



极地运维审计系统

快速使用手册

北京市海淀区安宁庄西路9号院金泰富地大厦
1203

电话：010 - 62659336

传真：010 - 62522762

邮编：100191

网站：www.jidisec.com

■ 版权声明

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属北京极地所有，受到有关产权及版权法保护。任何个人、机构未经北京极地的书面授权许可，不得以任何方式复制或引用本文的任何内容。

■ 版本变更记录

时间	版本	说明	修改人
2017.02.23	V1.1	重建	褚亚东

■ 适用性声明

文档用于撰写北京极地公司产品介绍、项目方案、解决方案、商业计划书等。

目录

一. 前言.....	1
1.1 文档目的.....	1
1.2 阅读对象.....	1
1.3 文档结构.....	1
1.4 格式约定.....	1
1.5 技术支持.....	2
1.6 意见反馈.....	3
二. 初始化配置.....	3
2.1 部署结构.....	3
2.2 系统初始化登录步骤.....	4
(2) 为 PC 配置 IP 地址, 保证能与设备互通.....	5
(3) 启动浏览器, 输入登录信息.....	5
三. 功能详解.....	8
3.1 登录首页.....	8
3.2 单点登录.....	17
3.2.1 单点登录控件下载安装.....	19
3.3 资源管理.....	8
3.3.1 添加资源.....	9
3.4 授权管理.....	13
3.4.1 添加授权规则.....	14
3.5 审计管理.....	17
3.5.1 内部审计.....	22
3.5.2 实时监控.....	23
3.5.3 实时阻断.....	24
3.5.4 内容审计.....	24
3.5.5 指令审计.....	25
3.5.6 录像回放.....	26
四. 进阶功能.....	27
4.1 发布服务器的配置及使用.....	27
4.2 数据库资源的配置.....	29
4.3 WEB 应用资源的配置.....	34
4.4 网络设备资源的配置.....	35

图目

图 1 逻辑部署	3
图 2 物理部署	4
图 3 管理连线	5
图 4 pc 网络配置	5
图 5 可信站点	6
图 6 可信站点区	6
图 7 可信站点安全配置	7
图 8 安全证书提示，采用安全协议 HTTPS，弹出此告警属于正常现象	7
图 9 登录页	8
图 40 资源管理页	9
图 42 添加资源	10
图 43 资源从账号	12
图 20 单点登录首页	19
图 22 单点控件安装	20

极地安全 内网版

一. 前言

欢迎使用极地运维审计系统 JOAS，本用户使用手册主要介绍极地运维审计系统 JOAS 部署结构、配置、使用和管理。通过阅读本文档，用户可以了解极地运维审计系统 JOAS 的基本设计思想，配置和使用方法。在安装、使用极地运维审计系统 JOAS 之前，请仔细阅读文档内容。

1.1 文档目的

本文档主要介绍如何快速配置和使用极地运维审计系统 JOAS。通过阅读本文档，用户能够正确地部署和配置极地运维审计系统 JOAS。

1.2 阅读对象

本安装手册适用于具有基本网络知识的系统管理员、运维工程师阅读，通过阅读本文档，他们可以独立完成以下一些工作：

- 极地运维审计系统 JOAS 的功能使用。
- 极地运维审计系统 JOAS 的基本策略配置与管理。

1.3 文档结构

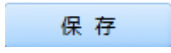
本文档包括以下章节及其主要内容：

- 前言，介绍了本手册各章节的基本内容、文档和技术支持信息。
- 安装指南，指导运维人员对设备进行上架及安装的注意事项。
- 初始化配置，介绍极地运维审计系统 JOAS 的部署结构和登录方法。
- 功能详解，详细介绍极地运维审计系统 JOAS 的功能。

1.4 格式约定

图形界面格式约定

文字描述	代替符合	举例
------	------	----

按钮	文字	 简化为【保存】按钮
导航栏	『 』	导航栏“系统设置”可简化为『系统设置』
连续选择导航栏及子菜单项	→	选择『系统设置』→『接口配置』
下拉框、单选框、复选框选项	[]	复选框选项“启用用户”可简化为[启用用户]
窗口名	【 】	如点击弹出【新增用户】窗口
提示信息	“ ”	提示框中显示“保存配置成功，配置已修改，需要重启 DLAN 服务才能生效，是否立即重启该服务？”

各类标志

文档中出现的注意、提示、说明例等，是关于用户在安装和配置堡垒机系统过程中需要特别注意的部分，其主要含义如下所述。请用户在明确可能的操作结果后，再进行相关配置。



注意

注意：提醒操作中应注意的事项，不当的操作可能会导致设置无法生效、数据丢失或者设备损坏。



提示

提示：一般为系统中不可更改的内容，提示用户操作避免出错。



说明

说明：对操作内容的描述进行必要的补充和说明。

1.5 技术支持

北京极地公司对于生产的安全产品提供远程的产品咨询服务，广大用户和合作伙伴可以通过多种方式获取在线文档、疑难解答等全方位的技术支持。

公司主页 www.jidisecc.com 提供交互网络服务，用户及合作伙伴可以在世界的任何地方，任何时候访问 www.jidisecc.com 技术支持中心，获取实时的网络安全解决方案、安全服务和各种安全资料。

传真：010 - 62522762

1.6 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：

电话：010 - 62659336

Email: sale@jidisec.com

感谢您的反馈，让我们做得更好。

二. 初始化配置

极地运维审计系统 JOAS 是极地安全内控解决方案的重要组成部分，部署在企业的内部网络中，用于保护企业内部核心资源的访问安全。使得企业内部网络管理合理化，专业化，信息化。

