ALIBABA CLOUD

阿里云

堡垒机

常见问题

文档版本：20220606

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.功能使用常见问题 ---------- 05

1.功能使用常见问题

本文介绍使用堡垒机时的常见问题及解决方案。

堡垒机通过不断地进行版本升级来提供更多的功能和更好的用户体验。堡垒机实例不同版本之间存在功能差异。更多信息，请参见版本说明。功能使用常见问题按照不同版本分为以下模块：

- **所有版本通用的常见问题**
  - 通过SSH方式运维登录堡垒机时，能否使用密钥作为认证方式？
  - 购买云盾堡垒机后，是否仍然能够直接连接ECS实例的IP？
  - 如果希望用户只能通过云盾堡垒机实例登录ECS进行运维，不允许以其他方式登录，应如何配置？
  - 登录堡垒机实例后，单击ECS实例进行登录时，提示失败，应该如何处理？
  - 使用WinSCP工具登录SFTP目标服务器时遇到“列出'/root'的目录项时出错”，应该如何处理？
  - 通过私钥方式登录云服务器ECS，仍然提示需要输入密码，该如何解决？
  - 堡垒机实例无法连接ECS云服务器，该如何解决？
  - 运维人员如何修改云盾堡垒机实例的登录密码？
  - 云盾堡垒机开放哪些端口，是否可以修改？
- **V3.2版本常见问题**
  - 堡垒机哪些版本的实例支持通过调用API接口使用主机、主机组、主机账户、用户、用户组和主机授权功能？
  - 如何将堡垒机的运维日志转存到日志服务（SLS）中？
  - 如何在ECS服务器的安全组中设置放行堡垒机出口IP的规则？
  - 在云盾堡垒机实例中，如何设置通过内网IP登录ECS服务器？
  - 目标ECS服务器使用的不是SSH、RDP等协议的标准端口，云盾堡垒机实例该如何配置？
  - 堡垒机实例中的审计录像能保存多久？
  - 使用RDP运维，如何切换主机？
  - 如何将服务器配置为HTTP和SOCKS5代理服务器？
- **V3.1版本常见问题**
  - 堡垒机本地用户的登录失败次数限制是否可以调整？
  - 子账号被锁定该如何处理？
  - 本地用户如何配置双因子认证？
  - 如何使用共享账号？
  - 金融云环境中如何登录堡垒机实例？例如，之前是要通过VPN访问服务器进行运维，将服务器接入堡垒机实例后是否仍需要通过VPN连接？
  - 登录堡垒机实例后，在一段时间内没有选择需要登录的ECS实例后自动断开，默认的超时时间是多久？是否支持自定义？
  - 在云盾堡垒机实例中，如何设置通过内网IP登录ECS服务器？
  - 堡垒机实例中的审计录像能保存多久？
  - 登录云盾堡垒机实例提示连接不安全？
- **V2版本常见问题**
  - 目前用于登录服务器的私钥是带有密码的，如何在凭据中输入私钥密码？

- 凭据是否必须是ECS服务器上的真实用户，还是创建凭据时堡垒机实例会自动在对应的ECS服务器中创建一个新用户？
- 系统管理员如何给不同运维人员配置不同主机的运维权限？
- 在云盾堡垒机实例中，如何设置通过内网IP登录ECS服务器？
- 目标ECS服务器使用的不是SSH、RDP等协议的标准端口，云盾堡垒机实例该如何配置？
- 堡垒机实例中的审计录像能保存多久？
- 登录云盾堡垒机实例提示连接不安全？

通过SSH方式运维登录堡垒机时，能否使用密钥作为认证方式？

可以。当使用SSH方式登录堡垒机60022端口时，您可以使用密钥或密码作为认证方式。

如何设置用户使用密钥登录堡垒机，具体操作，请参见托管用户公钥。

如何通过SSH方式登录堡垒机，具体操作，请参见：

- Windows系统：SSH协议运维
- Mac系统：SSH协议运维

购买云盾堡垒机后，是否仍然能够直接连接ECS实例的IP？

堡垒机实例本身对ECS实例的IP没有进行策略控制，如果您没有配置其他访问控制策略，仍然可以直接连接该ECS实例的IP。

> **说明** 为了保证您服务器运维的合规性及完整性，建议您配置相关访问控制策略，仅允许通过堡垒机实例登录ECS实例进行运维操作。配置访问策略，具体操作，请参见添加控制策略。

如果希望用户只能通过云盾堡垒机实例登录ECS进行运维，不允许以其他方式登录，应如何配置？

您可以通过设置该ECS实例的安全组，只允许堡垒机实例的IP访问该ECS实例；或者不要将服务器登录的凭据分发给用户，仅在堡垒机实例中保存登录凭据，实现用户只能通过堡垒机实例登录ECS云服务器。如何设置安全组，具体操作，请参见添加安全组规则。

