

UNIS A2000-G 系列运维审计系统

典型配置举例

北京紫光恒越网络科技有限公司 http://www.unishy.com

资料版本: 5W100-20180521

Copyright © 2018 北京紫光恒越网络科技有限公司及其许可者版权所有,保留一切权利。

未经本公司书面许可,任何单位和个人不得擅自摘抄、复制本书内容的部分或全部,并不得以任何 形式传播。

UNIS 为北京紫光恒越网络科技有限公司的商标。对于本手册中出现的其它公司的商标、产品标识 及商品名称,由各自权利人拥有。

由于产品版本升级或其他原因,本手册内容有可能变更。紫光恒越保留在没有任何通知或者提示的 情况下对本手册的内容进行修改的权利。本手册仅作为使用指导,紫光恒越尽全力在本手册中提供 准确的信息,但是紫光恒越并不确保手册内容完全没有错误,本手册中的所有陈述、信息和建议也 不构成任何明示或暗示的担保。

前言

本配置指导介绍了 UNIS A2000-G 系列运维审计系统的常用典型配置举例及其配置步骤。前言部分包含如下内容:

- 读者对象
- <u>本书约定</u>
- <u>技术支持</u>
- 资料意见反馈

读者对象

本手册主要适用于如下工程师:

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格式	意义
粗体	命令行关键字(命令中保持不变、必须照输的部分)采用加粗字体表示。
斜体	命令行参数(命令中必须由实际值进行替代的部分)采用斜体表示。
[]	表示用"[]"括起来的部分在命令配置时是可选的。
{ x y }	表示从多个选项中仅选取一个。
[x y]	表示从多个选项中选取一个或者不选。
{ x y } *	表示从多个选项中至少选取一个。
[x y] *	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由"#"号开始的行表示为注释行。

2. 图形界面格式约定

格式	意义
<>	带尖括号"<>"表示按钮名,如"单击<确定>按钮"。
[]	带方括号"[]"表示窗口名、菜单名和数据表,如"弹出[新建用户]窗口"。
1	多级菜单用"/"隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方,这些标志的意义如下:

▲ 警告	该标志后的注释需给予格外关注,不当的操作可能会对人身造成伤害。
1 注意	提醒操作中应注意的事项,不当的操作可能会导致数据丢失或者设备损坏。
₩ 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
💕 说明	对操作内容的描述进行必要的补充和说明。
🥽 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下:

	该图标及其相关描述文字代表一般网络设备,如路由器、交换机、防火墙等。
ROUTER	该图标及其相关描述文字代表一般意义下的路由器,以及其他运行了路由协议的设备。
Real Print	该图标及其相关描述文字代表二、三层以太网交换机,以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的 无线控制引擎设备。
((***))	该图标及其相关描述文字代表无线接入点设备。
TO	该图标及其相关描述文字代表无线终结单元。
(1)	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
))))	该图标代表发散的无线射频信号。
~	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
Brabingo	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插 卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例,并不代表设备上实际具有此编号的端口,实际使用中请以设备上存在的端口编号为准。

技术支持

用户支持邮箱: <u>zgsm_service@thunis.com</u> 技术支持热线电话: 400-910-9998(手机、固话均可拨打) 网址: <u>http://www.unishy.com</u>

资料意见反馈

如果您在使用过程中发现产品资料的任何问题,可以通过以下方式反馈: E-mail: zgsm info@thunis.com 感谢您的反馈,让我们做得更好!

AD&LDAP 认证配置举例

Copyright © 2018 北京紫光恒越网络科技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。



1 简介1
2 名词解释1
3 配置前提2
4 配置举例3
4.1 组网需求3
4.2 系统版本要求
4.3 Windows(AD) Digest-MD5 认证 ······3
4.3.1 收集信息
4.3.2 配置步骤
4.3.3 验证配置
4.4 Windows(AD)simple认证
4.4.1 收集信息6
4.4.2 配置步骤
4.4.3 验证配置
4.5 Ldap simple认证10
4.5.1 收集信息10
4.5.2 配置步骤
4.5.3 验证配置
4.6 Ldap用户批量导入13
4.6.1 新建批量导入13
4.6.2 编辑批量导入规则14
4.6.3 提交批量导入规则 15

1 简介

1. LDAP

LDAP 是轻量目录访问协议,英文全称是 Lightweight Directory Access Protocol,简称为 LDAP。 目录服务是一种特殊的数据库系统,其专门针对读取,浏览和搜索操作进行了特定的优化。目录一 般用来包含描述性的,基于属性的信息并支持精细复杂的过滤能力。目录一般不支持通用数据库针 对大量更新操作操作需要的复杂的事务管理或回卷策略。而目录服务的更新则一般都非常简单。这 种目录可以存储包括个人信息、web 链接、jpeg 图像等各种信息。为了访问存储在目录中的信息, 就需要使用运行在 TCP/IP 之上的访问协议—LDAP。

2. AD

AD 是 Active Directory 的缩写, AD 应该是 LDAP 的一个应用实例。比如: windows 域控的用户、 权限管理应该是微软公司使用 LDAP 存储了一些数据来解决域控这个具体问题,只是 AD 顺便还提 供了用户接口,也可以利用 ActiveDirectory 当做 LDAP 服务器存放一些自己的东西而已。比如 LDAP 是关系型数据库,微软自己在库中建立了几个表,每个表都定义好了字段。显然这些表和字段都是 根据微软自己的需求定制的,而不是 LDAP 协议的规定。然后微软将 LDAP 做了一些封装接口,用 户可以利用这些接口写程序操作 LDAP,使得 ActiveDirectory 也成了一个 LDAP 服务器。

2 名词解释

1. 条目

条目,也叫记录项,是 LDAP 中最基本的颗粒,就像字典中的词条,或者是数据库中的记录。通常 对 LDAP 的添加、删除、更改、检索都是以条目为基本对象的。

2. DN

每一个条目都有一个唯一的标识名,如

dn="cn=baby,ou=marketing,ou=people,dc=mydomain,dc=org"。通过 DN 的层次型语法结构,可以 方便地表示出条目在 LDAP 树中的位置,通常用于检索。

3. Basedn

LDAP 目录树的最顶部就是根,也就是所谓的"Base DN",如"dc=mydomain,dc=org"。 在运维审计系统的 BaseDN 是指,以当前的组织作为根,搜索当前组织的范围。

4. 属性

每个条目都可以有很多属性(Attribute),比如常见的人都有姓名、地址、电话等属性。每个属性都有名称及对应的值。

5. 用户Filter

运维审计系统的用户 Filter 是指,通过属性来过滤用户。

例如: (&(objectclass=person)(sAMAccountName=testuser)),代表过滤出 objectclass 为 person 并且 sAMAccountName 为 testuser 的用户。

6. Simple方法

Simple 需用绑定查询用户及口令,配置相对灵活复杂,几乎所有的目录服务器都支持该验证方法。

7. Digest-md5 方法

仅需要知道 Idap 服务器的 FQDN 和 IP 地址既可,不需要绑定用户名和密码,配置方法相对简单。

8. 查询用户

在域控中,具有查询权限的用户。

3 配置前提

1. Windows (AD)

- 准备 Windows 域控主机一台。
- 准备 Windows 域控主机的相关信息: IP 地址、端口、计算机全名、查询用户、查询用户密码、 BaseDN、用户 Filter。
- 确保域控主机到运维审计系统的网络可达。

2. LDAP

- 准备 LDAP 服务器一台。
- 准备 LDAP 服务器的相关信息: IP 地址、端口、查询用户、查询用户密码、BaseDN、用户 Filter。
- 确保 LDAP 服务器到运维审计系统的网络可达。

3. AD/LDAP典型配置

- DIGEST-MD5 设置:
 - o 状态: 启用服务器1
 - 。 名称: Windows_AD
 - 。 方法: DIGEST-MD5
 - 。 服务器 1 全名: ad1.abc.com(AD(LDAP)服务器主机名全称)
 - 。服务器1地址: 192.168.6.200
 - 。 服务器 1 端口: 389
 - 服务器 2 全名: ad2.abc.com
 - 。服务器2地址: 192.168.6.201
 - 服务器2端□:389
- SIMPLE 设置:
 - o 状态: 启用服务器 1
 - 。 名称: Windows_AD
 - 。 方法: SIMPLE
 - 。服务器1地址: 192.168.6.200
 - o 服务器1端口:389
 - 。服务器 2 地址: 192.168.6.201
 - o 服务器 2 端口: 389
 - 。 查询用户 DN: CN=Administrator,CN=Users,DC=dep,DC=com
 - o 查询用户密码: 123456

- 。 用户 basedn: CN=Users,DC=dep,DC=com
- 。用户 Filter: (&(objectclass=person)(sAMAccountName={username}))

4 配置举例

4.1 组网需求

图1 AD/LDAP 认证网络图



4.2 系统版本要求

适用产品版本: ESS 6102

4.3 Windows (AD) Digest-MD5认证

4.3.1 收集信息

- Windows 域控主机 IP 地址。
- Windows 域控主机的计算机全名。(控制面板\系统和安全\系统\计算机全名)
- Windows 域控主机 AD 服务的端口号。

4.3.2 配置步骤

1. 登录具有超级管理员角色的用户。

2. 创建ldap认证方式。

进入"策略配置 > 身份验证",选择 ldap 协议,点击"创建"。

图2 创建 Idap 认证方式

基本控制 > 事件审计 >	策略配置 系统设置 > 工 ^编	管理 🖌 双人复核 🖌				
系统策略 告警事件 字符	终端 会话配置 身份验证 计	备密码 设备类型 部门配置 改密方式	式 密码代填 正代填脚本			
您的当前位置: 策略配置 > 身份验证						
协议: Idap 🖌	新建					
名称		协议	状态	z力作		
1 本地i	и́ш	native	启用	<u>设置</u>		

3. 编辑ldap认证方式。

- (1) 选择认证方法为 "DIGEST-MD5"。
- (2) 选择状态为: "启用服务器 1"。
- (3) 填写"名称"、"服务器1全名"、"服务器1地址"、"服务器1端口"几个字段。
 - o 名称:填写此 AD 认证的名称。
 - 。 服务器 1 地址: Windows 域控主机 IP 地址。
 - 。 服务器 1 全名: Windows 域控主机的计算机全名。
 - 。 服务器1端口: 如果留空, 默认为389端口。
- (4) 点击"确定",提交配置。

图3 配置 Idap 认证方式

方式:	ldap		
状态 :	启用服务器1	~	2
名称 :	AD_digest		
方法 :	DIGEST-MD5	~	1
服务器1全名:	dc1.test.com](包含域名的正式全	:名)
服务器1地址:	192.168.8.172		(服务器地址)
服务器1端口:			(留空表示缺省端口)
服务器2全名:			(包含域名的正式全名)
服务器 <mark>2</mark> 地址:			<mark>(服务器地址)</mark>
服务器2端口:			(留空表示缺省端口)
SSL:			
海土 田沢	HT 334		
佣正 里设	以间		

4. 创建ldap用户。

进入"基本控制>用户账号"。点击"新建用户"。

图4 创建 Idap 用户

基本	空制 事件审计 ·	✓ 策略配置 ✓ 系统	设置 🗸 工单管	管理 🖌 🕺 双ノ	人复核 Y						
用户帧	用户帐号										
您的当	您的当前位置: 基本控制 > 用户帐号										
新建用	新建用户 批量导入 批量修改 导出用户 状态:活动 🗸 身份验证: 🗸 部门: ROOT 🔽 过期帐号:										
	登录名」	<u>姓名</u>	部门	状态	密码期限	帐号期限	角色				
1	admin	缺省管理员	ROOT	活动	有效	有效	超级				
2	mibao	密码管理员	ROOT	活动	有效	有效					

(1) 选择"身份验证方式"为刚才配置的名称。

(2) 填写"登录名"、"真实姓名"、"部门"、"ldap 用户名"这几个字段。

o 登录名:登录运维审计系统的账户名。

。 真实姓名: 该账户名的真实用户。

o 部门:选择相应的部门。

。 Idap 用户名:绑定该登录名对应的 Idap 账户,如果不填,则默认此项为登录名。

(3) 点击"保存"。

图5 配置 Idap 用户信息

基本属性	高级属性	
状态:	○禁用 ●活动	
登录名 :	testuser *	• 🥝
真实姓名 :	测试	• 🔮
邮件地址:		
手机号码:		
部门:	ROOT 🗸 *	:
职位:		
工号:		
身份验证方式:	AD_digest	
ldap用户名:		
权限:	🗆 超级管理员 🗆 审计管理员 🗆 配置管理员 🗆]密码保管员 🗹 普通用户
	审计权限: 🗆 下载会话 🗆 键盘事件	
	(需要下载会话权限,必须勾选键盘事件权限)	
	保存	

5. 登录ldap用户。

图6 Idap 用户登录



4.3.3 验证配置

进入超级管理员账户。

(1) 选择"策略配置 > 身份验证",选择相应的 ldap 认证,点击"测试"。

图7 身份验证

基本控制 🖌 📑	5件审计 ~	策略配置	系统	☆ 设置 →	工单管理 🗸	双人复核 🗸					
系统策略 告警	事件 字符	好终端 会话	郵置	身份验证	设备密码	设备类型	部门配置	改密方式	密码代填	IE代填脚本	
您的当前位置:	您的当前位置: 策略配置 > 身份验证										
协议: Idap	协议: Idap 🗸 新建										
	名称	1			协议				状态		动作
1 本地认证				nativ	native			启用		<u>设置</u>	
2	2 Idap			ldap	ldap 启用 结			编辑测试删除			

(2) 填写需要验证的账户密码,选择相应的服务器,点击"确定"。



图9 登录成功

您的当前位置: 策略配置 > 身份验证 > LDAP登录测试 登陆测试成功

4.4 Windows (AD) simple认证

4.4.1 收集信息

- Windows 域控主机 IP 地址。
- Windows 域控主机 AD 服务的端口号。
- Windows 域控主机的查询用户的 DN (打开 "cmd",通过命令 "dsquery user -name [username]"查询)。
- Windows 域控主机查询用户的密码。
- 用户 basedn (希望从哪一层组织下查找)。
- 用户 Filter (系统通过什么属性过滤用户)。

4.4.2 配置步骤

1. 登录具有超级管理员角色的用户。

2. 创建ldap认证方式。

进入"策略配置 > 身份验证",选择 ldap 协议,点击"创建"。

图10 创建 Idap 认证方式

基本控制 🗸 事件审计	+ 🗸 🛱 策略配置 系统设置 🗸	工单管理 🗸	双人复核 ~					
系统策略 告警事件	字符终端 会话配置 身份验证	设备密码	设备类型	部门配置	改密方式	密码代填	IE代填脚本	
您的当前位置: 策略配置 > 身份验证								
协议: Idap	∠ 新建 ■							
	名称	协议				状态		动作
1	本地认证	native	e			启用		设置

3. 编辑ldap认证方式。

- (1) 选择认证方法为"SIMPLE"。
- (2) 选择状态为: "启用服务器 1"。
- (3) 填写"名称"、"服务器 1 地址"、"服务器 1 端口"、"查询用户 DN"、"查询用户密码"、 "用户 BaseDN"、"用户 Filter"几个字段。
 - 。 名称:填写此 Idap 认证的名称。
 - 。 服务器 1 地址: Windows 域控主机 IP 地址。
 - 。 服务器1端口: 如果留空, 默认为389端口。
 - 。 查询用户 DN: 具有查询权限的用户的 DN。
 - 。 查询用户密码: 查询用户密码。
 - 。 用户 BaseDN:希望从那一层组织下查找。
 - 用户 Filter:系统通过什么属性过滤用户。对于 windows 的域控可以通过
 "(&(objectclass=person)(sAMAccountName={username}))"过滤。其中{username}代表提交的变量,代表将来传入的用户名。
- (4) 第4步: 点击"确定", 提交配置。

图11 配置 Idap 认证方式

方式:	ldap	
状态:	启用服务器1 ~	2
名称:	ldap	
方法:	SIMPLE	[帮助] 1
服务器1地址:	192.168.8.172	(服务器地址)
服务器1端口:		(留空表示缺省端口)
服务器2地址:		(服务器地址)
服务器2端口:		(留空表示缺省端口)
查询用户DN:	CN=testuser,OU=IT,DC=test,DC=com	(如CN=Administrator,CN=Users,DC=example,DC=com)
查询用户密码:	•••••	
用户basedn:	OU=IT,DC=test,DC=com	(如CN=Users,DC=example,DC=com)
用户filter:	(&(objectclass=person)(sAMAccountName=	(如(&(objectclass=person)(sAMAccountName={username})))
SSL:		
确定重设	取消	

4. 创建ldap用户。

进入"基本控制 > 用户账号"。点击"新建用户"。

图12 创建 Idap 用户

基本挂	空制 事件审计	➤ 策略配置 ➤ 系统	· 近日 🗸 🖌 🖓 🖓	管理 🖌 🕺 🕅	人复核 ~			
用户帐号								
您的当	您的当前位置: 基本控制 > 用户帐号							
新建用户 批量导入 批量修改 导出用户 状态: 活动 🗸 身份验证: 🗸 部门: ROOT 🔽 过期帐号:								
	登录名↓	姓名	部门	状态	密码期限	帐号期限	角色	
1	admin	缺省管理员	ROOT	活动	有效	有效	超级	
2	mibao	密码管理员	ROOT	活动	有效	有效		

- (1) 选择"身份验证方式"为刚才配置的名称。
- (2) 填写"登录名"、"真实姓名"、"部门"、"Idap 用户名"这几个字段。
 - o 登录名:登录运维审计系统的账户名。
 - 。 真实姓名: 该账户名的真实用户。
 - o 部门:选择相应的部门。
 - o Idap 用户名:绑定该登录名对应的 Idap 账户,如果不填,则默认此项为登录名。
- (3) 点击"保存"。

图13 配置 Idap 用户

状态 :	○禁用 ●活动
登录名 <mark>:</mark>	testuser 🛛 * 🤡
真实姓名 <mark>:</mark>	测试 * 🥑
邮件地址:	
手机号码 :	
部门 :	ROOT 🗸 *
职位:	
工号:	
身份验证方式:	ldap 🗸
ldap用户名:	
权限:	🗆 超级管理员 🗆 审计管理员 🗆 配置管理员 🗆 密码保管员 🗹 普通用户
	审计权限: 🗆 下载会话 🗆 键盘事件
	(需要下载会话权限,必须勾选键盘事件权限)
	保存

5. 登录ldap用户。

图14 Idap 用户登录

帐 号: test	tuser	
密码: 👥	•••••	
	登录	

4.4.3 验证配置

进入超级管理员账户。

(1) 选择"策略配置 > 身份验证",选择相应的 ldap 认证,点击"测试"。

图15 身份验证

基本控制 > 事件電	计 🖌 策略配置	系统设置 🖌 工单管理	▶ 双人复核	•				
系统策略 告警事件	: 字符终端 会话配置	t 身份验证 设备密闭	円 设备类型	部门配置	改密方式	密码代填	IE代填脚本	
您的当前位置: 策略配置 > 身份验证								
协议: Idap	协议:Idap 🗸 新建							
	名称	t	议			状态		动作
1	本地认证	n	ative			启用		<u>设置</u>
2	ldap	k	lap			启用		编辑测试删除

(2) 填写需要验证的账户密码,选择相应的服务器,点击"确定"。

图16 配置账户密码

服务器:◉1 ○2	
用户名 : testuser]
密码: ●●●●●●●]
确定取消	

(3) 返回"登录测试成功"。

图17 登录成功

您的当前位置:策略配置 > 身份验证 > LDAP登录测试 登陆测试成功

4.5 Ldap simple认证

4.5.1 收集信息

- Ldap 服务器的 IP 地址。
- Ldap 服务器的 ldap 服务的端口号。
- Ldap 服务器的的查询用户的 DN。
- Ldap 服务器的查询用户的密码。
- 用户 basedn。(希望从那一层组织下查找)。
- 用户 filter。(系统通过什么属性过滤用户)。

4.5.2 配置步骤

1. 登录具有超级管理员角色的用户。

2. 创建ldap认证方式。

进入"策略配置 > 身份验证",选择 ldap 协议,点击"创建"。

图18 创建 Idap 认证方式

基本控制 ~	事件审计 🗸 策略配	置 系统设置 >	工单管理 ~	双人复核	•				
系统策略	告警事件 字符终端 会	会话配置 身份验证	设备密码	设备类型	部门配置	改密方式	密码代填	IE代填脚本	
您的当前位置	您的当前位置: 策略配置 > 身份验证								
协议: Idap	< 新建	1.1.1							
	名称		协议				状态		动作
1	本地认证		nativ	e			启用		<u>设置</u>

3. 编辑ldap认证方式。

- (1) 选择认证方法为"SIMPLE"。
- (2) 选择状态为: "启用服务器 1"。
- (3) 填写"名称"、"服务器 1 地址"、"服务器 1 端口"、"查询用户 DN"、"查询用户密码"、 "用户 BaseDN"、"用户 Filter"几个字段。
 - 。 名称: 填写此 Idap 认证的名称。
 - 。 服务器 1 地址: Ldap 服务器的 IP 地址。
 - 。 服务器1端口: 如果留空, 默认为389端口。
 - 。 查询用户 DN: 具有查询权限的用户的 DN。
 - o 查询用户密码: 查询用户密码。
 - 。用户 BaseDN:希望从那一层组织下查找。
 - 。 用户 Filter: 系统通过什么属性过滤用户。这里通过 cn 属性可以过滤出用户,所以使用 cn={username}。
- (4) 点击"确定",提交配置。

图19 配置 Idap 认证方式

方式:	Idap	
状态:	启用服务器1 🗸	
名称:	ldap	
方法 :	SIMPLE	[帮助]
服务器1地址:	192.168.8.139	(服务器地址)
服务器1端口:		(留空表示缺省端口)
服务器2地址:		(服务器地址)
服务器2端口:		(留空表示缺省端口)
查询用户DN:	cn=Manager,dc=test,dc=com	(如CN=Administrator,CN=Users,DC=example,DC=com)
查询用户密码:	•••••	
用户basedn:	ou=People,dc=test,dc=com	(如CN=Users,DC=example,DC=com)
用户filter:	cn={username}	(如(&(objectclass=person)(sAMAccountName={username})))
SSL:		

4. 创建ldap用户。

进入"基本控制 > 用户账号"。点击"新建用户"。

图20 创建 Idap 用户

基本排	空制 事件审计	✓ 策略配置 ✓ 系	统设置 🖌 工单的	管理 🖌 🕅 双	人复核 🖌			
用户帧	用户帐号							
您的当	您的当前位置: 基本控制 > 用户帐号							
新建序	新建用户 批量导入 批量修改 号出用户 状态: 活动 > 身份验证: > 部门: ROOT > 过期帐号: [
	登录名	<u>姓名</u>	部门	状态	密码期限	帐号期限	角色	
1	admin	缺省管理员	ROOT	活动	有效	有效	超级	
2	mibao	密码管理员	ROOT	活动	有效	有效		

- (1) 选择"身份验证方式"为刚才配置的名称。
- (2) 填写"登录名"、"真实姓名"、"部门"、"Idap 用户名"这几个字段。
 - o 登录名:登录运维审计系统的账户名。
 - 。 真实姓名: 该账户名的真实用户。
 - o 部门:选择相应的部门。
 - 。 Idap 用户名:绑定该登录名对应的 Idap 账户,如果不填,则默认此项为登录名。
- (3) 点击"保存"。

图21 配置 Idap 用户信息

状态 :	○禁用 ●活动
登录名 <mark>:</mark>	testuser 🔹 🏈
真实姓名 <mark>:</mark>	测试 * 🥑
邮件地址:	
手机号码 <mark>:</mark>	
部门:	ROOT ×*
职位:	
工号:	
身份验证方式:	ldap 🗸
ldap用户名:	
权限 <mark>:</mark>	🗆 超级管理员 🗆 审计管理员 🗆 配置管理员 🗆 密码保管员 🗹 普通用户
	审计权限: 🗆 下载会话 🗆 键盘事件
	(需要下载会话权限,必须勾选键盘事件权限)
	保存

5. 登录ldap用户。

图22 Ldap 用户登录



4.5.3 验证配置

进入超级管理员账户。

(1) 选择"策略配置 > 身份验证",选择相应的 ldap 认证,点击"测试"。

图23 身份验证

基本控制 > 事件审论	+ ~ 策略配置 系	統设置 🖌 工单管理	→ 双人复核 →					
系统策略 告警事件	字符终端 会话配置	身份验证 设备密码	码 设备类型	部门配置	改密方式	密码代填	IE代填脚本	
您的当前位置: 策略翻								
协议: Idap	协议: Idap 🚽 新建							
	名称	ŧ	办议			状态		动作
1	本地认证	n	native			启用		<u>设置</u>
2	ldap	lo	dap			启用		编辑测试删除

(2) 填写需要验证的账户密码,选择相应的服务器,点击"确定"。

图24 配置账户密码

服务器:④1	02	
用户名: tes	tuser	
密码: 👓	•••••	
确定取消	¥.	

(3) 返回"登录测试成功"。

图25 登录成功

您的当前位置: 策略配置 > 身份验证 > LDAP登录测试 登陆测试成功

4.6 Ldap用户批量导入

Ldap 用户的批量导入功能,仅限 simple 配置的方法。

4.6.1 新建批量导入

(1) "基本控制 > 用户账号 > 批量导入"。

图26 批量导入

基本	空制	事件审计 🗸	策略配置 🗸	系统设置 🖌	工单管理 🖌	双人复核 🖌		
用户呐	用户帐号							
您的当	您的当前位置: 基本控制 > 用户帐号							
新建用	1月 1	批量导入批	崖修改 导出用	用户 状态: 流	舌动 〜 身份	验证: ~	部门: ROOT 🗸	过期帐号:
	登录名	z↓	姓名	部门	状态	密码期限	帐号期限	角色
1	admir	ı	缺省管理员	ROO	T 活动	有效	有效	超级
			· · · · ·					

(2) "批量新增用户方式"选择"LDAP 导入"。

图27 配置批量新增用户方式

基本控制	事件审计 🗸	策略配置 🖌	系统设置 🖌	工单管理 🖌	双人复核 🖌
用户帐号					
您的当前位置	: 基本控制 >	用户帐号 > LD/	AP导入		
批量新增用户	坊式: ○外部	导入 〇逐个墳	写	入	

4.6.2 编辑批量导入规则

- Ldap 身份验证方式:选择之前配置的 ldap 的名称。
- 服务器地址:填写需要从哪一个 Idap 服务器进行导入。
- LDAP 服务端口:如果不填写,默认为 389 端口。
- 查询用户 DN: 具有查询权限的用户的 DN。
- 查询用户密码
- 用户 basedn:希望从那一层组织下导入。
- 用户 filter:系统通过什么属性过滤用户。这里通过 cn 属性可以过滤出用户,所以使用 cn=*。

图28 编辑批量导入规则

ldap身份验证方式:	Idap 🗸	
服务器地址:	192.168.8.139	(服务器的IP地址)
LDAP服务端口:		(留空表示缺省端口)
查询用户DN:	cn=Manager,dc=test,dc=com	(如CN=Administrator,CN=Users,DC=example,DC=com)
查询用户密码:	•••••	
用户basedn:	ou=People,dc=test,dc=com	(如CN=Users,DC=example,DC=com)
用户filter:	cn=*	(如(&(objectclass=person)(sAMAccountName=*)))
ldap导入行数限制:	100行 🗸	
ldap结果集:	○导出excel ●页面展示 (注意:页面展示	;—次最多300行数据)
	□ 配置ldap用户属性关系	

如果需要将 ldap 上的用户属性也导入运维审计系统,可以在这里设置。

图29 配置 Idap 上的用户属性

	☑ 配置ldap用户属性关系
	LDIF.txt
登录名:	cn
真实姓名:	displayName
部门:	department
邮件地址:	mail
手机号码:	mobile

4.6.3 提交批量导入规则

运维审计系统会将查询到的用户以表格的方式列出。 如果确认无误,点击"确定",创建用户。

图30 提交批量导入规则

身份验	证方式: Idap 🛛 🗸				
	有效期: 2018-01-21 00:00	至2019-01-21 00:00 (留空	空表示永不过期, <u>清空</u> / 缺省)		
	登录名	真实姓名	邮件地址	公司部门	手机
1	ldapuser1	ldapuser1	ldapuser1@test.com	ROOT ~	
2	ldapuser2	ldapuser2	ldapuser2@test.com	ROOT ~	
3	raduser	raduser	raduser@test.com	ROOT ~	
4	xuhf	xuhf	xuhf@test.com	ROOT ~	
5	ldapuser3	ldapuser3	ldapuser3@test.com	ROOT ~	
确定	取消				

HA 部署配置举例

Copyright © 2018 北京紫光恒越网络科技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。



1 简介1
2 配置前提1
3 使用限制1
4 HA部署配置举例1
4.1 组网需求1
4.2 系统版本要求2
4.3 配置思路······2
4.4 配置注意事项2
4.5 配置步骤
4.5.1 登录Main menu菜单3
4.5.2 分别配置主备机IP地址5
4.5.3 分别配置主备机NTP(可选)6
4.5.4 配置主机HA······8
4.5.5 配置备机HA·······10
4.6 验证配置
4.6.1 使用虚IP登录运维审计系统。10
4.6.2 登录Main menu查看HA状态11
4.6.3 HA切换测试
4.6.4 HA配置备份·······13
4.6.5 HA拆除

1 简介

本文档介绍两台运维审计系统的双机热备模式,实现运维审计系统的系统配置定期同步,提供运维 审计系统的高可用性。

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,配置前设备的所有参数均采用出厂时的缺 省配置。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 HA 特性。

3 使用限制

- 必须是安装相同软件版本的两台相同硬件设备。
- 必须使用业务数据口作为管理口。
- 业务数据口需要属于同一网段。
- 两台机器心跳口需用网线直连。

4 HA部署配置举例

4.1 组网需求

为了解决单点故障问题,运维审计系统采用双机热备模式,使用虚 IP 对外提供服务。当一台主机出现问题后,服务自动切换到另外一台机器继续提供服务。具体应用如下:

- 正常情况下,用户访问虚 IP 登录运维审计系统。
- 配置 NTP 服务器,保证时间同步。
- 当主机出现故障后,备机自动接管服务,虚 IP 浮动到备机。
- 当主机恢复故障后,服务依旧在备机继续提供服务。
- 当备机出现故障后,则切换方式相同。
- 运维审计系统与被管理设备之间路由可达、协议可通。
- PC 端只可访问运维审计系统虚 IP 的 22、443、3389 与 5899 端口。

图1 HA 部署组网图



4.2 系统版本要求

适用产品版本: ESS 6102

4.3 配置思路

- 分别配置两台运维审计系统的网络接口 IP 地址,必须在同一网段。
- 分别配置两台运维审计系统的 HA 接口 IP 地址,并且直连。
- 选取其中一台作为主机,编写配置 HA 信息,启动主机 HA 服务。
- 在另外一台机器上, 配置 HA 信息, 启动 HA 服务并加入到 HA 中。
- 配置完成后,两台机器即为双机热备的工作模式。

4.4 配置注意事项

为了确保双机热备配置成功,需要注意以下几方面:

- 两台运维审计系统的软件版本必须相同。
- 主机与备机的网络接口 IP 地址需在同一网段。
- 主机与备机 HA 接口 IP 必须直连并互通。
- 先配置主机,服务正常启动后在配置备机。

4.5 配置步骤

4.5.1 登录Main menu菜单

#通过连接键盘、显示器到物理机登录 Main menu 菜单,用户名密码为 root/admin。 #通过 SSH 远程连接登录 Main menu 菜单,使用密钥进行加密认证。

🗑 提示

密钥为登陆运维审计系统后台管理菜单的唯一认证方式。

运维审计系统的密钥内容如下:

----BEGIN RSA PRIVATE KEY----

MIIEogIBAAKCAQEA7JSUgUq+1L9AlvK+6TRCN4mBTSVszAEu61lYhMOFcqM0I4o4 74ZaqWwi/JDwLnpi4HnW7h601M39I9qeKv109qbGUaXdgL+IkcJB4PVgCgeQKG1Z B3ng/iOFe47dTV6Dx3D5v3j7lxuihPJXwcHtRRjSD0GBH0IJeQAL2fK3rk4ldqhI FouqgoyjdONrV0YInRdNWzpl2Nxob33B/U4pwdvKVqDzWDk17+tZEdFvaoqzXFgt hGfnmDtNiGVSLrJjbH+lwN0JHVeUSZHQ0iTfHOna5f39ConGqwIkVDVsDjfYqAW1 VPuwV1ExOWLjzIOtiiN2Xx62kqefgCRhVpc+qwIBIwKCAQBy6RTuV4FCw0tCAOBi pFqtQsnGYqKO+UKsV0hAfDmA0u1wWRRXFV88WRhOyg5CdfWC+VnEHXh0KYmVEmoU 4XwqB9yrUJAol4t5/0SR1kSXKD60ivC6fQbh1r0tYqYBAgV+IO5Vr8qoeyMNX8Q5 ihQo4CuDwLsPLrQk1CMDdeQwFmTvcSeJ/KqEluVxoBqegKtWT52C4JIenp95I96Z CaFhHWaY8XjSKSO07In8RoIp2v24DXtNHy4rd5vhgUi0HjAihEA93eRog4rDsHSB 1fm2rJVtuImDPnFMjH75d3SwYPyca+4ZLZwnXgMjE7PJFtUe0niEr40wsPuq4i5L B6LrAoGBAP1/PnwPBdst4AhbNn8FmxLje/DZWtpmZoyITBDq129KCM4xGjS3FyDY 7169VdaiiFDBXHVDQ6SxQ85z69rk45oGgaU0AVzOb+ZCfTocYb6/xcOVFhLc8h6E HzdlW/vjyvYij+o5hNAyo+2VV7y8DZ92V0fMaVsxQzcU+6vKy6VRAoGBAPK/Jnqq IOMWhP7zgWo4g+9TM67OxeYkXHV1UUEirjH7LQrMhomlJ7yEYUencfY1md/Fssl1 L1xRPXpiUSzmCRsAz5pn1pnSFRfdmj1uN8PlDBDYa/w9gIJ/Z1DtPdpG0mH4Hx0j 3LzEkVtMxHiusHVq7a7q8ZMMNEQpdSkPcJU7AoGBAIdw9gjU9IztBJbSbgpwweWu sP8W6C1qyfSEgRB/fE06ec8EtnRjZF0o9m3xw0I6+Yrsn+fir7EtB41U3x80ii8K 2Koji7YJqnWvEMfGQ7CxP3jNRn9EvfNPCaG6rkbpX4zuMN48e0xzQwvx/G3FK/d6 waqiKpCXFdwStIHUfS3bAoGAUzo5FBmlsJoBtn9fkiIBWV5a3Nkt6IF+yS+JkqzO AoIA0ICjJ+DabIUoqtpS9VQ0wcAgCo6T5SMrBWOJi7yVaFgMqfe3Sq5tochSI7DC qZBb61S3TysHfTL+2erwopvwXBqOUy19DYU5Jp360AFhE1CMAXUfoCFxAW1MvZ7k

xXMCgYEApZ/k+CDP9R2gzq1vMAyG57Rq+/WDD748eb7bamesEvQuaZWpc/m+u7nV
pEQfHIxgOckaRkYnCHivOMRf8LUkNCoQ/hJoa3XV5hcb/jmXzcWpqSiB5eXqG/fv
AAWruTdhzpUo4dniY/ZYvAaIbgk7R8hjKc2t07u58on8E7DlhZ4=
END RSA PRIVATE KEY

将上文阴影内容复制粘贴进新建的文本文档中,并将其更名为"RSA-201801-openssh",将该 txt 文件保存在本地供使用。

- (1) 打开 secureCRT 工具(版本至少 6.5 以上),点击快速连接,在主机名一栏中填入运维审计 系统的 IP 地址。用户名栏输入 "root",并将公钥认证移至首行。
- 图2 新建连接

Quick Connect		×
Protocol: Hostname: Port: Username: Authentication Password V Password Keyboard I GSSAPI	SSH2 183.1.2.24 22 Firewall: root	None
Show quick co	onnect on startup	✓ Save session✓ Open in a tabConnectCancel

(2) 选择"公钥"后点击右边的属性,在公钥属性窗口中指定密钥(RSA-201801-openssh.txt)的存放路径。

图3 指定密钥路径

Public Key Properties
 Use global public key setting Use session public key setting Global settings Use identity or certificate file C:\Users\h14923\pesktop\RSA-201801-openssh.txt Fingerprint (MD5): 57:7d:e1:f5:12:4b:d2:e8:18:98:17:8e:05:52:ee:0a Create Identity File Upload Change Passphrase Use personal store certificate (CAPI) Each certificate will be tried until one succeeds.

