configuration File List page, select a region from the Region list.
- 4. Click **Delete** at the right of the configuration that you want to delete.

Container	Service	Configuration File List	Refresh	Create
Kubernetes	Swarm			
Overview		Region: China East 1 (Hangzhou) 🔹 2		
Applications		Configuration File Name Description	3 0	peration
Clusters		test_config	Delete	Modify
Nodes		Note: If the selected region contains no cluster, the configuration files of this region will not be displayed; these files will be displayed once a cluster is created under this region. The maximum nu allowed is 50.	mber of configural	tion files
Networks				
Data Volum	es			
Configuratio	ins 1			

10.Services 10.1. Instructions

An application is composed of one or more services. You can update the application by changing the application configurations or changing the configurations of a service.

10.2. View service details

Procedure

- 1. Log on to the Container Service console.
- 2. Click Swarm > Services in the left-side navigation pane.
- 3. Select the cluster in which the service you want to view resides from the Cluster drop-down list.
- 4. Click the service name. As shown in the following figure.

Container	Service	Service Lis	st						Refresh
Kubernetes	Swarm		2					Convice list undated	×
Overview		Help: & Ho	2 pose service	is to the internet 🛛 🗞	Add a domain name to a	a service exposed to the public network & Switc	n from HTTP to HTTPS & Change application (axterna Service list updated.	
Applications		Cluster: te	est-swarm 🔻 🗹	Hide System Services	Hide Offline Services	s Hide Online Services	Name 🔻	Q	×
Services	1	Name	Application	Status	Container Status	Image			Action
Clusters		db	wordpress	Ready	Ready:1	renistry aliviums com/acs-sample/mysol+	5.7	Monitor Stop Res	chedule
Nodes			The operation	(idd)	Stop:0	region your an arconn and ann prophysion		opullo i bolco i	Events
Networks					Ready:3			Monitor Stop Res	chedule
Data Volum	es	Web 3	worapress	Ready	Stop:0	registry.aiiyuncs.com/acs-sample/wordpr	ess:4.0	update Delete	Events

5. The service details page appears and you can view all the containers of this service.

Containers Logs	Configurat	ions Events					
Name/ID	Status	Health Check	Image	Port	Container IP	Node IP	Action
wordpress_web_1 () b0d0dcc11540c538	running	Normal	registry.aliyunc sha256:592af506c	172.	172.	172.	Delete Stop Monitor Logs Web Terminal
wordpress_web_2 () 085801b023754437	running	Normal	registry.aliyunc sha256:592af506c	172.	172.	172.	Delete Stop Monitor Logs Web Terminal
wordpress_web_3 () 79ae3e1838507c2b	running	Normal	registry.aliyunc sha256:592af506c	172	172	172.	Delete Stop Monitor Logs Web Terminal

6. Click the Logs tab to view the service-level logs.

 Containers
 Logs
 Configurations
 Events

 Entries Per Container:
 100ter Image: State Stat

7. Click the **Configurations** tab to view the configurations of the service.

			1					
Containers	Logs	Configurations	Events					
Port Mapping)							
	Container Port							
80								
Environment	Vacable							
Linvioliment	Valiable							
Variable Nam	ie							
WORDPRESS	_NONCE_/	AA						
WORDPRESS	_NONCE_H	KEY						
WORDPRESS	AUTH_S	ALT						
WORDPRESS	LOGGED	_IN_SALT						
WORDPRESS	_NONCE_S	5ALT						
WORDPRESS	_AUTH_KE	ΕY						
WORDPRESS_SECURE_AUTH_KEY								
WORDPRESS_LOGGED_IN_KEY								
WORDPRESS	SECURE	AUTH_SALT						

8. Click the Events tab to view the events of the service.

Containers	Logs	Configurations	Events			
© 2017-4-1 14	:21:03					
Create servic	e wordpr	ess_web complete	d.			
© 2017-4-1 14	:21:03					
Activate con	tainer wo	rdpress_web_2 suc	cceeded.			
O 2017-4-1 14	:21:03					
Activate container wordpress_web_1 succeeded.						
O 2017-4-1 14	:21:03					
Activate con	tainer wo	rdpress web 3 suc	cceeded.			

10.3. Activate or stop a service

Procedure

- 1. Log on to the Container Service console.
- 2. Click Swarm > Services in the left-side navigation pane.
- 3. Select the cluster in which the service you want to activate or stop resides from the Cluster dropdown list.
- 4. Activate or stop the service according to the status.

Click **Stop** at the right of the service that you want to stop.

Container Service	Service List					Refresh
Kubernetes Swarm	Help: & Hov 2 lose s	ervices to the Internet 🛛	Add a domain name to	a service exposed to the public network ${\mathscr O}$ Switch fr	rom HTTP to HTTPS 🔗 Change application externa	dated. $ imes$
Applications	Cluster: test-swarm 🔻	✓ Hide System Service	s 🔲 Hide Offline Service	B Hide Online Services	Name 🔻	Q X
Services 1	Name Application	Status	Container Status	Image		Action
Clusters Nodes	db wordpress	🔴 Ready	Ready:1 Stop:0	registry-allyuncs.com/acs-sample/mysql:5.7	Monitor Stop Update Deletr	Reschedule Restart Events
Networks Data Volumes	web wordpress	Ready	Ready:3 Stop:0	registry.aliyuncs.com/acs-sample/wordpress	::4.5 Monitor Stop Update Delete	Reschedule Restart Events

Click Activate at the right of the service that you want to activate.

Container	Service	Service L	ist				Refresh
Kubernetes	Swarm	Help: Ø H	low t 2 se servic	es to the Internet 🛛 🖉	Add a domain name to a s	service exposed to the public network $ $	m HTTP to HTTPS 🔗 Change application external port
Overview Applications		Cluster:	test-swarm 🔻	Hide System Services	Hide Offline Services	Hide Online Services	Name 🔻 🔍 🗶 🗶
Services	1	Name	Application	Status	Container Status	Image	Action
Clusters		db	wordpress	Ready	Ready:1 Stop:0	registry.allyuncs.com/acs-sample/mysql:5.7	Monitor Stop Reschedule Update Delete Restart 3 Events
Networks Data Volum	es	web	wordpress	Stopped	Ready:0 Stop:3	registry.allyuncs.com/acs-sample/wordpress	Monitor i Activate i Reschedule i 1:4.5 Update i Delete i Restart i Events

5. In the displayed dialog box, click OK.

10.4. Change service configurations

Procedure

- 1. Log on to the Container Service console.
- 2. Click Swarm > Services in the left-side navigation pane.
- 3. Select the cluster in which the service you want to change the configurations resides from the Cluster drop-down list.
- 4. Click **Update** at the right of the service that you want to change the configurations. As shown in the following figure.

Container Service	Service List						Refresh
Kubernetes Swarm	Help: & Hov 2 Jose ser	vices to the Internet 🛛 &	P Add a domain name to	a service exposed to the public network $\ \ {\mathscr O}$ Switc	h from HTTP to HTTPS 🔗 Change application	externa Service list update	i. ×
Applications	Cluster: test-swarm 🔻	Hide System Service:	s 🔲 Hide Offline Service	Hide Online Services	Name 🔻	٩	×
Services 1	Name Application	Status	Container Status	Image			Action
Clusters	db wordpress	Ready	Ready:1 Stop:0	registry.aliyuncs.com/acs-sample/mysql::	5.7	Monitor Stop Re Update Delete	eschedule Restart Events
Networks Data Volumes	web wordpress	Ready	Ready:3 Stop:0	registry.aliyuncs.com/acs-sample/wordpr	ess:4.5	Monitor Stop Ri Update Delete	eschedule Restart Events

- 5. The Update Service page appears. Change the configurations
- 6. and then click **Update**.

10.5. Reschedule a service

Context

To rebalance the cluster load, you can rebalance the number of containers running on each node by moving the containers from nodes with high loads to the newly added nodes or nodes with low loads.

Procedure

- 1. Log on to the Container Service console.
- 2. Click Services in the left-side navigation pane.
- 3. Select the cluster in which the service you want to reschedule resides from the Cluster list.
- 4. Click **Reschedule** at the right of the service you want to reschedule. As shown in the following figure.



5. In the displayed dialog box, select or clear the **Ignore Local Volumes** and **Force Reschedule** check boxes. Then, click **OK**.

Note		×
•	The selected services will be rescheduled . Are you sure you want to perform this operation? Ignore Local Volumes Force Reschedule	
	OK Cancel	

- **Ignore Local Volumes:** For containers with local volumes, rescheduling might move these containers to other machines and cause the data loss. To ignore the local volumes, select this check box. With this check box deselected, the containers with local volumes will not be rescheduled. To ignore the local volumes, select this check box. With this check box deselected, the containers with this check box deselected, the containers with local volumes will not be rescheduled.
- Force Reschedule: Currently, to ensure the stability of online services, rescheduling only occurs when the memory usage and CPU usage of the machine are over 60% To ignore this limit, select this check box. Then, Container Service ignores the usage limit and forces rescheduling the service. and 40% respectively by default. To ignore this limit, select this check box. Then, Container Service ignores the usage limit and forces rescheduling the service.

Onte The memory and CPU usage values are subject to the container configurations. Therefore, the values are not always the actual usage of the machine.

10.6. Delete a service

Procedure

- 1. Log on to the Container Service console.
- 2. Click Services in the left-side navigation pane.
- 3. Select the cluster in which the service you want to delete resides from the Cluster list.
- 4. Click Delete at the right of the service that you want to delete.

Container	Service	Service I	List							Refresh
Kubernetes	Swarm									
Overview		Help: 🖉	Hov 2 bose service	es to the Internet 🔞	Add a domain name to a	a service exposed to the public network	Switch from HTTP to HTTP	5 🔗 Change application externa	Service list updated	. ×
Applications		Cluster:	test-swarm 🔻 🗹	Hide System Services	Hide Offline Services	s 🔲 Hide Online Services		Name 🔻	٩	×
Services	1	Name	Application	Status	Container Status	Image				Action
Clusters		db	wordpress	Ready	Ready:1 Stop:0	registry.aliyuncs.com/acs-sam	ple/mysql:5.7	Monito Upd	r Stop Re late Delete	schedule Restart Events
NODES									3	
Networks Data Volume	es	web	wordpress	Ready	Ready:3 Stop:0	registry.aliyuncs.com/acs-sam	ple/wordpress:4.5	Monito Upd	r Stop Ret ate Delete	schedule Restart Events

5. In the displayed dialog box, click **OK**.

Note	×
•	The selected service: web will perform the Delete operation. Are you sure you want to perform this operation? Remove the Data Volumes Force Deletion
	OK Cancel

11.Networks 11.1. Container network interconnection

Container Service creates the global network for containers, and the containers in the cluster can access other containers by using the etho network interface of the container.

Orchestration example

For example, create containers on two machines respectively and record the IP addresses, names, and host names of the containers. Log on to the container web terminal and test the network communication across nodes for these two containers by using the ping command.

```
network-test1:
    image: busybox
    hostname: server1
    command: sh -c 'ifconfig eth0; sleep 100000'
    tty: true
    environment:
        - 'constraint:aliyun.node_index==1'
network-test2:
    image: busybox
    hostname: server2
    command: sh -c 'ifconfig eth0; sleep 100000'
    tty: true
    environment:
        - 'constraint:aliyun.node_index==2'
```

Test methods

The containers of these two services are distributed in different nodes.

Services Containers	Logs Ever	nts Routes					
Name/ID	Status	Health Check	Image	Port	Container IP	Node IP	Action
test_network-tes 2e83acc375160b4a	running	Normal	busybox:latest sha256:8ac485896		172.20.15.4	172.363.92	Delete Stop Monitor Logs Web Terminal
test_network-tes () 4eea59284ce76d4e	running	Normal	busybox:latest sha256:8ac485896		172.20.180.4	02.06.000	Delete Stop Monitor Logs Web Terminal

Test network communication by using container IP address

By using the Container Service console or the ifconfig eth0 log output by container test_networktest1_1, you can see the IP address of container test_network-test1_1 is 172.18.0.4 Then, you can connect to the web terminal to access the IP address of container test_network-test1_1 in container test_network-test2_1 to test whether or not the network communication works.

Enter sh in the shell field and then click Execute. Then, enter the command ping ping 172.18.0.4 . As shown in the following figure.

_								
		shell	sh					Execute
1	# pir	ng 172	2. 20. 15. 4					
PIN	IG 172.	20. 15.	4 (172, 20, 15,	4): 56	data	bytes		
64	bytes	from	172.20.15.4:	seq=0	ttl=62	time=0.167	ms	
64	bytes	from	172.20.15.4:	seq=1	ttl=62	time=0.151	ms	
64	bytes	from	172.20.15.4:	seq=2	ttl=62	time=0.137	ms	
64	bytes	from	172.20.15.4:	seq=3	ttl=62	time=0.181	ms	
64	bytes	from	172.20.15.4:	seq=4	ttl=62	time=0.316	ms	
64	bytes	from	172.20.15.4:	seq=5	ttl=62	time=0.147	ms	
64	bytes	from	172.20.15.4:	seq=6	ttl=62	time=0.153	ms	
64	bytes	from	172.20.15.4:	seq=7	ttl=62	time=0.127	ms	
64	bytes	from	172.20.15.4:	seq=8	ttl=62	time=0.124	ms	
64	bytes	from	172.20.15.4:	seq=9	ttl=62	time=0.125	ms	
64	bytes	from	172.20.15.4:	seq=10	ttl=62	time=0.121	ms	
64	bytes	from	172.20.15.4:	seq=11	ttl=62	time=0.142	ms	

Test network communication by using container name

You can view the container name on the details page of the corresponding container. The default container name is a follows.

Services	Containers	Logs	Events	Routes
Container:/te	est_network-tes	t1_1 ÷	Back to List	

Enter sh in the shell field and then click Execute. Then, enter the command ping test_network_test1_1 to test the network communication by using the container name. As shown in the following figure.

		shell	sh					Execute	
•	# nin	a tos	t natwork-tast	1 1					
, PTM	# pin 2 +ort	g tes notuos	d <u>eterti 1</u> (17	*_* 72 20 18	5 41) - 56	data hert			
1 110	J LESL		K (esci_i (i	- 20. 1	J. 4). J.) data byt	62		
64	bytes	from	172.20.15.4:	seq=0	tt1=62	time=0.147	ms		
64	bytes	from	172.20.15.4:	seq=1	ttl=62	time=0.114	ms		
64	bytes	from	172.20.15.4:	seq=2	ttl=62	time=0.140	ms		
64	bytes	from	172.20.15.4:	seq=3	ttl=62	time=0.135	ms		
64	bytes	from	172.20.15.4:	seq=4	ttl=62	time=0.131	ms		
64	bytes	from	172.20.15.4:	seq=5	ttl=62	time=0.139	ms		
64	bytes	from	172.20.15.4:	seq=6	ttl=62	time=0.125	ms		
64	bytes	from	172, 20, 15, 4:	seq=7	ttl=62	time=0.128	ms		

Test network communication by using hostname

In this example, the host name is specified in the orchestration template. Therefore, you can also test the network communication by using the host name. As shown in the following figure.

		shell	sh					Execute
1	# pir	ıg ser	ver1					
PIN	G serv	er1 ()	172.20.15.4):	56 da	ta byte	S		
64	bytes	from	172, 20, 15, 4:	seq=0	ttl=62	time=0.134	ms	
64	bytes	from	172.20.15.4:	seq=1	ttl=62	time=0.130	ms	
64	bytes	from	172, 20, 15, 4:	seq=2	ttl=62	time=0.115	ms	
64	bytes	from	172.20.15.4:	seq=3	ttl=62	time=0.115	ms	
64	bytes	from	172, 20, 15, 4:	seq=4	ttl=62	time=0.124	ms	
64	bytes	from	172, 20, 15, 4:	seq=5	ttl=62	time=0.118	ms	
64	bytes	from	172, 20, 15, 4:	seq=6	ttl=62	time=0.125	ms	
64	bytes	from	172.20.15.4:	seq=7	ttl=62	time=0.124	ms	

11.2. Use VPC in Container Service

This document introduces how to use Virtual Private Cloud (VPC) in Container Service and the corresponding notes.

VPC CIDR block

- To create a VPC container cluster in Container Service, plan the network according to the actual conditions first. Specify the ClasslessInter-Domain Routing (CIDR) to segment the corresponding subnetworks when creating a VPC.
- Each VPC can only specify one CIDR block. The CIDR block range is as follows. 172.16.0.0/12 is the default CIDR block of VPC.
 - 10.0.0/8
 - 172.16.0.0/12
 - o 192.168.0.0/16

Container CIDR block

Specify the corresponding container CIDR block when creating a VPC cluster in Container Service. Currently, Container Service supports the following container CIDR blocks:

- 192.168.1.0/24
- 172.[16-31]. 1.0/24

Network planning

To ensure the network intercommunication between containers, add each container CIDR block to the route table. Therefore, to avoid the conflict of CIDR blocks, perform the corresponding network planning for your application service according to the CIDR blocks of VPC and container.

CIDR block planning

Both VPC and container can have 172 as the CIDR block. Therefore, when selecting 172 as the CIDR block of VPC and container, you must pay attention. For example, if the VPC CIDR block is 172.16.0.0/12 and the VSwitch CIDR block is 172.18.1.0/24. Then, the IP address of the Elastic Compute Service (ECS) instance on the VSwitch is 172.18.1.1-172.18.1.252 according to the CIDR block definition of the VSwitch.

if the VPC CIDR block is 172.16.0.0/12 and the VSwitch CIDR block is 172.18.1.0/24. Then, the IP address of the Elastic Compute Service (ECS) instance on the VSwitch Then, the IP address of the Elastic Compute Service (ECS) instance on the VSwitch is 172.18.1.1-172.18.1.252 according to the CIDR block definition of the VSwitch. If the container CIDR block is also 172.18.1.0/24, the IP address of the container and that of the ECS instance are the same. In this way, an exception occurs in the network communication between containers. In this way, an exception occurs in the network communication between containers. So you must pay attention to the network planning when using a VPC.

Route table planning

Currently, up to 48 route entries can be included in a route table of a VPC.

Example

Use the following complete example to demonstrate the whole creation process of a VPC cluster in Container Service.

Step 1. Create a VPC

- 1. Log on to the VPC console.
- 2. Click VPC in the left-side navigation pane.
- 3. Select the region. In this example, select China East 1 (Hangzhou).
- 4. Click Create VPC. The Create VPC dialog box opens. Complete the configurations and then click Create VPC.

In this example, to avoid conflicting with the container CIDR block, select 10.0.0.0/8 as the CIDR. as the CIDR.

Crea	ate VPC	Create VSwitch	
*VPC Name :	test		
	The name can be 2 -128 characters in length, including letters, digits, hyphens (-), and underscores (_), and must begin with either English letters or Chinese characters.		
Description :	test		
	The description can be 2-256 characters in length, and cannot begin with "http://" or "https://".		
*CIDR :	10.0.0/8		
	① The CIDR cannot be changed once the VPC is created.		

Step 2. Create a VSwitch

After creating a VPC, create the corresponding VSwitch under this VPC.

1. On the VPC list,

VPC	China North 1 (Qingdao)	China North 2 (Beijing)	China North 3 (Zha	ngjiakou) China North 5 (Huheh	naote)		C Refresh	Create VPC
Overview	China East 1 (Hangzhou)	China East 2 (Shanghai) China South 1 (Sh	enzhen) Hong Kong				
	Asia Pacific NE 1 (Japan)	Singapore Asia Pacifi	c SE 2 (Sydney) As	ia Pacific SE 3 (Kuala Lumpur)				
VPC	US East 1 (Virginia) US	West 1 (Silicon Valley)	Middle East 1 (Dubai)	Germany 1 (Frankfurt)				
NAT Gateway								
✓ VPN	VPC ID/Name	CIDR	Status	B Description	Created At	Default VPC		Actions
VPN Gateway	vpc-bp1 test	10.0.0.0	i/8 Availa	ble test	2017-11-17 16:10:56	No	Manage	Edit Delete
Customer Gateway								

- 2. click Manage at the right of the created VPC.
- 3. Click VSwitches in the left-side navigation pane, and then click Create VSwitch in the upper-right corner.

<	VSwitch List You can create 24 VSwitches at most for a VPC. Create VSwitch
VPC Details	VSwitch ID V Enter a VSwitch ID to search the VSwitch. Search
VSwitches	VSwitch ID/Name Number of ECS Instances CIDR Status Zone Number of Available Private IPs Created At Default VSwitch Description Actions

4. The Create VSwitch dialog box opens. Complete the configurations and then click OK.

In this example, select a China East 1 zone and enter 10.1.1.0/24 as the CIDR. If you select this VSwitch when the IP address of the ECS instance will be 10.1.1.1-10.1.1.252. The number of available private IPs is 252 in total, which means you can purchase 252 ECS instances under the VSwitch of this CIDR block. creating an ECS instance, when the IP address of the ECS instance will be 10.1.1.1-10.1.1.252. The number of available private IPs is 252 in total, which means you can purchase 252 ECS instances under the VSwitch of this CIDR block. The number of available private IPs is 252 in total, which means you can purchase 252 ECS instances under the VSwitch of this CIDR block.

Create VSwitch		×
*VPC:	test / vpc-bp1bl3qwfa1lj43r9yuut	
VPC CIDR Block :	10 · 0 · 0 · 0 / 8 Show Binary	
*Name :	test The name can be 2 -128 characters in length, including letters, digits, hyphens (-), and underscores (_), and must begin with either English letters or Chinese characters.	
*Zone :	China East 1 Zone E ① It cannot be modified after creation.	
*CIDR :	10 · 1 · 1 · 0 / 24 Show Binary • It cannot be modified after creation. The specified CIDR must be the same as, or belong to, that of the VPC. The allowed block size is between a /29 netmask and /16 netmask. For example:10.194.131.0/24 Learn more.	
Number of Available Private IPs :	252 IPs	
Description :	The description can be 2- 256 characters in length,	

Step 3. View route table

After creating the VPC and VSwitch, you can view the route table.

Click **VRouters** in the left-side navigation pane. The network of VSwitch is the default system route table.

<	VRouter Information			You can create up to 48 c	ustom route entries in a route table.	CRefresh	Add Route Entry
VPC Details	VRouter Basic Information						Edit ^
VSwitches	Name: -		ID : vrt-bp	084	6		
HAVIP	Description: -						
	Route Entry List						
	Route Table ID	Status	Destination CIDR Block	Next Hop	Next Hop Type	Туре	Actions
	vtb-bp)	Available	10.1.1.0/24	-	-	System	-
	vtb-bp	Available	100			System	

Step 4. Create a container cluster

- 1. Log on to the Container Service console.
- 2. Click Clusters in the left-side navigation pane,
- 3. and then click **Create Cluster** in the upper-right corner.

=	Container Service	Create Cluster List You can create up to 5 clusters and can add up to 20 nodes in each cluster. Refresh Create Cluster
	Overview	Help: Ø Create duster Ø How to add existing ECS instances Ø Cross-zone node management Ø Log Service integration Ø Connect to cluster through Docker Client
8	Applications	Name 🔻
\$	Services	Cluster Name/ID Cluster Type Region Network Type Cluster Status Node Status 🖗 Number of Nodes Time Created Docker Version Action
ø	Clusters	You currently do not have any clusters. You can Create Cluster
*	Nodes	

4. Complete the configurations and then click Create Cluster.

Select China East 1 (Hangzhou) as the **Region**, and VPC as the **Network Type**. Select the created VPC and VSwitch from the corresponding list.

Container Service			Currently Selected
		* Cluster Name	Region: China East 1
Overview		The duster name should be 1-64 characters long, and Can contain numbers, Chinese characters, English letters and hyphens.	(Hangzhou)
Applications		Region : China North 1 China North 2 China East 1 China East 2 China South 1 Asia Pacific NE 1 US West 1 Asia Pacific SE 1	Networl//PC
Services		(Qingdao) (Beijing) (Hangzhou) (Shanghai) (Shenzhen) (Tokyo) (Silicon Valley) (Singapore)	OS: Ubuntu 14.04 64bit
Clusters		(Sydney) (Frankfurt) (Virginia) Hong Kong (Zhangijakou) (Kuala Lumpur)	Quantity2 set(s)
Nodes	>		Instancel-core, 2 GB (
Networks	rviev	Zone : China East 1 Zone E 🔹	Type: ecs.n1.small)
Data Volumes	Ove	Cluster Mode : 🗌 Swarm Mode (Beta)	Create Cluster
Configurations 🔤		The Swarm Mode cluster is on beta version	
 Images and Tem 		Network Type : VPC	
Docker Images		vm-hn1hl2mufa1642r0v + tast +	
Orchestration T		the obviousline share is a conception of the share sh	
Solutions		Initial CIDR Bloc 172.18.0.9/24 Existing CIDR Block of Container Service 🕖	

In this example, the **Initial CIDR Block of Container Service** is 172.18.0.0/24. Then, the container CIDR block on the nodes of this cluster is 0/24. The container IP address on each node is 172.18.x.[1-255]. 172.18.[1-254]. 0/24. The container IP address on each node is 172.18.x.[1-255].

Step 5. Verify node IP address

After creating the container cluster, you can verify the preceding theory of network planning by verifying the cluster node IP address, route table, and checking the application container IP address.

You can verify the VSwitch CIDR block by checking the ECS instance IP address in the container cluster node list.

- 1. Log on to the Container Service console.
- 2. Click **Nodes** in the left-side navigation pane.
- 3. Select the cluster where the node that you want to verify resides from the Cluster list.

From the following figure, we can see that the IP address of the newly purchased ECS instance belongs to the VSwitch CIDR block 10.1.1.0/24.

Container Service	Node List										Refresh
Overview	Cluster: test										
Applications	IP Address	Instance Type	Instance ID/Name	Status	Number of Containers	Configuration	Operating System	Docker Version	Agent		Action
Services	10.1.1.105 () c72c3d9721b98452	Alibaba Cloud Node	i-bp c72c3d0721b08452	 Normal 	7	CPU:1core(s) Memory:1.954.GR	Ubuntu 14.04.5 LTS	17.06.2-ce	0.10-189653f	Monitor	More +
Clusters	47.96.173.123 (eip)		C/2C309/21090432			Meriory.1.954 GB					
Nodes											
Network 1											
Data Voluties											
Configurations											
 Images and Tem 											

Step 6. Verify route table

Verify the route table after verifying the node IP address.

- 1. Log on to the VPC console.
- 2. Click **VPC** in the left-side navigation pane.
- 3. Click
- 4. Manage at the right of the created VPC.

VPC	China North 1 (Qingdao)	China North 2 (Beijing) China Nor	th 3 (Zhangjiakou) China	North 5 (Huhehaote)		C Refresh	Create VPC
Overview	China East 1 (Hangzhou)	China East 2 (Shanghai) China So	outh 1 (Shenzhen) Hong H	Kong			
VPC	Asia Pacific NE 1 (Japan)	Singapore Asia Pacific SE 2 (Sydn	ey) Asia Pacific SE 3 (Kua	ala Lumpur)			
NAT Gateway	US East 1 (Virginia) US W	/est 1 (Silicon Valley) Middle East	1 (Dubai) Germany 1 (Fra	ankfurt)			
▼ VPN	VPC ID/Name	CIDR	Status Descripti	ion Created At	Default VPC		Actions
VPN Gateway	vpc-bp1 test	10.0.0/8	Available test	2017-11-17 16:10:56	No	Manage	Edit Delete
Customer Gateway							

5. Click **VRouters** in the left-side navigation pane.

A route entry with 172.18.x.0/24 0/24 as the CIDR block is added to the route table. The next hop is the corresponding ECS instance ID.

<		VRouter Information			You can create up to 48 custo	om route entries in a route table.	CRefresh	Add Route E	Entry
VPC Details		VRouter Basic Information						Edit	^
VSwitches		Name: -		ID: vrt-bp	Created At: 2017-11-17 16	Created At: 2017-11-17 16:10:56			
HAVIP		Description.							
		Route Entry List							
	-	Route Table ID	Status	Destination CIDR Block	Next Hop	Next Hop Type	Туре	A	octions
		vtb-bp	Available	172.18.2.0/24	i-bp: encode the first of the	ECS Instance	Custom	D	elete

Step 7. Verify container IP address

Finally, verify whether the container IP address is correct or not.

In this example, deploy a WordPress application by using an orchestration template in Container Service console, and then verify the container IP address by checking the container list on a node.

For how to create the WordPress application, see Create an application by using an orchestration template.

- 1. Log on to the Container Service console.
- 2. Click **Applications** in the left-side navigation pane.
- 3. Select the cluster where the created application resides from the Cluster list.
- 4. Click the application name. Click the **Containers** tab.