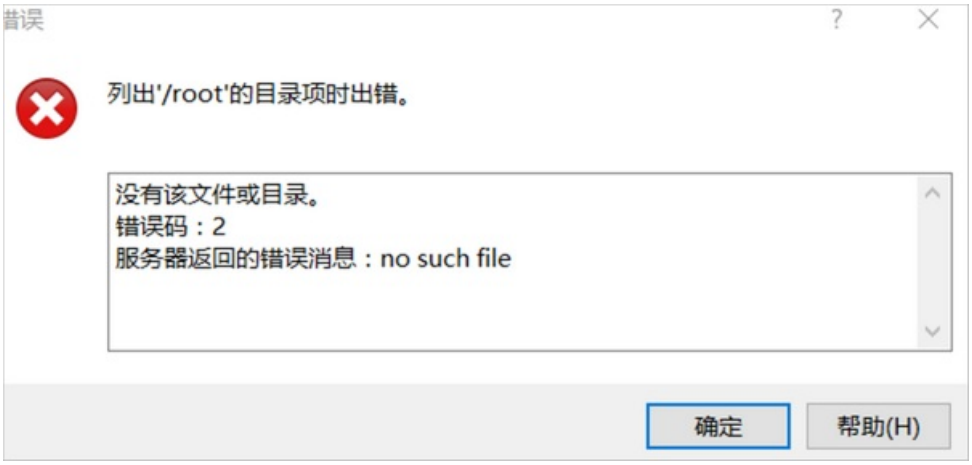
登录堡垒机实例后，单击ECS实例进行登录时，提示失败，应该如何处理？

请检查登录的ECS实例所在的安全组和ECS实例本身的防火墙设置，确认没有启用禁止堡垒机实例访问ECS服务器运维端口的任何访问控制规则。

使用WinSCP工具登录SFTP目标服务器时遇到“列出'/root'的目录项时出错”，应该如何处理？

问题现象

使用WinSCP工具登录SFTP目标服务器时遇到“列出'/root'的目录项时出错”，如下图所示：



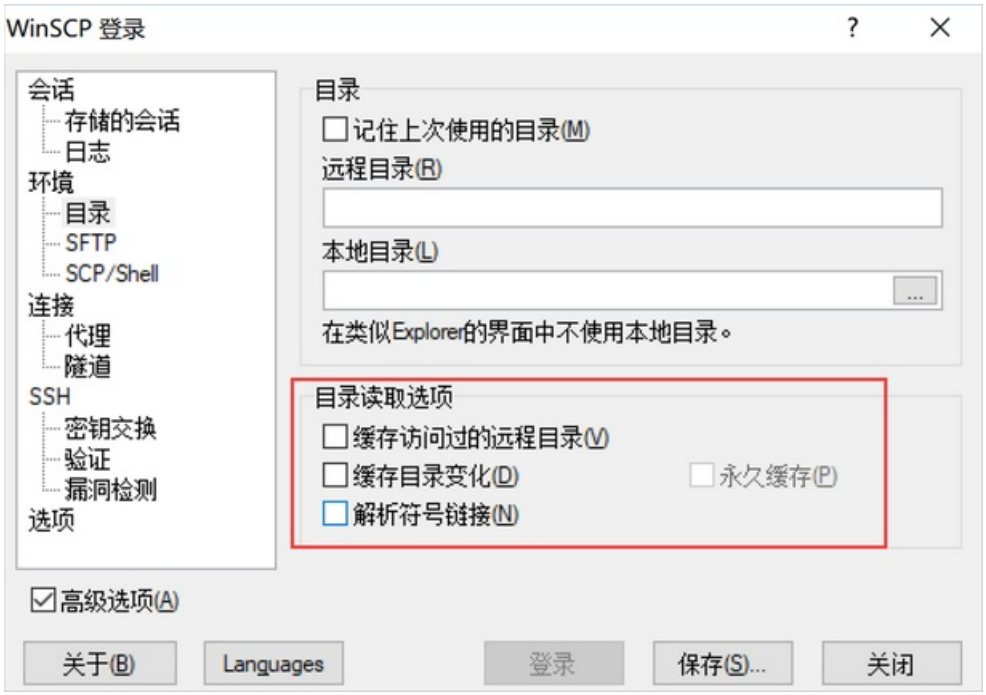
问题原因

可能是本地客户端存在缓存导致。

解决方案

您需要在WinSCP工具进行以下配置：

1. 打开WinSCP工具。
2. 在左侧导航栏，选择**环境 > 目录**。
3. 将**目录读取选项**全部取消选中。



4. 单击**保存**。
5. 在服务器列表中，单击目标服务器重新登录。

通过私钥方式登录云服务器ECS，仍然提示需要输入密码，该如何解决？

您需要通过以下方式进行排查：

1.确认您所添加的私钥类型。目前堡垒机实例仅支持通过ssh-keygen工具生成的RSA私钥（不支持带密码的私钥）登录ECS服务器。

2.确认所添加的授权组凭据是否正确。您可以通过使用私钥登录ECS云服务器的方式进行验证。

> **说明** 堡垒机版本不同，使用私钥登录ECS云服务器的方法也不同。请根据您堡垒机的版本，查看对应文档。
>
> - V3.1版本，请参见为帐户设置SSH私钥。
> - V3.2版本，请参见设置账户的私钥。