- (3) 登录后即可进入 Main menu 菜单。
- 图4 Main menu 菜单

Main Menu

- 1. Date and Time
- 2. Network Configuration
- 3. Service Management
- 4. Administrators
- H. High Availability
- S. System Status
- T. System Tools
- R. System Recovery
- A. Application Server

Enter selection:

4.5.2 分别配置主备机IP地址

- # 登录 Main menu 菜单。
- #按照索引选择 "2", 进入 "Network Configuration"。
- #选择对应数据网口前的索引,进行网络配置。
- #网络接口与 HA 接口都需要配置 IP 地址。

图5 网络配置菜单

#选择相应的配置项编号即可修改该配置参数,例如:选择1(IP Address),修改该网卡的 ip 地址,回车之后菜单中会提示您新设置的 IP 地址,确认没问题之后选择S(submit)进行提交生效。

图6 修改 IP 地址



#选择"S"提交配置更改。

4.5.3 分别配置主备机NTP(可选)

#登录 Main menu 菜单。

按照索引选择"1",进入"Date and Time",再选择"3",进入"Network Time Protocol"。

```
图7 NTP 设置
```

Main Menu
1. Date and Time
2. Network Configuration
3. Service Management
4. Administrators
H. High Availability
S. System Status
T. System Tools
R. System Recovery
A. Application Server
Enter selection: 1
Date and Time
1. Date : 2018-01-18
2. Time : 15:07:52
3. Network Time Protocol
0. Return
Enter selection: 3

#添加时钟服务器。

图8 添加时钟服务器

Network time Protocol 1. 0.rhel.pool.ntp.org 2. 1.rhel.pool.ntp.org 3. 2.rhel.pool.ntp.org X. NTP Service : stopped A. Add Server U. Update time
0. Return Enter selection: a Please input new NTP server :192.168.4.162 Network time Protocol 1. 0.rhel.pool.ntp.org 2. 1.rhel.pool.ntp.org 3. 2.rhel.pool.ntp.org 4. 192.168.4.162 A X. NTP Service : stopped A. Add Server U. Update time S. Submit 0. Return Enter selection:

启动 NTP Service 服务

图9 启动服务

Network time Protocol
1. 0.rhel.pool.ntp.org
1.rhel.pool.ntp.org
2.rhel.pool.ntp.org
4. 192.168.4.162 A
X. NTP Service : stopped
A. Add Server
U. Update time
S. Submit
0. Return
Enter selection: x
Select action (1. start, 2. stop, 3. restart, 0. return): 1
Starting ntpd: [OK]
1 A shal peal ptp arg
1. V. rhel.pool.ntp.org
2. 1. rhel.pool.ntp.org
3. 2. rnel.pool.ntp.org
4. 192.108.4.102 A
A Add Conver
A. AUU Server
S. Submit
V. Reluin



NTP 不是配置 HA 必要选项,但时钟不同步会导致 HA 节点状态异常。

4.5.4 配置主机HA

#使用超级管理员登录主机运维审计系统。
#进入[系统设置/HA 安装]页面,在双机部署中选择[主机配置]。
#在[主机信息]中,为网络接口与 HA 接口选择网卡接口。
#在[备机信息]中,填写网络接口与 HA 接口的 IP 地址。
#在[常规配置],填写"浮动 IP"与"Ping IP"。
#点击<执行安装>按钮。

图10 HA 主机配置示意图

基本控制 ~	事件审计 ~	策略配置~	系统设置	工单管理~	双人复核 ~	
授权管理	安全证书 节	点配置 HA安	装 定期任务	配置备份	系统时间	手册管理
您的当前位置	: 系统设置 >	HA 安装				
双机部署:	[主机配置]		¢			
[主机信息]						
网络接口:	GE0/0		\$			
IP 地址:	192.168.7.72					
HA接口:	GE0/1		\$			
IP 地址:	99.99.99.99					
[备机信息]						
网络接口:	GE0/0		≜ ▼			
IP 地址:	192.168.7.73					
HA接口:	GE0/1		*			
IP 地址:	99.99.99.98					
[常规配置]						
浮动 IP:	192.168.7.88					
Ping IP:	192.168.7.1					
	执行安装					

图11 主机部署成功

基本控制 🗸	事件审计 ~	策略配置	l~ .	系统设置	工单管理 ~	双人复核 ~		
授权管理	安全证书 节	点配置	HA安装	定期任务	6 配置备份	系统时间	手册管理	SNMP管理
授权管理 您的当前位置 2018-02-03 0 2018-02-03 0 2018-02-03 0 2018-02-03 0 2018-02-03 0 Generating pr Your public k The key finge 62:7a:e9:57: The key's ran +[RSA 204 o o + o o 0 o o + o o 0 o o + o + o + o + 2018-02-03 0 2018-02-03 0	安全证书 节 注 系统设置 >)9:24:14,916 pi)9:24:14,937 pi)9:24:14,937 pi)9:24:14,937 pi)9:24:14,938 pi ublic/private rsi ation has been ublic/private rsi ation has been ye has been sa erprint is: 15:d3:4c:51:6e domart image 18]+	点配置 HA 安装 d=3256 II d=3256 II d=3256 II d=3256 II a key pair. saved in / roc :22:bb:6f: is: id=3256 II id=3256 II id=3256 II	HA安装 NFO conf NFO conf NFO conf NFO crea (root/.ssh td/.ssh/id 72:a6:cf:	定期任务 ig /etc/crom ig /etc/rsyn ig /etc/ha.d ig ha.conf te ssh key /id_rsa. _rsa.pub. 7d root@nd	。 配置备份 .d/sync db_syr d.conf //ha.cf ode1	系统时间 nc	手册管理	SNMP管理
2018-02-03 09:24:15,034 pid=3256 INFO create ha authkey 2018-02-03 09:24:15,761 pid=3256 INFO config /etc/ha.d/haresources 2018-02-03 09:24:15,763 pid=3256 INFO Fullsync: main config done 2018-02-03 09:24:15,764 pid=3256 INFO Active node installed successfully! Please reboot your system!								
2018-02-03 09:24:15,764 pid=3256 INFO Active node installed successfully! Please reboot your system! Stopping High-Availability services: Done.								
Waiting to all	ow resource ta	keover to	complete	:Done.				
Starting High	-Availability ser	vices: Dor	ne.					

主机安装完毕,请等待浮动地址启动后,至备机器进行安装!

4.5.5 配置备机HA

当主机虚 IP 可以访问后,使用超级管理员登录备机运维审计系统。

- #进入[系统设置/HA 安装]页面。
- #选择双机部署为"[备机配置]"。
- #填写主机网络接口 IP 地址。
- #点击<执行安装>按钮。

图12 HA 备机配置示意图

基本控制 ~	事件审计 ~	策略配置 ~	系统设置	双人复核~	
授权管理	安全证书 节	点配置 HA安	民装 定期任务	§ 配置备份	系统时间
您的当前位置	註: 系统设置 >	→ HA 安装			
双机音	『署: 【备机酝]置]	\$		
主机网络接口	□IP: 192.168	.7.72			
	执行安徽	長			

图13 备机部署成功



4.6 验证配置

4.6.1 使用虚IP登录运维审计系统。

- (1) 使用虚 IP 可以登录运维审计系统。
- (2) 打开右上角向下箭头中的[HA 状态]页面,可查看 HA 状态。

(3) 点击<执行数据同步>,测试数据是否可正常同步。

图14 HA 状态示意图

基本控制 ~	事件审计 ~	策略配置→	系统设置~	双人复核 ~				
活跃会话	系统负载 H/	4状态						
您的当前位置	t: HA状态							
HA状态 守护进程: 正 主点名称: nc 备点名称: nc	常运行 ode_1 ode_2							
备点状态:活	动							
连接状态: G	E0/0活动, GE0/	1活动, 10.10.10	5.1活动					
本地资源: al	本地资源: all							
数据同步 2018-01-17 执行数据同	13:20:09 数据同 步	司步成功						



首次登陆时,可能会提示"备机同步数据失败",手动执行数据同步即可。

4.6.2 登录Main menu查看HA状态

(1) 登陆主机的 Main menu 菜单。

图15 Main menu 菜单

Main Menu

- 1. Date and Time
- 2. Network Configuration
- 3. Service Management
- 4. Administrators
- H. High Availability
- S. System Status
- T. System Tools
- R. System Recovery
- A. Application Server

Enter selection:

(2) 选择 H 进入 High Availability。

图16 High Availability 菜单



(3) 选择 X, 查看当前节点 HA 运行状态。





🕑 说明

"running" 表示 ha 服务正在运行。 "all" 表示当前节点为主机。 "none" 表示当前节点为备机。

4.6.3 HA切换测试

(1) 登陆 Main menu 菜单,选择 H 进入 High Availability 选项。

图18 High Availability 菜单



(2) 查看当前节点状态,如果当前节点为 "all",则选择 "S"选项,使当前节点变为备节点。
图19 切换 HA

High Availability Configuration
 Normal Sync(do at standby)
T. Takeover
S. Standby
X. Status
0. Return
Enter selection: s
Are you sure?(y/n) y
Going standby [all].

(3) 切换成功后,节点状态由 "all"为 "none"。

图20 主节点切换为备节点





操作前,应确定当前节点状态。在主机节点应选择 S 选项切换为备节点。在备机节点应选择 T 选项, 切换为主机节点。

4.6.4 HA配置备份

- (1) 使用超级管理员登录运维审计系统。
- (2) 打开[系统设置/配置备份],在导出系统配置中点击<下载配置>。

图21 配置备份



(3) 保存导出的配置备份文件即可。

4.6.5 HA拆除

1. 主节点退出HA

- (1) 使用超级管理员登录虚 IP, 打开[系统设置/HA 安装]。
- (2) 点击<退出 HA>按钮,并在弹出的提示框确认操作。
- (3) 节点退出 HA 后,需要重新启动系统。

图22 退出 HA



2. 备节点退出HA

- (1) 使用超级管理员登录虚 IP, 打开[系统设置/HA 安装]。
- (2) 点击<退出 HA>按钮,并在弹出的提示框确认操作。
- (3) 节点退出 HA 后,需要重新启动系统。

图23 备节点退出 HA





由于主节点退出 HA 后,再登录运维审计系统时会提示: "HA 状态错误:备机数据同步失败,备 点失败..."属正常现象。

Radius 认证配置举例

Copyright © 2018 北京紫光恒越网络科技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。



1 简介…	· · · · · · · · · · · · · · · · · · ·	1
2 配置育	前提	1
3 配置举	举例	1
3.1	组网需求	1
3.2	2 系统版本要求	2
3.3	3 创建RADIUS认证方式	2
3.4	4 创建用户,绑定RADIUS认证方式	2
3.5	5 登录认证	3
3.6	3 验证配置	3

1 简介

RADIUS 是一种用于在需要认证其链接的网络访问服务器(NAS)和共享认证服务器之间进行认证、 授权和记帐信息的文档协议。

RADIUS 在运维审计系统中,主要体现的是认证功能。

2 配置前提

收集 RADIUS 服务器信息: IP 地址、RADIUS 端口号、RADIUS 的通信密码。

- 典型 Radius 服务器配置
 - o 状态: 启用服务器 1
 - 。 名称: radius
 - 。 RADIUS 服务器 1: 192.168.6.220,端口: 1812,通讯密码: 123456
 - 。 RADIUS 服务器 2: 192.168.6.221,端口: 1812,通讯密码: 123456

3 配置举例

3.1 组网需求

图1 RADIUS 认证网络图



3.2 系统版本要求

适用产品版本: ESS 6102

3.3 创建RADIUS认证方式

登录"超级管理员","策略配置 > 身份验证",选择"radius",点击"新建"。

图2 创建 RADIUS 认证方式

基本控制 🗸	事件审计	~ 策略	配置 🧃	系统设置 🖌	工单管理 🖌	双人复核	•				
系统策略	告警事件	字符终端	会话配置	身份验证	设备密码	设备类型	部门配置	改密方式	密码代填	IE代填脚本	
您的当前位置	: 策略配置	置 > 身份验;	Æ								
协议: radius	5	▶ 新建									

配置 RADIUS 认证方式:

- 状态:选择为启用服务器 **1**。
- 名称: 该 radius 认证的名称。
- RADIUS 服务器 1: IP 地址:填写 RADIUS 的 IP 地址。
- 端口:填写 RADIUS 的认证端口,一般默认为 1812。
- 通信密码:填写 RADIUS 的通信密码。

图3 配置 RADIUS 认证方式

方式: radius
状态: 启用服务器1 ~
名称 radius
RADIUS 服务器1: IP地址: 192.168.8.139 ,端口 1812 ,通讯密码 ••••••
RADIUS 服务器2: IP地址:,端口:,通讯密码:
确定 重设 取消

3.4 创建用户,绑定RADIUS认证方式

"基本控制 > 用户账号",点击"新建用户"。

图4 创建用户

基本控制	权限控制 🗸	密码控制 🗸	事件审计 🗸	统计报表 >	工单管理 🗸	脚本任务 🗸	双人复核 ~				
用户帐号	系统帐号 目	标设备 用户分	组设备分组	B.							
您的当前位置	註: 基本控制 >	用户帐号									
新建用户	批量导入 批	量修改 导出用	戸 状态: 流	5动 ~ 身份	验证:	✓ 部门: ROC	ot v 过	期帐号: > ;	过滤:	过滤未登录用户 🗹	

- 登录名:登录运维审计系统的账户名。
- 真实姓名:该账户名的真实用户。
- 部门:选择相应的部门。
- 身份验证方式:这里选择之前配置的 radius。

• radius 用户名: 绑定该登录名对应的 radius 账户,如果不填,则默认此项为登录名。

图5 配置用户信息

状态 :	○禁用 ●活动 (查看登录日志 查看可登录设备 分配用户组 管理访问规则 用户帐户设置)
登录名:	test *
真实姓名 <mark>:</mark>	test *
邮件地址 <mark>:</mark>	
手机号码 <mark>:</mark>	
部门:	ROOT ×
职位 :	
工号 <mark>:</mark>	
身份验证方式 <mark>:</mark>	radius
radius用户名:	
权限:	🗆 超级管理员 🗆 审计管理员 🗆 配置管理员 🗆 密码保管员 🗹 普通用户
	审计权限:□下载会话 □ 键盘事件
	(需要下载会话权限,必须勾选键盘事件权限)
	保存删除

3.5 登录认证

图6 用户登录



3.6 验证配置

(1) 进入超级管理员账户,选择"策略配置 > 身份验证",选择相应的 radius 认证,点击"测试"。

图7 身份验证

基本控制 🖌 🔋	消止 (注意) (注意) (注意) (注意) (注意) (注意) (注意) (注意)	设置 ~ 工单管理 ~	双人复核 ~		起
系统策略 告警	事件 字符终端 会话配置	身份验证 设备密码	设备类型 部门	配置 改密方式	密码代填 正代填脚本
您的当前位置:	策略配置 > 身份验证				
协议: Idap	→ 新建				
	名称	协议	状态		动作
1	本地认证	native	启用		<u>设</u> 置
2	totp	totp	启用		编辑设置删除
3	ad	ldap	启用		编辑测试删除
4	totpmobile	totpmobile	启用		编辑删除
5	mix	mix	启用		编辑删除
6	radius	radius	启用		编辑测试删除

(2) 填写需要验证的账户密码,选择相应的服务器,点击"确定"。

图8 配置账户密码



(3) 返回"登录测试成功"。

图9 登录成功

您的当前位置:策略配置 > 身份验证 > RADIUS登录测试 登陆测试成功

TOTP 令牌(动态令牌)配置举例

Copyright © 2018 北京紫光恒越网络科技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。



E	录

1	简介1
2	配置前提1
3	配置举例1
	3.1 组网需求1
	3.2 系统版本要求
	3.3 新建TOTP认证方式1
	3.4 TOTP令牌管理2
	3.4.1 单个令牌管理2
	3.4.2 批量令牌管理4
	3.4.3 PIN码策略5
	3.5 创建用户,绑定TOTP令牌5
	3.6 TOTP使用6
	3.6.1 TOTP登录6
	3.6.2 TOTP双人复核7
	3.6.3 TOTP修改PIN1、PIN2 码

1 简介

TOTP 是基于时间的一次性密码算法的简称。这个算法通过一个共享密钥和当前时间来计算一次性 密码。经常被用于双因素认证的系统中。因为网络延时或者时钟没有完全同步的原因,一般生成一 次密码,需要 **60** 秒的发送间隔。

2 配置前提

因为 TOTP 令牌与时间密切相关,所以在配置 TOTP 令牌前,请确保运维审计系统的时间与北京时间一致。

3 配置举例

3.1 组网需求



3.2 系统版本要求

适用产品版本: ESS 6102。

3.3 新建TOTP认证方式

(1) 超级管理员,"策略配置 > 身份验证",选择"totp",点击"新建"。

图2 新建 TOTP 认证方式

基本控制 ~	事件审计	▼ 策略	配置 系	充设置 ➤	工单管理 🗸	双人复核、	*				
系统策略	告警事件	字符终端	会话配置	身份验证	设备密码	设备类型	部门配置	改密方式	密码代填	IE代填脚本	
您的当前位错	置: 策略配	置 > 身份验试	Æ								
协议: <mark>totp</mark>		─ 新建									

(2) 修改属性

- 状态:选择为启用。
- 名称: 填写此 totp 名称。

点击确定。

图3 修改属性

方式:totp	
状态 <mark>:启用 ~</mark>	
名称 <mark>totp</mark>	
确定 重设 取消	

3.4 TOTP令牌管理

点击"设置"。

图4 -	TOTP	令牌	管理
------	------	----	----

2	totp	totp	启用	编辑	设置	删除

3.4.1 单个令牌管理

- 1. 导入令牌
- (1) 点击"新建"。
- 图5 导入令牌

新建	批量导入	批量同步	PIN	策略
				SN

(2) 输入对应的 key 和 SN 号码,点击"确定"。

图6 输入对应的 key 和 SN 号码

SN:	21000	00259	874		*	Ø
KEY:	IIOBEA	0B577	7CE72A12D	A2A8FDE17	*	Ø
	确定	取消				

2. 令牌同步

方法一:

(1) 当令牌使用一段时间之后,可能由于时钟漂移,导致一次性密码产生错误,这时需要同步令牌。 选择相应令牌,点击"同步"。

图7 同步令牌

	SN	归属人	时钟漂移	动作
1	2100000259874		0	编辑同步删除

(2) 将令牌产生的两个一次性密码,依次填入"密码1"、"密码2"。

点击"同步"。

图8	输入	、密码
----	----	-----

TOTP令牌同步				
SN:	2100000259874			
密码1:	740312			
密码2:	051872			
	同步 取消			

方法二:

(1) 页面右上角,进入"账户设置"

图9 账户设置



(2) 将令牌产生的两个一次性密码,依次填入"密码1"、"密码2"。

点击"同步"。



TOTP同步		
密码1:	850322	
密码2:	590173	
	同步	

3.4.2 批量令牌管理

- 1. 批量导入令牌
- (1) 点击"批量导入"。

图11 批量导入令牌

新建	批量导入	批量同步	PIN码策略

(2) 将 key 和 SN 号写入文本。

格式: 13 位 SN + 一个空格 + 50 位 KEY。

图12 将 key 和 SN 号写入文本

📕 key	_SN.txt - i	己事本		
+++++(E)	(白橋(5)	#2-P(O)	本王へへ	±BB±/LD

又件(上) 漏額(上)	格式(<u>○</u>) 登者(<u>V</u>) 希!	即(H)	
2100000339639	11817F3BA4740460	07	F4AA2B207861FD8BB8
2100000339640	11D0707F3A3AA890	DC DC	CD6AE9D73099597D56
2100000339641	118A2C76D9B48456	68	9EDB2F21621F75D0F5
2100000339642	118F55A4156F5563	30	D508AFC0ECA8ECD9AB
2100000339643	117B88D649DA9689	97	88662A286AE9A72700
2100000339644	11521664103D682	18	57FB1785CA070B91CF
2100000339645	11ECE9565D4BE889	97	211819A7893FDC36DC
2100000339646	11CFA42FAB9D0996	66	295AB9D1F0C5F3F153
2100000339647	11B238EED2B31675	53	30E1877655381E6855
2100000339648	11A93201D3A4F607	70	CB2EBF2EAF7121DD75
2100000339649	118C33E22A79368E	01	1CD13C60DC5A6BCC85
2100000339650	110009AF7B589F73	3A .	5FEF072A249CF168AE

(3) 导入该文本。

图13 导入文本

批量导入数据:		
上传tnk文件:	浏览	key_SN.txt
	*上传文件内]容每行格式为: 13位SN + 一个空格 + 50位KEY
	上传 取消	ă

(4) 点击"确定导入"。

图14 确认

*注:	SN已存在的令牌,	若重复导入,	系统将自动覆盖SN所对应的KEY值。

	SN	KEY			移除
1	2100000339639	II817F3BA474046	F4AA2B207861FD8BB8]	<u>移除</u>
2	2100000339640	IID0707F3A3AA89	FCD6AE9D73099597D56]	<u>移除</u>
3	2100000339641	II8A2C76D9B4845	49EDB2F21621F75D0F5]	<u>移除</u>
4	2100000339642	ll8F55A4156F5563	7D508AFC0ECA8ECD9AB]	<u>移除</u>
5	2100000339643	II7B88D649DA968	8662A286AE9A72700]	<u>移除</u>
6	2100000339644	ll521664103D6821	'FB1785CA070B91CF]	<u>移除</u>

确定导入取消

2. 批量同步令牌

(1) 点击"批量同步"。

图15 批量同步令牌

新建	批量导入批量同	步PIN码第	語
(2)	设置时钟漂移,	然后点	击确定。
图16	设置时钟漂移		
			•
时钟漂移	· 4 确定 取消		* 💟

3.4.3 PIN码策略

TOTP 令牌不能单独作为验证工具,必须与另外的静态密码进行绑定,我们在运维审计系统中,将 这个静态密码称为 PIN 码。

点击"PIN 码策略"。

图17 PIN 码策略

新建	批量导入	批量同步	PIN码策略	
SN				

设置需要的 PIN 码复杂度。

图18 设置 PIN 码复杂度

最小PIN码长度:		*
最少数字字符个数:		*
最少大写字母个数:		*
最少小写字母个数:		*
最少其他字符个数:		*
	保存重设	

3.5 创建用户,绑定TOTP令牌

"基本控制 > 用户账号 > 新建用户"。

图19 创建用户

基本控制	事件审计 🗸	策略配置 🗸	系统设置 🖌	工单管理 ~	双人复核 ~	
用户帐号						
您的当前位置	: 基本控制 >	用户帐号				
新建用户	批量导入批	量修改 导出月	用户 状态: 混	动 > 身	分验证:	✓ 部门: ROC

- 登录名:登录运维审计系统的账户名。
- 真实姓名:该账户名的真实用户。
- 部门:选择相应的部门。
- 身份验证方式:这里选择之前配置的 totp。
- SN: 选择需要绑定的令牌 SN (一个令牌最多可以分配给 5 个用户使用)。
- PIN1: 用户登录时使用的静态密码。
- PIN2: 用户做双人授权时使用的静态密码。

图20 配置用户信息

状态 :	○禁用 ⑧活动 (查看登录日志 查看可登录设备 分配用户组 管理访问规则 用户帐户设置)
登录名:	test *
真实姓名:	test *
邮件地址:	
手机号码:	
部门 :	ROOT 🗸
职位 :	
工号:	
身份验证方式 :	totp
	SN: *2100000259874(已分配 1 位用户) 🚽 *
	PIN1:
	PIN2:
	□ 下次登录时须修改PIN码
权限:	🗆 超级管理员 🗆 审计管理员 🗆 配置管理员 🗌 密码保管员 🗹 普通用户
	审计权限:□下载会话 □ 键盘事件
	(需要下载会话权限,必须勾选键盘事件权限)
	保存删除

3.6 TOTP使用

3.6.1 TOTP登录

输入账户、密码。 密码格式为: PIN1 码+令牌

图21 TOTP 登录



3.6.2 TOTP双人复核

密码: 输入 PIN2 码。

图22 TOTP 双人复核

双人复核		×
夏核人	: test 🗸	
密码	3: •••	
	确定	

3.6.3 TOTP修改PIN1、PIN2 码

(1) 页面右上角,进入"账户设置"

图23 账户设置

普通用户	test 🗸 🕴 🕜 🗸
	帐户设置
	最近访问
	退出

(2) 输入: PIN1 码+令牌

图24 PIN1 码+令牌

当前设置	
登录名 :	test
姓名:	test
电子邮件:	
手机号码 <mark>:</mark>	
登录密码:	将于 90 天后过期 (2018-04-25)
用户身份 <mark>:</mark>	普通用户
修改设置	
当前登录密码:	••••••
	确定

- (3) 切换到"自由修改密码",修改 PIN1、PIN2 码。
- 图25 修改 PIN1、PIN2 码

个人设置	自由修改密码	设备访问表格设	置
新PIN码长度 最少要包含了	不应小于 个字符 ト数字字符・ 个大写言	字母, 个小写字母,	个其他字符;
PIN1:	•		
确定	Ē		

不托管密码模式配置举例

Copyright © 2018 北京紫光恒越网络科技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。



1 简介	I
2 配置举例	1
21 组网需求	1
	1
2.2 示沉顺平安示····································	1
2.3 癿直心龄	1
2.4 配直步骤	I
2.4.1 关联相应设备any账户的访问规则	l
2.4.2 登录设备	2

1 简介

不托管密码模式是指运维审计系统不托管目标设备的密码。普通用户通过运维审计系统登录目标设 备,需要手工输入密码。

运维审计系统中的"any"系统账号,用于未托管密码的场景,代表任意账号。

2 配置举例

2.1 组网需求

图1 运维审计系统网络图



2.2 系统版本要求

适用产品版本: ESS 6102。

2.3 配置思路

- (1) 新建目标设备,不托管密码。
- (2) 在访问规则中关联 any 账号。
- (3) 普通用户访问是自行输入账号和密码。

2.4 配置步骤

2.4.1 关联相应设备any账户的访问规则

登录"配置管理员","权限控制>访问权限"。

图2 配置访问权限

基本控制 ~ 权限控制	密码控制 🗸	事件审计 🗸	统计报表 🗸	工单管理 🗸	脚本任务 🗸	双人复核 🗸	
访问权限 命令权限							
您的当前位置: 权限控制 >	访问权限						

选择对应的规则,点击"系统账号"。

图3 选择规则

规师	9	部门	用户帐号	目标设备	系统帐号	服务类型	服务协议	服务名称	动作
1	test	ROOT	admin	<u>192.168.8.135</u>		字符终端	telnet ssh		编辑 登录规则 克隆规则
			<u>test</u>	<u>192.168.8.136</u>		图形终端	tn5250 rdp vnc		关联: <u>用户组(0)</u> 用户(2)
						<u>文件传输</u>	rdpapp ftp sftp		<u>设备组(0)</u> <u>设备(2)</u>
									系统帐号(0) 双人复核候选人(0)

选择"any"账户,点击"建立关联"。

图4 建立关联

×
■ 精确过滤 共1页 < 1 > G0 每页15条 ∨
administrator
any
enable
netscreen
null
root
self
super

建立关联	取消关联	关闭

2.4.2 登录设备

选择相应账户登录,切换到普通用户。 选择相应的目标设备,右键点击相应服务,选择"any"账户。点击确定。

图5 登录设备



字符类型设备:

手工输入账户、密码。

图6 字符类型设备



图形类型设备:

手工输入账户、密码。

图7 图形类型设备

any@192.168.8.135(192.168.8.135)		×
administrator	2	
Contraction Contra		

部门分权配置举例

Copyright © 2018 北京紫光恒越网络科技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。



1 简	ī介1
2 配	2置前提1
3 配	2置举例2
	3.1 组网需求2
	3.2 系统版本要求
	3.3 配置思路2
	3.4 配置步骤2
	3.4.1 新建部门2
	3.4.2 部门编辑
	3.4.3 部门删除
	3.4.4 分配设备所属部门
	3.4.5 分配用户所属部门
	3.4.6 分配访问权限所属部门5
	3.4.7 分配改密计划所属部门6
	3.4.8 部门分权模式下的命令权限管理 ······6
	3.5 配置验证6

1 简介

本文档介绍如何对运维审计系统配置部门分权。

运维审计系统中可以对用户账号、目标设备以及访问权限进行部门划分,方便用户按照部门来管理 用户和设备。运维审计系统中部门的结构类似于树形结构,最顶层的部门是 ROOT,往下可以由用 户自定义部门结构。

图1 部门分权组网图



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,配置前设备的所有参数均采用出厂时的缺 省配置。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部门分权所带来的特性。

3 配置举例

3.1 组网需求

图2 运维审计系统组网图



3.2 系统版本要求

适用产品版本: ESS 6102。

3.3 配置思路

- 建立部门。
- 为用户账号和目标设备分配部门。

3.4 配置步骤

3.4.1 新建部门

(1) 使用超级管理员身份登录运维审计系统,选择[策略配置/部门配置]。

图3 部门分权配置图

基本控制 ~	事件审计	 策略配 	置 系统	設置~ コ	「単管理 ~	双人复核 ~							超级管理员 🗸	l admin ∽ l
系统策略	告警事件	字符终端	会话配置	身份验证	设备密码	设备类型	部门配置	改密方式	密码代填	IE代填脚	本			
您的当前位	置: 策略配	置 > 部门配置	t											已用数: 4, 可
名称									超级		配置	审计	密码	动作
ROOT									admin		admin	admin	admin	新建 编辑
系统运	维部										zhangsan			新建 编辑
系统	组													新建 编辑
安全管	理组													新建 编辑

- (2) 在[部门配置]页面中,单击相应部门名称栏目右侧动作列中<新建>按钮。
- (3) 在跳转的[新建]部门页面中,输入新建部门名称,选择该部门隶属部门,单击<确定>按钮,完成部门新增。

图4 新建部门名称

基本控制	~ 事件审计、	策略配到	系统	设置~	工单管理~	双人复核 ~					超级管理员	- 1	admin ~	1 🕐 👻
系统策略	告警事件	字符终端	会话配置	身份验证	E 设备密码	设备类型	部门配置	改密方式	密码代填	IE代填脚本				
您的当前的	您的当前位置: 策略配置 > 部门配置 > 新建													
名称:	系统运维部			• 🥑										
隶属于:	ROOT		\$	•										
	确定 取消													

🕑 说明

第一次新建部门时,只能隶属于初始的 ROOT 部门。

3.4.2 部门编辑

- (1) 使用超级管理员身份登录运维审计系统,选择[策略配置/部门配置]。
- (2) 在[部门配置]页面中,在需要更换隶属部门的部门名称栏目右侧动作列中单击<编辑>按钮。
- (3) 在跳转的[编辑]页面中,从隶属于下拉菜单中选择需要更换到的部门名称,单击<确定>按钮。

3.4.3 部门删除

- (1) 使用超级管理员身份登录运维审计系统,选择[策略配置/部门配置]。
- (2) 在[部门配置]页面中,在需要删除或撤销部门名称栏目右侧动作列中单击<编辑>按钮。
- (3) 在跳转的[编辑]页面中,单击<删除>按钮即可删除不需要的部门。

3.4.4 分配设备所属部门

- (1) 使用隶属于 ROOT 部门的配置管理员登录运维审计系统,选择[基本控制/目标设备]。
- (2) 在[目标设备]页面中,单击需要调整设备栏目右侧<编辑>按钮。

图5 设备配置页面

基本技	記制 权限控制 ぞう	码控制 ~ 事件审计 ~	· 统计报表 ~ 工单管理	』→ 脚本任务→ 双人复核→				配置管理员	~ admin ~ 🕗 ~ .		
用户	非产帐号 系统帐号 目标设备 用户分组 设备分组										
您的当	i的当前位置: 基本控制 > 目标设备 已用数: 3, 可用数: 97										
新建	[建 批量导入 批量修改 导出设备 状态: 活动 ≑ 卸门: ROOT ≑ 系统类型: 所有设备类型 ≑ 重复IP: ≑ 过滤: 确定 共1页: <1> Go										
	<u>名称</u> ↓	部门	<u>IP地址</u>	系统类型	字符终端	图形终端	文件传输	动作			
1	192.168.7.198	ROOT	192.168.7.198	Microsoft Windows		rdp		编辑 密码管理 改密日志			
2	192.168.7.70	系统组	192.168.7.70	General Linux	ssh	vnc	sftp	编辑 密码管理 密钥管理	改密日志		
3	winsrv-2008	系统运维部	192.168.7.112	Microsoft Windows		rdp		编辑 密码管理 改密日志			

(3) 在弹出的[设备编辑]页面中,在部门下拉菜单中选择目标设备分配到指定的部门,单击<确定> 按钮。

图6 设备所属部门配置

设备编辑:w	insrv-2008(192.168.7.112)	服务列表	密码管理	分配设备组	访问规则	可登录用户	
状态:	○禁用 • 活动						
设备名:	winsrv-2008	*					
IP地址:	192.168.7.112						
	ping测试						
简要说明:	应用发布服务器	(将	在设备选择菜单	单中显示)			
部门:	系统运维部	\$ * (2				
设备类型:	Microsoft Windows (<u>编辑设备</u>	<u> </u>					
改密方式:	microsoft windows agent						
特权帐号:	administrator	\$					
编码类型:	GB18030	\$					
创建者:	admin (缺省管理员)						
创建于:	2018-01-24 20:51:16						
	确定删除						

