|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | |  |
|  | | |
|  | | |
| 方圆ok1 | | | |
|  | Bare Metal Server 6.1.20.2  Upgrade Guide | | 附件1-16K |
|  | |
| **Issue** | **01** |
| **Date** | **2017-11-11** |
|  | |
| HUAWEI TECHNOLOGIES CO., LTD. | |
|  | | |

|  |
| --- |
| Copyright © Huawei Technologies Co., Ltd. 2017. All rights reserved.  No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.  Trademarks and Permissions  附件3-图 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. |

|  |  |
| --- | --- |
| Huawei Technologies Co., Ltd. | |
| Address: | Huawei Industrial Base  Bantian, Longgang  Shenzhen 518129  People's Republic of China |
| Website: | <http://e.huawei.com> |

Contents

[1 Background 4](#_Toc498193719)

[2 Resolved Issues 5](#_Toc498193720)

[3 Prerequisites 6](#_Toc498193721)

[**3.1 Obtaining the Environment Information** 6](#_Toc498193722)

[**3.2 Obtaining Software Packages** 6](#_Toc498193723)

[**3.3 Obtaining the IP Addresses of Target Nodes** 6](#_Toc498193724)

[**3.4 Preparing the Ansible Server** 7](#_Toc498193725)

[4 Patch Installation 8](#_Toc498193726)

[**Operations at the Cascaded Layer** 8](#_Toc498193727)

[5 Patch Rollback 9](#_Toc498193728)

[**Operations at the Cascaded Layer** 9](#_Toc498193729)

[6 File Cleanup 10](#_Toc498193730)

[**6.1 Clearing the Compressed Package** 10](#_Toc498193731)

[**6.2 Clearing the Patch Package** 10](#_Toc498193732)

[**6.2.1 Prerequisites** 10](#_Toc498193733)

[**6.2.2 Procedure** 10](#_Toc498193734)

# Background

The BMS and KVM are deployed in the same POD, and the RabbitMQ database of Nova is sharded. The BMS Remote Console functional component ironic-console-proxy should use the IP address of the sharded RabbitMQ database. However, the ironic-console-proxy configuration script is not mediated to the sharding scenario and uses the default RabbitMQ IP address. As a result, the message queue is not processed properly and the Remote Console function is unavailable.

The Remote Console function of all BMSs in the POD is unavailable.

This document provides a solution for the preceding issue and guidance for field engineers.

This document applies to the following versions:

* FusionSphere OpenStack V100R006C10U20SPC001
* FusionSphere OpenStack V100R006C10U20SPC002

The patch applies to the following scenario:

The BMS and KVM are deployed in the same POD, and the RabbitMQ database of Nova is sharded.

# Resolved Issues

This patch resolves the following issue.

|  |  |
| --- | --- |
| **Trouble Ticket Number** | DTS2017111101006 |
| **Description** | [Public cloud][KVM][BMS service][α test][BMS remote login]  In the Open Telekom Cloud production environment, when the BMS and KVM are deployed in the same POD, and the RabbitMQ database of Nova is sharded, the Remote Console function is unavailable. |
| **Root Cause** | The BMS and KVM are deployed in the same POD, and the RabbitMQ database of Nova is sharded. The BMS Remote Console functional component ironic-console-proxy should use the IP address of the sharded RabbitMQ database. However, the ironic-console-proxy configuration script is not mediated to the sharding scenario and uses the default RabbitMQ IP address. As a result, the message queue is not processed properly and the Remote Console function is unavailable. |
| **Solution** | Modify the control script of the ironic-console-proxy component and add a process mediated for the database sharding scenario so that the rabbitmq\_host IP address can be configured based on the RabbitMQ name in the database sharding scenario. |

# Prerequisites

## **Obtaining the Environment Information**

Obtain the following information from O&M personnel:

* Ansible server login information
* Private key certificate **id\_rsa** for logging in to the cascading and cascaded FusionSphere OpenStack systems using SSH

If the certificate has a password, ensure that the Ansible server can connect to hosts in the cascading and cascaded FusionSphere OpenStack systems using SSH without a password.

