云备份

最佳实践

文档版本	01
发布日期	2025-08-05

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 通过自定义脚本实现数据库备份

1.1 通过自定义脚本实现 MySQL 一致性备份

本章节以SuSE 11 SP3操作系统下MySQL 5.5单机版为例，介绍如何通过自定义脚本来冻结、解冻MySQL数据库，以实现对于MySQL数据库的数据库备份。

场景介绍

某企业购买了云服务器，并在云服务器中安装了MySQL 5.5数据库用于存放业务数据。随着数据量的增加，之前的崩溃一致性保护已经满足不了RTO、RPO的要求，决定采用应用一致性备份，减小RTO与RPO。

数据准备

表 1-1 数据准备

准备项	说明	示例
MySQL用户名	连接MySQL数据库时使用的用户名	root
MySQL密码	连接MySQL数据库时使用的密码	Example@123

详细步骤

步骤1 加密MySQL密码，供自定义脚本使用

1. 登录MySQL服务器，输入**cd /home/rdadmin/Agent/bin/** ，进入Agent目录。
2. 执行**/home/rdadmin/Agent/bin/agentcli encpwd**，回显如下：
   ```
   Enter password:
   ```
   输入MySQL密码，并按“Enter”，屏幕上就会打印出加密后的密码，将其复制到剪贴板中。

   说明

   冻结解冻脚本中配置的明文密码长度不超过16位，否则配置后密码会被截断，应用一致性备份会失败。

步骤2 执行**cd /home/rdadmin/Agent/bin/thirdparty/ebk_user** ，进入自定义脚本目录，然后执行**vi mysql_freeze.sh**，打开MySQL示例冻结脚本。

将下图所示的**MYSQL_USER**与**MYSQL_PASSWORD**修改为实际值，其中**MYSQL_PASSWORD**为**步骤1**的屏幕输出。

```
#*********************************************************************************
#Importnata note
#Please change this parameters according to your Mysql system configuration!!!
MYSQL_USER="root"
MYSQL_PASSWORD="00000001000000010000000000000005000000010000000017334dcf36ace871b1
0001000000000000080400000001000000129678894e3225391233bac37497d37280000000000000
#*********************************************************************************
```

也可以使用sed命令来直接进行修改：

sed -i 's/^MYSQL_PASSWORD=.*/MYSQL_PASSWORD="*XXX*"/' mysql_freeze.sh mysql_unfreeze.sh ，其中***XXX***为步骤1中打印出的密码。

此操作会同时修改冻结解冻脚本，所以无需再执行**步骤3**。

步骤3 执行**vi mysql_unfreeze.sh**，打开MySQL示例解冻脚本，修改此脚本中的用户名和密码。

mysql_unfreeze.sh与**mysql_freeze.sh**脚本实现了基本的数据库冻结与解冻操作，如果您在冻结、解冻时有其它额外步骤需要执行，可以自行在其中进行修改。详细说明请参见 **通过自定义脚本实现其它Linux应用的一致性备份**。

⚠ 注意

MySQL的冻结是通过FLUSH TABLES WITH READ LOCK指令来实现的，该指令需在指定时间内（10s）获取全局读锁和刷新缓存到磁盘；如果数据库业务繁忙时执行，该指令可能执行超时，一致性备份失败，严重时可能会导致数据库上层业务操作失败等问题。

此指令不会触发bin log刷盘操作，如果开启了bin log，且sync_binlog参数不为1，则可能出现保存的备份映像中部分SQL操作未记录到bin log的情况，如果bin log也需要完整保护，请设置sync_binlog=1。

----结束

1.2 通过自定义脚本实现 SAP HANA 一致性备份

本章节以SuSE 11 SP4 for SAP操作系统下HANA 2.0单机版为例，介绍如何通过自定义脚本来冻结、解冻HANA数据库，以实现对HANA数据库的数据库备份。

场景介绍

某企业购买了云服务器，并在上面安装了HANA 2.0单机版数据库，用于存放业务数据，随着数据量的增加，之前的崩溃一致性保护已经满足不了RTO、RPO的要求，决定采用应用一致性备份，减小RTO与RPO。

数据准备

表 1-2 数据准备

准备项	说明	示例
HANA用户名	连接HANA SYSTEMDB 数据库时使用的用户名	system
HANA密码	连接HANA SYSTEMDB 数据库时使用的密码	Example@123
HANA实例编号	连接HANA数据库时使用的实例编号	00
HANA SID	连接HANA数据库时使用的SID	WXJ

详细步骤

步骤1 加密HANA用户密码，供自定义脚本使用

1. 登录HANA服务器，输入**cd /home/rdadmin/Agent/bin/** ，进入Agent目录。
2. 执行**/home/rdadmin/Agent/bin/agentcli encpwd**，回显如下：
   ```
   Enter password:
   ```
   输入HANA用户的密码，并按“Enter”，屏幕上就会打印出加密后的密码，将其复制到剪贴板中。

   说明

   冻结解冻脚本中配置的明文密码长度不超过16位，否则配置后密码会被截断，应用一致性备份会失败。

   执行**cd /home/rdadmin/Agent/bin/thirdparty/ebk_user** ，进入自定义脚本目录，执行**vi hana_freeze.sh** ，打开HANA示例冻结脚本。

步骤2 将下图所示的**HANA_USER HANA_PASSWORD INSTANCE_NUMBER DB_SID**修改为实际值，其中**HANA_PASSWORD** 为步骤1的屏幕输出。

```
#*****************************************************************************
#Importnata note
#Please change this parameters according to your HANA system configuration!!!

HANA_USER="system"
HANA_PASSWORD="00000001000000010000000000000005000000010000000161b3258428fbdf
001000000000000080400000001000000001c9562ef9b7f838e984dc3d1080975be00000000000
INSTANCE_NUMBER="00"
DB_SID="WXJ"

#*****************************************************************************
```

也可以使用sed命令来直接进行修改：

sed -i 's/^HANA_USER=.*/HANA_USER="*XXX*"/' hana_freeze.sh hana_unfreeze.sh ，其中***XXX***为数据库用户名。

sed -i 's/^HANA_PASSWORD=.*/HANA_PASSWORD="*XXX*"/' hana_freeze.sh hana_unfreeze.sh ，其中***XXX***为步骤1中打印出的密码。

sed -i 's/^INSTANCE_NUMBER=.*/INSTANCE_NUMBER="*XXX*"/' hana_freeze.sh hana_unfreeze.sh ，其中*XXX*为数据库实例编号。

sed -i 's/^DB_SID=.*/DB_SID="*XXX*"/' hana_freeze.sh hana_unfreeze.sh ，其中*XXX*为数据库SID。

此操作会同时修改冻结解冻脚本，所以无需再执行**步骤3**。

步骤3 执行**vi hana_unfreeze.sh** ，打开HANA示例解冻脚本，修改此脚本中的用户名、密码、实例编号与SID

hana_freeze.sh与**hana_unfreeze.sh**脚本实现了基本的数据库冻结与解冻操作，如果您在冻结、解冻时有其它额外步骤需要执行，可以自行在其中进行修改。详细说明请参见 **通过自定义脚本实现其它Linux应用的一致性备份**

警告

冻结SAP HANA数据库时，按照SAP官方建议，需要冻结Data卷的XFS文件系统，否则可能出现数据不一致的问题。在此示例脚本中，将会查询出HANA使用的Data卷挂载点，并用xfs_freeze 命令进行冻结。