3.4.5 分配用户所属部门

(1) 使用超级/配置管理员身份登录运维审计系统,选择[基本控制/用户账号]。

图7 用户配置页面

基	本控制	权限控制	→ 密码控制 →	事件审计~	统计报表、	工单管理~	脚本任务~	双人复核 ~						配置管理月	t 🗸 🕴 admin 🗸 🛛 🕐 👻
用用	户帐号	系统帐号	目标设备 用户	分组 设备分	组										
您的	的当前位置	: 基本控	制 > 用户帐号												已用数: 3, 可用数: 无限制
新3	建用户	此量导入	批量修改 导出用户	状态: 活道	动 🗘 身份	分验证: ;	部门: ROO	т 🛊 В	过期帐号		 过滤 	B:		过滤未登录用户 🛟	共 1 页: < 1 > Go
	登录行	£↓	姓名	部门	状态	密码期限	帐号期限	<u>角色</u>					身份验证	最后登录时间	动作
1	admir	1	缺省管理员	ROOT	活动	有效	有效	超级	审计	密码	配置	普通	本地认证	2018-01-25	管理登录日志 邮件
2	user0	1	测试用户01	ROOT	活动	有效	有效					普通	本地认证	2018-01-24	管理登录日志

(2) 在[用户帐号]页面中,单击<新建用户>按钮或在已有的帐号栏目右侧点击<管理>按钮,在新页 面中,输入相关用户信息,在部门下拉菜单中选择该用户分配到的部门即可。

图8 用户所属部门配置



单击<保存>按钮,完成部门管理员/普通用户的部门分配。



无法修改缺省管理员部门属性。

3.4.6 分配访问权限所属部门

使用配置管理员身份登录运维审计系统,选择[权限控制/访问权限]。 单击<新建>按钮或在己有的访问权限条目右侧点击<编辑>按钮,弹出的新窗口后,在部门下拉菜单 中选择需要修改的部门即可。 图9 访问权限

基本控制 🗸 🛛 权	限控制	密码控制 ~	事件审计 ~	统计报表 ~	工单管理 🗸	脚本任务 ~	双人复核~
访问权限 命令体	汉限						
您的当前位置: 机	又限控制 >	> 访问权限 > 编	辑规则				
创建者:	admin (#	缺省管理员)					
规则名称:	Linux操	作系统		*			
设备排序:	全局缺	省		♦ (终端)	登录菜单中的目	标设备排序方式	ť)
部门:	系统道	运维部		🕈 * 🥑			
服务类型:	🗌 字符约	冬端 🗌 图形终站	端 🗌 文件传输				
服务协议:	telnet	t 🔽 ssh 🗌 tn52	250 🗹 rdp 🗌 v	nc 🗌 rdpapp 🗌	🛛 ftp 🗹 sftp		
服务名称:	sftp			ssh			
	vnc						
	访问设备	时生成事件					
事件级别:	None			\$			
标题:							
磁盘映射:	🗸 允许值	吏用					
剪贴板:	□ 下行	□上行					
剪切板复制文件:	□ 下行	一上行					
	确定	删除 取消					

3.4.7 分配改密计划所属部门

- (1) 使用配置管理员身份登录运维审计系统,选择[密码控制/改密计划]。
- (2) 单击<新建计划>按钮或在已有的改密计划条目右侧点击<编辑>按钮,跳转到新窗口后,在部 门下拉菜单中选择需要修改的部门即可。

3.4.8 部门分权模式下的命令权限管理

命令权限为全局设置,只有 Root 部门的配置管理员可以进行配置和修改。

3.5 配置验证

1. 查看用户

#确认管理员只能查看本部门及下级部门用户。

(1) 使用系统运维组配置管理员登录运维审计系统,选择[基本控制/用户账号]。

图10 用户列表

基本排	2制 权限控制 ~	密码控制 ~	事件审计 > 统	むおおおし コンジェンジョン こうしん こうしん こうしん こうしん むしんしん しんしん しんしん しんしん しんしん しんしん しんしん	C单管理 ~	脚本任务~	双人复核 ~						16.30	管理员 zhangsan	• I 🕐	× .
用户	长号 系统帐号	目标设备 用户	为组 设备分组													
您的当	9当前位置:基本控制 > 用户帐号													已用数:	3, 可用数	: 无限制
新建用	11户 批量导入 批	量修改导出用	▶ 状态: 活动	\$ 身份验证	÷ \$	部门: 🧃	系统运维 🗧 过期	1帐号:	÷ 过滤	8:		过滤未登录用	₽ †	共 1 页: < 1	>	Go
	登录名」	姓名	部门	状态	密码期	限	帐号期限	角色				身份验证	最后登录时间	动作		
1	user01	user01	系统组	活动	有效		有效				普通	本地认证	2018-01-25	管理 登录日	志	
2	zhangsan	张三	系统运维部	活动	有效		有效			配置		本地认证	2018-01-25	管理 登录日	志	

(2) 使用部门选项进行过滤,只能选择当前部门与下级部门。

图11 部门过滤

基本	控制 权限控制 ~	密码控制 ~	事件审计~	统计报表 ~	工单管理 ~	脚本任务~	双人复核	~						1	記置管理员	zhangsan 🗸 🕖 🗸	
用户	帐号 系统帐号	目标设备 用序	中分组 设备分	组													
您的	当前位置: 基本控制	> 用户帐号					007									已用数: 3, 可用数: 无	;限
新建	用户 批量导入 批	量修改 导出用	户 状态: 活动	か 🗘 身份验	ti≣: 〔 \$)部にく「	系统运维部系统运维部	土 邦月中8	号:	\$ 过滤:			过滤未登录用	1P 🕈	共1	页: < 1 >	Gc
	登录名↓	姓名	部门	状态	密码期	限	安全管理组		<u>角色</u>				身份验证	最后登录时间		动作	
1	user01	user01	系统组	活动	有效		有效					普通	本地认证	2018-01-25		管理 登录日志	
2	zhangsan	张三	系统运维部	活动	有效		有效				配置		本地认证	2018-01-25		管理 登录日志	

2. 查看设备

#确认管理员只能查看本部门及下级部门的设备。

(1) 使用系统运维组配置管理员登录运维审计系统,选择[基本控制/目标设备]。

图12 设备列表

基本	空制 权限控制 >	密码控制 🗸 事件审计	✓ 统计报表 ✓	工单管理 ~	脚本任务 ~	双人复核~					配置管理员 zhangsan ~	🕗 ×
用户	账号 系统帐号 目板	设备 用户分组 设	备分组									
您的当	前位置: 基本控制 > 目	目标设备									已用数:3	8, 可用数: 97
新建	批量导入批量修改	导出设备 状态: 活动	約 💠 部门: 🚺	系统运维 🗧	系统类型: 所	有设备类型	◆ 重复IP:	· \$	过滤:	确定	共1页: < 1 >	Go
	<u>名称</u> ↓	<u>IP地址</u>	系统	类型		字符终端	图形终端	文件传输	动作			
1	192.168.7.70 系統组 192.168.7.70			Gene	eral Linux		ssh vnc sftp <u>编辑密码</u>			编辑 密码管理	聖密钥管理 改密日志	
2	winsrv-2008 系统运维部 192.168.7.112		Micro	osoft Windows			rdp		编辑 密码管理	<u> 改密日志</u>		

(2) 使用部门选项进行过滤,只能选择当前部门与下级部门。

图13 部门过滤

基本技	空制 权限控制	嶅码控制 ~ 事件审计	→ 统计报表 →	工单管理 ~	脚本任务 ~ 双	人复核~			配置管理员	& 🛛 zhangsan 🗸 🗌 🍞 🖌
用户(长号 系统帐号 目标	设备 用户分组 设	备分组							
您的当	前位置: 基本控制 > 目	目标设备	0							已用数: 3, 可用数:
新建	批量导入批量修改	导出设备 状态: 活动	边 ♦ 部门 ✔	/ 系统运维部	统类型: 所有设	备类型 🛟 重复I	P: \$	过滤:	确定 共	キ1页: < 1 > G
	<u>名称</u> 」	部门	<u>IP地址</u>	安全管理组	型	字符终端	图形终端	文件传输	动作	
1	192.168.7.70	系统组	192.168.7.70	Gen	eral Linux	ssh	vnc	sftp	编辑 密码管理 密钥管理 2	<u>权密日志</u>
2	winsrv-2008	系统运维部	192.168.7.112	Mich	osoft Windows		rdp		编辑 密码管理 改密日志	

3. 查看访问权限

#确认管理员只能查看本部门及下级部门的访问权限。

(1) 使用系统运维组配置管理员登录运维审计系统,选择[基本控制/目标设备]。

图14 访问权限列表

基本控	制~	权限控制	密码控制 ~	事件审计~	统计报表 ~	工单管理 ~	脚本任务~	双人复核~						13	管理员	zhangsan	v I 🕐 🔨
访问权	限																
您的当	前位置:	权限控制 >	访问权限														
新建	部门:	系统运维部 🗧	规则名:		用户:	18	2备:		系统帐号:		€ 服务:	所有协议 🗘	提交	全部显示导出	出 共1	页: < 1	> Go
规则			部门	用	户帐号	目标设备	3	《统帐号	服务类型	服务协议		服务名称	动	作			
1	Linux操作	乍系统	系统运维	部 <u>u</u> 고	<u>ser01</u> hangsan	<u>192.168.7.7</u>	0 i	any root		ssh rdp sftp			纑 关	辑 登录规则 引 联: <u>用户组(0</u>	<u> 下陸規则</u>) <u> 用户</u>)	(2)	
														设备组(0) <u>设备 (</u>	1)	A
														<u>系統帐号(</u>	2) 双人	复核候选人((<u>ນ</u> 🐒
																	向
																	1 1 1

(2) 使用部门选项进行过滤,只能选择当前部门与下级部门。

图15 部门过滤

基本控制	✓ 权限控制	密码控制 ~ 事(件审计~ 统计报表~	工单管理 > 脚本	任务 ~ 双人复核 ~				配置管理员	zhangsan 🗸 🕴	2) ×
访问权限											
您的当前	0 ⁻⁰⁰ - 40 m 40 m 1	达问权限									
新建 剖	★ 系统运维部 系统组	规则名:	用户:	设备:		系统帐号:	\$ 服务:	所有协议 🗘 🦉	交 全部显示 导出 共1	页: < 1 >	Go
规则	安全管理组	部门	用户帐号	目标设备	系统帐号	服务类型	服务协议	服务名称	动作		
1 L	nux操作系统	系统运维部	user01	192.168.7.70	any		ssh rdp sftp		编辑 登录规则 克隆规则		
			zhangsan		root				关联: <u>用户组(0)</u> 用户(2)	_
									<u>设备组(0)</u> 设备(1)	āč.
									<u>系统帐号(2)</u> 双人	复核候选人(0)	ï
											向
											导
											<

4. 查看改密计划

#确认管理员只能查看本部门及下级部门的访问权限。

使用系统运维组配置管理员登录运维审计系统,选择[密码控制/改密计划]。

图16 改密计划列表

基本控	텡~ 权限控制~	密码控制	事件审计~	统计报表 ~	工单管理 ~	脚本任务 ~	双人复核~		記置管理员	zhangsan 🗸 İ 🕐 👻
改密计	创 设备改密日志									
您的当	前位置: 密码控制:	> 改密计划								
新建计	划 导出									
任务	呂称	目标说	日本 3	系统帐号	上次	修改密码		距离下次修改密码	动作	
1	windows-plan		a	dministrator	2018	3-01-24 22:31			编辑历史修改记录 查看密码状态 立即修改	
									关联:设备组(0)设备(0)系统帐号(1)	
										83

单机配置举例

Copyright © 2018 北京紫光恒越网络科技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。



1 简介	·····	1
2 配置	看前提·····	1
2	2.1 组网需求	1
2	2.2 系统版本要求	1
2	2.3 配置步骤	2
2	2.4 验证配置	7
1 简介

本文档介绍如何部署单台运维审计系统。

2 配置前提

需要满足如下条件:

- 分配1个IP地址,用于用户登录访问。
- 配置 NTP 服务器,保证时间同步。
- 运维审计系统与被管理设备之间路由可达、协议可通。
- PC 端只可访问运维审计系统的 22、443、3389 与 5899 端口。

2.1 组网需求

运维审计系统以物理旁路,逻辑串联的方式部署在核心网络中。作为运维审计的唯一入口。



2.2 系统版本要求

适用产品版本: ESS 6102。

2.3 配置步骤

1. 登录Main menu菜单

#通过连接键盘、显示器到物理机登录 Main menu 菜单,用户名密码为 root/admin。 #通过 SSH 远程连接登录 Main menu 菜单,使用密钥进行加密认证。

₩ 提示

密钥为登陆运维审计系统后台管理菜单的唯一认证方式。

运维审计系统的密钥内容如下:

----BEGIN RSA PRIVATE KEY----

MIIEogIBAAKCAQEA7JSUgUq+1L9AlvK+6TRCN4mBTSVszAEu61lYhMOFcqM0I4o4 74ZaqWwi/JDwLnpi4HnW7h60lM39I9qeKv1o9qbGUaXdgL+IkcJB4PVgCgeQKGlZ B3ng/iOFe47dTV6Dx3D5v3j7lxuihPJXwcHtRrjSD0GBH0IJeOAL2fK3rk4ldghI FouqgoyjdONrV0YInRdNWzpl2Nxob33B/U4pwdvKVqDzWDk17+tZEdFvaoqzXFgt hGfnmDtNiGVSLrJjbH+1wN0JHVeUSZHQ0iTfHOna5f39ConGqwIkVDVsDjfYqAW1 VPuwV1ExOWLjzIOtiiN2Xx62kqefqCRhVpc+qwIBIwKCAQBy6RTuV4FCw0tCAOBi pFqtQsnGYqKO+UKsV0hAfDmA0u1wWRRXFV88WRhOyg5CdfWC+VnEHXh0KYmVEmoU 4XwgB9yrUJAol4t5/0SR1kSXKD60ivC6fQbh1r0tYqYBAgV+I05Vr8qoeyMNX8Q5 ihQo4CuDwLsPLrQk1CMDdeQwFmTvcSeJ/KqEluVxoBqegKtWT52C4JIenp95I96Z CaFhHWaY8XjSKS007In8RoIp2v24DXtNHy4rd5vhgUi0HjAihEA93eRog4rDsHSB 1fm2rJVtuImDPnFMjH75d3SwYPyca+4ZLZwnXgMjE7PJFtUe0niEr40wsPuq4i5L B6LrAoGBAP1/PnwPBdst4AhbNn8FmxLje/DZWtpmZoyITBDq129KCM4xGjS3FyDY 7169VdaiiFDBXHVDQ6SxQ85z69rk45oGgaU0AVzOb+ZCfTocYb6/xcOVFhLc8h6E HzdlW/vjyvYij+o5hNAyo+2VV7y8DZ92V0fMaVsxQzcU+6vKy6VRAoGBAPK/Jnqg I0MWhP7zgWo4g+9TM670xeYkXHV1UUEirjH7LQrMhomlJ7yEYUencfY1md/Fssl1 L1xRPXpiUSzmCRsAz5pn1pnSFRfdmj1uN8PlDBDYa/w9gIJ/Z1DtPdpG0mH4Hx0j 3LzEkVtMxHiusHVq7a7q8ZMMNEQpdSkPcJU7AoGBAIdw9gjU9IztBJbSbgpwweWu sP8W6C1qyfSEgRB/fE06ec8EtnRjZF0o9m3xw0I6+Yrsn+fir7EtB41U3x80ii8K 2Koji7YJqnWvEMfGO7CxP3jNRn9EvfNPCaG6rkbpX4zuMN48e0xzOwvx/G3FK/d6 waqiKpCXFdwStIHUfS3bAoGAUzo5FBmlsJoBtn9fkiIBWV5a3Nkt6IF+yS+JkqzO AoIA0ICjJ+DabIUoqtpS9VQ0wcAgCo6T5SMrBWOJi7yVaFgMqfe3Sq5tochSI7DC qZBb61S3TysHfTL+2erwopvwXBqOUy19DYU5Jp360AFhE1CMAXUfoCFxAW1MvZ7k xXMCgYEApZ/k+CDP9R2gzq1vMAyG57Rq+/WDD748eb7bamesEvQuaZWpc/m+u7nV pEQfHIxgOckaRkYnCHivOMRf8LUkNCoQ/hJoa3XV5hcb/jmXzcWpqSiB5eXqG/fv AAWruTdhzpUo4dniY/ZYvAaIbgk7R8hjKc2t07u58on8E7DlhZ4=

----END RSA PRIVATE KEY----

将上文阴影内容复制粘贴进新建的文本文档中,并将其更名为"RSA-201801-openssh",将该 txt 文件保存在本地供使用。

(1) 打开 secureCRT 工具(版本至少 6.5 以上),点击快速连接,在主机名一栏中填入运维审计系统的 IP 地址。用户名栏输入"root",并将公钥认证移至首行。

图2 新建连接

Quick Connect		X
Protocol: Hostname: Port: Username: Authentication	SSH2 • 183.1.2.24 • 22 Firewall: root •	None 🔻
PublicKey Password Keyboard I GSSAPI	interactive	Properties
Show quick co	onnect on startup	Save session Open in a tab Connect Cancel

(2) 选择"公钥"后点击右边的属性,在公钥属性窗口中指定**密钥**(RSA-201801-openssh.txt)的存放路径。

图3 指定密钥路径

Public Key Properties
 Use global public key setting Use session public key setting Global settings Use identity or certificate file C:\Users\h14923\Desktop\RSA-201801-openssh.txt Fingerprint (MD5) : 57:7d:e1:f5:12:4b:d2:e8:18:98:17:8e:05:52:ee:0a Create Identity File Upload Change Passphrase Use personal store certificate (CAPI) Each certificate will be tried until one succeeds.

- (3) 登录后即可进入 Main menu 菜单。
- 图4 Main menu 菜单



2. 配置IP地址

(1) 登录 Main menu 菜单。

按照索引选择 "2", 进入 "Network Configuration"。

#选择对应数据网口前索引,进行具体网络配置。

图5 网络配置菜单

Main Menu
1. Date and Time
2. Network Configuration
3. Service Management
4. Administrators
H. High Availability
S. System Status
T. System Tools
R. System Recovery
A. Application Server
Enter selection: 2
Network Devices
1. GE0/0
S. Status
R. Routes
N. DNS Servers
H. Host Info
A. Add Net Device
0. Return
Enter selection:

(2) 选择相应的配置项编号即可修改该配置参数,例如:选择1(IP Address),修改该网卡的 ip 地址,回车之后菜单中会提示您新设置的 IP 地址,确认没问题之后选择S(submit)进行提 交生效。

图6 修改 IP 地址

Network Devices	
1. GE0/0	
S. Status	
R. Routes	
N. DNS Servers	
H. Host Info	
A. Add Net Device	
0. Return	
Enter selection: 1	
Network Configuration	
1. IP Address :	192.168.4.111
2. Netmask :	255.255.254.0
3. Gateway :	192.168.4.1
0. Return	
Enter selection: 1	
New IP Address : 192.3	168.4.112
Network Configuration	
1. IP Address :	192.168.4.111 ==> 192.168.4.112
2. Netmask :	255.255.254.0
3. Gateway :	192,168,4,1
S. Submit	
0. Return	
Enter selection:	

(3) 选择"S"提交配置更改。

3. 配置NTP(可选)

(1) 登录 Main menu 菜单。

按照索引选择 "1",进入 "Date and Time",再选择 "3",进入 "Network Time Protocol"。

图7 NTP 设置

Main Menu	
1. Date and Time	
2. Network Configuration	
3. Service Management	
4. Administrators	
H. High Availability	
S. System Status	
T. System Tools	
R. System Recovery	
A. Application Server	
Enter selection: 1	
Date and Time	
1. Date : 2018-01-18	
2. Time : 15:07:52	
3. Network Time Protocol	
0. Return	
Enter selection: 3	

(2) 添加时钟服务器。

图8 添加时钟服务器

Network time Protocol
1. 0. rhel. pool. ntp. org
2 1 rhel pool ptp org
2. 2. shell peel atta are
3. 2. rhet.pool.ntp.org
X. NIP Service : stopped
A. Add Server
U. Update time
0. Return
Enter selection: a
Please input new NTP server :192.168.4.162
Network time Protocol
 0.rhel.pool.ntp.org
2. 1.rhel.pool.ntp.org
2.rhel.pool.ntp.org
4. 192.168.4.162 A
X. NTP Service : stopped
A Add Server
S. SUDMIT
0. Return
Enter selection:

(3) 启动 NTP Service 服务

图9 启动服务

Network time Protocol
1. 0.rhel.pool.ntp.org
2. 1.rhel.pool.ntp.org
2.rhel.pool.ntp.org
4. 192.168.4.162 A
X. NTP Service : stopped
A. Add Server
U. Update time
S. Submit
0. Return
Enter selection: x
Select action (1. start, 2. stop, 3. restart, 0. return): 1
Starting ntpd: [OK]
Network time Protocol
Network time Protocol 1. 0.rhel.pool.ntp.org
Network time Protocol 1. 0.rhel.pool.ntp.org 2. 1.rhel.pool.ntp.org
Network time Protocol 1. 0.rhel.pool.ntp.org 2. 1.rhel.pool.ntp.org 3. 2.rhel.pool.ntp.org
Network time Protocol 1. 0.rhel.pool.ntp.org 2. 1.rhel.pool.ntp.org 3. 2.rhel.pool.ntp.org 4. 192.168.4.162 A
Network time Protocol 1. 0.rhel.pool.ntp.org 2. 1.rhel.pool.ntp.org 3. 2.rhel.pool.ntp.org 4. 192.168.4.162 A X. NTP Service : running
Network time Protocol 1. 0.rhel.pool.ntp.org 2. 1.rhel.pool.ntp.org 3. 2.rhel.pool.ntp.org 4. 192.168.4.162 A X. NTP Service : running A. Add Server
Network time Protocol 1. 0.rhel.pool.ntp.org 2. 1.rhel.pool.ntp.org 3. 2.rhel.pool.ntp.org 4. 192.168.4.162 A X. NTP Service : running A. Add Server S. Submit
Network time Protocol 1. 0.rhel.pool.ntp.org 2. 1.rhel.pool.ntp.org 3. 2.rhel.pool.ntp.org 4. 192.168.4.162 A X. NTP Service : running A. Add Server S. Submit 0. Return
Network time Protocol 1. 0.rhel.pool.ntp.org 2. 1.rhel.pool.ntp.org 3. 2.rhel.pool.ntp.org 4. 192.168.4.162 A X. NTP Service : running A. Add Server S. Submit 0. Return Enter selection:



NTP 服务用于时间同步,如不具备配置条件,可跳过此步骤。

2.4 验证配置

使用浏览器访问配置的 IP 地址,如何通过 https://IP 可以成功登陆运维审计系统,则说明单台运维 审计系统部署成功。

工单配置举例

Copyright © 2018 北京紫光恒越网络科技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。



3
্যম

日录
1 简介1
2 配置前提
3工单配置举例1
3.1 组网需求1
3.2 系统版本要求1
3.3 普通用户新建工单1
3.4 配置管理员审批
3.5 工单访问4
3.5.1 查看可访问工单4

1 简介

运维审计系统内置了工单,用于普通用户向管理员申请设备的临时访问权限。

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,配置前设备的所有参数均采用出厂时的缺 省配置。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。

3 工单配置举例

3.1 组网需求

图1 运维审计系统组网图



3.2 系统版本要求

适用产品版本: ESS 6102。

3.3 普通用户新建工单

(1) 登录 web

图2 创建工单

设备访问 🗸 🚽 工单管理 🛛 双人复核	•
我的工单	
您的当前位置: 更多任务 > 我的工单	
新建工单 工单名称:	工单状态: 全部 🗸
标题	创建时间

- (2) 填写工单基本信息
- 图3 工单内容

设备访问 ~ 工单管理 双人复核 ~
我的工单
您的当前位置: 新建工单
标题:
操作原因:
10 0-1++>10
操作细还:
操作类型: 日常维护 🗸
开始时间: 2018 🗸 年 01 🗸 月 24 🗸 日 20 🗸 : 37 🗸
结束时间: 2018 🗸 年 01 🗸 月 25 🗸 日 20 🖌 : 37 🗸
(Demoisting 4)
设备: <u>洗 揉 设 备</u> 查 <u>看</u> 您已选择了 0 个设备
系统帐号:选择系统帐号 查看 您已选择了0个系统帐号
服务类型:□字符终端 □图形终端 □文件传输
服务协议: 🗆 ssh 🗆 telnet 🗆 tn5250 🔤 rdp 🔤 vnc 🔤 rdpapp 🔤 ftp 🗔 sftp
服务名称:法 <u>提服务名称 查看</u> 您已选择了0个服务
命令:
操作: <u>确 定</u> 删除
添加

- 标题:填写所建工单的名称。
- 操作原因:工单操作的原因。
- 操作描述:操作步骤。
- 操作类型:可选"日常维护、抢修、实施、测试"。

- 时间:选择申请工单的时间段。
- Permission:
 - 。 设备:关联需要使用的设备。
 - 。 系统账号:关联需要使用的系统账号
 - 。 服务类型/服务协议/服务名称:关联需要使用的服务。
 - 。 命令: 描述使用中需要执行的命令
 - 。 操作:确认以上填写完成后按"确定"不需要这条 permission 则按"删除"。

图4 工单任务信息

[Permissio	on 1]
设备:	<u>查 看</u> 您已选择了1个设备
系统帐号:	查看您已选择了1个系统帐号
服务类型:	
服务协议:	ssh
服务名称:	查看您已选择了0个服务
命令:	ifconfig
操作:	编辑删除

(3) 新建工单中选项填写完成后,可以选择相应配置管理员审批或者留作模板及草稿。

图5 提交工单

审批人: admin | 缺省' >> 提交 保存为草稿 保存为模板 取消

3.4 配置管理员审批

(1) 当普通用户管理员申请工单后,配置管理员进入 Web 页面后可在右上角看到黄色"消息"提示。

图6 消息提示



(2) 点击<消息>可看到未处理的工单。

图7 未处理的工单

	状态	类型	产生时间	简要说明	过期时间	操作
1	未读	工单	2018-01-24 20:20:47	user01: 4	2018-01-25 20:15:00	详细
2	未读	工单	2018-01-24 20:10:56	user01: 1	2018-01-25 20:09:00	详细

(3) 点击<详细>可查看当前工单主要内容,允许按<授权>,不允许则按<驳回>。

图8 处理工单

您的当前位置	:
授权驳回	二 於 注/m
	上里许强
工单标题:	4
7781年1月1日 1月111日 1月11日 1月111日 1月111日 1月111 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月1111 1月1111 1月1111 1月1111 1月1111 1月1111 1月11111 1月11111 1月11111 1月11111 1月11111 1月11111 1月111111	4
操作类型:	日常维护
申请人帐号:	user01
申请人姓名:	测试用户01
帮信孙道:	2016-01-24 20.20.47
状态:	待审
审批人:	
申批结果: 关闭人:	
工单内容:	=== BEGIN REQUEST PERMISSIONS ===
	Start Time=2018-01-24 20:15:00
	End lime=2018-01-25 20:15:00
	[Permission 1]
	Users=user01 Servers=192 168 7 70
	Accounts=root
	Service Types=
	Service Frotos=ssn Service Names=
	Commands=ifconfig
	=== END REQUEST PERMISSIONS ===

(4) 点击后页面将会提示"操作成功",返回至[工单管理/全部工单]可查看工单当前的状态。

(5) 若有特殊情况,需要中断该工单的使用,可以点击<停用>,点击后将终止该工单的使用时限。

图9 停用工单

我的工事	我的工单 全部工单									
您的当前	您的当前位置: 更多任务 > 全部工单									
工单标题:申请时间: 2018 》年01 》月 21 工单状态: 申请人: 确定 共 1 页: < 50 60										
	标题	创建时间	创建人	创建人登录名	操作类型	状态	操作			
1	4	2018-01-24 20:20:47	测试用户01	user01	日常维护	待审	详细 授权 驳回			
2	1	2018-01-24 20:10:55	测试用户01	user01	日常维护	有效	详细 <mark>停用</mark>			

3.5 工单访问

3.5.1 查看可访问工单

当"配置管理审批后","普通用户"可登录 web 页面,打开[设备访问/工单访问],可查看当前可以 使用工单,停用或过期工单不会显示。

图10 查看可访问工单

设备	设备访问 工单管理 × 双人复核 ×									
按订	按访问规则分组 按部门分组 会话共享 工单访问									
您的	您的当前位置: 设备访问 > 工单访问									
	申请时间:2018 🗸 年 01 🗸 月 🗸 日 确定									
	标题	创建时间	创建人	创建人登录名	操作类型	状态				
1	1	2018-01-24 20:10:55	测试用户01	user01	日常维护	有效	<u>详细 设备访问</u>			

1. 工单详细

点击相应工单<详细>,可查看该工单的描述、有效时间、可访问情况。

图11 工单详细

我的工单	
您的当前位置	:
工操操操请请申单 軍 工单作作作人人请后 审批关单 加达型号名间复态人果人容:1993年3月30日,1993年3月30日,1993年3月3月3日,1993年3月3月,1993年3月3日,1993年3月3日,1993年3月3日,1993年3月3日,1993年3月3日,1993年3月3日,1993年3月3日,1993年3月3日,1993年3月3日,1993年3月3日,1993年3月3日,1993年3月3日,1993年3月3日,1993年3月3日,1993年3月3日,1993年3月3日,1993年3月3日,1993年3月3日,1993年3月3日,1993年3月3月3月,1993年3月3月,1993年3月3月,1993年3月3月,1993年3月3月,1993年3月3月,1993年3月3月,1993年3月3月,1993年3月3月,1993年3月11日,1993年3月3月,1993年3月3月,1993年3月3月,1993年3月3月,1993年3月3月,1993年3月3月,1993年3月3月,1993年3月3月,1993年3月3月,1993年3月3月,1993年3月3月,1993年3月3月,1993年3月3月,1993年3月3月,1993年3月11月,1993年3月3月,1993年3月3月,1993年3月3月,1993年3月4月,1993年3月3月,1993年3月11月,1993年3月3月,1993年3月3月,1993年3月,1993年3月3月,1993年3月3月,1993年3月3月,1993年3月3月,1993年3月11月,1993年3月11月,1993年3月,19934年3月,19934年3月,19934年3月,1994年3月,19934月,19934年3月,19934年3月,1994年3月,1993年3月,1993年3月,1993年3月,1993年3月,1993年3月,1993年3月,1993年3月,1993年3月,1993年3月,1993年3月,1993年3月,1993年3月,1993年3月,1993年3月,1993年3月,1993年3月,199354月,199348月,199348月,199348月,199348月,199348月,199348月,199344月,1994449,1994444444444544444544444444444	工单详细 1 1 1 1 日常维护 user01 mit用户01 2018-01-24 20:10:56 2018-01-24 20:13:38 有效 admin(缺省管理员) 同意 === BEGIN REQUEST PERMISSIONS === Start Time=2018-01-24 20:09:00 End Time=2018-01-25 20:09:00 [Permission 1] Users=user01 Servers=192.168.7.70 Accounts=root Service Types= Service Protos=ssh Service Protos=ssh Service Names= Commands=ifconfig === END REQUEST PERMISSIONS ===

2. 工单访问

(1) 点击相应工单<设备访问>,进入到设备访问页面,列出可访问设备,点击服务即可访问。

图12 工单访问

设备访问 工单管理 → 双人复	核 🗸							
按访问规则分组 按部门分组 会	会话共享 工单访问	1						
您的当前位置: 设备访问								
返回								
<u>设备名</u> ∓	<u>IPthth</u>	默认登录帐号	设备类型	简要说明				
192.168.7.70	192.168.7.70	root	General Linux					
服务	ssh							



左键点击服务图标将按照上次选择的访问情况进行访问。

右键点击服务图标,将弹出高级选项窗口,手工选择分辨率、账号、磁盘映射等选项进行访问。

(2) 如果目标设备为字符设备,也可通过 SecureCRT、PUTTY 等工具,其中 ws_1_1 为工单生成 的访问规则组,选择设备进行访问。

图13 工单访问

Putty 192.168.4.183 - Putty
login as: pt
Using keyboard-interactive authentication.
Password:
Copyright(c) 2005-2011, QiZhi Technologies. All Rights Reserved.
License granted to Test Customer, from 2013-11-19 to 9999-12-31.
Selected group: ws_1_1
Selected server: import-206 (192.168.5.206)
Selected account: root
1: ssh import-206
2: ssh-1 import-206
Select service:

命令权限与命令复核配置举例

Copyright © 2018 北京紫光恒越网络科技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。



1 简介	
2 配置	前提1
2.	1 设定规则的使用范围1
2.2	2 使规则生效1
2.3	3 命令权限的优先级·······1
2.4	4 命令基本语法1
2.	5 正则表达式·······2
2.	6 Shell元字符
2.	7 最小检查单位3
3 配置	举例3
3.	1 组网需求3
3.2	2 系统版本要求
3.:	3缺省策略为accept下的局部白名单配置举例 ····································
	3.3.1 需求简介3
	3.3.2 配置过程
3.4	4 缺省策略为deny下的局部黑名单配置举例4
	3.4.1 需求简介4
	3.4.2 配置过程
3.	5 命令复核配置举例5
	3.5.1 需求简介5
	3.5.2 配置过程5
3.	5 命令告警配置举例(syslog)6
	3.6.1 需求简介6
	3.6.2 配置过程6

目 录

1 简介

命令权限允许配置管理员设置规则,对用户通过 ssh 和 telnet 访问时执行的命令进行匹配,并对匹 配到的操作采取拒绝、切换或者告警动作。实现命令行级别的权限控制。

2 配置前提

要使用命令权限需要先了解基本的配置规则和方法

2.1 设定规则的使用范围

通过关联用户、设备和系统帐号可以设定规则的适用范围,如下图:

图1 设定规则的适用范围

	用户帐号	目标设备	系统帐号	命令行匹配	动作	监控级别	
1	admin	192.168.7.70	root	passwd	deny	None	编辑 插入
				reboot			关联: <u>用户组(0)</u> 用户(1)
							<u>设备组(0)</u> 设备(1)
							<u>系统帐号(1)</u> 命令复核人(0)

- (1) 如果不关联任何用户帐号、设备和系统帐号该规则对所有用户、设备和系统帐号均有效。
- (2) 如果关联了用户、设备和系统帐号规则仅对已关联的用户、设备和系统帐号有效。

2.2 使规则生效

新建或者修改规则后规则的变更不会立即生效,如下图:

图2 使规则生效

```
您的当前位置: 权限控制 > 命令权限
新建 部署 (当前策略未部署)
```

只要有"当前策略未部署"的标记存在就说明变更未生效,要使变更生效必须点击"部署",部署 后规则将在1分种后生效,生效后对已经存在的和新建的字符会话均有效。

2.3 命令权限的优先级

对于多条命令权限:

- (1) 运维审计系统进行逐条规则匹配,执行第一条符合条件的结果,不再考虑之后的规则。
- (2) 如果所有规则均不满足,按照缺省策略进行。

2.4 命令基本语法

(1) 如果不包含空格,表示只对命令部分进行匹配。

- (2) 如果包含空格,第一个空格以前的部分是对命令的可执行文件部分进行匹配,与上面的规则相同;后面的部分(包括其他空格)对命令的参数部分进行匹配:就是把命令行去掉命令本身之外的所有参数部分作为一个整体,与进行匹配。
- (3) 如果以"^"开头,或者包含"/"字符,表示严格匹配,即命令部分必须完全匹配正则表达式。比如"^passwd\$"只匹配"passwd"本身,前面加上任何字符都认为不匹配。比如"/usr/bin/passwd\$"只匹配"/usr/bin/passwd",任何其他路径或不写路径都不接受。否则将把命令的最后一个"/"字符后的部分拿来做匹配。比如"passwd\$"匹配"passwd"、"/usr/bin/passwd"、"asdf/passwd" 等。

2.5 正则表达式

符号	含义
	匹配任意字符:代表1位
٨	匹配字符串的开头
\$	匹配字符串的结尾
*	表示之前的模式可重复0-N次
+	表示之前的模式可重复1-N次
?	表示之前的模式可重复0-1次
{m}	表示之前的模式可重复m次
{m,n}	表示之前的模式可重复m-n次
{,n}	表示之前的模式可重复不超过n次
[]	表示可匹配方括号内出现的任意字符,可用"-"表示范围,如a-z、0-9等
[^]	表示可匹配方括号内未出现的任意字符,可用"-"表示范围,如a-z、0-9等
	表示可匹配A或B,这里A和B都可以是正则表达式
1	转义符,表示取消后面字符的特殊含义,仅表示该字符本身
/d	表示可匹配任意数字字符: "\D"表示可匹配任意非数字字符
\s	表示可匹配任意空白字符: "\S"表示可匹配任意非空白字符
\w	表示可匹配任意字母、数字或下划线; "\W"表示可匹配任意非字母、数字或下 划线
\r	表示回车
\n	表示换行
\t	表示制表符

所有的匹配都基于正则表达式。下表为正则表达式通配符的介绍:

2.6 Shell元字符

- (1) 对于 "&" 和 ";" 可以当做普通字符处理,比如: 禁止 ls;cat 或者 top&,直接写成 ls;cat 或者 top&。
- (2) 对于"|"需要使用"/"进行转义,比如,禁止 ls|xargs ls,应该写成 ls/|xargs ls。

2.7 最小检查单位

运维审计系统对命令的检查是以回车符为界限进行的,只有当用户按下回车提交命令后才会执行命 令权限检查。因此运维审计系统不会对 shell 的 key binding 进行检查。

3 配置举例

3.1 组网需求





3.2 系统版本要求

适用产品版本: ESS 6102。

3.3 缺省策略为accept下的局部白名单配置举例

3.3.1 需求简介

当缺省策略为 accept 时,指定的用户或指定的设备只允许执行列出的指令,其余命令均被禁止执行, 而其它用户或设备均采用默认策略。

3.3.2 配置过程

- (1) 建任意一条动作为 accept 的权限控制策略;
- (2) 建一条拒绝用户对相关设备所有操作的权限控制策略:在操作规则里填写命令.*(代表所有命 令),动作为 deny,确定后再关联与上一条规则相同的用户,设备,系统帐号。

建完以上2规则后单击部署。如下图范例:

图4 部署策略

新建	₹ ⁸⁰ 署										
	用户帐号	目标设备	系统帐号	命令行匹配	动作	监控级别					
1	<u>user01</u>	<u>192.168.7.70</u>	root	ifconfig Is	accept	None	編選 下移 插入 关联: 用产组(0) 用产(1) 设备组(0) 设备(1) 系统帐号(1) 命令复核人(0)				
2	<u>user01</u>	<u>192.168.7.70</u>	root	.*	deny	None	<u>編輯 上移 下移 插入</u> 关联: <u>用户组(0) 用户(1)</u> 设备组(0) 设备(1) 系统张号(1) 会令复核人(0)				

根据权限规则的优先级,先匹配规则 1,再匹配规则 2,最后再匹配全局缺省策略。规则 1 使用户 user01 仅可对目标设备 192.168.7.70 执行 ifconfig 和 ls 命令。虽然全局缺省策略为 accept,但因 规则 2 的存在,用户 user01 对目标设备 192.168.7.70 执行其它命令时将被拒绝。

3.4 缺省策略为deny下的局部黑名单配置举例

3.4.1 需求简介

当缺省策略为 deny 时,指定的用户或指定的设备只禁止执行列出的指令,其余命令均被允许执行, 而其它用户或设备均采用默认策略。

3.4.2 配置过程

- (1) 建任意一条动作为 deny 的权限控制策略;
- (2) 建一条允许用户对相关设备进行所有操作的权限控制策略:在操作规则里填写命令.*(.*代表 所有命令),动作为 accept,确定后再关联与上一条规则相同的用户,设备,系统帐号。
 建完以上 2 条规则后单击部署。如下图范例:

图5 部署策略

<u>user01</u>	<u>192.168.7.70</u>	root	passwd	deny	None	编辑 上珍 下移 插入 关联: 田户组(0) 田户(1) 设备组(0) 设备(1)
user01	192.168.7.70	<u>root</u>	*	accept	None	系統版号(1) 命令夏核人(0) (編編 上終 拡入 关联: 田庄姐(0) 田庄(1) 设备组(0) 设备(1) 系統版号(1) 命令夏核人(0)

根据权限规则的优先级,先匹配规则 1,再匹配规则 2,最后再匹配全局缺省策略。规则 1 中使用 户 user01 不可对目标设备 192.168.7.70 执行 passwd 命令。即使全局缺省策略为 deny,但因规则 2 的存在,用户 user01 可对目标设备 192.168.7.70 执行除 passwd 以外的任何命令。

3.5 命令复核配置举例

3.5.1 需求简介

某些重要命令需要第二个人复核后才可以执行。

3.5.2 配置过程

(1) 建立动作为 confirm 的命令权限规则

触发双人复核的前提条件是设置命令的触发动作为 confirm (如图)。

图6 建立动作为 confirm 的命令权限规则

您的当前位置: 权限控制 > 命令权限 > 设置									
操作规则:	passwd	 ✓ ✓ 							
动作:	⊖accept ⊖deny ⊖kill ●confirm	需要设置命令复核人才能生效;复核人不能复核自己触发的命令权限							
时间范围:									
	格式示例:w[1-3,5,7]m[1,3-5,12]d[1,5,7,31]D[20100213,20100215-20100220]T[08:30:00-16:00:00] 标识说明:'w'-每周(1-7),'m'-月份(1-12),'d'-日期(1-31),'D'-格式时间(YYYYMMDD),'T'-24小时制格式时间(HH:mm:ss) 以上时间标识不能重复,可以在[]内用,分隔多值,标识组之间以空格分隔。								
监控级别:	None	\checkmark							
邮件标题:		(级别至少到 WARN 的才会发送邮件)							
	确定 删除 返回								

(2) 再关联上复核人即可

图7 关联上复核人

<u>user01</u>	<u>192.168.7.70</u>	1083、③王即《二大歌《小大歌》2388 	· □ 111 ¥¥9,2326 登录名 admin user01	☆ + 以 < 姓名 読省管理员 测试用户01	1 > 60 码页15余 V 部门 ROOT ROO1	 上松 工経 拡入 (: 田庄坦(①) 田庄(1) 设备组(①) 设备(1) 系統性合(1) 命令复核人(1)
<u>user01</u>	192.168.7.70	1025	passwd	confirm	None	編編 上路 工班 抵入 关联:田户组 (0) 田户 (1) 没量组 (0) 没备 (1) 系统账号 (1) <u>@ 令夏時人 (1)</u>

🕑 说明

触发人和复核人不能是同一人。

(3) 触发

当用户访问设备时,输入了我们设置的命令,会出现如下提示(如图):

H3C:此命令需要复核人进行批准,等待超时时间为五分钟,确认请按Y

H3C:正在等待复核人审批,直到复核人进行操作或者超时,您可以按 Ctrl+C 退出此次请求。

图8 触发



(4) 复核

同时,复核人打开"双人复核"中的"命令复核"页面中会出现提示(如图):

图9 复核

基本控制 +	机限控制 ~	2602N -	事件事计 ~	IRIHIER ~	1426 -	日本任務 -	双人复枝							配置管理员 ~ abia ~
命令質核														
2010/11/06/2202	: 双人复核 >	命令解核												
< 2018 ₩	年 01 1 月	24 ~ 8 > 1	xa:	*										共1页: < 1
89							0.0	H/A	秋市	用户	10 B	IP地址	96-9	操作
passwd							2018	-01-24 19:53:04	等待审核	user01	192.168.7.70	192.168.7.70	root	分连 接納 切斷 金运信息 金运装柱

此时存在以下操作:

- 允许:此命令正常执行。
- 拒绝:此时请求人 user01 会收到提示不被允许执行。
- 切断:将 user01 用户打开的 session 窗口关闭。

3.6 命令告警配置举例(syslog)

3.6.1 需求简介

用户触发被限制的命令时,通过 syslog 方式实现告警功能。

3.6.2 配置过程

(1) 使用超级管理员登录,打开[策略配置/告警事件]页面,在 syslog 日志事件来源中勾选"命令 防火墙",只发送所选源事件级别设置为"INFO"。

- (2) 在 syslog 日志发送对象的"远程主机"中填写 syslog 服务器的 IP 地址,标识填写"Command warning",方便 syslog 服务器识别日志消息来源。
- 图10 配置日志信息

基本控制 🗸 事件审计	计 - 新昭祝晋 系统设置 - 工单管理 - 双人复核 -									
系统策略 告警事件	字符终端 会话配置 身份验证 设备密码 设备类型 部门配置 改密方式 密码代填 IE代填脚本									
您的当前位置: 策略配置 > 告答事件										
配置告警事件各类监控通知运行规则										
syslog日志事件来源: 🗌 身份验证 🗌 设备访问 🗹 命令防火墙 🗌 双人授权,只发送所送源事件级别不低于 🚺 NFO 🛛 🖌 的事件消息										
syslog日志发送对象:	远程主机: 101.1.11.2 , syslog机制: LOCAL0 V, 标识: Command warning									
通知邮件事件来源:	☑ 身份验证 ☑ 设备访问 ☑ 命令防火墙 ☑ 双人授权,只发送所送源事件级别不低于 WARN 💙 的事件消息									
通知邮件收件人:										
	(邮件收件人可以写邮件地址或用户名,或"self"表示事件触发者,多个项目用","分隔)									
通知短信事件来源:	🗹 身份验证 🗹 设备访问 🗹 命令防火墙 🗹 双人授权,只发送所选源事件级别不低于 🗰 WARN 💙 的事件消息									
通知短信收件人:										
(短信收件人可以写手机号码或用户名,或"self"表示事件触发者,多个项目用","分隔)										
	保存重设									

- (3) 点击<保存>按钮。
- (4) 使用配置管理员新建任意一条命令权限,监控级别设置为"WARN",邮件标题设置为 "Command warning"。

图11 权	艮 设置							
基本控制 ~	权限控制	密码控制 🗸	事件审计 🗸	统计报表 ~	工单管理 🗸	脚本任务 🗸	双人复核 🗸	
访问权限	命令权限							
您的当前位	置: 权限控制 >	命令权限 > 设	置					
操作规则:	зуз		0	*:				
动作: 时间范围:	⊖accept ⊚d	eny Okill C	confirm					
	格式示例: w[1- 标识说明: 'W'-每 以上时间标识不	3,5,7] m[1,3-5, 寡周(1-7),'m'-, 能重复,可以在	12] d[1,5,7,31] 月份(1-12),'d'- []内用,分隔多值	D[20100213,2(日期(1-31),'D' 』,标识组之间	0 100215-20100 -格式时间(YYYY 以空格分隔。	220] T[08:30:00 /MMDD),'T'-24)-16:00:00] 小时制格式时间](HH:mm:ss)
监控级别:	WARN		~					
邮件标题:	命令告警			(级别至少到 W	ARN 的才会发送	曲件)		
	确定删除	返回						

🕑 说明

监控级别设置的值要比告警级别处所设置的级别高,否则无法触发告警。

(5) 当用户访问设备输入了命令权限中设置的命令,就会触发告警事件。

图12 告警事件日志

Command warning: 命令告警(id=1498 service=cmdcheck server=H3C_Switch(101.102.1.2) account=admin identity=admin from=101.1.11.2 sys)

使用同名账户和密码登录目标设备配置举例

Copyright © 2018 北京紫光恒越网络科技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 系统账户说明
3 配置举例
3.1 组网需求
3.2 系统版本要求
3.3 AD集成配置举例2
3.3.1 组网需求
3.3.2 配置思路
3.3.3 配置过程
3.4 LDAP集成配置举例5
3.4.1 组网需求
3.4.2 配置思路
3.4.3 配置过程
4 常见问题

1 简介

使用同名账户和密码登录目标设备:是指使用运维审计系统自身的账户、密码登录目标设备。 这种方式适用于运维审计系统、目标设备上拥有同样的账户密码的情况下,在域环境下较为常见。

2 系统账户说明

运维审计系统默认存在如下账户(使用同名账户和密码的模式主要使用的是下面的"self"账户):

账户	说明
administrator	windows设备的默认管理账户
any	代表手工输入账户密码
enable	一般网络设备切换特权模式的命令
null	空账户,代表不输入账户名
root	linux设备默认的超级管理员
self	代表运维审计系统的同名账户

3 配置举例

3.1 组网需求

图1 运维审计系统组网图



3.2 系统版本要求

适用产品版本: ESS 6102。

3.3 AD集成配置举例

3.3.1 组网需求

拥有一台 AD 域控服务器和一台 Windows 的主机,需要将 Windows 的主机加入到 AD 域环境中。运维审计系统采用 AD 域的认证方式。

3.3.2 配置思路

运维审计系统和需要访问的目标设备都通过 AD 域来认证。 使用 "self" 账号登录目标设备时,运维审计系统使用域账号密码来登录目标设备。

3.3.3 配置过程

(1) 运维审计系统增加 AD 的认证方式

登录"超级管理员",新增 Idap 协议的认证方式。配置通过 AD 域控进行认证。

图2 增加 AD 的认证方式



(2) 新增账户,使用 AD 的认证方式

"基本控制 > 用户账号 > 新建用户"。

登录名要和 AD 上的账户一致,选择"身份验证方式"为之前配置的 AD。 Idap 用户名如果不填写,默认和登录名一致。

图3 新增账户

状态 :	○禁用 ●活动 (查看登录日志 查看可登录设备 分配用户组 管理访问规则 用户帐户设置)
登录名 :	testuser *
真实姓名:	testuser *
邮件地址 <mark>:</mark>	
手机号码:	
部门:	ROOT 🗸 *
职位:	
工号:	
身份验证方式 <mark>:</mark>	ad
ldap用户名:	
权限:	🗆 超级管理员 🗆 审计管理员 🗆 配置管理员 🗆 密码保管员 🗹 普通用户
	审计权限:□下载会话 □ 键盘事件
	(需要下载会话权限,必须勾选键盘事件权限)
	保存删除

(3) 添加目标设备

添加目标设备,该目标设备需要是 AD 域认证,不需要托管密码。

(4) 关联访问规则

登录"配置管理员", "权限控制 > 访问权限"。

图4 关联访问规则

基本控制 🗸	权限控制	密码控制 🗸	事件审计 🗸	统计报表 🗸	工单管理 🗸	脚本任务 🗸	双人复核 🗸		
访问权限 命令权限									
您的当前位置:	权限控制 >	访问权限							

关联之前配置的 AD 域认证的账户,关联之前添加的目标设备。

图5 关联访问规则

规则		部门	用户帐号	目标设备	系统帐号	服务类型	服务协议	服务名称	动作
1	test	ROOT	<u>admin</u>	192.168.21.13	any	字符终端	teinet ssh tn5250 rdp		编辑 發录规则 克隆规则
			testuser	192.168.8.135	root	图形终端	vnc rdpapp ftp sftp		关联: <u>用户组(0)</u> 用户(2)
				192.168.8.136	self	文件传输			设备组(0) 设备(5)
				192.168.8.139					系统帐号(3) 双人复核候选人(1)
				192.168.8.172					

点击"系统账号"。

图6 关联访问规则

规	11	部门	用户帐号	目标设备	系统帐号	服务类型	服务协议	服务名称	动作
1	test	ROOT	admin	192.168.8.135		字符终端	telnet ssh		编辑 登录规则 克隆规则
			<u>test</u>	192.168.8.136		图形终端	tn5250 rdp vnc		关联: <u>用户组(0)</u> 用户(2)
						<u>文件传输</u>	rdpapp ftp sftp		<u>设备组(0)</u> <u>设备(2)</u>
									系统帐号(0) 双人复核候选人(0)

选择"self"账户,点击"建立关联"。

图7 建立关联

选择系统帐号:访问控制组		\$
状态:④全部〇已关联〇末关联 过滤:]□ 精确过滤	共1页 < 1 > G0 每页15条 >
□全选	帐号名称	
	administrator	
	any	
	enable	
	netscreen	
	nul	
	root	
	self	
	super	

选择相应账户登录,切换到普通用户。

选择相应的目标设备,右键点击相应服务,选择"self"账户。点击确定。

建立关联 取消关联 关闭

图8 登录设备

□全选	<u>设备名</u> ₹	<u>IP地址</u>	默认登录帐号	设备类型
	192.168.8.135	设备访问:高级		×
骄		系统帐号: *self > 屏幕大小: 800x600	e ☑ mstsc	
	192.168.8.136	磁盘映射: 🗌 c: 🗌 d	: 🗌 e: 🗌 f: 🗌 g: 🗌 h: 🗌 i: 🗌 j: <u>更多</u>	
	192.168.8.172	确定		

直接登录进入系统。

图9 登录设备



3.4 LDAP集成配置举例

3.4.1 组网需求

- (1) 拥有一台 Idap 服务器。
- (2) 拥有一台 linux 的主机,并且采用 ldap 方式认证。
- (3) 运维审计系统采用 Idap 的认证方式。

3.4.2 配置思路

- (1) 运维审计系统和需要访问的目标设备都通过 ldap 认证。
- (2) 使用"self"账号登录目标设备时,运维审计系统使用域账号密码来登录目标设备。

3.4.3 配置过程

- (1) 运维审计系统增加 ldap 的认证方式。
- 登录"超级管理员",新增 Idap 协议的认证方式。

图10 增加 Idap 的认证方式

方式:	Idap	
状态:	启用服务器1 ▼	
名称:	ldap	
方法:	SIMPLE •	[帮助]
服务器1地址:	192.168.8.139	(服务器地址
服务器1端口:		(留空表示缺
服务器 <mark>2</mark> 地址:		(服务器地址
服务器 <mark>2</mark> 端口:		(留空表示胡
查询用户DN:	cn=Manager,dc=test,dc=com	(如CN=Adn
查询用户密码:		
用户basedn:	ou=People,dc=test,dc=com	(如CN=Use
用户filter:	cn={username}	(如(&(objec
SSL:		

(2) 新增账户,使用 Idap 的认证方式

"基本控制 > 用户账号 > 新建用户"。

登录名要和 ldap 上的账户一致,选择"身份验证方式"为之前配置的 ldap。 ldap 用户名如果不填写,默认和登录名一致。

图11 新增账户

状态:	◎ 禁用 ● 活动 (查看登录日志 查看可登录设备 分配用户组 管理访问规)
登录名 :	Idapuser1 *
真实姓名:	Idapuser1 *
邮件地址:	
手机号码:	
部门:	ROOT *
职位:	
工号 :	
身份验证方式 <mark>:</mark>	Idap
ldap用户名:	
权限:	🔲 超级管理员 🔲 审计管理员 🔲 配置管理员 🔲 密码保管员 🗹 普通用户
	审计权限: 🔲 下载会话 🔲 键盘事件
	(需要下载会话权限,必须勾选键盘事件权限)
	保存删除

(3) 添加目标设备

添加目标设备,该目标设备需要是 ldap 认证,不需要托管密码。

(4) 关联访问规则

登录"配置管理员","权限控制 > 访问权限"。

图12 关联访问规则

基本控制 🗸 权限控制	密码控制 🗸	事件审计 🗸	统计报表 🗸	工单管理 🗸	脚本任务 🗸	双人复核 🗸	
访问权限 命令权限							
您的当前位置: 权限控制 >	访问权限						

关联之前配置的 AD 域认证的账户,关联之前添加的目标设备。

图13 关联访问规则

规贝		部门	用户帐号	目标设备	系统帐号	服务类型	服务协议	服务名称	动作
1	test	ROOT	<u>admin</u>	192.168.21.13	any	字符终端	telnet ssh tn5250 rdp		编辑 登录规则 克隆规则
			<u>testuser</u>	<u>192.168.8.135</u>	root	图形终端	vnc rdpapp ftp sftp		关联: <u>用户组(0)</u> 用户(2)
				192.168.8.136	self	文件传输			设备组(0) 设备(5)
				192.168.8.139					系统帐号(3) 双人夏核候决人(1)
				192.168.8.172					

点击"系统账号"。

图14 关联访问规则

规风	Ŋ	部门	用户帐号	目标设备	系统帐号	服务类型	服务协议	服务名称	动作
1	test	ROOT	admin	192.168.8.135		字符终端	telnet ssh		编辑 登录规则 克隆规则
			<u>test</u>	<u>192.168.8.136</u>		图形终端	tn5250 rdp vnc		关联: <u>用户组(0)</u> 用户(2)
						<u>文件传输</u>	rdpapp ftp sftp		<u>设备组(0)</u> <u>设备(2)</u>
									系统帐号(0) 双人复核候选人(0)

选择"self"账户,点击"建立关联"。

图15 建立关联

选择系统帐号:访问控制组			×
状态: ⑧全部〇已关联〇未关联 过滤:	□ 精确过滤	共1页 < 1 > G0 每页15条 >	
□全选	帐号名称		
	administrator		
	any		
	enable		
	netscreen		
	null		
	root		
	self		
	super		
		建立关联 取消关联 关闭	

(5) 登录设备

选择相应账户登录,切换到普通用户。

选择相应的目标设备,右键点击相应服务,选择"self"账户。点击确定。

图16 登录设备

192.168.8.22	0	192.16	8.8.220	无	Gene
1.000	REAL		设备访问]:高级	
<u>Ce</u>	Ve		系统帐号	≓: * selt ∨	
ssh	vnc			确定	

直接登录进入系统。

图17 登录设备



4 常见问题

在双因素认证情况下, self 账号使用什么密码登录? 答: 使用第一身份认证密码。

手机令牌(Mobile APP)配置举例

Copyright © 2018 北京紫光恒越网络科技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。


1 简介1
2 配置前提
3 配置举例1
3.1 组网需求1
3.2 系统版本要求1
3.3 创建手机令牌认证方式1
3.4 配置手机令牌认证方式2
3.5 配置MIX认证方式,绑定手机令牌2
3.6 创建用户3
3.7 登录认证4
4 常见问题6

1 简介

手机令牌(TotpMobile)是基于时间的一次性密码(Totp)在手机客户端上的一次实现。依赖于种子文件和算法,通过时间戳,每30秒产生一个6位随机密码,来提供用户的登录验证服务。运维审计系统的手机令牌功能只适用于双因素认证的场景。

2 配置前提

- (1) 因为手机令牌与时间密切相关,所以在配置手机令牌前,请确保运维审计系统的时间与北京时间一致。
- (2) 因为手机令牌与时间密切相关,所以在手机登录前,确保手机的时间和北京时间一致。

3 配置举例

3.1 组网需求





3.2 系统版本要求

适用产品版本: ESS 6102。

3.3 创建手机令牌认证方式

登录"超级管理员","策略配置 > 身份验证",选择"totp(mobile)",点击"新建"。

图2 创建手机令牌认证方式

基本控制 ~	事件审计	→ 策略	配置 3	系统设置 ~	工单管理 ~	双人复核、					
系统策略	告警事件	字符终端	会话配置	身份验证	设备密码	设备类型	部门配置	改密方式	密码代填	IE代填脚本	
您的当前位	悠的当前位置: 策略配置 > 身份验证										
▲ HA 状态错误:备机数据同步失败,备点失败,GE0/0 失败,GE0/1 失败											
协议 <mark>· totp(mobile) ✓ 新建</mark>											

3.4 配置手机令牌认证方式

状态:选择为启用。

名称: 该手机令牌认证的名称。

标识:手机 APP 上该用户的标识。(因为手机 APP 上可能存在多个账户,标识这个账户属于运维 审计系统)。

图3 配置手机令牌认证方式

重要提示: TOTP(mobile)需要开启NTP服务器,请在console2中进行配置 _{方式:totpmobile}

状态:启用 ~
名称 totpmobile
标识 secpath
确定 重设 取消

3.5 配置MIX认证方式,绑定手机令牌

将第二身份验证方式选择为刚才配置的手机令牌名称。

图4 配置 MIX 认证方式

□连续验证失败时锁定用户帐号								
协议:	Mix							
状态:	启用	v						
名称:	MIX							
第一身份验证方式:	本地认证 (native)	v						
第二身份验证方式:	totpmobile (totpmobile)							
逻辑验证方式:	与	✓ (逻辑验证"与":用户依次输入对应两种身份验证方式的密码并通过验证即为成功登录)						
*注:								
1、可选身份验证组合	锄议: native,ldap,radius							
2、两种身份验证方式	(不可选择相同的协议,例如: 第一和第二	身份验证方式同时选择ldap协议						
3、用户密码代填使用第一身份验证方式的登录密码								
4、配置逻辑验证方式"与":密码分割符默认为空格,例如:登录密码123 456,其中第一身份验证方式密码123,第二身份验证方式密码 456								
确定 重设 取消								

3.6 创建用户

"基本控制 > 用户账号 > 新建用户"。

图5 创建用户

基本控制	权限控制 🗸	密码控制 ~	事件审计 ~	统计报表 🗸	工单管理 ~	脚本任务 🗸	双人复核 ~				
用尸账号	系统帐号 目	目标设备 用户分	组 设备分组	E							
您的当前位置: 基本控制 > 用户帐号											
新建用户	批量导入 批	上 量修改 导出月	日户 状态: 沅	5动 ~ 身份	设验证:	✓ 部门: RO	от <u>~</u> 过	期帐号:	✓ 过滤:	 过滤未登录用户	4 ~

- 登录名:登录运维审计系统的账户名。
- 真实姓名:该账户名的真实用户。
- 部门:选择相应的部门。
- 身份验证方式:这里选择之前配置的 mix。
- 设置密码&确认密码:这里设置第一身份验证方式的本地密码。

图6 配置用户信息

状态:	○禁用 ●活动 (查看登录日志 查看可登录设备 分配用户组 管理访问规则 用户帐户设置)
登录名:	testuser *
真实姓名:	testuser *
邮件地址:	
手机号码:	
部门:	ROOT ×
职位:	
工号:	
身份验证方式:	MIX
密码:	手工输入 🛛 🔽 * 🤡
设置密码:	* 🔮
确认密码:	* 🔮
	□ 下次登录时提示进行OTP认证配置
	🗆 下次登录时须修改密码 🗆 设置密码有效期(90 天)
权限:	🗆 超级管理员 🗆 审计管理员 🗆 配置管理员 🗆 密码保管员 🗹 普通用户
	审计权限:□下载会话 □ 键盘事件
	(需要下载会话权限,必须勾选键盘事件权限)
	保存删除

3.7 登录认证

(1) 输入账户名密码,这里的密码是第一身份验证方式的本地密码。

图7 输入账户名密码



(2) 如果是第一次登录,需要扫码完成绑定。

首先点击"Google Authenticator",将出现下载二维码,下载手机 APP。

图8 下载手机 APP



- (3) 手机 APP 扫描二维码,完成绑定操作后,点击"完成绑定"。
- 图9 绑定手机



(4) 输入手机 APP 产生的,相应账户、相应标识的 6 位数密码。

图10 登录

两步认证	密码:●●●●●	
	登录	

4 常见问题

- (1) 为什么创建用户时,不能勾选手机令牌认证方式?
- 答: 在运维审计系统中, 手机令牌认证方式必须同其他认证方式绑定, 必须是双因素认证。
- (2) 如果手机丢失,或者换手机,如何重新绑定?
- 答:在相应用户账号中,勾选"下次登录时提示进行 OTP 认证配置"。

× *

密码: 不改变☑ 下次登录时提示进行OTP认证配置

□ 下次登录时须修改密码

- 权限: □ 超级管理员 □ 审计管理员 □ 配置管理员 □ 密码保管员 ☑ 普通用户 审计权限:□ 下载会话 □ 键盘事件 (需要下载会话权限,必须勾选键盘事件权限)
- (3) 为什么登录老验证不成功?
- 答: 请检查运维审计系统时间、手机时间是否与北京时间一致。
- (4) 进入账户设置、rdp 直连、ssh 直连时的密码如何输入?
- 答:格式为,第一身份验证方式+"空格"+手机令牌密码。

双因素认证(MIX)配置举例

Copyright © 2018 北京紫光恒越网络科技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。



1
1
1
·1
•1
·1
·2
.3
.3

1 简介

双因素认证(MIX)是指,将运维审计系统已有的认证方式(本地认证、ldap认证、radius认证、 TOTP 令牌认证、TOTPMobile认证)两两组合的一种更高强度的认证方式。被组合的两种认证方 式可以是逻辑关系上的"与""或"关系。"与"代表两种验证方式都验证成功,才能登录成功, "或"代表两种验证方式有一种成功,就能登录成功。

2 配置前提

准备两种运维审计系统已有的认证方式。

其中第一身份验证方式只能是本地认证、ldap 认证、raidus 认证其中之一。 第二身份验证方式只能是:本地认证、ldap 认证、raidus 认证、TOTPMobile 认证其中之一。

3 配置举例

3.1 组网需求





3.2 系统版本要求

适用产品版本: ESS 6102。

3.3 创建MIX认证方式

超级管理员登录后,选择"策略配置 > 身份验证"。

图2 创建 MIX 认证方式

基本控制 🗸	事件审计	→ 策略	配置 3	系统设置 🗸	工单管理 🗸	双人复核	~					超级管理员 🗸
系统策略	告警事件	字符终端	会话配置	身份验证	设备密码	设备类型	部门配置	改密方式	密码代填	IE代填脚本		
您的当前位置	您的当前位置: 策略配置 > 身份验证											
协议: Idap		< ✓ 新建										
		名称			协议				状态		动作	
1		本地认证			nativ	e			启用		设置	
2		ldap			ldap				启用		编辑测试删除	

选择"协议"为"双因素组合(MIX)",点击新建。

图3 选择协议

hivi:双因素组合(Mix) 1/ 新建											
	名称	协议	状态	动作							
1	本地认证	native	启用	<u>设置</u>							
2	ldap	ldap	启用	编辑 测试 删除							

3.4 编辑MIX认证方式

- 状态:选择为"启用"。
- 名称:给当前 MIX 认证取名。
- 第一身份认证方式:这里选择本地认证。
- 第二身份认证方式:这里选择之前配置的 ldap。
- 逻辑验证方式:这里选择"与"的关系,两个身份验证都通过则登录成功。

图4 编辑 MIX 认证方式

协议:	Mix	
状态:	启用	\checkmark
名称:	mix	
第一身份验证方式:	本地认证 (native)	\checkmark
第二身份验证方式:	ldap (ldap)	\sim
逻辑验证方式:	与	🔽 (逻辑验证"与": 用户依次输
*注:		
1、可选身份验证组合	协议:native,Idap,radius	
2、两种身份验证方式	不可选择相同的协议,例如:第一和第二身	P份验证方式同时选择ldap协议
3、用户密码代填使用;	第一身份验证方式的登录密码	
4、配置逻辑验证方式	"与":密码分割符默认为空格,例如:登录	密码123 456,其中第一身份验证
确定 重设 取消		

3.5 创建用户,绑定MIX认证方式

"基本控制 > 用户账号",点击"新建用户"。

图5 创建用户



- 登录名:登录运维审计系统的账户名。
- 真实姓名:该账户名的真实用户。
- 部门:选择相应的部门。
- 身份验证方式:这里选择之前配置的 mix。
- 设置密码&确认密码:这里设置第一身份验证方式的本地密码。
- Idap 用户名: 绑定该登录名对应的 Idap 账户,如果不填,则默认此项为登录名。

图6 配置用户信息



3.6 登录认证

密码部分填写 MIX 认证的双因素密码。 格式为: "第一验证密码"+"空格"+"第二验证密码"。

图7 登录设备



文件传输配置举例

Copyright © 2018 北京紫光恒越网络科技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。



1 简介1
1.1 文件传输方式1
1.2 文件传输客户端和服务端1
2 配置举例2
2.1 组网需求
2.2 系统版本要求
2.3 Windows磁盘映射文件传输配置举例2
2.3.1 管理员启用RDP磁盘映射2
2.3.2 普通用户使用方法
2.3.3 审计管理员查看审计记录
2.4 Linux/Unix rz/sz文件传输配置举例
2.4.1 配置前提
2.4.2 上传和下载
2.4.3 审计5
2.5 Linux/Unix sftp/scp 文件传输配置举例(不推荐)
2.5.1 配置前提6
2.5.2 管理员启用sftp服务
2.5.3 普通用户访问7
2.5.4 审计

1 简介

1.1 文件传输方式

运维审计系统传输文件的方式很多,根据目标设备的不同主要有两大类:

(1) Windows:

rdp 方式、ftp 方式。

(2) Linux 和类 UNIX:

rzsz 方式、sftp/scp 方式(仅 OpenSSH)、ftp 方式(仅 vsftpd)。 推荐在 Windows 环境下使用 rdp 方式;在 Linux 和类 UNIX 环境下使用 rzsz 方式。 Sftp、ftp 和 scp 的服务器及客户端环境配置复杂且存在存在兼容性问题,不推荐使用。

1.2 文件传输客户端和服务端

运维审计系统对文件传输的客户端和服务端的使用要求请参见如下两个表格

表1 文件传输客户端

客户端	使用备注
scp命令	scp 1.txt user@shtermip:/serverip/account/var/testdir
FileZilla客户端	WEB页面访问/客户端直连
WinSCP客户端	客户端直连
zmodem	SecureCRT/Xshell进行文件传输
rdp	rdp进行复制/粘贴文件

表2 文件传输服务端

服务端	FTP 服务/软件
Linux/Unix ftp	vsftpd
Linux/Unix sftp	openssh
Windows ftp	IIS自带的FTP(目录浏览样式设置为UNIX)

2 配置举例

2.1 组网需求

图1 文件传输配置组网图



2.2 系统版本要求

适用产品版本: ESS 6102。

2.3 Windows磁盘映射文件传输配置举例

2.3.1 管理员启用RDP磁盘映射

进入"配置管理员","基本控制 > 目标设备"。 选择相应的 windows 设备,点击"编辑",进入"服务列表",编辑 rdp 服务。 勾选"客户端磁盘映射",勾选剪切板相关的配置。

