虚谷数据库 V12.6

审计管理指南

文档版本 01

发布日期 2024-10-08

虚谷数据库
XUGU DB

成都虚谷伟业科技有限公司

地址：四川省成都市锦江区锦盛路 138 号佳霖科创大厦 5 楼 3-14 号

邮编：610023

网址：www.xugudb.com

前言

概述

本文档主要介绍了虚谷数据库的审计管理信息。

读者对象

数据库管理员

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
⚠ 注意	用于传递设备或环境安全警示信息，若不避免，可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。
🕮 说明	对正文中重点信息的补充说明。“说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

修改记录

文档版本	发布日期	修改说明
01	2024-10-08	第一次发布

目录

1 审计概述

1.1 概述

数据库审计是对数据库访问操作进行监管的行为，一般可以采用以下两种模式。

- 旁路部署审计监管系统。此方式通过镜像或探针采集所有数据库的访问流量，并基于 SQL 语法、语义的解析技术，记录下所有访问和操作数据库的行为的详细信息；例如，访问数据的用户（IP、账号、访问时间），操作（增、删、改、查），对象（表、字段）等。
- 数据库管理系统安全管理体系提供审计机制。针对数据库操作事件提供事后审计监督功能，记录不同的数据库操作使用行为。用户通过查找、分析、跟踪审计记录日志或系统表中的审计信息，可以查看个别用户对数据库系统的访问及操作行为，便于发现问题，从而采取积极、有效的控制措施。

数据库审计的主要价值有两点：

- 在发生数据库安全事件（例如数据篡改、泄露）后为事件的追责定责提供依据。
- 针对数据库操作的风险行为进行时时告警。

虚谷数据库审计提供数据库内部审计机制，通过定义系统级、语句级、对象级不同级别的审计条件，审计记录用户对虚谷数据库的操作行为。用户可通过审计结果记录表查看、分析、过滤审计行为，积极采取安全防控措施，也可制定数据库操作行为规则，结合监控、告警系统提供高风险操作实施告警，加强系统防范。

表 1-1 审计术语说明

审计术语	说明
审计管理员（SYSAUDITOR）	虚谷数据库审计权限管理员，拥有设置和取消数据库对象的审计策略最高权限，可查看和分析数据库对象的审计记录，可对数据库用户进行审计权限的授予与回收
接下页	

审计术语	说明
审计员	由 SYSAUDITOR 授权，具备授权审计功能的数据库用户
审计权	审计人员具有的审计权限
审计项	可设置审计行为的数据库操作行为项

1.2 审计模式

虚谷数据库审计系统的任务处理模式分为堆表模式和日志文件模式两种，审计模式决定审计过程中对审计记录的处理方式。堆表模式会将审计记录以虚谷数据库标准行数据格式写入审计结果表 SYS_AUDIT_RESULTS，日志文件模式会将审计记录以日志记录格式写入审计日志文件。通常在相同并发度的情况下，后者会具有更好的性能，原因在于堆表审计模式在面对并发写时，仍然是对一个数据块进行顺序写操作，此处的单点性能瓶颈明显；如果数据库系统是一个集群，还会有数据多副本同步的额外开销，这必将影响审计的并行处理能力。

2 审计开关

2.1 审计系统

审计系统为数据库进行可定制审计策略的全系统操作行为审计，审计结果记载在数据库审计结果记录表 SYS_AUDIT_RESULT 或审计日志中。

在虚谷数据库中，可通过属性 ENABLE_AUDIT 控制审计系统的开启与关闭，开启/关闭操作立即生效，无需重启数据库服务，若 ENABLE_AUDIT 未开启则在设置审计项时数据库会抛出警告但不影响审计项的设置。

开启/关闭虚谷数据库审计功能命令如下：

```
--开启审计功能
SQL> SET ENABLE_AUDIT ON;

--关闭审计功能
SQL> SET ENABLE_AUDIT OFF;
```

查看虚谷数据库审计功能状态命令如下：

```
--通过会话变量查看当前审计状态(T：审计状态开启；F：审计状态关闭(默认))
SQL> SHOW ENABLE_AUDIT;

ENABLE_AUDIT |
-------------------------------------------------------------
F |

--通过数据库配置文件/SETUP/xugu.ini查看当前审计状态(以Linux系统为例,true：审计状态开启；false：审计状态关闭)
[root@xugudb SETUP]#cat xugu.ini | grep -i "ENABLE_AUDIT"
enable_audit = false;   是否允许审计
```

> **说明**
>
> 审计项设置成功，触发审计操作后审计结果表中无数据，可查看 ENABLE_AUDIT 参数是否为启用状态。

2.2 创建审计表

审计系统提供两种记载模式：表模式、日志模式。审计结果表 SYS_AUDIT_RESULTS 需在用户开启审计项之前手动创建。

语法格式

```
createTableMode::=
    SET AUDIT TABLE PARTITION INTERVAL ICONST table_unit;

table_unit::=
    {YEAR | MONTH | DAY}

createFileMode::=
    SET AUDIT FILE PARTITION INTERVAL ICONST file_unit;

file_unit::=
    {YEAR | MONTH | DAY | HOUR | K | M | G}
```

参数说明

- createTableMode：初始化表模式审计信息，主要是创建审计表，表名为 sys_audit_results。
- createFileMode：初始化日志模式审计信息，主要是创建文件虚表和设置文件切片信息，表名为 sys_audit_texts，该表为文件虚表。
- table_unit：在创建审计结果表过程中可指定数据分区间隔，分区间隔单位支持 YEAR、MONTH、DAY；如 YEAR 表示审计表分区按 YEAR 进行分区管理，其中默认分区时间为’2020-01-01’，其余类似。
- file_unit：在创建日志文件时可指定数据分区间隔，分区切片间隔单位支持 YEAR、MONTH、DAY、HOUR、K、M、G，审计日志文件的切片仅支持库级；如 YEAR 表示审计日志文件按 YEAR 进行切片管理，K 表示审计日志文件按照 K 级大小进行切片管理，其余类似。

说明

- 使用表模式审计记载则按照表模式语法执行，使用日志模式审计记载则按照日志模式语法执行。
- 审计表只可由审计管理员创建，审计员只允许设置审计项，不允许创建审计表。
- 使用升级前的库，若已经存在审计项和审计表，则无需手动创建审计表。若使用新版本审计系统新建库，则必须使用上述语法创建相应模式审计表。