如果HANA系统未按照SAP官方建议使用一个独立分区来存放Data卷数据，而是与系统卷共用一个分区，则请修改**hana_freeze.sh**脚本，注释掉xfs_freeze相关行，防止整个系统都被冻结，但此时可能出现备份数据不一致的问题。

----结束

1.3 通过自定义脚本实现其它 Linux 应用的一致性备份

场景介绍

在Linux下，如果有其它应用需要一致性备份，可以编写自己的冻结、解冻脚本，来实现应用的保护。自定义脚本需放置在**/home/rdadmin/Agent/bin/thirdparty/ebk_user**目录中，供Agent在备份过程中调用。

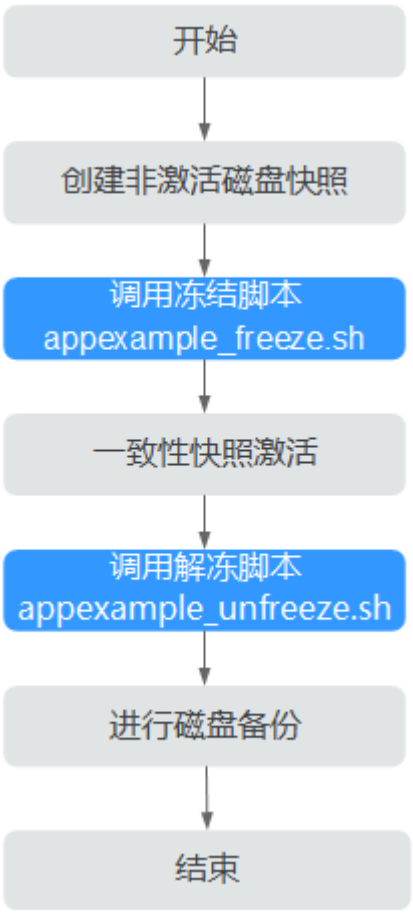
下面以一个虚构的应用appexample为例，来进行说明。

appexample是一款新的数据库，它对外提供了appexample -freeze与appexample -unfreeze两个命令来实现冻结与解冻。

用户需要开发自己的appexample_freeze.sh与appexample_unfreeze.sh脚本，供备份Agent调用以实现一致性备份。在备份过程中，会先调用appexample_freeze.sh脚本来冻结IO，冻结成功后，会进行磁盘的一致性快照激活，保证备份的数据是一致性的，最后再调用appexample_unfreeze.sh脚本解冻IO。

整体流程如**图1-1**所示：

图 1-1 数据库备份流程图



开发冻结脚本

appexample_freeze.sh示例如下：

```
#!/bin/sh
AGENT_ROOT_PATH=$1  #Agent程序调用脚本时，传入的的根目录，日志函数等会使用此变量，请不要改名
PID=$2 #Agent程序调用脚本时，传入的PID数字，用于结果的输出，请不要改名
. "${AGENT_ROOT_PATH}/bin/agent_func.sh"#引用脚本框架，提供了日志，加解密等功能
#结果处理函数，用于将结果写入到文件中，供脚本调用者获取返回值。
#入参 $1: 0表示成功，1表示失败
#无返回值
#RESULT_FILE在agent_func.sh中进行了定义
function ExitWithResult()
{
    Log "[INFO]:Freeze result is $1."
    echo $1 > ${RESULT_FILE}
    chmod 666 ${RESULT_FILE}
    exit $1
}
function Main()
{
    Log "********************************************************************"
    Log "[INFO]:Begin to freeze appexample."
    #查找appexample是否存在，如果appexample不存在，则返回0，退出
    #在冻结IO步骤中，Agent程序会依次调用每个冻结脚本，如果一个失败，总体就会失败。所以为了防止干扰其他程序的冻结过程，找不到appexample时，应返回0
    which appexample
    if [ $? -ne 0 ]
    then
            Log "[INFO]:appexample is not installed."
```



```
        ExitWithResult 0
    fi
    #调用实际的冻结命令
    appexample -freeze
    if [ $? -ne 0 ]
    then
        Log "[INFO]:appexample freeze failed."
        #冻结失败，记录结果并退出
        ExitWithResult 1
    fi
    Log "[INFO]:Freeze appexample success."
    #冻结成功，记录结果并退出
    ExitWithResult 0
}
Main
```

开发解冻脚本

appexample_unfreeze.sh示例如下：

```
#!/bin/sh
AGENT_ROOT_PATH=$1  #Agent程序调用脚本时，传入的的根目录，日志函数等会使用此变量，请不要改名
PID=$2 #Agent程序调用脚本时，传入的PID数字，用于结果的输出，请不要改名
. "${AGENT_ROOT_PATH}/bin/agent_func.sh"#引用脚本框架，提供了日志，加解密等功能
#结果处理函数，用于将结果写入到文件中，供脚本调用者获取返回值。
#入参 $1: 0表示成功，1表示失败
#无返回值
#RESULT_FILE在agent_func.sh中进行了定义
function ExitWithResult()
{
    Log "[INFO]:Freeze result is $1."
    echo $1 > ${RESULT_FILE}
    chmod 666 ${RESULT_FILE}
    exit $1
}
function Main()
{
    Log "*****************************************************************"
    Log "[INFO]:Begin to freeze appexample."
    #查找appexample是否存在，如果appexample不存在，则返回0，退出
    #在解冻IO步骤中，Agent程序会依次调用每个解冻脚本，如果一个失败，总体就会失败。所以为了防止干扰其他程序的解冻过程，找不到appexample时，应返回0
    which appexample
    if [ $? -ne 0 ]
    then
        Log "[INFO]:appexample is not installed."
        ExitWithResult 0
    fi
    #调用实际的解冻命令
    appexample -unfreeze
    if [ $? -ne 0 ]
    then
       Log "[INFO]:appexample freeze failed."
      #解冻失败，记录结果并退出
       ExitWithResult 1
    fi
    Log "[INFO]:Freeze appexample. success"
    #解冻成功，记录结果并退出
    ExitWithResult 0
}
Main
```

1.4 验证数据库备份结果

使用自定义脚本实现数据库备份完成后，可以通过如下操作验证数据库备份结果是否成功。

验证数据库备份结果（Linux）

下面以MY SQL数据库为例进行验证。

步骤1 登录MY SQL数据库，创建新的数据库。

步骤2 创建数据库成功后，创建存储过程，可以参考图1-2。

图 1-2 创建存储过程

```
DELIMITER //
CREATE DEFINER=`root`@`localhost` PROCEDURE `test_insert_xuwei3`()
BEGIN
declare i int;
declare v float;
set i = 0;
while i < 10000000
do
select RAND()*100 into v;
insert into xuwei1_test values(i, 'xxxxxx', now());
set i = i+1;
end while;
END
//
DELIMITER ;
```

步骤3 进入云服务器备份控制台，对目标弹性云服务器创建数据库备份，并勾选数据库备份。

步骤4 待备份完成后，进入/home/rdadmin/Agent/log/thirdparty.log，查看冻结、解冻日志，确定冻结解冻时间。

步骤5 使用新创建的数据库备份恢复目标弹性云服务器。恢复成功后，登录云服务器和数据库，查看表中最后一条插入数据对应的时间。

步骤6 对比步骤5日志显示的VSS冻结成功时间和步骤4的时间。冻结成功之前会停止插入数据，所以步骤5的时间比步骤4早。若步骤5的时间比步骤4早，则表示应用一致性备份成功。