2.1 部署结构

极地运维审计系统 JOAS 部署逻辑图：

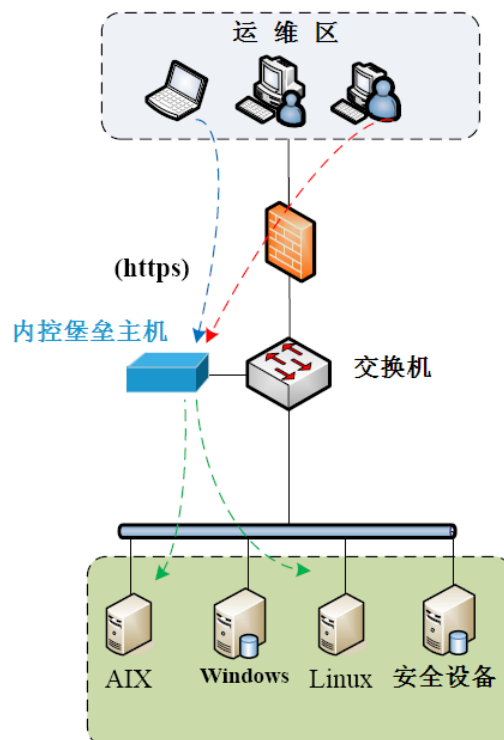


图 1 逻辑部署

极地运维审计系统 JOAS 部署物理图：

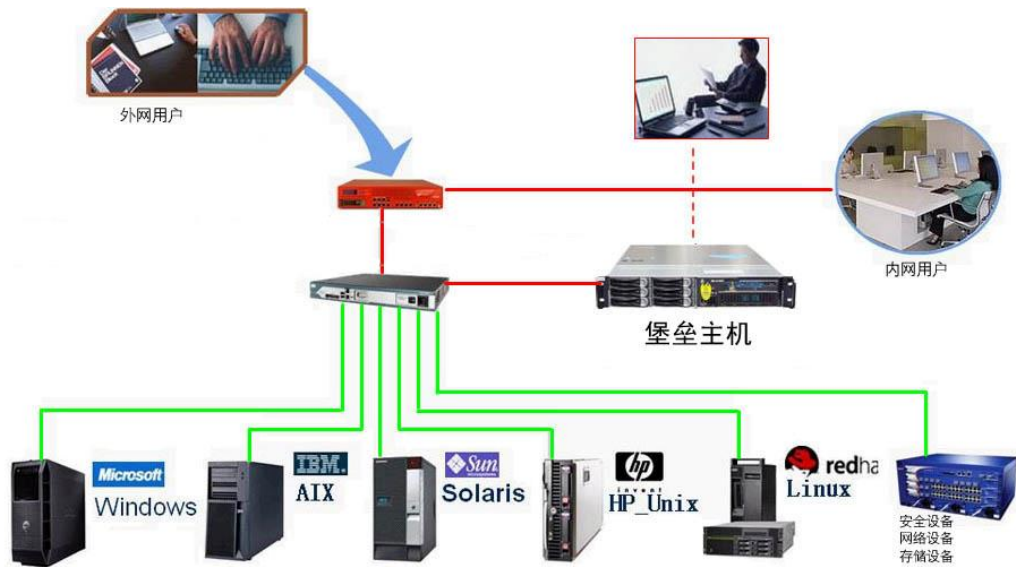


图 2 物理部署

如图，极地运维审计系统 JOAS 部署在被管服务器区的访问路径上。

极地运维审计系统 JOAS 接入用户网络中的方式为旁路部署，仅需要为系统分配一个 IP 地址，并确保该地址与需要运维的服务器路由可达，协议可访问。

2.2 系统初始化登录步骤

极地运维审计系统 JOAS 支持安全的 HTTPS 登陆，使用的是 HTTPS 协议的标准端口登陆。



说明

HTTPS 登录 WEB 界面管理 极地运维审计系统 JOAS 可以防止配置过程在传输过程中被截获而产生的安全隐患。

(1) 设备接通电源，连接设备和 PC

用交叉以太网线将 PC 和设备管理口 LAN1 相连。

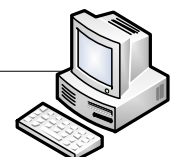
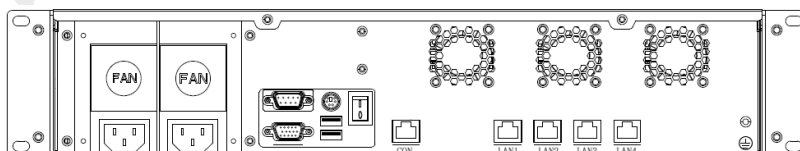


图 3 管理连线

(2) 为 PC 配置 IP 地址，保证能与设备互通

修改 PC 机的 IP 地址为 192.168.1.0/24 (除 LAN1 口地址)，例如 192.168.1.2。

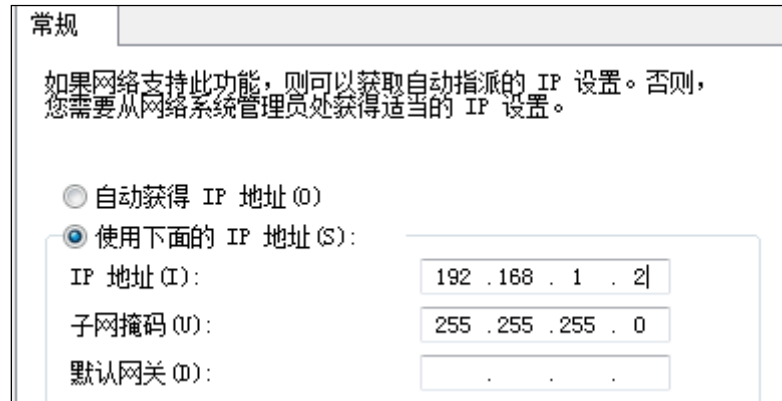


图 4 pc 网络配置

(3) 启动浏览器，输入登录信息

在 PC 上启动 IE 浏览器，在地址栏中输入 LAN1 口地址，点击【enter】按钮，即可进入堡垒主机登录页面。输入默认管理员，密码及验证码。点击【登录系统】按钮可进入系统进行管理操作。

 说明

1. 这里的 PC 是进行设备初始化配置时使用的 PC，不一定是内网管理终端。
2. 极地运维审计系统 JOAS 首次启用后，应及时修改口令，以免被非法登录。
3. 如维护工作站的浏览器软件为 IE，需要在其【Internet 选项】中把极地运维审计系统 JOASWEB 访问地址加入【可信站点】，并把【信任站点】的安全级别设为【低级】。

