CDP集群自定义告警脚本配置

CDP Performance Testing

|  |  |  |  |
| --- | --- | --- | --- |
| Revision History | | | |
| Version | Author | Description | Date |
| 0.1 | Li,Kangbiao |  | --th Sep 2021 |
| 0.2 | ShuaiPeng |  | 2023/2/2 |
|  |  |  |  |

# 前言

Cloudera Manager支持三种方式的告警输出，配置邮箱、使用SNMP方式以及通过自定义告警脚本方式接入告警。本文档是将Alert Publisher配置为运行用户编写的脚本以响应警报。

Alert Publisher将单个参数传递给脚本，该参数实施包含警报列表的UTF-8 JSON文件。该脚本在运行Alert Publisher服务的主机上运行，并且必须具有Cloudera-scm用户的读取和执行权限。一次只运行一个脚本实力，来自脚本的标准输出和标准错误消息将被记录到Alert Publisher日志文件中。

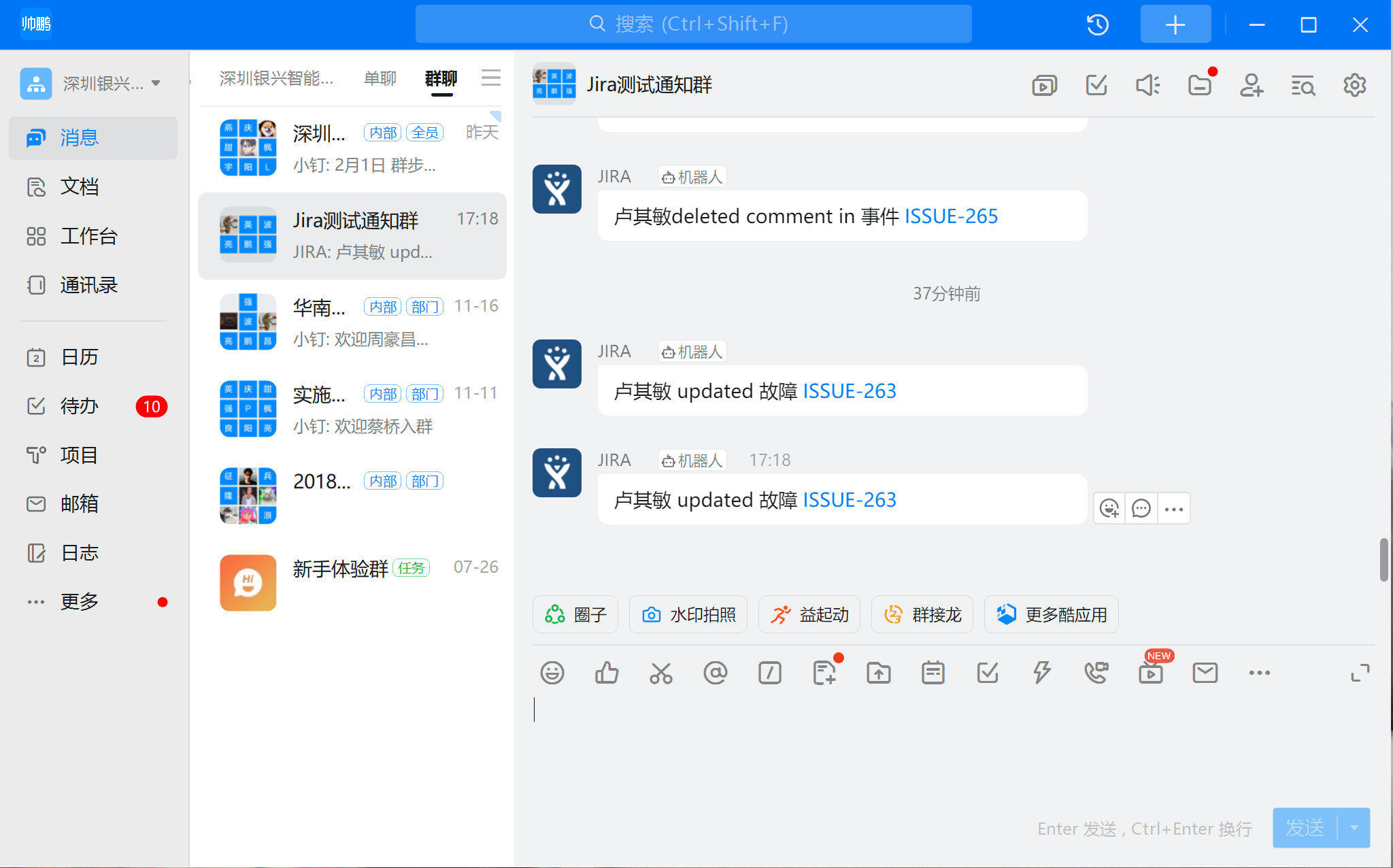
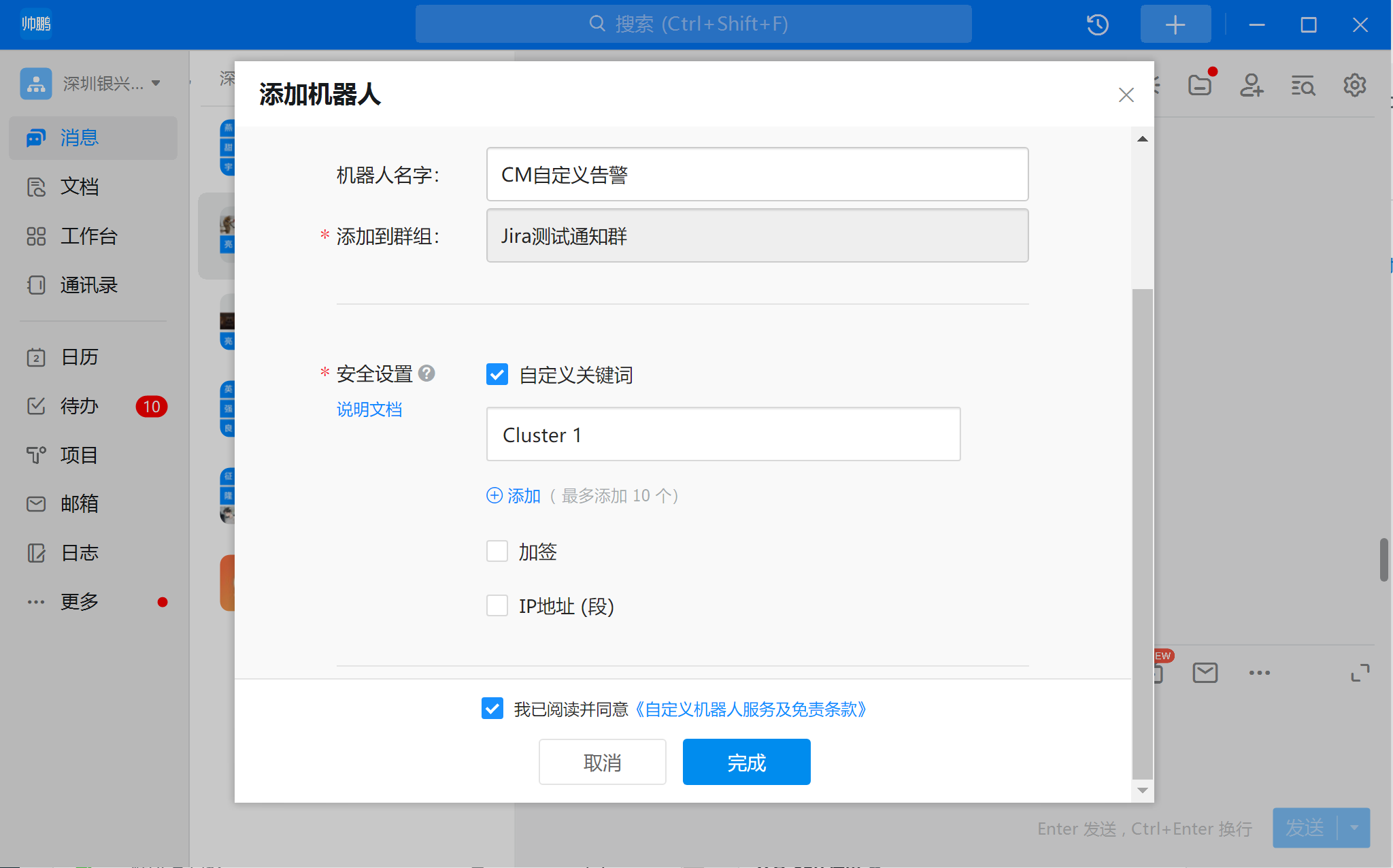
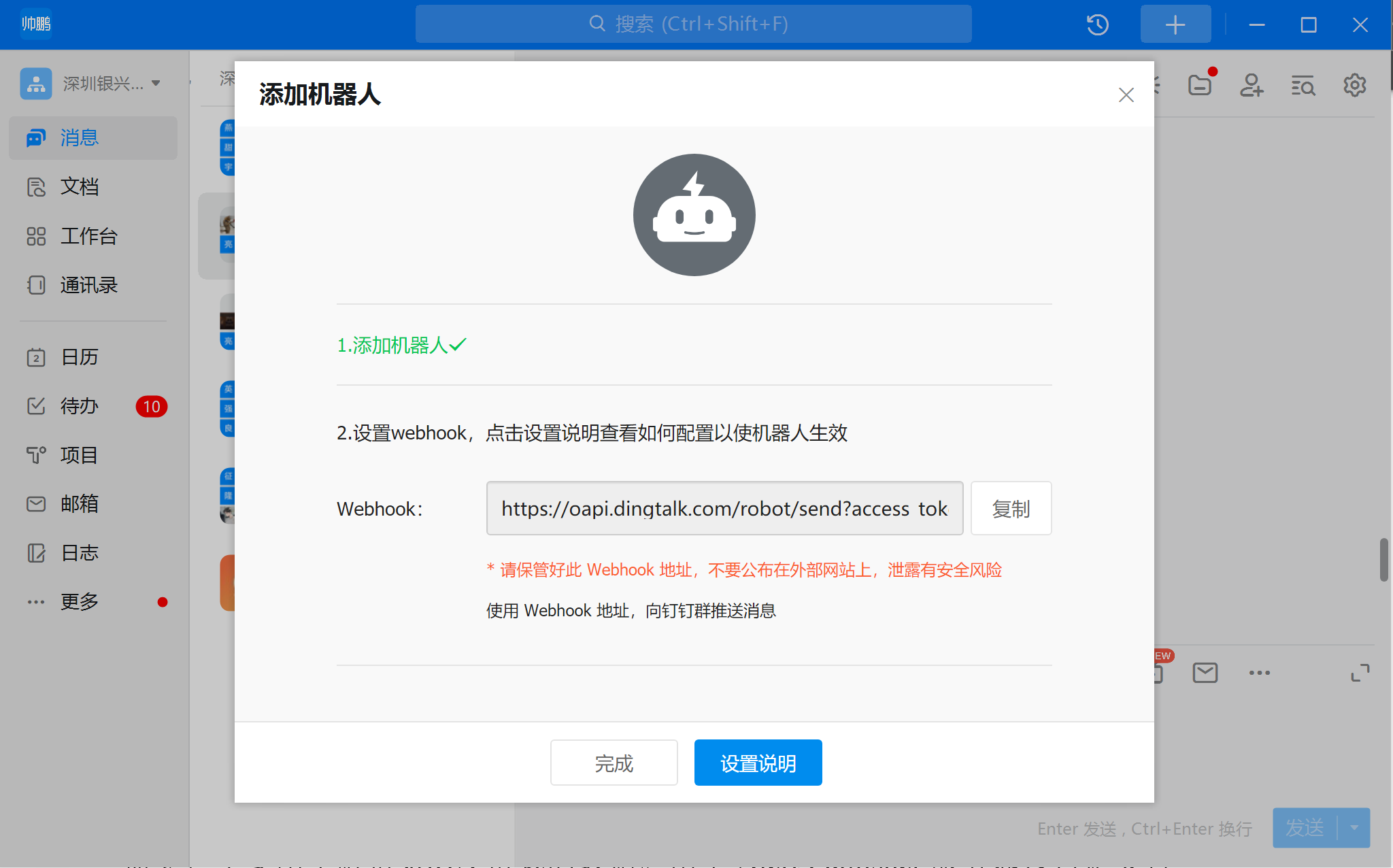
* 环境介绍：