2.3 DDL 审计

在虚谷数据库中，DDL 审计主要是针对用户的一些高危操作进行记载，如修改表结构、删除数据库对象。可通过属性 REG_DDL 控制 DDL 命令审计的开启与关闭，开启/关闭操作立即生效，无需重启数据库服务。

开启/关闭虚谷数据库 DDL 命令审计功能命令如下：

- 开启 DDL 命令审计功能。

```
SQL> SET REG_DDL ON;
```

- 关闭 DDL 命令审计功能。

```
SQL> SET REG_DDL OFF;
```

查看虚谷数据库 DDL 命令审计功能状态命令如下：

- 通过会话变量查看当前 DDL 命令审计状态（T：DDL 命令审计状态开启；F：DDL 命令审计状态关闭 (默认)）。

```
SQL> SHOW REG_DDL;

REG_DDL |
--------------------------------------------------------
F |
```

- 通过数据库配置文件/SETUP/xugu.ini 查看当前 DDL 命令审计状态（以 Linux 系统为例,true：DDL 命令审计状态开启；false：DDL 命令审计状态关闭）。

```
[root@xugudb SETUP]#cat xugu.ini | grep -i "REG_DDL"
reg_ddl = false;   是否记录DDL命令?
```

DDL 审计记载项

表 2-1 DDL 审计记载项

审计选项	说明
ALTER TABLE ... ADD COLUMN ...	在表上增加新列
ALTER TABLE ... DROP COLUMN ...	删除表上已有列
ALTER TABLE ... MODIFY COLUMN ...	修改表上已有列
ALTER TABLE ... RENAME COLUMN ... TO ...	重命名列名
ALTER TABLE ... ALTER COLUMN ... TYPE	修改表中列的数据类型
ALTER TABLE ... OWNER TO ...	修改表对象属主
ALTER TABLE ... ENABLE CONSTRAINT ...	启用表约束
ALTER TABLE ... DISABLE CONSTRAINT ...	禁用表约束
ALTER TABLE ... ADD PARTITON ...	在分区表上增加新分区
ALTER TABLE ... DROP PARTITION ...	删除分区表上已有分区
ALTER TABLE ... TRUNCATE PARTITION ...	清空分区表上指定分区数据
ALTER TABLE ... SET ONLINE	设置表状态为在线
ALTER TABLE ... SET OFFLINE	设置表状态为离线
ALTER TABLE ... SET PARTITION ... ONLINE	设置分区状态为在线
ALTER TABLE ... SET PARTITION ... OFFLINE	设置分区状态为离线
TRUNCATE TABLE ...	清空表数据
ALTER TABLE ... SET SLOW MODIFY ON/OFF	开启/关闭缓变表
ALTER TABLE ... REBUILD HEAP	整理表
ALTER TABLE ... RENAME TO ...	重命名表

接下页

审计选项	说明
ALTER TABLE... DISABLE INSERT	取消表上的插入许可
ALTER TABLE... DISABLE UPDATE	取消表上的更新许可
ALTER TABLE... DISABLE DELETE	取消表上的删除许可
ALTER TABLE... ENABLE INSERT	设置表上的插入许可
ALTER TABLE... ENABLE UPDATE	设置表上的更新许可
ALTER TABLE... ENABLE DELETE	设置表上的删除许可
DROP DATABASE ...	删除数据库对象
DROP SCHEMA ...	删除数据库模式对象
DROP TABLE ...	删除数据库表对象
DROP SEQUENCE ...	删除数据库序列值对象
DROP VIEW ...	删除数据库视图对象
DROP PROCEDURE ...	删除数据库存储过程对象
DROP FUNCTION ...	删除数据库存储函数对象
DROP INDEX ...	删除数据库索引对象
DROP TRIGGER ...	删除数据库触发器对象
DROP TYPE ...	删除数据库自定义类型对象
DROP USER ...	删除数据库用户对象
DROP ROLE ...	删除数据库角色对象
DROP DB_LINK ...	删除数据库链接对象
DROP SYNONYM ...	删除同义词

接下页

审计选项	说明
DROP PACKAGE ...	删除用户包
DROP POLICY ...	删除安全策略

审计结果查询

- 可通过查询 COMMAND.LOG 查看审计结果（COMMAND.LOG 位于 XGLOG）。

```
[root@xugudb XGLOG]# cat  COMMAND.LOG
```

- 可通过查询系统表 SYS_COMMAND_LOG 查看审计结果。

```
SQL> SELECT * FROM SYS_COMMAND_LOG;
```

说明

- 开启后，部分 DDL 记载在 COMMAND.LOG 中。
- 删除对象中的 DDL 语句执行成功后记载，失败时在 ERRER.LOG 中记载。
- 修改表中的 DDL 语句除 truncate table 执行成功记载外，其他均在执行之前记载。

3 审计设置

3.1 概述

数据库审计员指定被审计对象的行为称为审计设置，只有具备审计权限的用户才能进行审计设置。虚谷提供审计设置系统过程来实现这种设置，被审计的对象可以是某类操作，也可以是某些用户在数据库中的全部操作。只有预先设置的操作和用户才能被虚谷系统自动进行审计。虚谷的审计设置可分为三个级别，如表3-1所示。

表 3-1 审计级别

审计级别	说明
数据库全局审计	用于设置数据库全局操作行为的审计。如：创建实例、建立数据库连接会话、修改数据库配置等
局部语句级审计	用于设置对某一类数据库对象或者某一类操作语句进行的审计。如：AUDIT TABLE 将审计 CREATE TABLE、ALTER TABLE 和 DROP TABLE 等语句
局部对象级审计	用于设置对某些对象的操作行为进行审计。如：test 表上的 INSERT 语句

说明

- 只要审计功能被启用，系统级的审计记录就会产生。
- 在进行数据库审计时，审计员之间没有区别，可以审计所有数据库对象，也可取消其他审计员的审计设置。
- 语句级审计不针对特定的对象，只针对用户。
- 对象级审计针对指定的用户与指定的对象。
- 在设置审计时，审计选项不区分包含关系，都可以设置。
- 如果用户执行的一条语句与设置的若干审计项都匹配，只会在审计结果中生成一条审计记录。

3.2 数据库全局审计

在数据库指定对库级操作行为的审计功能称为数据库全局审计，全局审计支持的对象有：数据库、数据库连接。当审计对象为数据库时，表示对数据库的创建、修改、删除操作记录；审计对象为连接时，表示对一切连接数据库的行为进行记载。