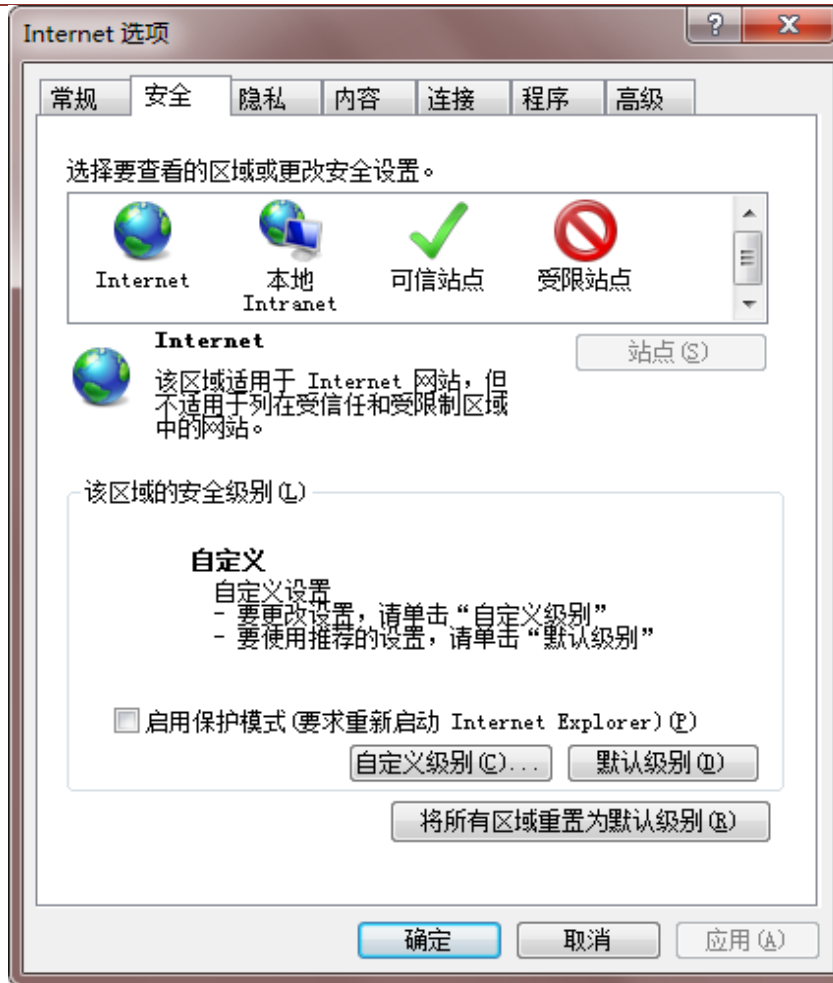


图 5 可信站点

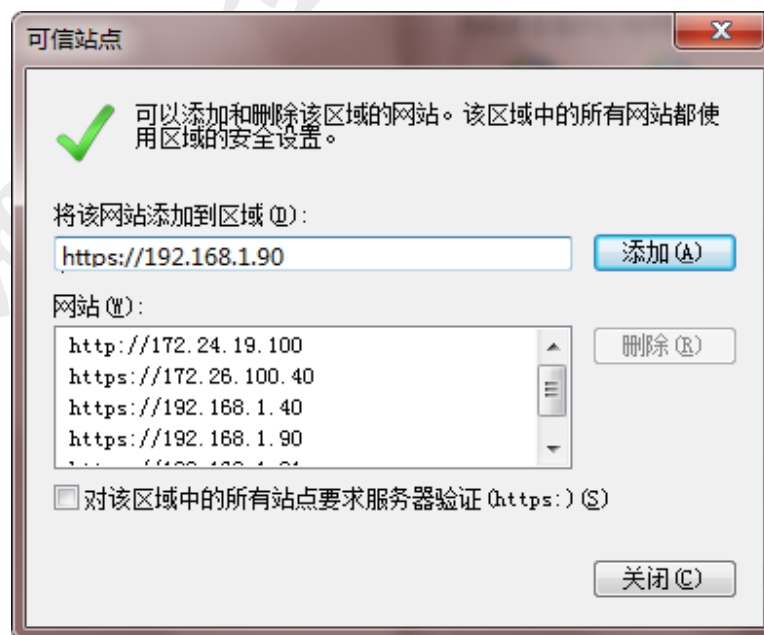


图 6 可信站点区

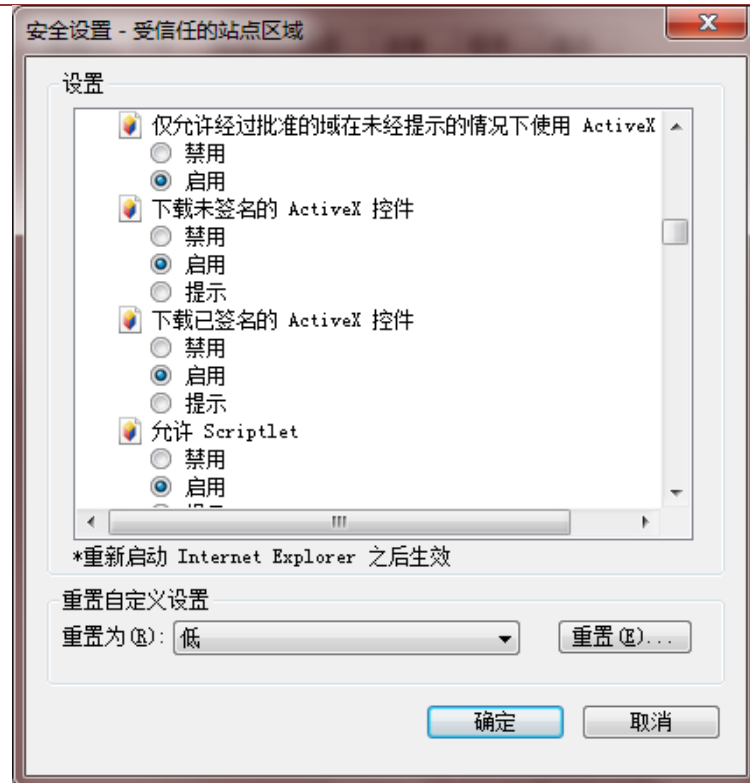


图 7 可信站点安全配置

4. 在地址栏输入 LAN1 口地址后，会出现安全证书告警画面，点击【继续浏览此网站】进入极地运维审计系统 JOAS 登录页面。



图 8 安全证书提示，采用安全协议 HTTPS，弹出此告警属于正常现象

三. 功能详解

3.1 登录首页



北京极地信息技术有限公司
© 2005 - 2017 Beijing Jidi Information Tech Co., Ltd. All rights reserved.

图 9 登录页

设备缺省信息

访问地址:

https://192.168.1.90

系统管理员权限:

admin

admin123



为向下兼容性问题，默认使用 IE9 以上内核的浏览器。火狐及部分安全性较高的浏览器访问页面需要调整后台源码文件(调整后无法兼容 IE)。

3.2 资源管理

资源管理就是要通过极地运维审计系统 JOAS 管理的各种设备资源，资源管理实现被管资

源的管理和被管资源的帐号管理。

【操作描述】

点击导航栏『资源管理』，进入资源管理界面。

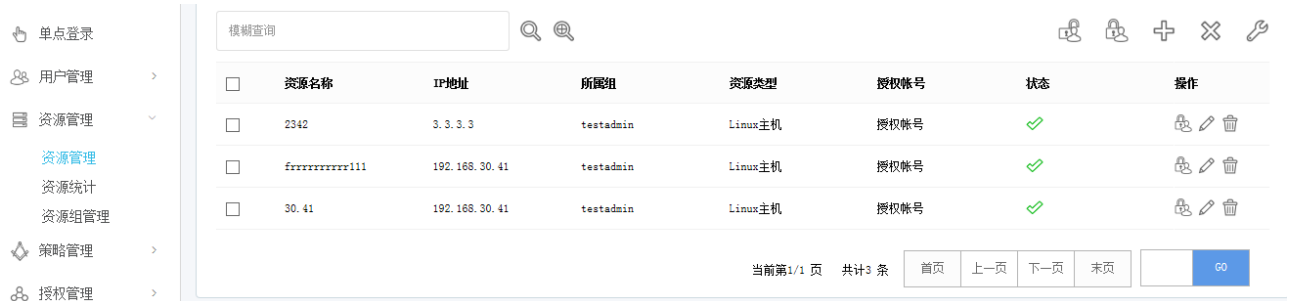


图 10 资源管理页

3.2.1 添加资源

点击【添加资源】按钮，进入资源添加界面。

资源信息①：输入添加的服务器资源名称、服务器类型及服务器 IP 地址；

资源信息

*资源名称:

*资源类型:

操作系统:

*资源IP:

*连接IP:

会话超时(秒):

连接超时(毫秒):

状态: 激活

所属组:

