## UNIS D2000-G 系列数据库审计系统

典型配置举例

Copyright © 2020 紫光恒越技术有限公司及其许可者版权所有,保留一切权利。 非经本公司书面许可,任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部, 并不得以任何形式传播。本文档中的信息可能变动,恕不另行通知。

目 录
-----

1 简介1
2 配置前提1
3 事件审计配置举例1
3.1 应用需求1
3.2 配置注意事项1
3.3 使用版本1
3.4 配置步骤1
3.4.1 网络配置1
3.4.2 监听数据库配置3
3.4.3 配置数据库审计规则5
3.4.4 配置事件响应
3.5 验证配置10
4 报表中心配置举例
4.1 应用需求11
4.2 配置注意事项11
4.3 使用版本11
4.4 配置步骤11
4.5 验证配置16
5 配置管理举例
5.1 应用需求
5.2 配置注意事项16
5.3 使用版本16
5.4 配置步骤16
5.4.1 备份配置
5.4.2 恢复配置18
5.5 验证配置18
6 数据归档举例
6.1 应用需求
6.2 配置注意事项18
6.3 使用版本18
6.4 配置步骤18
6.5 验证配置19

ii

# **1** 简介

本文档介绍了 UNIS 数据库审计系统的配置举例。

## **2** 配置前提

本文档不严格与具体软、硬件版本对应,如果使用过程中与产品实际情况有差异,请参考相关产品 手册或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证。如果您已经对设备进行了配置,为了保证 配置效果,请确认现有配置和以下举例中的配置不冲突。 本文档假设您已了解数据库审计、策略等特性。

## 3 事件审计配置举例

## 3.1 应用需求

为了保障数据信息的安全,运维人员可通过数据库审计系统监控和审计用户对数据库中的数据库表、视图、序列、包、存储过程、函数、库、索引、同义词、快照、触发器等的创建、修改和删除等,分析 SQL 操作语句。通过设置的规则,智能的判断出违规操作数据库的行为,并对违规行为进行记录、报警,及时地发现针对数据库的违规操作行为。

## 3.2 配置注意事项

- 短信通知需短信猫设备支持;
- 邮件通知中不同的邮箱类型需设置不同的服务器地址。

## 3.3 使用版本

本举例是在 UNIS i-Ware Software, Version 1.10, ESS 6201P01 版本上进行配置和验证的。

## 3.4 配置步骤

## 3.4.1 网络配置

- (1) 电脑终端通过交叉线直连设备第二网口(网卡 2,即 GE0/1);
- (2) 打开浏览器, 输入地址: https://1.0.0.1, 打开 WEB 登录页面;
- (3) 使用 sys 帐号登录数据库审计系统;
- (4) 点击左侧菜单栏的"系统管理"-"网络配置",打开"网络配置"页面;

(5) 配置管理口(网卡1,即GE0/0)的IP地址,在面板模式页面上,鼠标放置于第一个网口上时出现设置修改IP项。

### 图3-1 修改 IP-面板模式

01	IGRE FREE APRE						
	✔ 配置生效 美板模式	隶称模式					
		10008A5	iE-X				
	101 MM 101	MM.	MM N	M MM	MM.		
					15		
	ا لو لو	31					
	0	18/100/1000	BASE-T		7		
>	说酬纸:GE0/0						
	9811952 (911) 19802 (183.1.1.53						
	子网络码:255.255.255.0						
	<b>股以同</b> 死:103.1.1.1						
	勝吹登録 ( 317.49 M/B						
	■45篇:0% ● 28/9822						

在表格模式下,鼠标置于第一个网口,右键点击出现设置修改 IP 项。

## 图3-2 修改 IP-表格模式

✓ #28	TOPOSE REPORT	大学会社							
0 (1999-1	的建度服装条件的操作								
	同卡属	28	HCH2	PIER	子用掩藉	数以現所	HCO.	追求がの	2010+
1	用+1	GEO/O		183.1.1.53	255 255 255 0	183.1.1.1	318.00 MB	2.9	
2	用42	GEO/1	E 2040	1.0.0.1	255.255.0.0		2.61 Milli	8.9	
	IR40	GE0.2	90	113.1.1.111	255.255.255.0		0.00 108	80.77	