1. CDP7.1.7及CM7.6.5
2. CentOS Linux release 7.9.2009 (Core)

# 环境准备

1. 建立钉钉reboot并取得webhook

在想要添加告警机器人的钉钉群中点击群设置，在智能群助手中点击添加机器人，选择自定义机器人，选择一个安全设置后即可添加一个告警机器人，同时获取到webhook。

**webhook:** [**https://oapi.dingtalk.com/robot/send?access\_token=2e5eab4e097014401ba512ba7c498dd5b402b6f43ffbefbf1b96713b009c9e04**](https://oapi.dingtalk.com/robot/send?access_token=2e5eab4e097014401ba512ba7c498dd5b402b6f43ffbefbf1b96713b009c9e04)

2. 在Cloudera Manager服务器上安装JQ命令，用于解析JOSN数据文件

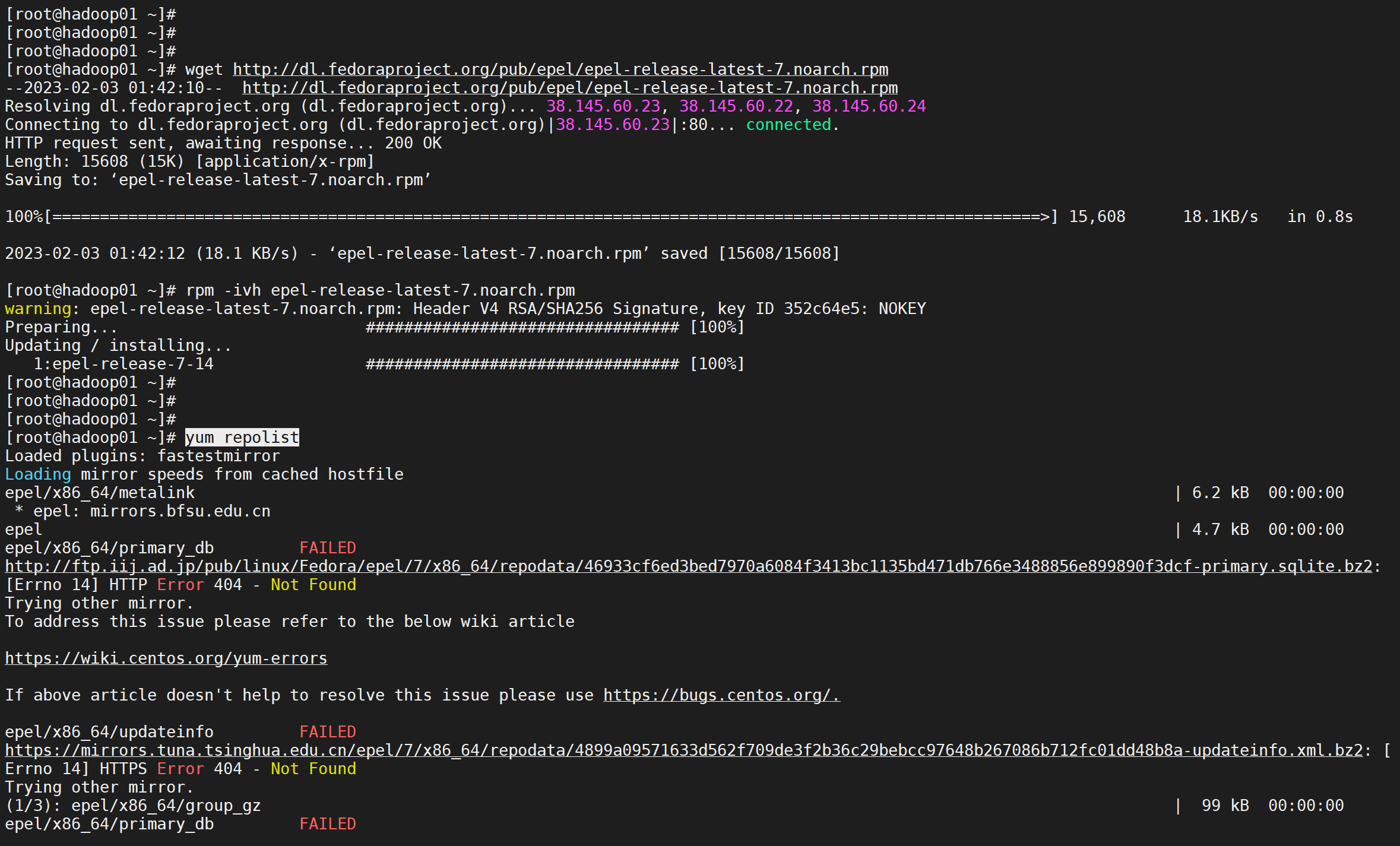
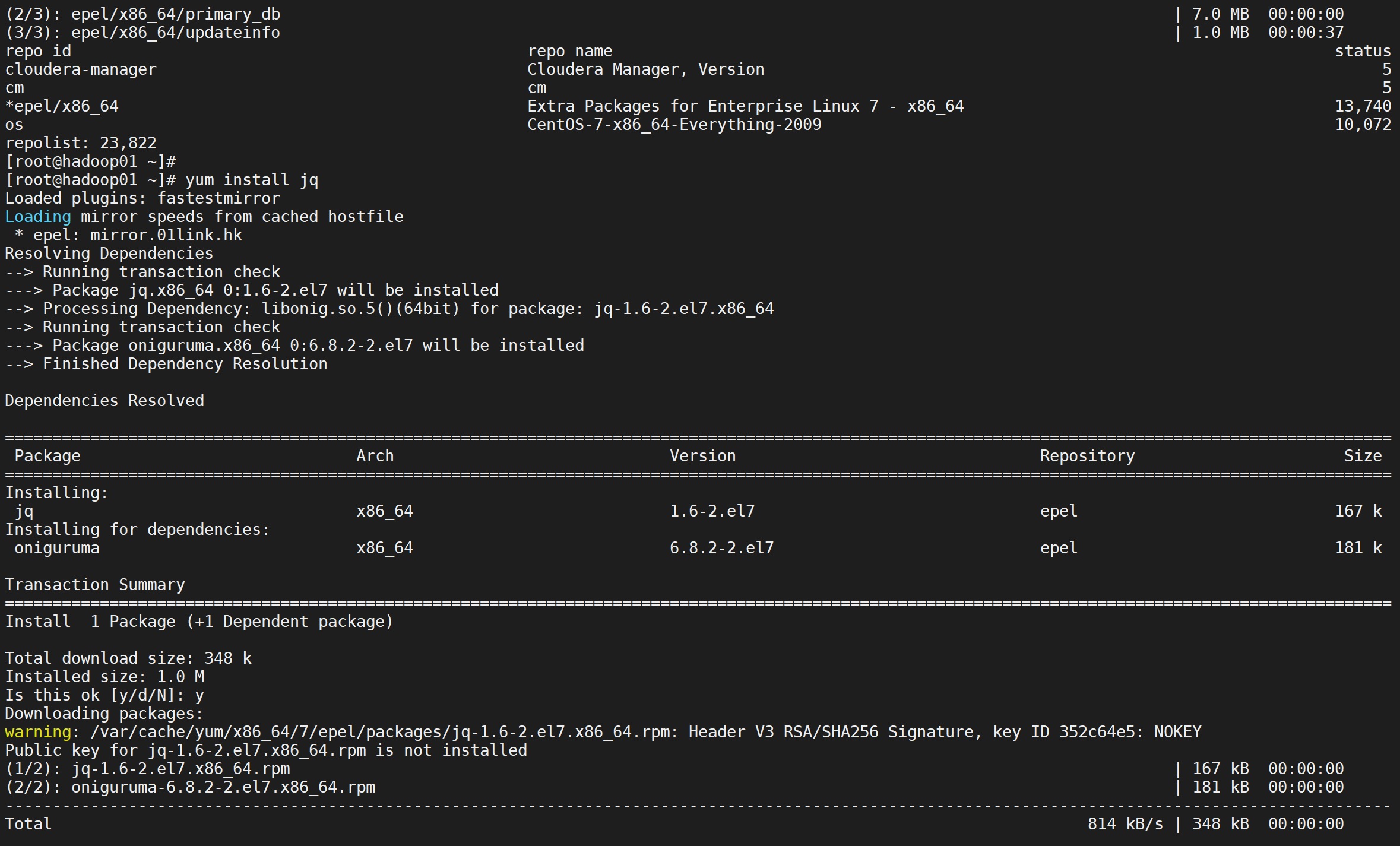
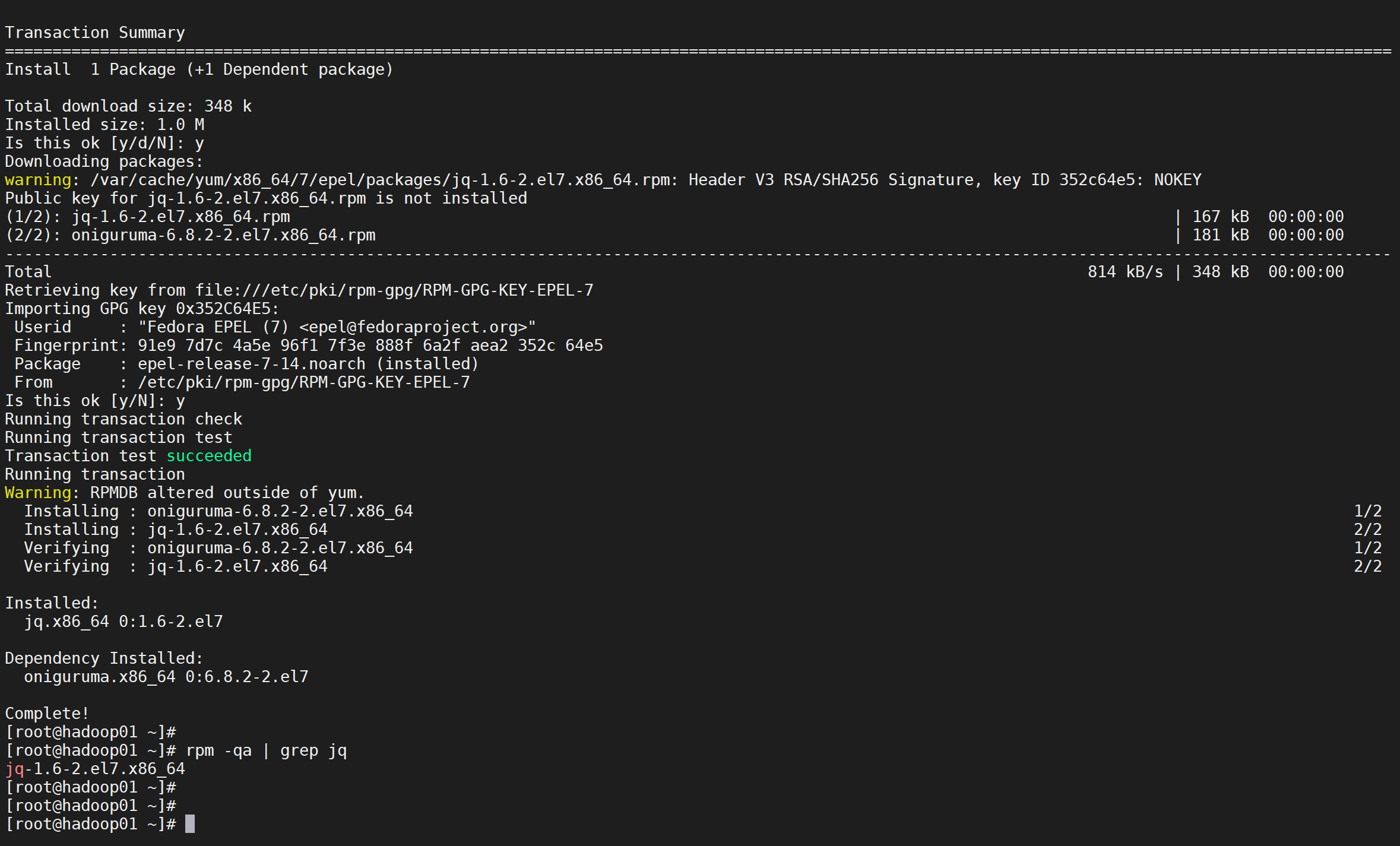
这里在Cloudera Management Service下的Alert Publisher服务所在节点安装了jq命令，主要用于解析JSON格式的数据。由于Alert Publisher服务通过自定义告警脚本方式输出的告警内容为json格式，为了能够方便的解析。