表 3-2 数据库全局审计选项

审计选项	审计的数据库操作	说明
CONNECT	-	数据库连接操作
DATABASE	-	创建/删除库操作

语法格式

```
{AUDIT | NOAUDIT} { TYPE } [BY USER_NAME] [TO FILE] [WHENEVER
   SUCCESSFUL | WHENEVER NO SUCCESSFUL]
```

参数说明

- 设置审计：AUDIT 设置审计项；NOAUDIT 取消审计项。
- TYPE：全局审计选项，即表3-2中的第一列。

- USER_NAME：用户名。审计指定用户的操作，若未指定用户则表示对当前库下所有用户操作进行审计。
- WHENEVER：审计时机，可选的取值如下，若不加则表示无论成功与否都作记载（注：新版本取消审计项不再支持 WHENEVER 子句）。
  - SUCCESSFUL：操作成功时
  - NO SUCCESSFUL：操作失败时
- TO FILE：若省略 TO FILE 则表示使用表模式进行审计，若选取 TO FILE 则表示使用日志模式进行审计；同一审计项只能选择其中一种模式，如需修改审计模式则根据审计语法重新执行一次设置审计项即可。

应用示例

- 审计 SYSDBA 用户建立数据库连接成功的操作。

```
SQL> AUDIT CONNECT BY SYSDBA WHENEVER SUCCESSFUL;
```

- 审计 SYSDBA 用户建立数据库连接成功的操作修改为日志模式。

```
SQL> AUDIT CONNECT BY SYSDBA TO FILE WHENEVER SUCCESSFUL;
```

- 取消审计 SYSDBA 用户建立数据库连接成功的操作。

```
SQL> NOAUDIT CONNECT BY SYSDBA;
```

3.3 局部语句级审计

语句级审计用于设置对某一类数据库对象或者某一类操作语句进行的审计，不对应具体的数据库对象。其审计选项如表3-3所示。

表 3-3 局部语句级审计选项

审计选项	审计的数据库操作	说明
USER	CREATE USER ALTER USER DROP USER	创建/修改/删除用户操作
		接下页

审计选项	审计的数据库操作	说明
ROLE	CREATE ROLE DROP ROLE	创建/删除角色操作
SCHEMA	CREATE SCHEMA DROP SCHEMA SET SCHEMA	创建/删除/设置模式操作
TABLE	CREATE TABLE ALTER TABLE DROP TABLE TRUNCATE TABLE	创建/修改/删除/清空基表操作
VIEW	CREATE VIEW ALTER VIEW DROP VIEW	创建/修改/删除视图操作
INDEX	CREATE INDEX DROP INDEX	创建/删除索引操作
PROCEDURE	CREATE PROCEDURE ALTER PROCEDURE DROP PROCEDURE	创建/修改/删除存储过程操作
TRIGGER	CREATE TRIGGER ALTER TRIGGER DROP TRIGGER	创建/修改/删除触发器操作
SEQUENCE	CREATE SEQUENCE ALTER SEQUENCE DROP SEQUENCE	创建/修改/删除序列操作

接下页

审计选项	审计的数据库操作	说明
TABLESPACE	CREATE TABLESPACE ALTER TABLESPACE DROP TABLESPACE	创建/修改/删除表空间操作
GRANT	GRANT	授予权限操作
REVOKE	REVOKE	回收权限操作
AUDIT	AUDIT	设置审计操作
NOAUDIT	NOAUDIT	取消审计操作
INSERT TABLE	INSERT INTO TABLE	表上的插入操作
UPDATE TABLE	UPDATE TABLE	表上的修改操作
DELETE TABLE	DELETE FROM TABLE	表上的删除操作
SELECT TABLE	SELECT FROM TABLE	表上的查询操作
LOCK TABLE	LOCK TABLE	表的加锁操作
EXECUTE PROCEDURE	EXECUTE PROCEDURE	调用存储过程或函数操作
POLICY	CREATE POLICY ALTER POLICY DROP POLICY	创建/修改/删除安全策略操作
USER POLICY	ALTER USER POLICY	赋予用户安全策略操作
TABLE POLICY	ALTER TABLE POLICY	赋予表安全策略操作
PACKAGE	CREATE PACKAGE DROP PACKAGE	创建/删除包规范操作
TYPE	CREATE TYPE DROP TYPE	创建/删除自定义类型操作

接下页

审计选项	审计的数据库操作	说明
DATABASE LINK	CREATE DATABASE LINK DROP DATABASE LINK	创建/删除数据库连接操作
INSERT ANY TABLE	INSERT INTO TABLE	表上的插入操作
UPDATE ANY TABLE	UPDATE TABLE	表上的修改操作
DELETE ANY TABLE	DELETE FROM TABLE	表上的删除操作
SELECT ANY TABLE	SELECT FROM TABLE	表上的查询操作
LOCK ANY TABLE	LOCK TABLE	表的加锁操作
EXECUTE ANY PROCEDURE	EXECUTE PROCEDURE	调用存储过程或函数操作
SYSARGS	SET sys_args TO ...	修改数据库参数命令

语法格式

```
{AUDIT | NOAUDIT} { TYPE } [ BY USER_NAME ] [TO FILE] [ WHENEVER
   SUCCESSFUL | WHENEVER NO SUCCESSFUL ];
```

参数说明

- 设置审计：AUDIT 设置审计项；NOAUDIT 取消审计项。
- TYPE：语句级审计选项，即表3-3中的第一列。
- USER_NAME：用户名。审计指定用户的操作，若未指定用户则表示对当前库下所有用户操作进行审计。
- WHENEVER：审计时机，可选的取值如下，若不加则表示无论成功与否都作记载（注：新版本取消审计项不再支持 WHENEVER 子句）。
  - SUCCESSFUL：操作成功时
  - NO SUCCESSFUL：操作失败时
- TO FILE：若省略 TO FILE 则表示使用表模式进行审计，若选取 TO FILE 则表示使用日志模式进行审计；同一审计项只能选择其中一种模式，如需修改审计模式则根据审计语法重

新执行一次设置审计项即可。

应用示例

- 审计 SYSDBA 用户操作 PACKAGE 对象成功的操作记录。

```
SQL> AUDIT PACKAGE BY SYSDBA WHENEVER SUCCESSFUL;
```

