Alibaba Cloud Threat Detection

Quick Start

Issue: 20190730

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 `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

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

Contents

Legal disclaimer..... I
Generic conventions..... I
1 Quick start..... 1

1 Quick start

Security Center provides multiple features, including security events, vulnerability detection, baseline check, asset fingerprints, and log retrieval. Security Center allows you to implement complete detection and protection for your servers and web applications. You can also view asset statistics and security information.

Procedure

1. Log on to the Security Center console.
2. Install the Cloud Security Center agent plug-in for your server.

   Note:
   The Security Center agent is a security plug-in running on your servers. It has been integrated into Alibaba Cloud public images. When you create an ECS instance, you can select a public image and enable Security enhancement to automatically install the Security Center agent on your instance. For more information about how to manually install the Security Center agent on an external server, see Install the Security Center agent.
3. After the Security Center agent has been installed, you can go to the Assets page in the Security Center console to view the security status of the servers under your Alibaba Cloud account.

   Note:
   The Security Center agent detects and collects the security status of the servers that Security Center protects. You can determine the status of the installed Security Center agent by verifying the security status of your server. If the security status of your server is protected, the installed agent is online and working properly. If the security status is unprotected, the installed agent is offline. For more information, see Troubleshoot the problem of Security Center agent going offline.

4. In the Security Center console, you can view and manage flaws and security events on your server and perform the following operations to enhance the security of your server:
   - Go to the Assets page to view detailed information about the security status of the servers under your Alibaba Cloud account. This page also allows you to add tags to assets and create asset groups. For more information about this page, see Assets.
   - Go to the Alerts page to view unusual activities and attacks that have been detected on your servers, such as unusual logon activities, brute force cracking, webshells, suspicious processes, suspicious network connections, sensitive file tampering, and malicious processes. For more information, see Security events.
   - Go to the Vulnerabilities page to view system software vulnerabilities and web content management system (WCMS) vulnerabilities. For more information, see Vulnerability fix prioritization.
   - Go to theBaseline Check page to view and manage vulnerable configurations that have been detected on your servers. For more information, see Server baseline check.
   - Go to the Asset Fingerprints page to view asset summary, including processes running on your servers, enabled system accounts, open ports, software version, and logons to the back end of your website. For more information, see Asset fingerprints.
   - The Security Center console also provides additional settings for you to use the Security Center features more efficiently. You can go to the Settings page to perform the following tasks:
     - Install or uninstall the Security Center agent.
     - Configure alert policies.

     For more information about this page, see Security Center settings.