备注: 最多输入 300 个字符

配置选项 ▼ 保存 取消

图 11 添加资源

资源信息②：可以为资源加入所属组。

状态: 激活

所属组: H3c交换机

点击『所属组』输入框栏，出现所属组页面。

资源组选择 ×

- ▾ 路由交换机
 - ▾ H3c交换机
 - ▾ 华为交换机

确定 取消

选择相应的所属组，点击【确定】。

资源信息③：在『授权端口』栏中，勾选服务器开放的服务，并填写对应的端口，最后点击对应端口的“ ”按钮，测试数据连通性。

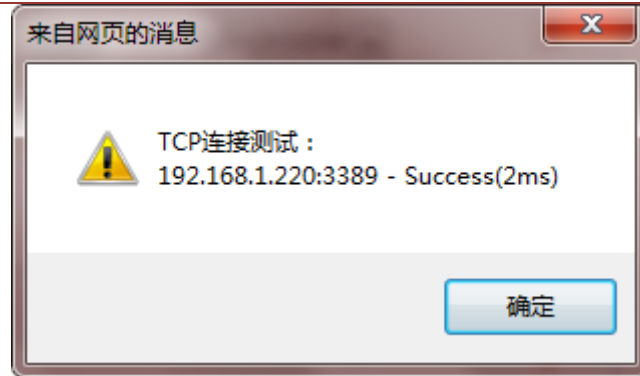
授权端口配置

<input checked="" type="checkbox"/>	RDP	端口	<input type="text" value="3389"/>			
<input type="checkbox"/>	SFTP_SCAN					
<input type="checkbox"/>	FTP_SCAN					
<input type="checkbox"/>	FTP	端口	<input type="text" value="21"/>			
<input type="checkbox"/>	VNC	端口	<input type="text" value="5900"/>			
<input type="checkbox"/>	X11	端口	<input type="text" value="177"/>			
<input type="checkbox"/>	RLOAIN	端口	<input type="text"/>			
<input type="checkbox"/>	SSH/SFTP	端口	<input type="text" value="22"/>	连接器	<input type="text" value="Linux服务器OS"/>	
		特权指令	<input type="text"/>	密码	<input type="text"/>	
<input type="checkbox"/>	TELNET	端口	<input type="text" value="23"/>	连接器	<input type="text" value="Linux服务器OS"/>	
		特权指令	<input type="text"/>	密码	<input type="text"/>	

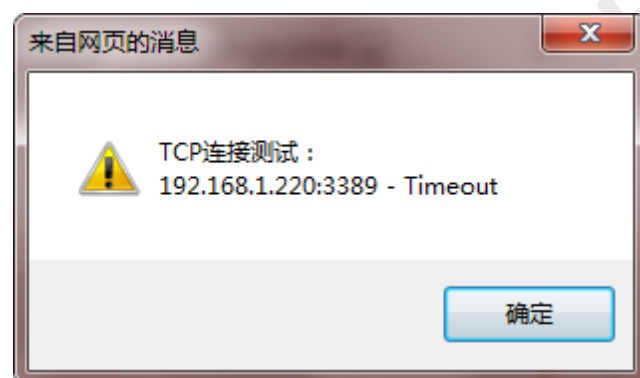
配置选项 ▼ 保存 取消



当点击连通性测试按钮“”后，会弹出测试结果窗口。当弹出窗口显示 Success 时，表示极地运维审计系统 JOAS 能够正常访问目标服务器；



当窗口显示 Timeout 时，表示堡垒主机无法访问目标服务器端口，请排查网络中是否存在访问控制策略。



资源信息④：添加资源管理员账号，资源管理员账号为服务器系统内部的管理员账号，它与计划任务模块相关联，具体介绍请见 1.12 的计划任务模块。

资源信息⑤：添加资源从账号，资源从账号为服务器系统内部的账号。

点击『资源从账号栏』→【添加】按钮，添加资源从账号。



图 12 资源从账号

在弹出的【新建资源从账号】上填写资源服务器系统内部的账号及密码，点击【确定】保存设置。

新建资源从账号

帐号组:

帐号:

使用空账号 随机密码

密码:

确认密码: 

密码策略:

完成以上基本信息填写后，点击界面下方的【保存】按钮，保存服务器资源。

模糊查询      

<input type="checkbox"/>	资源名称	IP地址	所属组	资源类型	授权帐号	状态	操作
<input type="checkbox"/>	Linux14	192.168.16.123		Unix主机	授权帐号	✓	  
<input type="checkbox"/>	Linux15	192.168.16.124		网络设备(Radius)	授权帐号	✓	  
<input type="checkbox"/>	Linux16	192.168.16.125		Unix主机	授权帐号	✓	  
<input type="checkbox"/>	Linux17	192.168.16.126		Unix主机	授权帐号	✓	  
<input type="checkbox"/>	Linux18	192.168.16.127		Unix主机	授权帐号	✓	  
<input type="checkbox"/>	Linux19	192.168.16.128		Linux主机	授权帐号	✓	  
<input type="checkbox"/>	Linux20	192.168.16.129		网络设备(Local)	授权帐号	✓	  

3.3 授权管理

授权管理是对给用户或用户组进行资源的授权，资源账号的授权，访问资源协议的授权，并且可以关联相关的策略进行访问资源限制。

【操作描述】

点击导航栏『授权管理』，进入授权管理页面。

规则名称	状态	授权用户/用户组	授权资源/资源组	关联策略	创建时间	修改时间	操作
testggddddd	✔	查看授权用户/用户组	查看授权资源/资源组	查看关联策略	2017-02-09 16:59:19	2017-02-10 14:34:04	
test666	✔	查看授权用户/用户组	查看授权资源/资源组	查看关联策略	2017-02-10 14:09:56	2017-02-10 14:26:48	
sfadfaefasfadsf	✔	查看授权用户/用户组	查看授权资源/资源组	查看关联策略	2017-02-09 15:55:45	2017-02-09 15:55:45	
erer	✔	查看授权用户/用户组	查看授权资源/资源组	查看关联策略	2017-02-09 15:48:25	2017-02-09 15:48:25	
test	✔	查看授权用户/用户组	查看授权资源/资源组	查看关联策略	2017-01-18 11:00:45	2017-02-06 10:33:11	
lkk	✔	查看授权用户/用户组	查看授权资源/资源组	查看关联策略	2017-01-24 18:17:36	2017-01-24 18:17:36	
30_41	✔	查看授权用户/用户组	查看授权资源/资源组	查看关联策略	2017-01-24 14:39:26	2017-01-24 14:39:26	
191	✔	查看授权用户/用户组	查看授权资源/资源组	查看关联策略	2017-01-24 10:54:39	2017-01-24 14:30:15	
test160	✔	查看授权用户/用户组	查看授权资源/资源组	查看关联策略	2017-01-24 14:14:11	2017-01-24 14:14:11	
阔213qqqqqqqqqqqq	✔	查看授权用户/用户组	查看授权资源/资源组	查看关联策略	2017-01-24 11:22:32	2017-01-24 11:22:32	

3.3.1 添加授权规则

点击【添加规则】按钮，进入添加规则界面。

授权规则信息

规则名称:

备注: 规则名称

授权用户: 用户、用户组

授权用户组:

选择策略:

资源:

资源信息: RDP SSH/SFTP SFTP_SCAN TELNET FTP FTP_SCAN X11 VNC WEB TOTALCMD DB RLOGIN 剪切板 磁盘映射 自动 操作

授权资源组: 资源、资源组

资源组信息: RDP SSH/SFTP SFTP_SCAN TELNET FTP FTP_SCAN X11 VNC WEB TOTALCMD DB RLOGIN 剪切板 磁盘映射 自动 操作

- 规则信息①：输入授权规则的规则名。

授权规则信息

规则名称: ✕

备注:

- 规则信息②：授权用户/用户组信息，点击【选择】按钮，在弹出窗口点选要授权的用户/用户组，点击【确定】按钮保存。

选择授权人员

- ▶ 所有用户
- ▶ 未分组
- ◀ 测试
 - ◀ 测试2
 - ◀ 测试3
 - ◀ test

🔍

	用户名称	角色
<input type="checkbox"/>	s(s)	系统管理员
<input type="checkbox"/>	测试1(ces)	密码管理员
<input type="checkbox"/>	用户组(yonghu)	密码管理员
<input type="checkbox"/>	用户组1(123123)	密码管理员
<input type="checkbox"/>	时间(shijian)	密码管理员