----结束

验证数据库备份结果（Windows）

下面以SQL_SERVER数据库为例进行验证。

步骤1 登录SQL_SERVER数据库，创建新的数据库。

步骤2 创建数据库成功后，创建存储过程，可以参考图1-3。

图 1-3 创建存储过程

```
use test;
CREATE TABLE student
(
id int,
name varchar(100),
shijian datetime
)
DECLARE @id1 INT,@name1 varchar(100)
SET @id1=1
SET @name1='zhangsan'
WHILE @id1<10000000000
BEGIN
INSERT INTO student VALUES(@id1, @name1,GETDATE())
SET @id1=@id1+1
END
```

步骤3 进入云备份控制台，对目标弹性云服务器创建数据库备份，并勾选数据库备份。

步骤4 待备份完成后，进入Cloud Server Backup Agent-WIN64\log\ rdagent.txt文件，查看冻结、解冻日志，确定冻结解冻时间。如图中所示的17:28:51。

图 1-4 查看日志

```
[2018-11-14 17:28:46][0x0000531600001536][2052][SYSTEM][INFO][Requester.cpp,1369]Start snap shot set.
[2018-11-14 17:28:46][0x0000531600001536][2052][SYSTEM][INFO][Requester.cpp,1372]Add to snapshot set.
[2018-11-14 17:28:46][0x0000531600001536][2052][SYSTEM][INFO][Requester.cpp,1375]Prepare for backup.
[2018-11-14 17:28:46][0x0000531600001535][2052][SYSTEM][INFO][Requester.cpp,1261]Begin prepare for backup.
[2018-11-14 17:28:46][0x0000531600001535][2052][SYSTEM][INFO][Requester.cpp,1272]Prepare for backup succ.
[2018-11-14 17:28:46][0x0000531600001536][2052][SYSTEM][INFO][Requester.cpp,1378]Do snapshot set.
[2018-11-14 17:28:46][0x0000531600001535][2052][SYSTEM][INFO][Requester.cpp,1278]Begin create the shadow (Do SnapShot Set).
[2018-11-14 17:28:51][0x0000531600001535][2052][SYSTEM][INFO][Requester.cpp,1317]Create the shadow (Do SnapShot Set) succ.
[2018-11-14 17:28:51][0x0000531600001536][2052][SYSTEM][INFO][Requester.cpp,227]Freeze volume succ.
[2018-11-14 17:28:51][0x0000531600001536][2052][SYSTEM][INFO][Requester.cpp,180]Freeze file sys, succ.
[2018-11-14 17:28:51][0x0000531600001536][2052][SYSTEM][INFO][App.cpp,383]Vss freeze success.
[2018-11-14 17:28:51][0x0000531600001536][2052][SYSTEM][INFO][AppPlugin.cpp,157]Freeze app succ.
[2018-11-14 17:28:51][0x0000531600001536][4872][SYSTEM][INFO][MessageProcess.cpp,1034]Json key "loop_time" does not exist.
[2018-11-14 17:28:51][0x0000531600001536][4872][SYSTEM][INFO][FTExceptionHandle.cpp,849]Update monitor obj freeze begin time
[2018-11-14 17:28:52][0x0000531600001536][544][SYSTEM][INFO][Communication.cpp,400]End accept fcgx
[2018-11-14 17:28:52][0x0000531600001536][544][SYSTEM][INFO][Authentication.cpp,104]strClientCertDN: CN=BCManager eBackup Cl
[2018-11-14 17:28:52][0x0000531600001536][544][SYSTEM][INFO][Authentication.cpp,130]Client IP address 100.125.1.142 Auth suc
[2018-11-14 17:28:52][0x0000531600001536][544][SYSTEM][INFO][Communication.cpp,390]Begin accept fcgx
[2018-11-14 17:28:53][0x0000531600001536][2052][SYSTEM][INFO][AppPlugin.cpp,168]Begin unfreeze app.
[2018-11-14 17:28:53][0x0000531600001536][2052][SYSTEM][INFO][App.cpp,392]Begin vss unfreeze.
[2018-11-14 17:28:53][0x0000531600001536][2052][SYSTEM][INFO][Requester.cpp,275]Begin unfreeze all.
[2018-11-14 17:28:53][0x0000531600001536][2052][SYSTEM][INFO][Requester.cpp,1703]Begin wait for async ex.
[2018-11-14 17:28:53][0x0000531600001536][2052][SYSTEM][INFO][Requester.cpp,1733]End wait for async ex, return 0x0004230a (V
[2018-11-14 17:28:53][0x0000531600001536][2052][SYSTEM][INFO][Requester.cpp,1579]VSS async finished.
[2018-11-14 17:28:53][0x0000531600001536][2052][SYSTEM][INFO][Requester.cpp,303]End unfreeze all.
[2018-11-14 17:28:53][0x0000531600001536][2052][SYSTEM][INFO][App.cpp,415]VSS unfreeze success.
[2018-11-14 17:28:53][0x0000531600001536][2052][SYSTEM][INFO][App.cpp,424]Begin vss endbakup.
[2018-11-14 17:28:53][0x0000531600001536][2052][SYSTEM][INFO][Requester.cpp,311]Begin end bakcup.
[2018-11-14 17:29:05][0x0000531600001536][2052][SYSTEM][INFO][Requester.cpp,333]End end backup.
[2018-11-14 17:29:05][0x0000531600001536][2052][SYSTEM][INFO][App.cpp,445]Vss endbakup success.
[2018-11-14 17:29:05][0x0000531600001536][2052][SYSTEM][INFO][App.cpp,342]Unfreeze all apps success.
[2018-11-14 17:29:05][0x0000531600001536][2052][SYSTEM][INFO][AppPlugin.cpp,185]Unfreeze app succ.
[2018-11-14 17:29:05][0x0000531600001536][4872][SYSTEM][INFO][MessageProcess.cpp,1034]Json key "loop_time" does not exist.
```

步骤5 使用新创建的数据库备份恢复目标弹性云服务器。恢复成功后，登录云服务器和数据库，查看表中最后一条插入数据对应的时间(17:28:49)的记录。

步骤6 对比**步骤5**日志显示的VSS冻结成功时间和**步骤4**的时间。冻结成功之前会停止插入数据，所以**步骤5**的时间比**步骤4**早。若**步骤5**的时间比**步骤4**早，则表示应用一致性备份成功。

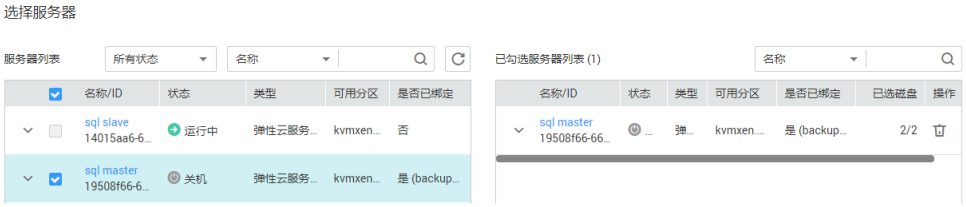
----结束

1.5 保护 SQL Server

保护 Failover Cluster 模式下的 SQL Server

当前云服务器备份只支持单个虚拟机的一致性备份，对于集群数据库暂不支持，完整支持将在后续版本中推出。

在Failover Cluster模式下，SQL Server服务只在主节点上是启动的，故在创建云服务器备份时，只需要将主节点加入策略进行备份。在主备发生切换后，及时调整策略，确保始终对主节点进行备份。在恢复时，请先停止所有备节点，然后还原主节点。