wget <http://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm>

rpm -ivh epel-release-latest-7.noarch.rpm

yum repolist

yum -y install jq

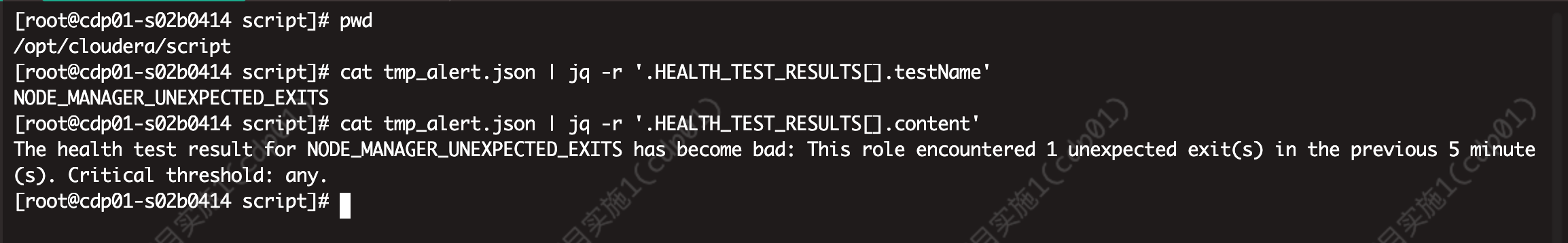
  

3. 在Linux上可以通过jq命令方便的解析JSON数据，如下所示：

cat tmp\_alert.json | jq -r

'.HEALTH\_TEST\_RESULTS[].testName'

cat tmp\_alert.json | jq -r '.HEALTH\_TEST\_RESULTS[].content'



# 自定义告警脚本及配置

1. 在Alert Publisher服务所在节点创建如下目录，并修改属主

mkdir -p /opt/cloudera/script

chown cloudera-scm. /opt/cloudera/script

ll /opt/cloudera/



注意：需要将脚本目录修改属主为cloudera-scm，因为该脚本会在改目录下产生一些临时文件。

1. 在/opt/cloudera/script目录下创建alert\_script.sh脚本，内容如下：

#!/bin/bash

OG\_ALERT\_FILE=$1

date=`date` # 定义告警日志

ALERT\_FILE=/tmp/alert\_test.log # 定义告警解析后日志文件

ALERT\_RESULT\_FILE=/opt/cloudera/script/alert\_result.log

#告警解析存放目录，将原始的告警日志转换为一行行的json存储

TMP\_ALERT\_FILE=/opt/cloudera/script/tmp\_alert.json

cat $OG\_ALERT\_FILE | jq -r '.[].body.alert|"\(.attributes)"' > $TMP\_ALERT\_FILE

while read -r line

do

cluster=$(echo -e $line | jq -r '.CLUSTER\_DISPLAY\_NAME[]')

hostname=$(echo -e $line |jq -r '.HOSTS[]')

timestamp=$(echo -e $line | jq -r "(.\_\_persist\_timestamp[])")