- 规则信息③：资源信息下点击【选择】按钮，授权资源为『文档工作站』，同时将文档工作站的从账户和关联协议进行授权，点击【确定】按钮保存。

选择授权资源

- ▶ 所有资源
- ▶ 未分组
- ◀ 测试测试
 - ◀ test
 - ◀ fefsa
 - ◀ cesces1
 - ◀ 分为
 - ◀

🔍

	资源名称	IP地址
<input type="checkbox"/>	Linux555	192.168.161.123
<input type="checkbox"/>	Linux556	192.168.161.124
<input type="checkbox"/>	Linux557	192.168.161.125
<input type="checkbox"/>	Linux558	192.168.161.126
<input type="checkbox"/>	Linux559	192.168.161.127

- 规则信息④：策略信息下点击【选择】按钮，授权资源为『禁止使用的命令（禁止）』，

点击【确定】按钮保存。

选择策略sss >

🔍
添加策略

<input type="checkbox"/> 允许策略名称	
<input type="checkbox"/> 测试	🗑️
<input type="checkbox"/> erer	🗑️
<input type="checkbox"/> 8888	🗑️
<input type="checkbox"/> asda	🗑️
<input type="checkbox"/> 白名单	🗑️

共6条记录
|
首页
|
上一页
|
下一页
|
末页
|

GO
当前第1/2页

<input type="checkbox"/> 禁止策略名称	
<input type="checkbox"/> eeeeeeeeeee	🗑️
<input type="checkbox"/> wew	🗑️
<input type="checkbox"/> 999	🗑️

授权规则完成后，就有使用该授权资源的权限。

<input type="checkbox"/>	191	✔️	查看授权用户/用户组	查看授权资源/资源组	查看关联策略	2017-01-24 10:54:39	2017-01-24 14:30:15	🗑️ ✎️
<input type="checkbox"/>	191(192.168.1.92)		测试测试	Windows主机	自动登录	root 0		✔️ 🗑️

说明

在使用授权用户组/授权资源组功能时，要给该用户分配一个具有用户组/资源组功能的角色。

角色名称:	<input type="text" value="汉字 字母 数字 下划线等非包含\ <>+*,?"/>	
角色描述:	<input type="text"/>	
用户/组:	<input type="text" value="已选择人员:"/> <input type="text"/>	<input type="text" value="已选择分组:"/> <input type="text"/>
	<input type="button" value="添加"/>	<input type="button" value="删除"/>
资源/组:	<input type="text" value="已选择资源:"/> <input type="text"/>	<input type="text" value="已选择分组:"/> <input type="text"/>
	<input type="button" value="添加"/>	<input type="button" value="删除"/>