保护 Always on Availability Groups 模式下的 SQL Server

当前云服务器备份只支持单个虚拟机的一致性备份，对于集群数据库暂不支持，完整支持将在后续版本中推出。

在Always On模式下，SQL Server服务在主备节点上都是启动的，数据由主复制到备，主上拥有全部的数据。故在创建云服务器备份时，只需要将主节点加入策略进行备份。在主备发生切换后，及时调整策略，确保始终对主节点进行备份。

由于SQL Server自身的机制，在恢复主时，可能会触发同步，使备节点上的数据也被覆盖，导致备份时刻之后新产生的数据丢失，所以建议只有在主备节点均不可用时才进行整机恢复，防止非预期的数据丢失。

1.6 自定义脚本问题定位方法

如果自定义脚本存在缺陷，可能导致数据库备份失败，此时可以打开**/home/rdadmin/Agent/log/thirdparty.log**，查看日志进行定位。

图1-5为一个冻结MySQL数据库失败时的日志样例

图 1-5 日志示例

```
18-09-13--22:30:10:[30243][root] ************************************************************
18-09-13--22:30:10:[30243][root] [INFO]:Begin to freeze mysql.
Id  User    Host    db  Command Time    State   Info
20  root    localhost   test123 Sleep   1063        NULL
21  root    localhost   test123 Sleep   1066        NULL
24  root    localhost   NULL    Query   23  User sleep  select 1 and sleep(60)
27  root    localhost   NULL    Query   0   NULL    show processlist
18-09-13--22:30:10:[30243][root] [ERROR]:MySQL already been freezed
18-09-13--22:30:10:[30243][root] [INFO]:mysql freeze result is 1.
18-09-14--10:07:54:[7162][root] ************************************************************
```

第一列 **18-09-13--22:30:10** 为日志记录时间

第二列 **[30243]** 为脚本的PID编号

第三列 **[root]** 为脚本的执行用户

第四列 **[INFO]** 或 **[ERROR]** 为日志级别

一般脚本调用失败时，打开日志文件，找到相应时间点的ERROR即可初步确定问题原因。例如**图1-5**中的错误就是因为MySQL已经处于冻结状态，再次冻结，就会出错。

2 通过数据备份开展定期恢复演练

背景

根据数据安全法，需要对数据容灾备份**定期开展数据恢复测试**。恢复是指利用备份软件把所备份的数据内容恢复到数据源。由于业务系统日常运行过程中，经常无法直接在所备份的服务器进行真实环境恢复操作。但为了验证备份数据的可用性、备份方案完整性和可靠性以及应对未来系统突发事件发生，可以通过备份新建资源的方式来对备份介质以及备份方案进行检验，来确保备份的可恢复验证。

演练原则

- 参考“通过业务分级制定最佳备份策略”**灾备策略**里的演练频率，有计划、周期性地对备份数据进行恢复演练。
- 以备份资源为单位在该资源的所有备份内抽样随机进行，不必每个备份都进行，但要保证在一定期限内每种资源的每类备份至少有一次备份被恢复验证过。
- 为防止干扰实际业务，恢复演练以使用备份创建新资源实例进行，禁止直接恢复源实例。
- 下发备份恢复任务后，恢复任务成功，备份能够正常恢复资源，且恢复的数据与原来一致，正确性与预期匹配，则视为恢复成功。
- 下发备份恢复任务后，如果恢复任务失败，或者恢复任务成功，但数据存在丢失、无法读取的情况，则视为恢复失败，请及时联系华为云工程师进行定位处理。
- 操作员应详细记录演练的周期、过程及结果。

资源与成本

表 2-1 资源和成本规划

资源	资源说明	数量	每月费用
云服务器备份存储库	存储库容量大于等于所需要备份云服务器资源的容量总和	1	具体的计费方式及标准请参考**计费说明**。

SFS Turbo备份存储库	存储库容量大于等于所需要备份SFS Turbo资源的容量	1	
弹性云服务器	与待演练服务器的配置相同	1	
SFS Turbo文件系统	与待演练的SFS Turbo文件系统大小相同	1	
RDS数据库实例	与待演练的RDS数据库配置相同	1	