堡垒机实例无法连接ECS云服务器，该如何解决？

您需要通过以下方式进行排查：

- 确保堡垒机与ECS服务器之前的网络互通。如何检查堡垒机与ECS服务器之前网络互通，具体操作，请参见网络诊断。
- 检查目标ECS服务器的相关安全组规则设置是否正确，确保堡垒机实例可以连通ECS实例的相关运维端口。
- 检查ECS服务器自身防火墙或其他中间设备是否存在其它访问连接限制，例如iptables等。
- 检查堡垒机实例中访问该ECS服务器的端口信息，确保所添加的相关凭据信息（服务器的账户、密钥或密码）正确。

运维人员如何修改云盾堡垒机实例的登录密码？

您可以通过以下方式修改您的云盾堡垒机实例登录密码：

- 联系堡垒机实例管理员进行修改。
- 登录堡垒机实例后，自行修改您的登录密码。具体操作，请参见用户修改密码。

云盾堡垒机开放哪些端口，是否可以修改？

云盾堡垒机默认开放以下端口：

- 443（https端口，Web管理页面）
- 60022（SSH运维端口）
- 63389（RDP运维端口）

> **说明** V2和V3.1版本不支持修改系统默认端口。V3.2版本支持修改系统默认端口。1~1024为堡垒机保留端口，自定义端口时请不要修改为保留端口。

堡垒机哪些版本的实例支持通过调用API接口使用主机、主机组、主机账户、用户、用户组和主机授权功能？

堡垒机V3.2.17及以上版本支持。如果您的堡垒机实例为3.2.17及以上版本，您可以通过调用API接口使用堡垒机提供的主机、主机组、主机账户、用户、用户组和主机授权功能。以下是堡垒机支持的API类型：

- 主机（仅支持V3.2.17及以上版本使用）
- 主机组（仅支持V3.2.17及以上版本使用）
- 主机账户（仅支持V3.2.17及以上版本使用）
- 用户（仅支持V3.2.17及以上版本使用）
- 用户组（仅支持V3.2.17及以上版本使用）

- 主机授权（仅支持V3.2.17及以上版本使用）

如何将堡垒机的运维日志转存到日志服务（SLS）中？

堡垒机支持将运维日志转存到日志服务对应的Logstore中。运维日志即运维人员使用堡垒机进行运维的操作记录。您配置了运维日志转存，堡垒机在接收到运维记录后，会自动将运维日志转存到日志服务中。您可以参考以下步骤配置堡垒机运维日志转存：

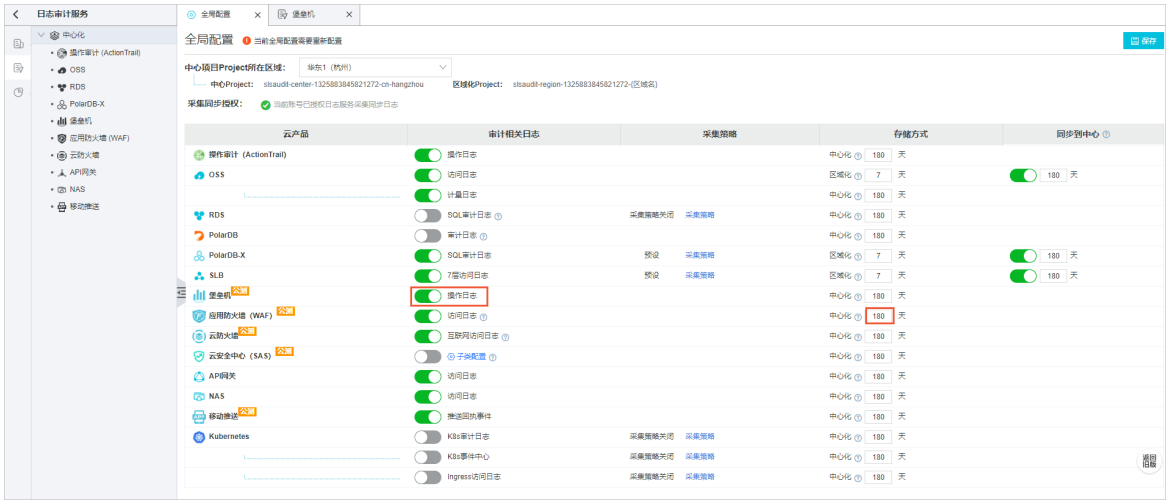
1. 登录日志服务控制台，并根据页面提示开通日志服务。
2. 在**日志应用**区域，单击**日志审计服务**。
3. 在**全局配置**页面，参考以下步骤配置审计信息。
   i. 在**中心项目Project所在区域**下拉列表中，选择日志中心化存储的目标地域。
   ii. 配置采集同步授权。