配置好 IP、子网掩码和网关后,点击确定按钮。

#### 图3-3 IP 配置界面

设	置/修改IP		– □ ×
	网卡名:	网卡1	
	IP地址:	183.1.1.53	
	子网掩码:	/24(255.255.255.0)	-
	默认网关:	183.1.1.1	
		确定	取消

最后需点击配置生效按钮,使得修改的配置生效。 注意事项:监听网卡建议不设置 IP。

### 3.4.2 监听数据库配置

- (1) 打开浏览器, 输入前面配置的管理 IP 地址, 打开登录页面;
- 图3-4 Web 登录界面

用户名		
密 码		
🗖 记住用户名		
	登录	

- (2) 使用 sec 帐号登录数据库审计系统;
- (3) 点击左侧菜单栏的"策略中心"-"监听配置",打开"监听配置"页面;

#### 图3-5 监听配置

	_						
😡 监控中心 🗸	☆ 运行状态	5 监听配3	<b>z</b> ×				
■ 审计中心 、	业务系	统配置	中间件服务器配置	应用审计配置 指定源IP审计			
幽 报表中心 →	* 添加	● 修改	1 删除				
😂 策略中心 🔷			好杰	山在天松々物	新聞使業可		
▶ 监听配置			10.00	77.92.3499.02494	奴贻冲关王	-2-10.04638694-3	
事件定义		1	启用	oracle	Oracle	自动识别	
对象管理 客户端信息		2	启用	mssql	SQLServer	自动识别	
敏感信息		3	启用	mysql	MySQL	自动识别	
事件响应 三层关联 ) (品給潮期回		4	启用	dfgdfgdfhgdfghdfgdfgbdf gbdfgdf	Oracle	自动识别	
交换机信息		5	停用	test	Oracle	自动识别	
豪 系统管理 <		6	启用	数据库数据库数据 库数据库	DM	自动识别	
19 31 32		7	启用	sybase	Sybase	自动识别	
星期二 2018-01-16		8	启用	db2	DB2	自动识别	
硬盘 已用:2.6768 献余:557.7268 预计可用:25959天 健康状态:正常							

(4) 在"业务系统配置"配置页中,点击"添加"按钮,弹出"添加业务系统"窗口;图3-6 添加业务系统-未填写

添加业务系统西	233					$-\Box \times$
业务系统名称:						
状态:	启用	<b>▼</b>	嗣策略:	自动识别	-	
数据库:	主流数据库	•	类型:	Oracle	•	
IP地址:			端口:	1521		-
	添加 返回值配置	1				
					确定	取消

- (5) 在弹出的窗口中进行数据库监听配置,其中:
  - 。 业务系统名称可以任意填写。
  - 。 状态设置为启用。
  - 。 编码策略可以选择自动识别或者是对应的编码类型。
  - 数据库有主流数据库、国产数据库和专用数据库,选择不同项目,类型中出现不同的数据 库类型选择项。
  - 。 类型选择为对应的数据库类型,本例为 MySQL 数据库。
  - 。 IP 填写数据库服务器 IP,本例为 183.1.0.154。
  - 。端口填写数据库服务器端口,本例为3306。

#### 图3-7 添加业务系统-已填写

添加业务系统						– □ ×
业务系统名称:	MySQL					
状态:	启用	•	编码策略:	自动识别	•	
数据库:	主流数据库	•	类型:	MySQL	•	
IP地址:	183.1.0.154		端口:	3306		-
	添加					
					确定	取消

(6) 配置完成后,点击"确定"按钮,完成数据库监听配置。

## 3.4.3 配置数据库审计规则

(1) 打开浏览器,输入前面配置的管理 IP 地址,打开登录页面;使用 sec 账户登录数据库审计系统;点击左侧菜单栏的"策略中心"-"事件定义",打开"事件定义"页面;