Services Contair	hers L	ogs Events	Routes				
Name/ID	Status	Health Check	Image	Port	Container IP	Node IP	
WordPress_db_1 () 99f7839f1c142936	running	Normal	registry.aliyunc sha256:ec7e75e52	3306/	172.18.2.4	10.1.	Delete Stop Monitor Logs Web
WordPress_web_1 aeee6e6614e85004	running	Normal	registry.aliyunc sha256:592af506c	10.1.1.	172.18.2.7	10.1.	Delete Stop Monitor Logs Web
WordPress_web_2 ① 3c1dbf0ea66d8731	running	Normal	registry.aliyunc sha256:592af506c	10.1.1.	172.18.2.6	10.1.	Delete Stop Monitor Logs Web
WordPress_web_3 () f0a23559b56e073d	running	Normal	registry.aliyunc sha256:592af506c	10.1.1.	172.18.2.5	10.1.	Delete Stop Monitor Logs Web

The preceding verification shows that a VPC container cluster is successfully created.

12.Data volumes

12.1. Overview

The characteristic of Docker determines the containers are non-persistent. Deleting a container also deletes its data. Data volumes provided by Docker can realize persistent storage by attaching to the host directories, but the data volumes in the host have the following limits in the cluster environment:

- Data cannot be migrated when containers are migrated between machines.
- Different machines cannot share data volumes.

To solve these issues, Alibaba Cloud Container Service provides third-party data volumes. By packaging various cloud storage resources as data volumes, these data volumes can be attached to containers directly and automatically reattached when containers are restarted or migrated. Currently, cloud disks and OSSFS are supported.

12.2. Create an OSSFS data volume

OSSFS is a FUSE-based file system provided by Alibaba Cloud (click https://github.com/aliyun/ossfs to view the project homepage). OSSFS data volumes can package Object Storage Service (OSS) buckets as data volumes.

The performance and functions of OSSFS differ from those of local file systems because data must be synchronized to the cloud by the means of network. Do not run databases, I/O-intensive applications, logs and other applications that require constantly writing files to OSSFS. OSSFS is suitable for sharing configuration files across containers, uploading attachments, and other scenarios without rewrite operations.

OSSFS differs from local file systems in the following ways:

- Random write or append write leads to the entire file being overwritten.
- Metadata operations, such as list directory, provide poor performance because the system must remotely access the OSS server.
- The file/folder rename operation is not atomic.
- Coordinate the actions of each client on your own when multiple clients are mounted to the same OSS bucket. For example, avoid multiple clients from writing the same file.
- Hard link is not supported.

Prerequisites

You can only use the data volume function when your cluster meets the following conditions:

• The cluster Agent is of version 0.6 or later.

You can check your Agent version on the Cluster List page. Select the target cluster, and click **More > Upgrade Agent** on the right.



If your Agent version is earlier than 0.6, upgrade the Agent first. For how to upgrade Agent, see Upgrade Agent.

• Deploy the acsvolumedriver application in the cluster. We recommend that you upgrade the acsvolumedriver application to the latest version.

You can deploy and upgrade the acsvolumedriver application by upgrading the system services. For more information, see Upgrade system services.

? Note When acsvolumedriver is upgraded or restarted, containers that use OSSFS data volumes are restarted, and your services are also restarted.

Step 1. Create an OSS bucket

- 1. Log on to the OSS console.
- 2. and create a bucket.

In this example, create a bucket in the region of China East 1 (Hangzhou).

Step 2. Create an OSSFS data volume

- 1. Log on to the Container Service console.
- 2. Click Data Volumes in the left-side navigation pane.
- 3. Select the cluster in which you want to create a data volume from the Cluster list. Click **Create** in the upper-right corner.

Container Service - Swarm	Data Volume Li	ist					Refresh
Overview	Help: 🖉 Data vol	ume guide					3
Applications	Cluster: test-swa	arm 🔻 🙎					
Services	Node	Volume Name	Driver	Mount Point	Container	Volume Parameters	Action
Clusters							
Nodes			U	Could not find any re	cord that met the condit	ion.	
Networks							
Data Volumes							
Configurations							

4. The **Create Data Volume** dialog box appears. Select **OSS** as the Type, configure the data volume parameters, and then click **Create**. Container Service creates a data volume with the same name on each cluster node.

Create Data Volume		×
Type:	OSS Cloud Disk	
Name.		
Access Key ID:		
Access Key Secret:		
Optional Parameters:	allow_other 🖉 📃 noxattr 🧭	
Other Parameters:		
	For the formats of other parameters, refer to this document. Example: -o allow_other -o default_permission=666 -onoxattr	
	Note: Only clusters with volume driver version 0.7 or above support these parameters. You can go to the application list, find the acsvolumedriver application, and view the volumedriver service's image version in the service list on the application details page. If the image version is lower than 0.7, please upgrade the volumedriver.	
Bucket ID:	Select Bucket	
Access Domain Name:	 Intranet Internet VPC 	
File Caching:	Enable I Close I Cl	
	Create	Cancel

- Name: The name of the data volume that must be unique within the cluster.
- Access Key ID/Access Key Secret : The AccessKey required to access OSS. You can obtain them from the AccessKey console.
- **Bucket ID**: The name of the OSS bucket to be used. Click **Select Bucket** in the dialog box, and click **Select**.
- Access domain name: If the bucket and ECS instances are in different regions, select external domain name. If they are located in the same region, you must select the corresponding cluster network type. For VPC network, select VPC domain name, and for classic network, select intranet domain name respectively.
- File Caching: Select Disable if you want to synchronize the modifications of the same file on multiple machines (for example, modify the file on machine A and read the modified contents on machine B).

? Note Turning off the File Caching causes ls folder to become slow, especially when a lot of files exist in the same folder. Therefore, when there is no such requirement, enable the File Caching and increase the speed of the ls command.

You can view the created OSSFS data volumes on the Data Volume List page.

Subsequent operations

After the data volumes are created, you can use the data volumes created in your app. For more information about how to use data volumes in an application, see Use third-party data volumes.

12.3. Creating NAS data volumes

Alibaba Cloud NAS is a file storage service for Alibaba Cloud ECs instance, providing a standard file access protocol, you do not need to make any changes to an existing application, ready to use with unlimited capacity and performance expansion, single namespace, multi-share, high reliability and high availability features such as distributed file systems.

Restrictions on Use

At present, Ali cloud NAS is open to North China 1, North China 2, North China 3, North China 5, East China 1, east China 2, South China 1, Asia Pacific Southeast 1, only clusters located in these areas can create NAS data volumes.

Prerequisites

You can only use the data volume function when your cluster meets the following conditions:

• The cluster Agent is of version 0.6 or later versions.

You can view your Agent version on the Cluster List page. Select the desired cluster and click more upgrade agents on the right.

If your version of the agent is too low, upgrade your agent first. For more information about how to upgrade the agent, see.

• Deploy the acsvolumedriver application in the cluster. We recommend that you upgrade the acsvolumedriver application to the latest version.

You can deploy and upgrade the acsvolumedriver application by upgrading the system services. See for details.

Procedure

This example shows an example of a VPC Container service cluster located in the East China 1 region.

Step 1 create a NAS File System

- 1. Log in to the file store management console.
- 2. Create a NAS file system.

Onte The NAS file system you created needs to be located in the same area as your cluster.

• Geography: select the same region as the container cluster. This example selects East China 1.

- Storage Type: this example selects the capacity type.
- Protocol type: Select NFS.

- Availability area: Select East China 1 Availability Zone B. Different available areas of the same region can be interfaced.
- Click OK.
- 3. After you click OK. This example creates a NAS file system located in the East China 1 region.

Step 2 Add a mount point for the container service cluster

- 1. Log in to the file store management console.
- 2. Click the list of file systems in the left-hand navigation bar to select the file systems that are created in step 1, click to the right to add a mount point.
- 3. Configure in the pop-up add mount point dialog box.
- 4. This example adds a VPC mount point.

(?) Note VPC network select where your container cluster is located Otherwise, an error occurs when you create a data volume.

Step 3 Add the cluster ECs instance network IP to the NAS File System whitelike list

In order for the ECS instance in the cluster to have access to the NAS file system, the internal network IP of the ECS instance needs to be added to the White List of NAS file systems.

• For clusters created after February 2017, when you create a NAS data volume, the internal network IP of the ECS instance in the cluster is automatically added to the White List of NAS file systems, you do not need to do anything.

After creating the NAS data volumes, When you expand the cluster (via, or, the container service automatically creates a NAS data volume for the newly added or expanded ECs instance and automatically the newly added nets IP of the ECS instance is added to the White List of NAS file systems.

- For clusters created before February 2017, you can add the internal network IP of the ECS instance in the cluster to the NAS File System in two ways.
 - Add White List manually.

Log in to the file storage management console, create a permission group and add a permission group rule to add the inner network IP of the cluster ECs instance to the White List. See NAS use documentation for details and use permission groups for access control.

Cluster Expansion after you add a whiteable list and create a NAS data volume through this method (, or, the container service automatically creates NAS data volumes for newly added or expanded ECs instances, but before using these volumes, you must manually and only add the internal network IP of the newly added ECs instance to the NAS file system. A white list.

- Authorization in Ram. The white list is automatically added after authorization, and cluster capacity will be expanded later (via, or) the newly added nets IP of the ECS instance is automatically added to the White List of NAS file systems.
 - a. Log in to the RAM Management Console.
 - b. Click User administration in the left-hand navigation bar.
 - c. Locate the user group named porter_[cluster_id] and click.
 - d. Click user authorization policies in the left-hand navigation bar, and click Edit authorization policies in the upper-right corner.
 - e. In the search box, enter Nas for the search, select, add to the list of selected Authorization Policy names and click OK.
 - f. Click OK to complete the authorization based on the page boot.

Step 4 Create NAS data volumes

- 1. Log on to the Container Service console.
- 2. Click **Data Volumes** in the left-side navigation pane.
- 3. Select the cluster where you want to create the data volume and click Create in the upper-right corner of the page.
- 4. In the pop-up dialog box, set the data volume parameters and click Create. The Container Service creates NAS data volumes with the same name on all nodes in the cluster.

You can log into the file store management console and click the ID of the NAS file system to be mounted by the cluster, view the details of the file system.

See the file system for details to complete the configuration of the data volumes.

- Data Volume name: the name of the data volume. The data volume name must be unique within the cluster.
- File System ID: ID of the NAS file system.
- Accesskey ID and accesskey secret: The accesskey for your account.

Onte The container service began supporting STS token functionality in December 5, 2017. If your cluster was created after this date, when you create a NAS data volume in this cluster, you enter accesskey.

- **Mount Point Domain Name**: Enter the mount address of the mount point in the NAS file system for the cluster.
- Sub-Directory: the sub-directory under the NAS path, which starts, once set, the data volume is mounted to the specified sub-directory.
 - If this sub-directory does not exist in the NAS root directory, the data volume is mounted after the sub-directory is created by default.

- If this field is left empty, the data volume is mounted to the NAS root directory by default.
- Privilege: Configure the access permission of the mount directory, such as 755, 644, and 777.
 - You can only configure the privilege when the data volume is mounted to the NAS subdirectory, that is, you cannot configure the privilege if the data volume is mounted to the NAS root directory.
 - If this field is left empty, use the permissions of the NAS files by default.

Note Upgrade the volume driver to the latest version when using the sub-directory, permissions option.

Subsequent operations

After the data volumes are created, you can use the data volumes created in your app. For more information about how to use data volumes in an application, see.

12.4. Create cloud disk data volumes

Cloud disk is a block storage system officially provided by Alibaba Cloud, and an elastic block storage product of distributed storage architecture that Alibaba Cloud provides to Elastic Compute Service (ECS). Cloud disk provides random storage of data block level, features in low latency, persistence, and high reliability, and adopts the distributed mechanism of three copies.

Cloud disk can be used for relational database applications or development and test applications. For more information, see Disks.

Limits

- The cloud disk and the ECS instances in the cluster must be in the same region and zone.
- Cloud disk data volumes only support being mounted to a single machine, but does not support the shared mode.
- A cloud disk data volume can be used by only one container at the same time.

Prerequisites

- Create a cloud disk manually in the ECS console before using the cloud disk data volume.
- Upgrade your Agent to the latest version. For more information, see Upgrade Agent.
- Deploy the acsvolumedriver application in the cluster. We recommend that you upgrade the acsvolumedriver application to the latest version.

You can deploy and upgrade the acsvolumedriver application by upgrading the system services. For more information, see Upgrade system services.

Procedure

Step 1 Create a cloud disk

In this example, create a cloud disk that is in the same region and zone as the cluster.

- 1. Log on to the ECS console.
- 2. Click Cloud Disks in the left-side navigation pane.
- 3. On the Disk List page, click Create Cloud Disk in the upper-right corner.

4. Configure the parameters for the cloud disk. Select the corresponding region and zone. Create the cloud disk according to the guidance on the page.

? Note The purchased cloud disk can be mounted only when you select the same zone as the server. The cloud disk cannot be mounted across zones or regions.

📚 Cloud Disk			Purchase ECS Inst	tances Related Products V
• Choose the Datacente	er Region and Zone			
Asia Pacific SE 1 (Singapore)	Asia Pacific SE 2 (Sydney)	Asia Pacific NE 1 (Tokyo)	EU Central 1 (Frankfurt)	Middle East 1 (Dubai)
Asia Pacific SE 1 Zone B 🔻	Asia Pacific SE 2 Zone A 🔻	Asia Pacific NE 1 Zone A 🔻	EU Central 1 Zone A	Middle East 1 Zone A
US East 1 (Virginia)	US West 1 (Silicon Valley)	Hong Kong	China North 1 (Qingdao)	China North 2 (Beijing)
US East 1 Zone A	US West 1 Zone B	Hong Kong Zone C 🛛 🔻	China North 1 Zone C 🔹	China North 2 Zone E
China North 3 (Zhangjiakou)	China East 1 (Hangzhou)	China East 2 (Shanghai)	China South 1 (Shenzhen)	China North 5 (Huhehaote)
China North 3 Zone A 🔹	China East 1 Zone F 🔹	China East 2 Zone D 🔻	China South 1 Zone B 🔹	China North 5 Zone A
Asia Pacific SE 3 (Kuala Lumpur)		1		
Asia Pacific SE 3 Zone A 🔻				
Choose Storage				
SSD Cloud Disk -	20 GB Create o	lisk with snapshot		
Instance Cost				
\$0.006 USD/hour			Add To Cart	Buy Now

Step 2 Create data volumes by using the cloud disk

- 1. Log on to the Container Service console.
- 2. Click **Data Volumes** in the left-side navigation pane.
- 3. Select the cluster in which you want to create the data volume from the Cluster list and then click **Create** in the upper-right corner.

Container Service - Swarm	Data Volume List	t					Refresh
Overview	Help: 🖉 Data volur	me guide					3
Applications	Cluster: test 🔻	2					
Services	Node	Volume Name	Driver	Mount Point	Container	Volume Parameters	Action
Clusters							
Nodes			(1)	Could not find any re	cord that met the condit	ion.	
Networks							
Data Volumes							

4. In the displayed dialog box, select **Cloud Disk** as the **Type**, configure the data volume parameters and then click **Create**. Container Service will create a data volume with the same name on each cluster node.

Create Data Volume	9	\times
Type:	OSS	
Name:		
Cloud Disk ID:	Select Cloud Disk	
Access Key ID:		
Access Key Secret:		
File System	ext4 🔻	
.,,,	Cloud Disk Snapshot (Snapshot makes data more safe)	
	Note: Please use this function after upgrading to the volume driver to the latest version. You can manage volume drivers through Cluster List > "More" > "Upgrade System Service".	
	Create Cance	el

- Name: The name of the data volume, The data volume name must be unique within the cluster.
- **Cloud Disk ID**: Select the cloud disk to be mounted and is in the same region and zone as the cluster. In this example, select the ID of the cloud disk created in step 1.
- AccessKey ID and AccessKey Secret: The AccessKey of your account.

(?) Note Container Service begins to support the STS Token function since December 5, 2017. If your cluster is created after that, you must enter the AccessKey when you create a cloud disk data volume in the cluster.

• File System Type: You can select the data type in which data is stored to the cloud disk. The supported types include ext4, ext3, xfs, and vfat.

After the data volume is successfully created, you can view the cloud disk data volume on the Data Volume List page.

Data Volume List						Refresh Create
Help: 🖉 Data volume guide						
Cluster: test 💌						
Node	Volume Name	Driver	Mount Point	Container	Volume Parameters	Action
 Ety1107Wampet/Ampv2 	test	Cloud Disk	/mnt/acs_mnt/acd/test		View	Delete All Volumes with the Same Name
 Copil/Milectoder/ValentZ 	test	Cloud Disk	/mnt/acs_mnt/acd/test		View	Delete All Volumes with the Same Name
Batch Delete						

Subsequent operations

You can manage the cloud disk data volumes, including deleting all the data volumes with the same name and viewing data volume parameters.

12.5. View and delete data volumes

You can view and delete the created data volumes.

Procedure

- 1. Log on to the Container Service console.
- 2. Click Data Volumes in the left-side navigation pane and select the target cluster.

All the data volumes in the selected cluster are displayed on the **Data Volume List** page, including the local data volumes and third-party data volumes.

On this page, you can view the containers that reference the data volumes.

Data Volume List						Refresh Create
Help: 🔗 Data volume guide						
Cluster:						
Node	Volume Name	Driver	Mount Point	Container	Volume Parameters	Action
0 c d	testNAS		/mnt/acs_mnt/nas/testNAS		View	Delete All Volumes with the Same Name
Batch Delete						

For local data volumes, the data volume name is in the format of node_name/volume_name .

For third-party data volumes, you can click **View** under Volume Parameters to view the parameters of the data volumes.

When you create a third-party data volume, Container Service creates the data volume with the same name on each node in the cluster, allowing containers to be migrated between nodes. You can also select to **Delete all volumes with the same name**.

? Note Data volumes referenced by containers cannot be deleted. The Data Volume List page displays the containers that reference the data volume. You must delete the containers that references the data volume before you can delete the data volume.

12.6. Use third-party data volumes

Third-party data volumes are used in the same way as local data volumes.

You can set the data volumes when creating an application or changing the configurations of an existing application.

Prerequisite

You have created a data volume in Container Service console. For details, see Create an OSSFS data volume .

Procedure

Take the OSSFS data volume test in the test cluster as an example.

Node	Volume Name	Driver	Mount Point	Container	Volume Parameters	Action
c9d5b559d38ee4138b62a682	test	OSS File System	/mnt/acs_mnt/ossfs/volum		View	Delete All Volumes with the Same Name
c9d5b559d38ee4138b62a682	test	OSS File System	/mnt/acs_mnt/ossfs/volum		View	Delete All Volumes with the Same Name
Batch Delete						

Create an application by using an image

1. Log on to the Container Service console.

- 2. Click **Applications** in the left-side navigation pane.
- 3. Click Create Application in the upper-right corner.
- 4. Enter the basic information for the application you want to create and then click **Create with Image**. In this example, enter volume as the Name and select test as the Cluster.

? Note The cluster on which the application will be deployed must be the same as the one of the OSSFS data volume that you want to use.

	Basic Information		Configuration	\rightarrow	Done
Name:	volume				
	The name should be 1-64 characters long, and can	contain numbers, Eng	lish letters and hyphens, but cannot st	art with a hyphen.	
Version:	1.0				
Cluster:	test				
Update:	Standard Release				
Description:					
	🗆 Pull Docker Image 🚺				
				Consta	with Tenners

5. Select the image you want to use and complete the other configurations.

? Note For how to create an application by using an image, see Create an application.

6. Click the plus icon in the **Volume** section. Enter the data volume name in the **Host Path** or Data Volume Name field. Enter the Container Path and select RW or RO as the data volume permission.

	Data Volume:	Ouse third-party data volumes		
		Host Path or Data Volume Name	Container Path	Permission
olume		test	/testvolume /	RW 🔻 🗢
~	volumes_from:			

7. Click Create at the right of the page after completing the settings.

On the Data Volume List page, you can see that the OSSFS data volume test is referenced by the container of the volume application.

Cluster: test						
Node	Volume Name	Driver	Mount Point	Container	Volume Parameters	Action
c9d5b559d38ee4138b62a682	test	OSS File System	/mnt/acs_mnt/ossfs/volum	volume_volume_1	View	Delete All Volumes with the Same Name
c9d5b559d38ee4138b62a682	test	OSS File System	/mnt/acs_mnt/ossfs/volum		View	Delete All Volumes with the Same Name
Batch Delete						

Create an application by using an orchestration template

- 1. Log on to the Container Service console.
- 2. Click **Applications** in the left-side navigation pane.
- 3. Click Create Application in the upper-right corner.
- 4. Enter the basic information for the application you want to create and then click **Create with Orchestration Template.** In this example, enter volume as the Name and select test as the Cluster.

? Note The cluster on which the application will be deployed must be the same as the one of the OSSFS data volume that you want to use.

	Basic Information		Configuration	>	Done
Name:	volume The name should be 1-64 characters long, a	and can contain numbers	s, English letters and hyphens, but cannot start	: with a hyphen.	
Version:	1.0				
Cluster:	test 🔻				
Update:	Standard Release				
Description:					
	🗉 Pull Docker Image 🕖				
				Creat	e with Image Create with Orchestration Template

5. Click Use Existing Orchestration Template or use your own orchestration template.

? Note For how to create an application by using an orchestration template, see Create an application.

6. In the volumes section of the template, enter the data volume name, container path, and permission.

	Basic Information	<u>}</u>	Configuration	
1 ~ 2 3 ~ 4 5 6 ~ 7 8	<pre>volume: restart: always expose: - 443/tcp - 80/tcp labels: aliyun.scale: '1' image: 'nginx:latest'</pre>			
10	- 'test:/testvolume:rw'			

7. Click Create and Deploy after completing the settings.

On the Data Volume List page, you can see that the OSSFS data volume test is referenced by the container of the volume application.

Cluster: test						
Node	Volume Name	Driver	Mount Point	Container	Volume Parameters	Action
c9d5b559d38ee4138b62a682	test	OSS File System	/mnt/acs_mnt/ossfs/volum	volume_volume_1	View	Delete All Volumes with the Same Name
c9d5b559d38ee4138b62a682	test	OSS File System	/mnt/acs_mnt/ossfs/volum		View	Delete All Volumes with the Same Name
Batch Delete						

Change the configurations of an existing application

- 1. Log on to the Container Service console.
- 2. Click **Applications** in the left-side navigation pane.
- 3. Select the cluster (the test cluster in this example) in which the application resides from the Cluster list. Click **Update** next to the application you want to change the configurations.

For how to change the application configurations, see Change application configurations.

? Note Make sure the application and the OSSFS data volume you want to use are in the same cluster.

4. The Change Configuration dialog box appears. In the volumes section of the template, enter the data volume name, container path, and permission.

Name:	volume	
*Version:	1.1	
	Note: The version of the application must be changed; otherwise, the "OK" button is not available.	
Description:		
Use Latest Image:	Force Reschedule :	
Release Mode:	Standard Release 💽 🕖	
Template:	<pre>1 - volume: 2 restart: always 3 - expose: 4 - 443/tcp 5 - 80/tcp 6 - labels: 7 aliyun.scale: '1' 8 image: 'nginx:latest' 9 volumes: 10 - 'test:/testvolume:rw'</pre>	
	Use Existing Orchestration Template Label description	

5. Click **OK** after completing the modifications.

On the Data Volume List page, you can see that the OSSFS data volume test is referenced by the container of the volume application.

Cluster: test						
Node	Volume Name	Driver	Mount Point	Container	Volume Parameters	Action
c9d5b559d38ee4138b62a682	test	OSS File System	/mnt/acs_mnt/ossfs/volum	volume_volume_1	View	Delete All Volumes with the Same Name
c9d5b559d38ee4138b62a682	test	OSS File System	/mnt/acs_mnt/ossfs/volum		View	Delete All Volumes with the Same Name
Batch Delete						

12.7. FAQ

The container fails to be launched and the system reports an error such as chown /mnt/acs_mnt/ossfs/XXXX: input/output error if you use the third-party data volume in the method of Data volume name: an existing directory in the image (for example, o1:/data, when the /data directory exists in the image).

This error occurs because for named data volumes, Docker copies the existing files in the image to the data volumes and uses chown to set the relevant user permissions. However, Linux prohibits the use of chown for mount points.

To solve this issue, you can use one of the following solutions:

Upgrade Docker to version 1.11 or later versions. Upgrade Agent to the latest version and specify no
 copy in the orchestration template. Docker will not copy the data and thereby, no
 chown error will occur.

• If you need to copy the data, use the mount point path instead of the data volume name to set the data volume. For example, /mnt/acs_mnt/ossfs/XXXX:/data. However, this method bypasses the volume driver. When the machine is restarted, the container might be started before the OSSFS is successfully mounted and the container might be attached to a local data volume. To avoid this issue, use two data volumes at the same time. One is set by the data volume name and the other is set by the mount point path. The data volume set by the data volume name is only used for synchronizing with the volume driver and is not used for storage.

volumes:

- ol:/nouse
- /mnt/acs mnt/ossfs/XXXX:/data
- /tmp:/bbb

13.Logs 13.1. View logs

View application logs

- 1. Log on to the Container Service console.
- 2. Click Swarm > **Applications** in the left-side navigation pane.
- 3. Select the cluster in which the application you want to view the logs resides from the Cluster dropdown list.
- 4. Click the name of the application that you want to view the logs. As shown in the following figure.

Container Service	Application List					Refresh Create Application
Overview	Help: Create an application Ch	ange application configuratio	ns Simple route blue-green	release policy Container auto scali	ng	
Applications	Cluster: routing-test-online		Hide Offline Applications	Hide Online Applications		Name 💌
Chusters	Name Description	2 Status	Container Status	Time Created 🔺	Time Updated 🔺	Action
Nodes	nginx	Ready	Ready:1 Stop:0	2017-04-01 10:03:56	2017-04-01 10:41:52	Stop Update Delete Redeploy Events
Data Volumes	wordpress	Ready	Ready:4	2017-04-01 16:29:15	2017-04-01 16:29:20	Stop Update Delete
Configurations	3	(Cuu)	Stop:0	2017-01-01 10:25:15	2017-01-01 10:25:20	Redeploy Events
Images and Temp						
Operation Logs						
Getting Started						

5. Click the Logs tab to view the application logs.

You can select how many log entries are displayed for each container and download all the logs to your local device.

Services	Containers	Logs	Events	Routes	
Entries Per C	ontainer: 10	Oitem: 🔻			Filter by Container Name: All V Filter by Start Time: Download Logs
test_jenk test_jenk test_jenk test_jenk test_jenk test_jenk test_jenk test_jenk test_jenk	ins_1 ins_1 ins_1 ins_1 ins_1 ins_1 ins_1 ins_1 ins_1	2017-12 2017-12 2017-12 2017-12 2017-12 2017-12 2017-12 2017-12 2017-12 2017-12 2017-12	-11T01:34 -11T01:34 -11T01:34 -11T01:34 -11T01:34 -11T01:34 -11T01:34 -11T01:34 -11T01:34	1:02.77186 1:02.77960 1:02.99430 1:02.99435 1:03.04069 1:03.04069 1:03.04071 1:03.05799 1:03.05801 1:04.12471	56322 Running from: /usr/share/jenkins/jenkins.war 19472 webroot: EnvVars.masterEnvVars.get("JENKINS_JONE") 19542 Dec 11, 2017 134924 AM Main deltektinstoneTempContents 35862 MARNING: Failed to deltet the temporary Minstone file /tmp/winstone/jenkins.war 24492 Dec 11, 2017 13493 AM org.eclipse.jetty.util.log.JavaUtillog info 37952 INFO: Logging initialized @441ms 39932 Dec 11, 2017 134493 AM winstone.logger logInternal 3302 INFO: Beginning extraction from war file 55442 Dec 11, 2017 134194 AM org.eclipse.jetty.util.log.JavaUtillog warn 55542 Dec 11, 2017 134194 AM org.eclipse.jetty.util.log.JavaUtillog warn
test_jenk	ins_1	2017-12	-11T01:34	:04.17115	5767Z Dec 11, 2017 1:34:04 AM org.eclipse.jetty.util.log.JavaUtilLog info

View service logs

- 1. Log on to the Container Service console.
- 2. Click Swarm > Services in the left-side navigation pane.
- 3. Select the cluster in which the service you want to view the logs resides from the Cluster dropdown list.
- 4. Click the name of the service that you want to view the logs. As shown in the following figure.