   日志审计服务支持手动授权和通过账号密钥辅助授权。您可以选择以下任一方式配置采集同步授权：

   - **通过账号密钥辅助授权**：输入账号的AccessKey和AccessSecret。

     AccessKey信息不会被保存，仅临时使用。此处AccessKey信息对应的RAM用户需具备RAM读写权限（例如已被授权AliyunRAMFullAccess策略）。
   - **手动授权**：具体操作，请参见自定义授权日志采集与同步。

   iii. 在云产品列表中，打开堡垒机**操作日志**开关并设置**存储方式**中的存储时间。



4. （可选）查看堡垒机运维日志。
   i. 在左侧导航栏，单击 图标。
   ii. 在左侧**中心化**菜单下单击**堡垒机**。
   iii. 在**堡垒机**页签下查看运维日志。

如何在ECS服务器的安全组中设置放行堡垒机出口IP的规则？

使用堡垒机对ECS服务器进行运维前，您需要在服务器的安全组中设置放行堡垒机的出口IP的规则。您的ECS服务器中配置了放行堡垒机出口IP的规则后，堡垒机才能和您的ECS服务器正常通信，进行运维审计操作。您可以执行以下步骤设置安全组规则：

1. 登录云盾堡垒机控制台。

2. 定位到进行运维操作的堡垒机实例，将鼠标移动到**出口IP**上方。

3. 复制并保存该堡垒机的公网IP地址和私网IP地址。
4. 在ECS服务器的安全组中设置放行堡垒机公网IP和私网IP的规则。

   设置安全组规则的具体操作，请参见添加安全组规则。

在云盾堡垒机实例中，如何设置通过内网IP登录ECS服务器？

您可以通过以下两种方式进行设置：

- 通过导入ECS实例方式导入的ECS服务器，默认是使用内网IP登录。更多信息，请参见导入阿里云ECS实例。
- 在**资产管理 > 主机**页面，选择需要修改运维连接IP的主机，并单击**批量 > 修改运维连接IP**。在**修改运维连接IP**对话框中，将**主机IP类型**选择为**内网IP**，并单击**确定**。

目标ECS服务器使用的不是SSH、RDP等协议的标准端口，云盾堡垒机实例该如何配置？

云盾堡垒机实例支持自定义运维端口，您可以在登录堡垒机实例后，在**资产管理 > 主机**页面，选择目标服务器，单击**批量 > 修改运维端口**。在**修改运维端口**页面，选择使用的协议并输入自定义的运维端口号，再单击**确定**。

堡垒机实例中的审计录像能保存多久？

V3.2版本堡垒机实例的审计录像一般可以保存半年以上，审计录像存储在OSS上，当堡垒机存储空间快满时，会自动清除最早的审计日志和录像。

> **说明** 云盾堡垒机实例直接保存运维协议的原始数据，根据流量不同所占用的空间大小也不同。

- SSH运维会话一般每天产生2 M左右日志数据。
- 远程桌面（RDP）运维会话（1024 * 768分辨率）一般每小时产生10 M左右日志数据。

堡垒机本地用户的登录失败次数限制是否可以调整？

是的。V3.1.X版本堡垒机本地用户可以自行设置登录失败次数限制。操作步骤如下：

1. 登录云盾堡垒机系统。
2. 在左侧导航栏，选择**系统 > 认证管理**。
3. 在**安全配置**页签下的**用户锁定**区域，修改**密码尝试次数**。

子账号被锁定该如何处理？

以下内容介绍了不同情况下，子账号被锁定的解决办法：

- 在1小时内，子账号的登录密码连续4次输入错误。此时，需要主账号在云盾堡垒机控制台的子账号管理页面，单击**解锁**为其解锁后，才能继续登录。
- 在15分钟内，子账号的MFA码连续4次输入错误。这种情况无法手动解锁，需要等待15分钟自动解锁。

本地用户如何配置双因子认证？

3.1.X版本中的双因子配置逻辑存在一些问题，后续版本会完善该配置。目前，请按照以下方式进行配置：

1. 登录云盾堡垒机实例。
2. 在左侧导航栏，选择**系统 > 认证管理**。
3. 单击**双因子认证**页签。
4. 在**双因子认证**页签下，配置认证方式。您可以选择以下认证方式：
   - 选中**短信口令**：开启密码和短信的双因子认证。