timestamp=`date -d @${timestamp: :-3} "+%Y-%m-%d %H:%M:%S"`

ipaddress=`cat /etc/hosts | grep ${hostname} | awk -F " \*" '{print $1}'`

if [ $? -ne 0 ];then

hostname=null

fi

echo -e $line | jq -r '.|"\(.HEALTH\_TEST\_RESULTS[])"' |while read alert; do

alert\_service=$(echo -e $alert | jq -r '.testName')

alert\_enent\_doce=$(echo -e $alert | jq -r '.code')

alert\_content=$(echo -e $alert | jq -r '.content')

alert\_severity=$(echo -e $alert | jq -r '.severity')

echo "告警集群:[$cluster],告警主机：[$hostname],告警级别：[$alert\_severity],告警服务:[$alert\_service],告警事件编码:[$alert\_enent\_doce],告警详细内容：[$alert\_content]" >> $ALERT\_RESULT\_FILE

message="告警集群：[$cluster]\n告警主机：[$hostname/$ipaddress]\n告警时间：[$timestamp]\n告警级别：[$alert\_severity]\n告警服务：[$alert\_service]\n告警详细内容：[$alert\_content]"

#将解析后的告警消息推送到钉钉中去

curl "https://oapi.dingtalk.com/robot/send?access\_token=2e5eab4e097014401ba512ba7c498dd5b402b6f43ffbefbf1b96713b009c9e04" -H "Content-Type: application/json" -d "{\"msgtype\": \"text\",\"text\": {\"content\": \"$message\"}}"

done

done < $TMP\_ALERT\_FILE

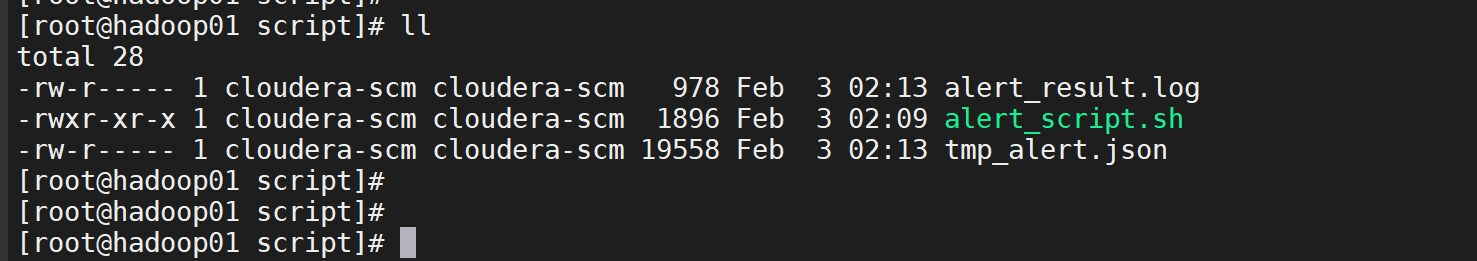
echo "$date: Wrting log to $ALERT\_RESULT\_FILE" >> $ALERT\_FILE