图2 编辑 rdp 服务

状态	○禁用 ◉活动	
名称:	rdp	*
RDP端口:	3389	
	连通检测	
协议选项:	☑ 客户端磁盘映射 ☑ console模式	
应用发布服务器:		
剪贴板:	☑下行☑上行	
剪切板复制文件:	☑下行☑上行	
服务图标:	9	
	确定 默认填写 返回前页	

进入"配置管理员","权限控制 > 访问权限"。 选择相应访问规则,点击"编辑"。

勾选"磁盘映射",勾选剪切板相应选项。

图3 编辑访问规则

创建者:	admin (缺省管理员)		
规则名称:	test		*
设备排序:	全局缺省	\sim	(终端登录菜单中的目标设备排序方式)
部门:	ROOT	\sim	*
服务类型:	🗹 字符终端 🗹 图形终端 🗹 文件传输		
服务协议:	🗹 telnet 🗹 ssh 🗹 tn5250 🗹 rdp 🗹 vno	c 🗹	rdpapp 🗹 ftp 🗹 sftp
服务名称:	□rdp □vnc	□ s	ish
	访问设备时生成事件		
事件级别:	None	\sim	
标题:			
磁盘映射:	☑ 允许使用		
剪贴板:	☑下行☑上行		
剪切板复制文件:	☑下行☑上行		
	确定 删除 取消		

2.3.2 普通用户使用方法

进入"普通用户"。 选择相应设备的 RDP 服务,右键点击。 勾选需要映射的磁盘。

图4 普通用户使用方法

	<u>设备名</u> ∓		<u>IP地址</u>	默认登录帐号	设备类型
	192.168.8.135	设备访问:高	级	AAP.	×
服务	rdp	系统帐号: 屏幕大小:	*self ~ 800x600 ~		
2	192.168.8.136	2分中山中 自十。	□ console ⊵ msts	50 4 1 - 1 1 1 1 1 1 1 1 1	_ii
3 🗆	192.168.8.172	W\$\$1111(1天为1)。		n; ∟ g; ∟ n; ∟ l; ∟]; <u>更多</u>	: \
			佣定		

2.3.3 审计管理员查看审计记录

进入"审计管理员","会话审计 > 文件传输"。

通过服务过滤 rdp 服务。

图5 审计管理员查看审计记录

≪ 2018 ∨ 年 01 ∨ 月	31 ~ 日 》 过滤	用户:	服务: <mark>rdp ~</mark>	类型:	``	✓ 结果:	< 1 >	(50 文	件查询
时间	来自	用户	去往	帐号	类型	路径	传输里	属性	结果	备注
2018-01-31 11:32:26	192.168.25.1	admin	192.168.8.135 (192.168.8.135)	self	下载文件	Toad for Oracle 12.10.1nk	1.8 KB		成功	
2018-01-31 11:32:19	192.168.25.1	admin	192.168.8.135 (192.168.8.135)	self	上传文件	软raid修复.docx	37.44 KB		成功	

2.4 Linux/Unix rz/sz文件传输配置举例

2.4.1 配置前提

目标 linux 设备安装有 lrzsz 的包。 本地 PC 需要有支持 ZModem 的 SSH 客户端。

2.4.2 上传和下载

通过运维审计系统访问目标设备。 输入"rz"命令,进行文件上传。 图6 上传文件



输入"sz 文件名",进行文件下载。

图7 下载文件

[root@localnost ~]#		
[root@localhost ~]#	浏览文件夹	×
[root@localhost ~]# sz key.pub		
	注洪这原方按收立他的立伊士,	
	谓匹件休行按收又件的又件关;	
	> 🐔 OneDrive	^
	> 🤱 xhf	
	✓ ■ 此电脑	
	> 🙀 视频	
	> 圖 文档	
	> 上 下载	
	→ 音乐	
		~
	文件夹(E): ^{吴山}	
	2	_
	新建文件夹(<u>M</u>) 确定 取消	

2.4.3 审计

进入"审计管理员", "会话审计 > 文件传输"。 通过服务过滤 zmodem 服务。

图8 审计

≪ 2018 ∨ 年 01 ∨ 月	31 ~日 》 这	滤用户: [服务: zmodem v	类型:		~ 结果:		⊻ 共1页: < 1 > 0	io 文	牛查询
时间	来自	用户	去往	帐号	类型	路径	传输量	属性	结果	备注
2018-01-31 13:49:42	192.168.25.1	admin	192.168.8.136-new (192.168.8.136)	root	下载文件	key.pub	408 B	perm:100644 mtime:1487041022	成功	
2018-01-31 13:41:37	192.168.25.1	admin	192.168.8.136-new (192.168.8.136)	root	下载文件	xuhf.pub	408 B	perm:100644 mtime:1488352641	成功	

2.5 Linux/Unix sftp/scp 文件传输配置举例(不推荐)

2.5.1 配置前提

sftp 和 scp 都依赖于目标设备提供 sshd 服务。 使用 sftp 需要本地 PC 拥有 filezilla 软件。

2.5.2 管理员启用sftp服务

1. 仅个别设备开启

进入"配置管理员","基本控制 > 目标设备"。 选择相应设备,进入"服务列表",增加 sftp 服务。

图9 增加 sftp 服务

设备编辑:19	92.168.8.13(192.16	8.8.136)	服务列表	密码管理	密钥管理	分配设备组	访问规则	可登录用户		
提示:正	常访问本页面需要	要装We	bClient.	「載 已安	装				Х	
	sftp 新增									
类型		名称		状态						
s	sh	ssh		活动		编辑删除				
v	/nc	vnc		活动		编辑 删除				

2. 特定设备类型默认开启

进入"超级管理员","策略配置"-"设备类型"。 选择需要默认开启的设备类型,点击"管理",新增默认文件传输方式为 sftp。

图10 选择需要默认开启的设备类型



进入"配置管理员","权限控制 > 访问权限"。 选择相应的访问规则,点击"编辑",勾选 sftp 服务。

图11 选择 sftp 服务

创建者:	admin (缺省管理员)		
规则名称 <mark>:</mark>	test		*
设备排序:	全局缺省	\sim	(终端登录菜单中的目标)
部门:	ROOT	\sim	*
服务类型:	🗹 字符终端 🗹 图形终端 🗹 文件传输		
服务协议:	⊻ telnet ⊻ ssh ⊻ tn5250 ⊻ rdp ⊻ vr	nc 🗹	d rdpapp 🗹 ftp 🗹 sftp
服务名称:	□ftp □sftp □vnc		rdp ash
	访问设备时生成事件		
事件级别:	None	\sim]
标题:	secpath_access		
磁盘映射:	☑ 允许使用		
剪贴板:			
剪切板复制文件 <mark>:</mark>	☑下行☑上行		
	确定 删除 取消		

2.5.3 普通用户访问

1. Web页面启动filezilla

进入"普通用户",选择相应设备,右键点击 sftp 服务。

• 托管密码方式

系统账户,选择已经托管密码的系统账户(前面有个*)。

图12 托管密码方式

全选	<u>设备名</u> ∓	<u>IP地址</u>	默认登录帐号	设备类型 简要
	192.168.8.135	192.168.8.135	self	Microsoft Windows
	192.168.8.136	192.168.8.136	root	
务	ssh vnc			设备访问记录数 系统帐号: <mark>*root ></mark> 确定
	192.168.8.136-new	192.168.8.136	root	
	192.168.8.172	192.168.8.172	any	

• 不托管密码方式

系统账户,选择 any 账户。输入用户名、密码。

图13 不托管密码方式

192.168.8.135	192.168.8.135	self		Microsoft Windows	
192.168.8.136	192.168.8.136	root	设备访问:高级		×
			系统帐号: 用户名 root	密码●●●●●●	
ssh vnc	ftp sft	р	确定		
192.168.8.136-new	192.168.8.136	root			
192.168.8.172	192.168.8.172	any			
192.168.8.220	192.168.8.220	self		General Linux	

2. Filezilla直连

- (1) 打开本地 PC 的 filezilla 软件。
- 主机格式为: sftp://运维审计系统 IP
- 用户名:运维审计系统普通用户账户名。
- 密码:运维审计系统普通用户密码。

图14 Filezilla 直连

) 	主机(日	: sftp://192.168.25. 用户名(U): admin	密码(<u>W</u>)	••••	端口(P):	快速连接(Q)	•
	状态:	正在连接 192.168.25.136					

(2) 选择目标设备。

图15 选择目标设备

	192.168.8.220 sftp (192.168.8.220)
	192.168.8.136 sftp (192.168.8.136)
	192.168.8.136 ftp (192.168.8.136)
	192.168.21.13 ftp (192.168.21.13)

(3) 选择目标设备的系统账户(该账户必须在运维审计系统托管了账户密码)。

图16 选择目标设备的系统账户

文件名	文件大小
	
self	
root	

(4) 列出目标设备的目录。

图17 列出目标设备的目录

文件名	文件大小	文件类型	最近修改	权限	所有者/组
autofsck	0	AUTOFSC	2017/12/13 8:47:12	-rw-rr	root root
111.txt	28	文本文档	2016/11/16 12:05:52	-rw-rr	root root
autorelabel	0	AUTOREL	2016/6/17 9:36:53	-rw-rr	root root
- root		文件夹	2018/1/31 14:10:11	dr-xr-x	root root
		文件夹	2018/1/31 3:27:02	drwxrwxrwt	root root
etc		文件夹	2018/1/26 12:48:28	drwxr-xr-x	root root
home		文件夹	2018/1/19 10:01:50	drwxr-xr-x	root root
dev		文件夹	2017/12/13 8:47:19	drwxr-xr-x	root root
sys		文件夹	2017/12/13 8:47:09	drwxr-xr-x	root root
proc		文件夹	2017/12/13 8:47:09	dr-xr-xr-x	root root
en media		文件夹	2017/12/12 18:49:30	drwxr-xr-x	root root

3. scp

支持 scp 命令的客户端可以直接将本地文件,通过运维审计系统发送至目标设备。

scp 的格式为:

scp 文件名 运维审计系统用户账号@运维审计系统主机地址:/目标设备地址/ftp 帐户/目标设备目录 如果 admin(用户帐户)要通过运维审计系统(192.168.25.136)使用 root 账户,将本机的 aa 文件上传到目标设备(192.168.8.136)的/root/xuhf 目录中,可以使用如下命令:

scp ./aa admin@192.168.25.136:/192.168.8.136/root/root/xuhf

- 运维审计系统用户账号为: admin
- 运维审计系统的主机地址为: 192.168.25.136
- 目标设备地址为: 192.168.8.136
- 目标设备的 sftp 帐户为: root
- 相应工作目录为 root/xuhf

[root@localhost ~]# scp ./aa admin@192.168.25.136:/192.168.8.136/root/root/xuhf Password: aa 100% 11 0.0KB/s 00:00

2.5.4 审计

进入"审计管理员","会话审计 > 文件传输"。

通过服务过滤 sftp/scp 服务。

图18 审计

≪ 2018 ∨ 年 01 ∨ 月 31	✓ 日 ▶ 过滤用户:		服务: scp v 类型:	~ 结	果:	\sim	共1页:	< 1 >	Go 戈	7件查询
时间	来自	用户	去往	帐号	类型	路径	传输里	属性	结果	备注
2018-01-31 16:47:56	192.168.25.131	admin	192.168.8.136 (192.168.8.136)	root	上传文件	aa	11 B	perm=0644	成功	
2018-01-31 16:41:56	192.168.25.131	admin	192.168.8.136 (192.168.8.136)	root	上传文件	aa	11 B	perm=0644	成功	
2018-01-31 16:40:54	192.168.25.131	admin	192.168.8.136 (192.168.8.136)	root	上传文件	aa	11 B	perm=0644	成功	

应用发布配置举例

Copyright © 2018 北京紫光恒越网络科技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。



1 应用中心介绍1
1.1 支持Windows server 2008 的版本1
1.2 RemoteApp应用发布介绍······1
1.3 RemoteApp对终端的要求······1
1.4 应用中心授权许可介绍1
2 配置前提
2.1 安装前准备
2.1.1 硬件配置
2.1.2 操作系统
2.1.3 网络2
2.1.4 RDS授权码
3应用发布服务器配置准备
3.1 安装远程桌面服务(必配步骤)3
3.2 应用中心激活授权(如果是测试客户,可忽略此操作)12
3.2.1 激活应用中心
3.2.2 安装应用中心授权许可证20
3.3 调整应用中心的策略(必配步骤)29
3.3.1 调整本地组策略
3.3.2 设置RD授权模式33
3.3.3 允许用户在初始连接时启动列出和未列出的程序
3.3.4 关闭windows防火墙
3.3.5 关闭IE增强的安全配置40
3.3.6 开启远程桌面
3.3.7 关闭屏幕保护 42
3.3.8 启用屏幕保护程序超时44
3.4 在应用中心中安装相关的工具 45
3.4.1 安装客户端工具
3.4.2 安装winlogon 45
4 运维审计系统与应用中心结合使用
4.1 组网需求
4.2 系统版本要求
4.3 运维审计系统添加应用发布服务器
4.4 C/S应用发布

目 录

	4.4.1 发布应用	49
	4.4.2 密码代填	50
4.5	B/S应用发布	56
	4.5.1 IE浏览器	- 56
	4.5.2 Chrome浏览器	63
4.6	配置访问权限	67
4.7	普通用户访问	68

1 应用中心介绍

应用中心由 windows server 2008 服务器平台搭建的。 应用中心用于安装应用程序,并能通过 RemoteApp 服务发布应用程序。

1.1 支持Windows server 2008的版本

Windows Server 2008 Standard Windows Server 2008 Enterprise Windows Server 2008 Datacenter

1.2 RemoteApp应用发布介绍

RemoteApp 是微软在 Windows Server 2008 之后,在其系统中集成的一项服务功能,使用户可以 通过远程桌面访问远端的桌面与程序,客户端本机无须安装应用程序的情况下也能正常使用远端发 布的各种的桌面与应用。

1.3 RemoteApp对终端的要求

由于是采用 RDP 协议访问应用中心提供的应用程序,所以对终端平台有以下要求:

- (1) 终端操作系统必须为 windows 操作系统。
- (2) windows 的 RDP 版本至少 6.1 版本。
- (3) 如果终端操作系统为 windows XP,请检查 RDP 版本,如果版本过低请升级 RDP 版本。

1.4 应用中心授权许可介绍

应用中心授权许可证是用于对 windows server 2008 的远程桌面服务(RDS)进行授权许可,只有 正确 RDS 授权许可成功之后,运维审计系统访问应用中心的远程桌面服务就没有时间限制;未进 行 RDS 授权许可的应用中心只有 120 天的使用有效期。

2 配置前提

2.1 安装前准备

2.1.1 硬件配置

堡垒机对于应用发布服务器的硬件配置需求取决于访问应用发布会话的并发数,以及各应用程序所 需要消耗系统资源的多少,推荐的配置如下表所示:

表1 推荐的硬件配置

硬件	需求
处理器	最低:双核CPU
内存	最低: 8GB RAM
可用磁盘空间	最低: 100GB

2.1.2 操作系统

1. 版本

Microsoft Windows Server 2008 R2

2. 补丁

由于 Windows Server 2008 R2 的 bug,使用 RemoteApp 过程中可能会出现"由于协议错误,会话将被中断。请重新连接到远程计算机",因此请务必保证应用发布服务器为 Windows Server 2008 R2,并安装 sp1 补丁,然后安装 Windows6.1-KB2696020-x64.msu、

Windows6.1-KB2699817-x64.msu、Windows6.1-KB2798286-x64.msu 三个补丁。

SP1 补丁请从这里下载: http://support.microsoft.com/kb/976932。

2.1.3 网络

堡垒机到应用发布服务器之间网络不要做限制,并且保证应用发布服务器上所安装的客户端能正常 访问服务端。

2.1.4 RDS授权码

想要长期使用应用中心,须配备一套 RDS 授权码。如下图:

图1 RDS 授权码示意图

	Marine wet fals at a M	
运维审计系统-应用中心	RDS 许可证信息为:	
父级计划: <u>OPEN 1</u> 2	4	
开放式许可证详细信息:		
该许可证仅限于序列号为	02,0000 的运维审计系统	吏用。
	请注意	呆管。

示意图中的"父级计划"号码和"开放式许可证详细信息"号码是一组无效的示例号码;请勿使用! 否则应用中心授权失败。

RDS 授权码可以向运维审计系统供应商采购,也可以直接向微软销售渠道采购。 默认 windows 的 RDS 安装好之后,有 120 天的有效试用期,足以满足测试试用。

3 应用发布服务器配置准备

本章节以 Windows Server 2008 R2 Enterprise 的配置为例。

3.1 安装远程桌面服务(必配步骤)

(1) 在 windows server 2008 系统中,进入[服务器管理器/角色]窗口。

图2 服务器管理器示意图

12. 服务器管理器		<u>-0×</u>
文件 (E) 操作 (A) 查看 (V) 帮助	h 90	
🗢 🔿 🖄 📅 🛛 🔀		
La 服务器管理器 (WIN-7NG599MOTE	角色	
 □ /ul>	查看安装在服务器上角色的运行状况,以及添加或删	除角色和功能。
	⊙ 角色摘要	角色摘要帮助
		☆ 加角色 ☆ 加角色 聞除角色
	▲ 上次刷新时间:今天 22:42 間盂刷新	

(2) 单击<添加角色>,进入添加角色向导窗口。

图3 添加角色向导示意图

添加角色向导		×
开始之前		
 开始之前 服务器角色 确认 进度 结果 	此向导帮助你在此服务器上安装角色。根据要求此服务器执行的任务来确定要安装的角色,例如共 享又档或主持例结。 继续操作之前,请验证以下事项: • Administrator 帐户具有强密码 • Om常网络设置,例如静态 IP 地址 • 已安装 Windows Update 中的最新安全更新 如果您必须结束上述的任何操作,请取消此向导,结束操作,然后再次运行向导。 若要继续,请单击"下一步"。	
	□ 默认情况下将跳过此页 (S)	
	< 上一步 (1) 下一步 (2) > 安装 (1) 取消	

- (3) 单击<下一步>进入选择服务器角色窗口,勾选"远程桌面服务"。
- 图4 选择服务器角色示意图

添加角色向导		×
选择服务器角色		
开始之前 服务器角色 远程桌面服务 角色服务 确认 进度 结果	 法择要安装在此服务器上的一个或多个角色。 角色 ②: Active Directory Rights Management Services Active Directory 联合身份验证服务 Active Directory 经型目录服务 Active Directory 证书服务 DMCF 服务器 DMCF 服务器 DMSF器% Windows 影響服务 传真服务器 打印和文件服务 应用程序服务器 文件服务 应用程序服务器 ✓ 远程桌面服务 	描述: 远程桌面服务(以前称为终端服务)) 提供的技术使用户能够访问安装在 RD 会话主机服务器上的基于 Windows 與面。使用远程桌面服 务,用户可以从企业网络或 Internet 访问 RD 会话主机服务器 或虚拟机。
	< 上一步 (t) 下一步 (t)	D > 安装 ① 取消

- (4) 单击<下一步>进入远程桌面服务窗口。
- 图5 远程桌面服务简介示意图

添加角色向导		×
远程桌面服务		
开始之前 服务器角色 远程桌面服务 角色服务 确认 进度 结果	 远程桌面服务的分 远程桌面服务的为试验器服务)提供的技术使用户能够访问安装在 ED 会话主机服务器上的基于 Windows 的程序,访问 ED 会话主机服务器以后要求 Tindows 桌面,或访问虚拟机。使用远程桌面服务,用户可以从企业网络或 Internet 访问 ED 会话主机服务器或虚拟机。 注意事项 全成为进行管理而允许远程连接,则不必安装远程桌面会话主机。但是,请确保已启用远程桌面设置。 其他信息 远程桌面服务概述 	12
	< 上一步 (2) 下一步 (2) > 安装 (2) 取消	

(5) 单击<下一步>进入选择角色服务窗口,勾选"远程桌面会话主机"和"远程桌面授权"服务。

图6 选择角色服务示意图

添加角色向导		X
选择角色服务		
开始之前 服务器角色 远程桌面服务 向色服务 应用程序兼容性 身份验证方法 授权模式 用户组 客户端体验 即 授权配置 确认 进度 结果	法择为远程桌面服务安装的角色服务: 角色服务 @): ✓ 远程桌面会话主机 ✓ 近程桌面虚拟化主机 ✓ <mark>远程桌面透积</mark> □ 远程桌面连接代理 □ 远程桌面网关 □ 远程桌面 Web 访问	描述: 远程桌面微视(RD 授权)以前是 TS 授权,它管理连接到 RD 会话主机 服务器所需的远程桌面服务客户端 访问许可证(RDS CAL)。可以使用 RD 授权来安装、颁发和跟踪 RDS CAL 的可用性。
	有关角色服务的详细信息。 	
	〈上一步 @) 下一步	(10) > 安裝 (1) 取消

- (6) 单击<下一步>进入应用程序兼容性窗口。
- 图7 应用程序兼容性提示示意图

添加角色向导		×
卸载并重新安装制	兼容的应用程序 ————————————————————————————————————	
开始之前 服务器角色 远程桌面服务 角色服务 <u>应用程序兼容性</u> 身份验证方法 授权模式 用户组 客户端体验 如 授权配置 确认 进度 结果	建议在安装任何要让用户可用的应用程序之前安装远程桌面会话主机。 如果在已经安装了应用程序的计算机上安装远程桌面会话主机,某些现有的应用程序可能无法在 多用户环境下正常工作。卸载并随后重新安装受影响的应用程序能解决这些问题。 一些应用程序只需进行少量的设置修改就能在远程 № 会话主机服务器上正常运行。	
	有关在 120 会话主机服务器上安装应用程序的详细信息	
	< 上→步 (2) 下→歩 (2) > 安装 (2) 取消	

(7) 单击<下一步>进入身份验证方法窗口,选择"不需要使用网络级别身份验证"。

图8 选择身份验证方法示意图

添加角色向导	×
指定远程桌面会计	舌主机的身份验证方法
 开始之前 服务器角色 远程桌面服务 角色服务 应用程序兼容性 身份验证方法 授权模式 用户组 客户端体验 D 授权配置 确认 进度 结果 	 网络级别的身份验证是一种新的身份验证方法,当客户端连接到 起 会话主机服务器时,它通过在连接进程早期提供用户身份验证来增强安全性。网络级别的身份验证在远程桌面与 № 会话主机服务器 之间建立完全的连接之前,就进行了用户身份验证。 "需要使用网络级别身份验证。 雷要使用网络级别身份验证。 四方计算机同时运行 Windows 版本和支持网络级别身份验证的远程桌面连接的客户端版本,它才能连接到此 20 会话主机服务器。如果远程连接到此服务器,请确保计算机支持网络级别身份验证 (2) 运行往何版本的远程桌面连接客户端的计算机都可以连接到此 № 会话主机服务器。 " 不需要使用网络级别身份验证 (2) 运行任何版本的远程桌面连接客户端的计算机都可以连接到此 № 会话主机服务器。 此选项不如使用网络级身份验证时安全,因为用户身份验证发生在连接过程的后期。
	有关网络级别的身份验证和支持的客户端的详细信息
	< 上一步 (2) 下一步 (2) > 安装 (2) 取消

- (8) 单击<下一步>进入授权模式窗口,选择"以后配置"。
- 图9 选择授权模式示意图

添加角色向导		X
指定授权模式		
开始之前 服务器角色 远程桌面服务 角色服务 应用程序兼容性 身份验证方法 授权模式 用户组 客户端体验 知 授权配置 确认 进度 结果	 过程桌面授权模式确定远程桌面服务客户端访问许可证(BDS CAL)的类型,许可证服务器会将此 NDS CAL 微复给主接到此 ND 会话主机服务器的客户端。 指定希望此 ND 会话主机服务器使用的远程桌面授权模式。 ④ 以后配置(C) 在接下来的 120 天内,提示我使用远程桌面会话主机配置工具或组策略来配置授权模式。 ⑦ 每设备 QD 必须有 NDS 每设备 CAL 可用于连接到此 ND 会话主机服务器的每个设备。 ⑦ 每用户(U) 必须有 RDS 每用户 CAL 可用于连接到此 ND 会话主机服务器的每个用户。 ⑦ 指定的授权模式必须与远程桌面授权服务器中可用的 RDS CAL 相匹配。 着关远程桌面授权模式的详细信息 〈上一步 C) 下一步 QD 〉 安裝 CD 取消	

(9) 单击<下一步>进入用户组窗口,可在"用户或用户组"框添加允许远程访问的用户或用户组。

图10 添加用户组示意图

添加角色向导		X
选择允许访问此	RD 会话主机服务器的用户组	
开始之前 服务器角色 远程桌面服务 角色服务 应用程序兼容性 身份验证方法 授权模式 用户组 客户端体验 加 授权配置 确认 进度 结果	添加可以注接到此 ED 会话主机服务器的用户或用户组。这些用户和用户组将被添加到本地 Bemote Desktop Users 组中。數认情况下已添加 Administrators 组,因此无法删除。 用户或用户组 (D): 添加 (D) 承Administrators 添加 (D) 删除(G) 問除(G)	
	< 上一步 (2) 下一步 (2) > 安裝 ① 取消	

(10) 单击<下一步>进入客户端体验窗口,不选择任何功能项。

图11 选择客户端体验示意图

添加角色向导	×
配置客户端体验	
开始之前 服务器角色 远程桌面服务 角色服务 应用程序兼容性 身份验证方法 授权模式 用户组 客户端体验 取 授权配置 确认 进度 结果	 次回以配置 ND 会话主机服务器,以便连接到远程桌面会话的用户可以使用与 Windows 7 所提供功能 ☆ 提供此功能需要附加系统和带宽资源,因而可能影响 ND 会话主机服务器的可伸缩性。 选择要提供的功能。使用"远程桌面会话主机配置"工具可配置附加功能。 ④ 如果选择音频和视频播放或桌面元素,则将在 ND 会话主机服务器上安装桌面体验功能。 ● 當频和视频播放 (A) ● 常音重定向 (B) ● 桌面元素 (提供 Windows Aero 用户界面元素) (D) ④ 如果某个选择变略,则当前正在对计算机应用阻止配置该功能的组策略设置。有关详细信息,请参阅<u>出策略设需和配置客户端体验</u>。
	关于配置客户端体验的详细信息
	< 上一歩 (2) 下一歩 (2) > 安装 (2) 取消

(11) 单击<下一步>进入 RD 授权配置窗口,不选择任何功能项。

图12 RD 授权配置界面示意图

添加角色向导	×
为 RD 授权配置	搜索范围
开始之前 服务器角色 远程桌面服务 角色服务 应用程序兼容性 身份验证方法 授权模式 用户组 客户端体验 加授权配置 确认 进度	 ご せいたい いっかい いっかい いっかい いっかい いっかい いっかい いっかい い

(12) 单击<下一步>进入确认窗口

图13 确认安装选择示意图

添加角色向导		×
确认安装选择		
开始之前 服务器角色 远程桌面服务 角色服务 应用程序兼容性 身份验证方法 授权模式 用户组 客户端体验 取 授权配置 通	 若要安装以下角色、角色服务或功能,请单击"安装"。 ▲ 1 条警告消息,2 条提示性消息显示如下 ④ 安装完成之后,必须重新启动该服务器。 ④ 安装完成之后,必须重新启动该服务器。 ● 应程桌面服务 ● 应程桌面服务 ● 应程桌面低务 ● 耐能需要重新安装现有应用程序。 ● 耐能需要重新安装现有应用程序。 ● 印第二、增强的安全配置。 ● 好验证方法:	
	打印、保存或通过电子邮件发送此信息。 1991年1月19日 - 1991年1月1日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日	
	< 上一步 @) 下一步 (10) > 安装 @) 取消	
- (13) 单击<安装>进入安装进度窗口。
- 图14 安装进度示意图

添加角色向导	
安装进度	
开始之前 服务器角色 远程桌面服务 角色服务 应用程序兼容性 身份验证方法 授权模式 用户组 客户端体验 取授权函置 确认 进度	正在安装以下角色、角色服务或功能: 远程桌面服务
	< 上一步 (2) 下一步 (2) > _ 安装 (2) _ 取消 取消

(14) 等待安装进度完成后,自动进入安装结果窗口,并提示需要重启服务器才能完成安装过程。 图15 安装结果示意图

添加角色向导			×
安装结果			
开始之前 服务器角色 远程桌面服务	您需要重新启动以下一个或多个 ① 1 条警告消息显示如下	角色、角色服务或功能:	
角色服务	◇ 远程桌面服务		
应用程序兼容性	▲ 必须重新启动此服务器以		
身份验证方法			
授权模式			
用户组			
客户端体验			
RD 授权配置			
确认			
进度			
结果			
	1101、保存或通知电干邮件发达		
		<上一步(1) 下一步(10) > 关闭(10)	取消

(15) 单击<关闭>后自动提示"是否希望立即重新启动"。

图16 是否需要重启提示示意图

添加角色向导		×
安装结果		
开始之前 服务器角色 远程桌面服务	您需要重新启动以下一个或多个角色、角色服务或功能: ① 1 条警告消息显示如下	_
角色服务	◎ 远程桌面服务	
应用程序兼容性	添加角色向导	
身份验证方法	是否希望立即重新启动?	
授权模式		
用尸组 安古温住政	安次等和中心也能力解决,就是不是任。如本个素和方动服务器,则无法添加或删除其他角色、角色服务或功	
客/T%而PP验 RD 授切两罢	HE *	
确认	(是0) 否00	
进度		
结果		
	打印、保存或通过电子邮件发送安选报告	
	< 上一歩 (2) 下一歩 (2) > (注闭 (2) 取消	

- (16) 单击<是>后,系统自动重新启动。
- (17) 登录系统后,系统自动继续执行配置进度。

恢复配置向导	
安装进度	
继续执行配置	正在安装以下角色、角色服务或功能:
进度	远程桌面服务
结果	
	< 上一步 (P) 下一步 (M) > 安装 (L) 取消

(18) 自动完成安装结果,单击<关闭>即可。

图18 安装成功提示示意图

恢复配置向导		x
安装结果		
继续执行配置 进度 结果	已成功安装以下角色、角色服务或功能: 金、客響告消息,1 条提示性消息显示如下 · 未启用 Windows 目动更新。为确保自动更新最新安装的角色或功能,请启用"控制面板"中 的 Windows Update。 · 不可容。 · ⑦ 安装成功 · 改唱桌面の話 ② 安装成功 · ご程桌面会话主机 · ② 安装成功 · ご程桌面の話 · ② 安装成功 · 二、「一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一	
	< 上一步(2) 下一步(2) >	

3.2 应用中心激活授权(如果是测试客户,可忽略此操作)

3.2.1 激活应用中心

(1) 进入[控制面板/系统和安全/管理工具/远程桌面服务]界面中。

图19 远程桌面服务管理界面示意图

● 🕞 - 控制面板	→ 系统和安全 → 管理工具 → 远程桌面服务	▼ 65	搜索 远程桌面服务		
织 ▼ 包含到库中 ▼	共享 🔻 新建文件夹			= -	(
~ 收藏夹	名称 🔺	修改日期	类型	大小	
🚺 下载	🔝 RemoteApp 管理器	2015/6/7 23:04	快捷方式	2 KB	
■ 桌面 ◎ 見ぶぶたいつんり分開	🔝 远程桌面	2009/7/14 12:58	快捷方式	2 KB	
🎽 取近功回的立面	🔝 远程桌面服务管理器	2009/7/14 12:58	快捷方式	2 KB	
库	🚮 远程桌面会话主机配置	2009/7/14 12:58	快捷方式	2 KB	
 ■ 视频 ■ 文档 ■ 文档 ● 音乐 ■ 计算机 ■ 研络 	▶ 远程桌面授权管理器	2015/6/7 23:04	快捷方式	2 KB	
5 个对象					

(2) 双击<远程桌面授权管理器>进入 RD 授权管理器界面,右击计算机名称。

图20 RD 授权管理器示意图

🐂 RD 授权管理	器			
操作(A) 查看	(V) 帮助(H)			
🗆 🙀 所有服务	5器 <u>许可证版</u>	本和类型	许可证计划	许可证总数
	刷新 (R)	ws 2000 Server - 内置的每设备	内置式	无限制
Ģ	复查配置(N)			
	安装许可证 (I)			
	激活服务器(S)			
	高级(V) 🌇			
	创建报告(0) ▶			
	刪除报告 (0)			
	管理许可证(M)			
	属性(P)			
	帮助(H)			

- (3) 单击<激活服务器>进入服务器激活向导界面。
- 图21 服务器激活向导示意图

服务器激活向导		×
	欢迎使用服务器激活向导	
	若要安全地安装许可证,远程桌面授权服务器必须先被 Microsoft 激活。 许可证服务器成功完成激活之后,您将可以安装和颁发 许可证。 如果在宽限时间到期之前 RD 会话主机或 RD 虚拟化主 机服务器 如果适用)找不到已安装有相应许可证的已激 活的许可证服务器,RD 会话主机或 RD 虚拟化主机服务 器将得止接受未经授权客户端的连接。	
	<u>有关激活远程桌面授权服务器的详细信息</u> 。	
	< 上一步 (B) 下一步 (B) >	取消

(4) 单击<下一步>进入连接方法界面,本手册以"Web 浏览器"的连接方法为例。

图22 选择连接方法示意图

服务器激活向导		×
连接方法 请选择最合适的语	接方法。	9
安裝许可证时,为 Clearinghouse。 若要在激活后更改 法"选项卡。 连接方法(C): Web 浏览器 自动连接(推荐) Web 浏览器 电话	许可证服务器激活而选择的连接方法也将用于联系 Microsoft 连接方法,请转到许可证服务器"属性"对话框的"连接方 ▼	
要求:	这个方法需要一台有 Web 浏览器和能访问 Internet 的计算机。此计算机不一定要连接到许可证服务器。	
	〈上一步(33) 下一步(37) 〉	取消

表2 连接方法说明

连接方法	描述
自动连接(推荐)	使用此方法的前提是要确保应用中心能连通互联网,否则无法进行授权许可。
Web浏览器	此方法适用于应用中心无法连通互联网,但需要进行授权许可。 找一台能连通互联网的windows电脑,在浏览器中输入https://activate.microsoft.com, 进入远程桌面服务器授权页面进行授权许可。
电话	此方法适用于通过微软的服务热线进行电话授权许可,此方法比较繁琐,需要提供各种 详细信息。

(5) 单击<下一步>进入许可证服务器激活界面。

图23 许可证服务器激活示意图

服务器激活向导	×
许可证服务器激活 输入许可证服务器 ID。	9
若要激活许可证服务器,请转到以下远程桌面授权网站:	
<u>https://activate.microsoft.com</u>	
若要完成此操作,您需要提供产品 ID。您的产品 ID 是:	
在远程桌面授权网站上完成事务后,请在下面的框中键入许可证服务器 ID(A)。	
< 上一步 (8) 下一步 (8) >	取消