- 选中**密码**，或同时选中**密码**和**短信口令**：只开启密码认证，不开启双因子认证。

5. 单击**保存更改**。

如何使用共享账号？

堡垒机上托管的不同服务器有相同的主机账号时（账号名和密码都相同），您可以使用共享账号来简化管理。

创建共享账号后，选择绑定主机，即可将该账号添加到指定的服务器中。

已购买云盾堡垒机实例，为什么在控制台中的管理页面无法登录堡垒机实例？

无法登录可能是当前登录页面已过期，建议您刷新云盾堡垒机管理控制台页面后重新单击**管理**登录堡垒机实例。

金融云环境中如何登录堡垒机实例？例如，之前需要通过VPN访问服务器进行运维，将服务器接入堡垒机实例后是否仍需要通过VPN连接？

首先，您需要通过VPN连接才可以通过内网IP登录堡垒机实例。通过堡垒机实例登录目标服务器进行运维时，则不需要使用VPN，通过内网IP方式连接ECS云服务器即可。

> **说明** 您需要确保堡垒机实例与目标服务器在同一专有网络VPC中。

登录堡垒机实例后，在一段时间内没有选择需要登录的ECS实例后自动断开，默认的超时时间是多久？是否支持自定义？

以下是不同方式连接堡垒机实例的超时时间说明：

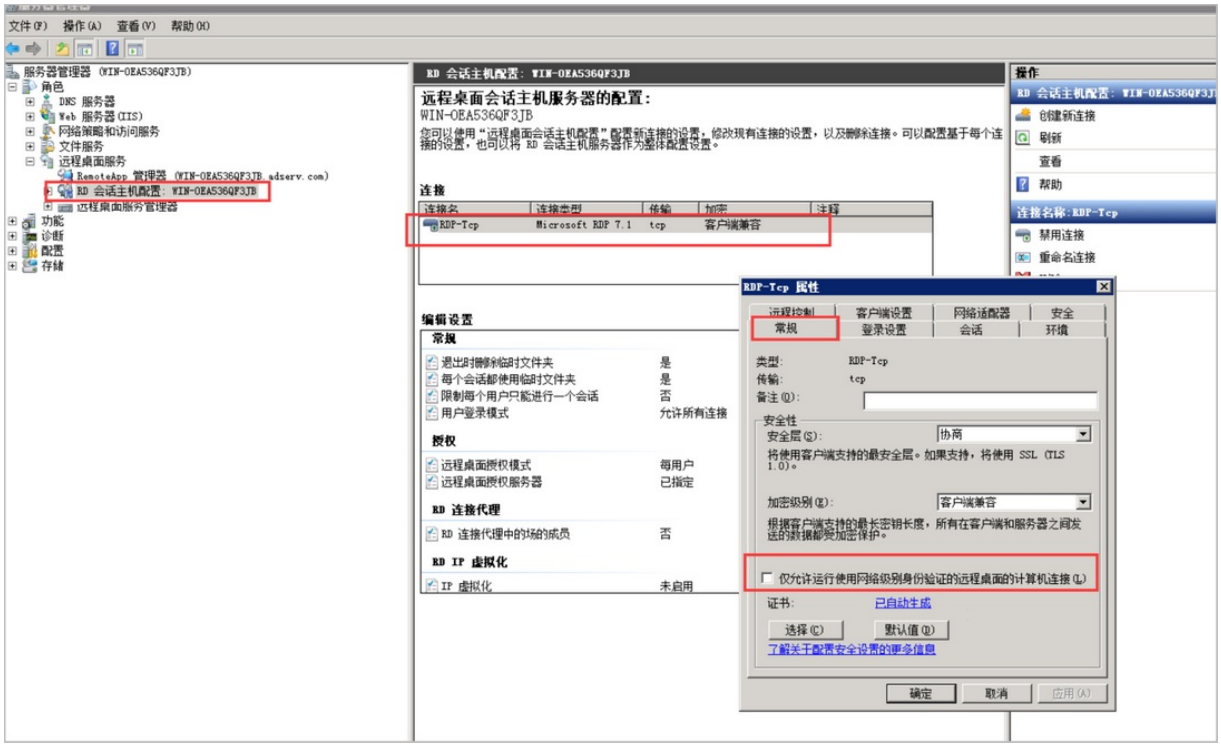
- 如果您通过RDP方式连接堡垒机实例，在选择服务器界面等待100秒后仍未登录ECS实例，将自动断开连接。
- 如果您通过SSH方式连接堡垒机实例，在选择服务器界面等待10分钟后仍未登录ECS实例，将自动断开连接。