- 审计授予权限成功的操作记录。

```
SQL> AUDIT GRANT WHENEVER SUCCESSFUL;
```

- 审计查询表成功的操作记录。

```
SQL> AUDIT SELECT TABLE WHENEVER SUCCESSFUL;
```

- 取消审计创建、修改、删除序列值成功的操作。

```
SQL> NOAUDIT SEQUENCE;
```

- 取消审计创建、删除包成功的操作。

```
SQL> NOAUDIT PACKAGE;
```

3.4 局部对象级审计

对象级审计发生在具体的对象上，需要指定模式名以及对象名。其审计选项如表3-4所示。

表 3-4 局部对象级审计选项

审计选项	TABLE	VIEW	PROCEDURE/FUNCTION
INSERT	√	√	-
UPDATE	√	√	-
DELETE	√	√	-
SELECT	√	√	-
EXECUTE	-	-	√

接下页

审计选项	TABLE	VIEW	PROCEDURE/FUNCTION
ALL（所有对象级审计选项）	√	√	√

语法格式

```
{AUDIT | NOAUDIT} { TYPE } ON OBJ_NAME[BY USER_NAME ] [TO FILE] [
   WHENEVER SUCCESSFUL|WHENEVER NO SUCCESSFUL];
```

参数说明

- 设置审计：AUDIT 设置审计项；NOAUDIT 取消审计项。
- TYPE：局部对象级审计选项，即表3-4中的第一列。
- OBJ_NAME：模式名. 表名或模式名. 存储过程名等。
- USER_NAME：用户名。审计指定用户的操作，若未指定用户则表示对当前库下所有用户操作进行审计。
- WHENEVER：审计时机，可选的取值如下，若不加则表示无论成功与否都作记载（注：新版本取消审计项不再支持 WHENEVER 子句）。
  - SUCCESSFUL：操作成功时
  - NO SUCCESSFUL：操作失败时
- TO FILE：若省略 TO FILE 则表示使用表模式进行审计，若选取 TO FILE 则表示使用日志模式进行审计；同一审计项只能选择其中一种模式，如需修改审计模式则根据审计语法重新执行一次设置审计项即可。

应用示例

- 审计 SYSDBA 用户对表 test_audit 执行成功的查询操作。

```
SQL> AUDIT SELECT ON SYSDBA.test_audit BY SYSDBA WHENEVER
   SUCCESSFUL;
```

- 取消审计 SYSDBA 用户对表 test_audit 执行成功的查询操作。

```
SQL> NOAUDIT SELECT ON SYSDBA.test_audit BY SYSDBA;
```

- 审计 SYSDBA 用户对表 test_audit 执行成功的查询、更新、插入、删除操作。

```
SQL> AUDIT SELECT,UPDATE,INSERT,DELETE ON SYSDBA.test_audit BY
   SYSDBA WHENEVER SUCCESSFUL;
```

3.5 选择性审计规则

选择性审计规则是指审计管理员可从用户身份、操作类型、权限级别、可审计安全事件以及其他额外属性或标准中集中选择可审计的事件，从而有针对性的选择审计数据库操作行为。

表 3-5 选择性审计

审计对象	对象细分	是否支持审计	选择说明
用户身份	客体身份	×	-
	用户身份	√	选择指定的数据库用户进行审计
	角色身份	√	选择指定的数据库角色进行审计
	主体身份	×	-
	主机身份	×	选择指定的主机 IP 或主机名称进行审计
操作类型	定义语句	√	选择指定的数据库定义语句进行审计
	查询语句	√	选择指定的数据库查询语句进行审计
	更新语句	√	选择指定的数据库更新语句进行审计
	控制语句	√	选择指定的数据库控制语句进行审计

接下页

审计对象	对象细分	是否支持审计	选择说明
权限级别	数据库系统级	√	选择指定的数据库系统操作行为进行审计(如：服务启停、配置变更)
	数据库实例级	×	选择指定的数据库实例配置操作行为进行审计 (如：TCP 监听)
	数据库库级	√	选择指定的数据库库级操作行为进行审计
	对象模式级	√	选择指定的数据库对象操作行为进行审计
	细粒度数据操作级	√	选择指定的数据库数据操作行为进行审计
安全事件	成功	√	选择所有执行成功的 SQL 语句进行审计
	失败	√	选择所有执行失败的 SQL 语句进行审计
	全部	√	选择所有执行的 SQL 语句进行审计

应用示例

- 审计 SYSDBA 用户在客体 test_audit 上所有的数据库操作行为。

```
SQL> AUDIT ALL ON SYSDBA.test_audit BY SYSDBA;
```

- 审计 SYSDBA 用户对表 test_audit 执行成功的更新、删除操作。

```
SQL> AUDIT UPDATE,DELETE ON SYSDBA.test_audit BY SYSDBA WHENEVER
   SUCCESSFUL;
```

3.6 审计定义系统表

3.6.1 字段说明

表 3-6 字段说明

序号	字段名	类型	说明
0	DB_ID	OID_TYPE	库 ID
1	USER_ID	OID_TYPE	用户 ID
2	OBJ_ID	OID_TYPE	对象 ID
3	OBJ_TYPE	INTEGER	对象类别
4	AUDIT_MASK	BIGINT	审计项目掩码
5	WHENEVER	INTEGER	审计时机 （1: 操作成功时记录审计项 2: 操作失败时记录审计项 3: 无论成功与否都记录审计项）

3.6.2 审计项目掩码 (AUDIT_MASK)

表 3-7 审计项目掩码

序号	审计项目	成功	失败	所有
1	AUDIT_CONNECT	4	8	12
2	AUDIT_DATABASE	16	32	48
3	AUDIT_USER	64	128	192
4	AUDIT_ROLE	256	512	768
5	AUDIT_SCHEMA	1024	2048	3072

接下页

序号	审计项目	成功	失败	所有
6	AUDIT_TABLE	4096	8192	12288
7	AUDIT_VIEW	16384	32768	49152
8	AUDIT_INDEX	65536	131072	196608
9	AUDIT_PROCEDURE	262144	524288	786432
10	AUDIT_TRIGGER	1048576	2097152	3145728
11	AUDIT_SEQUENCE	4194304	8388608	12582912
12	AUDIT_GRANT	16777216	33554432	50331648
13	AUDIT_REVOKE	67108864	134217728	201326592
14	AUDIT_AUDIT	268435456	536870912	805306368
15	AUDIT_NOAUDIT	1073741824	2147483648	3221225472
16	AUDIT_INSERT	4294967296	8589934592	12884901888
17	AUDIT_UPDATE	17179869184	34359738368	51539607552
18	AUDIT_DELETE	68719476736	137438953472	206158430208
19	AUDIT_SELECT	274877906944	549755813888	824633720832
20	AUDIT_LOCK_TAB	1099511627776	2199023255552	3298534883328
21	AUDIT_EXECUTE	4398046511104	8796093022208	13194139533312
22	AUDIT_POLICY	17592186044416	35184372088832	52776558133248
23	AUDIT_USER_POLICY	70368744177664	140737488355328	211106232532992