备份演练

三种备份类型的备份演练操作流程如下：

云服务器备份演练

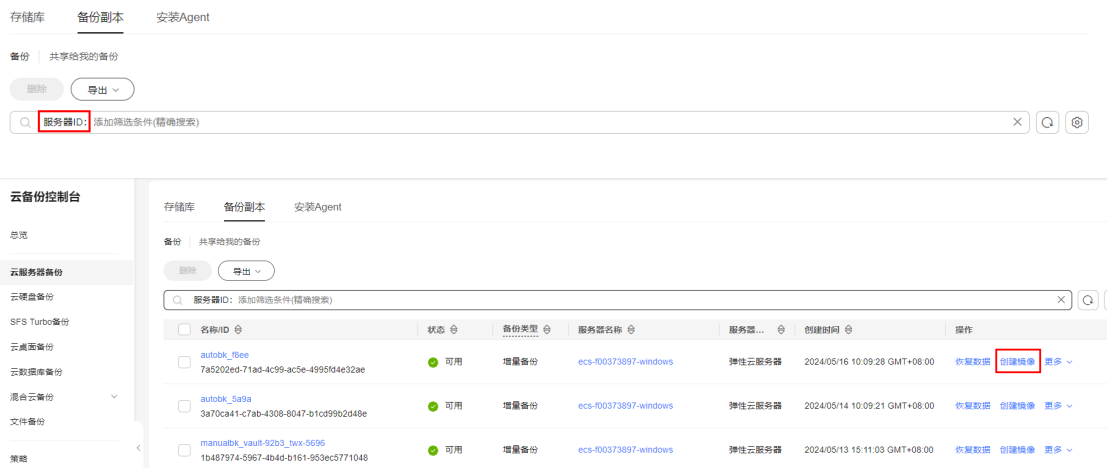
步骤1 以核心系统的某个云服务器为例，每月进行备份恢复演练任务。

步骤2 登录云备份管理控制台。

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域。
3. 单击“”，选择“存储 > 云备份”。

步骤3 选择“云服务器备份”页签，选择“备份副本”。

步骤4 获取该云服务器的备份列表：选择“服务器ID”，输入需要验证的云服务器ID，单击“搜索”。



步骤5 选择任意一个备份副本，单击“创建镜像”，进入IMS创建私有镜像界面，输入镜像名称后，单击“确定”。

步骤6 待镜像创建完成后，使用该镜像申请云服务器。

步骤7 将新创建的云服务器与当前云服务器进行对比，查看数据是否一致，符合预期，观察业务是否正常。

----结束

云文件系统备份演练

步骤1 以核心系统的某个云文件系统为例，每月进行备份恢复演练任务。

步骤2 登录云备份管理控制台。

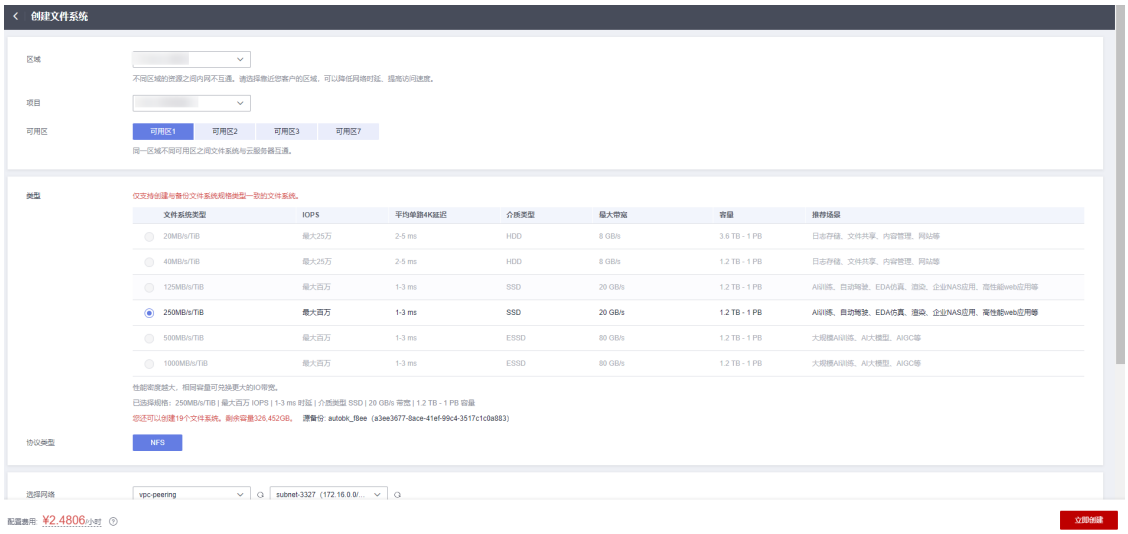
1. **登录管理控制台**。
2. 单击管理控制台左上角的，选择区域。
3. 单击“ ”，选择“存储 > 云备份”。

步骤3 选择“SFS Turbo备份”签页，选择“备份副本”。

步骤4 获取该云文件系统的备份列表：选择“文件系统ID”，输入需要验证的文件系统ID，单击“搜索”。

步骤5 选择需要恢复的备份，单击“创建文件系统”，并跳转到文件系统创建页。

步骤6 选择云文件系统创建参数，确认提交，完成创建新的文件系统。



步骤7 查看比对新创建的云文件系统数据，校验数据是否符合预期。

----结束

云数据库备份演练

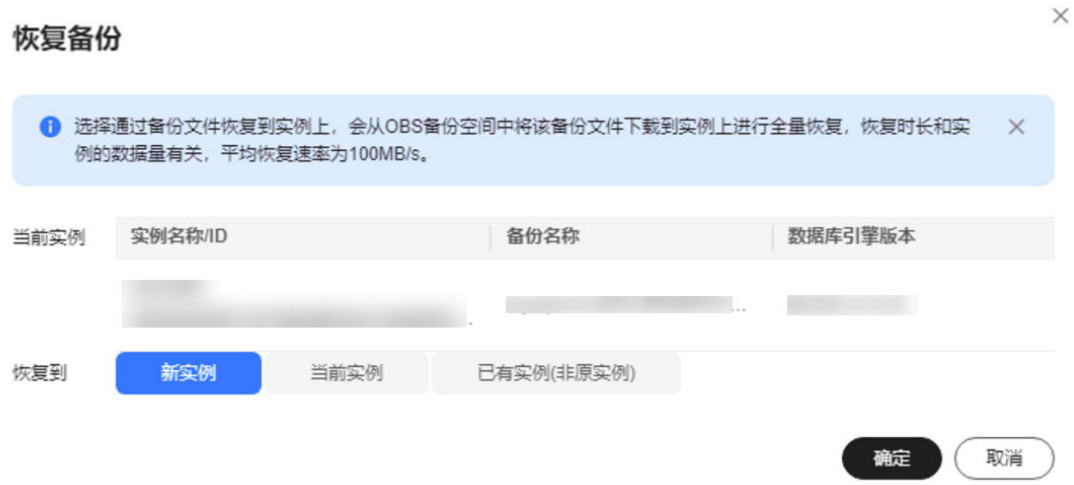
步骤1 登录云备份管理控制台。

1. **登录管理控制台**。
2. 单击管理控制台左上角的 ，选择区域。

3. 单击“ ☰ ”，选择“数据库 > 云数据库 RDS”。

步骤2 单击“备份管理”，选择需要恢复的备份，单击操作列的“恢复”。

步骤3 选择恢复到“新实例”，单击“确定”，进入“恢复到新实例”的服务选型页面。



步骤4 新实例的数据库引擎和数据库版本，自动与原实例相同。存储空间大小默认和原实例相同，且必须大于或等于原实例存储空间大小。其余参数详情可参考**帮助指导**。

步骤5 单击“立即购买”，按照指导购买新数据库，等待数据库实例状态由“创建中”变为“正常”，说明恢复成功。

步骤6 恢复成功后登录数据库实例进行验证，校验数据是否匹配预期。

----结束

3 通过业务分级制定最佳备份策略

背景

资源的备份策略决定了备份周期与保留规则，实践中需要根据数据的重要程度、用户云上部署的业务系统的不同分级，配置不同的数据备份策略。

资源与成本规划

表 3-1 资源和成本规划

资源	资源说明	数量	每月费用
备份存储库	创建备份策略后，需要绑定备份存储库，以实现按照创建的备份策略进行定时备份	1	具体的计费方式及标准请参考**计费说明**。

业务分级

同时结合业务实际，按照业务系统重要性及业务系统中断对整个公司业务影响的范围和程度，可考虑将业务系统分为三类：

- **核心系统**
  a. 支撑公司核心业务流程，一旦停止服务会给公司运营造成重大影响或重大财务损失，如购买系统；
  b. 支撑公司关键应用的重要基础设施和办公系统，一旦中断，导致大量员工正常工作瘫痪。
- **重要系统**
  a. 支撑公司重要的业务流程，一旦停止服务会给公司业务运营造成严重影响，或造成严重财务损失；
  b. 支撑公司重要应用的基础设施和办公系统，一旦中断，会严重影响员工的正常办公。
- **一般系统**
  a. 支撑公司业务流程，一旦停止服务对公司运营或财务造成损失，如培训系统；

b. 支撑公司普通应用的基础设施或办公系统，一旦中断，会影响员工的正常办公。

一般情况下，可根据业务系统影响评估数据等级，核心数据对应于核心系统，重要系统对应于重要数据，一般系统对应一般数据。如有数据分类与业务系统类别不匹配的情况，则业务系统向更高级别系统定级。例如业务系统被评估为重要系统，但是数据类型属于数据安全法的核心数据，则该系统向上一级定义为核心系统。

灾备策略

按照用户云上部署的业务系统的不同分级，建议配置不同的数据备份策略，针对常见的云内资源采用如下数据备份策略，该策略可根据实际业务情况自行调整。参照策略管理章节**创建备份策略**。

系统分类	备份对象	RPO	保留时间	全量备份	增量备份	异地备份	演练频率
核心系统	云服务器	4h	1年以上	每周	6次/日	是	月
	云数据库	4h	1年以上	每周	6次/日	是	月
	云文件系统	4h	1年以上	每周	6次/日	是	月
重要系统	云服务器	12h	1年	双周	2次/日	是	季度
	云数据库	12h	1年	双周	2次/日	是	季度
	云文件系统	12h	1年	双周	2次/日	是	季度
一般系统	云服务器	24h	6个月	每月	1次/日	否	半年
	云数据库	24h	6个月	每月	1次/日	否	半年
	云文件系统	24h	6个月	每月	1次/日	否	半年