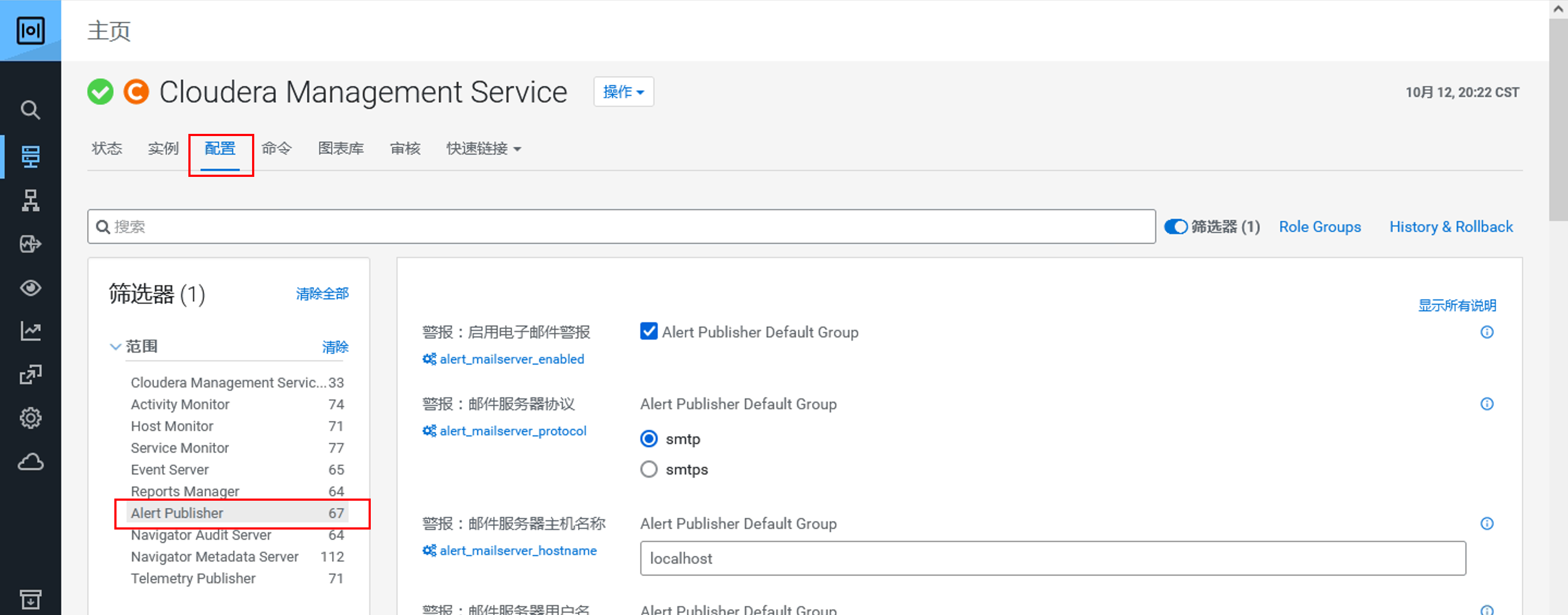
1. 执行脚本属主及执行权限

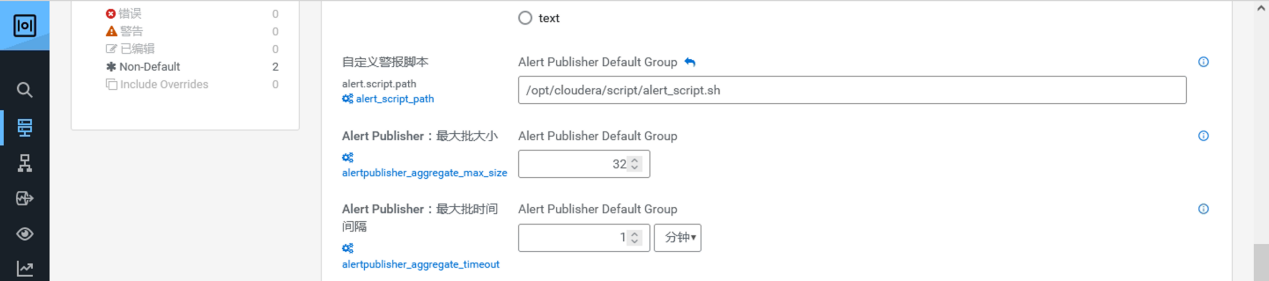
chown cloudera-scm. alert\_script.sh

chmod +x alert\_script.sh



1. 登陆进入Cloudera Manager Service配置页面，配置自定义告警脚本路径

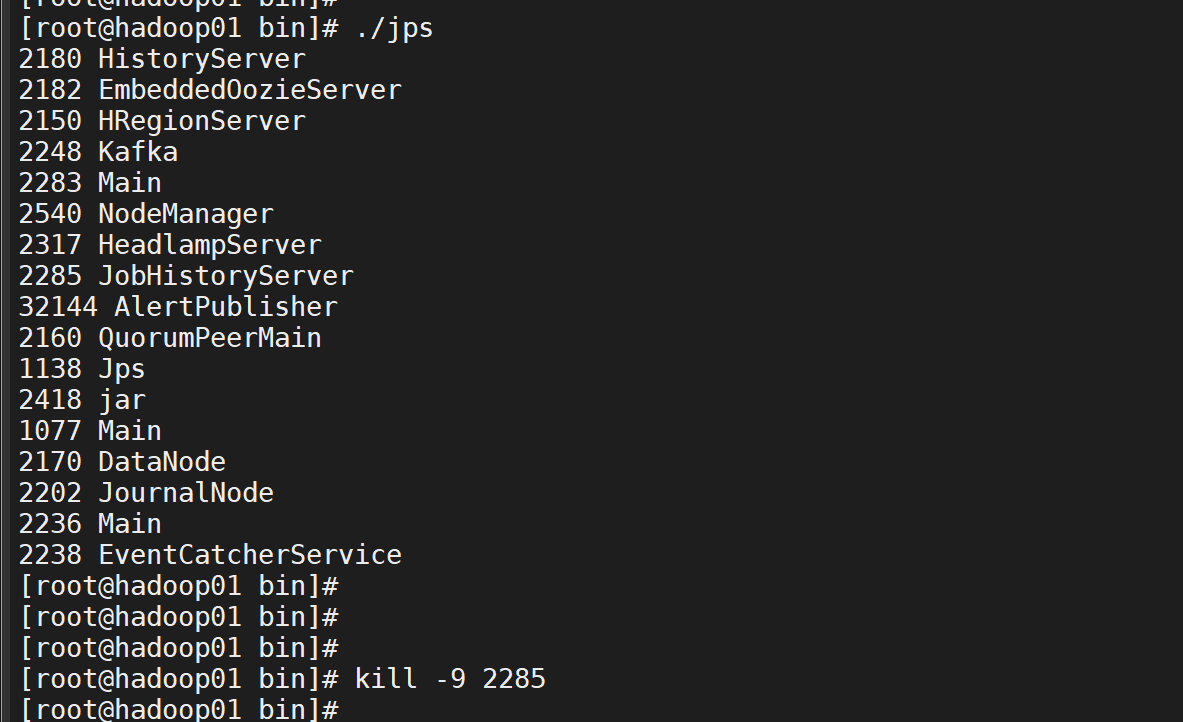




完成上述配置后，重启Alert Publisher服务即可，不需要重启CMS所有服务。

# 告警脚本测试

1. 在集群中手动Kill掉几个服务的进程

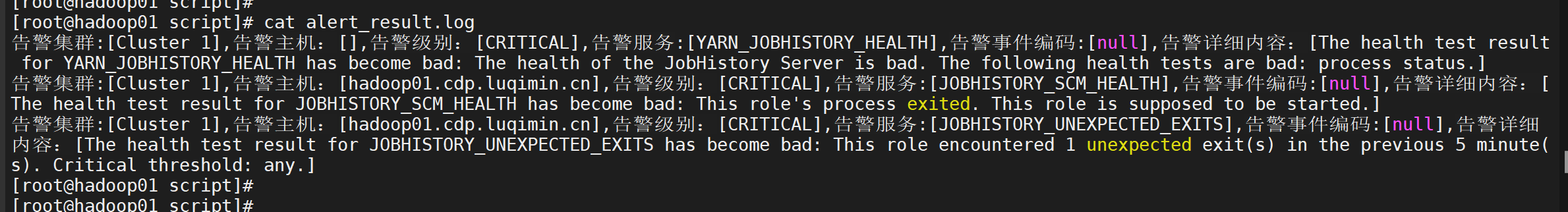


这里将hadoop01.cdp.luqimin.cn/192.168.2.11节点的[JobHistory Server](https://192.168.2.11:7183/cmf/services/1546334813/instances/1546334832/status" \o ")