3.4 负载均衡配置

添加万授权之后负载均衡配置，实现单点登录功能。

【操作描述】

点击『系统设置』→【网络设置】→【负载均衡设置】，点击添加按钮，进入应用发布服务器设置界面。



输入堡垒机



3.5 单点登录

单点登录功能能使用户在访问资源时使用各种授权资源。

【操作描述】

点击导航栏下『单点登录』，进入单点登录界面。资源名称列表中会显示所有授权给此用户的资源。

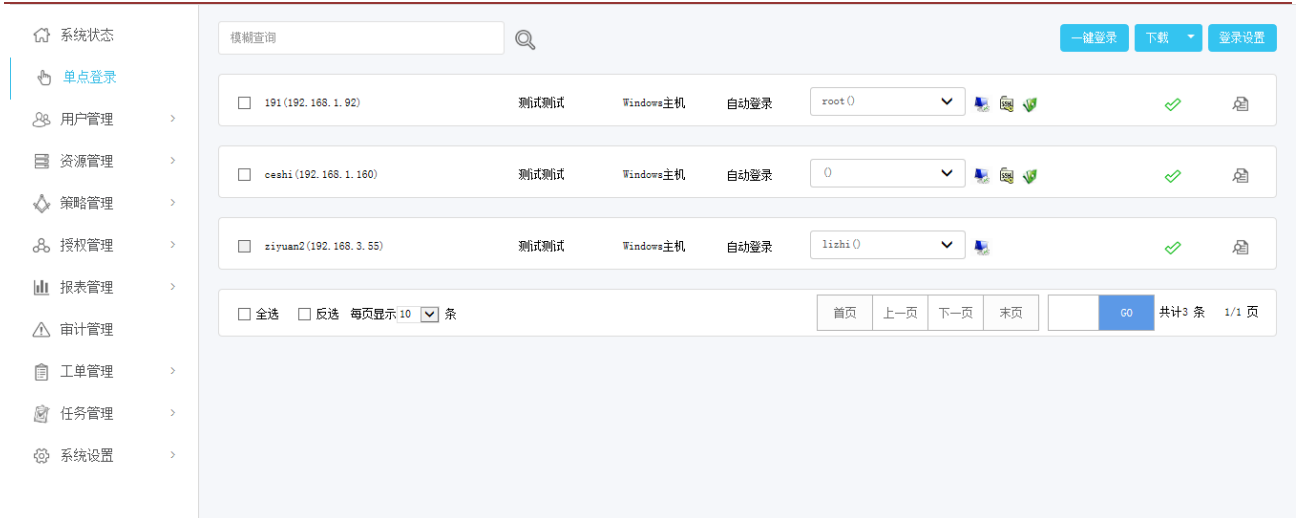


图 13 单点登录首页

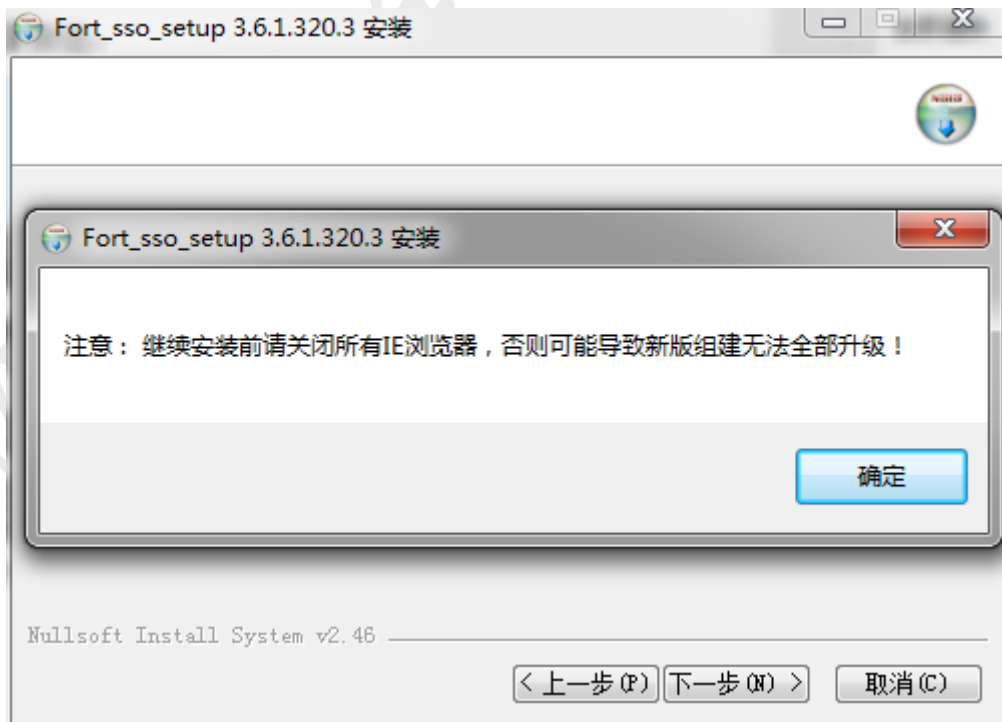
3.5.1 单点登录控件下载安装

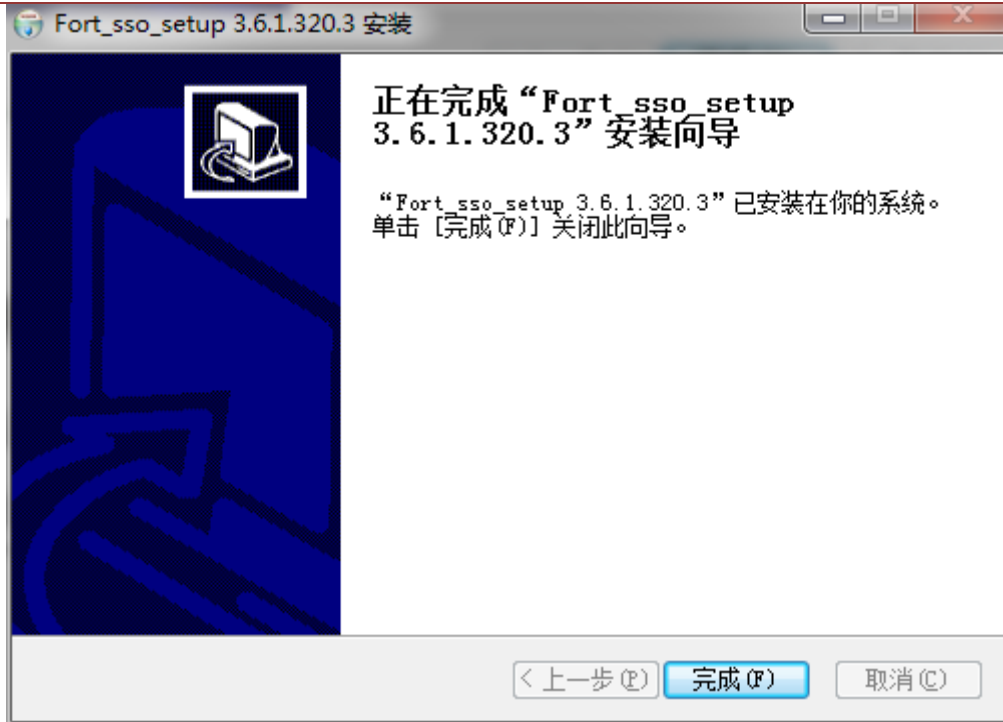
用户进行单点登录前必须在个人终端上安装单点登录控件，否则无法再堡垒机上进行单点登录。点击单点登录右上方【下载】按钮。





图 14 单点控件安装



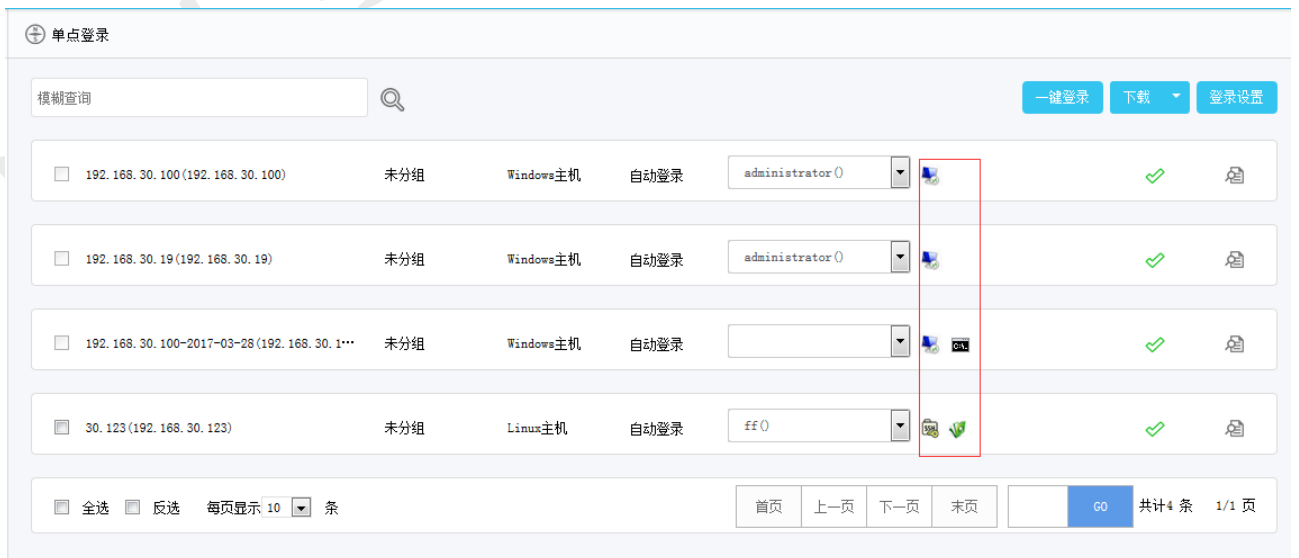


说明

控件安装过程中请用户将堡垒主机的登陆页面退出，否则会导致单点登录控件安装不成功。安装完成后用户即可进行单点登录操作。

3.5.2 单点登录

控件安装完成后可进行单点登录操作。



3.6 审计管理

极地运维审计系统 JOAS 提供的行为审计功能实现资源操作过程的实时监控及阻断。

【操作描述】

点击导航栏『审计管理』，进入审计管理界面。



3.6.1 内部审计

内部审计实现极地运维审计系统 JOAS 自身日志的审计，可以点击查询查找符合条件的审计记录。审计内容包括，帐号登入登出的情况，资源变更，用户变更等情况。管理员还可以通过导出内部审计记录按时间段对审计结果进行备份。

<input type="checkbox"/>	登录名	源IP	操作时间	操作日志	操作类型
<input type="checkbox"/>	admin	192.168.3.43	2017-02-15 10:12:04	操作日志	系统登录
<input type="checkbox"/>	lizhi	192.168.3.43	2017-02-15 09:49:47	操作日志	更新授权
<input type="checkbox"/>	lizhi	192.168.3.43	2017-02-15 08:27:37	操作日志	系统登录
<input type="checkbox"/>	lizhi	192.168.3.43	2017-02-15 08:27:31	操作日志	系统登录失败
<input type="checkbox"/>	admin	192.168.3.57	2017-02-14 19:35:17	操作日志	用户注销
<input type="checkbox"/>	ry	192.168.3.64	2017-02-14 19:29:16	操作日志	用户注销
<input type="checkbox"/>	ss	192.168.3.97	2017-02-14 19:15:16	操作日志	用户注销
<input type="checkbox"/>	admin	192.168.3.57	2017-02-14 18:34:14	操作日志	系统登录