表3 服务器激活条件说明

激活条件	描述
远程桌面授权网站	https://activate.microsoft.com
产品ID	• 操作系统的产品 ID, 服务器激活向导界面会自动识别本操作系统的产品 ID。
许可证服务器ID	• 许可证服务器 ID 是由产品 ID 生成的,有了许可证服务器 ID 才能许可证服务器激活成功。

(6) 使用一台可以连通互联网的电脑,在浏览器中输入 https://activate.microsoft.com 进入 RDS 授权页面,选择"启用许可证服务器"。

图24 RDS 授权页面示意图

② 元程桌面腸务器授权 - Vindows Internet Explorer
😋 😔 🗢 🔊 https://activate.microsoft.com/
👷 收藏夹 🥫 远程桌面服务器授权 🏠 🔹 🗟 👻 豆面 (2) ・ 安全 (3) ・ 工具 (0) ・ 😥 ・
Microsoft
Remote Desktop Services
删除 常见问题解答 帮助
要访问特定语言的网站,请选择该语言,然后 欢迎使用远程桌面授权网站。该安全站点设计用来帮助您管理适用于 Windows Server 2012、Windows 单击转到'。 Chinese (Simplified) マ (ス) (DJ用于获取远程桌面服务客户端访问许可证 (RDS CAL)。在该站点收集的所有信息都将用来帮助您管理 _ 远程桌面服务资源。
从该站点获取的 RDS CAL 受相应的 Windows Server EULA 的制约。 为了您的安全,该站点中提供的所有信息都经过加密。有关数据隐私的信息,请参阅 关于远程桌面授权管理。
选择选项
● 启用许可证服务器○ に用许可证服务器
C 安装客户端访问许可证 [详细信息]
下一步

(7) 单击<下一步>进入 RDS 信息填写页面,输入应用中心的产品 ID、公司名称、国家(地区)。 图25 RDS 授权页面示意图

🌈 远程桌面服务器授权 - Windows	Internet Explorer		
🕒 🕑 🗢 🙋 https://activate.a	icrosoft.com/	💌 🔒 🔁 🐓 🗙 📴 Ding	ρ.
👷 收藏美 🛛 🏀 远程桌面服务器板板	2	🏠 • 🖸 - 📼 🖶 • 页面(P) • 安全(S) • I	用(0) • 🔞 •
Microsoft			^
Remote Des	sktop Services		
删除 常见问题解答	帮助		
	要激活许可证服务器,需要提供以下信息。	通过选择"远程桌面接权管理器"工具中的"激活服务器"可以找到产品 [D.
产品信息	#局 ID:	* 🖏 🐮	
公司信息	公司: test *	国家(地区): 中国 v	
			一步
() () () () () () () () () ()		□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	100% • //

表4 RDS 授权信息说明

填写项	描述
产品ID	将服务器激活向导界面的产品ID填写进去 如需查看产品ID,请右击应用中心里的"计算机",单击<属性>进入系统属性界面查看
公司	填写使用用户单位的名称
国家(地区)	选择应用中心所在国家或地区

(8) 单击<下一步>进入 RDS 授权信息确认页面。

图26 RDS 授权页面示意图

🌈 远程桌面服务器授权 - Windows Inter	net Explorer					- 🗆 🗙
💽 🗢 🖉 https://activate.microsof	t.com/CompanyInfo.aspx	_	📘 🗟 😏 🗙 🕨	Bing		P -
🖕 收藏夹 🏾 🏉 远程桌面服务器授权			🏠 • 🔊 ·	🖃 🖶 🔹 页面(0) 🗸	安全(S) • 工具(0)	• 🔞 •
Microsoft						
Remote Deskte	op Services					
删除 常见问题解答 帮助	1					
	远程桌面授权已准备处理您的请求, 一步"。	,请确认提供的信息准确	私法律,然后单击"	下一步"。如果需要进	打更正,请单击"	E
产品信息 	产品 ID: 00486-001-7021515-84069					
公司信息	公司: test 国家(地区): 中国					
				<u> </u>	步 下一步	;
 完成]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]	保护模式:禁用		• •

(9) 单击<下一步>RDS 授权一个许可证服务器 ID,将其复制并保存好。

图27 RDS 授权页面示意图



(10) 返回到应用中心里的[服务器激活向导]界面,输入 RDS 授权页面生成的许可证服务器 ID。

图28 许可证服务器激活示意图

服务器激活向导	×
许可证服务器数活 输入许可证服务器 ID。	9
若要激活许可证服务器,请转到以下远程桌面授权网站:	
<u>https://activate.microsoft.com</u>	
若要完成此操作,您需要提供产品 ID。您的产品 ID 是:	
C	
在远程桌面授权网站上完成事务后,请在下面的框中键入许可证服务器 ID(A)。	
	1112年 1
	取用

(11) 单击<下一步>进入正在完成服务器激活向导界面。

图29 完成服务器激活向导示意图

服务署激活向导		×
	正在完成服务器激活向导	
	您已完成服务器激活向导。 状态: 已成功激活许可证服务器。 若要安装许可证,请单击"下一步"。 若要推迟许可证安装,请清除"立即启动许可证安装 向导"复选框,然后单击"完成"。	
	▶	
	<上一步(B) 下一步(A) >	取消

(12) 如果单击<下一步>则直接进入许可证安装向导界面,如 3.2.2 (2)图 31。 如果单击<取消>则直接退出服务器激活向导界面。

3.2.2 安装应用中心授权许可证

(1) 在[RD 授权管理器]中右击计算机名称。

图30 RD 授权管理器示意图

♣BD 授权管理器							- 🗆 ×
操作(A) 查看(V) 帮助(H)							
□ 🙀 所有服务器 다可证版	版本和类型	许可证计划	许可证总数	可用	已颁发	到期日期	
E Wind	pws 2000 Server - 内置的每设备	内置式	无限制	无限制	0	永不过期	
刷新 (R)	pws Server 2008 或 Windows Ser	批量许可证	1	0	1	永不过期	
复查配置(11)							
安装许可证 (I)							
激活服务器 (S)							
高级(V) ▶							
创建报告(0) ▶							
刑除报告 (0)							
管理许可证(11)							
属性(2)							
帮助 (H)]						

- (2) 单击<安装许可证>进入许可证安装向导界面。
- 图31 许可证安装向导示意图

服务器激活向导		×
	欢迎使用许可证安装向导	
	该向导会将许可证安装到远程桌面授权服务器上。 您需要提供许可证购买信息(例如零售许可证代码或批 重许可证协议号码)才能完成此向导。	
	「许可证服务器设置 激活对象: 	
	<u>有关安装许可证的详细信息</u> 。	
	<上一步(B) 下一步(D) > 取消	

(3) 单击<下一步>进入获取客户端许可证密钥包界面。

图32 获取客户端许可证密钥包界面示意图

服务器激活向导	×
获取客户端许可证密钥包 提供客户端许可证密钥包 ID。	q_
若要安装许可证,必须从以下位置的远程桌面授权网站获取许可证密钥包 ID:	
<pre>https://activate.microsoft.com</pre>	
若要获取许可证密钥包 ID,将需要使用已从许可证计划(例如,零售产品包装、 Enterprise Agreement 或 Select License)收到的许可证代码信息。	
还需要使用许可证服务器 ID。您的许可证服务器 ID 是:	
CHARLE LEDIC HIMOU GATO, MONOD_MUKDU	
从远程桌面授权网站获取许可证密钥包 ID 之后,在下列框中键入此 ID。	
请记下此 ID。拥有此信息,便于您在恢复许可证需要帮助时与 Microsoft Clearinghouse 进行通信。	
<上一步(B)下一步(N) > I	取消

表5 获取客户端许可证密钥包条件说明

获取条件	描述
远程桌面授权网站	https://activate.microsoft.com
许可证服务器ID	许可证安装向导界面会自动识别本操作系统的许可证服务器ID。
许可证密钥包ID	许可证密钥包ID是由许可证服务器ID、父级计划和开放式许可证详细信息的号码共同生成的。 在 <u>(6)</u> 中会用到应用中心授权许可证中的父级计划和开放式许可证详细信息的号码。

(4) 使用一台可以连通互联网的电脑,在浏览器中输入 https://activate.microsoft.com 进入 RDS 授权页面,选择"安装客户端访问许可证"。

图33 RDS 授权页面示意图

🌽 远程桌面服务	务器授权 - Windows Interne	t Explor	er								_	
00 - 6	https://activate.microsoft.	com/				-	🗟 🐓 🎽	🕑 Bing				P -
🚖 收藏夹 🛛 👔	🏉 远程桌面服务器授权						🟠 • 6	3 · 🗆 🖶	• 页面(₽) •	安全(S) •	工具(0) -	•
- Mic	crosoft											^
Rer	mote Deskto	p Se	ervices									
删除	常见问题解答 帮助											
要访 单击 Chi	间特定语言的网站,请选择该语言 ·转到"。 inese (Simplified)	言,然后 <i>议</i> 入	欢迎使用远程桌 Server 2008 R 器,以及用于获 远程桌面服务资	面授权网站。 2、Windows 取远程桌面服 源。	该安全站。 s Server 200 服务客户端访	気设计用す)8、Winc 前问许可证	、 帮助您管理這 lows Server 2 [(RDS CAL)。	i用于 Windov 003 或 Wind 在该站点收集	vs Server 20 ows 2000 Se 的所有信息都	12、Wind erver 的许 济用来帮助	ows 可证服务 协您管理	
			从该站点获取的 为 了 您的安全	RDS CAL 引 该站占由提(受相应的 Wir	idows Se	rver EULA 的 廖 右关数据	制约。	星參阅 天士犯	记得点面将	▽管理	
S. 1. 197 S. L.	•7		733 AGA 2 4	BOOLDING TODEL						2123604000		
选择选	坝	0 mv		6关细信自1								
			H可证服劳器 2.白端访问许可证	[详细信息]								
		の重新調	(活许可证服务器	[详细信息]								
		○管理(CAL:	[详细信息]								
											下一步	
												•
							🚯 🗸 可信站	点 保护模式	:禁用	1	• 🔍 100%	• //

(5) 单击<下一步>进入 RDS 授权信息填写页面,输入正确的许可证服务器 ID,在许可证程序里选择"开放式许可证",填写公司名称,选择正确的国家(地区)。

图34 RDS 授权页面示意图

<i>(6</i> is	程桌面服务	·苦授权 - Tinders	: Internet Explorer	_ D X
G	🕘 = 🙋	https://activate.e	sicrosoft.com/	P -
* 8	職夫 🔏	這程桌面服务器授作	R 👌 • 🖸 - 🗔 🦛 • 页面(9) • 安全 0	5)• 工具(0)• 😧•
	IVIIC	roson		-
	Ren	note De	sktop Services	
	删除	常见问题解答	帮助	
			要安装许可证,需要提供以下信息。通过选择"远程桌面接权管理器"工具中的"安装许可证"可以找到许可证服务 方法应设置为 Web 浏览器 (Windows Server 2008) 或 Web 浏览器 (Windows Server 2003)。要更改连接方法,引 面授权管理器"工具的"视图"菜单上单击"属性",然后单击"连接方法"选项卡。	器 ID. 连接 附在"远程桌
			红色星号表示必需填写的信息 (*).	
	产品信息		1+ 27/2 20/44 MB 115	
	授权信息		许可证程序: 开放式许可证	
	公司信息			
			公司: 国家(地区): test ・ 中国 ▼・	
	202 		上一步	下-步
完成			1200 日本 1100	√ _h • [★] 100% • //

表6 RDS 授权信息说明

填写项	描述
许可证服务器ID	将获取客户端许可证密钥包界面的许可证服务器ID填写进去。
许可证程序	选择"开放式许可证"。
公司	填写使用用户单位的名称。
国家(地区)	选择应用中心所在国家或地区。

(6) 单击<下一步>进入 RDS 授权许可证信息填写页面,选择 "windows server 2008 R2 每设备 CAL 或 windwos server 2008 TS 每设备 CAL",填写正确的 RDS 授权数量、授权号码、许 可证号码。

图35 RDS 授权页面示意图

(S iz A	桌面	服务書授权 - Ti	adows Internet Explorer				
Ge)•[🙋 https://acti	vate microsoft.com /LicenseInfo.asy	P.K.	💌 🔒 😔 😽 🗶 📴 Ding		P -
🚖 收着	秩	🏉 远程桌面服务	蓄摂权		👌 • 🖸 - 🗆 🖶 •	页面(P) • 安全(S) •	工具 (0)・ 😧・
	Re	mote [Desktop Servic	es			-
4	删除	常见问题解	答 帮助				
			要安装客户簿访问许可证,需要想	B供以下信息。			
			红色星号表示必需填写的信息(*)				
	许可证	服务器 ID	YM8RQ-K2DXC-HWM68-QX7	78Q-VVMRC-H8M2D-HMKB	н		_
	产品体	息	产品类型:				
			Windows Server 2008 R2 RDS	6 每设备 CAL 或 Windows Serv	er 2008 TS 每设备 CAL 💌 *		
			数量:				
	挭权值	息					_
·			许可证程序:				
			升放丸件可止 授权号码:				
				•			
			许可证 号码:				
			2705 100				_
						上一步	
< 宗成					□ □ @ ↓ □ @ ↓ @ ↓ @ ↓ @ ↓ @ ↓ @ ↓ @ ↓ @	MR 🖗	• • 1005 • 4
				, , , , ,	, , , , , , , , , , , , , , , , , , , ,	1.1	16

表7 RDS 授权信息说明

填写项	描述
许可证服务器ID	将获取客户端许可证密钥包界面的许可证服务器ID,此处不需要填写。
产品类型	请选择"windows server 2008 R2每设备CAL或windwos server 2008 TS每设备CAL"的RD授权模式。
数量	填写RDS对应的数量,数量自定义,可以根据堡垒机的资产数量填写数量。
许可证程序	开放式许可证
授权号码	根据应用中心授权许可证中提供的"父级计划"号码填写。
许可证号码	根据应用中心授权许可证中提供的"开放式许可证详细信息"号码填写。

(7) 单击<下一步>进入 RDS 授权信息确认页面。

图36 RDS 授权页面示意图

Attacidation and a state of the	aft conditions Infolmen area		
· ·	I I I I I I I I I I I I I I I I I I I		
藏夫 🌈 远程桌面服务器授权		🛐 • 🔂 - 🖾 👘 • 页面(?) • 3	安全(S) · 工具(D) ·
	远程桌面授权已准备处理您的请求。请帮	角认提供的信息准确无误,然后单击"下一步"。如果需要进行要	正,请单击"上
	一步".		
许可证服务器 ID			
	YM8RQ-K2DXC-HWM68-QX78Q-V	VMRC-H8M2D-HMKBH	1998
产品信息			
	产品类型:		
	Windows Server 2008 R2 RDS 每设	备 CAL 或 Windows Server 2008 TS 每设备 CAL	
	教堂:		
iali in rie da			
戊 伏清熄	许可证程 成 -		
	开放式许可证		
	授权号码:		
	100000000000000000000000000000000000000		
	许可证号码:		
	80000		
公司信息			
	公司:		
	test		
	国家(地区):		
	PIN		
		上一步	下一步
		1 一 一 司信報書 1 保持講書 1 田田	(A

(8) 单击<下一步>RDS 授权一个许可证密钥包 ID 号,将其复制并保存好。

图37 RDS 授权页面示意图

Ø远程桌面服务書版权 − Tindows Internet Explorer		
🚱 💿 🗢 🔊 https://activate.microsoft.com/LicenseInfoSelectConfirm.aspx	💌 🔒 🖯 👉 🗙 📴 Bing	ρ.
🔆 收藏夫 🏾 🏂 远程桌面服务器授权	🏠 • 🖾 · 📑 👼 • 页面(P) • 安全(S)	• 工具の)• 😧•
Microsoft		-
Benesta Deslaten Comisso		
Remote Desktop Services		
删除 常见问题解答 帮助		
已成功处理您的客户请访问许可证请求。请打印此页面作为参考。 需要在"证程点面 CAL 安装向导"中输入的许可证密相如 ID 为:		
under all all all and an an an an an and an an an and an an an and an and an		
PWHSE-SR42B-BWISS-SS62V-Q6Q	MITTOHO KOQ7M	
许可征服劳器具有以下许可征服劳器 ID: YM8RQ-K2DXC-HWM68-QX78Q-VVMRC-H8M2D-HMKBH		
谢谢您激活远程桌面服务客户簿访问许可证 (RDS CAL)。		
		64-35
		始果
¥[>
実成 [] [] [] [] [] [] [] [] [] [🛛 💦 🗸 可信站点 保护模式: 禁用 🔗	🚡 • 🔍 100% • 🎢

(9) 返回至获取客户端许可证密钥包界面,输入 RDS 授权页面生成的许可证密钥包 ID。

图38 服务器激活向导示意图

服务器激活向导	×
获取客户端许可证密钥包 提供客户端许可证密钥包 ID。	9
若要安装许可证,必须从以下位置的远程桌面授权网站获取许可证密钥包 ID:	
<u>https://activate.microsoft.com</u>	
若要获取许可证密钥包 ID,将需要使用已从许可证计划(例如,零售产品包装、 Enterprise Agreement 或 Select License)收到的许可证代码信息。	
还需要使用许可证服务器 ID。您的许可证服务器 ID 是:	
WHODS-KZUXI-REMICO GRIDG YYMLG HONOD-DHERDY	_
从远程桌面授权网站获取许可证密钥包 ID 之后,在下列框中键入此 ID。	
jannak (35760 bulanen (appike (dedm?)appike (1992)	
请记下此 ID。拥有此信息,便于您在恢复许可证需要帮助时与 Microsoft Clearinghouse 进行通信。	
〈上一步(33) 下一步(33) 〉	取消

(10) 单击<下一步>进入正常完成许可证安装向导界面。

图39 完成许可证安装向导示意图

服务器激活向导		×
1 Marshart	正在完成许可证安装向导	
	您已完成许可证安装向导。	
	状态:	
	C.网络女女用小田庄。	
	〈 上一步 (8) 完成	取消

(11) 单击<完成>后即可在 RD 授权管理器界面中看到已成功授权,并且已经变成绿色的勾勾。

图40 RD 授权管理器示意图

💁 BD 授权管理器									
操作 (A) 查看 (V) 帮助 00									
□ 寫 所有服务器	许可证版本和类型	许可证计划	许可证总数	可用	已颁发	到期日期			
🖨 🗔 WIN-7NG599MOTER	🐚 Windows 2000 Server - 内置的每设备	内置式	无限制	无限制	0	永不过期			
- 🕞 Windows 2000	🖶 Windows Server 2008 或 Windows Ser	批量许可证	1	1	0	永不过期			
日本 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一									

3.3 调整应用中心的策略(必配步骤)

3.3.1 调整本地组策略

(1) 在运行窗口中输入 "gpedit.msc"。

图41 运行窗口示意图

📨 运行		×
	Windows 将根据您所输入的名称,为您打开相应的程序、 文件夹、文档或 Internet 资源。	
打开(O):	gpedit.msc 💌	
	🔋 使用管理权限创建此任务。	
	确定 取消 浏览(B)	

(2) 单击<确定>进入[计算机配置/管理模板/windows 组件/远程桌面服务/远程桌面会话主机/连接] 界面。

图42 本地组策略示意图

」 本地组策略编辑器				
文件(F) 操作(A) 查看(V) 帮助(H)				
🗢 🄿 🖄 📷 🗟 🖬 🛛 🔻				
本地计算机 策略 秋田 和 和 和 和 和 和 和 和 和 和 和 和 和 和 和 和 和	■ 连接 操一个项目来查看它的描述。	设置 注 自动重新连接 匠 行计用户使用远程桌面服务进行远程连接 匠 拒绝将已经登录到控制台会话的管理员注诮 重配活动连接的时间间隔 匠 限制连接的数量 匠 为远程桌面服务用户保制到单独的远程桌面服务会话 匠 介许远程启动未列出的程序 匠 关闭公平份额 CPU 调度	<u>状态</u> 未配置 未配置 未配置 未配置 未配置 未配置 未配置 未配置 未配置 未配置	
+ Tablet PC		4		F
I Indows berender	广展 /标准 /	<u></u>		
9 个设置				

(3) 双击<将远程桌面服务用户限制到单独的远程桌面服务会话>,在配置界面中选择"已禁用"。

图43 策略配置示意图

💭 将远程桌面朋	服务用户限制到	则单独的远程桌面服务会	£	_ 🗆 🗙
📑 将远程桌面	服务用户限制到	刘单独的远程桌面服务会话	上一个设置(P) 下一个设置(N)	
〇 未配置(C)	注释:			
〇 已启用(E)				
● 已禁用(D)		<u> </u>		V
	支持的平台:	至少 Windows Server 2	003	A V
选项:			帮助:	
			使用此策略设置可以将用户限制到单独的远程桌面服务会如果启用此策略设置,则将使用远程桌面服务远程登录的 到该服务器上的单独会话(活动状态或断开连接状态)。如 会话保持在断开连接状态,则下次登录时用户将自动重新 会话。 如果禁用此策略设置,则允许用户使用远程桌面服务进行 的同时远程连接。 如果未配置此策略设置,则"远程桌面会话主机配置"] 限制每个用户一个会话"设置将确定是否将用户限制到单 桌面服务会话。	浙话。 ●
			确定取消	应用(A)

单击<确定>即可。

(4) 双击<限制连接的数量>,在配置界面中选择"已启用",并设置允许的 RD 最大连接数为 "999999"。

图44 策略配置示意图

氯 限制连接的数量	
100 限制连接的数量	上一个设置(P) 下一个设置(N)
 ○ 未配置(C) 注释: ○ 已启用(E) ○ 已禁用(D) 支持的平台: 至少 Windows Server 1 	2003 A
选项:	帮助:
允许的 RD 最大连接数 999999 → 为无限制连接数键入 999999。	 指定远程桌面服务是否限制同时连接到服务器的数量。 可以使用此设置限制服务器上活动的远程桌面服务会活的数量。如 果超出此数量,则尝试连接的其他用户将收到错误消息,以通知他 们服务器正忙,需要稍后再试。限制会话的数量可提高性能,因为 请求系统资源的会话较少。默认情况下,RD 会话主机服务器不限 制远程桌面服务会话的数量,并且管理远程桌面允许两个远程桌面 服务会话。 若要使用此设置,请输入希望为服务器指定的最大连接数量。若要 指定不受限制的连接数量,请键入 999999。 如果将状态设置为 "启用",则最大连接数量限制为与服务器上运 行的 Windows 版本和远程桌面服务的模式相一致的指定数量。 如果将状态设置为 "禁用"或 "未配置",则在"组策略"级别上 不强制限制连接的数量。 注意:此设置专门为在 RD 会话主机服务器(即,运行安装有远程桌
	确定 取消 应用(A)

单击<确定>即可。

(5) 双击<允许用户使用远程桌面服务进行远程连接>,在配置界面中选择"已启用"。

图45 策略配置示意图

💭 允许用户使用	目远程桌面服务	进行远程连接	
📑 允许用户使	用远程桌面服务	进行远程连接	上一个设置(P) 下一个设置(N)
○ 未配置(C) ◎ 已启用(E) ○ 已禁用(D)	注释: 支持的平台:	至少 Windows XP Prot	▲ ▼ fessional 或 Windows Server 2003 系列 ▼
选项:			帮助:
			 使用此策略设置,可以使用远程桌面服务配置对计算机的远程访问。 如果启用此策略设置,则目标计算机上的"远程桌面用户"组成员可以使用远程桌面服务远程连接到目标计算机。 如果禁用此策略设置,则用户无法使用远程桌面服务远程连接到目标计算机。目标计算机将保持当前的所有连接,但不会接受任何新传入的连接。 如果未配置此策略设置,则远程桌面服务使用目标计算机上的"远程桌面"设置来确定是否允许远程连接。此设置位于"系统属性"的"远程"选项卡上。默认情况下,不允许远程连接。 注意:通过配置"计算机配置\管理模板\Windows 组件\远程桌面服务\远程桌面会话主机\安全\要求使用网络级别的身份验证对远程连接进行用户身份验证"策略设置,可以限制哪些客户端可以使用远程桌面服务进行远程连接。通过配置"计算机配置\管理模板\Windows 组件\远程桌面服务,远程桌面服务,远程桌面最易,远程桌面会话主机\连接\限制连接
			确定 取消 应用(A)

单击<确定>即可。

- (6) 进入[计算机配置/管理模板/windows 组件/远程桌面服务/远程桌面会话主机/会话时间限制]界面。
- 图46 本地组策略示意图

」 本地组策略编辑器			
文件(F) 操作(A) 查看(V) 帮助(H)			
🗢 🔿 🞽 📷 🗟 👔 🛛 🍸			
 ● 教字保险箱 ● 网络访问保护 ● 网络货间保护 ● 网络货制仪 ● 位置和传感器 ● 演示文稿设置 ● 应用程序兼容性 ● 游戏浏览器 ● 通程真面服务 ● 逐 逻程真面服务 ● 逐 逻程真面易务 ● 逐 逻程真面易务 ● 逐 逻辑真面影务 ● 10 连接 Broker ● 安全 ● 170利重定向 ● 全流时间限制 ● 连接 ● 哈哈文件夹 ● 電置文件 ● 資子和淡源重定向 ● 資子和淡源重定向 ● 資子和淡源重定向 	▲ ● 会話时 回限制 选择一个项目来查看它的描述。	设置 E 设置已中断会话的时间限制 E 设置活动的远程桌面服务会话的时间限制 E 设置活动的远程桌面服务会话的时间限制 E 达到时间限制时终止会话 E 设置 RemoteApp 会话的注消时间限制	<u>扶漆</u> 未 <u>配置</u> 未配置 未配置 未配置 未配置
□ 投放 □ 応用程序兼容性	<u>_</u>	•	
	」 \扩展 〈标准 /		

- (7) 双击<设置已中断会话的时间限制>,在配置界面中选择"已启用",并设置结束已断开连接的会话为"1分钟"。
- 图47 策略配置示意图

💭 设置已中断会话的时间限制	
🔚 设置已中断会话的时间限制	上一个设置(P) 下一个设置(N)
 ○ 未配置(C) 注释: ○ 已启用(E) ○ 已禁用(D) 支持的平台: 至少 Windows XP Profe 	► essional 或 Windows Server 2003 系列 ▼
选项:	帮助:
结束已断开连接的会话 1分钟 ▼	 使用此策略设置可以对已断开连接的远程桌面服务会话配置时间限制。 使用此策略设置可指定某个已断开连接的会话在服务器上能保持活动状态的最长时间。默认情况下,远程桌面服务允许用户从远程桌面服务会话断开连接,而不用注销和结束会话。 会话处于断开连接状态时,即使用户不再处于活动连接状态,运行中的程序仍保持活动。默认情况下,这些已断开连接的会话在服务器上可以不受时间限制地保持该状态。 如果启用此策略设置,则达到指定时间后将从服务器中删除已断开连接的会话。若要强制使用默认行为,使已断开会话的保留时间不受限制,请选择"从不"。如果是控制台会话,则已断开会话的时间限制不适用。 如果禁用或未配置此策略设置,则已断开会话的保留时间不受限制。可以在"远程桌面会话主机配置"工具中的"会话"选项卡上指定已断开会话的时间限制。
	确定 取消 应用(A)

单击<确定>即可。

3.3.2 设置RD授权模式

(1) 进入[控制面板/系统和安全/管理工具/远程桌面服务]界面。

图48 远程桌面服务项示意图

🎴 远程桌面服务					_ 🗆 ×
	▼ 系统和安全 ▼ 管理工具 ▼ 远程桌面服务		▼ 🔯 捜素 远程員	桌面服务	2
组织 🔻 💽 打开 新建文	て件夹				
🚖 收藏夹	名称 ▲	修改日期	类型	大小	
📔 下载	🔝 RemoteApp 管理器	2015/6/7 23:04	快捷方式	2 KB	
三 桌面 97 是话话问的位果	🝺 远程桌面	2009/7/14 12:58	快捷方式	2 KB	
₩ 報知 約月月月7日	💼 远程桌面服务管理器	2009/7/14 12:58	快捷方式	2 KB	
🧊 库	📸 远程桌面会话主机配置	2009/7/14 12:58	快捷方式	2 KB	
 ● 视频 图片 文档 章 	🕞 远程桌面授权管理器	2015/6/7 23:04	快捷方式	2 KB	
▶ ● 计算机					
• 阿络					
远程桌面会话主 快捷方式	机電置 修改日期: 2009/7/14 12:58 创 大小: 1.19 KB	建日期: 2009/7/14 12:5	58		

(2) 双击<远程桌面会话主机配置>进入配置界面。

图49 授权诊断示意图

幣远程桌面会话主机配置				
文件() 操作(A) 查看(V)	帮助 (H)			
SD 会话主机配置: WIN-7NG59		▲	操作	
Ⅲ φ 授权诊断	编辑设置		RD 会	话主机配置: WIN-7NG599NOTEE 🔺
	常规		â 🍰	J建新连接
	🔁 退出时删除临时文件夹	是	🖸 吊	小新
	┃ < <p>2 每个会话都使用临时文件夹 ▲ 2 四刺每本田白口能讲行一本全活</p>	是	🚡 ið	[接到远程桌面会话主机服务器
	┃ ≧ 限約等「用戶六能送们」「云は ┃ ≧ 用户登录模式	定 允许所有连接		ē者
			? 寿	『助
		土地会		
	▲ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	未指定		
	👔 RD 连接代理中的场的成员	否		
	RD IP 虚拟化			
	☑ IP 虚拟化			

(3) 双击<远程桌面授权服务器>进入配置属性界面,选择"每设备"模式。

图50 授权属性示意图

属性 ×
常规 授权 RD 连接代理 RD IP 虚拟化
远程桌面授权模式
○ 未指定 (37)
● 每设备(P)
C 毎用户(V)
远程桌面授权服务器 远程桌面会话主机服务器将按列出许可证服务器的顺序向指定的许可证服务器发送 RDS CAL 的请求。 指定的许可证服务器 (S):
上移 00) 下移 (0)
添加 (0) 册除 (R)
确定 取消应用(A)

(4) 单击<添加>进入添加许可证服务器界面,将本地服务器添加到指定的许可证服务器中。

图51 添加许可证服务器示意图

添加许可证服务器		×			
从已知许可证服务器列表中选择许可证服务器,或者键入许可证服务器的名称或 IP 地址,然后单击"添加"。仅本 地许可证服务器和 SCP 注册许可证服务器位于已知许可证服务器中。					
已知许可证服务器(K):	指定的许可证服务器(S):				
[本地] WIN-7NG599MOTEE	WIN-TNG599MOTEE				
	添加(A)> 上移 (M)				
	(明除 (R) 下移 (V)	j			
	添加(0)>				

(5) 单击<确定>即可返回配置属性界面。

图52 授权属性示意图

属性 🛛 🛛 🛛 🗶
常规 授权 RD 连接代理 RD IP 虚拟化
远程桌面授权模式
○ 未指定 (17)
● 每设备 (P)
○ 毎用户(V)
远程桌面授权服务器 远程桌面会话主机服务器将按列出许可证服务器的顺序向指定的许可证服务器发送 RDS CAL 的请求。 指定的许可证服务器 (S):
上移 (9) 下移 (0)
添加 (0) 删除 (8)
确定 取消 应用 (A)

(6) 单击<确定>后提示已更改系统注册表的配置。

图53 远程桌面会话主机配置提示示意图



(7) 单击<确定>接口生效,并可以查到配置界面已指定。

图54 授权诊断示意图

《》远程桌面会话主机配置			
文件(F) 操作(A) 查看(V)	帮助 (H)		
SE S		_	操作
王 q 授权诊断	编辑设置		RD 会话主机配置: WIN-7NG599NOTEE 🔺
	常规		🚢 创建新连接
	📔 退出时删除临时文件夹	是	🖸 刷新
	■ 一〇一〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇	是不	🚡 连接到远程桌面会话主机服务器
	■ ■ 限制每千用户只能进行一千会储 ■ ■ 用户登录模式	户 允许所有连接	查看
	授权		👔 帮助
	🖆 远程桌面授权模式	每设备	
	🚰 远程桌面授权服务器	已指定	
	RD 连接代理		
	📔 BD 连接代理中的场的成员	音 日本	
	RD IP 虚拟化		
	F IP 虚拟化	未启用	
			J

(8) 单击<授权诊断>可以看到"授权诊断信息-警告"中为空,表示授权设置正常。

图55 授权诊断示意图

《警远程桌面会话主机配置					
文件(F) 操作(A) 查看(V)	帮助 00				
🗢 🔿 🖄 📷 🛛 🖬					
 RD 会话主机配置: WIN-7NG50 Ⅲ el 授权诊断 	授权诊断(WIN-7NG599M0TEE)				
	授权诊断提供的信息有助于确定远程桌面会话主机服务器可能存在的授权问题。				
	受授权诊断未发现远程桌面会话主机服	服务器的任何授权问题。	-		
	远程桌面会话主机服务器配置详细信题	意思			
	WIN-7NG599MOTEE				
	① 客户端可用的许可证数量:	1			
	远程桌面会话主机服务器版本:	Windows Server 2008 R2			
	Active Directory 域: 注回増ゴ・	小适用 每边冬			
	· · · · · · · · · · · · · · · · · · ·	·····································	_		
	NTA-AND 2012				
		授权诊断未识别任何要报告的问题。			
	问题	建议的解决方案			
		<u>v</u>			
1					

3.3.3 允许用户在初始连接时启动列出和未列出的程序

(1) 进入[控制面板/系统和安全/管理工具/远程桌面服务]界面。

图56 远程桌面服务项示意图

🎴 远程桌面服务					
🕞 🕞 マ 🍌 マ 控制面板 -	▼ 系统和安全 ▼ 管理工具 ▼ 远程桌面服务		▼ 🛂 捜索 远程員	真面服务	<u> </u>
组织 ▼ 💽 打开 新建5	2件夹			:EE •	- 🔳 🔞
🗙 收藏夹	名称 🔺	修改日期	类型	大小	
📕 下载	🗊 RemoteApp 管理器	2015/6/7 23:04	快捷方式	2 KB	
	🝺 远程桌面	2009/7/14 12:58	快捷方式	2 KB	
224 取见的凹口近面	🔂 远程桌面服务管理器	2009/7/14 12:58	快捷方式	2 KB	
🧊 库	🕞 远程桌面会话主机配置	2009/7/14 12:58	快捷方式	2 KB	
 ● 初频 ●	园 远程桌面授权管理器	2015/6/7 23:04	快捷方式	2 KB	
i≣ 计算机					
• 网络					
RemoteApp 管H 快捷方式	里器 修改日期: 2015/6/7 23:04 创建日; 大小: 1.20 KB	期: 2015/6/7 23:04			