接下页

序号	审计项目	成功	失败	所有
24	AUDIT_TAB_POLICY	281474976710656	562949953421312	844424930131968
25	AUDIT_SPACE	112589990684262 0	225179981368525 0	337769972052787 0
26	AUDIT_PACKAGE	112589990684262 4	225179981368524 8	337769972052787 2
27	AUDIT_TYPE	180143985094819 84	360287970189639 68	540431955284459 52
28	AUDIT_DB_LINK	720575940379279 36	144115188075855 872	216172782113783 808
29	AUDIT_SYNONYM	288230376151711 744	576460752303423 488	864691128455135 232
30	AUDIT_DOMAIN	115292150460685 0000	230584300921369 0000	345876451382054 0000
31	AUDIT_ARGS	1	2	3

⚠ 注意

当前版本不支持 DOMAIN。

4 审计信息查询

4.1 审计结果系统表

4.1.1 概述

当使用虚谷提供的审计机制进行了表模式审计设置后，这些审计操作信息都记录在当前库 SYS_AUDIT_RESULTS 表中，该表结构如表4-1所示。审计类型用户可以通过此表查询审计设置信息。

当使用虚谷提供的审计机制进行了日志模式审计设置后，这些审计操作信息都记录在当前库 SYS_AUDIT_TEXTS 表中，该表字段结构与记载数据均同 SYS_AUDIT_RESULTS 表一致，但 SYS_AUDIT_TEXTS 为文件虚表且不具有分区结构。

表 4-1 SYS_AUDIT_RESULTS 表结构

序号	字段名	类型	说明
1	SCHEMA_ID	INTEGER	对象所属模式
2	USER_ID	INTEGER	执行 SQL 的用户
3	OBJ_ID	INTEGER	对象 ID
4	OBJ_NAME	CHAR(128)	对象名称
5	OBJ_TYPE	INTEGER	对象类型
6	ACTION	INTEGER	动作类型
7	SUCCESS	BOOLEAN	SQL 执行成功
8	IP	CHAR(20)	客户端 IP
9	SQL_TEXT	VARCHAR	SQL 语句
10	ERR_INFO	VARCHAR	错误信息

接下页

序号	字段名	类型	说明
11	OPTIME	DATETIME	操作时间
12	AUDIT_TYPE	INTEGER	审计类型
13	NODEID	INTEGER	节点号

参数说明：

- SCHEMA_ID：审计结果对象所属模式 ID，与 SYS_SCHEMAS 系统表连接可获取模式详细信息。
- USER_ID：执行 SQL 的用户 ID，与 SYS_USERS 系统表连接可获取用户详细信息。
- OBJ_ID：审计结果对象 ID。
- OBJ_NAME：审计结果对象名称。
- OBJ_TYPE：审计结果对象类型。
- ACTION：审计记录动作类型。
- SUCCESS：审计记录 SQL 执行状态 (T：执行成功；F：执行失败)。
- IP：审计记录 SQL 执行客户端 IP 地址。
- SQL_TEXT：审计记录执行 SQL 语句。
- ERR_INFO：审计记录 SQL 执行失败时，错误消息。
- OPTIME：审计记录 SQL 执行时间。
- AUDIT_TYPE：审计类型。
- NODEID：节点号。

说明

- 创建表操作无对象 ID。
- 审计记录的 SQL 数据长度最大限制为 32K，超过 32K 的 SQL 在审计时会进行截断处理。
- 记载和写系统表异步执行，可能导致查看审计表数据时无数据的情况，等待几秒即可。
- 黑白名单连接失败不会被记载。

4.1.2 审计动作对应表 (ACTION)

表 4-2 审计动作对应表

代码	动作类型	说明	是否在审计中使用
0	ACTION_READ	查询表数据	是
1	ACTION_INSERT	插入表数据	是
2	ACTION_UPDATE	更新表数据	是
3	ACTION_DELETE	删除表数据	是
4	ACTION_EXECUTE	执行过程或函数	是
5	ACTION_REF	引用	否
6	ACTION_ALT_DB	修改库	否
7	ACTION_DROP_DB	删除库	否
8	ACTION_ALT_SCHE	修改模式	否
9	ACTION_DROP_SCHE	删除模式	否
10	ACTION_CREATE	创建对象	是

接下页

代码	动作类型	说明	是否在审计中使用
11	ACTION_CRE_IDX	创建索引	否
12	ACTION_ALT_IDX	修改索引	否
13	ACTION_DROP_IDX	删除索引	否
14	ACTION_TRACE_DB_MODI	创建库变更跟踪	否
15	ACTION_UNTRACE_DB_MODI	删除库变更跟踪	否
16	ACTION_TRACE_SCHE_MODI	创建模式变更跟踪	否
17	ACTION_UNTRACE_SCHE_MODI	删除模式变更跟踪	否
18	ACTION_TRACE_TAB_MODI	创建表变更跟踪	否
19	ACTION_UNTRACE_TAB_MODI	删除表变更跟踪	否
20	ACTION_CRE_JOB	创建定时作业	否
21	ACTION_ALT_JOB	修改定时作业	否
22	ACTION_DROP_JOB	删除定时作业	否
23	ACTION_CRE_TRIG	创建触发器	否
24	ACTION_ALT_TRIG	修改触发器	否
25	ACTION_DROP_TRIG	删除触发器	否
26	ACTION_ALTER	修改对象	是
27	ACTION_DROP_FK	删除外键约束	否
28	ACTION_REN_OBJ	更改对象名	否
29	ACTION_REN_COL	更改表字段名	否
30	ACTION_ONLINE	设置在线	否

接下页

代码	动作类型	说明	是否在审计中使用
31	ACTION_OFFLINE	设置离线	否
32	ACTION_DROP	删除对象	是
33	ACTION_ENCRYPT	加密对象	否
34	ACTION_VACUUM	-	否
35	ACTION_TRUNC	清空表数据	是
36	ACTION_ANALYZE	分析表	否
37	ACTION_ANA_CFG	-	否
38	ACTION_GRANT	收授权限	是
39	ACTION_REFRESH	-	否
40	ACTION_REPLICATION	-	否
41	ACTION_BACKUP	备份数据	是
42	ACTION_RESTORE	恢复数据	是
43	ACTION_SHUTDOWN	关闭服务	否
44	ACTION_CONNECT	创建连接 (LOGIN)	否
45	ACTION_DROP_DBC	-	否
46	ACTION_ALL	-	否
47	ACTION_POLICY	设置安全策略	否
48	ACTION_NOPOLICY	取消安全策略	否
49	ACTION_AUTH_NOT	-	否
50	ACTION_AUDIT	设置审计	是