Container Service	Service Li	st				Refres	ih
Overview	Help: H	low to expose service	s to the Internet A	dd a domain name to a se	ervice exposed to the public network Switch from HTTP to	HTTPS	
Applications	Cluster:	routing-test-online 📔	Nide System S	ervices 🔲 Hide Offline Se	ervices 🔲 Hide Online Services	Service Name	
Clusters	Name	Application	2 Status	Container Status	Image	Acti	ion
Nodes Data Volumes	nginx	nginx	Ready	Ready:1 Stop:0	nginx:latest	Monitor i Stop i Reschedui i Update i Delete i Restar i Event	le rt ts
Configurations Images and Temp 	db	wordpress	Ready	Ready:1 Stop:0	registry.aliyuncs.com/acs-sample/mysql:5.7	Monitor Stop Reschedul Update Delete Restar Event	le rt ts
Operation Logs Getting Started	web	wordpress	Ready	Ready:3 Stop:0	registry.alyuncs.com/acs-sample/wordpress:4.5	Monkor Stop Reschedul Update Delete Resta Event	le rt ts

5. Click the Logs tab to view the service logs.

You can select how many log entries are displayed for each container and download all the logs to your local device.

Containers Logs Configurations Events Entries Per Containers 100/tem: • Filter by Start Time: Download How to view logs test jenkins 1 2017-12-11701:34:02.7718666322 Running from: /usr/share/jenkins/jenkins.war Image: Start Time: Download How to view logs					
Entries Per Container: 100/tern: Filter by Start Time: Download How to View log: test jenkins 1 2017-12-11701:34:02.7718666322 Running from: /usr/share/jenkins/tenkins.war	Containers Lo	gs Configurations Events			
test jenkins 1 2017-12-11T01:34:02.771866632Z Running from: /usr/share/jenkins/jenkins.war	Entries Per Contain	n: 100item: T	Filter by Start Time:	Download	How to view logs
test_jenkins_1 2017-12-11701:34:02.779601947Z webroot: EnvVars.masterEnvVars.get("JEHKINS_HOME") test_jenkins_1 2017-12-11701:34:02.99301594Z Dec 11, 2017 1:34:02 AM Main deleteWinstoneFmpContents test_jenkins_1 2017-12-11701:34:03309582 MARMING: Failed to delet the temporary Minstone file /tmp/winstone/jenkins.war test_jenkins_1 2017-12-11701:34:03.040692449Z Dec 11, 2017 1:34:03 AM org.eclipse.jetty.util.log.JavaUtillog info	<pre>test_jenkins_1 test_jenkins_1 test_jenkins_1 test_jenkins_1 test_jenkins_1</pre>	2017-12-11T01:34:02.7718666322 Running from: /usr/share/jenkins/jenkins.war 2017-12-11T01:34:02.779601947Z webroot: EnvVars.masterEnvVars.get("DENLINS_HOME") 2017-12-11T01:34:02.994301594Z Dec 11, 2017 1:34:02 AM Main deleteWinstoneTempContents 2017-12-11T01:34:02.994305585Z WANNING: Failed to delete the temporary Winstone file // 2017-12-11T01:34:03.040692449Z Dec 11, 2017 1:34:03 AM org.eclipse.jetty.util.log.Java	tmp∕winstone∕jenkins.war UtilLog info		

View container logs

- 1. Log on to the Container Service console.
- 2. Click Swarm > Services in the left-side navigation pane.
- 3. Select the cluster from the Cluster drop-down list.
- 4. Click the service name. As shown in the following figure.

Container Service	Service List	t				Refresh
Overview	Help: Ho	ow to expose servi	ces to the Internet Ac	ld a domain name to a se	ervice exposed to the public network Switch from HTTP to HTTP	'S
Applications	Cluster: r	outing-test-online	💌 🖉 Hide System Se	ervices 🔲 Hide Offline Se	ervices 🗏 Hide Online Services	Service Name
Clusters	Name	Application	2 Status	Container Status	Image	Action
Nodes Data Volumes	nginx	nginx	Ready	Ready:1 Stop:0	nginx:latest	Monitor Stop Reschedule Update Delete Restart Events
Configurations Images and Temp 	db	wordpress	Ready	Ready:1 Stop:0	registry.aliyuncs.com/acs-sample/mysql:5.7	Monitor Stop Reschedule Update Delete Restart Events
Operation Logs Getting Started	web	wordpress	Ready	Ready:3 Stop:0	registry.allyuncs.com/acs-sample/wordpress:4.5	Monitor Stop Reschedule Update Delete Restart Events

5. Under the Containers tab, click **Logs** at the right of the container you want to view logs. As shown in the following figure.

Containers	Logs	Configurations	Events					
Name/ID		Status	Health Check	Image	Port	Container IP	Node IP	Action
test_jenkins_ 50fc4eeac72e	1 🕖 ed921	running	Normal	registry.cn-hang sha256:fe4d0ef25	50000/tcp 8080/tcp	17513-043	0.97.6.35	Delete Stop Monitor Logs Web Terminal

You can view the logs of this container.

Containers Logs Configurat	ons Events
Container:/wordpress_web_1 == Bac	k to List Monitor Logs Web Terminal Details
wordpress_web_1 2017-04-01 wordpress_web_1 2017-04-01 wordpress_web_1 2017-04-01 wordpress_web_1 2017-04-01 wordpress_web_1 2017-04-01 wordpress_web_1 2017-04-01	<pre>108:36:55.5196781312 172.17.0.1 - [01/Apr/2017:16:36:55 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" "Go-http-client/1.1" 108:36:95.06090356952 172.17.0.1 - [01/Apr/2017:16:37:03 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" "Go-http-client/1.1" 108:37:07.55093732 172.17.0.1 - [01/Apr/2017:16:37:03 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" "Go-http-client/1.1" 108:37:07.55093732 172.17.0.1 - [01/Apr/2017:16:37:03 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" "Go-http-client/1.1" 108:37:07.55093732 172.17.0.1 - [01/Apr/2017:16:37:10 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" "Go-http-client/1.1" 108:37:07.150900571 172.17.0.1 - [01/Apr/2017:16:37:10 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" Go-http-client/1.1" 108:37:07.150900571 172.17.0.1 - [01/Apr/2017:16:37:07 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" Go-http-client/1.1" 108:37:07.150900571 172.17.0.1 - [01/Apr/2017:16:37:07 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" Go-http-client/1.1" 108:37:07.150900571 172.17.0.1 - [01/Apr/2017:16:37:07 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" Go-http-client/1.1" 108:37:07.150900571 172.17.0.1 - [01/Apr/2017:16:37:07 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" Go-http-client/1.1" 108:37:07.150900571 172.17.0.1 - [01/Apr/2017:16:37:07 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" Go-http-client/1.1" 108:37:07.150900571 172.17.17.0.1 - [01/Apr/2017:16:37:07 +0800] "GET /license.txt HTTP/1.1" 200 7603 "-" Go-http-client/1.1" 109:37:05 170000571 172.17" [01/Apr/2017:16:37"]</pre>

13.2. Enable Log Service

Log Service is a platform service for log scenarios. You can collect, distribute, ship, and query logs quickly without development, which is applicable to scenarios such as log transfer, monitoring, performance diagnosis, log analysis, and audit. Container Service integrates with Log Service, which allows you to send the application logs to Log Service.
Note On the cluster management page, choose **Enable Log Service** > OK. After Log Service is successfully enabled, the log index is created for each automatically created Logstore by using the built-in Resource Access Management (RAM) account. With this feature enabled, you are charged for the Alibaba Cloud Log Service usage after configuring the following settings. For more information, see Pay-as-you-go. Make sure you know your log volume to avoid large unexpected costs.

Enable Log Service

- 1. Log on to the Container Service console.
- 2. Click **Clusters** in the left-side navigation pane.
- 3. Click Manage at the right of the cluster.

Container Service	- Gluster List			Yo	u can create	up to 5 cluste	rs and can add	up to 20 nodes in each o	duster. Re	fresh Create Cluster +
Overview	Help: Ø Create cluster Ø How to add	d existing ECS inst	ances 🔗 Cross-zon	e node management 🔗 Log	Service integr	ration 🔗 Co	nnect to cluster	through Docker Client		
Applications	Name 🔻									
Services	Cluster Name/ID	Cluster Type	Region	Network Type	Cluster Status	Node Status 🕜	Number of Nodes	Time Created	Docker Version	3 Action
Nodes Networks	test ch75cs34cs88400fs40e0015756000e	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc- hg/kcm/MiterApmol/7c2pm	Running	Healthy C	2	04/18/2018,14:48:27	17.06.2- Ce	Manage View Logs Delete Monitor More +
Data Volumes Configurations	test-swarmmode swarm mode	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc- tiptikonätikevkpmail/kalpm	Running	Healthy $oldsymbol{C}$	1	04/04/2018,17:15:40	17.06.2- ce	Manage View Logs Delete Monitor More •
▼ Images and Tem ^Ξ										

4. Click Enable Log Service in the upper-right corner.

Cluster:test				Enable Log Service Log on to Hub Refresh
Basic Information			Upgrad	e Agent Upgrade System Service Clear Disk
Cluster ID:	VPC	Running	Region: China East 1 (Hangzhou)	Number of Nodes 2 Expand Add Existing Instances
Security Group ID:	Group Rebind			

5. In the dialog box, click **OK**.

Before enabling Log Service in Container Service, activate the RAM service and Log Service first. Click **Activate It** to activate the RAM service and Log Service if they are not activated yet. The created Log Service project is displayed after Log Service is successfully enabled.

Enable Log Service - test	×
Are you sure you want to enable the Log Service?	
The Log Service must be enabled for application log collection. Log data will be stored in Alibaba Cloud Log Service even after a cluster is deleted.	
Help on using Log Service in clusters:Alibaba Cloud Log Service Integration	
1. The RAM service must be activated before using Log Service. Please activate it if you have not. Activate It	
 Please activate Log Service if you have not.Activate It Aliyun log service will have costs, see product price 	
 The RAM service must be activated before using Log Service. Please activate it if you have not.Activate It Please activate Log Service if you have not.Activate It Aliyun log service will have costs, see product price OK Cancel	

Check installation result of acslogging service

Container Service installs the Agent required by Log Service on your machine if this is the first time Log Service is enabled. You can use Log Service after the application is installed successfully. You can find this application on the Application List page. You can use Log Service after the application is installed successfully.

- 1. Log on to the Container Service console.
- 2. Click **Applications** in the left-side navigation pane.
- 3. Select the cluster from the Cluster list and clear the Hide System Applications check box.

The acslogging application is successfully installed.

Container Service	Application List	0	•				Refresh Create Application
Overview	Help: 8 Create an a	perform a change application	Sonfigurations 8	Simple route blue-green re	lease policy 🔗 Container auto	scaling	
Applications	Cluster: test	Q X					
Service 2	Name	Description	Status	Container Status	Time Created 🔺	Time Updated 🔺	Action
Clusters	acslogging default	Logging Service	Running	Running:4 Stop:0	04/18/2018,14:53:57	04/18/2018,14:54:12	Stop Redeploy Events
Networks	acsmonitoring default	Monitoring Service	Running	Running:2 Stop:0	04/18/2018,14:53:57	04/18/2018,14:54:07	Stop Redeploy Events
Configurations	acsrouting default	Routing Service	Running	Running:2 Stop:0	04/18/2018,14:53:57	04/18/2018,14:54:13	Stop Redeploy Events
 Images and Tem Docker Images 	acsvolumedriver system	Data Volume Service	Running	Running:2 Stop:0	04/18/2018,14:53:57	04/18/2018,14:54:02	Redeploy Events

The system creates a corresponding project in Alibaba Cloud Log Service. You can view the project in the Log Service console. The project name contains the Container Service cluster ID.

acslog-project-cfb72ca34c-mavbu	cfb72ca34ca68433fba20e2	China East 1 (Hangzhou)	2018-04-18 15:14:20	Modify	Delete

Use Log Service in orchestration files

Most Docker applications write the logs directly to stdout, now you can do this as well (for the scenarios of writing logs to files, see Use file logs in the following section). After enabling Log Service, stdout logs are automatically collected and sent to Alibaba Cloud Log Service.

In the following example a WordPress application is created. It contains two services: WordPress service and MySQL service. Logs are collected to Alibaba Cloud Log Service. which contains two services: WordPress service and MySQL service. Logs are collected to Alibaba Cloud Log Service.

MySQL and WordPress

Container Service

```
mysql:
 image: mysql
 ports:
     - 80
  labels:
     aliyun.scale: "1"
 environment:
     - MYSQL ROOT PASSWORD=password
web:
 image: registry.aliyuncs.com/jiangjizhong/wordpress
 ports:
    - 80
  labels:
    aliyun.routing.port 80: wordpress-with-log
    aliyun.log store dbstdout: stdout # Collect stdout logs to the dbstdout Logstore.
    aliyun.log_ttl_dbstdout: 30 # Set the data retention time for the dbstdout Logstore t
o 30 days.
 links:
      - mysql
```

In the preceding orchestration file:

- aliyun.log_store_dbstdout: stdout indicates to write the container standard to the Logstore a cslog-wordpress-dbstdout .The label format is aliyun.log_store_{name}: {logpath} 。 Wherein:
 - name is the name of the Alibaba Cloud Log Service Logstore. The actually created Logstore name is acslog-\${app}-\${name}.
 - app is the application name.
 - logpath is the log path in the container.
 - stdout is a special logpath , indicating the standard output.
- aliyun.log_ttl_<logstore_name> is used to set the data retention time (in days) for the Logstore. The value range 1-365. If left empty, logs are kept in the Logstore for two days by default.

(?) Note The value configured here is the initial configuration value. To modify the data retention time later, modify it in the Log Service console.

You can create an application named wordpress in the Container Service console by using the preceding orchestration file. After the application is started, you can find the Logstore acslog-wordpress-dbstdout in the Log Service console, in which stores the logs of application wordpress.

View logs in Log Service console

After deploying an application by using the preceding orchestration file, you can view the collected logs in the Alibaba Cloud Log Service console. Log on to the Log Service console. Find the Log Service project corresponding to the cluster. You can view the Logstore acs-wordpress-dbstdout used in the orchestration file.

Logstore List						Endpoint List	Create
Searching by logstore name	Search						
Logstore Name	Data Import	Monitor	Log Collection Mode	Log	g Consumption Mo	ode	Action
Logstore Name	Wizard	PIOIIILOF	Log collection Plode	LogHub	LogShipper	LogSearch	ACTION
acslog-wordpress-		ĸ	Logial Config (Manage) Diagnose More Data -	Preview	055	Search	Modify Delete

Click Search at the right of the Logstore to view the logs.

Use file logs

To write the logs directly to files (for example, */var/log/app.log*) instead of stdout, configure as follows:

```
aliyun.log_store_name: /var/log/app.log
```

name is the Logstore name. /var/log/app.log is the log path in the container.

To output multiple log files to Log Service, configure as follows to put the files under multiple directories:

```
aliyun.log_store_s1: /data/logs/access/access.log
aliyun.log_store_s2: /data/logs/error/error.log
aliyun.log store s3: /data/logs/exception/*.log #Wildcards are supported
```

Note Currently, multiple Logstores cannot correspond to the same log directory. The log files corresponding to the three Logstores s1, s2, and s3 in the preceding example must be under three directories.

Enable timestamp

You can select whether to add timestamp when Docker is collecting logs. Configure timestamp by using the aligun.log.timestamp label in Container Service. label in Container Service. The timestamp is added by default.

• Add timest amp

aliyun.log.timestamp: "true"

• Remove timest amp

aliyun.log.timestamp: "false"

14.Monitoring 14.1. Container monitoring service

Context

Container monitoring service depends on Alibaba Cloud CloudMonitor service, and provides container Operation & Maintenance (O&M) users with services such as default monitoring and alarm rule configurations. The monitoring service of Container Service provides the capabilities to demonstrate the monitoring data at the container dimension and give an alarm. Besides, Container Service can integrate with the third-party open-sourced monitoring solutions (for more information, see Integrate with third-party monitoring solutions).

Set alarm rules.

In some key services, you can add alarm rules according to your actual business situations. The container monitoring service will send an SMS notification to the cloud account contact when the monitoring metric reaches the alarm threshold.

Procedure

- 1. Log on to the Container Service console.
- 2. Go to the container list page by using:
 - Nodes.
 - Click Nodes in the left-side navigation pane.
 - Click the IP address of the node.
 - Applications.
 - Click Applications in the left-side navigation pane.
 - Select the cluster in which the application you want to view resides from the Cluster dropdown list.
 - Click the name of the application you want to view and then click the **Containers** tab.
 - Services.
 - Click Services in the left-side navigation pane.
 - Select the cluster in which the service you want to view resides from the Cluster drop-down list.
 - Click the name of the service you want to view.
- 3. In the container list, click **Monitor** at the right of the container you want to view.

Containers	Logs	Confi	gurations	Events	nts						
Name/ID			Status	Health Check	Image	Port	Container IP	Node IP	Action		
wordpress_wo 5f9e5c651918	ordpress_wordpr In running Normal wordpress:latest sha256;34947222d.		wordpress:latest sha256:34947222d	80/tcp	17548-03	381.198.148.112	Delete Stop Monitor Logs Web Terminal				

You can view the real-time monitoring information of the container.

0.01 0.01 0.05.00	18:10:00 • Ci	16:15:00 YU Utilization	18.20.00	1 0.5 0.4 0 10.0500	16.10.00 © Containe	18:15:00 er Memory Utilization	192000
40M 30M 20M 10M 0 18:05:00	16-10-00 Process Resident Memory (rss)	16:15:00 9 Sub-process Resident Memory	16 20.00 ((034_745)	00M 40M 20M 10.05.00	16 10 00 © Cotainer Memory	10:15:00 / Usage @ Max Memory Usage	10.20.00

- 4. Log on to the CloudMonitor console. Click Cloud Service Monitoring > Container Service in the leftside navigation pane. Click **Container Service Monitoring** on the Clusters page. Select the container from the Container Service list. Click Monitoring Charts to view the history monitoring data of the container.
- 5. Set alarm rules.

In some key services, you can add alarm rules according to your actual business situations. The container monitoring service will send an SMS notification to the cloud account contact when the monitoring metric reaches the alarm threshold.

- i. Click the Alarm Rules tab and then click **Create Alarm Rule** in the upper-right corner.
- ii. Based on your actual business requirements, configure the related resource, set the alarm rules,

FIGURES .	Container Service-Cluster -						
Resource Range :	ResourceDimensions	/ou can us	se an alarm ter	mplate. Click View	alarm template	e best prac	tice
Region :	China East 1 (Hangzhou)						
Cluster :	test Totally1unit Service : wordpress_wordpress	-	Container :	wordpress_word	press	-	
Type : Alarm Rule :			0.00				
Alarm Type :	Threshold Value Alarm Event Alarm		0.01				
Rule	CPU Usage	%	0.00				
Describe :		_	0.00				
+Add Ala	m Rule		0.00 07:41:00 08:36:	40 10:00	11:23:20	12:46:40	13:
Mute for :	24h - @	Usage	e—Average—cd9c0e	e0620a1a4c03b142ad54	b91f6b69—wordpre	.ss_wordpress-	-wor
Triggered							

- iii. and select the notification contact and method.
- iv. Complete the configurations as instructed on the page. Click Confirm.
- v. View the created alarm rule under the Alarm Rules tab.

14.2. View monitoring information

Log

- 1. on to the Container Service console.
- 2. Click **Clusters** in the left-side navigation pane.
- 3. navigation pane.

Container Service	Ouster List You can create up to 5 clusters and can add up to 20 nodes in each cluster. Refresh								Refresh Creat	te Cluster	
Overview	Help: ${\mathscr O}$ Create cluster ${\mathscr O}$ How to add	existing ECS instan	ces 🖉 Cross-zone no	de management 🛛 Ø Log	Service Integr	ration 🔗 Con	nect to cluster th	rough Docker Clien	t		
Applications	Name 🔻										
Services	Cluster Name/ID	Cluster Type	Region	Network Type	Cluster Status	Node Status	Number of Nodes	Time Created	Docker Version		Action
Clusters Nodes	test 2 Ethichaid Collar 1 a Action: 54 Courts 4	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc- bp19aqopjihwfxcjv516z	Running	Healthy 🕽	1	2017-12-25 18:11:44	17.06.2-ce	Manage Vie Monitor	Delete

4. Click **Monitor** at the right of the cluster.

Cluster: test 🔻										
IP Address	Instance Type	Instance ID/Name	Status	Number of Containers	Configuration	Operating System	Docker Version	Agent		Action
192.168.340.013 0 cd4cm406000.13400 47.95.172.250 (kip)	Alibaba Cloud Node	He12x221c17986x8448 cdw2x48x255c2472	 Normal 	9	CPU:4core(s) Memory:7.796 GB	Ubuntu 14.04.5 LTS	17.06.2-ce	0.10-e21a3d0	Monitor	More •

You can view the monitoring information of this cluster.

Monitoring information	
Please go to the CloudMonitor console to view detailed monitoring data for the cluster nodes. Instance: Host	2412 2017 Mitchet 40 Monitoring information
Select 2017-12-27 08:25 - 2017-12-27 09:25	
Ranne:	
r ser riger	
3	
2	ou
1	40
	20
0	0
CPU Utilization %	Outbound Bandwidth to Public Network in ktops Inbound Bandwidth from Public Network in ktops Outbound Bandwidth to Private Network in ktops Inbound Bandwidth from Private Network in ktops
2	-
٤	800
1.5	
	400
0.5	200
U 08:30:00 08:45:00 09:00 09:15:00	0 08:30:00 08:45:00 09:00 09:15:00
 System Disk Read IOPS (times/s) System Disk Write IOPS (times/s) 	Total System Disk Read BPS MB/s G Total System Disk Write BPS MB/s

View container monitoring information

- 1. Log on to the Container Service console.
- 2. Go to the container list page by using:
 - Nodes.
 - Click Nodes in the left-side navigation pane.
 - Click the IP address of the node.
 - Applications.
 - Click **Applications** in the left-side navigation pane.
 - Select the cluster in which the application you want to view resides from the Cluster list.
 - Click the name of the application you want to view. Click the Containers tab.
 - Services.
 - Click Services in the left-side navigation pane.

- Select the cluster in which the service you want to view resides from the Cluster list.
- Click the name of the service you want to view.
- 3. In the container list, click **Monitor** at the right of the container you want to view.

Containers	Logs	Confi	gurations	Events					
Name/ID			Status	Health Check	Image	Port	Container IP	Node IP	Action
wordpress_w 5f9e5c65191	ordpr () 86f51		running	Normal	wordpress:latest sha256:34947222d	80/tcp	172.18.0.5	192.168.140.113	Delete Stop Monitor Logs Web Terminal

You can view the monitoring information of this container.



14.3. Custom monitoring

The container monitoring service integrates with the Alibaba Cloud CloudMonitor service and provides you with monitoring and alarm services for containers, applications, clusters, and nodes. The container monitoring service meets the basic requirements for container monitoring. However, in many business scenarios, you might need custom monitoring to meet the monitoring requirements of your systems and applications. Therefore, besides the basic monitoring capabilities, the container monitoring service provides two custom monitoring modes, allowing you to report custom monitoring data by writing data and collecting scripts on your own or exposing your HTTP monitoring data interface. Container Service monitoring framework collects data every one minute by running the script or calling the HTTP interface.

Prerequisites

Before using the custom monitoring feature, you must integrate the container monitoring service with third-party monitoring solutions (for more information, see Integrate with third-party monitoring solutions).

? Note Currently, Container Service monitoring integration only supports InfluxDB and Prometheus by default.

Your custom monitoring data is reported to your InfluxDB or Prometheus, and then connected with your data presentation and analysis service.

Report monitoring data by using custom monitoring scripts

1. Create a Docker image and add a custom data collection script to this image.

The output data of this collection script must comply with the InfluxDB data format protocol. comply with the InfluxDB data format protocol.

```
weather,location=us-midwest temperature=82 1465839830100400200
|measurement|,tag set| |field set| |timestamp|
```

For more information about the data format protocol, see InfluxDB line protocol. protocol.

 Log on to the Container Service console. Create an application by using an orchestration template. Use the aliyun.monitoring.script label to declare the data collection script used by the monitoring service.

The sample template is as follows:

The aligun.monitoring.script label defines the command in the application container that monitoring service runs to collect the monitoring data. The label is configured as follows:

```
labels:
    aliyun.monitoring.script: "command used to run the script"
```

3. Open the web interface of InfluxDB to view the database tables named after data indexes.

For information about how to view the database tables, see Integrate with third-party monitoring solutions.

Collect data by using the custom HTTP monitoring data interface

1. Create a Docker image and expose the HTTP interface in the application.

This interface outputs the monitoring data. You can customize the monitoring data format by conforming to the JSON syntax. In addition, the system cannot determine whether the JSON data returned from the custom HTTP interface is a data index field or a metadata tag of the data index. data returned from the custom HTTP interface is a data index field or a metadata tag of the data tag of the data index. Therefore, use another configuration to specify what type of JSON data has the tag attribute. Telegraf JSON data format. For more information, see Telegraf JSON data format.

2. Log on to the Container Service console and create an application by using an orchestration template. In the template, add the aliyun.monitoring.http label to declare the data collection interface, and use aliyun.monitoring.tags: "your tag attribute name 1, your tag attribute name 2," to declare what type of data fields returned from the HTTP data interface has the tag attribute. aliyun.monitoring.http label to declare the data collection interface, and use ali yun.monitoring.tags: "your tag attribute name 1, your tag attribute name 2," to declare what type of data fields returned from the HTTP data collection interface, and use ali yun.monitoring.tags: "your tag attribute name 1, your tag attribute name 2," to declare what type of data fields returned from the HTTP data interface has the tag attribute.

Sample template:

```
nodejsapp:
command: "bash /run.sh"
ports:
    - "3000:3000"
image: 'Your own image repository address'
labels:
    aliyun.monitoring.http: "http://container:3000/metrics/data"
    aliyun.monitoring.tags: "tag1,tag2"
```

The data returned from the data interface http://container:3000/metrics/data exposed by the application nodejsapp is as follows: http://container:3000/metrics/data exposed by the appli
cation nodejsapp is as follows:

```
"tag1": "tag1value",
"tag2": "tag2value",
"field1": 1,
"field2": 2,
"field3": true,
"field4": 1.5
```

The aligun.monitoring.tags: "tag1,tag2" label defines that in the reported JSON data, attributes tag1 and tag2 are the tags of the reported data.

3. Open the web interface of InfluxDB to view the database tables whose names consist of the htt
pjson_ prefix and the container name.

For example, if the container name is nodejsapp_nodejsapp_1, the name of the database table in InfluxDB is httpjson_nodejsapp_nodejsapp_1.

For more information about how to view the database tables, see Integrate with third-party monitoring solutions.

14.4. Integrate with third-party monitoring solutions

Prerequisites

Create an application to be monitored. In this example, create an Nginx application. For more information, see Create an Nginx webserver from an image.

Context

Container Service provides the capability to integrate with third-party open-sourced monitoring solutions.

(?) Note Currently, Container Service monitoring integration only supports InfluxDB and Prometheus by default.

The following example introduces how to integrate the Container Service monitoring service with thirdparty monitoring solutions by taking InfluxDB as an example.

Procedure

- 1. Log on to the Container Service console.
- 2. Click **Applications** in the left-side navigation pane.
- 3. Click Create Application in the upper-right corner.

Container	Service	Application List				Refr	Create Applica	ation
Kubernetes	Swarm	Help: & Create	configurations 🔗 Simple route blue-	green release policy 🔗	Container auto scaling		3	
Applications		Cluster: test-swarm 🔻 🗹 Hide System Applications	Hide Offline Applications	de Online Applications		Name 🔻	Q	×
Services		Name Description Status	Container Status	Time Created 🔺	Time Updated 🔺			Action
Clusters					٦	Fotal: 4 item(s) , Per Page : 15 🔻 item(s	5) « < 1 >	> >

4. Enter the basic information of the application and click Create with Orchestration Template.In this example, the name of the application is influxdb.

	Basic Information		Configuration	>	Done
Name:	influxdb	s long, and can contain num?	are. English lattore and humbons, but cannot start u	with a hyphon	
Version:	1.0	siong, and can contain hume	ers, English lewers and hypitens, but cannot start w	ил а пурнен.	
Cluster:	test	Y			
Update:	Standard Release	T			
Description:					
	Pull Docker Image ()				
				Crea	te with Image Create with Orchestration Template

5. Enter the following orchestration template and click Create and Deploy.

? Note In a real production environment, the template in this example needs to be modified. Do not expose the port to the host in the influxdb service definition.

```
version: '2'
services: #Define influxdb.
influxdb:
    image: tutum/influxdb:0.9
    volumes:
        - /var/lib/docker/influxdb:/data
    ports:
        - "8083:8083" #Expose Web interface port.
        - "8086:8086" #Expose data API Web interface port.
```

6. After the application is successfully created, click the application name influxdb on the Application List page to view the application details. Click the **Containers** tab to view the node IP and port exposed by this application. Copy the node IP and port. (In this example, copy the node IP and port number of the port 8086. These are the data reporting address exposed by influxdb.)