- (2) 双击<RemoteApp管理器>进入配置界面。
- 图57 RemoteApp 管理器示意图

警RemoteApp 管理器				
文件 (F) 操作 (A) 查看 (V) 帮助 (H)				
RemoteApp 管理器	操作			
RemoteApp程序是通过远程桌面访问的程序,它们	RemoteApp 管理器 (本地) ▲			
KemoteApp 程序之前,必须将具添加到 KemoteApp		🧐 连接到计算机		
				📑 添加 RemoteApp 程序
概述			•	RD 会话主机服务器设置
ᇝᅀᆦᆂᆊᄜᇂᇔᇧᆇᆂᇪ	庙田 RD Web 讨	词分发		RD 网关设置
	🔥 TS Web 访问]计算机组为空。月	月户可能无法使用	▶ 数字签名设置
⑦ 各戶調将建接到: Wilk-7NG399M0TEE ✓ 用户只能在初始连接时启动列出的 RemoteApp 程序。(RemoteApp	程序。了解详细信 程序列表为穷		👔 导出 RemoteApp 设置
推荐)	KenoteApp Ik服备器的	但予列表为空。 一个远程卓面连接A	F RD Web 访问中不可	🚏 导入 RemoteApp 设置
RD 网关设置更改	见。更改			▶ 刷新
● 各戶碼将便用田具域的組策略定义的 RD 网关设置。	🕜 有关使用 RD)Web 访问的详细(言息	查看 ▶
	the All Street			📝 帮助
	▶ 创建.rdp 文件			
	▶ 创建 Windows Installer 程序包			
	☞ 有大方友选り	和功并细情思。		
Remotedana 程序			•	
Activity 在所	BD Web 访问	参数	-	
HIT.	NO THEO AJIPJ	and a second		

(3) 单击<RD 会话主机服务器配置更改>进入设置界面,选择"允许用户在初始连接时启动列出和 未列出的程序"。 图58 RemoteApp 部署设置示意图

RemoteApp 部署设置	×				
RD 会话主机服务器 RI	网关 数字签名 通用 RDP 设置 自定义 RDP 设置				
。 客户端在连接到此 RD	会话主机服务器时将使用这些设置。				
计 地名美国克尔					
□ 注接设置 服务器名称(S):	WIN-TNG599MOTER				
	如果 RD 会话主机服务器位于场中,请输入该场的 DNS 名称。				
RDP 端口(R):	3389				
┌────────────────────────────────────					
🗆 在 RD Web 访问中	显示到此 BD 会话主机服务器的远程桌面连接(D)				
访问未列出的程序 —					
○ 不允许用户在初始连接时启动未列出的程序(推荐)(20)					
● 允许用户在初始连接时启动列出和未列出的程序(L)					
	确定 (0) 取消 (C) 应用 (A)				

单击<确定>即可。

3.3.4 关闭windows防火墙

进入[控制面板/系统和安全/windows 防火墙/自定义设置]界面,关闭 windows 防火墙。

图59 Windows 防火墙设置示意图

☆自定义设置	
☆ ◆ 控制面板 • 系统和安全 • Windows 防火墙 • 自定义设置 ▼ ☆ 授加 加 授加 受 授加 受加 受加	
自定义每种类型的网络的设置 您可以修改您所使用的每种类型的网络位置的防火墙设置。 什么是网络位置?	
家庭或工作(专用)网络位置设置	—
■ 阻止所有传入连接,包括位于允许程序列表中的程序	
☐ Windows 防火墙阻止新程序时通知我	
🔞 💿 关闭 Windows 防火墙(不推荐)	
	_
🜍 🔿 启用 Windows 防火墙	
🖉 阻止所有传入连接,包括位于允许程序列表中的程序	
☐ Windows 防火墙阻止新程序时通知我	
🔞 💿 关闭 Windows 防火墙(不推荐)	
*	
	_

单击<确定>即可。

3.3.5 关闭IE增强的安全配置

- (1) 进入[服务器管理器]界面。
- 图60 服务器管理器示意图

■ 服务器管理器				. 🗆 ×
文件(F) 操作(A) 查看(V) 帮	助(H)			
🗢 🔿 📘 🖬				
- 服务器管理器 (WIN-TNG599MOTE	服务器管理器(WIN-7NG599MOTEE)			
 ■ 用巴 □ 功能 ■ 診断 ● 読む ● 読む ● 読む ● 読む 	获取有关此服务器状态的概	述,执行首要管理任务,并添加或删除服务器角色和功能	0	
	◇ 服务器摘要		👔 服务器摘要帮助	1
	◇ 计算机信息		🎨 激活 Windows	
	计算机完整名称:	WIN-7NG599MOTEE	● 更改系统属性 ◎ 恋馬网络法協	
	工作组:	WORKGROUP	·····································	
	本地连接:	192.168.27.233, IPv6 已启用	La 配置服务器管理器远程管理	
	远程桌面:	已启用		
	服务器管理器远程管理:	已启用		
	产品 ID:	没有激活		
	□ 登录时不要显示此控制台(0)			
	◇ 安全信息		🎬 转到 Windows 防火墙	
	Windows 防火墙:	公用:关闭	雷王更新 《 · · · · · · · · · · ·	
	Windows Update:	未配置	 ◆→ 检查新角色 ■ 运行安全配置向量 	
	上次检查更新的时间:	从未安装	№ 配置 IE ESC	
	上次安装更新的时间:	从未安装		
	IE 增强的安全配置(ESC):	为 Administrator 打开 为用户关闭		-
↓	〇 上次刷新时间: 今天 0:42 配置刷新	f		

- (2) 单击<配置 IE SEC>进入 IE 增强的安全配置界面,将管理员和用户禁用。
- 图61 IE 增强的安全配置示意图

Naternet Explorer 増强的安全配置
Internet Explorer 増强的安全配置(IE ESC)降低了您的服务器暴 露于来自基于 Web 内容的潜在攻击的风险。 Internet Explorer 増强的安全配置默认情况下为 Administrators 组和 Users 组启用。
管理员(A):
② ○ 启用(推荐)
😵 💿 禁用
用户の:
② ○ 启用(推荐)
😵 💿 禁用
有关 Internet Explorer 增强的安全配置的详细信息
确定 取消

3.3.6 开启远程桌面

- (1) 右击计算机,单击<属性>进入系统属性界面。
- 图62 系统属性示意图

₽ 系统					
●●●● 控制面板	▼ 系统和安全 ▼ 系统	▼ 🛂 捜索控制面板	<u></u>		
控制面板主页	查看有关计算机的基本(言息	Q		
 ·设备管理器 · · ·	Windows 版本 Windows Server 2008 版权所有 © 2009 Mic Service Pack 1	Windows 版本 Windows Server 2008 R2 Enterprise 版权所有 © 2009 Microsoft Corporation。保留所有权利。 Service Pack 1			
	系统	Pentium (R) Dual-Core CPV E8500 @ 2.93GHz	2.93 GHz (2		
	安装内存 (BAM): 系统类型: 笔和融摸:	处理器) 2.00 GB 64 位操作系统 没有可用于此显示器的笔或融控输入			
	计算机名称、域和工作组 计算机名: 计算机全名: 计算机通述: 工作组:	设置 WIN-TNC599MOTEE 會 WIN-TNC599MOTEE WORKGRDUP	更改设置		
另请参阅 操作中心 Windows Update	Windows 激活 秋余 3 天 可以自 产品 ID: 00488-001-	动数活。立即数活 Windows 2001076-84738 更改产品密钥			

- (2) 单击<远程设置>进入远程桌面配置窗口,选择"允许运行任意版本远程桌面的计算机连接(较 不安全)"。
- 图63 远程桌面设置示意图

系统属性	×
计算机名 硬件 高级 远程	
┌远程协助─────	
■ 允许远程协助连接这台计算机 (B)	
	高級(7)
单击一个选项,然后指定谁可以连接(如果	需要)。
不允许连接到这台计算机(0)	
◎ 允许运行任意版本远程桌面的计算机连	接(较不安全)(L)
 ○ 仅允许运行使用网络级别身份验证的远 算机连接(更安全)(M) 	程桌面的计
帮助我洗择	选择用户(S)
确定	取消 应用(A)

单击<确定>即可。

3.3.7 关闭屏幕保护

(1) 进入"控制面板"中,找到"个性化"。

图64 控制面板示意图

🧱 控制面板									_ 8 ×
00 1	• 控制面板 →					▼ 🐼 搜	t.		<u></u>
文件 (2) 编辑 (2) 查看(Y)	工具(T) 帮助(H) ←⊑∥ [_[
控制面板主页 经典视图		Flash Player	internet 选	iscsi 发起 程序	Java	Windows CardSpace	Windows Update	windows 防 火墙	
		尼 程序和功能	大 印机	山口 电话和调制 解调器选项	します 电源选项	更改」 不性化	<mark>比计算机的主题</mark> 管理工具	<mark>函设置。</mark> 键盘	
		大 默认程序	经公司 公司 日本 日本	区域和语言 选项	任务栏和「 开始」菜单	日期和时间	设备管理器	声音	
		「記标	之 索引选项	正 添加硬件	脱机文件	948和共享 中心	文本到语音 转换) 文件夹选项	
		问题报告和 解决方案	[] 系统	颜色管理	SEA 用户帐户	在终端服务器上安	国 自动播放	字体	

(2) 双击<个性化>后,进入管理界面,找到"屏幕保护程序"。

图65 个性化设置示意图



(3) 双击<屏幕保护程序>后,弹出设置窗口,在"屏幕保护程序"下拉框中选择"(无)"。

图66 屏幕保护程序设置示意图

2	性化	
	🔮 屏幕保护程序设置	
	屏幕保护程序	
文1		
	Image: state in the state	图片来装饰桌面。 春保护程序是一张覆盖屏幕的图片或动画,当您的计算机 台出现。 电子邮件和清空回收站等。 主执行单击和选择等操作时的外观。 印视觉元素,包括菜单、图标、背景、屏幕保护程序、一 更在屏幕上容纳更多或更少的项。还可以控制监视器闪烁

单击<确定>即可。

(4) 最后,重启应用中心。

3.3.8 启用屏幕保护程序超时

- (1) 在运行窗口中输入 "gpedit.msc"。
- (2) 在本地组策略中,进入[用户配置/管理模板/控制面板/个性化]菜单管理页面。



如果没有[个性化]菜单项,那就找[显示]菜单项。

(3) 找到"屏幕保护程序超时"配置项,编辑为"己启用",并且将"启用屏幕保护程序之前等待的秒数"设置为"0"秒。

图67 屏幕保护程序超时设置示意图



3.4 在应用中心中安装相关的工具

3.4.1 安装客户端工具

在应用中心中安装需要使用的客户端工具。如: plsql、sqlplus、SQL server management studio、 MySQLQueryBrowser、VMware vSphere Client 等。

安装好之后,确保能找到可执行程序的绝对路径,在发布应用的时候,需要填写这些客户端工具的 路径。

3.4.2 安装winlogon

在应用发布服务器使用管理员登录堡垒机,在"工具下载"栏下载 winlogon 安装程序,双击 winlogon 安装程序,选择安装路径(默认即可),点击"安装",如下图:
图68 安装 winlogon 向导示意图

🖁 Install Tinlogon: 安装文件夹 📃 🗖 🗙
■ Setup 将安装 自动化组件 在下列文件夹。要安装到不同文件夹,单击 [浏览 @)] 并选择其他的文件夹。 单击 [安装 (I)] 开始安装 进程。
目标文件夹 C:\Winlogon 浏览 (B)
所需空间: 0.0 KB 可用空间: 29.1 GB
取消C) Nullsoft Install System 安装C)

一直选择默认安装,在"Winsync允许 IP"和"服务器 IP"栏中填入堡垒机的 ip 地址,如下图:

图69 Winlogon 配置示意图

船 config		×
安装路径:	C:\Winlogon	
版本:	0. 3. 1. 66	
Winsync允许IP:	192. 168. 10. 234; 192. 168. 10. 235	
服务器IP:	192. 168. 10. 234; 192. 168. 10. 235	
🥅 Wintrace 自动	启动	
✔ 注册 IE 插件		
	确定	取消

点击"确定"完成 winlogon 安装。

🥂 注意

如果有多台堡垒机请用分号间隔各 IP。如果需发布 IE,请勾选"注册 IE 插件"。勾选之后应用发 布服务器上的 IE 浏览器不允许在本地直接使用,必须通过堡垒机的应用发布调用。

4 运维审计系统与应用中心结合使用

用于统一对应用程序进行管理和审计。

4.1 组网需求

图70 应用发布配置组网示意图



4.2 系统版本要求

适用产品版本: ESS 6102

4.3 运维审计系统添加应用发布服务器

利用配置管理员登录堡垒机,在"基本控制">"目标设备"界面中先将应用发布服务器做为普通的 Windows 设备添加到堡垒机,然后编辑应用发布服务器,在服务列表中编辑"RDP"服务,如下图:

图71 编辑应用发布服务器 RDP 服务示意图

设备编辑	RemoteAPP(192.168.	10.233)	服务列表	密码管理	分配设备组	访问规则	可登录用户	
							te	elnet ▼ 新增
类型		名称		状态				
	rdp	rdp		活动		编辑删除		

将"应用发布服务器"勾选上,点击"测试连接"之后,堡垒机会自动获取应用发布服务器上的 Winlogon 信息(版本、路径),如下图:

图72 应用发布服务器 winlogon 测试连接示意图

设备编辑:Remote/	APP(192.168.10.233) 服务列表	密码管理	分配设备组	访问规则	可登录用户	
状态	◎ 禁用 ● 活动					
名称:	rdp	*				
RDP端口:	3389					
协议选项:	☑ 客户端磁盘映射 ☑ console模式					
应用发布服务器:						
	✓ 支持Remoteapp					
Winlogon路径:	C:\Winlogon\					
Winlogon信息:	版本: 0.3 • 同步: 🗹 测试连接 win	llogon版本:0.3	.1.66 .			
剪贴板:	剪贴板: 🕑 下行🕑 上行					
剪切板复制文件:	🗹 下行🗹 上行					
服务图标:	9					
	确定 默认填写 返回前页					

同步:若勾选此选项,堡垒机会在应用发布服务器上创建和普通用户同名的系统账号。当普通用户 访问应用程序时,登录该应用发布服务器都使用各自的同名系统账号,密码由堡垒机随机产生并完 成登录。

图73 勾选同步用户示意图

设备编辑:Remote/	APP(192.168.10.233) 服务	列表 密码管理	分配设备组	访问规则	可登录用户	
状态	◎ 禁用 :● 活动					
名称:	rdp	*				
RDP端口:	3389					
协议选项:	✓ 客户端磁盘映射 ✓ console	∈模式				
应用发布服务器:	*					
	✓ 支持Remoteapp					
Winlogon路径:	C:\Winlogon\					
Winlogon信息:	版本: 0.3 ▼ 同步 🗹 测试连	接				
剪贴板:	✔ 下行✔ 上行					
剪切板复制文件:	🗹 下行🗹 上行					
服务图标:	9					
	确定默认填写返回前	页				

若未同步成功,管理员可以在应用发布服务器的基本信息配置页面手动点击同步,如下图:

图74 手动同步用户密码示意图

设备编辑:RemoteAPP(192.168.10.233)		服务列表	密码管理	分配设备组	访问规则	可登录用户	
状态:	◎ 禁用 💿 活动						
设备名:	RemoteAPP		*				
IP地址:	192.168.10.233						
简要说明:	应用发布服务器		(将在设备选	择菜单中显示)			
部门:	ROOT	•	*				
设备类型:	Microsoft Windows (🛓	<u> 编辑设备类型</u>)					
改密方式:	microsoft windows						
特权帐号:	administrator	•					
编码类型:	GB18030	•					
应用发布服务器:	同步用户和密码						
创建者:	admin (缺省管理员)						
创建于:	2018-01-14 23:49:04						
	确定删除						

1 注意

堡垒机需要访问应用发布服务器 TCP/5156 端口,如果此处获取不到 winlogon 版本和路径信息,请检查 Winlogon 配置页面堡垒机地址是否填写正确,以及应用发布服务器防火墙是否允许该服务端口。

4.4 C/S应用发布

4.4.1 发布应用

新建目标设备之后添加 rdpapp 服务,配置方法如下图所示:

图75 C/S 应用发布 rdpapp 服务示意图

设备编辑:VMware_	_vSphe 服务列表 密码管理 分配设备组 访问规则 可登录用户
状态	◎ 禁用 ● 活动
名称:	192.168.10.160 *
app类型:	general V
RDP服务:	rdp@RemoteAPP •
Agent:	● 禁用 ○ 活动 (仅当目标设备部署了agent服务后生效)
Winlogon:	应用程序: <mark>C:\Program Files (x86)\VMware\In</mark> ♂
	工作目录:
	参 数:
RemoteApp程序:	sirdp 🥑
左键启动会话:	□ 使用无缝模式(仅适用于java模式的会话)
磁盘映射:	☑ 允许客户端磁盘映射
剪贴板:	☞ 下行 上行
剪切板复制文件:	
登录脚本:	v
服务图标:	2
	确定 默认填写 返回前页

- 名称:该应用程序的名称。
- app 类型:这里选择 general。
- Winlogon: "应用程序"一栏填入应用程序的绝对路径。
- RemoteApp 程序:填入 slrdp。
- 其余选项类似 rdp 服务的配置,这里不再重复介绍。

1 注意

少数应用程序除了需要填写绝对路径还需要填写工作目录和参数,请参考应用程序的快捷方式的属性进行设置。

4.4.2 密码代填

对于一些需要登录认证的应用程序,堡垒机提供了一套自动登录的机制来完成用户认证信息的填写。 用户在设备列表中选择应用程序和相应的系统账号之后,堡垒机会在应用发布过程中自动填写登录 页面的用户名和密码等相关信息。

1. 兼容列表

应用程序账号密码代填兼容版本信息如下表所示:

表8 B/S 应用程序账号密码代填兼容列表

类别	软件	已适配的版本
	SOL BlueW	Oracle Client 9i
		Oracle Client 10g
		7.1
Oracle安白崖	PI/SQL Developer	9
Ofacie 合/ ¹ ¹ ¹ ¹ ¹		10
		11
	Tood for Oracle	9.7
		10.5
	SQL Server 查询分析器	2000
		2005简易版中文
SQL Server客户		2008简易版中文
端	SQL Server Management Studio	2005中文
		2008中文
		2012中文
DB2客户端	Quest Central for DB2	V5.0英文
\/NA.vere空内型	VMware vSphere Client	5.5 中文
VIVIWATE各广响	VMware vSphere Client	6.0 中文
甘心	Radmin	3.4 中文版
其它	PowerBuilder	9.0 企业版



内置 CS 代填脚本是根据可执行文件名进行代填脚本的匹配,同一个应用存在多个版本时,默认启 用了最高版本的代填脚本,如果要使用低版本的应用,管理员可以在"策略配置">"密码代填" 栏进行修改。

2. 一般应用密码代填举例

新建目标设备之后添加 rdpapp 服务, 配置方法如下图:

图76 一般应用密码代填 radapp 服务示意图

设备编辑:VMware	vSphe 服务列表 密码管理 分配设备组 访问规则 可登录用户
状态	◎ 禁用 : ● 活动
名称:	*
app类型:	general •
RDP服务:	rdp@RemoteAPP ▼
Agent:	● 禁用 ○ 活动 (仅当目标设备部署了agent服务后生效)
Winlogon:	应用程序:"C:\Program Files (x86)\VMware\I 最近填写
	工作目录:
	参 数:
RemoteApp程序:	sirdp
左键启动会话:	□ 使用无缝模式(仅适用于java模式的会话)
磁盘映射:	✓ 允许客户端磁盘映射
剪贴板:	● 下行● 上行
剪切板复制文件:	● 下行● 上行 ● □
登录脚本:	T
服务图标:	2
	确定 默认填写 返回前页

其中"名称"填入需要访问的ip地址,"Winlogon应用程序"中填写vsphere的绝对路径,"RemoteApp 程序"中填写 slrdp。

接着在"密码管理"页面中配置好 vsphere 登录的账号及密码,配置好访问权限后使用普通用户即可登录,如下图:

图77 一般应用密码代填登录界面示意图

ł	批量启动	过滤 (设备名/IP/简要	说明)	所有组▼	所有设备类型	•	所有协议 🔻	所有部门 🔻	确定
	□ 全选	<u>设备名</u> ∓		IP地址	默认登录帐号		设备类型		
	1	VMware_vSphere_Cli	ient		root		Microsoft Wir	ndows	
		<u>_</u>	设备访问:高级	ž			×		
	服务 53%帐号:			*root					
		192.168.10.1	屏幕大小: 📑	无缝 ▼					
			4	mstsc					
			磁盘映射: 🗌	□ c: □ d: □ e: □ f:	🔲 g: 🔲 h: 🔲 i: 🔲 j: <u>更多</u>				
				确定					

可以看到, ip 地址、用户名以及密码已经被自动填入并且已经自动开始登录, 如下图:

图78 一般应用密码代填结果示意图

🛃 VIIware vSphere Cli	ent 🗙
vmware [•] VMware vSphere ^{••} Client	
 vSphere 5.5 和更高 通过 vSphere Web 续运行,支持与 vS 	版本中引入的所有 vSphere 功能都只能 Client 使用。传统的 vSphere Client 将继 iphere 5.0 相同的功能集。
要直接管理单个主机, i 要管理多个主机, 请输, 或名称。	青输入 IP 地址或主机名称。 入 vCenter Server 的 IP 地址
IP 地址/名称(N):	192.168.10.160
用户名(<u>U</u>):	root
密码(P):	yokokokokokokok
]0	これ ● ● ↓ 15 会话凭据(図)
○ 正在连接…	

3. Oracle应用密码代填

新建目标设备之后添加 rdpapp 服务,配置方法如下图:

图79 Oracle 应用 radapp 服务示意图

设备编辑:orcl10g-	.6.1(10.10.16.11) 服务列表 密码管理 分配设备组 访问规则 可登录用户	
状态	◎ 禁用 ● 活动	
名称:	orcl10g *	
app类型:	general ▼	
RDP服务:	rdp@windows ▼	
Agent:	● 禁用 ○ 活动 (仅当目标设备部署了agent服务后生效)	
Winlogon:	应用程序: <mark>"C:\Program Files (x86)\PLSQL D</mark> 最近填写	
	工作目录:	
	参 数:	
RemoteApp程序:	sirdp	
左键启动会话:	□ 使用无缝模式(仅适用于java模式的会话)	
磁盘映射:	✓ 允许客户端磁盘映射	
剪贴板:	☞ 下行● 上行	
剪切板复制文件:	☞ 下行● 上行	
登录脚本:	T	
服务图标:		
	确定 默认填写 返回前页	

其中"名称"填入需要访问的数据库名称,"Winlogon 应用程序"中填写 plsqldev.exe 程序的绝对 路径,"RemoteApp 程序"中填写 slrdp。

接着在"密码管理"页面中配置好登录 oracle 数据库的账号及密码,配置好访问权限使用后普通用 户即可登录,如下图:

图80 Oracle 应用密码代填登录示意图

批量启动	过滤 (设备名/IP/简要说明)	所有组▼	所有设备类型	所有协议▼ 所有部门▼ 确定	
□全选	<u>设备名</u> ∓	<u>IP地址</u>	默认登录帐号	设备类型	
1	Linux	10.10.16.21	root	General Linux	
2	orcl10g-16.11	10.10.16.11	system_as_0	Microsoft Windows	
服务	rdp orcl10g	设备访问:高级 × 系统帐号: *sys_as_1 ▼ 屋İ土小: 200-500 ▼			
3 🗆	Windows	✓ ms	tsc		
		磁盘映射: 2 c: 6 确 定	□ d: □ e: □ f: □ g: □ h: □ i: □ j: ਭੁ	<u>18</u>	

成功进入界面即为代填成功,如下图:

图81 Oracle 应用密码代填结果示意图

sys_as_1@orcl10g-16.11(10.10.16.11) -	
sys@orcl10g as SYSDBA - PL/SQL Developer	
<u>File V</u> CS <u>P</u> roject <u>E</u> dit <u>S</u> ession <u>D</u> ebug <u>T</u> ools Deployment <u>R</u> eports <u>W</u> indow <u>H</u> elp	
[☆• ☞• 週• 周日 創 各 各 ♡ ○ ※ 陶 電 為 為 중 • ┣ • ┣ 非 年 母 ? [?]?	* 🖻 * 🖸 *
[Q, - >] & = < <	
Connections □ 4 ×	
C + - L	
Imported Fixed Users	
Objects	
Objects Files	
C +	
<current user=""></current>	
All ohierts	
Window list	
Window list Templates	
Find	4 ×
✓ # ♥ △ 羅 Ø	
	Сн 🚎 🥳

• **Oracle** 系统账号说明

Oracle 类型的应用发布系统账号比较特殊, 堡垒机在原有系统帐号的基础上做了扩展, 扩展方式为 "原账号_as_登录角色代码", (其中 as_0 代表角色为 "normal"的 oracle 帐号, as_1 代表角色为 "sysoper", as_2 代表角色为 "sysdba")例如:

oracle 的管理员账号为 "sys",该帐号在用 plsql 登录的时候要选择角色为 "sysdba",所以我们要 新建一个名为 "sys_as_2" 的系统帐号。

图82 Oracle 系统账号说明示意图

设备	编辑:orcl10g-16.1(10	0.10.16.11)	服务列表	密码管理	分配设备组	访问规则	可登录用户
灭火卫士	·测试呢么.rdp •	车 7曲 初分	ᇓᅳ				
·重四 (注:	rdpapp服务的登录测·	」 加建於沈 试,不支持Re	emoteapp程序,	只支持Winlog	on发布的应用程J	字)	
系	统帐号	切换自	密码	提示符	自动运行	Domain	操作
*	administrator						新建
	any						新建
	enable						新建
	netscreen						<u>新建</u>
	null						<u>新建</u>
	root						新建
	self						新建
	super						新建
	sys_as_1		密码已设置				编辑 <u>帐号改密</u> 登录测试
	system_as_0		密码已设置				<u>编辑 帐号改密 登录测试</u>

4.5 B/S应用发布

4.5.1 IE浏览器

1. Winlogon配置

通过 IE 浏览器来访问的系统,我们需要通过 http 类型的应用发布来进行访问。需要开启 Winlogon 的"注册 IE 插件"功能,如下图所示:

图83 注册 IE 插件示意图

船 config	×				
安装路径:	C:\Winlogon				
版本:	0. 3. 1. 66				
Winsync允许IP:	192. 168. 10. 234; 192. 168. 10. 235				
服务器IP:	192. 168. 10. 234; 192. 168. 10. 235				
🔲 Wintrace 自动	启动				
▼注册 IE 插件					
	确定 取消				

2. 发布应用

新建目标设备之后添加 rdpapp 服务,配置方法如下图:

图84 B/S 应用发布 rdpapp 服务示意图

设备编辑:Internet	Exp	服务列表	密码管理	分配设备组	访问规则	可登录用户
状念	□禁用 (リ活动				
名称:	堡垒机			* 🥑		
app类型:	http	•				
RDP服务:	rdp@Rer	moteAPP	¥			
Agent:	● 禁用 〔)活动 (仅	当目标设备部署	署了 agent 服务后:	生效)	
Winlogon:	应用程序: <mark>(</mark>	C:∖Progran	n Files\Interne	et Explorer 最近	填写	
	工作目录:					
	参数:					
RemoteApp程序:	slrdp					
左键启动会话:	🔲 使用无线	逢模式 <mark>(</mark> 仅适	用于java模式的	內会话)		
磁盘映射:	🗹 允许客户	白端磁盘映射	时			
剪贴板:	✔ 下行✔	上行				
剪切板复制文件:	🗹 下行🗹	上行		_		
入口URL:	https://192	2.168.10.2	234/	* 🥑		
登录脚本:		¥				
允许域名:	192.168.1 * 其他可访 * 例如www	l0.234 问域名白名		,用空格或回车分	}隔,除此之 外	谢不可访问。
		v.baluu.com	172.100.1.1			
服务图标:	\bigcirc					
	确定對	\\\	返回前页			

- 名称:该应用程序的名称。
- App 类型:本节介绍 http 方式,这里选择 http。
- Winlogon: "app 类型"选择 http 之后"应用程序"一栏会自动填上 IE 浏览器的路径。
- RemoteApp 程序:填入 slrdp。
- 入口 URL: 填入要访问的 URL 链接
- 允许域名:填上允许访问的 ip 地址或者域名(格式参考下面的说明文字)。
- 其余选项类似 rdp 服务的配置,这里不再重复介绍

配置好访问权限之后便可直接访问,访问过程中 IE 浏览器会自动跳转至配置好的 URL。

3. 密码代填

• 全自动脚本

全自动脚本是 HTTP 类型密码代填中最简单配置的方式,编辑相关服务,如下图:

图85 http 类型面	己置全自动脚本登录示意图
--------------	--------------

设备编辑:http	服务列表密码管	理 分配设备组	访问规则	可登录用户	
状态	○禁用 ◉活动				
名称:	堡垒机	*			
app类型:	http 🔻				
RDP服务:	rdp@RemoteAPP	•			
Agent:	◉禁用 ○活动 (1	R当目标设备部署了a	gent服务后生效	()	
Winlogon:	应用程序:C:\Progra	n Files\Internet Ex	plorei		
	工作目录:				
	参数:				
RemoteApp程序:	slrdp				
左键启动会话:	🔲 使用无缝模式(仅)	用于java模式的会话	i)		
磁盘映射:	✔ 允许客户端磁盘映	射			
剪贴板:	🗹 下行🗹 上行				
剪切板复制文件:	☑ 下行☑ 上行				
入口URL:	https://192.168.4.1	11/ *	2		
登录脚本:	全自动脚本 ▼				
Url pattern:	http[s]?://{domain}/	\$ +*	就认填写		
允许域名:	192.168.4.111 * 其地回注词地名白	<u>//</u> 	허생 ᆤ ᇢ ᄎ 八명	요. 비, 는 노, 코마, 구,	a)+ (a
	*例如www.baidu.co	中(小肥市 //),用. n 192.168.1.1	工俗蚁凹于刀隔	,所此之外御个	니띠이
服务图标:					

选择登录脚本为"全自动脚本"。

填写网页匹配的 Url pattern,可以点击"默认填写"生成左边的默认 Url pattern, Url pattern 是指 HTTP 类型密码代填中的匹配。



- 当 Url pattern 匹配网页的 URL 时,堡垒机就会提交用户名、密码进行代填操作,所以需要确定。Url pattern 不能匹配成用户登录成功后的网页 URL,否则堡垒机就会一直尝试代填。
- Url pattern 采用的是正则表达式的结构。

进入"密码管理"菜单,托管账号密码,并分配相应的权限,直接使用普通用户进行登录测试,如下图:

图86 http 类型配置全自动脚本登录页面示意图

批量启动	过滤 (设备名/IP/	新要说明) 所有组▼ 所有设备类型	▼ 所有协议 ▼ 所有部门 ▼ 确定
□全选	<u>设备名</u> ₹	<u>IP地址</u> 默认登录帐号	<u>设备类型</u>
1	http	设备访问:高级	crosoft Windows
服务	经 至机	系统帧号: <mark>*admin ▼</mark> 屏墓大小: 无缝 ▼ ✓ mstsc	
2	Oracle_PLSQL_[磁盘映射: □ c: □ d: □ e: □ f: □ g: □ h: □ i: □ j: 更多	icrosoft Windows
3 🗆	VMware_vSpher	确定	icrosoft Windows

登录网页进行了账号密码代填并成功进入网页,即为成功,如下图:

图87 http 类型配置全自动脚本登录成功示意图

🖉 https://192.168.4.111/ - Windows I	nternet Explorer	
💽 🕤 🗢 😰 https://192.168.4.111/	💌 😵 证书错误 💀 😏 🗙 🔎 Bing	P -
🙀 收藏夹 🛛 🍰 建议网站 🔹 🙋 网页快讯	\库 ▼	
🔾 https://192.168.4.111/	🚵 • 🗟 • 🖃 🖶 • 页面 🕑 • 安全 🕃 •	工具 (1) • 🔞 •
		<u> </u>
	运维审计系统	
	帐号: admin	
	密 码:	
and the second se		
Store (登录	
		-
•		<u>)</u>
摹待 https://192.168.4.111/lo	😜 Internet 保护模式: 禁用 🍡	СН 🍝 🙆 -



因为登录测试不允许进行操作,如果遇见"证书错误"等需要先进行交互式操作才能出现登录页面 的,请先建立访问权限,然后用普通用户测试。

• 半自动脚本

使用半自动脚本方式,需要获取登录界面 html 的标签属性,配置比全自动复杂。 首先使用浏览器,访问目标设备页面,如下图:

图88 http 类型半自动脚本登录页面示意图

▲ 不安全 | https://192.168.4.111



接着点击键盘 "F12", 打开浏览器开发人员调试工具, 如下图:

(1) 点击"选择元素"按钮。

(2) 将鼠标移动到用户名输入框后单机。确认该元素被锁定。

(3) 查看该 html 元素的属性。其中需要获取 "name" 字段属性或者 "id" 字段属性。

图89 http 类型半自动脚本页面元素示意图



以同样的方式获取密码框和登录按钮的"name"或者"id"属性,编辑相关服务,如下图:

图90 半自动脚本服务配置示意图



- 选择登录脚本为"半自动脚本"。
- 填写网页匹配的 Url pattern,可以点击"默认填写"生成左边的默认 Url pattern。
- 编辑"用户名框标识","密码框标识","提交按钮标识"为上一步获取到的内容。

接着进入"密码管理",托管账号密码,并分配相应的权限,直接使用普通用户进行登录测试。

图91 半自动脚本登录测试页面示意图

批量启动	过滤 (设备名/IP/简	简要说明) 所有组	▼ 所有设备类型	▼所	有协议 🔨 所有部门 🔨 确定
□全选	<u>设备名</u> ₹	<u>IP地址</u>	默认登录帐号	<u>B</u>	<u> </u>
1	http	设备访问:高级		×	icrosoft Windows
服务	经 至机	系统帐号: <mark>*admin ▼</mark> 屏墓大小: <u>无缝</u> ▼ ✓ mstsc			
2	Oracle_PLSQL_[磁盘映射: □ c: □ d: □ e: □ f: □	g: □ h: □ i: □ j: <u>更多</u>		icrosoft Windows
3 🗆	VMware_vSpher	确定			icrosoft Windows

登录网页进行了账号密码代填并成功进入网页,即为成功。

图92 半自动脚本登录测试成功示意图



<u>人</u>注意

B/S 应用的密码代填仅支持 form 表单有明确的 id 或者 name,无验证码,登录按钮没有绑定特殊 JavaScript 事件的情况。

• URL 限制

IE 浏览器可以做 URL 限制,在允许域名栏填入允许访问的 IP 或域名白名单,如下图:

图93 IE 浏览器 URL 限制示意图

设备编辑:http	服务列表	密码管理	分配设备组	访问规则	可登录用户	
Agent:	●禁用 ○)活动 (仅当目	目标设备部署了aq	gent服务后生效	()	
Winlogon:	应用程序: C	:∖Program Fi	les\Internet Ex	olorei		
	工作目录:					
	参数:					
RemoteApp程序:	sIrdp					
左键启动会话:	🔲 使用无缝	逢模式 <mark>(</mark> 仅适用于	⁻ java模式的会话)		
磁盘映射:	🗹 允许客户	□端磁盘映射				
剪贴板:	✔ 下行✔ .	上行				
剪切板复制文件:	🗹 下行🗹 .	上行				
入口URL:	https://192	2.168.4.112/	*			
登录脚本:	全自动脚	本 ▼				
Url pattern:	http[s]?://{	domain}/\$	* 🗒	<u>t认填写</u>		
允许域名:	192. 168. 4 * 其他可访 * 例如www	11山 问域名白名单([.] .baidu.com 19	不能带"八"),用雪 2.168.1.1	2格或回车分隔	,除此之外都不	可访问。
服务图标:		认填写词	可前页			
	, and					

4.5.2 Chrome浏览器

1. 准备条件

Chrome 浏览器用于支持 vSphere_Web_Client 密码代填,在应用发布服务器上需配置以下内容:

- (1) 安装 jave8: 需要确保系统环境变量中包含 Java 的路径需要确保系统环境变量中包含 Java 的路径
- (2) 安装 Chrome 浏览器: Chrome v59 至 v61 之间的版本
- (3) 安装.net3.5

2. 发布

新建目标设备之后添加 rdpapp 服务, 配置方法如下图:

图94 Chrome 类型 radapp 服务示意图

设备编辑:vSphere	_Web 服务列表 密码管理 分配设备组 访问规则 可登录用户
状态	◎ 禁用 : ● 活动
名称:	vSphere_Web_Client * 🧭
app类型:	chrome v
RDP服务:	rdp@RemoteAPP ▼
Agent:	● 禁用 ── 活动 (仅当目标设备部署了agent服务后生效)
Winlogon:	应用程序: <mark>C:\Users\Administrator\AppData\L</mark> 🥑
	工作目录:
	参 数:
RemoteApp程序:	
左键启动会话:	□ 使用无缝模式(仅适用于java模式的会话)
磁盘映射:	□ 允许客户端磁盘映射
剪贴板:	□ 下行□ 上行
剪切板复制文件:	□ 下行□ 上行
入口URL:	https://10.10.18.201/vsphere-clien * 🧭
登录模式:	不代填▼
服务图标:	(2)
	确定 默认填写 返回前页

- 名称:该应用程序的名称
- App 类型:本节介绍 Chrome 方式,这里选择 Chrome。
- RDP 服务: 配置应用发布服务器及登录该应用发布服务器的系统账号,若之前配置应用发布服务器勾选了"同步"则这里只需要选择应用发布服务器。
- Winlogon: "应用程序"一栏填入 Chrome 浏览器的绝对路径。
- RemoteApp 程序:不填
- 入口 URL: 填入要访问的 URL。
- 登录模式:不带填、自动和高级三种模式

配置好访问权限之后便可直接访问,访问过程中 Chrome 浏览器会自动跳转至配置好的 URL。

- 3. 密码代填
- **chrome** 类型自动代填

自动寻找需要代填的用户名,密码框和提交按钮,该模式只能处理简单场景,可适用于 vSphere_Web_Client 密码代填

编辑目标设备 rdpapp 服务, 配置方法如下图:

设备编辑:vSphere_	_Web	服务列表	密码管理	分配设备组	访问规则	可登录用户
状态	○禁用(◉ 活动				
名称:	vSphere_	_Web_Client		* 🥑		
app类型:	chrome	•				
RDP服务:	rdp@Re	moteAPP •]			
Agent:	●禁用(○活动 (仅当)	4目标设备部署	了agent服务后生	效)	
Winlogon:	应用程序 <mark>:</mark>	C:\Users\Adı	ministrator\Ap	pData\L 🥑		
	工作目录 <mark>:</mark>					
	参数:					
RemoteApp程序:						
左键启动会话:	🔲 使用无	缝模式 (仅适用	于java模式的会	≿话)		
磁盘映射:	🔲 允许客	户端磁盘映射				
剪贴板:	□ 下行□	上行				
剪切板复制文件:	□ 下行□	上行				
入口URL:	https://10).10.18.201/v	sphere-clien	* 🥑		
登录模式:	自动	·				
服务图标:	Ø					
	确定	默认填写 返	反回前页			

图95 Chrome 类型密码自动代填 radapp 服务示意图

其中登录模式选择"自动",其它参考 chrome 类型的发布。

• 高级代填

如果自动代填没有代填成功,可以使用高级代填配配置,编辑目标设备 rdpapp 服务,配置方法如下图:

设备编辑:vSphere	_Web	服务列表	密码管理	分配设备组	访问规则	可登录用户
状态	○禁用	• 活动				
名称:	vSphere	_Web_Client	t	* 🥑		
app类型:	chrome	•				
RDP服务:	rdp@Re	emoteAPP •				
Agent:	●禁用	○活动 (仅当)	当目标设备部署 ⁻	了 <mark>agent服</mark> 务后生	效)	
Winlogon:	应用程序 <mark>:</mark>	"C:\Program	Files (x86)\G	oogle\C 🥑		
	工作目录:					
	参数:					
RemoteApp程序:						
左键启动会话:	🔲 使用无	缝模式 (仅适用	于java模式的会	∃		
磁盘映射:	✔ 允许客	户端磁盘映射				
剪贴板:	🗹 下行🗹	上行				
剪切板复制文件:	✔ 下行✔	上行				
入口URL:	https://10	0.10.18.201/\	/sphere-clier	* 🥑		
登录模式:	高级	•				
用户名框标识:	#usernar	me		* 🥑		
密码框标识:	#passwo	ord		* 🥑		
提交按钮标识:	#submit			* 🥑		
iframe标识:	#websso)		v		
服务图标:	Ø					
	确定	默认填写 辺	包前页			

图96 Chrome 类型密码高级代填 radapp 服务示意图

登录模式:选择"高级",填入用户名框、密码框、提交按钮标识(都为 css 选择器),右击页面"用 户框 > copy > copy selector",具体操作如下图所示:

图97 Chrome 类型密码代填高级模式示意图



4.6 配置访问权限

使用配置管理员登录到堡垒机,进入"权限配置","权限配置"进行应用访问权限的配置,其中对应的服务协议需选择 rdpapp,如下图所示

图98 应用发布访问权限配置示意图

基本	控制 🗸	权限控制	密码控制 🗸	事件审计 ~	统计报表 🗸	双人复核 🗸					配置管理员 🗸 adsin 🗸 💮 🔪
访问	权限 命	i令权限									
您的	当前位置:	权限控制:	> 访问权限								
新菇	主 部门: F	ROOT • #	则名	用户:		设备:	系统帐号:	服务:所有协议 🔻	提交 全部型	時日 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本	共1页: < 1 >
规	则			部门	用户帐号	目标设备	系统帐号	服务类型	服务协议	服务名称	动作
1	Internet	t_Explorer		ROOT	admin	http	admin		rdpapp		编辑 登录状则 克隆規則 关联: <u>用户组(0) 用户(1)</u> 设备组(0) 设备(<u>1</u>) <u>运给纸(0)</u> 设备(<u>1</u>)
2	Oracle_	PLSQL_Deve	loper	ROOT	<u>admin</u>	Oracle PLSQL Developer	<u>scott as 0</u>		rdpapp		編攝 登景規则 克隆規则 关联: <u>用户组(0) 用户(1)</u> 设备组(0) 设备(1) <u>系统统号(1)</u> 双人复技候选人(0)
3	ReoteAp	pp_VpxClient		ROOT	<u>admin</u>	<u>VMware vSphere Client</u>	administrator any root		rdpapp		編輯 臺法規則 克建規則 关联:用户组(0) 用户(1) 设备组(0) 设备(1) 系统财号(3) 双人裏技強法人(0)

如果某设备发布了多个应用程序,限制只能使用某个设备中特定应用,可以在访问权限对应的"服 务名称"栏进行配置。如下图所示

图99 限制只能使用某个设备中特定应用示意图

您的当前位置: ₹ 创建者: admin (缺省管理员) 规则名称: Internet_Explorer 设备排序: 全局缺省 (终端登录菜单中的目标设备排序方式) 部门: ROOT * 服务类型: 字符终端 图形终端 2 文件传输 服务为说议: telnet 3sh 1 th5250 rdp 1 vnc xdmcp € rdpapp ftp 3ftp 服务方法议: 192.168.10.160 LSQL_Developer 市问设备时生成事件 要结机 新興 None ▼ 服务 「方印设备时生成事件 正 「方印设备时生成事件 正 「市印 原期號: 「下行 上行 剪切版复制文件: 下行 上行 御法 「取消	设备访问 🗸	双人复核 🗸							
您的当前位置: V限控制 > 访问权限 > 编辑规则 创建者: admin (缺省管理员) 规则名称: Internet_Explorer 设备排序: 全局缺省 (终端登录菜单中的目标设备排序方式) 部门: ROOT * 服务类型: 字符终端 圖形终端 □ 文件传输 服务协议: telnet □ ssh □ th5250 □ rdp □ vnc □ xdmcp ☑ rdpapp □ ftp □ sftp 服务协议: telnet □ ssh □ th5250 □ rdp □ vnc □ xdmcp ☑ rdpapp □ ftp □ sftp 服务表称: 192.168.10.160 ☑ LSQL_Developer □ rdp 運 差轧 访问设备时生成事件 事件级别: None ▼ 磁盘映射: ① 允许使用 剪切板复制文件: 下行□ 上行 剪切板复制文件: 下行□ 上行 确定 Ⅲ除 取消									
创建者: admin (缺省管理员) 规则名称: Internet_Explorer 设备排序: 全局缺省 (终端登录菜单中的目标设备排序方式) 部门: ROOT * 服务类型: 字符终端 图形终端 文件传输 服务协议: telnet ssh th5250 rdp vnc xdmcp rdpapp ftp sftp 服务名称: 192.168.10.160 DLSQL_Developer rdp 正 正 新日: None 又 磁盘映射: ① 允许使用 剪切板复制文件: 下行 上行 正行 解定: Image: Image	您的当前位置:	权限控制 > 访问权限 > 编辑规则							
規则名称: Internet_Explorer * 设备排序: 全局缺省 (终端登录菜单中的目标设备排序方式) 部门: ROOT ▼ 服务类型: 字符终端 図形终端 文件传输 服务协议: telnet ssh tn5250 rdp vnc xdmcp rdpapp ftp sftp 服务名称: 192.168.10.160 ✓ LSQL_Developer # # jnin设备时生成事件 事件级别: None ▼ #<	创建者	ă: admin (缺省管理员)							
设备排序: 全局缺省 (终端登录菜单中的目标设备排序方式) 部门: ROOT ★ 服务类型: 字符终端 图形终端 2件传输 服务热议: telnet ssh th5250 rdp vnc vdmcp rdpapp ftp sftp 服务名称: 192.168.10.160 ✓ LSQL_Developer 市内设备时生成事件 * 野件级别: None ▼ 磁盘映射: 公允许使用 ● 剪贴板: 下行 L行 ● 頭板定 町消	规则名称	ت: Internet_Explorer *							
部门: ROOT ▼* 服务类型: 字符终端 图形终端 文件传输 服务本程: 192.168.10.160 ℃ LSQL_Developer 定差单机 访问设备时生成事件 事件级别: None ▼ 标题: ① 前期 ① 前期 ② 允许使用 剪贴板: ① 下行 上行 前时 ② 前时 ② 前日 ② 前日 <th>设备排序</th> <th>第: 全局缺省 ▼ (终端登录菜单中的目标设备排序方:</th>	设备排序	第: 全局缺省 ▼ (终端登录菜单中的目标设备排序方:							
服务类型: □字符终端 图形终端 文件传输 服务协议: telnet ssh tn5250 rdp vnc xdmcp rdpapp ftp sftp 服务本部: 192.168.10.160 rdp LSQL_Developer 访问设备时生成事件 事件级别: None 标题: 可以定 解告 市均 前问设备时生成事件 事件级别: None 市和: 可以定 解告 即號 ○方行使用 剪助板: 下行 算切板复制文件: 中行 取消	部门]: ROOT • *							
服务协议: telnet ssh tr5250 rdp vnc xdmcp rdpapp ftp sftp 服务内认识: 192.168.10.160 rdp 2450L_Developer 访问设备时生成事件 2450L_OP 事件级别: None 标题: 磁盘映射: 公允许使用 剪贴板: 下行 单时板复制文件: 下行 旗定 即除	服务类型	2: 🔲 字符终端 🔲 图形终端 💭 文件传输							
服务名称: 192.168.10.160 ✔ DLSQL_Developer rdp ♂ 量 並机 访问设备时生成事件 事件级别: None 标题: 磁盘映射: ✓ 允许使用 剪贴板: 下行 算切板复制文件: 下行 确定 剛除 取消	服务协议	服务协议: 📃 telnet 🔍 ssh 💭 tn5250 💭 rdp 💭 vnc 🔜 xdmcp 🗹 rdpapp 💭 ftp 💭 sftp							
访问设备时生成事件 事件级别: None 标题: ▼ 磁盘映射: ② 允许使用 剪贴板: □ 下行□ 上行 剪切板复制文件: □ 下行□ 上行 确定 删除	服务名称	济: □ 192.168.10.160							
事件级别: None ▼ 标题: ● ● 磁盘映射: ● ○ 剪贴板: ● 下行● 上行 剪切板复制文件: ● 下行● 上行 确定 删除 取消		访问设备时生成事件							
 标题: 磁盘映射: 公许使用 剪贴板: □ 下行□ 上行 剪切板复制文件: □ 下行□ 上行 确定 删除 取消 	事件级别	il: None ▼							
磁盘映射: 公许使用 剪贴板: 下行 上行 剪切板复制文件: 下行 上行 确定 删除 取消	标题	<u>ā</u> :							
剪 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	磁盘映射	寸: ✔ 允许使用							
剪切板复制文件: □ 下行□ 上行 确定 删除 取消	剪贴板	反: 🔲 下行 上行							
确定 删除 取消	剪切板复制文件	キ: □ 下行□ 上行							
		确定 删除 取消							

4.7 普通用户访问

普通用户先登录堡垒机,然后选择相应的应用程序完成登录,整个过程跟在本地机器上打开应用程 序一样。

图100 普通用户访问应用发布器的应用

您的当船位置: 设备访问 > 按访问规则分组										
访问组	系统提示									
过滤: 清空	您的授权还有 11 天就要过期,请及时授权									
具近法词	批量启动	过滤(设备名/IP/简要说明)		所有组▼	所有设备类型	▼ 所有协议 ▼	所有部门 ▼ 确定			
	□ 全选	<u>设备名</u> ∓		<u>IP地址</u>	默认登录帐号	设备类型		简要说明		
<u> 所有可访问设备(3)</u>	1 http				admin	Microsoft W	lindows			
Internet Explorer (1)			_				ו			
Oracle PLSQL Developer (1)	10 2		设备访问:高级 ×							
ReoteApp VpxClient (1)	HR 95		系统帐号	: *admin ▼						
		堡垒机	屏幕大小	: 无缝 ▼						
	2	Oracle_PLSQL_Developer		✓ mstsc			ndows			
	服务		磁盘映射	: □ c: □ d: □ e: 确定	□ f: □ g: □ h: □ i: □ j: <u>更多</u>					
		PLSQL_Devel								
	3 🗆	VMware_vSphere_Client			root	Microsoft W	findows			
	服务	192.168.10.1								

自动化改密配置举例

Copyright © 2018 北京紫光恒越网络科技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。



1 简介1
2 配置前提1
2.1 选择密码备份方式
2.1.1 邮件1
2.1.2 文件服务器
2.2 设置加密密码3
3 配置举例
3.1 组网需求
3.2 系统版本要求
3.3 修改Unix/Linux密码5
3.3.1 配置思路
3.3.2 配置步骤
3.4 修改Windows密码
3.4.1 配置思路8
3.4.2 配置步骤8
3.5 备份密码到文件服务
4 常见问题

1 简介

自动化改密可以实现对目标设备的系统账号的密码的自动修改、自动备份。

2 配置前提

2.1 选择密码备份方式

密码备份支持邮件服务器发送与文件服务器上传两种方式,选择一种即可。

2.1.1 邮件

(1) 设置 SMTP

使用超级管理员登录,打开[策略配置/系统策略]页面,在系统邮件配置中填写 SMTP 服务器地址与用户名密码。

图1 设置 SMTP

基本控制~	事件审计	✓ 策略	置 系统	€设置 ∽	工单管理~	双人复核 ~					超级管理员 🗸
系统策略	告警事件	字符终端	会话配置	身份验证	正 设备密码	设备类型	部门配置	改密方式	密码代填	IE代填脚本	
您的当前位了	【: 策略配]	置 > 系统策时	各								
一系统邮件	記置										
系统邮件系	来源: root@	Diware.com	_	(请使用带	完整域名的正式	忧邮件地址)					
SMTP服务	务器: 地址	192.168.7.2	5 , 端口 2	25 ,安全道	重讯: N/A ♦	, 用户名 adm	in@iv,密码		则试		

点击<测试>按钮,可以测试邮件是否可以正常发送。

图2 测试





默认情况下运维审计系统使用内置的 SMTP,但是需要正确配置运维审计系统的 DNS 服务器。 如果使用其它 SMTP,需提供正确的 SMTP 信息及用户名密码。

(2) 设置密码保管员邮件地址

使用超级管理员登录,打开[基本控制/用户账号]页面,找到密码管理员用户,点击<管理>按钮,添加邮件地址。

图3 设置密码保管员邮件地址

基本控制事件	审计 - 策略配置 -	系统设置 🗸 🔳	「单管理 →	双人复核 ~					
用户帐号									
您的当前位置:基	本控制 > 用户帐号 > 用]户编辑							
基本属性	高级属性								
状态:	○禁用 • ○活动(查	看登录日志 查看可	<u>]登录设备 5</u>	分配用户组 管理访问规则 用户帐户设置)					
登录名:	user01		*						
真实姓名:	user01		*						
邮件地址:	root@iware.com		 						
手机号码:									
部门:	系统运维部		*						
职位:									
工号:									
身份验证方式:	本地认证		\$						
密码:	不改变		★ *						
	🗌 下次登录时须修改	密码							
权限:	🗌 超级管理员 🗌 审计管理员 🗌 配置管理员 🗹 密码保管员 🗹 普通用户								
	审计权限: 🗌 下载会话 🗌 键盘事件								
	(需要下载会话权限,)	必须勾选键盘事件机	又限)						
	保存删除								

2.1.2 文件服务器

使用超级管理员登录,打开[策略配置/系统策略]页面,在文件服务器配置中的文件服务器 1,协议 支持 "ftp 或 sftp",剩余填写服务信息即可。

图4 设置文件服务器

文件服务器1:	协议: sftp 💲			
	名称:SecPath	地址:192.168.7.60	端口:22	用户名:admin
	密码:••••	工作目录:passwd	子目录:%Y-%m-%d	编码:UTF-8
文件服务器2:	协议: None \$			
	(子目录填写格式说明:%)	/-%m-%d 则自动生成的目录格式为:	YYYY-MM-DD %Y %m %d 次序可	以自定义)

₩ 提示

文件服务器中使用的用户需要具有创建目录与创建文件的权限,否则会由于权限错误导致传输失败。

2.2 设置加密密码

使用密码保管员登录,把鼠标移动到右上角账号名字上,在弹出的下拉菜单中选择[账户设置],输入当前登录密码后点击<确定>按钮,进入账户设置页面。

图5 设置加密密码



在账户设置页面中,选择<信息交换加密方式>选项卡,在 **ZIP** 文件密码中输入用于打开保存改密结果的压缩包。

图6 设置加密密码

基本控制 ~	权限控制 ~	密码控制 ~	事件审计 ~	统计报表 ~	工单管理 ~	脚本任务 ~	双人复核 ~			
帐户设置										
您的当前位置	: 修改帐户设	置								
个人设置	信息交排	與加密方式	自由修改密码	马 设备访	问表格设置					
	这里设置的 1.加密包含 2.用户自行 ZIP 文件密码 (算法强度软	密码的作用: 敏感内容系统曲 下载的敏感信息 码 较弱,请设置8位	3件的附件 。 立以上的复杂密码	马)						
设置		••••••								
确认密码	:									
	确定									

3 配置举例

3.1 组网需求

图7 运维审计系统组网图



3.2 系统版本要求

适用产品版本: ESS 6102。

3.3 修改Unix/Linux密码

3.3.1 配置思路

- 托管 root 密码,并保证登录测试成功
- 创建改密计划,定期修改设备密码。

3.3.2 配置步骤

(1) 使用配置管理员登录,打开[基本控制/目标设备],找到要改密的设备点击<密码管理>按钮。

图8 密码管理

基本技	2制 权限控制 - 1	密码控制 ~ 事件审	计 ~ 统计报表 ~	工单管理 ~	脚本任务~	双人复核~				配置管理员 🗸 🕴 admin 🗸 🕴 🍘 🗡
用户中	用户帐号 系统帐号 目标设备 用户分组 设备分组									
您的当	2的当前位置: 基本控制 > 目标设备 已用数: 3, 可用数									
新建	批量导入批量修改	导出设备 状态:	活动 🗘 部门:	ROOT \$	系统类型: A	所有设备类型	•	重复IP:	♦ 过滤:	确定 共1页: < 1 >
	<u>名称</u> ↓	部门	<u>IP地址</u>	系统美	性型	字符	守终端	图形终端	文件传输	动作
1	192.168.7.198	ROOT	192.168.7.198	Micros	soft Windows			rdp		编辑 密码管理 改密日志
2	192.168.7.70	系统组	192.168.7.70	Gener	ral Linux	ssh	i	vnc	sftp	编辑 密码管理 密钥管理 改密日志
3	winsrv-2008	系统运维部	192.168.7.112	Micros	soft Windows			rdp		编辑 密码管理 改密日志

(2) 托管特权账号 root 密码,并可以登录测试成功。

图9 登录测试

			运	推审计系统 -	运维审计系统	ξ. L						
▲ 不好	▲ 不安全 https://192.168.7.72/manager/server_edit_index.php?tab=2&id=1&nomenu=1											
设备组	扁辑:192.168.7.70(1	192.168.7.70)	服务列表	密码管理	密钥管理	分配设备组	访问规则	可登录用户				
登陆	测试服务: ssh ✦	新建系统帐号										
系	统帐号	切换自	密码	提示符	自动运行	Domain	操作					
	administrator						新建					
	any						<u>新建</u>					
	enable						<u>新建</u>					
	netscreen						新建					
	null						<u>新建</u>					
*	root		密码已设置				编辑 帐号改图	整 <u>登录测试</u>				
	self						新建					
	super						新建					
		Last login: Last failed There were Last login: <u>froot@Serve</u> Auto-login	Thu Feb 1 0 login: Thu F 2 failed logi Thu Feb 1 1 rWorld ~1# succeeded.	orld:~ — exp 9:44:29 201 eb 1 10:44 n attempts 0:19:10 201	ect -f /var/fol 18 from 192. 3:09 CST 20 5 ince the 18 from 192.	ders/gt/gr1d8r 168.7.34 8 from 192.1 ast success1 168.7.72	9947x0wvnq 168.7.60 on ful login.	y9l1klmh000				

(3) 打开[密码控制/改密计划],点击<新建计划>按钮,创建定期改密计划。

图10 创建定期改密计划

基本控制 ~	权限控制 ~	密码控制	事件审计 ~	统计报表~	工单管理 ~	脚本任务 ~	双人复核~
改密计划	设备改密日志						
您的当前位置	[: 密码控制 >	改密计划 > 新	键				
定期自动修	改						
21.41.47.4%。							
印め合称に	inux-pian						
:L 14E	ROOT		÷ *				
[-]任务排	丸行						
任务时间:	00 \$: 00 \$						
任务日期:	2018-02-02 清	空 / <u>恢复(</u> 下次	执行任务的日期	朋, 例如今天为	2018-02-01,留	空表示任务不会	生效)
任务间隔:	每 3 \$ 个月	或每	天,执行一次 ()	先填一项,月数;	占优)		
登录测试:	□ 改密后执行,(又用于改密结果	參考				
-[-]密码第	策略						
设定: • 随	机生成不同密码	○自动设置	相同密码	手动指定密码			
策略: • 全	:局 ○定制						
[-]改密道	通知						
发送邮件:	🗸 admin 缺省管	理员					
	以下用户不可选	择[+]					
密码发送							
发送格式:	⊖txt ⊙xls						
[注意: 必须	须以下2种方式中	选择一种密码	发送方式]				
[-]邮件	牛发送						
发送邮件	⊧: 🗹 admin 缺省	管理员					
	以下用户不可	选择[+]					
[+1文	件服务器						
确定 取消	4						

(4) 设置好的改密计划会按照预期时间进行修改,也可以通过手动方式立即执行。

图11 立即执行

基本控制 ~	权限控制 ~	密码控制	事件审计~	统计报表~	工单管理 ~	脚本任务 ~	双人复核~	記量管理员 🗸 📔 admin 🗸 🕴 🕖 🎽
改密计划	设备改密日志							
您的当前位	置: 密码控制 > i	改密计划						
新建计划	导出							
任务名称		目标设备		系统帐号	上次何	修改密码	距离下次修改密码	动作
1 linux	x-plan	<u>192.168.7.</u>	<u>70</u>	root			1 day after the 00:00	编辑 历史修改记录 查看密码状态 <mark>: 立即修改</mark> 关联: <u>设备组(0)设备(1)系统帐号(1)</u>



只有同时具备配置管理员和密码保管员权限的用户才可以手工设置密码。

3.4 修改Windows密码

3.4.1 配置思路

- 在目标设备上安装 Winsync 程序。
- 创建改密计划,定期修改设备密码。

3.4.2 配置步骤

(1) 登录目标设备,安装 winsync 程序,保持默认安装即可。

图12 安装 winsync 程序

🛃 Setup - WinSync	- 🗆 ×
	Welcome to the WinSync Setup Wizard
	This will install WinSync 1.1.3 on your computer.
	It is recommended that you close all other applications before continuing.
	Click Next to continue, or Cancel to exit Setup.
	Next > Cancel

(2) 在开始菜单中打开"配置 WinSync"工具,填写允许连接的来源 IP 地址,多个地址时使用分号分隔。

图13 填写登录参数

船 WinSync	Config	×
允许的IP:	192. 168. 7. 72	
TCP 端口:	5156	
日志级别:	NO 👻	保存并退出
注意:多个	IP以分号(;)分隔	退出



配置管理员和密码保管员可以在工具下载页面获取 Winsync 工具。 需使用超级管理员权限安装,并确保 SecPath运维审计系统可以连接目标设备的 5156 端口。

- (3) 在开始菜单中点击"重启WinSync",重启后配置即可生效。若RDP设备改密仍不能与WinSync 连接成功,可参考章节 <u>4</u>1.进行静默安装WinSync工具。
- 图14 重启 WinSync

记事本 Wireshark	•	
PLSQL Developer		Administrator
E Internet Explorer	۲	—————————————————————————————————————
DNS		网络
 命令提示符 通 m m m m n 		 控制面板
SecureCRT 7.1	•	设备和打印机
SemoteApp 管理器		管理工具 ▶
重启WinSync		运行
·		Windows 安全
搜索程序和文件	2	注销▶
🏹 дана 🛃 🗾 🚞	1	O

(4) 使用配置管理员登录,打开[基本控制/目标设备],找到要改密的设备点击<密码管理>按钮。

图15 密码管理

基本招	空制 权限控制 -	密码控制 🗸 🛛 事件目	■计~ 统计报表~	工单管理 > 脚本任务	5~ 双人复核~				配置管理员	∽∣ admin ∽ ∣	?	
用户帧	长号 系统帐号 目标	市设备 用户分组	设备分组									
您的当	内当前位置: 基本控制 > 目标设备 已用数: 3, 可用数: 97											
新建	建 批量导入 批量修改 导出设备 状态: 活动 🕴 部门: ROOT 💠 系统类型: 所有设备类型 💠 重复IP: 🗘 过滤: 确定 共1页: <1> Go											
	<u>名称</u> ↓	部门	<u>IPt也址</u>	系统类型		字符终端	图形终端	文件传输	动作			
1	192.168.7.198	ROOT	192.168.7.198	Microsoft Windo	ws		rdp		编辑 密码管理 改密日	志		
2	2 192.168.770 系统组 192.168.770 General Linux ssh vnc sftp 编辑 宏铅管理 改密日志											
3	winsrv-2008	系统运维部	192.168.7.112	Microsoft Windo	ws		rdp		编辑密码管理改密日;	志	1	
											1	

(5) 托管特权账号 administrator 密码,并可以登录测试成功。

图16 登录测试

	▶ ● ● 运维审计系统 - 运维审计系统											
▲ 不安全 Https://192.168.7.72/manager/server_edit_index.php?tab=2&id=3&nomenu=1												
设备约	设备编辑:winsrv-2008(192.168.7.112) 服务列表 密码管理 分配设备组 访问规则 可登录用户											
登陆	登陆测试服务: rdp ◆ <u>新建系统帐号</u>											
系	统帐号	切换自	密码	提示符	自动运行	Domain	操作					
*	administrator		密码已设置				编辑 帐号改密 登录测试					
	any						新建					
	enable						新建					
	netscreen						新建					
	null						新建					
	root						新建					
	self						新建					
	super						新建					

(6) 打开[密码控制/改密计划],点击<新建计划>按钮,创建定期改密计划。

图17 创建定期改密计划

基本控制 ~	权限控制 ~	密码控制	事件审计~	统计报表 🗸	工单管理 ~	脚本任务~	双人复核~						
改密计划	设备改密日志							00000000					
您的当前位重	您的当前位置: 密码控制 > 改密计划 > 编辑												
计划名称: w 定期自动修	计划名称: <u>windows-plan</u> , 修改记录: <u>1</u> 条 定期自动修改												
计划名称:	计划名称: windows-plan *												
部门:	部门: 系统运维部 💠 *												
[-]任务	[-]任务执行												
任务时间:	00 \$: 00 :	•											
任务日期:	2018-02-02 温		次执行任务的日期	朝, 例如今天为	2018-02-01,留	空表示任务不会	生效)						
任务间隔:	每 3 \$ 个/	月或每	天,执行一次 ()	选填一项,月数。	与优)								
登录测试:	🗌 改密后执行,	仅用于改密结果	果参考										
[-]密码	策略												
设定: • 阳	前机生成不同密码	- ○自动设置	『相同密码 ○:	手动指定密码									
策略: • • 4	≧局 ○定制	01	0										
[-1改瘿	通知												
发送邮件:	 ☑ admin 缺省领	查理员											
ACCEPTT.	以下用户不可选	择[+]											
密码发送													
发送格式:	Otxt oxis												
[注意:必	须以下2种方式中	中选择一种密码	3发送方式]										
[+]邮	件发送												
[±1文	性服务器												
	ממ כל אמידוו												
确定删	除 清除 取消												

(7) 设置好的改密计划会按照预期时间进行修改,也可以通过手动方式立即执行。

图18 立即执行

基本技	空制 ~ 权限控制、	密码控制	事件审计~	统计报表~	工单管理~	脚本任务~	双人复核~		記 置管理员 🗸	admin 🗸	1 🕐 👻
改密计	十划 设备改密日志	i.									
您的当	当前位置: 密码控制	> 改密计划									
新建	计划 导出										
任务	名称	目标设备	f	系统帐号	上次	修改密码	距离下次修	改密码	动作		
1	windows-plan	winsrv-2	008	administrator	2018	-01-24 22:31	1 day after	the 00:00	编辑历史修改记录查看密码状态立即修改 关联: <u>设备组(0)设备(1)系统帐号(1)</u>		
3.5 备份密码到文件服务

(1) 使用超级管理员登录,打开[策略配置/设备密码],在密码备份规则中勾选"文件服务器"选项。

图19 备份密码到文件服务

基本控制 ~ 事件审计	十~ 策略配置	系统设置	✓ 工单管理 √	双人复核~						
系统策略 告警事件	字符终端	会话配置 身份	计验证 设备密	码 设备类型	部门配置	改密方式	密码代填	IE代填脚本		
您的当前位置: 策略	配置 > 设备密码									
一随机密码强度设定一										
随机密码长度:	8	*								
最少数字字符个数:	0	*								
最少大写字母个数:	0	*								
最少小写字母个数:	0	*								
最少其他字符个数:	0	*								
(设备随机密码强度配置,可作为设备改密的全局密码策略)										
- 全局改密通知										
以下用户不可选择[+]										
(邮件将通知所有设备改密事件,包括执行改密计划及手工改密)										
密码备份规则										
允许: □本地磁盘										
☑ 文件服务器 (文件服务器在系统策略中配置)										
格式: xis \$										
(勾选允许的密码备份方式,相应功能于密码控制的密码备份模块中提供支持)										
确定 重设										

- (2) 使用密码保管员登录,打开[密码控制/密码备份],点击<上传全部密码>按钮,在弹出的窗口 中选择要上传的服务器即可。
- 图20 备份密码到文件服务

密码控制 工单管理 ~	双人复核 ~							密码保管员	•	admin 🗸
改密计划 设备改密日志	密码备份	手工改密								
您的当前位置: 密码控制 >	密码备份									
过滤: 🛟						E	专全部密码	下载未设置密码设备	共1页	< 1 >
名称↓		<u>IP地址</u>		系统类型	字符终端	图开	形终端	文件传输		动作
1 <u>192.168.7.198</u>		192.168.7.198		Microsoft Windows		rdp				密码管理
2 192.168.7.70		192.168.7.70		运维审计系统 - 运维审计系	系统		:	sftp		密码管理
3 <u>winsrv-2008</u>	winsrv-2008 192.168.7.112			https://192.168.7.72/srvpw_worker/h	packup_srvpw_de	ev_selec				密码管理
			请选择 文件 filesrv: C 备份	服务器						

4 常见问题

1. 如何静默安装Winsync工具

(1) 打开 CMD 工具,进入到 Winsync 存放路径。

图21 进入到 Winsync 存放路径

C:\>cd Download	
C:\Download>dir 驱动器 C 中的卷没有标签。 卷的序列号是 72BD-8344	
C:\Download 的目录	
2018/02/01 19:17 〈DIR〉 . 2018/02/01 19:17 〈DIR〉 . 2018/02/01 13:15 1,210,163 ¥inSync-1.1.3.e 1 个文件 1,210,163 子节 2 个目录 71,781,441,536 可用字节	xe
C:\Download>_	

(2) 输入静默安装命令,并指定来源地址。

图22 输入静默安装命令,并指定来源地址



(3) WinSync 静默安装到默认路径,并指定来源地址为 192.168.7.72。

图23 配置登录参数

🔠 WinSync (Config	X
	Free cost of the	
允许的IP:	192. 168. 7. 72	
TCP 端口:	5156	
日志级别:	NO 🔻	仅在并退中
注意:多个:	LP以分号(;)分隔	退出

₩ 提示

安装时指定参数 /verysilent 为静默安装, /allow_ip=ip;ip;ip 则可指定允许连接的来源地址, 多个地 址用分号隔开。