### 图3-8 事件定义

☞ 监控中心 🔹	▲ 运行状态	事件定义	×											
■ 审计中心 、	数据库店	用规则	应用服务器	#规则										
屾 报表中心 →	1 添加	₽ 修改	<b>11</b> 1119:	<b>∅</b> 清空規則	:■保存規則排序	🔊 上传规则文件	各份规则	▲ 备份规则文件管理	《 清空单条规则触发命中数	( 💣 清空所有规则)	成发命中数			
😂 策略中心 🗸 🗸						规则名			餉发念中教	网络探索	状态	动作	#0.0¢	描述
监听配置	_					100-04			and the					-
▶ 事件定义		1		P	录像测试				702	高可疑	可用	记录		
对象管理 客户端信息		2		P	医院统计药方表				39372	高可疑	可用	记录		
敏感信息		3		P	test_高可疑事件				114	高可疑	可用	记录		
事件明显 三层关联		4		P	sqlServer数据库				0	高可疑	可用	记录		
入侵检测规则		5		P	oracle数据库规则				0	高可疑	可用	记录		
豪 系统管理 〈		6		P	东软统方规则				0	高可疑	可用	记录		
¢		7		P	东软_工号验证				0	高可疑	不可用	记录		
19 33 45		8		P	执行时长大于20s				0	高可疑	可用	记录		
星期二 2018-01-16		9		ρ	东软_工号				0	高可疑	可用	记录		
硬盘		10		ρ	验证设置为统方				0	高可疑	可用	记录		
已用: 2.8768  動余: 557.7268		11		P	drhis_统方工号				0	高可疑	可用	记录		
預计可用: 25959天		12		P	低可擬專件验证				0	低可疑	可用	记录		
健康状态:正常		13		P	test_中可疑事件				4872	中可疑	可用	记录		
		14		P	中文表触发验证				0	中可疑	可用	记录		
		15		p	统方事件test				0	高可疑	可用	记录		

- (2) 在"数据库应用规则"配置页中,点击"添加"按钮,弹出"增加数据库应用规则"窗口;
- (3) 在弹出的窗口中进行数据库审计规则配置;

#### 图3-9 事件定义具体配置

数据科	应用规则 应用	服务器规则	J									
🎽 添加	增加数据库应用	规则							_ □ ×	备份规则文件管理	🚿 清空单条规则触发命中数	🛛 🚿 清空所有规则
	常规设置								^		触发命中数	风险级别
	规则名:	acb									702	高可疑
	规则状态: 规则描述:	可用	▼ 风 <u>₿</u>	金级别:	高可疑	*	规则动	作:记录	<b>▼</b>		39372	高可疑
	一家白逆舳岩条件	公署									114	高可疑
	时间范围:	= *	请选择:					• +				高可疑
	客户端地址:	or 🔻	请选择:					• +			0	高可疑
	计算机名:	or 🔻	请选择:					• +				高可疑
	数据库用户名: 应用程序名:	or •	请选择:					• +			0	高可疑
	操作表名:	or 🔻	请选择:					• +				高可疑
	统计时长 : 操作方式 ·	> •	NaN 清洗择 ·	小时		天		月			0	高可疑
	操作内容:	or 🔹	请选择:					• +				高可疑
		增加出	<b>删除</b> 操作	内容(量	最多加5行)	)			~		0	高可疑
								确定	取消	J		

(4) 配置完成后,点击"确定"按钮,完成数据库审计规则配置;

数据库规则配置举例如下:

常规设置

- 规则名: test。
- 规则状态:可用。
- 风险级别:高可疑。
- 规则动作:记录。
- 规则描述: 查看每周二早上 8 点到下午 18 点 101.1.12.2 主机对 183.1.0.154 数据库服务器上的数据库进行查询操作的情况。

客户端触发条件设置

- 时间范围=08:00-18:00 每周周二。
- 客户端地址: Or: 101.1.12.2。
- 操作方式: Or: select。

服务端触发条件设置

- 服务端地址: 183.1.0.154。
- 记录返回值:记录,记录不超过4096字节。

### 图3-10 增加数据库应用规则

增加数据库应用	规则	– 🗆 ×
常规设置		<b>^</b>
规则名:	test	
规则状态:	可用 ▼ 风险级别: 高可疑 ▼ 规则动作: 记录	-
规则描述:		车服
一客户端触发条件计		
时间范围:	= ▼ 每周二8点到18点 × +	
客户端地址:	or • 101.1.12.2 × • +	
计算机名:	or ▼ 请选择: + +	
数据库用户名:	or ▼ 请选择: ▼ +	
应用程序名:	or ▼ 请选择: ・ +	
操作表名:	or ▼ 请选择: ・ +	
操作方式:	or 🔻 select 🗙 🔹 +	
操作内容:	or ▼ 请选择: ・ +	
	<b>增加 删除</b> 操作内容(最多加5行)	
统计时长:	> <b>▼</b> /小时 <b>▼</b>	-
	确定	取消
统计时长:	> ▼	
高级匹配:	?	
一服労)病肥友条件)		
服务端地址:	or • 183.1.0.154 × • +	
数据库名:	or ▼ 请选择: • +	
错误代码:	or ▼ 请选择: ▼ +	
执行结果:		
记录返回值?:	▼记录,记录不超过 4096 字节	
执行时长:	> ▼ 秒	
触发阈值:	次/分钟	
	确定	取消

