Container Guard Security

Best Practices

Issue	02
Date	2021-06-04

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Container Intrusion Response

Container Guard Service (CGS) can detect escapes, high-risk system calls, abnormal processes, abnormal files; and can check the container environment. After the alarm notification function is enabled, you can receive alarm notification emails and SMS messages sent by CGS when it detects abnormal events.

This document describes the emergency response measures during and after a container intrusion.

Context

An increasing number of enterprises are using cloud-native technologies, deploying their applications on containers. However, many containers are exposed to attacks. Containers share resources such as OS kernels and storage. If attackers intrude a container, they can exploit vulnerabilities to escape from the container to attack server OS, breach data, or compromise servers. Therefore, you need to take countermeasures immediately when a container intrusion is detected.

Prerequisites

You have confirmed that the CGS intrusion alarm is true.

Handling a Container Intrusion Emergency

Step 1 **Log in to the management console**.

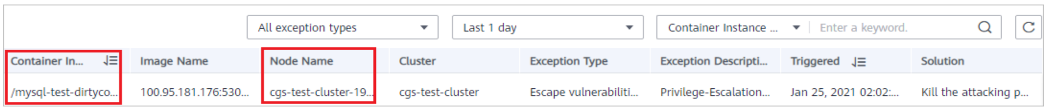
Step 2 In the upper part of the page, select a region, click ☰, and choose **Security & Compliance** > **Container Guard Service**.

Step 3 In the navigation pane, choose **Runtime Security**.

Step 4 Obtain the container instance name and node name of the intrusion program.

Click a tab (**Escapes**, **High-risk System Calls**, **Abnormal Programs**, **Abnormal Files**, or **Container Environment**) according to the alarm information and check the container instance name and node.

Figure 1-1 Abnormal event list



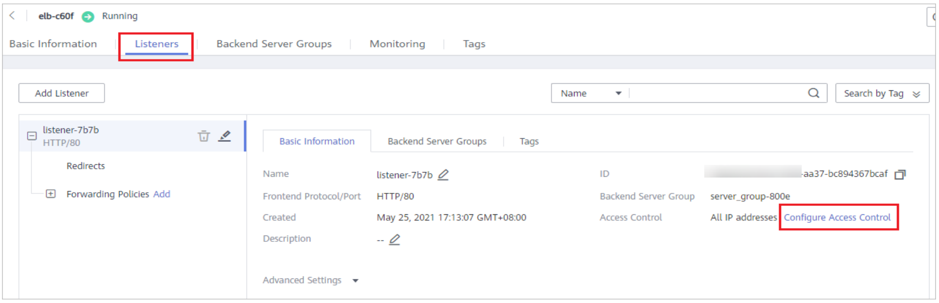
Container In...	Image Name	Node Name	Cluster	Exception Type	Exception Descripti...	Triggered	Solution
/mysql-test-dirtyco...	100.95.181.176:530...	cgs-test-cluster-19...	cgs-test-cluster	Escape vulnerabiliti...	Privilege-Escalation...	Jan 25, 2021 02:02:...	Kill the attacking p...

Step 5 Disconnect the container from the Internet.

For example, use Elastic Load Balance (ELB) to configure an access control policy to allow only specific IP addresses to access the container.

1. Click ☰ and choose **Network** > **Elastic Load Balance**.
2. Find the ELB instance used by the container.
3. Click the instance name. Click the **Listeners** tab.
4. In the **Basic Information** area, click **Configure Access Control**.

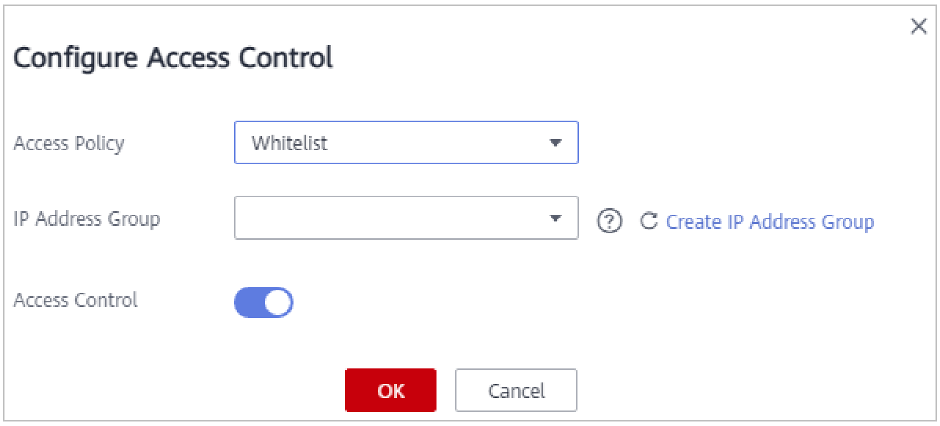
Figure 1-2 Configuring access control



Name: listener-7b7b
Frontend Protocol/Port: HTTP/80
Created: May 25, 2021 17:13:07 GMT+08:00
Description: --
ID: [redacted]-aa37-bc894367bcaf
Backend Server Group: server_group-800e
Access Control: All IP addresses Configure Access Control

5. In the **Configure Access Control** dialog box, add IP addresses to the whitelist.
   - Set **Access Policy** to **Whitelist**.
   - Select an IP address group.
   - Enable **Access Control**.