Application:influxdb	Application:influxdb Ref							əfresh			
Overview											
Name: influxdb			Time Cr	eated: 2018-01-11	Time Updated	2018-	-01-11	Cluster: test			
Trigger 1. You can onl	Trigger 1. You can only have one of each trigger type.										
No trigger is available at t	he momer	nt. Click "Create 1	Trigger" in the	upper-righ	it corner.						
Services Containers	Logs	Events R	toutes								
Name/ID	Status	Health Check	Image		Port	Container	IP I	Node IP			Action
influxdb_influxd () 17428ece7125e242	running	Normal	tutum/influx sha256:7aa2	d b:0 2a38f2	10.150.011 18086->8086/tc	p 173.18.1.	5	381.081.08132	Delete Stop Monitor	Logs Web Te	rminal

7. Return to the Application List page. Click **Update** at the right of influxdb. Add the following contents to the template to declare the integration of InfluxDB and the container monitoring service. Then, click **OK**.

labels: aliyun.monitoring.addon.influxdb: "http://The node IP and port are the ones you co pied in step 7.

aliyun.monitoring.addon.influxdb_retention_policy: "default"

(?) Note Currently, the third-party open-sourced monitoring integration only supports InfluxDB and Prometheus. The labels for InfluxDB and Prometheus integration are aligun. monitoring.addon.influxdb and aligun.monitoring.addon.prometheus respectively. The format of the label value must be schema:hostIp:port.

Container Service cannot use link to identify InfluxDB because the container monitoring service Agent adopts host network mode. Therefore, create the influxdb application and then add the data reporting address exposed by influxdb to the application labels so as to inform the data collection client. Then, the monitoring service automatically writes the running status data of containers collected by application influxdb to influxdb.

8. On the Application List page, click the application name influxdb and then click the **Containers** tab. Copy the port exposed by influxdb container.

Services	Containers	Logs	Events R	loutes				
Name/ID		Status	Health Check	Image	Port	Container IP	Node IP	Action
influxdb_influ 17428ece712	uxd () 25e242	running	Normal	tutum/influxdb:0 sha256:7aa2a38f2	180.158.181.130:8086->8086/tcp	17518435	192,166,381,432	Delete Stop Monitor Logs Web Terminal

9. We recommend that you access InfluxDB by using the Web proxy.

To access InfluxDB by using Internet, follow these steps: Perform Internet authentication. Configure the inbound security group rules of ports 8083 and 8086 for the node in which the application influxdb resides. Access InfluxDB by using http://EIP:8083 port.

- 10. Access the InfluxDB page in the browser to view the metric data written by the container monitoring service.
 - i. Select telegraf. If telegraf does not exist, run CREATE DATABASE telegraf first and then redeploy the application that needs to be monitored.
 - ii. Click Query Templates and select Show Measurements from the drop-down list.
 - iii. Press Enter.

You can view the database table.

0 8083	익 🗟 ☆
SinfluxDB Write Data Documentation	Database: telegraf 🚽 🌣
Query: SHOW MEASUREMENTS	
	Query Templates -
measurements	Show Databases Create Database
name 2	Show Measurements
docker	Show Tag Keys
docker_container_blkio	Show Tag Values
docker_container_cpu	Show Retention Policies
docker_container_mem	Drop Retention Policy
docker_container_net	Show Users Create User Create Admin User Drop User
	·

View detailed data in a table.

 ≩InfluxD	B Write Data Documentatio	on			Database: telegraf -	¢
Query: sele	ect * from docker_container_cpu					
					Query Templates	•
docke	r_container_c	pu				
docke	r_container_c	pu aliyun_instance_id	aliyun_project_id	aliyun_service_id	container_id	

What's next

After Container Service is integrated with InfluxDB, select other data charts and frameworks, such as Grafana, to display your monitoring data based on your own business situation.

14.5. Container auto scaling

To meet the demands of applications under different loads, Container Service supports auto scaling for the service, which automatically adjusts the number of containers according to the container resource usage in the service.

You can configure the container auto scaling rules when creating applications or add the container auto scaling rules for existing applications by changing application configurations.

Auto scaling policies:

- When the monitoring metric value exceeds the configured upper limit, Container Service increases the number of containers at your configured step.
- When the monitoring metric value is lower than the configured lower limit, Container Service reduces the number of containers at your configured step.

Service monitoring metrics:

- Average CPU usage
- Average memory usage
- Container inbound rate (currently only support being configured by using orchestration templates)
- Container outbound rate (currently only support being configured by using orchestration templates)

Prerequisites

- Upgrade the cluster Agent to the latest version. For more information, see Upgrade Agent.
- Upgrade the cluster monitoring service (acsmonitoring) to the latest version. For more information, see Upgrade system services.
- Activate the RAM service and update the RAM authorization information in the cluster by completing the following steps: Log on to the Container Service console. Click **Clusters** in the left-side navigation pane. Click **More** at the right of the cluster. Select **Update RAM Authorization Information** from the list.

Instructions

- When determining whether the monitoring metric value exceeds the configured upper limit or lower limit, Container Service uses the average value of the monitoring metrics (namely, the average CPU usage and the average memory usage) within a sample period (one minute). Container Service triggers scaling only when the average monitoring metrics of three consecutive sample periods all exceed the configured upper limit or lower limit so as to avoid frequent scaling caused by monitoring data jitter.
- During container contraction, the system deletes the containers in the cluster. Therefore, back up the data in advance.

Set container auto scaling

Create an application by using an image

- when creating
- Create an application by using an orchestration template
- Change application configurations

Note Click Create with Image when creating an application. For how to create an application, see Create an application. What if the auto scaling rule does not take effect Create with Image

when creating

1. an application.

For how to create an application, see Create an application.

	Basic Information		Configuration	>	Done
Name:	test The name should be 1-64 characters	long, and can contain	numbers, English letters and hyphens, but cannot st	tart with a hyphen.	
Version:	1.0				
Cluster:	test	v			
Update:	Standard Release	Ŧ			
Description:		le le			
	Pull Docker Image				
				Creat	e with Image Create with Orchestration Template

2. In the **Scaling** section at the bottom of the page, select the **Enable** check box for Auto Scaling and set the auto scaling parameters.

Constraint rules:

- The range of the **Expansion Condition** is 50%–100%. The range of the **Contraction Condition** is 0%–50%.
- The Expansion Condition must be at least 30% higher than the Contraction Condition.
- The range of the **Step** is 1–5. The default value is 1.
- Set the Min Number of Containers and Max Number of Containers. For contraction, if the number of containers is less than or equal to the Min Number of Containers, contraction is not performed. For expansion, if the number of containers is greater than or equal to the Max Number of Containers, expansion is not performed.
 - ? Note
 - Set the scaling policies
 - with due care. If the application already meets the configured scaling conditions when you set the scaling rules and the application still meets the scaling conditions after the scaling, the monitoring will continuously trigger the scaling.

٨	Auto Scaling:	Enable Note: Before using auto scaling, upgrade the cluster Agent to the latest version.								
Deplo		Metric: CPU Usage v								
		Contraction Condition: Usage< 0 % Expansion Condition: Usage> 70 %								
		Step: 1 Range of valid values: 1–5								
		Max Number of Containers: 10 Range : 2-100								
		Min Number of Containers: 1 Range : 1-100								

Create an application by using an orchestration template

1. Click Create with Orchestration Template when creating an application.

For how to create an application, see Create an application.

	Basic Information		Configuration	>		Done
Name:	test					
	The name should be 1-64 characters	s long, and can contain	, numbers, English letters and hyphens, but (cannot start with a hyphen.		
Version:	1.0					
Cluster:	test	Ŧ				
Update:	Standard Release	Ŧ				
Description:						
		li li				
	Pull Docker Image Ø					
					Create with Image	Create with Orchestration Template

- 2. Click Use Existing Orchestration Template or write your own orchestration template.
- 3. Add the configurations of the container auto scaling by:
 - Clicking Add Service.

In the displayed dialog box, select the image and configure the corresponding parameters. Click **More Settings**. Select the **Enable** check box for Auto Scaling and set the auto scaling parameters.

Basi	ic Information	Configuration	Done	
1			, l	dd Service
You can use an orchestration to https://docs.docker.com/co	template to define and deploy a multi-container application. The Dock ompose/	er Compose format is supported. For more information, refer		
Use Existing Orchestration Te	emplate		Save Template	Prev Create and Deploy

• Manually configuring in the template.

In the labels configurations of the orchestration template, add the corresponding labels:

- Specify the step (the default value is 1): aligun.auto_scaling.step
- Specify the minimum number of containers (the default value is 1): aliyun.auto_scaling.min_instances 1):
 aliyun.auto_scaling.min_instances 1):
- Specify the maximum number of containers (the default value is 10): aligun.auto_scaling.m ax instances
- CPU usage as the metric
 - Specify the upper limit: aliyun.auto_scaling.max_cpu
 - Specify the lower limit: aliyun.auto_scaling.min_cpu
- Memory usage as the metric
 - Specify the upper limit: aliyun.auto_scaling.max_memory
 - Specify the lower limit: aliyun.auto_scaling.min_memory
- Outbound rate as the metric
 - Specify the upper limit: aligun.auto_scaling.max_internetOutRate
 - **Specify the lower limit:** aliyun.auto.scaling.min internetOutRate
- Inbound rate as the metric
 - Specify the upper limit: aliyun.auto_scaling.max_internetInRate
 - Specify the lower limit: aligun.auto_scaling.min_internetInRate

Example

1 Predervice BiochS1515474848076; 2 Predervice BiochS1515474848076; 3 retart: always 4 retart: always 5 - 80/fcp 6 Jabelis; 7 allyun-auto_scaling-max_cpu; '70' 11 allyun-auto_scaling-max_cpu; '70' 12 allyun-auto_scaling-max_cpu; '70' 13 allyun-auto_scaling-max_cpu; '70' 14 allyun-auto_scaling-max_cpu; '70' 15 allyun-auto_scaling-max_cpu; '70' 16 allyun-auto_scaling-max_cpu; '70' 17 allyun-auto_scaling-max_cpu; '70' 18 allyun-auto_scaling-max_cpu; '10' 19 allyun-auto_scaling-max_iteners: '1' 10 allyun-auto_scaling-max_in_innteners: '1' 11 allyun-auto_scaling-max_in_innteners: '1' 12 allyun-auto_scaling-max_in_innteners: '1' 13 allyun-auto_scaling-max_in_innteners: '1' 14 allyun-auto_scaling-max_in_innteners: '1' 15 allyun-auto_scaling-max_in_innteners: '1' 16 to define and deploy a multi-container application. The Docker Compose format is supported. For more information, refer <td< th=""><th>Basic Information</th><th>Confi</th><th>guration</th><th></th><th>Done</th><th></th></td<>	Basic Information	Confi	guration		Done	
2 inange: ''ngini:latest' 4 repose: 4 repose: 4 repose: 5 repose: 6 repose: 6 repose: 7 repose: 1 repose:	1 newServiceBlock1515147483076:				Service(s) C	ontained
* aligum.auto.scialing.emac.cou: *79* * aligum.auto.scialing.emin.cou: *79* * aligum.auto.scialing.emin.cou: *0* * aligum.auto.scialing.emin.cou: *0* * aligum.auto.scialing.emin.cou: *0* * aligum.auto.scialing.emin.instances: *1* * aligum.auto.scialing.emin.instances: *1* * aligum.auto.scialing.emin.instances: *1* * aligum.auto.scialing.emin.instances: *1* * vou can use an orchestration template to define and deploy a multi-container application. The Docker Compose format is supported. For more information, refer * to be fixing Orchestration template * Save Template	2 image: 'nginx:latest' 3 restart: always 4 expose: 5 - 60/tcp 6 labels: 7 allyun.scale: 'l'			Servic newSe Image:	e Name: rviceBlock1515 nginx:latest	147483 Edit Delete
or most-indextorm composer	<pre>i aliyon.avio.scaling.msr.cpu: '?0' aliyon.avio.scaling.star.cpu: '?0' aliyon.avio.scaling.star.iv aliyon.avio.scaling.star.instances: '6' aliyon.avio.scaling.min_instances: '1' aliyon.avio.scaling.min_instances: '1' </pre>	ulti-container application. The Docker Com	pose format is supported. For more infor	mation, refer	Add Ser	vice
abre remplate frei diote and bopoy	Use Existing Orchestration Template			Save Ten	plate Prev	Create and Deploy

Change application configurations

You can add container auto scaling settings by changing the configurations of an existing application.

1. On the Application List page, click **Update** at the right of the application you want to add the container auto scaling settings.

For how to change the application configurations, see Change application configurations.

Applications	Cluster: te	est 🔻	Hide System Applications	Hide Offline Applications	Hide Online Applications	Name 🔻	Q #
Services	Name	Description	Status	Container Status	Time Created 🔺	Time Updated 🔺	Action
Clusters Nodes	test		Ready	Ready:1 Stop:0	2018-01-05 18:23:19	2018-01-05 18:23:25	Stop Update Delete Redeploy Events

2. In the labels configurations in Template, add the corresponding container auto scaling labels.

Change Configura	ation	×
Name: *Version:	test 1.1 Note: The version of the application must be changed; otherwise, the "OK" button is not available.	
Description:		
Use Latest Image:	Force 🖉 Reschedule :	
Release Mode:	Standard Release 🔻 🔞	
Template:	<pre>1 pewServiceBlock1515147483076: 2 image: 'nginx:latest' 3 restart: always 4 expose: 5 - 80/tcp 6 labels: 7 aliyun.scale: '1' 8 aliyun.auto_scaling.max_cpu: '70' aliyun.auto_scaling.min_cpu: '0' aliyun.auto_scaling.step: '1' 11 aliyun.auto_scaling.max_instances: '6' aliyun.auto_scaling.min_instances: '1' 12 Use Existing Orchestration Template Label description</pre>	
	ок с	ancel

View created container scaling rules

You can view the created container scaling rules.

- 1. Log on to the Container Service console.
- 2. Click **Applications** in the left-side navigation pane.
- 3. On the **Application List** page, click **Update** at the right of the application.

You can view the created container scaling rules. You can modify the container scaling rules in the Template.

Change Configura	ation	×
Name: *Version:	test 1.1 Note: The version of the application must be changed; otherwise, the "OK" button is not available.	
Description:		
Use Latest Image:	Force Reschedule :	
Release Mode:	Standard Release 🔻 🕐	
Template:	<pre>1 hewServiceBlock1515147483076: 2 image: 'nginx:latest' 3 restart: always 4 expose: 5 - 80/tcp 6 labels: 7 aliyun.scale: '1' 8 aliyun.auto_scaling.max_cpu: '70' 9 aliyun.auto_scaling.min_cpu: '0' 10 aliyun.auto_scaling.step: '1' 11 aliyun.auto_scaling.max_instances: '6' 12 aliyun.auto_scaling.min_instances: '1' 13 Use Existing Orchestration Template Label description</pre>	
	ОК Са	ancel

14.6. Node auto scaling

To meet the demands of applications under different loads, Container Service provides the auto scaling both for containers and nodes. The node auto scaling is to automatically adjust the number of nodes by monitoring the node resource usage.

Node scaling policies:

- When the monitoring metric value exceeds the configured expansion condition, Container Service increases the number of nodes at your configured expansion step.
- When the monitoring metric value is lower than the configured contraction condition, Container Service reduces the number of nodes at the system default step 1.

Auto scaling monitoring metrics:

- Cluster CPU average usage
- Cluster memory average usage

Prerequisite

- Upgrade the cluster Agent to the latest version. For more information, see Upgrade Agent.
- Upgrade the cluster monitoring service (acsmonitoring) to the latest version. For more information, see Upgrade system services.
- Activate the RAM service and update the RAM authorization information in the cluster (Complete the

following steps: Log on to the Container Service console. Click **Clusters** in the left-side navigation pane. Click **More** at the right of the cluster. Select **Update RAM Authorization Information** from the list.

Instructions

- When determining whether the monitoring metric value exceeds the configured upper limit or lower limit, Container Service uses the average value of the monitoring metrics (namely, the average CPU usage and the average memory usage) within a sample period (one minute). Container Service triggers scaling only when the average monitoring metrics of three consecutive sample periods all exceed the configured upper limit or lower limit so as to avoid frequent scaling caused by monitoring data jitter.
- Node contraction only contracts nodes that are created by means of node expansion. Your manually added or created nodes are not affected. To perform auto contraction on those manually added nodes, add the following label for those nodes:

aliyun.reschedule==true

- During node contraction, the system deletes the Elastic Compute Service (ECS) instances in the cluster. Therefore, back up data in advance.
- Do not schedule services with statuses to nodes that can be contracted.
- The ECS instances added by expansion do not affect the deployed containers. The newly deployed containers are deployed according to the container deployment rules.
- During node contraction, Container Service migrates containers on the deleted ECS instances to other ECS instances.

Create node scaling rules

- 1. Log on to the Container Service console.
- 2. Click Clusters in the left-side navigation pane.
- 3. On the **Cluster List** page, click **Manage** at the right of the cluster.

Applications	Name 🔻										
Services	Cluster Name/ID	Cluster Type	Region	Network Type	Cluster Status	Node Status 🕜	Number of Nodes	Time Created	Docker Version	2	Action
Nodes Networks	routing-test-online of Conclusion (14 August Manufactor (17 Aug	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc- bp1vvet9csb16vac2jqoc	Running	Healthy 🕽	2	2017-12-04 15:26:27	17.06.2-ce	Manage View Monitor	Logs Delete More +

4. Click **Node Scaling** in the left-side navigation pane and click **Create Scaling Rule**.

Basic Information			000 4444 - 1004 1110	1070 ID								
Load Balancer Se.		Cluster ID: cd142dad	800C141499C0994600D1	87803		Kunning			Region: China East I (Hangzhou)			
User Tags		Scaling rule	Saling rule 2									
Image List		Create Scaling Rule										
Control List		Note: 1. Node contraction backup in advance.	on only contracts nodes	that are added through nod	le expansion;	nodes created or added n	nanually will not be af	fected. 2. While scaling	in, ECS instances w	vill be deleted. You	need to perform	data
Evones		Node List										
Node Scaling		IP Address	Instance Type	Instance ID/Name	Status	Number of Containers	Configuration	Operating System	Docker Version	Agent	Ac	ction
	Ξ	192.193.131.237 0 cf1424a6558c1414	Alibaba Cloud Node	Hot Rth-ActiHnanz cD Cole888c1404	Normal	9	CPU:2core(s) Memory:3.859 GB	Ubuntu 16.04.2 LTS	17.06.2-ce	0.10-f574e56	Monitor Mo	ore≁
		180.158.131.235 @ ed.425ed806;3434	Alibaba Cloud Node	Hop (Bin Helmolob Hultur ccl. 426ad800c) 414	Normal	7	CPU:2core(s) Memory:3.859 GB	Ubuntu 16.04.2 LTS	17.06.2-ce	0.10-f574e56	Monitor Mo	ore +

5. Configure the scaling rule and click Next.

Constraint rules:

- The range of the **Expansion Condition** is 50%–100%. The range of the **Contraction Condition** is 0%–50%.
- The Expansion Condition must be at least 30% higher than the Contraction Condition.

- The range of the expansion step is 1–5. Currently, the default **contraction step** is 1 and cannot be configured.
- Set the **Min Number of Cluster Nodes** and **Max Number of Cluster Nodes**. For contraction, if the number of nodes is less than or equal to the **Min Number of Cluster Nodes**, contraction is not performed. For expansion, if the number of nodes is greater than or equal to the **Max Number of Cluster Nodes**, expansion is not performed.

(?) Note Set the scaling policies with due care. If the cluster already meets the configured scaling conditions when you set the scaling rule and the cluster still meets the scaling conditions after the scaling, the monitoring will continuously trigger the scaling.

Configure Node Scaling Rule tReturn to Node Scaling					
Scaling Metrics	Select Instance Specification				
Metrics (Only one of CPU or memory can be selected as a scalable monitoring indicators) @ Auto scaling by	/ monitoring indicators				
CPU Usage	Memory Usage				
# Expansion Condition: CPU Usage > 70 % (Range: 50-100, difference between the expansion and contraction values cannot be less than 30%) Contraction Condition: Not set	Expansion Condition: Not set Contraction Condition: Not set				
Expansion Step					
Step: 1 (Range: 1-5)					
Restrictions					
Min Number of Cluster Nodes: 2 (Range: 1-10) Max Number of Cluster Nodes: 10 (Range: 1-20, the maximum number of nodes must be greater than the minimum number of nodes)					
	Back Next				

6. Configure the instance specifications and click Submit.

Configure the specifications for the nodes added by expansion after setting the expansion condition. For more information about how to configure the instance specifications, see Create a cluster.

You can also configure whether or not to add the IP addresses of the nodes added by expansion to the RDS instance whitelist, which facilitates the ECS instances to access the RDS instances.

(?) Note The ECS instance must be in the same region as the RDS instance so that the IP address of the ECS instance can be added to the RDS instance whitelist.

Click **Select RDS Instances** in the Advanced section at the bottom of the page. The Add to RDS instance whitelist dialog box appears. Select the RDS instances and then click **OK**.



View created node scaling rules

You can view the crated node scaling rules.

- 1. Log on to the Container Service console.
- 2. Click Clusters in the left-side navigation pane.
- 3. On the Cluster List page, click Manage at the right of the cluster.
- 4. Click Node Scaling in the left-side navigation pane. You can view the created node scaling rules.

Scaling rule				
Trigger condition	Scaling Step	Scaling Range	Instance Type	Action
CPU Utilization: Maximum: 70 % Minimum: 10 % Memory Utilization: Not set	Expansion Step 1 Scale in Step 1	Min Number of Cluster Nodes: 2 Max Number of Cluster Nodes: 10	2-core, 4GB (ecs.n4.large)	Modify Delete

You can click **Modify** to modify the node scaling rule or click **Delete** to delete this rule.

View monitoring metrics

- 1. Click **Clusters** in the left-side navigation pane.
- 2. On the **Cluster List page**, click **Monitor** at the right of the cluster.

Application	Name 🔻									
Services	Chuster Massa (TD	Chuster Tune	Decise	Network Type	Cluster	Node Chatura 🙆	Number of	Time Created	Docker	Action
Clusters	Cluster Name/1D	cluster Type	Region	Network Type	Status	Status 🕡	Nuces	Time created	Version	2 4001
Nodes	routing-test-online	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc-	Running	Healthy 🕽	2	2017-12-04 15:26:27	17.06.2-ce	Manage View Logs Delete
Networks				DD1//vet9csb16vac2jdoc						Monitor More+

You are redirected to the CloudMonitor console and can view the cluster monitoring information.

(?) Note If the monitoring data does not exist, check whether or not the monitoring service (acsmonitoring) is correctly installed. If not, redeploy the monitoring service (acsmonitoring). Check whether or not the cluster Agent is in the latest version. If not, upgrade the cluster Agent. Check whether or not the monitoring service (acsmonitoring) is in the latest version. If not, upgrade the monitoring service (acsmonitoring).

* Back to Instance List			Create Alarm Rule	View Instance Detail	C Refresh
Monitoring Charts Alarm Rules					
:: =					
CPU Usage(%) Period: 60s Method: Average	Network Inbound Traffic(bit/s) Period: 60s Method: Average	Network Outbound Traffic(bit/s) Period: 60s Method: Average	*		
2	0	0			
0 15:00 15:20 16:00 16:20	15:00 15:30 16:00 16:80	15:00 15:20 16	00 16:30		

3. Click **Container Service** in the left-side navigation pane. Click **View All Rules**.

C	lusters				C Refresh
E	iterto search		Searc	h Application Groups	
	Cluster Name	Status Network	Region	Monitor	Actions
	k8s-test	Running VPC	China East 1 (Hangzhou)	Node Monitoring Service Monitoring Container Service Monitoring	Monitoring Charts Alarm Rules
	routing-test-online	Running VPC	China East 1 (Hangzhou)	Node Monitoring Service Monitoring Container Service Monitoring	Monitoring Charts Alarm Rules
	Set Alarm Rules	View All Rules			

4. On the Alarm Rules page, you can view the automatically configured alarm rules of auto scaling.

If no monitoring alarm rule exists, update the RAM authorization information in the cluster (On the **Cluster List** page, click**More > Update RAM Authorization Information** at the right of the cluster). Activate the RAM service before updating the RAM authorization information. Otherwise, the system reports an error.



Aliyun API Error: RequestId: 51C6F096-5A42-41D2-9FC3-16472F34A45A Status Code: 4 04 Code: Inactive Message: Account is inactive to this service

5. Select an alarm rule to modify the alarm conditions and notification contacts who can be notified in SMSs, e-mails, and other ways. You can also disable the alarm rule.

Troubleshoot

If your configured node auto scaling rule does not take effect, see What if the auto scaling rule does not take effect for troubleshooting.

14.7. Monitoring metrics

Container Service provides multi-dimensional monitoring services. You can view the monitoring information in the Container Service console or CloudMonitor console.

The monitoring metrics of Container Service are divided into two parts: the automatic monitoring metrics and the cloud monitoring plug-in metrics. memory, network, I/O, and exception of Container Service helps you understand the usage of Container Service. You can log on to the CloudMonitor console and enter the Container Service page to view the monitoring details, and set alarm rules on monitoring metrics to receive alarm notifications when the metrics encounter an exception. Monitoring the metrics such as CPU usage, Monitoring the metrics such as CPU usage, memory, network, I/O, and exception of Container Service helps you understand the usage of Container Service. You can log on to the CloudMonitor console and enter the Container Service page to view the monitoring details, and set alarm rules on monitoring metrics to receive alarm notifications when the usage of Container Service. You can log on to the CloudMonitor console and enter the Container Service page to view the monitoring details, and set alarm rules on monitoring metrics to receive alarm notifications when the metrics encounter an exception.

Container Service provides monitoring information in the following dimensions:

- Cluster
- Node
- Service
- Container

Note Install the cloud monitoring plug-in when creating a cluster to obtain the cluster and node memory metrics. For more information, see Create a cluster. To view more detailed metrics of Elastic Compute Service (ECS) instances, go to the CloudMonitor console to view the ECS monitoring metrics. For more information, see Metrics.

Monitoring metrics description

Cluster monitoring metrics

Monitoring metrics	Dimension	Unit	Minimum monitoring granularity	Means of aggregation
CPU usage	Cluster dimension	Percentage	60 seconds	Average
Network inbound traffic	Cluster dimension	bit/s	60 seconds	Average

User Guide• Monit oring

Monitoring metrics	Dimension	Unit	Minimum monitoring granularity	Means of aggregation
Network outbound traffic	Cluster dimension	bit/s	60 seconds	Average
Memory usage	Cluster dimension	Percentage	60 seconds	Average
GPU memory usage	Cluster dimension	Bytes	60 seconds	Average
GPU usage	Cluster dimension	Percentage	60 seconds	Average
GPU temperature	Cluster dimension	Degree centigrade	60 seconds	Average

Node monitoring metrics

Monitoring metrics	Dimension	Unit	Minimum monit oring granularit y	Means of aggregation
CPU usage	Node dimension	Percentage	60 seconds	Average
Network inbound traffic	Node dimension	bit/s	60 seconds	Average
Network outbound traffic	Node dimension	bit/s	60 seconds	Average
Memory usage	Node dimension	Percentage	60 seconds	Average
GPU memory usage	Node dimension	bytes	60 seconds	Average
GPU usage	Node dimension	Percentage	60 seconds	Average
GPU temperature	Node dimension	Degree centigrade	60 seconds	Average

Service monitoring metrics

Monitoring metrics	Dimension	Unit	Minimum monitoring granularity	Means of aggregation
CPU usage	Service dimension	Percentage	60 seconds	Average
Network inbound rate	Service dimension	Bytes/s	60 seconds	Average
Network outbound rate	Service dimension	Bytes/s	60 seconds	Average
Service I/O read	Service dimension	Bytes	60 seconds	Average

Container Service

Monitoring metrics	Dimension	Unit	Minimum monitoring granularity	Means of aggregation
Service I/O write	Service dimension	Bytes	60 seconds	Average
Memory usage	Service dimension	Bytes	60 seconds	Average
Memory usage	Service dimension	Percentage	60 seconds	Average
Network inbound traffic	Service dimension	Bytes	60 seconds	Average
Network outbound traffic	Service dimension	Bytes	60 seconds	Average
Container I/O read rate	Container dimension	Bytes/s	60 seconds	Average
Container I/O write rate	Container dimension	Bytes/s	60 seconds	Average
Service GPU memory usage	Service dimension	Bytes	60 seconds	Average

Container monitoring metrics

Monitoring metrics	Dimension	Unit	Minimum monitoring granularity	Means of aggregation
CPU usage	Container dimension	Percentage	60 seconds	Average
Network inbound rate	Container dimension	Bytes/s	60 seconds	Average
Network outbound rate	Container dimension	Bytes/s	60 seconds	Average
I/O read	Container dimension	Bytes	60 seconds	Average
I/O write	Container dimension	Bytes	60 seconds	Average
Memory usage	Container dimension	Percentage	60 seconds	Average
Memory usage	Container dimension	Bytes	60 seconds	Average
Network inbound traffic	Container dimension	Bytes	60 seconds	Average

Monitoring metrics	Dimension	Unit	Minimum monitoring granularity	Means of aggregation
Network outbound traffic	Container dimension	Bytes	60 seconds	Average
Container I/O read rate	Container dimension	Bytes/s	60 seconds	Average
Container I/O write rate	Container dimension	Bytes/s	60 seconds	Average
GPU memory usage	Container dimension	Bytes	60 seconds	Average

Precautions:

Go to the CloudMonitor console to view history monitoring data or set monitoring alarm rules.