接下页

代码	动作类型	说明	是否在审计中使用
51	ACTION_NOAUDIT	取消审计	否
52	ACTION_RMAUDIT	移除审计缓存	否
53	ACTION_LOCK	锁表	是
54	ACTION_COMMIT	提交	否
55	ACTION_ROLLBACK	回滚	否
56	ACTION_TRACE	-	否
57	ACTION_AND	-	否
58	ACTION_OR	-	否
62	ACTION_ARGS	修改参数	否

4.1.3 审计类型对应表 (AUDIT_TYPE)

表 4-3 审计动作对应表

代码	审计类型	说明
0	AUDIT_SYSARGS	参数
1	AUDIT_CONNECT	连接
2	AUDIT_DATABASE	库
3	AUDIT_USER	用户
4	AUDIT_ROLE	角色
5	AUDIT_SCHEMA	模式
6	AUDIT_TABLE	表

接下页

代码	审计类型	说明
7	AUDIT_VIEW	视图
8	AUDIT_INDEX	索引
9	AUDIT_PROCEDURE	存储过程和函数
10	AUDIT_TRIGGER	触发器
11	AUDIT_SEQUENCE	序列值
12	AUDIT_GRANT	授权
13	AUDIT_REVOKE	回收权限
14	AUDIT_AUDIT	设置审计
15	AUDIT_NOAUDIT	取消审计
16	AUDIT_INSERT	插入
17	AUDIT_UPDATE	更新
18	AUDIT_DELETE	删除
19	AUDIT_SELECT	查询
20	AUDIT_LOCK_TAB	锁表
21	AUDIT_EXECUTE	执行
22	AUDIT_POLICY	安全策略
23	AUDIT_USER_POLICY	主体策略
24	AUDIT_TAB_POLICY	客体策略
25	AUDIT_SPACE	表空间
26	AUDIT_PACKAGE	包

接下页

代码	审计类型	说明
27	AUDIT_TYPE	自定义类型
28	AUDIT_DB_LINK	dblink
29	AUDIT_SYNONYM	同义词
30	AUDIT_DOMAIN	存储域

4.2 审计结果应用示例

- 审计动作（创建表）。

```
SQL> CREATE TABLE audit_info(id INT);
```

- 查看审计结果。

```
SQL> SELECT * FROM sys_audit_results;

SCHEMA_ID | USER_ID | OBJ_ID | OBJ_NAME | OBJ_TYPE | ACTION |
   SUCCESS | IP | SQL_TEXT | ERR_INFO | OPTIME | AUDIT_TYPE |
   NODEID |

---------------------------------------------------------

1 | 1 | 0 | AUDIT_INFO| 5 | 10 | T | 192.168.30.222| CREATE TABLE
    audit_info(id INT);| <NULL>| 2022-05-11 09:58:25.116 AD
    | 6 | 1 |
```

4.3 审计结果分区规则

为了方便审计结果的管理，系统自建的审计系统表为用户指定分区信息的分区表，具体分区规则如下：

- 包含一个默认分区 PINIT(起始时间为‘2020-01-01’)，此分区不可删除。
- 分区间隔为创建表所设置的分区间隔时间，根据设置的分区间隔时间计算产生一个新分区进行审计记录记载。

```
SQL> SELECT * FROM sys_partis;

DB_ID | TABLE_ID | PARTI_NO | PARTI_NAME | PARTI_VAL | GSTO_NOS |
   ONLINE | RESERVED1 | RESERVED2 |
-----------------------------------------------------------
```

```
1 | 1048576 | 0 | PINIT| '2020-01-01'| 201 | T | <NULL>| <NULL>|
1 | 1048576 | 1 | EXT_PART_1655856000| '2022-06-22 00:00:00'
   | 206 | T | <NULL>| <NULL>|
```

4.4 审计结果筛选

审计系统表记录了审计事件产生的所有元素，授权用户可以通过审计数据字段中的值的搜索与分类条件提供对查阅的审计数据进行搜索和排序。审计系统表字段信息请参见章节4.1。

- 选择需要查询的字段，筛选指定用户的审计记录并通过记录时间进行排序。

```
SQL> SELECT user_id,obj_name,action,success,ip,sql_text,err_info,
   optime,audit_type FROM SYS_AUDIT_RESULTS WHERE user_id='102'
   order by optime;

USER_ID | OBJ_NAME | ACTION | SUCCESS | IP | SQL_TEXT | ERR_INFO
    | OPTIME | AUDIT_TYPE |
-------------------------------------------------------
102 | TAB_T1| 10 | T | 192.168.1.239| CREATE TABLE TAB_T1(col1
   INT,col2 VARCHAR);| <NULL>| 2022-06-21 14:26:38.247 AD | 6 |
102 | TAB_T1| 26 | T | 192.168.1.239| ALTER TABLE TAB_T1 ADD
   COLUMN col3 VARCHAR(20);| <NULL>| 2022-06-21 14:27:03.436 AD
    | 6 |
102 | TAB_T1| 1 | T | 192.168.1.239| INSERT INTO TAB_T1(col1,col2
   ,col3) VALUES(1,'VAL1','VAL1');| <NULL
   >| 2022-06-21 14:30:47.829 AD | 16 |
102 | TAB_T1| 2 | T | 192.168.1.239| UPDATE TAB_T1 SET col3='
   NEW_VAL1' WHERE col1=1;| <NULL>| 2022-06-21 14:31:12.490 AD
    | 17 |
102 | TAB_T1| 32 | T | 192.168.1.239| DROP TABLE TAB_T1;| <NULL
   >| 2022-06-21 14:31:26.917 AD | 6 |
102 | TAB_TT| 10 | T | 192.168.1.239| CREATE TABLE TAB_TT(col1
   int);| <NULL>| 2022-06-21 14:32:44.126 AD | 6 |
102 | TAB_TT| 10 | F | 192.168.1.239| CREATE TABLE TAB_TT(col1
   int);| 同名Table对象TAB_TT已存在| 2022-06-21 14:32:45.104 AD
    | 6 |
```