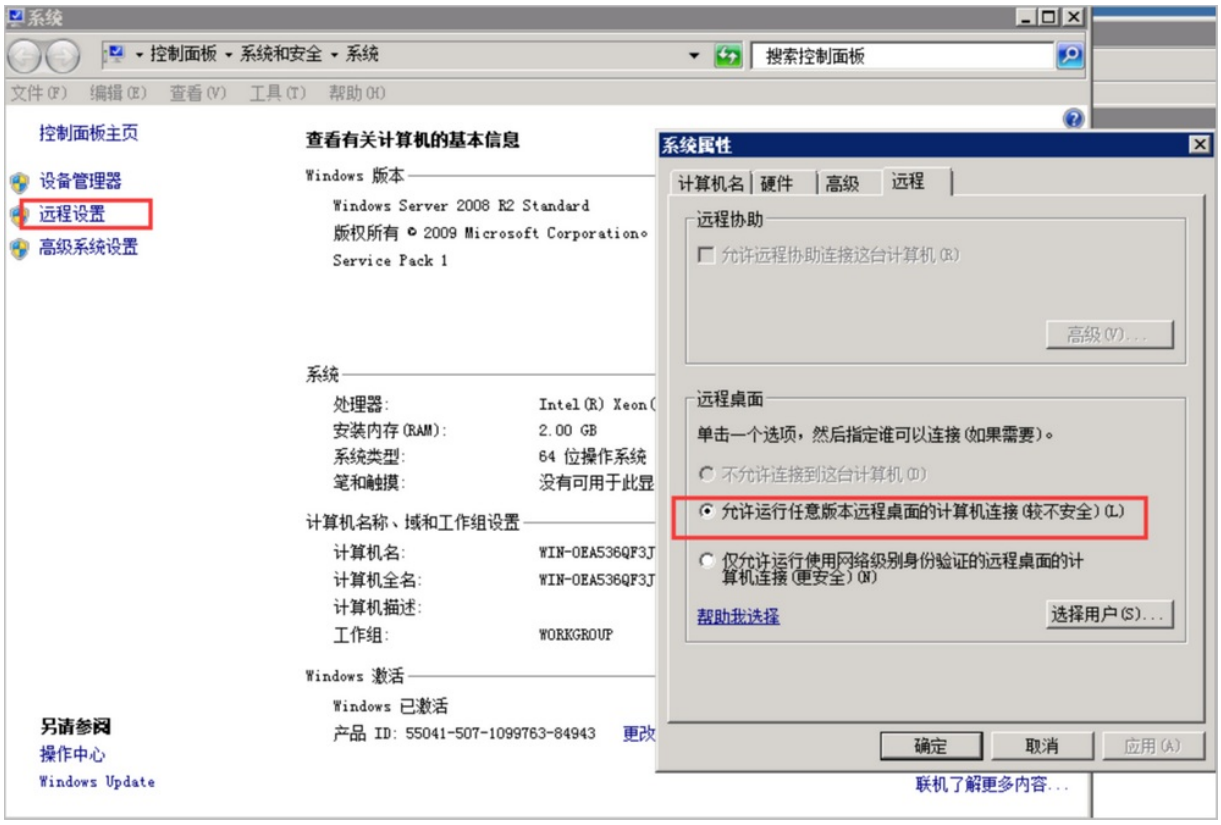
默认超时时间不支持更改。

通过堡垒机实例以RDP方式登录目标服务器遇到错误，应该如何处理？

错误信息如下：

提示该错误是由于该ECS服务器启用了网络级别的身份验证，您需要在目标服务器中进行以下配置后重新登录。





目前用于登录服务器的私钥是带有密码的，如何在凭据中输入私钥密码？

目前资产凭据不支持带有密码的私钥。

凭据是否必须是ECS服务器上的真实用户，还是创建凭据时堡垒机实例会自动在对应的ECS服务器中创建一个新用户？

凭据中设置的登录名必须是目标ECS服务器上已有的用户（如root），堡垒机实例本身不会对ECS服务器进行任何操作。

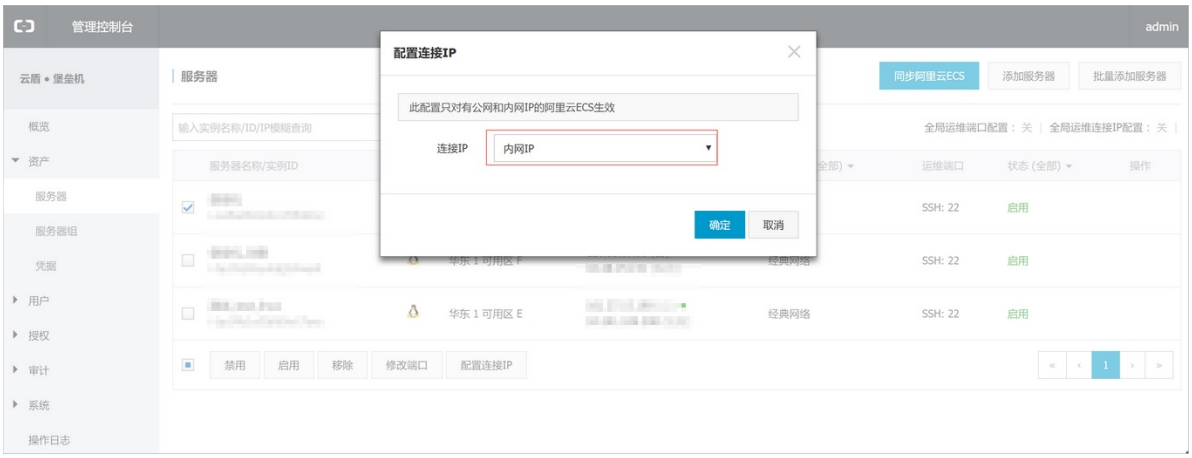