* Private key certificate **id\_rsa.ppk** for logging in to the cascading and cascaded FusionSphere OpenStack systems over PuTTY

If the certificate is encrypted, obtain the password of the certificate.

* IP address and password of user **root** for logging in to controller nodes in the cascading and cascaded FusionSphere OpenStack systems

Ensure that the passwords of users **root** for logging in to all controller nodes in the cascading and cascaded FusionSphere OpenStack systems are the same.

## **Obtaining Software Packages**

Obtain the **Bare\_Metal\_Server\_6.1.20.2\_Patch.zip** package.

Visit <http://support.huawei.com/carrier/> and choose **Software** > **Carrier IT** > **Cloud Computing** > **FusionCloud** > **FusionSphere** > **Bare Metal Server** > **Bare Metal Server 6.1.20.2**.

Decompress the package on the jump server to obtain the **Bare\_Metal\_Server\_6.1.20.2\_Patch.tar.gz** patch package.

## **Obtaining the IP Addresses of Target Nodes**

Copy the **Bare\_Metal\_Server\_6.1.20.2\_Patch.tar.gz** package to the jump server.

Run the following commands to log in to the controller node of the cascaded BMS POD, switch to user **root**, and import environment variables:

**ssh fsp@***OM IP address of the controller node of the cascaded BMS POD*

**su - root**

**source set\_env**

**1**

**FusionSphere123**

**TMOUT=0**

Run the following command to obtain the OM IP addresses of the nodes where the ironic-console-proxy component is deployed at the cascaded layer:

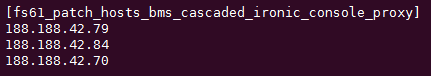
**cps template-instance-list --service ironic ironic-console-proxy | grep -v omip |awk -F '|' '{print $6}' |xargs -i echo "{}"**

**----End**

## **Preparing the Ansible Server**

Log in to the Ansible node, open the **/etc/ansible/hosts** file, add a hostgroup named **[fs61\_patch\_hosts\_bms\_cascaded\_ironic\_console\_proxy]**, and add the OM IP addresses obtained in [the previous section](#obtainOMIPstep3) to **[fs61\_patch\_hosts\_bms\_cascaded\_ironic\_console\_proxy]**:

**vim /etc/ansible/hosts**



Upload the **Bare\_Metal\_Server\_6.1.20.2\_Patch.tar.gz** package to the **/home/admin** directory of the Ansible server.

Run the **ll /home/admin** command to check whether the **Bare\_Metal\_Server\_6.1.20.2\_Patch.tar.gz** package exists.

Upload the **id\_rsa** file to the **/home/admin** directory of the Ansible server and run the following command to change its permissions:

**chmod 600 /home/admin/id\_rsa**

**----End**

# Patch Installation

## **Operations at the Cascaded Layer**

Log in to the Ansible server, run the following command to upload the patch package to the ironic-console-proxy nodes at the cascaded layer, and enter the BMS cascaded POD password of user **root** as prompted:

**ansible fs61\_patch\_hosts\_bms\_cascaded\_ironic\_console\_proxy -m copy -a "src=/home/admin/Bare\_Metal\_Server\_6.1.20.2\_Patch.tar.gz dest=/home/fsp/ owner=fsp group=fsp mode=0777" -u fsp --su --su-user=root --ask-su-pass --private-key=/home/admin/id\_rsa**

On the Ansible server, run the following command to decompress the patch package on the ironic-console-proxy nodes at the cascaded layer, and enter the BMS cascaded POD password of user **root** as prompted:

**ansible fs61\_patch\_hosts\_bms\_cascaded\_ironic\_console\_proxy -m command -a "tar zxf /home/fsp/Bare\_Metal\_Server\_6.1.20.2\_Patch.tar.gz -C /home/fsp" -u fsp --su --su-user=root --ask-su-pass --private-key=/home/admin/id\_rsa**