- Monitoring data is preserved for at most 31 days.
- You can view monitoring data for at most 14 consecutive days.
- You can set the alarm rules in batches.

14.8. What if the auto scaling rule does not take effect

If your created container auto scaling rule or node auto scaling rule does not take effect, you can perform troubleshooting according to the following methods.

View monitoring metrics, and confirm that monitoring metrics have data and the data reaches the configured threshold for a certain period of time

- View the monitoring metrics of container auto scaling
 - i. Click Services in the left-side navigation pane.
 - ii. Select the cluster in which the service resides from the Cluster drop-down list.
 - iii. Click Monitor at the right of the service.

You are redirected to the CloudMonitor console and can view the container monitoring information. Confirm that monitoring metrics have data and the data reaches the configured threshold for a certain period of time.

(?) Note When determining whether the monitoring metric value exceeds the configured upper limit or lower limit, Container Service uses the average value of the monitoring metrics (namely, the average CPU usage and the average memory usage) within a sample period (one minute). Container Service triggers scaling only when the average monitoring metrics of three consecutive sample periods all exceed the configured upper limit or lower limit so as to avoid frequent scaling caused by monitoring data jitter.



- View the monitoring metrics of node auto scaling
 - i. Click Clusters in the left-side navigation pane.
 - ii. Click Monitor at the right of the cluster.

You are redirected to the CloudMonitor console and can view the cluster monitoring information. Confirm that monitoring metrics have data and the data reaches the configured threshold for a certain period of time.

? Note When determining whether the monitoring metric value exceeds the configured upper limit or lower limit, Container Service uses the average value of the monitoring metrics (namely, the average CPU usage and the average memory usage) within a sample period (one minute). Container Service triggers scaling only when the average monitoring metrics of three consecutive sample periods all exceed the configured upper limit or lower limit so as to avoid frequent scaling caused by monitoring data jitter.



If no monitoring data is displayed

Check the following possibilities: Whether or not the monitoring service (acsmonitoring) is correctly installed (whether or not the status and number of containers are correct). If not, redeploy the monitoring service (acsmonitoring). Whether or not the cluster Agent is in the latest version. If not, upgrade the cluster Agent. Whether or not the monitoring service (acsmonitoring) is in the latest version. If not, upgrade the monitoring service (acsmonitoring service (acsmonitoring). For more information, see Upgrade system services and Upgrade Agent.

View monitoring alarm rules and status, and confirm the rules are created and in the correct status

1. In the CloudMonitor console, clickCloud Service Monitoring > Container Service in the left-side navigation pane.

You can view the cluster list.

2. Click **View All Rules** on the Clusters page to view the alarm rules automatically configured by auto scaling.

Clusters		C Refresh
Enterto search	Search Application Groups	
Cluster Name Status Network	Region Monitor	Actions
kBs-test Running VPC	China East 1 Node Monitoring Service Monitoring Container Service Monitoring (Hangzhou)	Monitoring Charts Alarm Rules
routing-test-online Running VPC	China East 1 Node Monitoring Service Monitoring Container Service Monitoring (Hangzhou)	Monitoring Charts Alarm Rules
Set Alarm Rules View All Rules		

- If no monitoring alarm rule is displayed
- Update the RAM authorization information in the cluster by completing the following steps: On the **Cluster List** page, click**More > Update RAM Authorization Information** at the right of the cluster. Activate the RAM service before updating the RAM authorization information. Otherwise, the system reports an error.



Aliyun API Error: RequestId: 51C6F096-5A42-41D2-9FC3-16472F34A45A Status Code: 4 04 Code: Inactive Message: Account is inactive to this service

• Check the following possibilities: Whether or not the monitoring service (acsmonitoring) is correctly installed (whether or not the status and number of containers are correct). If not, redeploy the monitoring service (acsmonitoring). Whether or not the cluster Agent is in the latest version. If not, upgrade the cluster Agent. Whether or not the monitoring service (acsmonitoring) is in the latest version. If not, upgrade the monitoring service (acsmonitoring service (acsmonitoring). For more information, see Upgrade system services and Upgrade Agent.

View alarm history

If the status of an alarm rule is abnormal (in the **Alarm** status) on the Alarm Rules page, you can view the alarm history of this rule to locate the problem.

Under Actions, click View at the right of the alarm rule.

Click the **Alarm Logs** tab, and you can select the time to view the alarms occurred within specified time period.

15.DevOps 15.1. Jenkins-based continuous delivery

As an important step in agile development, continuous integration aims to maintain high quality while accelerating product iteration. Every time codes are updated, an automated test is performed to test the codes and function validity. The codes can only be delivered and deployed after they pass the automated test. This document mainly introduces how to integrate Jenkins, one of the most popular continuous integration tools, with Alibaba Cloud Container Service to realize automated test and image building push.

The following example demonstrates how to perform automated test and build a Docker image by using Alibaba Cloud Container Service Jenkins, which realizes high-quality continuous integration.

Background information

Every time codes are submitted to nodejs project in GitHub, Alibaba Cloud Container Service Jenkins will automatically trigger a unit test. If the test is successful, Jenkins continues to build images and then pushes them to a target image repository. Finally, Jenkins notifies you of the results by email.



A general process is as follows.

Slave-nodejs is a slave node used for unit test and building and pushing the image.

Jenkins introduction

Jenkins is an open-sourced continuous integration tool developed on Java. It monitors and triggers continuously repeated work and supports expansion of multiple platforms and plug-ins. Jenkins is an open-sourced tool featuring easy installation and interface-based management. It uses job to describe every work step, and node is a project execution environment. The master node is a default execution environment of a Jenkins job and also the installation environment for Jenkins applications.

Master/slave

Master/slave is equivalent to the server/agent concept. A master provides Web interface with which you manage the job and slave. The job can run on the master or be assigned to the slave. One master can be associated with several slaves to serve different jobs or different configurations of the same job.

Several slaves can be configured to prepare a separate test and building environment for different projects.

(?) **Note** The Jenkins job and project mentioned in this document all refer to a build unit of Jenkins, namely, an execution unit.

Step 1 Deploy Jenkins applications and slave nodes

The building and testing of different applications need different dependencies. The best practice is to use different slave containers with corresponding runtime dependencies and tools to perform the test and building. By using the slave images and sample templates provided by Alibaba Cloud Container Service for different environments such as Python, Node.js, and Go, you can quickly and easily generate Jenkins applications and various slave nodes, configure node information in Jenkins applications, and specify the execution nodes in the build projects so as to implement the entire continuous integration process.

Note For images provided by Alibaba Cloud Container Service for developing slave nodes, see https://github.com/AliyunContainerService/jenkins-slaves.

1.1 Create a Jenkins orchestration template

Create a template and create the orchestration based on the following contents.

The labels supported by Alibaba Cloud Container Service Jenkins master are: 1.651.3, 2.19.2, and 2.32.2.

(?) Note For how to create an orchestration template, see Create an orchestration template.

```
jenkins:
   image: 'registry.aliyuncs.com/acs-sample/jenkins:1.651.3'
   volumes:
       - /var/lib/docker/jenkins:/var/jenkins home
   restart: always
   labels:
       aliyun.scale: '1'
       aliyun.probe.url: 'tcp://container:8080'
       aliyun.probe.initial_delay_seconds: '10'
       aliyun.routing.port 8080: jenkins
   links:
       - slave-nodejs
slave-nodejs:
   image: 'registry.aliyuncs.com/acs-sample/jenkins-slave-dind-nodejs'
   volumes:
       - /var/run/docker.sock:/var/run/docker.sock
   restart: always
   labels:
       aliyun.scale: '1'
```

1.2 Use the template to create Jenkins application and slave node

Use the orchestration template created in the preceding section or the Jenkins sample template provided by Alibaba Cloud Container Service to create the Jenkins application and slave node.

Note For how to create an application by using an orchestration template, see Create an application.

Orches	tration List Sample My Orchestrations		Search Create
Ø	gitlab Details VI	Service:Image postgresql : registry.cn-hangzhou.aliyuncs.com/acs-sample/postgresql-sameersbn:9.4-24 gittab : registry.cn-hangzhou.aliyuncs.com/acs-sample/gittab-sameersbn:latest redis : registry.cn-hangzhou.aliyuncs.com/acs-sample/redis-sameersbn:latest	Create Application ->
00 00	jenkins Details VI	Service:Image jenkins : registry.cn-hangzhou.aliyuncs.com/acs-sample/jenkins:2.60.3 slave-golang : registry.aliyuncs.com/acs-sample/jenkins-slave-dind-golang slave-java : registry.aliyuncs.com/acs-sample/jenkins-slave-dind-java slave-nodejs : registry.aliyuncs.com/acs-sample/jenkins-slave-dind-nodejs slave-python : registry.aliyuncs.com/acs-sample/jenkins-slave-dind-python slave-php : registry.aliyuncs.com/acs-sample/jenkins-slave-dind-php	Create Application +

After a successful creation, the Jenkins application and slave node are displayed in the service list.

Application;	jenkins								Refresh
Overview									
Name: jen	ikins				Time Created: 2	018-01-16	Time Updated: 2018-01-16	Cluster: test	
Trigger 1.	You can only	have one	of each trigg	ger type.@					Create Trigger
No trigger is	available at t	he moment	. Click "Crea	te Trigger'	in the upper-right corne	r.			
Services	Containers	Logs	Events	Routes					
Name	Ap	plication	Status	5	Container Status	Image			Action
jenkins	je	nkins	Rea	ady	Ready:1 Stop:0	registry.cn-hangzhou	u.aliyuncs.com/acs-sample/jen		Stop Restart Reschedule Update Delete Events
slave-golang	j je	nkins	● Rea	ady	Ready:1 Stop:0	registry.aliyuncs.con	n/acs-sample/jenkins-slave-d		Stop Restart Reschedule Update Delete Events
slave-java	je	nkins	● Rea	ady	Ready:1 Stop:0	registry.aliyuncs.con	n/acs-sample/jenkins-slave-d		Stop Restart Reschedule Update Delete Events
slave-nodejs	s je	nkins	● Rea	ady	Ready:1 Stop:0	registry.aliyuncs.con	n/acs-sample/jenkins-slave-d		Stop Restart Reschedule Update Delete Events

Open the access endpoint provided by Container Service to use the deployed Jenkins application.

Service:jenkir	ns_jenkin:	5									Re	efresh Scale
Overview												
Service Nan	ne: jenkin	IS		Application: jer	nkins	Is Image: registry.cn-hangzhou.aliyuncs.com/acs-sample/jenkins:2.60.3					Number: 1	Ready
Access End	point: http	p://jenkins.i	nd een	marcarta-shoeld	sacaeousda 1115	.cn-hangzhou	.alicontainer.co	m				
Containers	Logs	Configura	ations	Events								
Name/ID		Statu	5	Health Check	Image		Port	Container IP	Node IP			Action
jenkins_jenki 8402cbd5713	ns 0	runni	ng	Normal	registry.cn- sha256:a33	nang 929a9c	8080/tcp 50000/tcp	17218-68	192,168,381,239	Delete Stop	Monitor Logs	Web Terminal

Step 2 Realize automated test and automated build and push of image

2.1 Configure the slave container as the slave node of the Jenkins application

Open the Jenkins application. Click Manage Jenkins in the left-side navigation pane. Click Manage Nodes on the right pane. Click New Node in the left-side navigation pane. Enter the node name and then click OK. Then, complete the parameters as follows.

Name	slave-nodejs-ut	
Description	slave-nodejs-ut	0
# of executors	1	
Remote root directory	Vry homeljenkins	
Labels	slave-nodejs-ut	
Usage	Utilize this node as much as possible	• 0
Launch method	Launch slave agents on Unix machines via SSH	• 0
Г	Host 172 IBD I	
	Credentials jenkins/****** • • Add •	Ø
		Advanced
Availability	Keep this slave on-line as much as possible	• @
Node Properties		
 Environment variable Tool Locations Save 	iables	

? Note

- Label is the unique identifier of the slave.
- The slave container and Jenkins container run on the Alibaba Cloud platform at the same time. Therefore, enter a container node IP address that is inaccessible to the Internet to isolate the test environment.
- When adding the credentials, use the jenkins account and password (the initial password is jenkins) in Dockerfile for the creation of the slave-nodejs image. The image Dockerfile address is jenkins-slave-dind-nodejs.

2.2 Create a project to implement automated test

- 1. Go back to the Jenkins home page. Click New Item in the left-side navigation pane. Enter the item name, select Freestyle project, and then click OK.
- 2. Enter the project name and select a node for running the project. In this example, enter the slavenodejs-ut node prepared in the preceding section.

Project name	nodejs-ut	
Description		
	[Plain text] Preview	
GitHub project	I tain toxi I Torion	
Project url	Lu. 11-14. L	
,	nttps://github.com/qinyujia/containero	ps/
		Advanced
GitLab connection	gitlab	
Discard Old Builds		
This build is parameter	ized	
Disable Build (No new	builds will be executed until the project is	re-enabled.)
Execute concurrent bui	ilds if necessary	
Restrict where this proj	ect can be run	
Label Expression	slave-nodejs-ut	
	Label is serviced by 1 node	

3. Configure the source code management and code branch. In this example, use GitHub to manage source codes.

None		
CVS		
CVS Projectset		
Git Repositories	Repository URL	
	https://github.com/qinyujia/containerops.git	
	Credentials 756 com/***** + Add -	
		Advanced
		Add Repository Delete Repository
Branches to build	Branch Specifier (blank for 'any') •/jenkins-test	
		Add Branch Delete Branch

4. Configure the build trigger. In this example, automatically trigger project execution by combining Git Hub Webhooks & services.

Bu	Ild Triggers	
	Build after other projects are built	0
	Build periodically	0
	Build when a change is pushed to GitHub	0
	Build when a change is pushed to GitLab. GitLab CI Service URL: http://jenkins.c11267d36daf04ee3960854773128225e.cn-hangzhou.alicontainer.com/project/test2	0
	Poll SCM	0

5. Add the Jenkins service hook to GitHub to implement automatic triggering.

On the GitHub project home page, click the Settings. Click Webhooks & services, click Add Service, and then select Jenkins(Git plugin) from the drop list. In the dialog box of Jenkins hook url, enter \${Jenkins IP}/github-webhook/. For example:

qinyujia / containerops forked from ringtail/containerops	O Unwatch ▼ 1 ★ Star 0 Ÿ Fork
<> Code	🎹 Projects 0 💷 Wiki 🦘 Pulse 🔟 Graphs 🗘 Settings
Options	Services / Add Jenkins (Git plugin)
Collaborators	Install Notes
Branches	
Webhooks	 Requires Git Plugin v1.1.18, released 2012-04-27, and the "Poll SCM" build trigger needs to be enabled. (Though you can have it poll very infrequently, I recommend something like @ */3 * * *)
Integrations & services	 "Jenkins Url" is the base URL of your Jenkins server. For example: http://ci.jenkins-ci.org/. We will hit /eit/notifyCommit_under this URL (See the Git plugin wiki page for more details.)
Deploy keys	
	Jenkins is a popular continuous integration server. If you're using the standard Jenkins Git plugin to poll & check out your repository, you can quickly and easily switch to a push model using this service. It will send a request to your Jenkins instance telling it about the repositories and branches that changed. Jenkins will then poll the repository and build if needed. See push notification from repository on the Jenkins wiki for information.
	Jenkins url http://jenkins.c112 -hang
	Active

6. Add a build step of Execute shell type and write shell scripts to perform the test.

Build		
Execute	shell	0
Command	pwd ls cd chapter2 npm test	
	See the list of available environment variables	3

The commands in this example are as follows:

pwd ls cd chapter2 npm test

SVN source code example:

Select **Subversion** in Source Code Management and enter the SVN repository address in the Repository URL field (if the Jenkins master and SVN server are in different time zones, add **GHEAD** at the end of the repository address). Add the username and password of the SVN server in Credentials.

Source Code Managemen	t		
O None			
CVS			
CVS Projectset			
Git			
Repositories	Repository URL https://github.com/qinyujia/containerops.git		0
	Credentials 756 Add -		
		Advanced	
		Add Repository Delete Repository	
Branches to build	Branch Specifier (blank for 'any') •/jenkins-test		0
		Add Branch Delete Branch	

Configure the build trigger. In this example, Post-commit hook is used to automatically trigger the project execution. Enter your configured token in Token Name .

Build Triggers		
 Build after other 	projects are built	0
Projects to watch nodejs-ut	nodejs-ut	
	O Trigger only if build is stable	
	Trigger even if the build is unstable	
	 Trigger even if the build fails 	
 Build periodically 		
 Build when a cha 	ange is pushed to GitHub	
 Build when a cha build 	ange is pushed to GitLab. GitLab CI Service URL: http://jenkins.c11267d36daf04ee3960854773128225e.cn-hangzhou.alicontainer.com/project/nodejs-	
Poll SCM		

Log on to the SVN server. Create a *post-commit* file in the *hooks* directory of the code repository (svn-java-demo).

cd	/hc	ome/	svn/	′svn-ja	va-demo/hooks
ср	pos	st-c	ommi	t.tmpl	post-commit
chr	nod	755	pos	st-comm	it

Add the curl -u \${Jenkins_account}:\${password}

in the <g id="1">post-commit</g> file. For example:

```
curl -u test:test
http://127.0.0.1:8080/jenkins/job/svn/build?token=qinyujia
```

2.3 Create a project to automatically build and push images

- 1. Go back to the Jenkins home page. Click New Item in the left-side navigation pane. Enter the item name, select Freestyle project, and then click OK.
- 2. Enter the project name and select a node for running the project. In this example, enter the slavenodejs-ut node prepared in the preceding section.
- 3. Configure the source code management and code branch. In this example, use GitHub to manage source codes.
- 4. Add the following trigger and set to automatically build the image only after the unit test is successful.

Build Triggers				
 Build after other j 	projects are built	0		
Projects to watch	ich nodejs-ut			
	 Trigger only if build is stable 			
	Trigger even if the build is unstable			
	O Trigger even if the build fails			
 Build periodically 		?		
Build when a character	nge is pushed to GitHub	?		
 Build when a cha build 	nge is pushed to GitLab. GitLab CI Service URL: http://jenkins.c11267d36daf04ee3960854773128225e.cn-hangzhou.alicontainer.com/project/nodejs-	0		
Poll SCM		?		

5. Write the shell script for building and pushing images.

Execute shell	
Command cd chapter2 sudo docker build -t registry.aliyuncs.com/qinyujia-test/nodejs-demo . sudo docker login -u \${yourAccount} -p \${yourPassword} registry.aliyuncs.com sudo docker push registry.aliyuncs.com/qinyujia-test/nodejs-demo	
See the list of available environment variables	
	Delete

The commands in this example are as follows:

```
cd chapter2
sudo docker build -t registry.aliyuncs.com/qinyujia-test/nodejs-demo .
sudo docker login -u ${yourAccount} -p ${yourPassword} registry.aliyuncs.com
sudo docker push registry.aliyuncs.com/qinyujia-test/nodejs-demo
```

Step 3 Automatically redeploy the application

3.1 Deploy the application for the first time

Use the orchestration template to deploy the image created in step 2.3 to Container Service and create the nodejs-demo application.

Example:

```
express:
image: 'registry.aliyuncs.com/qinyujia-test/nodejs-demo'
expose:
        - '22'
        - '3000'
restart: always
labels:
        aliyun.routing.port_3000: express
```

3.2 Automatic redeployment

- 1. Select the created application nodejs-demo and create the trigger.
 - Onte For how to create a trigger, see Triggers.

Trigger 1. You can only have one of each trigger type.		Cr	eate Trigger 🔷
Trigger Link (move mouse over to copy)	Secret (move mouse over to copy)	Туре	Action
https://undefined/hook/trigger?triggerUrl=Y2kHW11NTkMzhZTQxMzhW1bhNigyY2caxHiY3NzhFGpbmtpbnN8cmVkZX8sb38MTjYTNiMTYy8cmVkZX8sb38MTjYTNiMTYy8cmVkZX8sb38MTjYTNiMTYy8cmVkZX8sb38MTjYTNiMTYy8cmVkZX8sb38MTjYTNiMTYy8cmVkZX8sb38MTjYTNiMTYy8cmVkZx8sb38MTjYTNiMTY	74386f737245553732703738674b7966439e	Redeploy	Delete Trigger

2. Add a line to the shell script in 2.3. The address is the trigger link of the created trigger.

curl 'https://cs.console.aliyun.com/hook/trigger?triggerUrl=***==&secret=***'

3. Change the command in the example of 2.3 as follows:

```
cd chapter2
sudo docker build -t registry.aliyuncs.com/qinyujia-test/nodejs-demo .
sudo docker login -u ${yourAccount} -p ${yourPassword} registry.aliyuncs.com
sudo docker push registry.aliyuncs.com/qinyujia-test/nodejs-demo
curl `https://cs.console.aliyun.com/hook/trigger?triggerUrl=***==&secret=***'
```

After pushing the image, Jenkins automatically triggers the redeployment of the nodejs-demo application.

Step 4 Configure email notification of the results

To send the unit test or image building results to relevant developers or project execution initiators by email, perform the following configurations:

1. On the Jenkins homepage, click Manage Jenkins > Configure System, and configure the Jenkins system administrator email.

Jenkins Location		
Jenkins URL	http://jenkins.c11267d36daf04ee3960854773128225e.cn-hangzhou.alicontainer.com/	0
System Admin e-mail address	jenkins-cs@alibaba-inc.com	0

2. Install the Extended Email Notification plug-in, configure the SMTP server and other relevant information, and then set the default email recipient list, as shown in the following figure:
| E-mail Notification | | |
|---|----------------------------|---|
| SMTP server | smtp.alibaba-inc.com | Ø |
| Default user e-mail suffix | | Ø |
| Use SMTP Authentication | | 0 |
| User Name | jenkins-cs@alibaba-inc.com | |
| Password | | |
| Use SSL | | 0 |
| SMTP Port | 465 | Ø |
| Reply-To Address | | |
| Charset | UTF-8 | |
| Test configuration by sending test e-mail | | |

The preceding example shows the parameter settings of the Jenkins application system. The following example shows the relevant configurations for Jenkins projects whose results are to be pushed by email.

3. Add post-building steps in the Jenkins project, select Editable Email Notification and enter the email recipient list.

Add build step -		
Post-build Actions		
Editable Email Notification		0
Disable Extended Email Publishe	ar 🗌	0
	Allows the user to disable the publisher, while maintaining the settings	
Project Recipient List	@alibaba-inc.com	
		0
		U

4. Add a trigger to send emails.

Triggers	Always	Ø
	Recipient List	2 Delete
	Developers	(2) Delete
	Requestor	Detete
	Add 👻	Advanced
		Remove Trigger

16.Service discovery and load balancing

16.1. Overview

Service discovery and Server Load Balancer mainly solves the issue of communication reliability. To guarantee the reliability, Container Service introduces Server Load Balancer. Communication is divided into two types: communication that exposes services and communication between internal services. See the following scenarios for different solutions.

Scenario 1

We recommend that you use simple routing service for simple Layer-7 protocol Server Load Balancer and web service reverse proxy. For more information, see Simple routing - supports HTTP and HTTPS, Simple routing - Configure domain names, and Simple routing - Change HTTP to HTTPS.

Scenario 2

Server Load Balancer distributes the loads evenly to containers with the same functions in Layer-4 protocol Server Load Balancer and services of non-container clusters access the services of containers in container clusters when a traditional architecture is migrated to a container architecture. We recommend that you use Server Load Balancer routing.

Scenario 3

Services in the same cluster need to discover and communicate with each other, and need the Server Load Balancer capabilities. We recommend that you use 集群内服务间路由和负载均衡

Scenario 4

Services in the same cluster need to discover and communicate with each other, but do not need the Server Load Balancer capabilities. We recommend that you use Service discovery between containers.

Scenario 5

Server Load Balancer and service discovery have high customization requirements, such as the support for extensive domain names, custom error page, record accessing logs, selection of backend services based on URL parameter values, and custom HAProxy configuration files. We recommend that you use Custom routing - User guide. For more information, see Custom routing - simple sample.

16.2. Simple routing - supports HTTP and HTTPS

Scenarios

Simple Layer-7 protocol load balancingWeb routing service Services in a container cluster access each other using Layer-7 protocol by means of communication proxy and Server Load Balancer

Principles

See the following figure. When you create a cluster, a Server Load Balancer instance is assigned to the cluster by default. The Server Load Balancer instance adds all the nodes in the cluster to the backend. Port 80 is exposed at the frontend, and port 9080 is exposed on the machines of all the backend nodes. Container Service starts a routing application acsrouting, namely, the Alibaba Cloud Container Service Routing. The Server Load Balancer instance adds all the nodes in the cluster to the backend. Port 80 is exposed at the frontend, and port 9080 is exposed on the machines of all the backend. Port 80 is exposed at the frontend, and port 9080 is exposed on the machines of all the backend nodes. Container Service starts a routing application acsrouting in namely, the Alibaba Cloud Container Service starts a routing application acsrouting in namely, the Alibaba Cloud Container Service Routing. This routing application has only one service, the routing service. The routing service is global, which means a copy of this service (or image), namely, a container, is deployed on each node (a node is also called a host or a virtual machine (VM) instance of Elastic Compute Service (ECS)). The routing service (ECS)). is also called a host or a virtual machine (VM) instance of Elastic Compute Service (ECS)). Each node uses this container to route HTTP services or HTTPS services.



As shown in the preceding figure, for HTTP services, the mapping between Server Load Balancer instance frontend and backend ports is 80:9080, and the port mapping between the host and the container used for routing is 9080:80, indicating that port 80 is exposed on the containers used for routing. Any ports can be exposed on the other containers used as the web service. After you set the port mapping between host and container during container startup, the routing service can obtain the corresponding port for request routing.

Setup methods

? Note Make sure that the following kernel parameters (in the /etc/sysctl.conf file) of the related Container Service nodes are set to 0. Otherwise, the nodes might not be accessed.

```
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.all.rp_filter = 0
net.ipv4.conf.eth0.rp filter = 0
```

Set in the Container Service console

Set by Services > Update

- 1. Log on to the Container Service console.
- 2. Log on to the Container Service console.
- 3. Click Services in the left-side navigation pane.
- 4. Select the cluster in which the service to be exposed resides from the Cluster list.
- 5. Click Update at the right of the service to be exposed (wordpress in this example).

Container Service	Service List					Refresh					
Overview	Help: If How to expose services to the Internet If Add a domain name to a service exposed to the public network If Switch from HTTP to HTTPS If Change application external port										
Applications	Cluster: test 🔻 🗶 2	system Services 🗉 Hide Offlin	ne Services 🗏 Hide Online Serv	lices	Name	۲ Q Ж					
Services 1	Name	Application	Status	Container Status	Image	Action					
Clusters Nodes	nginx	nginx	Running	Running:1 Stop:0	nginx:latest	Monitor Stop Reschedule Update Delete Restart Events					
Networks Data Volumes Configurations	wordpress	wordpress	Running	Running:1 Stop:0	wordpress:latest	Monitor Stop Reschedule Update Delete Restart Events					
Images and Tem					Total: 7 iter	n(s) , Per Page: 15 V item(s) 《 < 1 > »					

6. Configure the port mapping between host and container on the Update Service page.

The host port is empty, indicating that a random port on the host is exposed (when HTTP or HTTPS port 80 of the wordpress service to provide the HTTP service. The protocol used is TCP. services are exposed, you do not need to know what port is exposed on the host, because the container port can be directly accessed by using an overlay network or Virtual Private Cloud (VPC) network). The container port is 80. Use port 80 of the wordpress service to provide the HTTP service. The protocol used is TCP.

Port Mapping:	• Add domain names to services exposed to the p	oublic network	(
	Host Port		Container Port		Protocol				
	e.g. 8080 > 80 / TCP								
Web Routing:	The host port cannot be set to9080,2376,3376 Expose HTTP services through acsrouting								
	Container Port	Domain							
[80	http://wo	rdpress		•				
	Note: All domain names for a port must be entered	l in one entry							

Routing configuration exposes the service by using a domain name. Specify the port to be exposed (port 80 of the wordpress service in this example). Enter the domain name prefix in the Domain field. If the domain name prefix is XXX, the domain name

XXX.\$cluster_id.\$region_id.alicontainer.com is obtained for testing. In this example, the domain name wordpress.cb668bde43f054cd7bd515c8739f38310.cn-hangzhou.alicontainer.com is obtained. You can enter your own domain name, which needs to add the resolution to the IP address of the corresponding Server Load Balancer instance. XXX, the domain name xxx.\$cluster _id.\$region_id.alicontainer.com is obtained for ______ is obtained for testing. In this example, the domain name wordpress.cb668bde43f054cd7bd515c8739f38310.cn-hangzhou.alicontainer.com _______ is obtained. You can enter your own domain name, which needs to add the resolution to the IP address of the corresponding Server Load Balancer instance. For how to configure the container port used for routing and the domain name of HTTP services, see routing.