Figure 1-3 Configuring the IP address whitelist



Configure Access Control

Access Policy: Whitelist
IP Address Group:
Access Control: ●

6. Click **OK**.

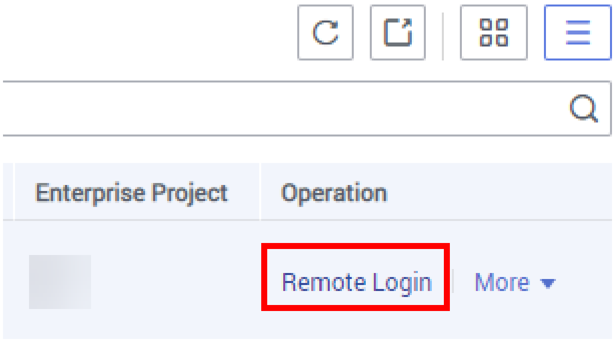
Step 6 Stop the container.

For example, remotely log in to the intruded node on the ECS console and stop the container.

1. In the navigation pane, choose **Elastic Cloud Server**.
2. In the **Operation** column of the **intruded node**, click **Remote Login**.

   If the login fails, rectify the fault by referring to **What Should I Do If I Cannot Log In to My Linux ECS?**

   Figure 1-4 Remote login

3. Run the following command to obtain the ID of the container:

   docker ps|grep *Container_instance_name*
4. Run the following command to suspend the container:

   docker pause *Container_ID*

Step 7 Retain intrusion traces.

1. Run the following command to export the image:

   docker save *ID* **-o** *Image_file***.tar**
2. (Optional) Run the following command to export the configuration:

   docker inspect *ID* **>** *Image_file***.json**

Step 8 Analyze the attack source.

1. On another node, import the image that was exported from **Step 7.1**. Run the following command:

   docker load - *Image_file.tar*
2. Use the imported image to start the new container.

   Run the following command:

   docker run -d -it --name *Container_name Image_ID* **/bin/bash**
3. Contact technical support to query system logs and search for malicious files to locate the intrusion cause and decide emergency response measures.

----End

2 Fixing the runc Symlink Mount and Container Escape Vulnerability (CVE-2021-30465)

Context

runc is vulnerable to a symlink exchange attack whereby an attacker can request a seemingly-innocuous POD or container configuration that actually results in the host filesystem being bind-mounted into the container (allowing for a container escape). CVE-2021-30465 has been assigned for this vulnerability. Currently, the details and POC of this vulnerability have been disclosed and the risk is high.

If you are a runc user, check your runc version and implement timely security hardening.

Vulnerability ID

CVE-2021-30465

Vulnerability Name

runC symlink mount and container escape vulnerability

Scope of Impact

- Affected versions: runc 1.0.0-rc94 and earlier
- Secure version: runc 1.0.0-rc95

Official Solution

This vulnerability has been fixed in the latest official version. If your service version falls into the affected range, upgrade it to the latest secure version.

Download address: **https://github.com/opencontainers/runc/releases**

Detecting and Fixing the Vulnerability

CGS can prevent and monitor the escape that exploited this vulnerability.

CGS monitors the status of containers in a cluster in real time, generates alarms for abnormal events, and provides solutions.

- **Check frequency**

  Real-time check

- **Detection mechanism**

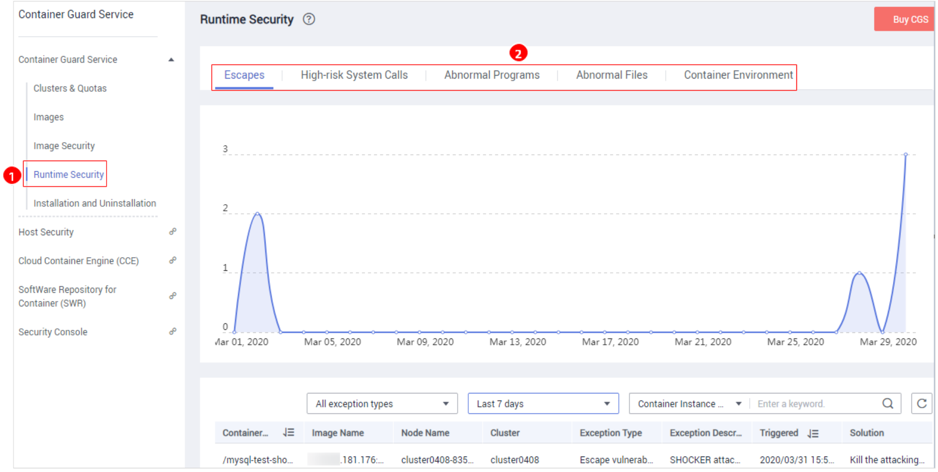
  For details about how the vulnerability is detected, see **Viewing Container Runtime Security Details**.

- **Viewing detection details**

  On the **Runtime Security** page, you can check the container escape trend chart and event list (see **Figure 2-1**), and can handle abnormal events based on the solutions provided.

  - On the **Container Environment** tab, you can monitor and prevent container escapes.
  - On the **Container Escapes** tab, you can monitor container escape behavior.

Figure 2-1 Runtime security



Container...	Image Name	Node Name	Cluster	Exception Type	Exception Descr...	Triggered	Solution
/mysql-test-sho...	[redacted].181.176:...	cluster0408-835...	cluster0408	Escape vulnerab...	SHOCKER attac...	2020/03/31 15:5...	Kill the attacking...

A Change History

Release Date	Description
2021-07-08	This issue is the third official release. The service entry is updated.
2021-06-04	This issue is the second official release. Added **Fixing the runc Symlink Mount and Container Escape Vulnerability (CVE-2021-30465)**.
2021-05-27	This issue is the first official release.