系统管理员如何给不同运维人员配置不同主机的运维权限？

云盾堡垒机实例的权限控制依赖于目标服务器的凭据权限。例如，您可以在授权组A中添加目标服务器的root权限凭据，在授权组B中添加目标服务器的普通权限凭据，这样在授权组A中的用户（运维人员）即具有目标服务器的root权限，而授权组B中的用户只拥有普通权限。

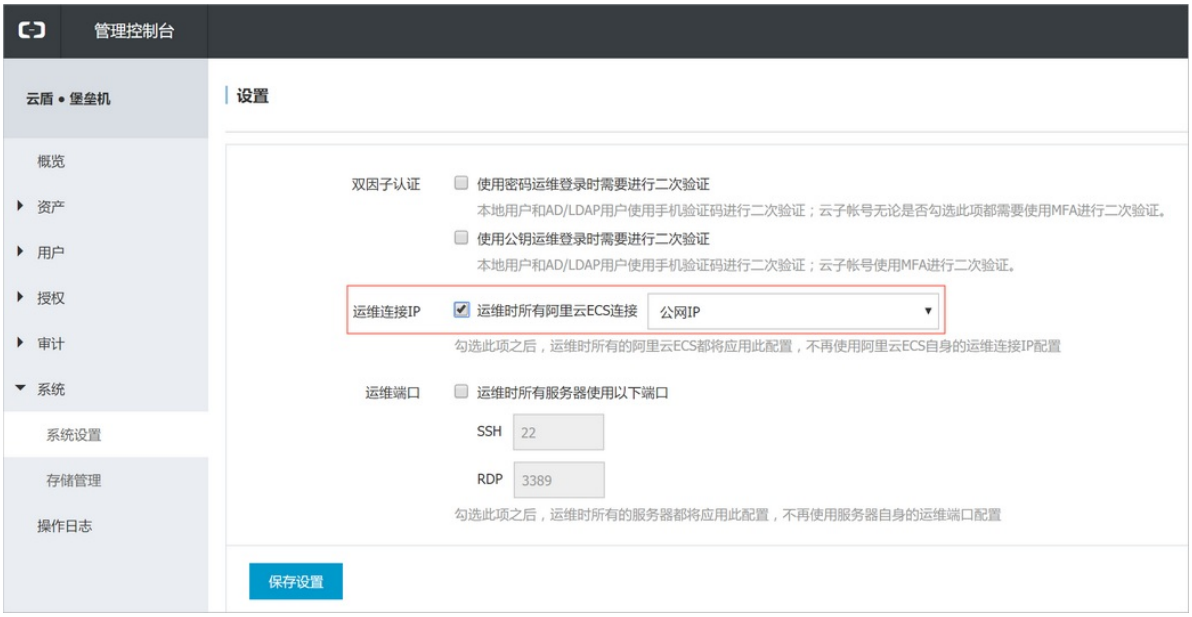
在云盾堡垒机实例中，如何设置通过内网IP登录ECS服务器？

您可以通过以下两种方式进行设置：

- 通过设置单台服务器的**连接IP**配置：在云盾堡垒机实例中，定位到**资产 > 服务器**页面，选择目标服务器，单击**配置连接IP**，选择**内网IP**。