7. Click **Update** after completing the configurations. Click the service name on the **Service List** page and then click the access endpoint

Service:wordp	ervice:wordpress_wordpress Refresh Scale												
Overview													
Service Name: wordpress Application: wordpress Image: wordpressletest Number: 1 • Running													
Access Endpoint: http://wordpress.edfordelit&out_aktility.uktility.edu/aktility.e													
Containers	Logs	Conf	igurations	Events									
Name/ID			Status	Health Check	Image	Port	Container IP	Node IP				Action	
wordpress_wo 5f9e5c651918	ordpr () 36f51		running	Normal	wordpress:latest sha256:34947222d	80/tcp	171.18.0.5	192,168,340,213	Delete Stop Monitor Logs Web Terminal				



8. to access the wordpress page. The wordpress welcome page appears.

Set by application template editor

- 1. Log on to the Container Service console.
- 2. Log on to the Container Service console.
- 3. Click **Applications** in the left-side navigation pane.
- 4. Select the cluster from the Cluster list.
- 5. Click **Update** at the right of the application (wordpress in this example).

Container Service	Application List. Refresh Create A											
Overview	Help: 🖉 Create an application 🧳 Change application configurations 🖉 Simple route blue-green release policy 🧳 Container auto scaling											
Applications 1	Cluster: swarm-test 🔻 🗷 Hide	Name 🔻										
Services	Name Description	Status	Container Status	Time Created 🔺	Time Updated 🔺	۸						
Clusters Nodes	wordpress	Ready	Ready:3 Stop:0	2017-09-01 10:23:22	2017-09-01 10:53:36	Stop Update Delete	Redeploy					

6. Add a routing label in Template, define the corresponding domain name or domain name prefix, update the application version, and confirm whether or not to pull the latest Docker image. routing corresponding domain name or domain name prefix, update the application version, and confirm whether or not to pull the latest Docker image. Then, click **OK** to update the domain name.

Change Configurat	tion	\times
Name: *Version:	wordpress 1.3 Note: The version of the application must be changed; otherwise, the "OK" button is not available.	
Description:		
Use Latest Image:	Force O @ Reschedule :	
Release Mode:	Standard Release 🔻 🕖	
Template:	<pre>1 • wordpress-web: 2 image: registry.aliyuncs.com/acs-sample/wordpress :yunqi 3 · ports: 4</pre>	
	ОК Са	ncel

7. Click the application name on the Application List page and then click the Routes tab. Click the **Route address** to access the wordpress welcome page.

Services	Containers	Logs	Events	Routes		
Route Addr	ess					Action
wordpress.	adik be 062 ha be	Ac035:345	265409155	osilum-hang	zhou.alicontainer.com	Set service weight

Set by client

- docker help run: View the used "-p" option. Set the routing configuration in the Container Service console.
- docker-compose: View the supported "ports" option . For routing configuration rules, see routing.

16.3. Simple routing - Configure domain names

Context

Procedure

- 1. Log on to the Container Service console.
- 2. Click Swarm > **Services** in the left-side navigation pane.
- 3. Select the cluster in which the service you want to add a domain name resides from the Cluster drop-down list.
- 4. Click **Update** at the right of the service you want to add a domain name (the service web of the application wordpress in this example).

Applications	Cluster: t	est	v ⊗⊦	lide System Servic	es 🗉 Hide Offline Services	Hide Online Services	Name 🔻	Q X
Services	Name	Application	0	Status	Container Status	Image		Action
Clusters Nodes	db	wordpress	9	Ready	Ready:1 Stop:0	registry.aliyuncs.com/acs-sample/mysql:5.7		Monitor Stop Reschedule Update Delete Restart Events
Networks Data Volumes Configurations	web	wordpress		Ready	Ready:3 Stop:0	registry,aliyuncs.com/acs-sample/wordpress:4.	.5	Monitor Stop Reschedule Update Delete Restart Events

5. Click the plus icon next to **Web Routing**. Enter the domain name to be added (www.51ili.com is added in this example), and click **Update** to update the configurations.

? Note To add multiple domain names under the same port for the same service, enter the domain names in one entry and separate them by semicolons (;).

Web Routing:	Expose HTTP services through acsrouting	
	Container Port	Domain
	80	wordpress;www.51ili.com
	Note: All domain names for a port must be entered	in one entry.

Wait until the service finishes the update and changes to the Ready status. After that, the routing service acsrouting_routing finishes configuring the domain name. When requests containing the domain name www.51ili.com are sent to access the service web, the requests can be correctly resolved and forwarded to the corresponding service.

- 6. Resolve the domain name to the Container Service cluster. When you create a cluster, Container Service assigns a Server Load Balancer instance to the cluster by default. The assigned Server Load Balancer instance only belongs to you.
 - i. Log on to the Container Service console.
 - ii. Click Swarm > Clusters in the left-side navigation pane.
 - iii. Click Manage at the right of the cluster (test in this example).

Applications	Name 🔻										
Services	Cluster Name/ID	Cluster Type	Region	Network Type	Cluster Status	Node Status 🕜	Number of Nodes	Time Created	Docker Version	2	Action
Nodes Networks	test critici incluent pret democratica estima-	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc- lip swiget specificarity	Running	Healthy C	2	2018-01-03 18:10:35	17.06.2-ce	Manage View Monitor	w Logs Delete More≁

iv. Click Load Balancer Settings in the left-side navigation pane and view the Server Load Balancer ID.

Cluster:test		
Server Load Balancer Settings	Set Domain Name	
Server Load Balancer ID:	Ib-3.clim?ips0tv0khik	hy .
Re-bind	Server Load Balancer	Unbind Server Load Balancer

7. Click Products > Server Load Balancer to go to the Server Load Balancer console. View the IP address of the Server Load Balancer instance according to the instance ID.

Basic Information	^
Server Load Balancer ID: Ib-Jun Provide Conductor	Status: Status: Status
Server Load Balancer Name: wchuth-c15M11kba	Region: China East 1 (Hangzhou)
Instance IP Type: Public IP	Zone: cn-hangzhou-f(Master)/cn-hangzhou-e(Slave)
Network Type: Classic Network	
Billing Information	Billing Details Release
Billing Method: Pay by Traffic	Created At: 2018-01-03 18:10:55
Instance IP Address:	Automatic Release Time: -

- 8. Log on to the Alibaba Cloud DNS console and add a DNS record (www.51ili.com in this example).
 - i. Add a domain name. Skip this step if the domain name already exists.
 - ii. Add a DNS record.
 - Type: Select A IPV4 address.
 - Host: Enter www. This is the domain name prefix. You can also enter another prefix.
 - ISP Line: Select Default.
 - Value: Enter the IP address of the bound Server Load Balancer instance.
 - TTL: Select the time.

Add Record		\times
Туре:	A - IPV4 address	
Host	www .51ili.com (?)	
ISP Line:	Default - Return to the default value when the query is not \checkmark (?)	
Value:	114.55.48.61	
TTL:	10 minute(s)	
	Confirm Cance	el

9. Access www.51ili.com .



16.4. Simple routing - Change HTTP to HTTPS

Prerequisites

The HTTP domain name access has been configured. For more information, see Simple routing - Configure domain names.

Procedure

1. HTTPS is supported at the Server Load Balancer layer. To support HTTPS, create a Server Load Balancer certificate.

- i. Log on to the Server Load Balancer console.
- ii. Click **Cert if icates** in the left-side navigation pane and click **Upload Cert if icate** in the upperright corner.

Server Load Bala	Certificates	China North 1 (Qingdao)	China North 2 (B	eijing) Ch	hina North 3 (.	Zhangjiakou)	China North 5 (Huhehaot	China East 1 (Hangzhou)	China East 2 (Shanghai)		-
Testeres		China South 1 (Shenzhen)	Hong Kong As	sia Pacific N	NE 1 (Japan)	Singapore	Asia Pacific SE 2 (Sydney)	Asia Pacific SE 3 (Kuala Lump	our) US East 1 (Virginia)		2
Instances		US West 1 (Silicon Valley)	Middle East 1 (E)ubai) Ge	ermany 1 (Fra	nkfurt)					
Certificates										C Refresh	Upload Certificate
Tags					2 certific	ate(s) have t	een created in this region.	/ou can create up to 100 certif	icate(s).Certificates are on	ly required when	using HTTPS listening.

iii. Enter the certificate information and click Confirm.

Upload Certificate t R	eturn to Certificate List
Certificate Name:	www.example.com
	It must be 1-80 characters in length, , only the letters, digits, and the characters '-''/''.' and '_' are allowed.
*Certificate Region:	 China North 1 (Qingdao) China North 2 (Beijing) China East 1 (Hangzhou) China East 2 (Shanghai) China South 1 (Shenzhen) Hong Kong Singapore US East 1 (Virginia) US West 1 (Silicon Valley) (China East 1 (Hangzhou)) is the current region.
*Certificate Type:	Server Certificate O CA Certificate
*Certificate Content:	The editor is used to verify the format of the certificate, not used to verify the validation of the certificate. Learn more. 1BEGIN CERTIFICATE 2 MITURE/CCA1+PAWIRAETIALD30x4K13P0MARGCS06STb3D0EBR0UAMHYxCzA3BeNV
	3 BAYTARNONQswCQYDVQQIEwJCSjELMAKGA1UEBX/KCQKoxDDAKBgMVBA01AB4MSTEP 4 MA@GA1UECXMGQUXJWVOMQ@wCwYDVQQDEwR0ZXN0MR8wHQYJKoZIhvcNAQkBFhB0 5 ZXN0QGhvdG1haMuVJ29tHBAXDTE0MTEyNDA2HQQNV0XDTI0MTEyMTA2HDQyNVow 6 djELMAkGA1UEBMCQ04xCzAJBgNVBAgTAXJKMQswCQVDVQQHEwJCSjEMAAGGA1UE 7 ChMQQUXJNQ8wDQYDVQQLEwZBTE1ZVU4xDTALBgNVBAMTBHRL:3QxHzAdBgKqhkiG 8 9w0BCQEWERRI:3RAaG90BwFpbC5jb20wgZ8wQQYXCaZIhvcNAQEBBQADgY8AMIGJ 9 AoGBAM7SS3e9+Nj0HKAsRuIDNSsS3UK6b+62YQb2uuhKrp1HMrOx61WSDR2qkAnB 10 coG00Uz3BEE+9DLYNUVQBK7a5gLP5M1Ak4wr4GqQCgjejzzh3DshUzLCCy2rook 11 KUN#TP2+hD1:PTLfr5Mregncas5i2F1XYCH_BTD1VDrcsAn6MBBAGGiafswgmgw
	(PEM Code) Import Sample
*Private Key:	<pre>1BEGIN RSA PRIVATE KEY 2 MIICXAIBAAKBgQDO0kt3vfjY9BygLEbiAzUrEt1Cum/utmEG9rroSq6dRzKzsetV 3 kg0dqpAJwXKBtNFM9/BBPvQy2DVFUASu2koCz+TNQJOMK+BqhsgoI3o884dw7TVM 4 ywgstq6KJCjskUSTJrK0z6xNX3Ejc4HqXGnuYtrBNV118y9SAyL0MXLKQIDAQAB 5 AoGAfe3NxbsGKhN42o4bGsKZPQDfeCHMxayGp5bTd10BtQIE/ST4BcJH+ihAS7Bd 6 6FwQ1KzivNd4QP1Mckemk1CXfsVckd194e8zbJ123Gdwl13v8V+Knd3Hqv5yJ3mP 7 hwWoKimwIBTb2s0ctVryr2f18N4hhyFw1yGp0Vxc1GHkjgECQQD9Cv11sn0wHpP4 8 MdrDHbdb29QrobKyKN8pFcDd+sth+kP6Y8MnCVuAKXCKj5FeIsgVtf1uP0sZjPzz 9 71QQWS1dAkEA0T0KX08gaBQwJhIco/w6hy53GZnrNSp0Pp5xvJuMAafs2eyvmhJm 10 Ev9SN/Pf2VYa1z6FEnBaL0VD6hf6VQIsPQJAX/CZP0W6dzwgvim0J/GcY6eleiWE 11 opgra@hbsb71d/3bz7vtEAn5vchzKB3xvchzK9GP6sU4[ExyHafsw0JA4xf8</pre>
	(PEM Code) Import Sample
	Confirm Cancel

2. After the certificate is successfully created, locate the Server Load Balancer instance that is assigned during cluster creation.

When you create a cluster, Container Service assigns a Server Load Balancer instance to the cluster, and the instance only belongs to you.

- i. Log on to the Container Service console.
- ii. Click **Clusters** in the left-side navigation pane. Click **Manage** at the right of the cluster (test in this example).

	Applications	Name 🔻										
	Services	Cluster Name/ID	Cluster Type	Region	Network Type	Cluster Status	Node Status	Number of Nodes	Time Created	Docker Version	2	Action
	Clusters			10051011							<u> </u>	
ľ	Nodes	test CollictionActorPatitionAllicesIP-0702	Alibaba Cloud Cluster	China East 1 (Hangzhou)	VPC vpc-	Running	No node status 🙄	2	2018-01-10 09:28:17	17.06.2-ce	Manage	View Logs Delete
	Networks				the subscription of the second second						MO	nitor More -

iii. Click Load Balancer Settings in the left-side navigation pane and view the Server Load Balancer ID.

<	Cluster:test
Basic Information	
Load Balancer Se	Server Load Balancer Settings Set Domain Name
User Tags	Server Load Balancer ID: Ib-address to block
Image List	
Container List	Re-bind Server Load Balancer Unbind Server Load Balancer
Events	
Node Scaling	

Click **Products** > Server Load Balancer to go to the Server Load Balancer console. View the **IP address** of the Server Load Balancer instance according to the instance ID.

Basic Information	^
Server Load Balancer ID: Ib-Judiod wile Tomolick Shu	Status: Status: Status:
Server Load Balancer Name: and a comparison of the	Region: China East 1 (Hangzhou)
Instance IP Type: Public IP	Zone: cn-hangzhou-f(Master)/cn-hangzhou-e(Slave)
Network Type: Classic Network	
Billing Information	Billing Details Release ^
Billing Method: Pay by Traffic	Created At: 2018-01-10 09:28:37
Instance IP Address: # (Public IP)	Automatic Release Time: -

3. Click List eners in the left-side navigation pane and click Add List ener. The Add List ener dialog box appears. Enter the port information as follows:



- i. Select HTTPS for the frontend protocol.
- ii. Set the frontend port to 443 and backend port to 9080 (port 9080 is exposed by the routing service acsrouting_routing on each Elastic Compute Service (ECS) host. According to the HTTP HOST header, all the HTTP requests are forwarded on the routing service acsrouting_routing to corresponding containers that provide various services).
- iii. Select the preceding certificate www.example.com .
- iv. Complete other settings based on your needs.
- v. Click Next.

Front-end Protocol [Port]: *	HTTPS • 443 Port range is 1-65535. •
Backend Protocol [Port]: *	HTTP : 9080 Port range is 1-65535.When the front-end protocol is HTTPS, the backend protocol is HTTP.
Peak Bandwidth:	1 M Cancel Instances charged by traffic are not limited by peak bandwidth. Peak bandwidth range is 1-5000.
Scheduling Algorithm:	Weighted Rou 🔻
Use VServer Group:	0
Mutual Authentication:	Disable
Server Certificate : *	www.example.com/100-194011-404018_1466555555_444466
Automatically Enable Listener After Creation:	Enable
Show Advanced Options	
	Next Cancel

4. Complete the settings in the Health Check Configuration step and then click Confirm.

You can select to disable or enable the health check. To enable the health check, enter your own domain name in the **Domain Name** field or enter /haproxy-monitor in the **Health Check Path** field. Otherwise, the health check reports an exception.

Add Lister	ner		\times							
1	Listener Configuration	2.Health Check 3.Success	Þ							
	Health Check: 🕖	Enable								
	Domain Name:	It must be 1-80 characters								
	Health Check Port:	Only letters a-z, numbers 0-9, hyphens (-), and periods (.) are allowed. If no domain is specified, the intranet IP addresses of the ECS instances added in the backend server pool are used. Health Check Port range is 1-65535. Port: By default, the backend server's port is used for health								
	Health Check Path:	/haproxy-monitor The URI of the file page that is used to do the health check. It is recommended using a static page. The URI must be 1-80 characters long, and only the letters a-z,								
		numbers 0-9, and the characters '-' '/' ''%' '?' '#' '& and '=' are allowed.								
	Normal Status Code:	Inttp_2xx I http_3xx ■ http_4xx ■ http_5xx Status code used for successful health check								
	Show – Advanced Options									
		Back Confirm Cance								

5. Click **Confirm** after completing the configurations.

Add Listener					×
1.Listener Co	nfiguration $>$	2.Health Check		3.Success	
0	New listen	er is successfully o	onfigure	d.	
	 New listene The listene 	er is created. er is started.			
	Close this wine	dow to view the new list	ener.		
				Co	nfirm

6. Access the page https://www.example.com.

What's next

After the preceding configurations, to directly redirect to https://www.example.com after accessing
http://www.example.com, see Simple routing - Force redirect from HTTP to HTTPS.

16.5. Simple routing - Force redirect from HTTP to HTTPS

Step 1. Implement the HTTPS protocol to access the helloworld application

1. You can create a "hello world" application by using an orchestration template.

The application template sample is as follows:

```
app:
    ports:
        - 80/tcp
    image: 'registry.cn-hangzhou.aliyuncs.com/linhuatest/hello-world:latest'
    labels:
        # http/https/ws/wss protocol here
        aliyun.routing.port_80: "http://www.example.com"
    restart: always
```

2. After configuring the Server Load Balancer, access the HTTPS website according to Simple routing - Change HTTP to HTTPS Simple routing - change HTTP to HTTPS.



Step 2. Configure the Nginx container to implement a Forced Jump to HTTPS

1. You can configure to force the HTTP request to redirect to HTTPS.

The following example configures an Nginx container and adds the rewrite rules to the configuration file, namely, when request http://www.example.com is received, 301 is returned and the request rewrite rules to the configuration file, namely, when request the configuration file, namely,

when request http://www.example.com is received, 301 is returned and the request 301 is automatically redirected to is automatically redirected to www.example.com .

• Log on to each machine in the cluster. Create the Nginx configuration file /ngx/nginx.conf, which will be mounted to the Nginx container as a volume. which

```
will be mounted
to the Nginx container
as a volume.
```

• The /ngx/nginx.conf is as follows:

```
user nginx;
error log /var/log/nginx/error.log warn;
pid /var/run/nginx.pid;
events {
  worker connections 65535;
http {
 include /etc/nginx/mime.types;
  default type application/octet-stream;
  log_format main '$remote_addr - $remote_user [$time_local] "$request" '
                    '$status $body bytes sent "$http referer" '
                    '"$http user agent" "$http x forwarded for"';
  access log /var/log/nginx/access.log main;
  keepalive timeout 65;
  gzip on;
  server {
     listen 80;
      server name localhost;
      return 301 https://$host$request uri;
```

2. Create an Nginx application by using an orchestration template.

The Nginx sample is as follows:

```
nginx:
    ports:
        - 80:80/tcp # Map to port 80 of the host.
    Image: 'nginx: Latest'
    labels:
        aliyun.global: true # Deploy an Nginx container on each machine to guarantee the
high availability.
    volumes:
        - /ngx/nginx.conf:/etc/nginx/nginx.conf
    restart: always
```

 Configure the listening rules for the Server Load Balancer of the cluster as follows (frontend port 80 > backend port 80, namely, Server Load Balancer frontend port 80 > backend Elastic Compute Service (ECS) instance port

as follows (frontend port 80 > backend port 80, namely, Server Load Balancer frontend port 80 > backend Elastic Compute Service (ECS) instance port 80):

u	stener									Add Listener	Refresh
	Front-end Protocol/Port	Backend Protocol/Port	Status	Forwarding Rules	Session Persistence	Health Check	Peak Bandwidth	Server Group			Action
	HTTPS: 443	HTTP: 9080	Running	Weighted Round Robin	Close	Activated	No limit	-	Configure Details	Add Forwarding Rule	s More +
	TCP: 80	TCP: 80	Running	Weighted Round Robin	Close	Activated 🕖	No limit	-	Configure Details	Add Forwarding Rule	s More v
	Activate Stop	Delete									

4. Verify if the HTTP request is forced to redirect to HTTPS.

When you access http://www.example.com, This means the request is correctly redirected to https://www.example.com.the returned HTTP is as follows. This means the request is correctly redirected to https://www.example.com.



16.6. Server Load Balancer routing

Expose HTTP or HTTPS services

We recommend that you use simple routing service (namely, routing) to expose HTTP or HTTPS services. To build your own routing link, activate a new intranet or Internet Server Load Balancer instance routing to the virtual machine (VM) port by using the Alibaba Cloud extension label lb, and configure the mapping between host and container to route requests.

Scenarios:

In Layer-7 protocol Server Load Balancer, a route is customized for each service. Services of noncontainer clusters access the services in container clusters when a traditional architecture is migrated to a container architecture.

Expose TCP or UDP services

Currently, to expose TCP services, configure a Server Load Balancer instance or a public IP address, and configure the port mapping between host and container by using the Alibaba Cloud extension label lb.

(?) Note To use Server Load Balancing routing, you need to buy a new Server Load Balancer instance. Multiple services cannot share the same Server Load Balancer instance, and the default Server Load Balancer instance of the cluster cannot be used for Server Load Balancer routing.

Scenarios:

In Layer-4 protocol Server Load Balancer, a route is customized for each service. Services of noncontainer clusters access the services in container clusters when a traditional architecture is migrated to a container architecture.

Example:

Expose the Redis service in a container cluster to the Python application outside the container cluster by customizing a Server Load Balancer instance.

1. In the Server Load Balancer console, click **Create Server Load Balancer** in the upper-right corner to purchase and create a Server Load Balancer instance used for routing.

Select Internet as the Instance type in this example. Select Internet or Intranet as the Instance type based on your needs.

Note Server Load Balancer does not support cross-region deployment. Therefore, select the same region in which your Container Service cluster resides.

Se	rver Load Ba	lancer					
	Region	Singapore US West 1	Asia Pacific SE 2 China East 1	2 Asia Pacific SE 3 / China East 2	Asia Pacific NE 1 China South 1	Hong Kong China North 1	US East 1 China North 2
tion		Northern China 3	China North 5	Europe Central 1	Middle East 1		
sic Configura	Zone type	Multi-zone					
Bas	Primary zone	China East 1 Zo	ne F 🔻				
	Backup zone	China East 1 Zo	ne E 🛛 🔫				
ance type	Instance type	e Internet	Intranet				
nd inst	Instance Spe	Select a specific	ation 🔫				
Network a	Bandwidth	By traffic					
Purchase Plan	Quantity	1 ¢ You currently have	e 4 instances. Yo	ou can create 26 m	ore instances		

2. Return to the Server Load Balancer console and name the created Server Load Balancer instance as slb_redis_app. Container Service can use this name or the instance ID to reference the Server Load Balancer instance.

Click **Instances > Server Load Balancer** in the left-side navigation pane. Select the region in which the Server Load Balancer instance resides. Edit the instance name and then click **OK**.

Server Load Bala	Instance	S China North	n 1 (Qingdao)	China North 2 (B	Beijing) China	North 3 (Zhangjiakou)) China North 5 (Hu	hehaote) China East	1 (Hangzhou) China	East 2 (Shanghai)		
Instances		China South	n 1 (Shenzhen)	Hong Kong A	sia Pacific NE 1	(Japan)	Singapore	Asia Pacific SE 2 (S)	vdney) Asia Pacific Si	E 3 (K 2 impur) U	S East 1 (Virginia)		
Castificates		US West 1	(Silicon Valley)	Middle East 1 (Dubai) Germa	iny 1 (Fra	inkfurt)						
Certificates											C Refre	sh Create Server	Load Balancer
Tags	Server L	oad Balancer N	ame 🔻	Enter instance	e names separa	ted by co	mmas S	arch 🔊 Tag					2 0
Logs													
Documentation	Server	Load Balancer ne	Zone	IP Address	i(All) - Stat	tus ·	Network(All) *	Port/Health Check	Backend Server	Instance Specification	Bandwidth Billing Method(All) -	Billing Method(All)	Actions
	B-1ud (None)	31xh9v 🗢	cn-hangzhou f(Master) cn-hangzhou		H(Public 🛛 🛛 F	Running (Classic Network	Not ConfiguredConfigure	Not ConfiguredConfigure	Shared-Performance Instance	Pay by Traffic	Pay-As-You-Go 2018-01-10 15:41:30 Created	Manage More+
4	Serv	er Load Balanc	er Instance Nar	1e :									
-	slb	_redis_app								d-P 3 ance		Pay-As-You-Go	
	The	name must be	1-80 characters	in length, includ	ding Chinese ch	aracters, I	letters, digits	s, hyphens (-), period	s (.), and underscores	(_). Ice	Pay by Traffic	2018-01-10 09:28:37 Created	Manage More +
	C	onfirm Ca	incel									concorror created	

3. Create a listening port.

Click **Configure Listener** at the right of the instance. On the **Configure Server Load Balancer** page, configure listening rules as follows: . select TCP as the listener protocol, add a backend server, and configure the port mapping as 6379:6379. As shown in the following figure.

Protocol and Listener	Backend Servers	Health Check		Submit
Submit				
Protocol and Listener				Modify
Listener Protocol		Listening Port		
TCP		6379		
Scheduling Algorithm		Session Persistence		
Weighted Round-Robin		Disabled		
Access Control		Peak Bandwidth		
Disabled		No Limit		
Idle Timeout				
900 Seconds				
Health Check				Modify
Health Check		Health Check Protocol		
Enabled		TCP		
Response Timeout		Health Check Interval		
5 Seconds		2 Seconds		
Healthy Threshold		Unhealthy Threshold		
3 Times		3 Times		
Backend Servers				Modify
Default Server Group				
ECS Instance ID/Name	Public/Internal IP Address	Port	Weight	
-node2	STATISTICS OF	6379	100	

4. Log on to the Container Service console, select an existing cluster, create an application named redis-demo, and click **Create by Image**.

For how to create an application, see Create an application.

(?) Note Server Load Balancer does not support cross-region deployment. Therefore, the used Container Service cluster must be in the same region as the Server Load Balancer instance created in the preceding steps.

	Basic Information		Configuration	\rightarrow	Done
Name:	redis-demo				
	The name should be 1-64 characters long, and	l can contain numbers, E	nglish letters and hyphens, but cannot start w	ith a hyphen.	
Version:	1.0				
Cluster:	test 🔻				
Update:	Standard Release				
Description:					
	🖉 Pull Docker Image 🕼				
				Create	with Image Create with Orchestration Template

5. Select the redis image and set the **Port Mapping**.

(?) Note The Redis image only enables port 6379 on the container. To route the created Server Load Balancer instance to this container port, you must specify the port mapping between host and container of the Redis image.

In **Port Mapping**, specify the host port as 6379, which is the backend host port bound to the Server Load Balancer instance, and select TCP as the Protocol.

Port Mapping:	• Add domain names to services exposed to the public ne	etwork					
	Host Port		Container Port		Protoc	ol	
	6379	>	6379	1	TCP	۳	۰
	The host port cannot be set to9080,2376,3376						

- 6. To configure custom Server Load Balancer, let the Redis service know the information of the used Server Load Balancer instance by adding a label to the Redis service or configuring the Load Balancer.
 - Add a label to the service. In this example, the label is aligun.lb.port_6379: tcp://slb_redis_app:6379 .

	Labels:	• Label description		
pel		Tag Name	Tag Value	
Lal		aliyun.lb.port_6379	tcp://slb_redis_app:6379	•

The label syntax is as follows, where variables with s are placeholders.

aliyun.lb.port_\$container_port:\$scheme://\$[slb_name|slb_id]:\$front_port

- \$container_port indicates the port to be exposed by the container.
- \$scheme indicates the protocol supported by the listening port of the Server Load Balancer instance, whose value might be tcp , http , https , or udp .
- \$[slb name|slb id] indicates the name or ID of the Server Load Balancer instance.
- front_port indicates the frontend port to be exposed by the Server Load Balancer instance.

For more information, see Alibaba Cloud extension label lb.

• On the **Create Application** page, click the plus icon next to **Server Load Balancer Routing Configuration** and set the information about the Server Load Balancer instance.

This setting corresponds to the label 6379: tcp://slb redis app:6379 .