## 3.4.4 配置事件响应

在"策略中心"-"事件响应",在"事件响应"页面中,系统将识别到的事件分三个等级:高可疑、中可疑、低可疑三级。响应策略主要有:windows报警、syslog告警、发送邮件、短信猫四种。

#### 图3-11 事件响应

☆ 运行状态 事件响应 ×		
风险响应策略 响应策略	配置	
✔ 修改		
	可疑程度	响应策略
1	低可疑	无动作
2	中可疑	无动作
3	高可疑	无动作
¢.		

## 1. 风险响应策略

为各类风险事件设置统一响应策略,并以列表形式展示设置结果。选择某类可疑程度后,后点击"修改"按钮,可修改该可疑类的响应策略。

#### 图3-12 修改风险响应策略

修改风险响应策略	– □ ×
级别描述:高可疑	
□ syslog □ SNMP 预警动作组:□ windows消息框 □ 邮件 □ 录像	
确定	取消

### 2. 响应策略配置

响应策略配置主要是配置各类响应策略的参数。 响应策略配置举例如下:

Windows 报警配置

- IP 地址: 10.5.8.244。
- 发送最小时间间隔(分钟): 60。
- 保存配置后选择测试。

#### 图3-13 Windows 告警配置

▼ Windows告答配置		
IP地址:	10.5.8.244	<b>Ø</b>
发送最小时间间隔(分钟):	60	0
	测试 保存配置	

syslog 告警配置

- IP 地址: 10.5.8.244。
- 端口:514。

## 图3-14 Syslog 告警配置

▼ syslog告警配置		
IP地址:	10.5.8.244	0
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;	514	0
	测试 保存配置	

邮件服务器配置

- DNS 服务器: 114.114.114.114。
- 邮件服务器地址: smtp.exmail.qq.com。
- 发件人地址: 1126631187@qq.com。
- 密码:。
- 发送最小时间间隔(分钟): 60。
- 收件人地址: 1126631187@qq.com;6237485866@qq.com。

## 图3-15 邮件服务器配置

▼ 邮件服务器配置		
DNS服务器:	114.114.114.114	0
邮件服务器地址:	smtp.exmail.qq.com	0
发件人地址:	1126631187@qq.com	0
密码:	•••••	
发送最小时间间隔(分钟):	60	0
收件人地址:	1126631187@qq.com;6237485866@qq.com	<b>S</b>
	测试 保存配置	

短信猫配置

- 启用:打钩。
- 电话号码: 15705954758。
- 保存配置后选择测试。

## 图3-16 短信猫配置

▼ 短信猫配置	
启用: ☑	
电话号码: 15705954758	0
测试 保存配置	

#### 风险响应策略

- 高可疑响应策略: windows 告警、syslog。
- 中可疑响应策略:邮件。

#### 图3-17 风险响应策略

☆ 运行状	态 报表任务 × <b>事件响应</b> ×		
风险	响应策略 响应策略配置		
N 183			
		可疑程度	响应策略
	1	低可疑	无动作
	2	中可疑	邮件服务器
	3	高可疑	syslog告罄,windows告罄

## 3.5 验证配置

- (1) 对数据库进行操作,触发审计规则;
- (2) 在"审计中心"-"语句查询"页面的实时语句能查询到语句数据;
- (3) 在"监控中心"-"事件查看"页面中能查询到根据预设定的规则产生的事件;
- (4) 各级别可疑事件能够按既定的告警方式发送日志信息。

## 图3-18 验证 Windows 消息框

信使服务	×
从 GUEST 到 2017-12-25 20:40:27 上 PC-20110915JTVB 的消息	
尊敬的用户, 从 2017-12-26 16:51:09 到 2017-12-26 16:56:09,共有 3 条规则被触发 2613 次,详情请登陆安全审计系统查考	

#### 图3-19 验证 Syslog 告警



#### 图3-20 验证邮件告警

尊敬的用户:

从 2018-02-02 17:43:39 到 2018-02-02 17:48:39,安全审计系统检测到您的系统存在风险,共有 1 条规则被触发 4 次,具体如下:

1.规则名: oi90(规则 ID: 2289177976) 被触发 4 次; 详情请登陆安全审计系统查看。

发送者: 安全审计系统(183.1.1.53) 发送时间: 2018-02-02 17:48:39

## 4 报表中心配置举例

## 4.1 应用需求

报表功能是审计日志大数据系统化、可视化分析的具体表现。UNIS 数据库审计系统可提供根据安 全经验和行业需求预定义的报表模板和审计报告,如审计设备自身健康状态分析报告、特权账号与 异常时段分析报告、业务流量分析报告、塞班斯(SOX)法案数据库安全审计符合性报告等等。通 过报表功能中的审计报告、周期报送等,直观体现了审计日志和风险分析中数据库安全趋势,帮助 安全管理人员更加便捷、深入的剖析数据库运行风险。

## 4.2 配置注意事项

- 目前系统默认会在每天的 00:00-07:00 期间生成报表。
- 可将流量周期统计报表添加到"监控中心"-"流量钻取"中展示,但要求"报表对象"列表 中的统计对象最多两种。

## 4.3 使用版本

本举例是在 UNIS i-Ware Software, Version 1.10, ESS 6201P01 版本上进行配置和验证的。

## 4.4 配置步骤

报表任务,是生成报表的依据,包含两种类型:自定义和系统默认。自定义报表任务,是系统根据 用户制定的任务生成符合条件的报表;系统默认提供了七个报表任务,生成的报表也可以在"监控 中心"-"流量钻取"中查看。

报表任务界面主要操作有:查看报表、新建报表、编辑报表、中止报表、删除报表、导入报表配置、 导出报表配置等功能。 报表任务配置举例如下:

#### 1. 流量周期统计报表

例如:对数据库用户名进行统计,排除 y(如: ktrans)和 z(如: AHSIMIS)帐号。

- 报表类型:流量周期统计报表。
- 报表名称:数据库用户名排除 yz 统计。
- 展示方式:按排名展示。
- 报表对象:数据库用户名 not ktrans;数据库用户名 not AHSIMIS,点击"确定"按钮。

#### 图4-1 新增流量周期性报表

新増报表		- 🗆	×
常规参数			-
报表类型:	流量周期统计报表		
报表名称:	数据库用户名排除yz统计		
报表描述:			
发送邮件:			
目标地址:			
展示方式			E
展示方式:	◎ 按时间走势展示 💿 按排名展示 📄 添加到"流量钻取" 累计次数:	7	
周期类型:	日 ▼ 排序方式: 升序 ▼ 排名位数: 10	]	
报表对象			
	数据库用户名 ! ktrans		
	数据库用户名 ▼ not ▼ AHSIMIS ▼		
对象选择:			*
	确定。	取消	

#### 2. 流量一次性报表

例如:在7号当天0点到15点时间段中,除10.4.8.202 主机外,统计主机对数据库的访问量。

- 报表类型:流量一次性报表。
- 报表名称: 主机数据库访问量排除 10.4.8.243。
- 时间范围: 2017-12-07 00:00 到 2017-12-07 15:15。
- 展示方式:按排名展示。
- 报表对象:源IP not 10.4.8.243;数据库名=全部,点击"确定"按钮。

## 图4-2 新增流量一次性报表

新増报表			-	- 🗆 ×
常规参数				<b>^</b>
报表类型:	流量一次性报表	•		
报表名称:	排除10.4.8.243的登录数据库统计			
时间范围:	2017-12-07 00:00 到	2017-12-07 15:15		
报表描述:				
发送邮件:	■ 是否发送			
目标地址:				=
展示方式	● 按时间走势展示 ● 按排名	展示 累计次数:		
精确度:	小时 1 排序方式: 升序	▼ 排名位数: 10		
报表对象			•	
	☞IF :10.4.0.243 数据库名 全部		~	
1		× ±=	确定	取消

## 3. 特权周期跟踪类报表

- 报表类型:特权周期跟踪类报表。
- 报表名称: Rollback 等操作方式统计。
- 特权操作方式: ROLLBACK、DROP TABLE、CREATE TABLE、REVOKE, 点击"确定"按钮。