On the Ansible server, run the following command to install the patch on the ironic-console-proxy nodes at the cascaded layer, and enter the BMS cascaded POD password of user **root** as prompted:

**ansible fs61\_patch\_hosts\_bms\_cascaded\_ironic\_console\_proxy -m command -a "sh /home/fsp/Bare\_Metal\_Server\_6.1.20.2\_Patch/patch\_opts.sh install" -u fsp --su --su-user=root --ask-su-pass --private-key=/home/admin/id\_rsa**

Run the following commands to log in to the controller node of the cascaded BMS POD using SSH, switch to user **root**, and import environment variables:

**ssh fsp@***OM IP address of the controller node of the cascaded BMS POD*

**su - root**

**source set\_env**

**1**

**FusionSphere123**

**TMOUT=0**

**cps template-params-update --service ironic ironic-console-proxy --parameter mq\_instance=rabbitmq\_nova**

**cps commit**

On the Ansible server, run the following command to check the file privilege on the ironic-console-proxy nodes at the cascaded layer, and enter the BMS cascaded POD password of user **root** as prompted:

**ansible fs61\_patch\_hosts\_bms\_cascaded\_ironic\_console\_proxy -m command -a "sh /home/fsp/Bare\_Metal\_Server\_6.1.20.2\_Patch/patch\_opts.sh recover\_pyc\_privilege" -u fsp --su --su-user=root --ask-su-pass --private-key=/home/admin/id\_rsa**

**----End**

# Patch Rollback

## **Operations at the Cascaded Layer**

Log in to the Ansible server and run the following command to roll back the patch on the ironic-console-proxy nodes at the cascaded layer:

**ansible fs61\_patch\_hosts\_bms\_cascaded\_ironic\_console\_proxy -m command -a "sh /home/fsp/Bare\_Metal\_Server\_6.1.20.2\_Patch/patch\_opts.sh rollback" -u fsp --su --su-user=root --ask-su-pass --private-key=/home/admin/id\_rsa**

Log in to the controller node of the cascaded BMS POD and run the following commands to make the rollback take effect:

**ssh fsp@***OM IP address of the controller node of the cascaded BMS POD*

**su - root**

**source set\_env**

**1**

**FusionSphere123**

**TMOUT=0**

**cps template-params-update --service ironic ironic-console-proxy --parameter mq\_instance=rabbitmq**

**cps commit**

On the Ansible server, run the following command to check the file privilege on the ironic-console-proxy nodes at the cascaded layer, and enter the BMS cascaded POD password of user **root** as prompted:

**ansible fs61\_patch\_hosts\_bms\_cascaded\_ironic\_console\_proxy -m command -a "sh /home/fsp/Bare\_Metal\_Server\_6.1.20.2\_Patch/patch\_opts.sh recover\_pyc\_privilege" -u fsp --su --su-user=root --ask-su-pass --private-key=/home/admin/id\_rsa**

**----End**

# File Cleanup

## **Clearing the Compressed Package**

Log in to the Ansible server, run the following command to clear the compressed package on each ironic-console-proxy node at the cascaded layer, and enter the BMS cascaded POD password of user root as prompted:

**ansible fs61\_patch\_hosts\_bms\_cascaded\_ironic\_console\_proxy -m command -a "rm -rf /home/fsp/Bare\_Metal\_Server\_6.1.20.2\_Patch.tar.gz" -u fsp --su --su-user=root --ask-su-pass --private-key=/home/admin/id\_rsa**

## **Clearing the Patch Package**

### **Prerequisites**

After the patch is issued and the environment is running properly, perform the required operations to clear the patch package.

### **Procedure**

Log in to the Ansible server, run the following command to clear the patch package on the ironic-console-proxy nodes at the cascaded layer, and enter the BMS cascaded POD password of user **root** as prompted:

**ansible fs61\_patch\_hosts\_bms\_cascaded\_ironic\_console\_proxy -m command -a "rm -rf /home/fsp/Bare\_Metal\_Server\_6.1.20.2\_Patch" -u fsp --su --su-user=root --ask-su-pass --private-key=/home/admin/id\_rsa**