- 筛选指定用户操作失败的审计结果。

```
SQL> SELECT user_id,obj_name,action,success,ip,sql_text,err_info,
   optime,audit_type FROM SYS_AUDIT_RESULTS WHERE success='F';

USER_ID | OBJ_NAME | ACTION | SUCCESS | IP | SQL_TEXT | ERR_INFO
    | OPTIME | AUDIT_TYPE |
-------------------------------------------------------
102 | TAB_TT| 10 | F | 192.168.1.239| CREATE TABLE TAB_TT(col1
   int);| 同名Table对象TAB_TT已存在| 2022-06-21 14:32:45.104 AD
    | 6 |
```

4.5 审计结果表删除

审计系统表记录了审计事件产生的所有元素，为了方便用户可重新设置分区规则，表模式的审计结果表在当前库下无审计项时可删除，删除后可重新设置审计系统表分区规则，若库下存在表模式审计项则该表不可删除。日志模式审计结果表在存在审计项或不存在审计项时均可进行删除操作。

语法格式

```
DROP TABLE sys_audit_results;
DROP TABLE sys_audit_texts;
```

> ⚠ 注意
>
> - 表模式审计结果表删除后原审计数据丢失。
> - 日志模式审计结果表为文件虚表，故删除不影响原审计数据，重新生成审计表后原文件数据依旧存在。

4.6 审计结果表清除

为了方便用户管理审计数据，表模式提供清空审计结果表和分区数据功能。日志模式读取文件记载信息，故不提供清空审计表结果功能。

语法格式

```
TRUNCATE TABLE sys_audit_results;
ALTER TABLE sys_audit_results TRUNCATE PARTITION part_name;
```

> ⚠ 注意
>
> 表模式审计结果表清空后原审计数据丢失。

5 审计信息安全

5.1 审计数据高可用

虚谷数据库控制节点为主备双机方案，数据存储版本数可按需进行配置，最多支持 3 个数据存储版本。多版本数据存储模式下主版本轮转分布，副本随机分布的策略将数据均匀分布到整个数据库集群节点中，从而保证存储的高可用。

5.2 审计数据防丢失

虚谷数据库除了多副本存储机制保障数据安全外，还可以通过数据库自带控制台工具的导入导出功能进行审计数据的备份，具体方式如下：

使用控制台工具查询审计结果表记载并导出到指定文件进行审计记录备份。

```
SQL> SELECT * FROM sys_audit_results; >$ /home/DBMS/out_audit.exp;
```

6 审计权限的收授

6.1 审计用户收授权

用户或角色可通过被授予审计员权限来获得审计权限。

语法格式

- 授予权限。

```
GRANT AUDITOR TO USER_NAME|ROLE_NAME;
```

- 回收权限。

```
REVOKE AUDITOR FROM USER_NAME|ROLE_NAME;
```

- 授予普通审计员可读审计表权限。

```
GRANT SELECT ON sys_audit_results TO USER_NAME;
```

参数说明

- USER_NAME：用户名。
- ROLE_NAME：角色名。

示例

- 在 SYSDBA 下创建用户 audit_test_user。

```
SQL> CREATE USER audit_test_user IDENTIFIED BY '1234@WQQ';
```

- 登录 SYSAUDITOR 用户，授予用户 audit_test_user AUDITOR 权限。

```
SQL> GRANT AUDITOR TO audit_test_user;
```

- 登录用户 audit_test_user，审计表。

```
SQL> AUDIT TABLE;
```

- 登录 SYSDBA 用户，创建表 test。

```
SQL> CREATE TABLE TEST(a INT);
```

- 录 SYSAUDITOR 用户，查询 SYS_AUDIT_RESULTS。

```
SQL> SELECT OBJ_NAME,SQL_TEXT FROM SYS_AUDIT_RESULTS;
OBJ_NAME | SQL_TEXT |
```

```
-------------------------------------------------
TEST| CREATE TABLE TEST(a INT);|
```

- 回收用户 audit_test_user 审计权限。

```
SQL> REVOKE AUDITOR FROM audit_test_user;
```

- 登录用户 audit_test_user，审计表。

```
SQL> AUDIT TABLE;
Error: [E18012] 权限不够
```

6.2 限制审计查阅

数据库审计结果记录在审计系统表 SYS_AUDIT_RESULTS 表中，默认情况下只有审计管理员 SYSAUDITOR 能够访问及维护审计记录。

- 除了授权管理员具有明确的访问审计数据的权限外，禁止所有授权用户对审计记录进行访问。
- 普通的审计用户也需要赋予查询权限才能查看审计结果表，但是不能变更以及删除审计记录。
- 审计管理员可以赋予任何用户操作审计系统表的权限（查询权限生效，其他对该表操作报失败）。
- 审计管理员可以查询审计结果表，可以清空审计系统表，可以清空/删除审计系统表分区。

7 审计日志的维护

7.1 概述

审计管理员有权对审计结果表进行查询、清空以及删除自动扩展分区操作，以维护审计日志。审计员只能对审计结果表进行 SELECT 操作。所有用户包括审计管理员 SYSAUDITOR 不能修改审计记录，确保审计记录的正确性。

审计结果表-SYS_AUDIT_RESULTS

表 7-1 审计结果表-SYS_AUDIT_RESULTS

维护操作	审计员	审计管理员	权限说明
CREATE	×	√	创建审计结果表
SELECT	×（需 SYSAUDITOR 授权）	√	查询审计结果表结果数据
INSERT	×	×	插入审计结果表结果数据
UPDATE	×	×	更新审计结果表结果数据
DELETE	×	×	删除审计结果表结果数据
TRUNCATE	×	√	清空审计结果表数据
接下页			

维护操作	审计员	审计管理员	权限说明
DROP	×	√	删除除初始化分区 PINIT 外的指定分区（删除分区及分区内全部审计结果数据）

审计结果表-SYS_AUDIT_TEXTS

表 7-2 审计结果表-SYS_AUDIT_TEXTS

维护操作	审计员	审计管理员	权限说明
CREATE	×	√	创建审计结果表
SELECT	×	√	查询审计结果表结果数据
INSERT	×	×	插入审计结果表结果数据
UPDATE	×	×	更新审计结果表结果数据
DELETE	×	×	删除审计结果表结果数据
TRUNCATE	×	×	清空审计结果表数据
DROP	×	√	删除除初始化分区 PINIT 外的指定分区（删除分区及分区内全部审计结果数据）

7.2 查询审计结果表

示例

- 示例 1

  SYSAUDITOR 用户查询审计结果表。

```
SELECT * FROM SYS_AUDIT_RESULTS;
```

- 示例 2

  1. 在 SYSDBA 下创建用户 audit_test_user。

```
SQL> CREATE USER audit_test_user IDENTIFIED BY '1234@WQQ';
```