### 图4-3 新增特权周期类报表

新増报表 □	×
常规参数	•
报表类型: 特权周期跟踪类报表 ▼	
报表名称: Rollback等操作方式统计	
报表描述:	
发送邮件: 🔄 是否发送	
目标地址:	
展示方式 精确度: 日 ▼ 排名位数: 10	ш
特权操作方式 特权操作方式:   ROLLBACK × DROP TABLE × CREATE TABLE ×     REVOKE ×	
确定取消	

## 4. 特权一次性跟踪类报表

- 报表类型:特权一次性跟踪类报表。
- 报表名称: Alter\_Role 等操作方式统计。
- 特权操作方式: ALTER ROLE、DROP VIEW、CREATE USER、DROP INDEX、DROP TABLE、CREATE,点击"确定"按钮。

## 图4-4 新增特权一次性报表

增加报表		– □ ×
常规参数一		
报表类型:	特权一次性跟踪类报表	
报表名称:	Alter_Role等操作方式统计	
时间范围:	2018-01-16 00:00     到     2018-01-16 18:45	
报表描述:		
发送邮件:	■ 是否发送	=
目标地址:		
展示方式		
排名位数:	10	
	<u></u>	
15120361 F73.		
特权操作方	ALTER ROLE × DROP VIEW × CREATE USER ×	
	DROP INDEX × DROP TABLE × CREATE ×	
		+
	确定	取消

## 5. 流量钻取展示配置

流量周期统计报表,支持添加到"监控中心"-"流量钻取"中展示。

## 图4-5 展示方式

展示方式		
展示方式: 🔘 按时间走势展示	◎ 按排名展示	☑ 添加到"流量钻取" 累计次数:
周期类型: 日 ▼	排序方式: 升序	▼ 排名位数: 10

## 6. 报表邮件发送配置

四种报表类型均支持自动发送邮件。

图4-6 常规参数

常规参数		
报表类型:	流量周期统计报表	
报表名称:	数据库用户名排除yz统计	
报表描述:		
发送邮件:	▼ 是否发送	

## 4.5 验证配置

- (1) 除了一次性报表可立即查看外,其他制定的报表隔天能够在"报表任务"和"报表查看"页面中查 看。
- (2) 添加"流量钻取"展示后,可在"监控中心"-"流量钻取"页面查看到该报表的相关展示。
- (3) 配置邮件发送后,隔日可在收件人邮箱中查看是否收到报表邮件,报表以压缩包形式发送。

## 5 配置管理举例

## 5.1 应用需求

在用户环境中配置数据的重要性不言而喻,为防止系统出现操作失误或系统故障导致数据丢失等问题,因此,需精细化的配置管理,能将全部或部分配置数据集合恢复到设备。UNIS 数据库审计系统支持对审计配置全集和分量(模块)的配置,执行备份与还原。当用户发生设备损坏,更换备机等情况时,能快速进行审计系统配置还原,实现无损更换使用。方便运维人员对审计系统维护,快速还原某个模块的某个配置,实现精细化的配置管理。

## 5.2 配置注意事项

- 在不同环境选择恢复网络配置时,应注意设备 IP 冲突,避免发生无法登录的情况。
- 配置管理主机时,建议先配置自身 PC 的 IP 地址,避免发生无法登录的情况。

## 5.3 使用版本

本举例是在 UNIS i-Ware Software, Version 1.10, ESS 6201P01 版本上进行配置和验证的。

## 5.4 配置步骤

## 5.4.1 备份配置

(1) 使用 sys 帐号登录数据库审计系统,点击左侧菜单栏的"系统管理"-"配置备份",打开"配置备份"页面;

#### 图5-1 配置管理

● 600331 ●	全国行时志	ista <b>kritt</b> ×						
● 然助中心 <	M nones		I BRARE DINER DINE! DRIN					
A M M M     M			配置集份名	1400 B				
用机配置		102.7						
20.07-95.08	0	1	con1512111073	2017 12 16 10 14 11				
运行日本		2	cont1512368423	2017.12.18 10:16.58				
日本地位		з	conf1514518529	2017 12 29 11 35 30				
· 628818			con/1515393389	2018.01.08 15:31.56				
5408		5	cont1515395241	2018 01.06 15 07 21				
6.9.1.51		6	cont1515514248	2018.01.10.00.10.48				
10 07 20		7	cont1515656072	2018 01 11 15 34 33				
2018-01-17 4		8	conf1515999425	2018.01.15.14.57.07				
na .		9	conf1516001564	2018 01 15 15:32 44				
00 2.6768 Mile: 557.7168		10	conf1516001821	2018.01.15 15:37:03				
25959天 1988年: 25959天								

