

Alibaba Cloud Alibaba Cloud Container Service for Kubernetes

Bulletin

Issue: 20190820

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.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized 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 due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information 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.
	This warning information 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 restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK.
Courier font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 Vulnerability fix: CVE-2019-11249 related to kubectl cp.....	1
2 Upgraded the Terway network plugin.....	2
3 Upgraded Cloud Controller Manager.....	3
4 A notice about the ACK security policy upgrade.....	4
5 Vulnerability fix: CVE-2019-1002101.....	5
6 Fixed a bug that caused disks to fail to be mounted to a multi-zone Kubernetes clusters.....	6
7 Announcement about billing of ECI instances that support serverless Kubernetes clusters.....	7
8 Vulnerability fix: <i>CVE - 2018 - 18264</i> for Kubernetes dashboard.....	8

1 Vulnerability fix: CVE-2019-11249 related to kubectl cp

The vulnerability CVE-2019-11246 related to kubectl cp was exposed several months ago. Kubernetes recently announced another vulnerability CVE-2019-11249 related to kubectl cp. This vulnerability provides attackers with the opportunity to write malicious files saved in a TAR package into any paths on your host through directory traversal by running the kubectl cp command. This process is only restricted by the system permissions of the current user. We recommend that you upgrade the kubectl client version to a more secure version as soon as possible. For more information about the CVE-2019-11249 vulnerability, see [#unique_4](#).

2 Upgraded the Terway network plugin

- v1.0.9.15-g3957085-aliyun

Fixed the bug that caused upgrade failures that occurred to the Terway network plugin.

- v1.0.9.14-ga0346bb-aliyun

- Fixed the bug that caused the Terway network plugin to fail to obtain the EIP information.
- Fixed the bug that caused the error message failed to move veth to host netns: file exists. The error message was displayed when a container was created.
- Added a new feature that enables the system to detect the status of an EIP and retrieve its exception releases.
- Changed the health check method for the Terway network plugin from the HTTP path check to the TCP port check.

The preceding upgrades do not affect application functionality.

We recommend that you use the Container Service console to upgrade the Terway network plugin to the latest version.

3 Upgraded Cloud Controller Manager

v1.9.3.105-gfd4e547-aliyun

- Fixed the bug where the annotation settings did not take effect.
- Added the feature where you can rename an SLB instance in the SLB console. If you want to rename an SLB instance created by using Cloud Controller Manager (CCM) V1.9.3.10 or earlier, you must first add a tag to the manager. For more information, see [#unique_7](#)

We recommend that you use the Container Service console to upgrade Cloud Controller Manager to the latest version.

4 A notice about the ACK security policy upgrade

Starting from April 17, 2019, the security policy of ACK for managing the permissions required to access a Kubernetes cluster are upgraded. After this release, the upgrade security policy denies any cluster accesses performed by RAM users not granted with the required permissions. That is, RAM users can only access the Kubernetes clusters for which they have been granted the required permissions.

You must grant the required RAM permissions to all the RAM users under your management for them to access corresponding clusters. For more information, see [#unique_9](#).

5 Vulnerability fix: CVE-2019-1002101

The vulnerability fixed in this update caused damages through the `kubectl cp` command that is used to copy files and directories to and from containers. Specifically, this vulnerability allowed attackers to implant a malicious tar package that contains a symbolic link header into an image or a running container. During the process in which the tar package is extracted, it modifies or monitors any files stored in the directory that shares the same name with the symbolic link header.

This vulnerability was fixed in `kubectl` V1.11.9, V1.12.7, V1.13.5, and V1.14.0. You must use one of these versions of `kubectl`. For more information, see [Install and set up kubectl](#).

6 Fixed a bug that caused disks to fail to be mounted to a multi-zone Kubernetes clusters

- The multi-zone Kubernetes clusters created on or after January 28, 2019 are unaffected by this bug.
- For any multi-zone Kubernetes cluster created before January 28, 2019, ACK offers a solution to this bug that allows you to mount a disk to the cluster. For more information, see [#unique_12](#).

7 Announcement about billing of ECI instances that support serverless Kubernetes clusters

From January 22, 2019, ECI instances that are used to support serverless Kubernetes clusters will incur charges. For more information, see [#unique_14/unique_14_Connect_42_section_np1_7pb_qqv](#).

8 Vulnerability fix: *CVE - 2018 - 18264* for Kubernetes dashboard

This vulnerability that is fixed was discovered in Kubernetes dashboards of V1.10 and earlier. This vulnerability allowed attackers to bypass identity authentication and read secrets within the cluster by using the dashboard logon account. For more information, see [Fix the vulnerability CVE-2018-18264](#).