点击右上角的【导出】，可导出审计信息。

在线 登录历史 内部审计 模糊查询 导出

登录名	源IP	操作时间	操作日志	操作类型
admin	192.168.3.43	2017-02-15 10:12:04	操作日志	系统登录
lizhi	192.168.3.43	2017-02-15 09:49:47	操作日志	更新授权
lizhi	192.168.3.43	2017-02-15 08:27:37	操作日志	系统登录
lizhi	192.168.3.43	2017-02-15 08:27:31	操作日志	系统登录失败
admin	192.168.3.57	2017-02-14 19:35:17	操作日志	用户注销
ry	192.168.3.64	2017-02-14 19:29:16	操作日志	用户注销

内部审计Excel报表(20170215)

编号	用户	源IP	操作	操作时间	操作内容
1	admin	192.168.3.102	系统登录	2017-01-16 19:12:40	admin(admin)
2	admin	192.168.3.102	系统登录	2017-01-16 19:31:22	admin(admin)
3	admin	192.168.3.102	用户注销	2017-01-16 20:16:27	用户admin注销系统!
4	admin	192.168.3.102	系统登录	2017-01-16 20:16:35	admin(admin)
5	admin	192.168.3.102	添加指令字对象	2017-01-16 20:42:55	对象名称: 123 指令字: 123
6	admin	192.168.3.102	新增禁止/允许策略	2017-01-16 20:43:05	允许/禁止策略: 123 状态: 启用 备注: 类型: 允许
7	admin	192.168.3.102	新增禁止/允许策略	2017-01-16 20:43:17	允许/禁止策略: 123123 状态: 启用 备注: 类型: 禁止

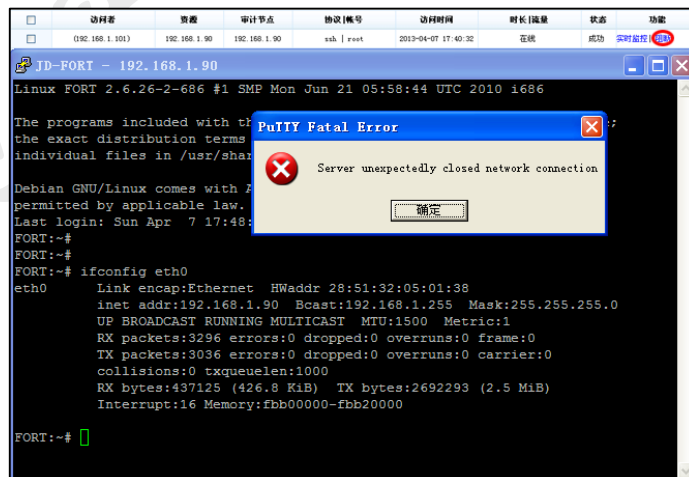
3.6.2 实时监控

点击导航栏『审计管理』→【行为审计】，如果操作人员对资源的操作还没有结束，则审计记录上会多出一种监视的展现方式，点击【实时监控】可以实时查看资源使用者对资源的操作过程。



3.6.3 实时阻断

点击导航栏『审计管理』→【行为审计】，如果操作人员对资源的操作还没有结束，则审计记录上还会多出一种阻断的展现方式，点击【阻断】按钮可以实现阻断资源使用者对资源的操作。



3.6.4 内容审计

当审计协议为命令行系统时，行为审计为用户提供内容审计功能。点击审计的条目的右

方【内容】按钮，查看该审计条目在命令行下出现过哪些内容。



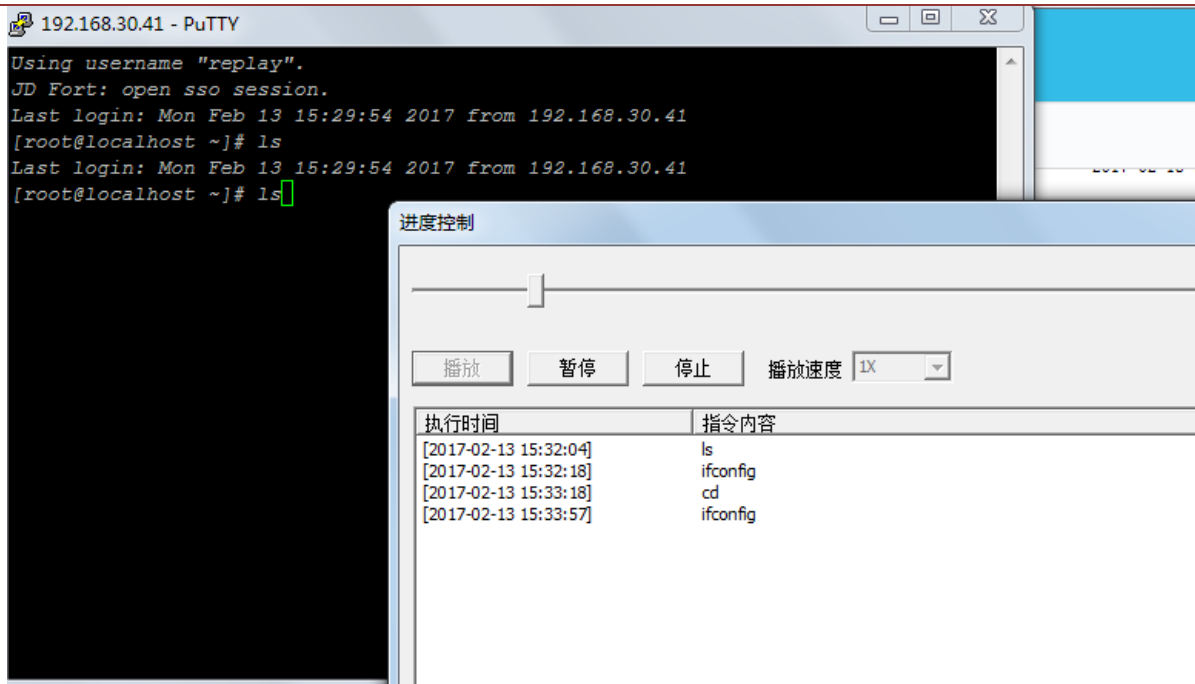
3.6.5 指令审计

当审计协议为命令行系统时，行为审计为用户提供指令审计功能。点击审计的条目的右方【指令】按钮，能查看该用户在该资源下敲打过哪些命令。



3.6.6 录像回放

堡垒主机对每次的单点登录都会做出录屏的审计，审计管理员可以通过点击【回放】按钮，查看运维人员的整个运维过程。



四. 进阶功能

4.1 发布服务器的配置及使用

此功能需配搭极地发布服务器使用，堡垒机系统将在配置完毕后自动调度发布服务器上的 C/S 架构软件，进行单点登录的代填操作，并保持全程审计的功能。

【操作描述】

点击『系统设置』→【连接设置】→【应用发布服务器设置】按钮，进入应用发布服务器设置界面。

- 发布服务器配置
- 任务计划FTP外发
- SNMP设置
- Syslog配置
- 时间同步

应用发布服务器配置

应用发布服务器IP:

应用账号:

数据库客户端配置

oracle客户端:

plsql	<input type="text"/>	<input type="text"/>
toad	<input type="text"/>	<input type="text"/>
sqlplus	<input type="text"/>	<input type="text"/>

sqlServer客户端:

Mysql数据库配置:

IE浏览器配置:

chrome浏览器配置:

Firefox浏览器配置:

X11配置:

NetTerm配置:

用户可根据下表说明填入信息。

参数	说明
应用发布服务器 IP	设定应用发布服务器 IP 地址，如有多个则可点击添加多个

	IP 地址，右侧闪电图标用于测试连通性；
应用账号	设定用于登录发布服务器的应用账号，默认情况下为 administrator；
Oracle 数据库配置 (PLSQL)	可选项，当需要使用 PLSQL 登录数据库时，可在此处设定应用发布服务器中的 PLSQL 安装路径及监听端口；
Oracle 数据库配置 (TOAD)	可选项，当需要使用 TOAD 登录数据库时，可在此处设定应用发布服务器中的 TOAD 安装路径及监听端口；
Oracle 数据库配置 (SQL PLUS)	可选项，当需要使用 SQL *PLUS 登录数据库时，可在此处设定应用发布服务器中的 SQL *PLUS 安装路径及监听端口；
SQL Server 数据库配置	可选项，当需要使用 SQL Server Management Studio 登录数据库时，可在此处设定应用发布服务器中的 SQL Server Management Studio 安装路径；
Mysql 数据库配置	可选项，当需要使用 Mysql 登录数据库时，可在此处设定应用发布服务器中的 Mysql 安装路径；
DB2 数据库配置	可选项，当需要使用 DB2 登录数据库时，可在此处设定应用发布服务器中的 DB2 安装路径；
Sysbase 数据库配置	可选项，当需要使用 Sysbase 登录数据库时，可在此处设定应用发布服务器中的 Sysbase 安装路径；
IE 浏览器配置	必填项，需要使用 Web 网管的设备，需要在此处设定应用发布服务器 IE 浏览器安装路； 默认为 C:\Program Files (x86)\Internet Explorer\iexplore.exe；
X11 窗口系统配置	可选项，当需要使用 X11 登录时，可在此处设定应用发布服务器中的 X11 安装路径。

4.2 数据库资源的配置

堡垒机通过运行发布服务器打开相应的 C/S 架构软件对 oracle、mysql、sqlserver、sybase 等数据库资源的管理。

【操作描述】

① oracle 数据库配置：

点击『资源管理』→【添加资源】按钮，进入资源添加界面，在资源类型中选择数据库（独立）或数据库（系统），在操作系统中选择 oracle。

*资源名称:

*资源类型:

操作系统:

*资源IP:

*连接IP:

勾选转发审计，选择应用发布服务器的账号和 IP 地址。

转发审计:

应用发布服务器:

应用发布服务账号:

数据库信息

*数据库版本:

*端口:

*数据库服务:

*维护工具:

*登录方式:

备注:

数据库信息配置:

数据库版本	堡垒机提供有 10G 和 11G 两个版本。
端口	填写数据库相应的端口号。

数据库服务	填写建立的数据库名称。
维护工具	堡垒机提供有 PLSQL、TOAD 和 SQLPULS 三个维护工具。
登录方式	堡垒机提供有 Normal、SYSDBA 和 SYSOPER 三种登录方式

在【资源从账号】栏中填写数据库账号。

资源账号:

② sqlserver 数据库配置

点击『资源管理』→【添加资源】按钮，进入资源添加界面，在资源类型中选择数据库（独立）或数据库（系统），在操作系统中选择 sqlserver。

*资源名称:

*资源类型:

操作系统:

*资源IP:

*连接IP:

需要勾选转发审计，选择应用发布服务器账号和 IP 地址，在【数据库信息】栏中填写数据库的端口号以及登录方式。

转发审计:

应用发布服务器:

选择

应用发布服务账号:

选择

数据库信息

*端口:

1433

数据库实例:

*登录方式:

SQL Server 身份验证

备注:

最多输入300个字符



提示

登录方式提供有 SQL Server 身份验证和 windows 身份验证。

(1)SQL Server 身份验证，在【资源从账号】栏中填写数据库账号。

资源账号:

添加

编辑

删除

(2)windows 身份验证，在【资源从账号】栏中填写 windows 域控账号。

*从属域控:

选择

③ Mysql 和 sybase 数据库配置

点击『资源管理』→【添加资源】按钮，进入资源添加界面，在资源类型中选择数据库（独立）或数据库（系统），在操作系统中选择 Mysql 或 sybase。

*资源名称:

*资源类型:

操作系统:

*资源IP:

*连接IP:

这两个数据库只需要勾选转发审计、对应的端口和填写数据库账号就可以了。

转发审计:

应用发布服务器:

应用发布服务账号:

数据库信息

*端口:

备注:

资源账号:

添加

编辑

删除

4.3 WEB 应用资源的配置

用户能通过极地运维审计系统 JOAS 添加 Web 应用资源。

【操作描述】

选择导航栏的【资源管理】>【添加资源】，资源类型选择【web 应用】。

*资源名称:

汉字 字母 数字 下划线等非包含八[]*::|<>+,?*

*资源类型:

web应用

操作系统:

标准web资源

*URL地址:

如果勾选转发审计，选择应用发布服务器账号和 IP 地址，则在单点登录的时候，会通过发布服务器转发 WEB 资源。

转发审计:

应用发布服务器:

选择

应用发布服务账号:

选择

信息配置

资源账号:

添加

编辑

删除

WEB参数信息 | 参数个数:

账号表单:

密码表单:



注意

WEB 系统单点登录需要使用者分析对应 WEB 系统登录模块脚本，找到相关验证参数，包括：登录验证 URL 地址、用户名表单名称，密码表单名称、页面参数等所有信息。

4.4 网络设备资源的配置

用户能通过极地运维审计系统 JOAS 添加 Web 应用资源。

【操作描述】

选择导航栏的【资源管理】>【添加资源】，资源类型选择【网络设备应用】。

*资源名称:

汉字 字母 数字 下划线等非包含八〇"::|<>=,?*

*资源类型:

网络设备 (Local)

操作系统:

Cisco

*资源IP:

*连接IP:

选择相应的授权端口。

TELNET 端口 23 连接器

Linux服务器OS
 Unix服务器OS
 H3交换机OS
 Cisco交换机OS
 中兴交换机OS
 其他 OS

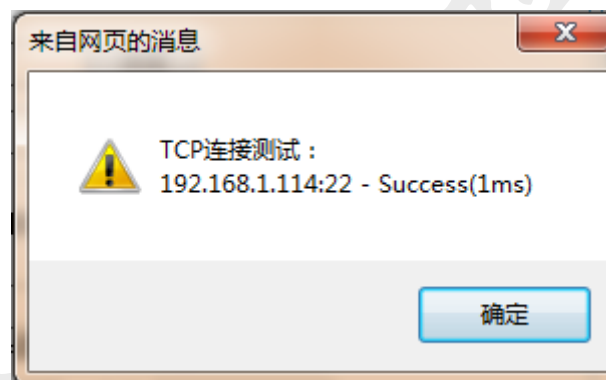
 特权指令 密码
⚡

输入特权指令和密码后，点击右边的闪电图标 ⚡，测试是否能连通。

TELNET 端口 23 连接器 Linux服务器OS

 特权指令 密码
⚡
连接测速

如果出现下图图标，说明设备已连通。



在资源从账号中选择空账号。

帐号组:

帐号:

使用空账号 随机密码

密码:

确认密码:

密码策略:

资源账号:

添加

编辑

删除

试拨

点击保存按钮。