4 通过 CBR+HSS 搭建云上备份防勒索系统

应用场景

勒索病毒，也称为勒索软件，是一种特殊的恶意软件，与其他病毒最大的不同在于攻击手段伴随着有组织的网络威胁攻击和加密数据后勒索赎金。

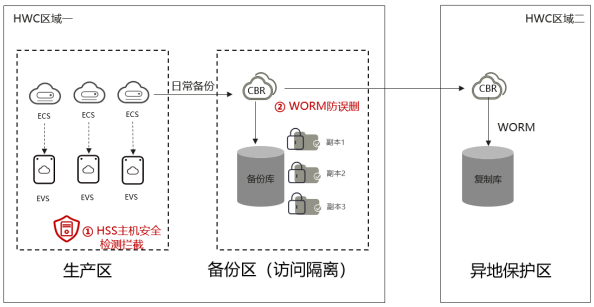
勒索病毒已成为全球主要网络威胁，严重影响着数字经济的发展，而面对勒索病毒的侵害，大多数企业并没有全面和有效的方法予以应对。不得不通过支付高额的赎金来请求黑客对加密的数据进行解锁。而在企业遭受到攻击的同时，会造成企业的重要数据丢失、企业停工停产、合同违约、商誉减值、企业管理者离职以及众多不可预计的后果。

华为云备份防勒索解决方案与主机安全服务HSS结合，为客户提供有效云上防勒索解决方案，满足客户对数据安全保护的需求。

方案架构

云备份所提供的防勒索解决方案服务，从业务实际出发，以客户数据安全要求为导向，帮助客户搭建一个安全可靠的备份防勒索系统，满足客户对于勒索病毒防护的需求，保护数据资产，尽可能减小损失。通过存储库天然具备的访问隔离属性、WORM等特性，实现当云服务器发生勒索攻击时，能提供至少一份干净可用、不被篡改的数据用于安全恢复，提升数据安全的韧性能力，满足客户对于勒索病毒防护的需求。

图 4-1 基于 HSS+CBR 的云上备份防勒索解决方案



方案优势

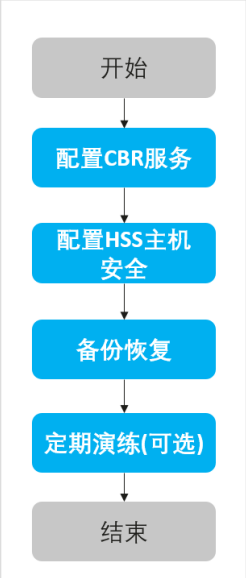
- HSS主机安全服务与CBR云备份服务联动，当HSS检测到病毒入侵后立即触发CBR备份，有效减小数据损失；

- CBR备份存储库天然具备隔离属性，结合WORM能力，实现本地备份的防篡改防误删；
- 将CBR备份复制到其他区域，结合WORM能力，实现异地备份的防篡改防误删。

操作流程

本章节介绍云备份防勒索解决方案的操作流程如图4-2所示。

图 4-2 云上备份防勒索方案操作流程



配置 CBR 备份并开启备份锁定

购买云服务器备份存储库

备份存储库是CBR服务的基本单元，使用CBR服务前必须要先购买备份存储库。如果使用量超过购买的容量后将不能再进行备份，因此购买存储库时建议购买自动扩容存储库，避免因为容量问题导致备份失败。

步骤1 登录云备份管理控制台。

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域。
3. 单击“ ”，选择“存储 > 云备份 CBR”。选择对应的备份目录。

步骤2 在界面右上角单击“购买云服务器备份存储库”。

步骤3 选择计费模式。

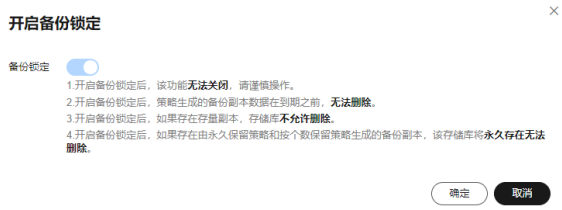
- 包年包月是预付费模式，按订单的购买周期计费，适用于可预估资源使用周期的场景，价格比按需计费模式更优惠。
- 按需计费是后付费模式，根据实际使用量进行计费，可以随时购买或删除存储库。费用直接从账户余额中扣除。

说明

如果选择的是按需计费的存储库，则自动扩容建议选择“立即配置”，避免因为容量问题导致备份失败。

步骤4 选择是否启用备份锁定，也可以后续选择开启。

开启备份锁定后，可以避免备份被误删除或者恶意删除，提升数据安全性。



须知

- 开启备份锁定后，该功能无法关闭，策略生成的备份只支持过期自动删除，存在存量副本的存储库不允许删除。手动创建的备份不受备份锁定的约束，支持手动删除。
- 请详细阅读说明并确认是否开启，建议开启。
- 在购买存储库时若没有选择启用备份锁定，可以在任一备份页面，找到目标存储库，单击存储库所在列的“更多 > 开启备份锁定”，在备份锁定弹框中，打开备份锁定开关。更多详细内容请参见**开启备份锁定**。

步骤5 其余选项按需配置，具体操作可参见**购买云服务器备份存储库**。

存储库购买完成后，可以进行备份策略或复制策略的创建、修改、删除、绑定至存储库等操作。具体操作请参照**策略管理**章节。

----结束

配置 HSS 主机安全

本最佳实践方案需要使用到HSS主机安全服务，详情请参考**HSS防勒索最佳实践**。

备份恢复

当遭受勒索病毒攻击后，当前尚无有效工具能够破解勒索病毒，唯一的方案只能通过备份快速恢复数据。通过备份恢复云服务器时，首先判断该备份是否已被勒索病毒感染，如果备份正常，则参考**使用云服务器备份恢复数据**；如果备份为勒索加密备份，则建议的备份恢复操作如下：

步骤1 用**IAM管理员账号登录管理控制台**。

步骤2 单击管理控制台左上角的 ，选择区域。

步骤3 在控制台的左侧导航窗格中选择“计算 > 弹性云服务器 ECS”，进入弹性云服务器界面。

步骤4 按照**购买ECS**在**独立的VPC内**购买弹性云服务器。

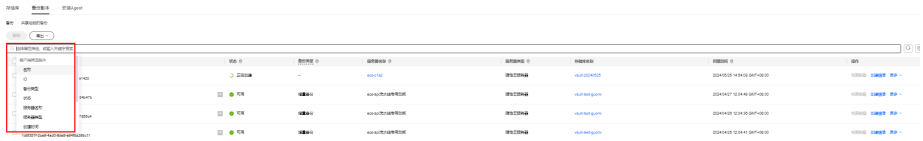
说明

此处使用独立VPC，防止勒索病毒在干净区域内感染。

步骤5 在IAM控制台的左侧导航窗格中选择“存储 > 云备份 CBR”，进入云备份服务界面。

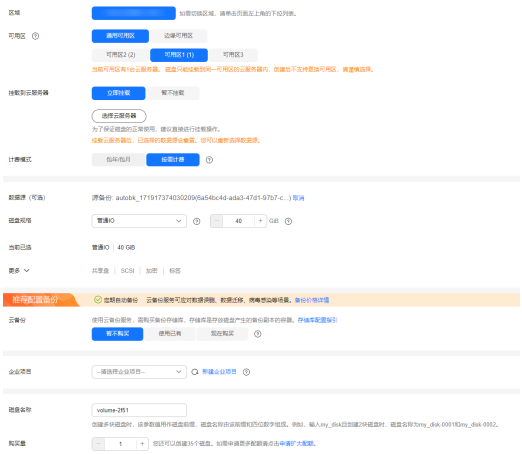
步骤6 在左侧导航栏单击“云服务器备份 > 备份副本”，在备份列表上方，可以通过备份名称、存储库ID、服务器名称、服务器ID等条件搜索，搜索需要恢复的云服务器备份。