Load Balancer:	Expose services using custom Server Load 6	Balancer		
	Container Port	Custom Server Load Balancer		
	6379	tcp://slb_redis_app:6379	•	
	Note: SLB should not be shared between different services.			

In this example, set the destination container port as 6379, reference the Server Load Balancer instance name slb_redis_app, set the listening port protocol as TCP, which corresponds to the protocol configured in the port mapping between host and container, and set the front end port of the Server Load Balancer instance as 6379.

(?) Note In this example, set 6379 as the frontend port and backend port (namely, the host port) of the Server Load Balancer instance and the container port, you can set a different frontend port and host port as per your needs.

- 7. Click **Create** to create the Redis application. During the creation process, the slb_redis_app Server Load Balancer instance is automatically bound to the backend host deployed with the Redis image.
- 8. When the Redis application is ready, log on to the Server Load Balancer console to view the status of the Server Load Balancer instance named <code>slb_redis_app</code>.

Click the Server Load Balancer instance ID, and then on the instance details page, click **Default** Server Group.

The health status shows that the Server Load Balancer instance is correctly bound to the Redis backend.



- 9. You can view the IP address of the Server Load Balancer instance on the Instances page of the Server Load Balancer console, and use the command line tool telnet \$Server_Load_Balancer_IP_ address 6379 to check port accessibility.
- 10. To test the preceding configurations, start a simple Python application locally to access Redis in the container cluster by using the slb_redis_app Server Load Balancer instance.

(?) Note The Redis host address is the IP address of the Server Load Balancer instance.

app.py

```
from flask import Flask
from redis import Redis
app = Flask(__name__)
redis = Redis(host='$Server_Load_Balancer_IP_address', port=6379)
@app.route('/')
def hello():
redis.incr('hits')
return 'Hello World! I have been seen %s times.' % redis.get('hits')
if __name__ == "__main__":
app.run(host="0.0.0.0", debug=True)
```

requirements.txt

flask redis

shell

```
$ pip install -r requirements.txt
$ python app.py
Running on http://0.0.0.0:5000/ ## Press CTRL+C to quit
Restarting with stat
Debugger is active!
Debugger pin code: 243-626-653
```

The access result is as follows.

← → C □ 127.0.0.1:5000 Hello World! I have been seen 5 times.

16.7. Service discovery between containers

Container Service provides multiple methods of service discovery for the services and containers in the cluster. The service can be discovered by using the container name, link, or host name.

Container name

Container Service can be accessed by using the container IP address or the name of another container in the network. In the example described in Container network interconnection, you can access the container test network-test1 1 by using its container name in the container test network-test2 1.

If the container_name is not specified in the orchestration file, the default container name is {project-name}_{service-name}_{container-index} . After connecting to the web terminal of a container, you can access a container of another service by using the container name to test the network interconnection. As shown in the following illustration.

-1-1		F under
shell	sn	Execute
•		
/ # ping test	t_network-test1_1	
PING test_netw	ork-test1_1 (172.18.0.4): 56 data bytes	
64 bytes from	172.18.0.4: seq=0 ttl=62 time=0.245 ms	
64 bytes from	172.18.0.4: seq=1 ttl=62 time=0.276 ms	
64 bytes from	172.18.0.4: seq=2 ttl=62 time=0.263 ms	
64 bytes from	172.18.0.4: seq=3 ttl=62 time=0.304 ms	
64 bytes from	172.18.0.4: seq=4 ttl=62 time=0.254 ms	
64 bytes from	172.18.0.4: seq=5 ttl=62 time=0.281 ms	
64 bytes from	172.18.0.4: seq=6 ttl=62 time=0.270 ms	
64 bytes from	172.18.0.4: seq=7 ttl=62 time=0.278 ms	
64 bytes from	172.18.0.4: seq=8 ttl=62 time=0.308 ms	
64 bytes from	172.18.0.4: seq=9 ttl=62 time=0.244 ms	

Link

Container Service supports the link between services in an orchestration template. The link between services can link the containers of a service to the containers of another service. In containers, you can access the dependent containers by using the alias of the linked service. When the IP address of the dependent container changes, the alias resolved IP address will be dynamically updated. For a specific example, see the WordPress orchestration in Container Service sample orchestration. The web service in WordPress links the db:mysql service to the containers as follows. Then, the containers can access the containers of the db service by using the MySQL domain name.

links:
 - 'db:mysql'

Hostname

If the host name configuration is defined in the orchestration template service, the container can be accessed by using this host name in the cluster.

For example,

```
testhostname:

image: busybox

hostname: xxserver

command: sleep 100000

tty: true
```

In the cluster, you can resolve and access the container of this service by using xxserver. For more information, seeContainer network interconnection the orchestration example in Container network interconnection. If this service contains several containers, accessing the containers by using this host name allows Server Load Balancer to take effect.

If the service does not configure the hostname, Container Service will use the container name as the internal hostname of the container. If an application in the container needs to know the container name for service registration, such as Eureka Client, register an accessible address to Eureka Server. The process in the container can obtain the container name for service registration and enable other service callers to access each other by using the container name.

16.8. Custom routing - simple sample

In this example, an acs/proxy container is deployed, services are exposed by using a Server Load Balancer instance (with the lb label) externally, and an Nginx server is attached at the backend. This example only shows the Nginx homepage, and other functions will be added based on the basic example.

Note Different services cannot share the same Server Load Balancer. Otherwise, the backend machines of Server Load Balancer will be deleted and the services will become unavailable.

Basic example

The compose template is as follows:

lb: image: registry.aliyuncs.com/acs/proxy:0.6 ports: - '80:80' restart: always labels: # Addon allows the proxy image to function as a subscription registry center and d ynamically load the service route. aliyun.custom addon: "proxy" # A proxy image container is deployed on each virtual machine (VM). aliyun.global: "true" # A Server Load Balancer instance is bound to the frontend. aliyun.lb.port 80: tcp://proxy test:80 environment: # Indicates the range of backend containers that support route loading. "*" indica tes the whole cluster. By default, it indicates the services in applications. ADDITIONAL SERVICES: "*" appone: expose: # For proxied services, use expose or ports to tell proxy containers which port is to be exposed. - 80/tcp image: 'nginx:latest' labels: # http/https/ws/wss are supported. Use your own domain name instead of the test d omain name provided by Container Service. aliyun.proxy.VIRTUAL_HOST: "http://appone.example.com" restart: always

After the service is successfully started, the following figure appears.



Enable session persistence

```
lb:
   image: registry.aliyuncs.com/acs/proxy:0.6
   ports:
           - '80:80'
   restart: always
   labels:
        # Addon allows the proxy image to function as a subscription registry center and d
ynamically load the service route.
       aliyun.custom addon: "proxy"
        # A proxy image container is deployed on each VM.
       aliyun.global: "true"
        # A Server Load Balancer instance is bound to the frontend.
        aliyun.lb.port 80: tcp://proxy test:80
   environment:
        # Indicates the range of backend containers that support route loading. "*" indica
tes the whole cluster. By default, it indicates the services in applications.
       ADDITIONAL SERVICES: "*"
appone:
   ports:
       - 80/tcp
       - 443/tcp
   image: 'nginx:latest'
   labels:
        # http/https/ws/wss are supported.
        aliyun.proxy.VIRTUAL HOST: "http://appone.example.com"
        # Session persistence is enabled, the cookie method is applied, and the key is CON
TAINERID.
       aliyun.proxy.COOKIE: "CONTAINERID insert indirect"
    restart: always
```

Customize 503 page

When the VIP address of the Server Load Balancer instance instead of the domain name is entered, the 503 error page is returned as follows.



To add messages to the 503 page, add the /errors folder to the VM where the container resides and add the /errors/503.http file with the following content:

HTTP/1.0 503 Service Unavailable Cache-Control: no-cache Connection: close Content-Type: text/html;charset=UTF-8 <html><body><h1>503 Service Unavailable</h1> <h3>No server is available to handle this request.</h3> If you are the visitor of this application, contact the application maintainer to solve the problem. If you are the application maintainer, view the following information. You are using the simple routing service. The request is sent from Server Load Balancer to the acsrouting application container then to your application container. Follow these st eps for troubleshooting. Log on to the Container Service console. Click "Services" in the left-side navigation p ane. Select the corresponding cluster on the "Service List" page. Click the name of the ser vice exposed to the public network. View the "Access Endpoint" of the service, and check wh ether your access domain name is the same as the domain name configured in the correspondin g service. Locate and troubleshoot the problem. View Routing FAQs. If the problem persists, open a ticket and contact the technical staff for help. We will l serve you faithfully. </body></html>

You can modify the error page as per your needs. The compose template is modified as follows:

```
lb:
   image: registry.aliyuncs.com/acs/proxy:0.6
   ports:
           - '80:80'
   restart: always
   labels:
       # Addon allows the proxy image to function as a subscription registry center and dy
namically load the service route.
       aliyun.custom addon: "proxy"
        # A proxy image container is deployed on each VM.
       aliyun.global: "true"
        # A Server Load Balancer instance is bound to the frontend.
       aliyun.lb.port_80: tcp://proxy_test:80
   environment:
        # Indicates the range of backend containers that support route loading. "*" indica
tes the whole cluster. By default, it indicates the services in applications.
       ADDITIONAL SERVICES: "*"
       EXTRA FRONTEND SETTINGS 80: "errorfile 503 /usr/local/etc/haproxy/errors/503.http"
   volumes:
       - /errors/:/usr/local/etc/haproxy/errors/
appone:
   ports:
      - 80/tcp
       - 443/tcp
   image: 'nginx:latest'
   labels:
          # You can specify paths when configuring URLs. In this example, http/https/ws/wss
are supported.
       aliyun.proxy.VIRTUAL HOST: "http://appone.example.com"
   restart: always
```

After entering the VIP address of the Server Load Balancer instance, the 503 page is displayed as follows.

$\leftarrow \rightarrow \mathbb{C}$ 0 47.88.66.202	🖈 💩 📕 😔 🖬 💥
503 Service Unavailable	
No server is available to handle this request.	
If this page is returned, a problem occurs during the service access process. Take the following steps for troubl	leshooting:
 If you are the visitor of this application, contact the application maintainer to solve the problem. If you are the application maintainer, view the following information. 	
You are using the simple routing service. The request is sent from Server Load Balancer to the acsrouting application container then Log on to the Container Service Management Console, select "Services" in the left navigation pane and select the corresponding "clubered".	n to your application container. Take the following steps for troubleshooting luster" in "Service List". Click the "services" exposed to the public network
 Locate and solve the problem in accordance with <u>Simple routing service link troubleshooting</u>. 	8.

Refer to Routing FAQs

Support extensive domain names

Modify the configurations as follows to enable the backend of Nginx to support extensive domain names (that is, the Nginx homepage can be accessed by using appone.example.com and

*.example.com).

```
lb:
   image: registry.aliyuncs.com/acs/proxy:0.6
   ports:
           - '80:80'
   restart: always
   labels:
        # Addon allows the proxy image to function as a subscription registry center and dy
namically load the service route.
       aliyun.custom addon: "proxy"
        # A proxy image container is deployed on each VM.
       aliyun.global: "true"
        # A Server Load Balancer instance is bound to the frontend.
        aliyun.lb.port 80: tcp://proxy test:80
   environment:
        # Indicates the range of backend containers that support route loading. "*" indica
tes the whole cluster. By default, it indicates the services in applications.
       ADDITIONAL SERVICES: "*"
       EXTRA FRONTEND SETTINGS 80: "errorfile 503 /usr/local/etc/haproxy/errors/503.http"
    volumes:
        - /errors/:/usr/local/etc/haproxy/errors/
appone:
   ports:
       - 80/tcp
       - 443/tcp
   image: 'nginx:latest'
   labels:
        # You can specify paths when configuring URLs. In this example, http/https/ws/wss a
re supported.
        aliyun.proxy.VIRTUAL HOST: "http://*.example.com"
    restart: always
```

Bind a host and enter the domain name www.example.com . The Nginx homepage is displayed as follows.



Configure default backend

Remove the URL configuration and modify the configurations as follows to enable access to Nginx at the backend by using an IP address.

```
lb:
   image: registry.aliyuncs.com/acs/proxy:0.6
   ports:
           - '80:80'
   restart: always
   labels:
        # Addon allows the proxy image to function as a subscription registry center and d
ynamically load the service route.
       aliyun.custom addon: "proxy"
        # A proxy image container is deployed on each VM.
       aliyun.global: "true"
        # A Server Load Balancer instance is bound to the frontend.
        aliyun.lb.port 80: tcp://proxy test:80
   environment:
        # Indicates the range of backend containers that support route loading. "*" indica
tes the whole cluster. By default, it indicates the services in applications.
       ADDITIONAL SERVICES: "*"
        # Specify the error page when 503 is returned.
       EXTRA FRONTEND SETTINGS 80: "errorfile 503 /usr/local/etc/haproxy/errors/503.http"
   volumes:
        # Mount the error page to the container from the host.
        - /errors/:/usr/local/etc/haproxy/errors/
appone:
   ports:
        - 80/tcp
       - 443/tcp
   image: 'nginx:latest'
   labels:
         # Indicates that the service must be proxied.
        aliyun.proxy.required: "true"
   restart: always
```

After entering the VIP address of the Server Load Balancer instance, the Nginx homepage is displayed as follows.



Select backend based on URL parameter values

You can use different backend proxies based on different URL parameter values.

The following example shows how to access the appone service, that is, the Nginx homepage, by using http://www.example.com?backend=appone and how to access the apptwo service, that is, the hello
world homepage, by using http://www.example.com?backend=apptwo. The application template
codes are as follows:

```
lb:
    image: registry.aliyuncs.com/acs/proxy:0.6
   ports:
           - '80:80'
    restart: always
   labels:
        # Addon allows the proxy image to function as a subscription registry center and d
ynamically load the service route.
        aliyun.custom addon: "proxy"
        # A proxy image container is deployed on each VM.
       aliyun.global: "true"
        # A Server Load Balancer instance is bound to the frontend.
        aliyun.lb.port 80: tcp://proxy test:80
   environment:
        # Indicates the range of backend containers that support route loading. "*" indica
tes the whole cluster. By default, it indicates the services in applications.
       ADDITIONAL SERVICES: "*"
        \# Obtain the value of the "backend" parameter in the URL and modify the HOST heade
r to the backend domain name which needs to be matched.
       EXTRA FRONTEND SETTINGS 80: " http-request set-header HOST %[urlp(backend)].example
.com"
appone:
   ports:
       - 80/tcp
        - 443/tcp
   image: 'nginx:latest'
   labels:
        # You can specify paths when configuring URLs. In this example, http/https/ws/wss
are supported.
       aliyun.proxy.VIRTUAL HOST: "http://appone.example.com"
   restart: always
apptwo:
   ports:
       - 80/t.cp
   image: 'registry.cn-hangzhou.aliyuncs.com/linhuatest/hello-world:latest'
   labels:
        # You can specify paths when configuring URLs. In this example, http/https/ws/wss
are supported.
       aliyun.proxy.VIRTUAL HOST: "http://apptwo.example.com"
    restart: always
```

Bind a host and enter the link http://www.example.com?backend=appone. Then, the Nginx homepage for the appone service is displayed as follows.



Bind a host and enter the link http://www.example.com?backend=apptwo. Then, the hello world homepage for the apptwo service is displayed as follows.

$\leftarrow \rightarrow \mathbb{C}$ () www.example.com/?backend=app	two
	Hello world!
	My hostname is 11614a37b5a3-custom-routing-apptwo-1

Record access logs

lb: image: registry.aliyuncs.com/acs/proxy:0.6 ports: - '80:80' restart: always labels: # Addon allows the proxy image to function as a subscription registry center and dy namically load the service route. aliyun.custom addon: "proxy" # A proxy image container is deployed on each VM. aliyun.global: "true" # A Server Load Balancer instance is bound to the frontend. aliyun.lb.port_80: tcp://proxy_test:80 environment: # Indicates the range of backend containers that support route loading. "*" indica tes the whole cluster. By default, it indicates the services in applications. ADDITIONAL SERVICES: "*" EXTRA_DEFAULT_SETTINGS: "log rsyslog local0,log global,option httplog" links: - rsyslog:rsyslog rsyslog: image: registry.cn-hangzhou.aliyuncs.com/linhuatest/rsyslog:latest appone: ports: - 80/tcp - 443/tcp image: 'nginx:latest' labels: # http/https/ws/wss are supported. aliyun.proxy.VIRTUAL HOST: "http://appone.example.com" restart: always

Logs are printed directly to the standard output of the rsyslog container. The access logs of custom routing can be viewed by using docker logs \$rsyslog_container_name .

Server Load Balancer between services

The following template creates a Server Load Balancer service1band an application serviceapponeto provide services externally with the domain nameappone.example.com.

```
lb:
   image: registry.aliyuncs.com/acs/proxy:0.6
   Hostname: proxy # Specify the domain name of the service as proxy, which is resolved to
all containers with this image deployed.
   ports:
           - '80:80'
   restart: always
   labels:
         # Addon allows the proxy image to function as a subscription registry center and d
ynamically load the service route.
       aliyun.custom addon: "proxy"
        # A proxy image container is deployed on each VM.
        aliyun.global: "true"
        # A Server Load Balancer instance is bound to the frontend.
       aliyun.lb.port 80: tcp://proxy test:80
   environment:
        # Indicates the range of backend containers that support route loading. "*" indicat
es the whole cluster. By default, it indicates the services in applications.
       ADDITIONAL SERVICES: "*"
appone:
   ports:
       - 80/tcp
       - 443/tcp
   image: 'nginx:latest'
   labels:
        # http/https/ws/wss are supported.
        aliyun.proxy.VIRTUAL HOST: "http://appone.example.com"
   restart: always
```

The following template is used as a client to access the appone application service, but the access path is used to request access to the Server Load Balancer service 1b and then provide a reverse proxy for the appone application service.

In the containers of the restclient service, the appone.example.com domain name is resolved to the IP addresses of all containers of the Server Load Balancer service 1b .

```
/ # drill appone.example.com
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 60917
;; flags: qr rd ra ; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; appone.example.com. IN A
;; ANSWER SECTION:
appone.example.com. 600 IN A 172.18.3.4
appone.example.com. 600 IN A 172.18.2.5
appone.example.com. 600 IN A 172.18.1.5
;; AUTHORITY SECTION:
;; ADDITIONAL SECTION:
;; Query time: 0 msec
;; SERVER: 127.0.0.11
;; WHEN: Mon Sep 26 07:09:40 2016
;; MSG SIZE rcvd: 138
```

Configure monitoring page

```
lb:
   image: registry.aliyuncs.com/acs/proxy:0.6
   ports:
             '80:80'
           - '127.0.0.1:1935:1935' # The port that monitoring page exposes to the public
network. Configure the port with due care because of the potential security risk.
   restart: always
   labels:
      aliyun.custom addon: "proxy"
       aliyun.global: "true"
       aliyun.lb.port_80: tcp://proxy_test:80
   environment:
      ADDITIONAL SERVICES: "*"
      STATS AUTH: "admin:admin" # The logon account and password used for monitoring, whi
ch are customizable.
       STATS PORT: "1935" # The port used for monitoring, which is customizable.
appone:
   expose:
     - 80/tcp
   image: 'nginx:latest'
   labels:
      aliyun.proxy.VIRTUAL HOST: "http://appone.example.com"
   restart: always
```

Log on to each machine where the custom routing image resides (each machine can receive the request, no matter the application container is on which machine) and request the acs/proxy health check page.

? Note Configure the correct username and password according to the environment variable STATS_AUTH of the application template.

```
root@c68a460635b8c405e83c052b7c2057c7b-node2:~# curl -Ss -u admin:admin 'http://127.0.0.1:1
935/' &> test.html
```

Copy the pagetest.htmlto a machine with browsers and open the local filetest.htmlwith thebrowser. View the stats monitoring statistics page. Green indicates the network from containeracs/proxyto backend containers is connected and the container acs/proxy is working normally.Other colors indicate an exception.

16.9. Custom routing - Supports TCP

When Alibaba Cloud Container Service is in use, the following problem may occur to TCP Server Load Balancer: when the client image and server image of an application are deployed on the same Elastic Compute Service (ECS) instance, the application client cannot access the local server by using Server Load Balancer due to the limitation of Server Load Balancer. In this document, take the common TCPbased Redis as an example acs/proxy to describe how to solve the problem by using the custom routing acs/proxy.

Note Different services cannot share the same Server Load Balancer instance. Otherwise, the backend machine of the Server Load Balancer is deleted and the services are unavailable.

Solution 1: Deploy client and server containers on different nodes by scheduling containers

The following is a sample application template (the **lb** label and **swarm filter** function are used):

```
redis-master:
    ports:
        - 6379:6379/tcp
    image: 'redis:alpine'
    labels:
        aliyun.lb.port_6379: tcp://proxy_test:6379
redis-client:
    image: 'redis:alpine'
    links:
        - redis-master
    environment:
        - 'affinity:aliyun.lb.port_6379!=tcp://proxy_test:6379'
    command: redis-cli -h 120.25.131.64
    stdin_open: true
    tty: true
```

? Note

- Follow these steps if the scheduling does not take effect: Log on to the Container Service console. Click Swarm > Services in the left-side navigation pane. Select the cluster in which the service you want to reschedule resides from the Cluster drop-down list. Click Reschedule at the right of the service you want to reschedule. > Select the Force Reschedule check box in the displayed dialog box and then click OK.
- The volumes of existing containers will be lost if you select the **Force Reschedule** check box. Backup and migrate the data in advance.

Solution 2: Clients inside the container cluster access the server by using links, while clients outside access the server by using Server Load Balancer

The following is a sample application template (the lb label is used):

```
redis-master:
    ports:
        - 6379:6379/tcp
    image: 'redis:alpine'
    labels:
        aliyun.lb.port_6379: tcp://proxy_test:6379
redis-client:
    image: 'redis:alpine'
    links:
        - redis-master
    command: redis-cli -h redis-master
    stdin_open: true
    tty: true
```

Solution 3: Clients inside the container cluster access the server by using Custom routing (which is based on HAProxy and serves as a proxy server), while clients outside access the server by using Server Load Balancer

The following is a sample application template (the lb label and Custom routing - simple sample are used):

```
lb:
    image: registry.aliyuncs.com/acs/proxy:0.6
    ports:
        - '6379:6379/tcp'
    restart: always
    labels:
        # Addon allows the proxy image to function as a subscription registry center and dy
namically load the service route.
        aliyun.custom_addon: "proxy"
        # A proxy image container is deployed on each virtual machine (VM).
        aliyun.global: "true"
        # A Server Load Balancer instance is bound to the frontend, and the lb label is use
        d
```

```
u.
        aliyun.lb.port_6379: tcp://proxy_test:6379
        # Indicates that the custom routing must be started after the master Redis and slav
e Redis are started, and the custom routing depends on the master Redis and slave Redis.
        aliyun.depends: redis-master, redis-slave
   environment:
       # Indicates the range of backend containers that support route loading. "*" indicat
es the whole cluster. By default, it indicates the services in applications.
       ADDITIONAL SERVICES: "*"
       EXTRA DEFAULT_SETTINGS: "log rsyslog local0,log global,option httplog"
        # Configures HAProxy to work in TCP mode.
       MODE: "tcp"
    links:
       - rsyslog:rsyslog
rsyslog:
    image: registry.cn-hangzhou.aliyuncs.com/linhuatest/rsyslog:latest
redis-master:
   ports:
     - 6379/tcp
   image: 'redis:alpine'
    labels:
        # Indicates that the custom routing is to expose the port 6379.
       aliyun.proxy.TCP PORTS: "6379"
        # Indicates that the service route is to be added to the custom routing.
       aliyun.proxy.required: "true"
redis-slave:
   ports:
     - 6379/tcp
   image: 'redis:alpine'
   links:
     - redis-master
   labels:
     # Indicates that the custom routing is to expose the port 6379.
     aliyun.proxy.TCP PORTS: "6379"
      # Indicates that the service route is to be added to the custom routing.
     aliyun.proxy.required: "true"
      # Indicates that the slave Redis depends on the master Redis and must be started afte
r the master Redis is started.
     aliyun.depends: redis-master
   command: redis-server --slaveof redis-master 6379
redis-client:
   image: 'redis:alpine'
   links:
     - lb:www.example.com
   labels:
     aliyun.depends: lb
   command: redis-cli -h www.example.com
   stdin open: true
    tty: true
```

This solution provides a master-slave Redis architecture and balances load by using the Server Load Balancer between services to make Container Server become highly available.
16.10. Custom routing - supports multiple HTTPS certificates

Use the acs/proxy image acs/proxy in this example.