- (2) 点击"备份当前配置"按钮,弹出"备份当前配置"窗口;
- (3) 对系统中各配置项进行备份,可选配置备份项包括 SQL 模版、报表任务、事件报表过滤规则、 监听配置、事件定义、对象管理、客户端信息、敏感信息、事件响应、入侵检测规则、交换机 信息、用户管理、数据归档参数、日志响应、网络配置、管理主机、引擎相关配置、数据库相 关配置。选择备份项后,点击"确定"按钮,系统提示是否备份,继续点击"确定"按钮后, 系统进行配置备份。

### 图5-2 备份当前配置

▲ 运行状态	× 配置管理					
🅈 备份配置	▶ 导入配置	达 下载配置 📗	删除配置	恢复配置	へ 恢复出)	备份当前配置 — □ >
				配置备	份名	备注
	1			conf151	2111073	填写备注信息
	2			conf151	2369423	审计中心
	3			conf151	4518529	□ SQL模板
	4			conf151	5393389	报表中心
	5			conf151	5395241	□ 报表任务 □ 事件报表过滤规则
	6			conf151	5514248	策略中心
	7			conf151	5656072	🗌 监听配置 🗌 事件定义 🗌 对象管理 🗌 客户端信息 🗌 敏感信息
	8			conf151	5999425	🗌 事件响应 🔲 入侵检测规则 🔲 交换机信息
	9			conf151	6001564	系统管理
	10			conf151	6001821	□ 用户管理 □ 数据归档参数 □ 日志响应 □ 网络配置
						只と配置 □ 引擎相关配置 □ 数据库相关配置
						柳正 取消

## 5.4.2 恢复配置

配置恢复能将审计系统的配置恢复到之前的某个版本。

- (1) 导入之前的备份配置文件;
- (2) 选择某个配置备份记录,点击"恢复配置"按钮,在弹出的"选择要恢复的配置"窗口中选择 相应项,然后点击"确认"按钮;
- (3) 系统提示是否回复配置,继续点击"确定"按钮后,系统进行配置恢复。当前的系统配置将恢 复到该配置。默认不选择网络配置、管理主机的配置,恢复可能导致系统无法访问,需谨慎选 择。

## 5.5 验证配置

- (1) 成功备份配置。
- (2) 成功恢复配置。
- (3) 配置能够成功下载、导入。
- (4) 逐一查看各个配置是否准确恢复。

## 6 数据归档举例

## 6.1 应用需求

审计系统自带的硬盘容量有限,审计的历史数据永久保存,系统会根据硬盘剩余空间动态删除最早的历史数据。因此,系统支持将储存的历史归档数据外传,实现归档数据的无限扩展和永久存储。

## 6.2 配置注意事项

- 实现数据归档的外传,需先配置好归档参数。
- 设置外传的服务器上要有足够的磁盘空间存储归档文件。

## 6.3 使用版本

本举例是在 UNIS i-Ware Software, Version 1.10, ESS 6201P01 版本上进行配置和验证的。

## 6.4 配置步骤

归档参数配置

- (1) 使用 sec 帐号登录数据库审计系统,点击左侧菜单栏的"系统管理"-"数据归档",打开"数据 归档"页面;
- (2) 点击"归档参数配置"分项页;
- (3) 设置归档文件外传功能的开启以及外传服务器的相关参数设置;

#### 图6-1 数据归档

金 运行状态 数据归档 ×								
归档文件管理 归档参数配置 回档数据挂载配置								
▼ 基础配置								
是否外传归档文件:	■ 是							
服务器类型:	磁盘共享    ▼							
服务器IP:	10.5.8.65							
服务器目录:	share	0						
用户名:	administrator							
密码:	•••••							
	保存配置							

- (4) 填写参数后,点击"保存配置"按钮,系统能自动检测配置是否正确,如有错误,根据提示进行 修改,正确后会保存配置;
- (5) 系统默认每天凌晨两点执行归档操作。

## 6.5 验证配置

系统正常运行后,隔日到设置的外传服务器磁盘目录上查看,是否有归档文件生成。