图 4-3 筛选备份



步骤7 单击选中的云服务器备份，进入详情页后，单击“磁盘级备份”。

步骤8 单击“创建磁盘”，进入到“购买磁盘”界面，按需创建磁盘。



步骤9 待磁盘创建成功后，将磁盘挂载到**步骤4**创建的虚拟机上，登录虚拟机查看磁盘下的数据是否正常。

步骤10 步骤9中正常的未加密的数据，可以通过对象存储obsutil工具上传到对象存储桶里。

在OBS**管理控制台**左侧导航栏选择“桶列表”，在页面右上角单击“创建桶”，系统弹出如下所示的页面，创建临时桶ransomware_anti_bucket_tmp，用于临时保存数据。具体操作可参见**创建桶**。

图 4-4 创建桶

步骤11 在控制台的左侧导航窗格中选择“管理与监管 > 统一身份认证服务 IAM”，进入统一身份认证服务界面。

步骤12 单击“权限管理 > 权限 > 创建自定义策略”，策略名称填写ransomware_anti_access，策略配置方式选择json视图，填写权限如下：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:object:GetObject",
                "obs:bucket:HeadBucket",
                "obs:object:GetObjectAcl",
                "obs:object:PutObject"
            ],
            "Resource": [
                "OBS:*:*:object:*",
                "OBS:*:*:bucket:ransomware_anti_bucket_tmp"
            ]
        }
    ]
}
```

单击“确定”。

步骤13 单击“用户组 > 创建用户组”，输入用户组名“ransomware_anti_group”,单击确定后，在该用户组的操作栏里单击“授权”，选择策略“ransomware_anti_access”后，确定。

步骤14 单击“创建用户”，输入用户名ransomware_anti_user，访问方式选择“编程访问”，凭证类型选择“访问密钥”，单击“下一步”，选择用户组“ransomware_anti_group”后，“创建用户”创建子用户。

步骤15 创建成功后，获取用户的AK/SK信息，参考**obsutil上传对象**，将文件上传到临时桶里后，下载即可。

步骤16 文件传输完成后，删除虚拟机，删除临时用户、权限组和临时桶。

----结束

周期性演练（可选）

根据数据安全法，需要对数据容灾备份**定期开展数据恢复测试**。恢复是指利用备份软件把所备份的数据内容恢复到数据源。由于业务系统日常运行过程中，经常无法直接在所备份的服务器进行真实环境恢复操作。但为了验证备份数据的可用性以及备份方案完整性、可靠性以及应对未来系统突发事件发生，可以通过备份新建资源的方式来对备份介质以及备份方案进行检验，来确保备份的可恢复验证。

通过数据备份可开展定期恢复演练，具体步骤可参见**云服务器备份演练**。

5 CBR 安全最佳实践

安全性是华为云与您的共同责任。华为云负责云服务自身的安全，提供安全的云；作为租户，您需要合理使用云服务提供的安全能力对数据进行保护，安全地使用云。详情请参见**责任共担**。

本文提供了CBR使用过程中的安全最佳实践，旨在为提高整体安全能力提供可操作的规范性指导。根据该指导文档您可以持续评估CBR资源的安全状态，更好地组合使用CBR提供的多种安全能力。

本文从以下几个维度给出建议，您可以评估CBR使用情况，并根据业务需要在本指导的基础上进行安全配置。

建议妥善管理认证凭证，减小因凭证泄漏导致的数据泄露风险

建议对AK/SK进行定期凭证轮转，同时加密存储，避免凭证长期使用过程中预置的明文凭证泄露导致数据泄露。详情请参见**CBR的认证鉴权**。

正确使用访问控制能力，确保备份数据不泄露或不被误删

- 建议根据CBR常用操作与系统权限的授权关系，对IAM用户设置最小权限，避免由于IAM用户权限过大导致备份数据泄露或被误删。详情请参见**CBR的权限管理**。
- CBR支持敏感操作保护，开启后执行删除备份等敏感操作时，系统会进行身份验证，进一步保证云备份配置和数据的安全性。详情请参见**敏感操作**。

正确使用 CBR 提供的数据保护能力对备份数据进行保护

- 备份数据加密：当备份的目标磁盘为加密磁盘时，如果磁盘启用备份加密，则备份数据会加密存储。当用户执行备份恢复时，存储的加密数据会先解密之后再恢复到目标磁盘。
- 跨区域复制：跨区域复制是指通过创建复制策略，将一个区域的备份自动、异步的复制到不同区域的另外一个存储库。跨区域复制能够为用户提供备份数据的跨区域容灾能力，满足用户备份数据复制到异地进行存储的需求。
- 备份锁定：备份锁定功能是指将备份数据置为WORM（一次写入，多次读取）状态。开启该功能后，存储库中的所有备份都将进入WORM状态。处于WORM状态的备份数据，任何用户都不能提前删除。

利用操作日志审计是否存在异常数据访问操作

- 开启云审计服务记录CTS的所有访问操作便于事后审查

  云审计服务（Cloud Trace Service，CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

  开通云审计服务并创建和配置追踪器后，CTS可记录CBR的管理事件和数据事件用于审计。详情请参见**审计与日志**。

- 使用云监控服务对安全事件进行实时监控、告警

  云监控（Cloud Eye， CES）为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。使您全面了解华为云上的资源使用情况、业务的运行状况，并及时收到异常报警做出反应，保证业务顺畅运行。

  开通云监控服务，CES帮助用户监控账号下的存储库和备份情况，详情请参见**审计与日志**。

6 备份指标概览

云备份不同备份之间的最小备份粒度、最小备份间隔、最长保留时间等功能指标有所不同。本文介绍云备份中云内备份各数据源支持的备份指标。

备份指标

表 6-1 备份指标概览

数据源	最小备份粒度	最小备份时间间隔	最长保留时间	跨region复制	备份共享	细粒度授权
云服务器	云服务器	小时	永久	支持	支持	支持
云硬盘	云硬盘	小时	永久	不支持	支持	支持
SFS Turbo	SFS Turbo	小时	永久	支持	不支持	支持
RDS	实例	小时	732天	不支持	不支持	支持
云桌面	云桌面	小时	永久	不支持	不支持	支持

您可以根据业务需求为不同的账号或IAM用户授予备份、恢复的权限。请参见**创建用户并授权使用CBR**。

7 为用户设置禁止删除备份和恢复操作的权限

为保障业务和数据安全，您可以通过统一身份认证服务IAM的策略限定用户对云备份的某些特定行为的操作权限，防止用户误操作导致的数据丢失风险产生。本文介绍如何为用户配置禁止删除备份和禁止恢复操作的权限。

应用场景

企业A购买了ECS实例部署业务，同时为这些ECS实例设定了每日22:00执行备份任务的备份策略。为了确保其业务和数据安全，企业希望运维人员不能随意对ECS实例进行删除备份和数据恢复操作。

根据以上场景，企业可以根据需求创建自定义策略，然后为IAM用户授予对应的权限，从而保证IAM用户只能进行删除备份或恢复外的操作。

步骤一：创建自定义策略

步骤1 管理员登录IAM控制台。

步骤2 在统一身份认证服务，左侧导航窗格中，选择“权限管理>权限”页签，单击右上方的“创建自定义策略”。

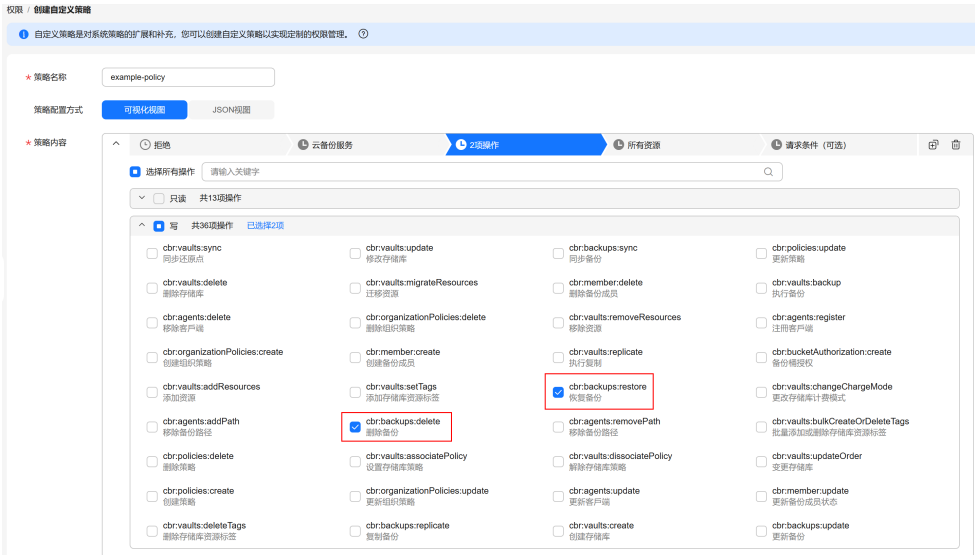
图 7-1 创建自定义策略

步骤3 输入“策略名称”，以“example-policy”为例。

步骤4 “策略配置方式”选择“可视化视图”。

步骤5 在“策略内容”下配置策略。

图 7-2 配置策略



步骤6 （可选）“策略配置方式”选择“可视化视图”。在“策略内容”下配置策略。

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cbr:backups:restore",
        "cbr:backups:delete"
      ]
    }
  ]
}
```