  2. 登录 SYSAUDITOR 用户，授予用户 audit_test_user AUDITOR 权限。

```
SQL> GRANT AUDITOR TO audit_test_user;
```

  3. 登录 SYSAUDITOR 用户，赋予 audit_test_user 查询表 SYS_AUDIT_RESULTS 的权限。

```
SQL> GRANT SELECT ON SYS_AUDIT_RESULTS  TO audit_test_user;
```

  4. 登录 audit_test_user 用户，查询审计结果表。

```
SQL> SELECT * FROM SYSAUDITOR.SYS_AUDIT_RESULTS;
```

⚠ 注意

被授予审计权限的用户还需要被授予查询 SYS_AUDIT_RESULTS 表的权限，才能在当前用户下查询审计结果表。

7.3 维护审计结果表

为了保证审计记录的正确性、安全性，审计结果系统表记载的审计记录，任何用户 (包括审计管理员) 均不可进行数据变更或更新操作。

审计结果系统表仅能由审计系统管理员 (SYSAUDITOR) 进行维护，SYSAUDITOR 维护审计结果系统表的权限是清空审计结果记录表 (TRUNCATE) 以及删除审计结果记录表除固定分区之外的指定分区内审计记录。

审计结果表-SYS_AUDIT_RESULTS

表 7-3 审计结果表-SYS_AUDIT_RESULTS

维护操作	审计员	审计管理员	权限说明
TRUNCATE	√	√	清空指定范围内的审计结果表数据
DROP	×	√	删除除初始化分区 PINIT 外的指定分区（删除分区及分区内全部审计结果数据）

审计结果表-SYS_AUDIT_TEXTS

表 7-4 审计结果表-SYS_AUDIT_TEXTS

维护操作	审计员	审计管理员	权限说明
TRUNCATE	×	×	清空指定范围内的审计结果表数据
DROP	×	×	删除除初始化分区 PINIT 外的指定分区（删除分区及分区内全部审计结果数据）

示例

- SYSAUDITOR 清空审计结果表。

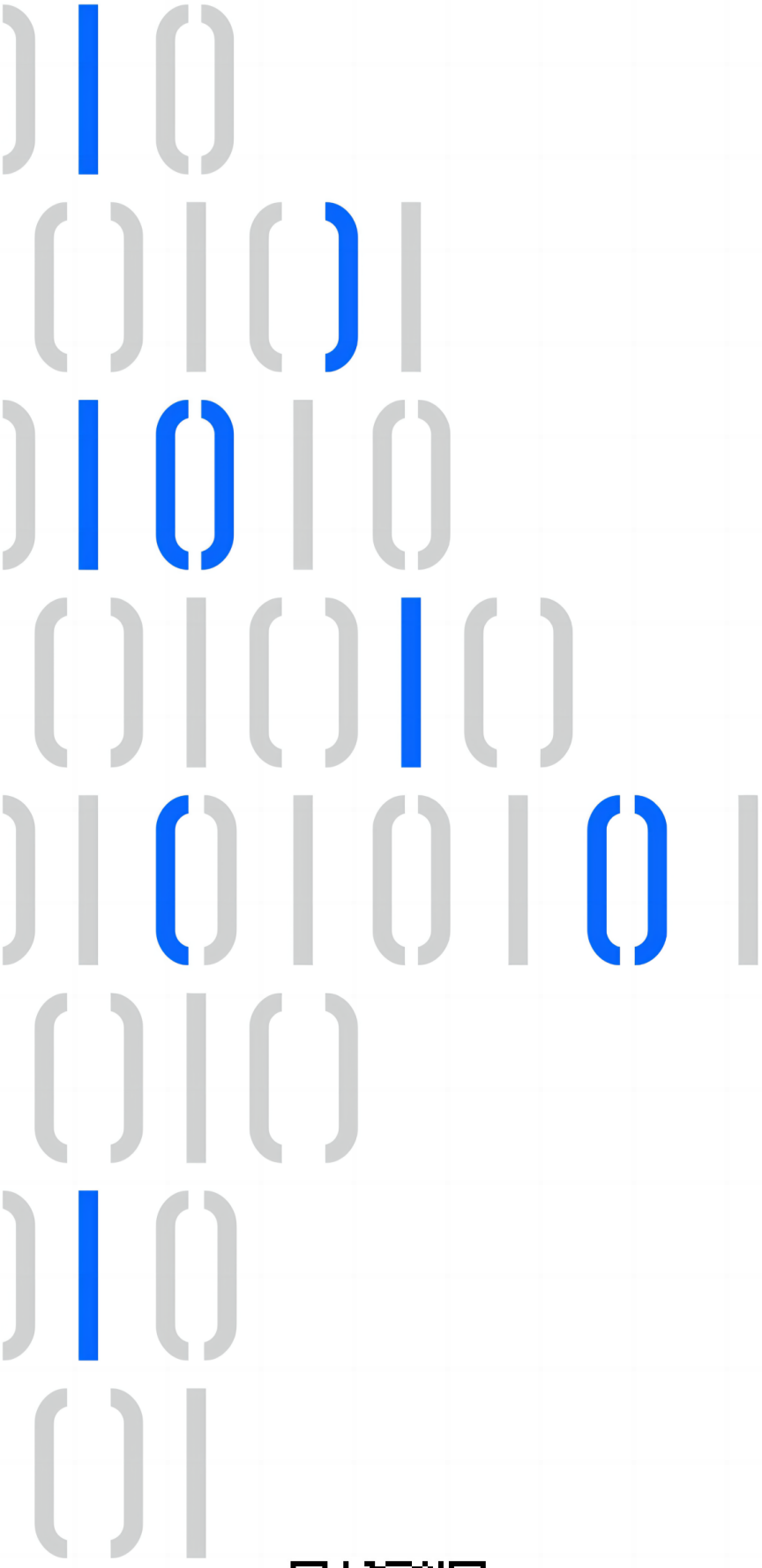
```
TRUNCATE SYS_AUDIT_RESULTS;
```

- 清除审计结果表指定分区，EXT_PART_1655856000 为自动扩展分区名。

```
ALTER TABLE SYS_AUDIT_RESULTS TRUNCATE PARTITION
   EXT_PART_1655856000;
```

- 删除审计结果表指定分区，EXT_PART_1655856000 为自动扩展分区名。

```
ALTER TABLE SYS_AUDIT_RESULTS DROP PARTITION EXT_PART_1655856000;
```



成都虚谷伟业科技有限公司

联系电话：400-8886236

官方网站：www.xugudb.com