服务进行Kill掉了，在CM上已经显示这个服务异常。

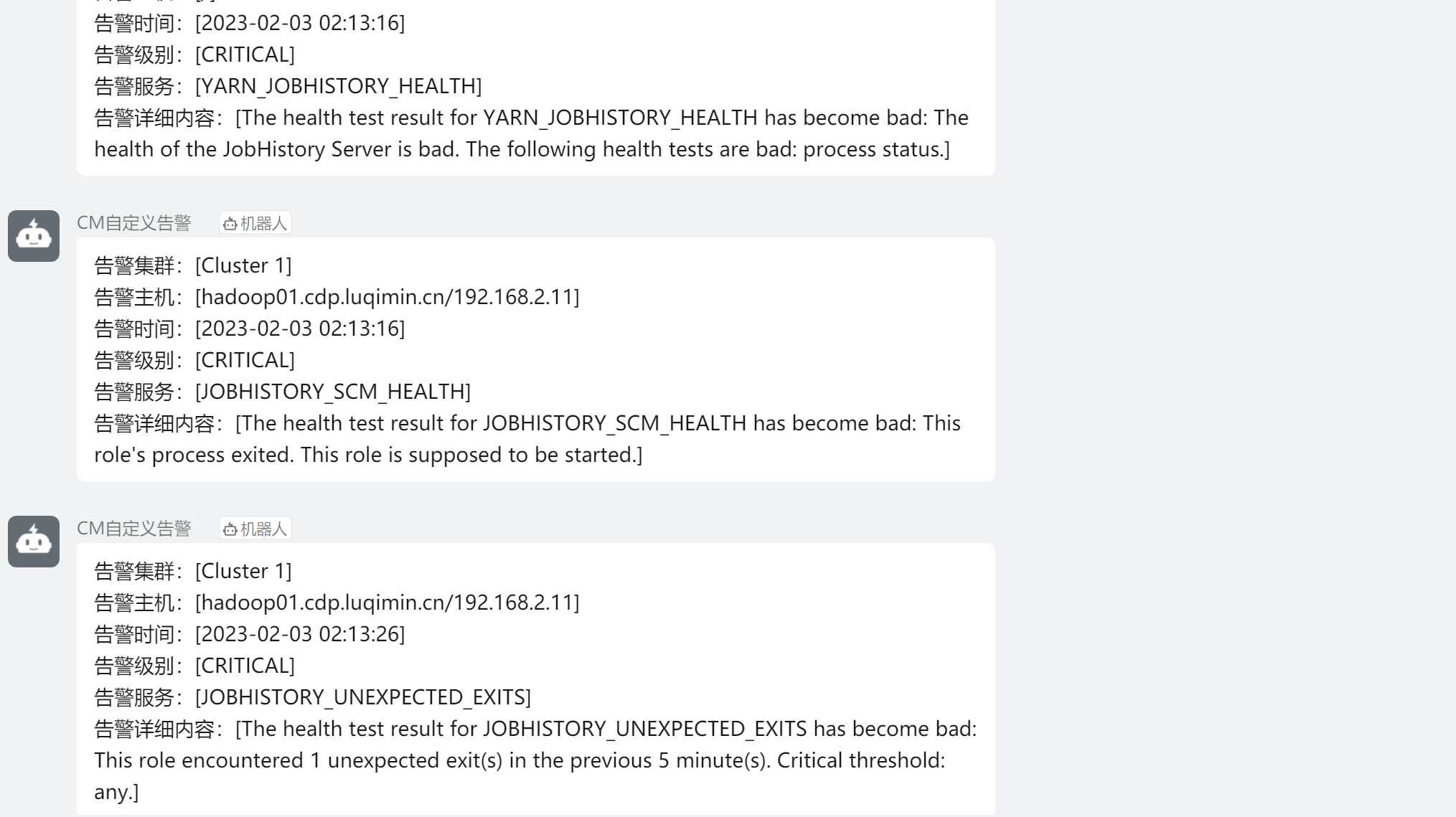


1. 登陆Alert Publisher所在服务器上，进入/opt/cloudera/script目录下



可以看到alert\_result.log日志文件中保存着已解析好的告警日志。

1. 登陆钉钉群里，查看Reboot是否正确发送集群告警信息



可以看到钉钉的Reboot可以正确发送集群告警信息，证明钉钉发送的告警信息正确。再通过对比服务异常告警时间，时间证明对比符合。

# 总结

1. Alert Publisher服务负责将集群的告警信息转发，通过自定义脚本会在/opt/cloudera/script目录下生成一个tmp\_alert.json原始告警文件，文件内容为JSON格式。
2. 通过自定义告警脚本将原始告警解析后，在脚本中还可以将解析好的告警通过HTTP或其他采集方式将告警上报
3. 本次使用的jq命令解析JSON文件，或可以采用python、JAVA等方式。
4. Cloudera自定义告警参考：<https://docs.cloudera.com/cdp-private-cloud-base/7.1.7/monitoring-and-diagnostics/topics/cm-alerts-script.html>
5. 安装jq参考：[centos7 yum 安装jq - Captain林 - 博客园 (cnblogs.com)](https://www.cnblogs.com/CaptainLin/p/7064520.html)
6. 设置钉钉群告警机器人参考：[获取钉钉机器人Webhook地址 (aliyun.com)](https://help.aliyun.com/document_detail/332880.html)