Note Services cannot use the same Server Load Balancer; otherwise, the backend machine of the Server Load Balancer will be deleted, and the service will be unavailable.

```
1b:
   image: registry.aliyuncs.com/acs/proxy:0.6
   ports:
            - '80:80'
            - '443:443' # HTTPS must expose this port
    restart: always
   labels:
        # Addon allows the proxy image to function as a subscription registry center and dy
namically load the service route.
       aliyun.custom addon: "proxy"
        # A proxy image container is deployed on each virtual machine (VM).
        aliyun.global: "true"
        # A Server Load Balancer instance is bound to the frontend.
        aliyun.lb.port 80: tcp://proxy test:80
        aliyun.lb.port 443:tcp://proxy test:443
   environment:
        # Indicates the range of backend containers that support route loading. "*" indicat
es the whole cluster. By default, it indicates the services in applications.
       ADDITIONAL SERVICES: "*"
appone:
   expose: # For proxied services, use expose or ports to tell proxy containers which por
t is to be exposed.
       - 80/tcp
   image: 'nginx:latest'
   labels:
       # You can specify paths when configuring URLs. In this example, http/https/ws/wss a
re supported.
        aliyun.proxy.VIRTUAL HOST: "https://appone.example.com"
        # Configure the appone certificate.
        aliyun.proxy.SSL CERT: "----BEGIN RSA PRIVATE KEY----\nMIIEpQIBAAKCAQEAvqnKhephWH
KWYDEiBiSjzst7nRP0DJxZ5cIOxyXmncd2kslr\nkUIB5qT/MSiJGBL3Lr4advs6kI/JFmxloFrPtwEe2FGkLBfCDXX
DrWgxyFhbuPQY\nBLNueUu94sffIxg+4u5Mriui7ftindOAf0d21PSM9gb/ZUypxIgAd3RHCe/gtT0h\nVCn6FikXyn
XLDTODYWCthQHBwSZS88HNU+B0T9Y165JiQ0mV+YF+h3D/c232E6Gp\nzK+8ehVB13s5hecUx3dvdUQPBUhJYvzsPjC
hqsXSMDRexiN66kbhH6dJArsrYb8t\nEBWXfCZaTcF82wkAsUe/fhlGhh97h+66lh60QQIDAQABAoIBAQC4d8ifNWRI
9vIB\nbbAZRne7xMm5MCU2GI8q97Rgm+nAPl5bHinMVsaBnKgaj76EH+TQ+re1xyiSKwCH\nQ7FidsQqYGwQjy9NncJ
ATpAjQ4EPeLWQU2D9Ly+NjnhEKr/u0Ro6LhdA+hqt59dS\nXHvfEP/It5odN62yJzikDWBmk/hhK0tu28dPYUuPoWsw
XWFMkaNttmfLgZlagiqr\nYp7rxAFqQurzctQ2VNwezekDHQoh8ounHGEniZ+fA6sFtYi83KTKWkvFom1chZQr\nxxP
bbgANJJJlNgtkl6JZNxj6SYimmWvzmrrU25khKg/klP5EtQzIx6UFhURnuTKu\nzNgqcIABAoGBAOqUOerveEUePvsA
lta8CV/p2KKwenv+kUofQ4UpKFXfnHbQHQfr\nZHS29OQiPxqjVXYLu8gNfLRfKtUNyqV+TDrzJ1elW2RKc00GHAwPb
XxijPhmJ2fW\neskn8tlDcyXpvoqWJG34896vo4IbcL0H/eUs0jJo6OJlCQBKXik+t3gxAoGBAM9k\nVOTV2caKyrZ4
ta0Q1LKqKfOkt0j+vKz167J5pSLjVKQSUxGMyLnGwiQdDtB4iy6L\nFcCB/S0HM0UWkJWhNYAL8kHry53bVdHtQG0tu
YFYvBJo7A+Nppsn9MtlVh8KbVu4\nhOz/3MWwbQNnvIVCGK/fSltS1GhTk4rKL7PjNwMRAoGBALK0n3bqXj6Rrzs7FK
6c\na6vlE4PFXFpv8jF8pcyhMThSdPlSzHsHCe2cn+3YZSie+/FF0RZLqBAlXBUZP6Na\nFyrlqLgtofVCfppUKDPL4
```

QXccjaeZDDIBZyPUYPQzb05WE5t2WzqNqcUOUVaMEXh\n+7uGrM94espWXEqbX6aeP91RAoGAR1JQ7t8MXuQE5GZ9w9 cnKAXG/9RkSZ4Gv+cL\nKpNQyUmoE5lbFKJWFZgtkC1CLrIRD5EdqQ7q1/APFGgYUoQ9LdPfKzcW7cnHic0W\nwW51r kQ2UU++a2+uhIHB4Y3U6+WP00CP4gTICUhPTo5IQC8vS8M85UZqu41LRA5W\nqnpq1uECgYEAq+6KpHhlR+5h3Y/m0n $84 y J 0 Y u Cmr 17 HFRz BMdOca W 30 a YL 83 r Aaq \ n6d Jqp A V geu 3 HP8 A ti G V Z Re 78 J + n4d 2 JG Y S qg t P 2 1 FF T d F 9 H f h c R 2 P 9 b S A ti G V Z Re 78 J + n4d 2 JG Y S qg t P 2 1 FF T d F 9 H f h c R 2 P 9 b S A ti G V Z Re 78 J + n4d 2 JG Y S qg t P 2 1 FF T d F 9 H f h c R 2 P 9 b S A ti G V Z Re 78 J + n4d 2 JG Y S qg t P 2 1 FF T d F 9 H f h c R 2 P 9 b S A ti G V Z Re 78 J + n4d 2 JG Y S qg t P 2 1 FF T d F 9 H f h c R 2 P 9 b S A ti G V Z Re 78 J + n4d 2 JG Y S qg t P 2 1 FF T d F 9 H f h c R 2 P 9 b S A ti G V Z Re 78 J + n4d 2 JG Y S qg t P 2 1 FF T d F 9 H f h c R 2 P 9 b S A ti G V Z Re 78 J + n4d 2 JG Y S qg t P 2 1 FF T d F 9 H f h c R 2 P 9 b S A ti G V Z R 2 F A ti G A ti$ UBNYtWols\nEs3iw53t8a4BndLGBwLPA31klf7J5stYanRv6NqaRaLq4FQMxsW1A0Q=\n----END RSA PRIVATE K EY-----Nn----BEGIN CERTIFICATE-----\nMIIDvDCCAqSgAwIBAgIBATANBgkqhkiG9w0BAQUFADBgMQswCQYDV QQGEwJDTjER\nMA8GA1UECBMIWmhlamlhbmcxETAPBgNVBAcTCEhhbmd6aG91MRQwEgYDVQQKEwth\nbGliYWJhLmNv bTEVMBMGA1UECxMMd3d3LnJvb3QuY29tMB4XDTE1MDIwOTA1MzQx\nOFoXDTE2MDIwOTA1MzQxOFowZjELMAkGA1UEB hMCQ04xETAPBgNVBAgTCFpoZWpp\nYW5nMRQwEgYDVQQKEwthbGliYWJhLmNvbTEVMBMGA1UECxMMd3d3LnJvb3QuY2 $\label{eq:structure} $$ t\mtext{PydvQQDew53d3cubGluaHVhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP\nADCCAQoCggEBAL4JyoXqY} and the structure an$ VhylmAxIgYko87Le50T9AycWeXCDscl5p3HdpLJa5FC\nAeak/zEoiRgS9y6+Gnb70pCPyRZsZaBaz7cBHthRpCwXwg 11w61oMchYW7j0GASz\nbnlLveLH3yMYPuLuTK4rou37Yp3TgH9HdtT0jPYG/2VMqcSIAHd0Rwnv4LU9IVQp\n+hYpF 8p1yw0zg2FgrYUBwcEmUvPBzVPgdE/WJeuSYkNJ1fmBfodw/3Nt9hOhqcyv\nvHoVQdd7OYXnFMd3b3VEDwVISWL87D 4woYLF0jA0XsYjeupG4R+nSQK7K2G/LRAV\nl3wmWk3BfNsJALFHv34ZRoYfe4fuupYejkECAwEAAaN7MHkwCQYDVR0 $\texttt{TBAIwADAs} \ \texttt{NBglghkgBhvhCAQ0EHxYdT3BlblNTTCBHZW51cmF0ZWQgQ2VydGlmaWNhdGUwHQYD} \ \texttt{NVR00BBYEFM6ESm}$ kDKrqnqMwBawkjeONKrRMQMB8GA1UdIwQYMBaAFFUrhN9ro+Nm\nrZn14WQzDpqTbCBhMA0GCSqGSIb3DQEBBQUAA4I BAQCQ2D9CRiv8brx3fnr/RZG6\nFYPEdxjY/CyfJrAbij0PdKjzZKk1067chM10xs2JhJ6tMqg2sv50bGx4XmbSPmEe \nYTJjIXMY+jCoJ/Zmk3Xgu4K1y1LvD25PahDVhRrPN8H4WjsYu51pQNshi15E/3iQ\n2JoV0r8QiAsPiiY5+mNCD1f m+QN1tyUabczi/DHafgWJxf2B3M66e3oUdtbzA2pf\nYHR8RVeSFrjaBqudO8ir+uYcRbRkroYmY5Vm+4Yp64oetrPp KUPWSYaAZ0uRtpeL\nB5DpqXz9GEBb5m2Q4dKjs5Hm6vyFUORCzZcO4XexDhcgdLOH5qznmh9oMCk9QvZf\n----EN D CERTIFICATE----\n"

restart: always

apptwo:

expose: # For proxied services, use expose or ports to tell proxy containers which por t is to be exposed.

- 80/tcp

image: 'registry.cn-hangzhou.aliyuncs.com/linhuatest/hello-world:latest'

labels:

You can specify paths when configuring URLs. In this example, http/https/ws/wss a re supported.

aliyun.proxy.VIRTUAL_HOST: "https://apptwo.example.com"

Configure the apptwo certificate.

aliyun.proxy.SSL CERT: "----BEGIN RSA PRIVATE KEY----\nMIIEpQIBAAKCAQEAvqnKhephWH KWYDEiBiSjzst7nRP0DJxZ5cIOxyXmncd2kslr\nkUIB5qT/MSiJGBL3Lr4advs6kI/JFmxloFrPtwEe2FGkLBfCDXX DrWgxyFhbuPQY\nBLNueUu94sffIxg+4u5Mriui7ftindOAf0d21PSM9gb/ZUypxIgAd3RHCe/gtT0h\nVCn6FikXyn XLDTODYWCthQHBwSZS88HNU+B0T9Y165JiQ0mV+YF+h3D/c232E6Gp\nzK+8ehVB13s5hecUx3dvdUQPBUhJYvzsPjC hqsXSMDRexiN66kbhH6dJArsrYb8t\nEBWXfCZaTcF82wkAsUe/fhlGhh97h+66lh60QQIDAQABAoIBAQC4d8ifNWRI 9vIB\nbbAZRne7xMm5MCU2GI8q97Rgm+nAPl5bHinMVsaBnKgaj76EH+TQ+re1xyiSKwCH\nQ7FidsQqYGwQjy9NncJ ATpAjQ4EPeLWQU2D9Ly+NjnhEKr/u0Ro6LhdA+hqt59dS\nXHvfEP/It5odN62yJzikDWBmk/hhK0tu28dPYUuPoWsw XWFMkaNttmfLgZlagigr\nYp7rxAFqQurzctQ2VNwezekDHQoh8ounHGEniZ+fA6sFtYi83KTKWkvFom1chZQr\nxxP bbqANJJJlNqtkl6JZNxj6SYimmWvzmrrU25khKq/klP5EtQzIx6UFhURnuTKu\nzNqqcIABAoGBAOqUOerveEUePvsA lta8CV/p2KKwenv+kUofQ4UpKFXfnHbQHQfr\nZHS29OQiPxqjVXYLu8gNfLRfKtUNyqV+TDrzJ1e1W2RKc00GHAwPb XxijPhmJ2fW\neskn8tlDcyXpvoqWJG34896vo4IbcL0H/eUs0jJo60JlCQBKXik+t3qxAoGBAM9k\nVOTV2caKyrZ4 ta0Q1LKqKfOkt0j+vKz167J5pSLjVKQSUxGMyLnGwiQdDtB4iy6L\nFcCB/S0HM0UWkJWhNYAL8kHry53bVdHtQG0tu YFYvBJo7A+Nppsn9MtlVh8KbVu4\nhOz/3MWwbQNnvIVCGK/fSltS1GhTk4rKL7PjNwMRAoGBALK0n3bqXj6Rrzs7FK 6c\na6vlE4PFXFpv8jF8pcyhMThSdPlSzHsHCe2cn+3YZSie+/FFORZLqBAlXBUZP6Na\nFyrlqLgtofVCfppUKDPL4 QXccjaeZDDIBZyPUYPQzb05WE5t2WzqNqcUOUVaMEXh\n+7uGrM94espWXEqbX6aeP91RAoGAR1JQ7t8MXuQE5GZ9w9 cnKAXG/9RkSZ4Gv+cL\nKpNQyUmoE5lbFKJWFZgtkC1CLrIRD5EdqQ7q1/APFGgYUoQ9LdPfKzcW7cnHic0W\nwW51r kQ2UU++a2+uhIHB4Y3U6+WPO0CP4qTICUhPTo5IQC8vS8M85UZqu41LRA5W\nqnpq1uECqYEAq+6KpHhlR+5h3Y/m0n 84 y J 0 Y u Cmr 17 HFrz BMdOca W 3 oa Y L 83 r Aaq n 6 d Jqp A V geu 3 HP 8 A ti G V Z Re 7 8 J + n 4 d 2 JG Y S qg t P 2 1 FFT d F 9 H f h c R 2 P 9 b 1 f r 2 A fUBNYtWols\nEs3iw53t8a4BndLGBwLPA31klf7J5stYanRv6NqaRaLq4FQMxsW1A0Q=\n----END RSA PRIVATE K EY-----Nn----BEGIN CERTIFICATE-----\nMIIDvDCCAqSgAwIBAgIBATANBgkqhkiG9w0BAQUFADBgMQswCQYDV QQGEwJDTjER\nMA8GA1UECBMIWmhlamlhbmcxETAPBqNVBAcTCEhhbmd6aG91MRQwEqYDVQQKEwth\nbGliYWJhLmNv $b {\tt TEVMBMGA1UECxMMd3d3LnJvb3QuY29tMB4XDTE1MDIwOTA1MzQx \ nOFoXDTE2MDIwOTA1MzQxOFowZjELMAkGA1UEB} to the the term of term o$ hMCQ04xETAPBgNVBAgTCFpoZWpp\nYW5nMRQwEgYDVQQKEwthbGliYWJhLmNvbTEVMBMGA1UECXMMd3d3LnJvb3QuY2 9t\nMRcwFQYDVQQDEw53d3cubGluaHVhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP\nADCCAQoCggEBAL4JyoXqY VhylmAxIgYko87Le50T9AycWeXCDscl5p3HdpLJa5FC\nAeak/zEoiRgS9y6+Gnb70pCPyRZsZaBaz7cBHthRpCWXwg 11w61oMchYW7j0GASz\nbnlLveLH3yMYPuLuTK4rou37Yp3TgH9HdtT0jPYG/2VMqcSIAHd0Rwnv4LU9IVQp\n+hYpF 8p1yw0zg2FgrYUBwcEmUvPBzVPgdE/WJeuSYkNJ1fmBfodw/3Nt9hOhqcyv\nvHoVQdd70YXnFMd3b3VEDwVISWL87D 4woYLF0jA0XsYjeupG4R+nSQK7K2G/LRAV\n13wmWk3BfNsJALFHv34ZROYfe4fuupYejkECAwEAAaN7MHkwCQYDVR0 TBAIwADAs\nBg1ghkgBhvhCAQ0EHxYdT3BlblNTTCBHZW51cmF0ZWQgQ2VydGlmaWNhdGUwHQYD\nVR00BBYEFM6ESm kDKrqnqMwBawkjeONKrRMQMB8GA1UdIwQYMBaAFFUrhN9ro+Nm\nrZn14WqzDpgTbCBhMA0GCSqGSIb3DQEBBQUAA4I BAQCQ2D9CRiv8brx3fnr/RZG6\nFYPEdxjY/CyfJrAbij0PdKjzZKk1067chM10xs2JhJ6tMqg2sv50bGx4XmbSPmEe \nYTJjIXMY+jCoJ/Zmk3Xgu4K1y1LvD25PahDVhRrPN8H4WjsYu51pQNshi15E/3iQ\n2JoV0r8QiAsPiiY5+mNCD1f m+QN1tyUabczi/DHafgWJxf2B3M66e3oUdtbzA2pf\nYHR8RVeSFrjaBqud08ir+uYcRbRkroYmY5Vm+4Yp64oetrPp KUPWSYaAZ0uRtpeL\nB5DpqXz9GEBb5m2Q4dKjs5Hm6vyFUORCzZcO4XexDhcgdL0H5qznmh9oMCk9qvzf\n-----EN D CERTIFICATE-----\n"

restart: always

Services appone and apptwo use aligun.proxy.VIRTUAL_HOST to specify the domain names. If you must configure the certificate, set the protocol to https. Then, use aligun.proxy.SSL_CERT to specify the certificate content. The method of configuring the certificate content is as follows:

Assume that the *key.pem* is a private key file, and *ca.pem* is a public key file. Run the following commands in the bash (the current directory contains the public key file and private key file).

\$ cp key.pem cert.pem
\$ cat ca.pem >> cert.pem
\$ awk 1 ORS='\\n' cert.pem

Finally, enter the output of the awk command as the value of label aligun.proxy.SSL_CERT . Use double quotation marks (") for separation. For other information, such as lb label, lb see the preceding template and the corresponding Custom routing - simple sample.

17.Release policy 17.1. Introductions on release strategies

Container Service provides two release strategies: blue-green release and standard release. These two release strategies differ in:

Release strategies	Differences
Standard release	Delete the earlier version when deploying the new version of application. Your service will be temporarily interrupted in the process of release.
Blue-green release	Blue version and green version are generated when the application is updated. These two versions play an active-standby role to each other and go online or offline based on your configured route weight. This kind of release strategy has the following features: The service is not interrupted. The application never goes down. Users do not realize the restart in the process of release. The application automatically rolls back if the update fails. Multiple updates and iterations can be performed on the same resource stack.
	Note Applications created by using images cannot be updated using blue-green release strategy.

Usage scenarios of standard release

The standard release, a traditional release strategy for applications, deploys the new version of the application in the current environment. This release strategy is generally used except for special needs. The usage scenarios include:

- The new version has been fully tested, with no need of online test run.
- The application includes database service and has been updated in an unreversible manner, such as datasheet structure change. In this scenario, standard release avoids business transformation, such as data migration and rollback.

Usage scenarios of blue-green release

Application forms that are applicable to blue-green release include the frontend services and backend services. Blue-green release is often used in the incremental update of applications. The specific customer-facing business scenarios that use this kind of release strategy include:

Guarantee of the business continuity

The frequent iterations of application versions is a real challenge to Internet enterprises with quicklychanging business. It is necessary to ensure the continuity of online business. The main value of bluegreen release strategy is to achieve application update with no downtime, ensure the service is not interrupted, and meet the requirements of sustainable release of updated applications in the cloud environment.

Online evaluation of new version

Blue-green release strategy enables you to perform the version test in the online environment, and fully test the service functions, performance, and security of the new version by keeping the earlier and the latest versions coexisting for a period of time. When the new version is stable, bring the earlier version offline.

17.2. Blue-green release policy with simple routing

(?) Note By default, simple routing performs session persistence. During a blue-green release, when the new service weight is set to 100%, old requests might be forwarded to the old version of the service. To forward requests to the new version of the service, disable session persistence for the application before the release, see routing.session_sticky or clear cookies after the release.

Background information

Blue-green release is a zero downtime application update policy. During a blue-green release, the old and new service versions of an application coexist, and also share routes. By adjusting route weights, you can switch traffic between different service versions. After the new version passes the verification, you can delete the old service version by confirming the release. If the new version does not pass the verification, the release is rolled back and the new version is deleted.

Prerequisites

The routing service must be upgraded to the latest version. For more information, see Upgrade system services.

Scenario

In the following example, assume that you perform a blue-green release for an Nginx static page application. The initial application template is as follows:

```
nginx-v1:
image: 'registry.aliyuncs.com/ringtail/nginx:1.0'
labels:
    aliyun.routing.port_80: nginx
    restart: always
```

After the deployment, the page is as follows.

Welcome to nginx! ×	- ANNA ANA ANNA ANNA ANNA ANNA ANNA ANN	3
← → C 🗋 nginx.c89d1a3987e0a4	ad1a30a728e67b60fa5.cn-beijing.alicontainer.com/?spm=5176.2 🟠	

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to <u>nginx.org</u>. Commercial support is available at <u>nginx.com</u>.

Thank you for using nginx.

Procedure

- 1. Log on to the Container Service console.
- 2. Under Swarm, click **Applications** in the left-side navigation pane.
- 3. Select the cluster in which the application resides from the Cluster drop-down list.
- 4. Click **Update** at the right of the application.

Container Service	Application List					Refresh	Create Ap	plication
Swarm Kubernetes								
Overview	Help: & Create an applic	ation & Change application configurations & Simple rout	e blue-green release po	licy & Container auto scalin	g			
Applications	Cluster: test	Cluster: test 🔻 2 System Applications 🗉 Hide Offline Applications 🔛 Hide Online Applications 🛛 Name 🔻					۹	ж
Services	Name Description	Status	Container Status	Time Created 🔺	Time Updated 🔺		3	Action
Clusters	Nginx	Running	Running:1 Stop:0	2018-02-05 10:14:08	2018-02-05 10:14:15	Stop	Update Redeploy	Delete Events
Nodes								

- 5. Set the release mode and the configurations of the new service version.
 - The new and old versions cannot share the same name.
 - To make sure that the application does not experience downtime when switching versions, the weight of the new service version is set to 0 by default. On the route management page, you must adjust the weight to switch traffic to the new version.

Change Configura	ation	\times
Name:	Nginx	
*Version:	1.1	
	Note: The version of the application must be changed; otherwise, the "OK" button is not available.	
Description:		
Use Latest Image:	Force 🖉 Reschedule :	
Release Mode:	Blue-Green Release 🔻 🕢	
Template:	1 nginx-v2: image: 'registry.aliyuncs.com/ringtail nginx:2.0' iabels: aliyun.routing.port_80: nginx 5 restart: always 5 restart: always	
	ОКС	ancel

The template sample is as follows:

6. Click **OK** to release the changed version.

The release process goes through two statuses:

- Blue-green release in progress: Indicates that the startup of the new service version is not completed.
- Blue-green release awaiting confirmation: Indicates that the startup of the new service version is completed. Another release can be performed until this release is confirmed or rolled back.

Click the application name to go to the application details page. You can see that the new and old application versions coexist.

Application:	Application: Nginx Refree								
Overview									
Name: Ng	jinx			Time Created: 2018-	02-05	Time Updated: 2018-02-05	Cluster: test		
Trigger 1.	Trigger 1. You can only have one of each trigger type. O Create Trigger								
No trigger is	available at the mor	ment. Click "Crea	ate Trigger"	in the upper-right corner.					
Services	Containers Lo	gs Events	Routes						
Name	Application	Statu	15	Container Status	Image			Action	
nginx-v1	Nginx	● Ri	unning	Running:1 Stop:0	registry.al	registry.aliyuncs.com		Stop Restart Reschedule Update Delete Events	
nginx-v2	Nginx	🔴 Ri	Inning	Running:1 Stop:0	registry.al	registry.aliyuncs.com		Stop Restart Reschedule Update Delete Events	

7. Click the Routes tab and then click Set service weight.

As shown in the following figure, the old service has a weight of 100 and the new service has a weight of 0.

Bouto Addresso			
Route Address:	ingen.com/certain/de/		de contacto cara
Route Weight:	Name	Weight	%
	Nginx_nginx-v1	100 ~	100%
	Nginx_nginx-v2		0%
			OK Cancel

To realize zero downtime update, set the weight of the new version to 100. Now the new version and old version account for 50% of the weight respectively. Test if both versions have stable traffic.

? Note Adjusting the weights of the new version and old version at the same time might result in the failure of some requests. Therefore, adjust the weights in two steps and only adjust the weight of one version in each step. For example, adjust the weight of the new version from 0 to 100 first, and then adjust the weight of the old version from 100 to 0 after the traffic is stable.

Then, adjust the weight of the old version to 0 and that of the new version to 100.

Dauta Waiaht Catting			\sim
Route weight Setting	5		~
Route Address:	ngnu ci-Maletalization	monotorem).o-to	photolostan
Route Weight:	Name	Weight	%
	Nginx_nginx-v1	0 🔶	0%
	Nginx_nginx-v2	100 ~	100%
			OK Cancel

8. The routing service enables the session persistence by default. Therefore, you can open a new browser window to access the new version.

	nginx.c89d1a3987e0a4ad1a30a728e67b60fa5.cn-beijing C	(†) (†
Welco	ome to nginx blue-green!	
If you see th working. Fur	is page, the nginx web server is successfully installed and ther configuration is required.	
For online do Commercial	ocumentation and support please refer to <u>nginx.org</u> . support is available at <u>nginx.com</u> .	
Thank you fo	or using nginx.	

9. After the entire release process has been verified, click **Confirm Release Completion** on the Application List page. Select whether or not to automatically perform the **smooth update** in the displayed dialog box and click **OK** to confirm the release before you can release subsequent versions.

Application List		Release Confirmation	Release Confirmation			Refreeb Create Application
Help: & Create an application	n 🔗 Change applic	Are you sure you want to complete this release?			caling	
Cluster: test v	r ⊮ Hide System Ap	automatic smooth update	. 0		Name 🔻	Q #
	atus			OK Cancel	Time Updated 🔺	Action
Nginx	Blue-green release a	waiting confirmation 🥝	Running:1 Stop:0	2018-02-05 10:14:08	2018-02-05 10:18:20	Stop Update Delete Redeploy Events Confirm Release Completion Roll Back
test		waiting confirmation 🕖	Running:1 Stop:0	2018-02-05 09:52:02	2018-02-05 09:57:39	Stop Update Delete Redeploy Events Confirm Release Completion Roll Back

Now the service list of the application has been updated and the old service version has been taken offline and deleted.

Services	Containers	Logs	Events	Routes				
Name	Appl	cation		St	atus	Container Status	Image	Action
nginx-v2	ngin:	<		•	Ready	Ready:1 Stop:0	registry.aliyuncs.com/ringtail/nginx:2.0	Stop Restart Reschedule Update Delete Events

17.3. Blue-green release policy with Server Load Balancer routing

Blue-green release is a zero downtime application update policy. During a blue-green release, the old and new service versions of an application coexist, and also share the Server Load Balancer instance. By adjusting the Server Load Balancer weights, you can switch traffic between different service versions. After the new version passes the verification, you can delete the old service version by confirming the release. If the new version does not pass the verification, the release is rolled back and the new version is deleted.

Scenarios

In the following example, assume that you want to perform a blue-green release for an Nginx static page application. The initial application template is as follows:

After the deployment, the page is as follows.



Instructions

Each container needs to expose the host port. Therefore, when performing blue-green release with Server Load Balancer routing, make sure that the number of containers in a service is less than or equal to half the number of machines in the cluster. Otherwise, the port conflict occurs. We recommend that you contract the number of containers to half the number of machines in the cluster before performing blue-green release with Server Load Balancer routing. Expand the number of containers to the original amount after the blue-green release is completed.

Procedure

- 1. Log on to the Container Service console.
- 2. Click Swarm > **Applications** in the left-side navigation pane.
- 3. Select the cluster in which the application resides from the Cluster drop-down list.
- 4. Click **Update** at the right of the application.

Containe	er Service	Applicati	cation List							
Swarm	Kubernetes	Help: Ø	Ø Create an application Ø Change application configurations Ø Simple route blue-green release policy Ø Container auto scaling							
Applicat	ions 1	Cluster:	luster: test 🔻 🕐 29 System Applications 🗉 Hide Offline Applications 🖾 Hide Online Applications 🕅 Name 🔻							X
Services	3	Name	Description	Status	Container Status	Time Created 🔺	Time Updated 🔺		ె	Acti
Clusters Nodes		test		Running	Running:1 Stop:0	2018-02-05 09:52:02	2018-02-05 09:52:09	Stop	Update Redeploy	Delete Event

5. Set the release mode and the configurations of the new service version.

? Note

- $\circ\;$ The new and old versions cannot share the same name.
- To make sure that the application does not experience downtime when switching versions, the weight of the new service version is set to 0 by default. On the route management page, you must adjust the weight to switch traffic to the new version.

Change Configura	ation	×
Name:	test	
"Version:	1.1 Note: The version of the application must be changed; otherwise, the "OK" button is not available.	
Description:		
Use Latest Image:	Force Reschedule :	
Release Mode:	Blue-Green Release 🔻 🞯	
Template:	<pre>1 nginx-v2: 2 image: 'registry.aliyuncs.com/ringtail/nginx:2.0' 3 ports: 4 - 80:80/tcp 5 labels: 6 aliyun.lb.port_80: tcp://proxy_test:80 7 restart: always</pre>	
	Use Existing Orchestration Template Label description	
	ОК	Cancel

The template sample is as follows:

```
nginx-v2:
  image: 'registry.aliyuncs.com/ringtail/nginx:2.0'
  ports:
    -80: 80/tcp
  labels:
    aliyun.lb.port_80: tcp://proxy_test:80
  restart: always
```

6. Click OK to release the changed version.

The release process goes through two statuses:

- Blue-green release in progress: Indicates that the startup of the new service version is not completed.
- Blue-green release awaiting confirmation: Indicates that the startup of the new service version is completed. Another release can be performed until this release is confirmed or rolled back.

Click the application name to go to the application details page. You can see that the new and old application versions coexist.

Application:	:test						Refresh		
Overview									
Name: te	st		Time Created: 2018-02-05		Time Updated: 2018-02-05	Cluster: test			
Trigger 1	Trigger 1. You can only have one of each trigger type.								
No trigger is available at the moment. Click "Create Trigger" in the upper-right corner.									
Services	Containers Logs	Events Routes							
Name	Application	Status	Container Status	Image			Action		
nginx-v1	test	Running	Running:1 Stop:0	registry.a	registry.aliyuncs.com/		Stop Restart Reschedule Update Delete Events		
nginx-v2	test	Running	Running:1 Stop:0	registry.aliyuncs.com/ingla.lingla.cl			Stop Restart Reschedule Update Delete Events		

7. Click the Routes tab and then click Set service weight.

The Server Load Balancer weight of the old version is 100 and that of the new version is 0.

Route Weight Setting	S		×
Route Address:	130.39.32.308		
Route Weight:	Name	Weight	%
	test_nginx-v1	100 ^	100%
	test_nginx-v2	0 ^	0%
			OK Cancel

To realize zero downtime update, set the weight of the new version to 100. Now the new version and old version account for 50% of the weight respectively. Test if both versions have stable traffic.

Note Adjusting the weights of the new version and old version at the same time might result in the failure of some requests. Therefore, adjust the weights in two steps and only adjust the weight of one version in each step. For example, adjust the weight of the new version from 0 to 100 first, and then adjust the weight of the old version from 100 to 0 after the traffic is stable.

Then, adjust the weight of the old version to 0 and that of the new version to 100.

Route Weight Settings								
Route Address:	110.55.32.305							
Route Weight:	Name		Weight	%				
	test_nginx-v1		0 ^	0%				
	test_nginx-v2		100 ^	100%				
				OK Cancel				

8. You can open a new browser window to access the new version.

Welcome to nginx-blue-green ×	.
← → C ① 118.178.32.24/?spm=5176.2020520152.221.11.midrs4	☆ :
Welcome to nginx blue-green!	
new	
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.	
For online documentation and support please refer to <u>nginx.org</u> . Commercial support is available at <u>nginx.com</u> .	
Thank you for using nginx.	

9. After the entire release process has been verified, click **Confirm Release Completion** on the Application List page. Select whether or not to automatically perform the **smooth update** in the displayed dialog box and click **OK** to confirm the release before you can release subsequent versions.

L Applica	ation List	Release Confirmation	×		Pofrach Create Application
Applice	addir Lat				Treffeen
Help:	S Create an application S Change applic	Ale you sure you want to complete this release? Ale you sure you want to complete this release?		caling	
Cluster:	test 🔹 🕷 Hide System Ap			Name 🔻	Q X
Name			OK Cancel	Time Updated 🔺	Action
test	Blue-green release a	waiting confirmation 2 Running;1 Stop:0	2018-02-05 09:52:02	2018-02-05 09:57:39	Stop Update Delete Redeploy Events Confirm Release Completion Roll Back

Now the service list of the application has been updated and the old service version has been taken offline and deleted.

Services	Containers	Logs	Events	Routes				
Name	Appl	cation		St	atus	Container Status	Image	Action
nginx-v2	ngin:	¢		•	Ready	Ready:1 Stop:0	registry.aliyuncs.com/ringtail/nginx:2.0	Stop Restart Reschedule Update Delete Events