步骤7 （可选）输入“策略描述”。

步骤8 单击“确定”。

----结束

步骤二：创建 IAM 用户组

步骤1 在统一身份认证服务，左侧导航窗格中，单击“用户组”>“创建用户组”。

图 7-3 创建用户组

步骤2 在“创建用户组”界面，输入“用户组名称”为“运维人员组”。

用户组名称只能包含中文、大小写字母、数字、空格或特殊字符(-_)。

图 7-4 输入用户组信息

步骤3 单击“确定”，完成用户组创建。

返回用户组列表，创建成功的用户组“运维人员组”将会展示在用户组列表中。

----结束

步骤三：为 IAM 用户组授权

步骤1 在统一身份认证服务，左侧导航窗格中，单击“用户组”。

步骤2 在用户组列表中，单击新建用户组“运维人员组”右侧的“授权”。

图 7-5 授权

步骤3 在用户组选择策略页面中，勾选步骤一创建的策略“example-policy”。单击“下一步”。

图 7-6 选择权限

步骤4 选择权限的作用范围。系统会根据您所选择的策略，自动推荐授权范围方案，便于为用户选择合适的授权作用范围，表1为IAM提供的所有授权范围方案。

表 7-1 授权范围方案

可选方案	方案说明
所有资源	授权后，IAM用户可以根据权限使用账号中所有资源，包括企业项目、区域项目和全局服务资源。
指定企业项目资源	选择指定企业项目，IAM用户可以根据权限使用该企业项目中的资源。**仅开通企业项目后可选。** 如果您暂未开通企业项目，将不支持基于企业项目授权，了解企业项目请参考：**什么是企业项目管理**。如需开通，请参考：**开通企业项目**。
指定区域项目资源	选择指定区域项目，IAM用户可以根据权限使用该区域项目中的资源。 如果选择作用范围为“区域项目”，且所勾选的策略包含全局服务权限，系统自动将全局服务权限的作用范围设置为**所有资源**，勾选的区域项目权限的作用范围仍为指定区域项目。 **说明** 不支持选择专属云DEC的区域项目。

步骤5 单击“确定”，完成用户组授权。

----结束

步骤四：将 IAM 用户加入运维人员组

步骤1 在统一身份认证服务，左侧导航窗格中，单击“用户组”。

步骤2 在用户组列表中，单击新建用户组“运维人员组”的名称，进入用户组详情页。

步骤3 选择“用户管理”页签。单击“添加”。

图 7-7 添加用户

步骤4 勾选需要加入的用户，单击“确定”。已添加的用户将会出现在用户列表中。

----结束

步骤五：IAM 用户登录控制台

步骤1 IAM用户在“IAM用户登录”页面，输入**“租户名/原华为云账号名”**、**“IAM用户名/邮件地址”**和**“IAM用户密码”**。

图 7-8 IAM 用户登录

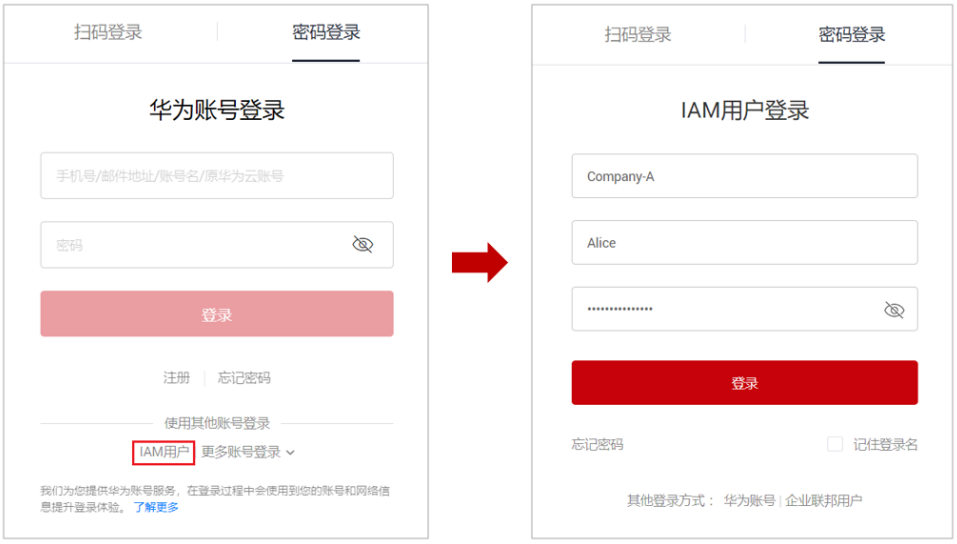


表 7-2 登录信息

参数	说明
租户名/原华为云账号名	IAM用户所属的账号。此处假设A公司的账号名为“Company-A”。
IAM用户名/邮件地址	在IAM创建用户时，输入的IAM用户名/邮件地址。如果不知道IAM用户名及初始密码，请向管理员获取。此处假设运维人员的IAM用户名为“Alice”。
IAM用户密码	IAM用户的密码，非账号密码。

步骤2 单击“登录”，IAM用户登录华为云。

步骤3 进入云备份控制台，对备份进行删除操作，如无法执行该操作，表示策略生效。

----结束