- 通过设置全局运维连接IP配置：在云盾堡垒机实例中，定位到**设置**页面，选中**运维连接IP**并选择**内网IP**。



目标ECS服务器使用的不是SSH、RDP等协议的标准端口，云盾堡垒机实例该如何配置？

云盾堡垒机实例支持自定义运维端口，您可以通过以下方式进行设置：

- 单台服务器配置：在云盾堡垒机实例中，定位到**资产 > 服务器**页面，选择目标服务器，单击**修改端口**，填写自定义的运维端口号。

- 全局配置：在云盾堡垒机实例中，定位到**设置**页面，选中运维端口，填写自定义的运维端口号。

堡垒机实例中的审计录像能保存多久？

V2和V3.1版本堡垒机实例的审计录像一般可以保存半年以上，且支持手动删除。当堡垒机实例磁盘快满时，会自动清除最久的审计日志和录像。

> **说明** 云盾堡垒机实例直接保存运维协议的原始数据，根据流量不同所占用的空间大小也不同。

- SSH运维会话一般每天产生2 M左右日志数据。
- 远程桌面（RDP）运维会话（1024 * 768分辨率）一般每小时产生10 M左右日志数据。

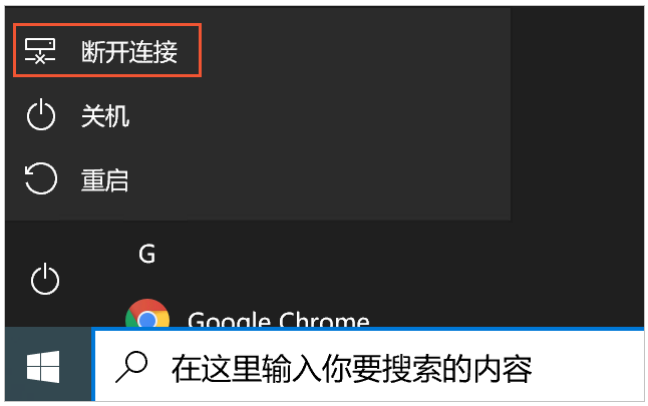
登录云盾堡垒机实例提示连接不安全？

该提示是由于自签名证书未被浏览器信任，并不会影响云盾堡垒机实例的安全性。

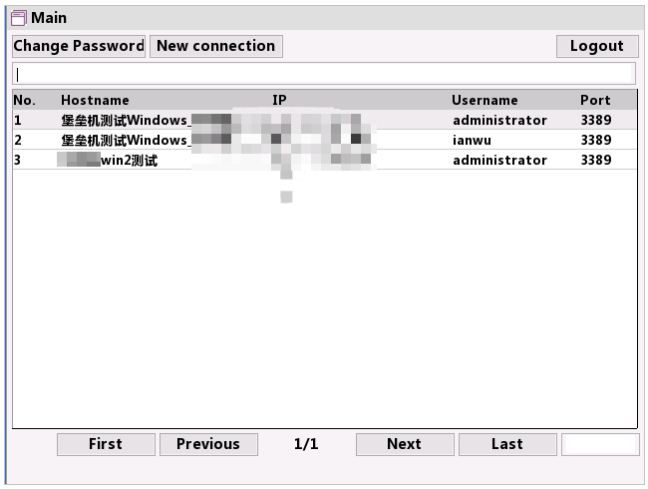
使用RDP运维，如何切换主机？

在使用RDP运维过程中想切换主机，您可以通过以下方式进行切换：

1. 单击电脑桌面左下角的**开始**按钮。
2. 在弹出的**开始**菜单中，单击**电源**按钮。
3. 在**电源**菜单中，单击**断开连接**。



4. 返回主机列表界面后，选择您要运维的主机并登录，即可完成主机切换。



如何将服务器配置为HTTP和SOCKS5代理服务器？

本教程以阿里云服务器（操作系统为CentOS 8.3）为例，介绍如何将服务器配置为HTTP和SOCKS5代理服务器。

> **说明**
> - 配置代理服务器前，请确保堡垒机与代理服务器网络互通。
> - linux服务器可以直接使用SSH代理，不需要安装其他组件及配置。

1. 登录代理服务器。
2. 执行**yum install 3proxy**命令，安装3proxy代理工具。
3. 执行**vim /etc/3proxy.cfg**命令，修改以下配置文件。
   - 配置代理服务器的主机账户和密码。

```
users 3APA3A:CL:3apa3a "test:CR:$1$qwer$CHFTUFGqkjue9HyhcMHEe1" ceshi:CL:1qaz@WSX
# note that "" required, overvise $... is treated as include file name.
# $1$qwer$CHFTUFGqkjue9HyhcMHEe1 is 'test' in MD5 crypt format.
#users $/usr/local/etc/3proxy/passwd
# this example shows you how to include passwd file. For included files
# <CR> and <LF> are treated as field separators.
```

- 配置权限控制参数。

```
# for different clients.
allow ceshi
```

- 启用HTTP和SOCKS5代理，指定监听端口和访问代理服务器的来源IP。

```
auth strong
# We want to protect internal interface
deny * * 127.0.[redacted].,192.168.[redacted]
# and llow HTTP and HTTPS traffic.
allow * * * 80-88,8080-8088 HTTP
allow * * * 443,8443 HTTPS
proxy -i0.0.0.0 -p8080
socks -i0.0.0.0 -p1080
flush
```

4. 执行bin/systemctl start 3proxy.service命令，启用代理服务。
5. 执行iptables -F命令，关闭服务器的防火墙，确保服务器可以被访问。
6. 为该服务器添加安全组规则。具体操作，请参见添加安全组规则。

> **说明** 在配置安全组规则时，端口范围请设置为步骤3中配置的监听端口，授权对象请设置为堡垒机实例的出口IP（堡垒机实例的出口IP可在堡垒机实例列表中，单击对应实例左上方的**出口IP**获取）。

为服务器添加安全组规则后，代理服务器配置完成。