数据加密服务

快速入门

文档版本 02

发布日期 2025-01-20

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 创建密钥进行云服务加密

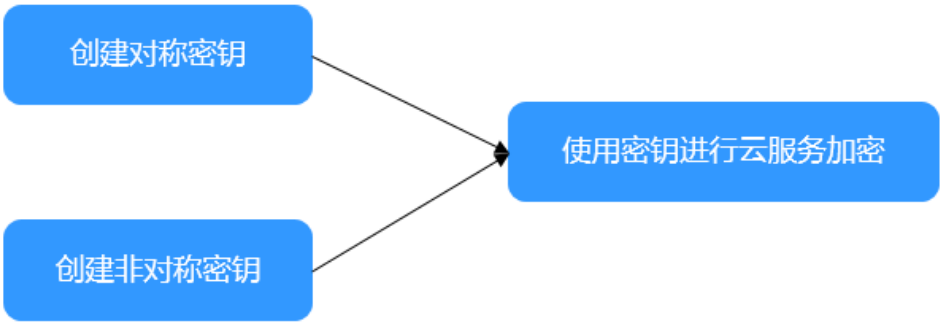
密钥分为“对称密钥”和“非对称密钥”。

- 对称密钥使用同一个密钥去加密和解密数据。它的最大优势是加、解密速度快，适合于对大量数据进行加密。
- 非对称密钥使用不同的密钥分别完成加密和解密操作，即一对公钥和私钥互相关联，其中的公钥可以被分发给任何人，而私钥必须被安全的保护起来，只有受信任者可以使用。适合于实现数字签名验签或者加密传递敏感信息。

操作流程

本章节以“AES-256”对称密钥、“RSA-2048”非对称密钥为示例介绍创建密钥操作以及绑定云服务，流程如**图 创建密钥以及云服务加密**所示。

图 1-1 创建密钥以及云服务加密



操作步骤	说明
准备工作	注册华为账号、开通华为云，为账户充值、赋予KMS权限。
• **创建对称密钥** • **创建非对称密钥**	创建密钥，选择密钥算法类型等。

操作步骤	说明
云服务加密	创建密钥后，在云服务实例创建或使用场景选择目标密钥与实例绑定，实现加密。

准备工作

1. 在创建密钥之前，请先注册华为账号并开通华为云。具体操作详见**注册华为账号并开通华为云**。

   如果您已开通华为云，请忽略此步骤。
2. 请确保已为账号拥有KMS CMKFullAccess及以上权限。具体操作请参见**创建用户并授权使用DEW**。

   表 1-1 表 1 KMS 系统角色

角色名称	描述	类别	依赖关系
KMS Administrator	密钥管理服务(KMS)管理员，拥有该服务下的所有权限。	系统角色	无
KMS CMKFullAccess	密钥管理服务(KMS)的加密密钥所有权限。拥有该权限的用户可以完成基于策略授权的所有操作。	系统策略	无
KMS CMKReadOnlyAccess	密钥管理服务(KMS)的加密密钥只读权限。拥有该权限的用户可以完成基于策略授权的所有操作。	系统策略	无

创建密钥

以创建“AES-256”对称密钥、“RSA-2048”非对称密钥为例进行介绍。

创建对称密钥

1. **登录管理控制台**。
2. 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。
3. 单击界面右上角“创建密钥”。
4. 进入“创建密钥”页面，填写以下参数。
   - 密钥算法选择“AES-256”。

     创建的密钥只能在当前选择的区域使用，如需在其它区域使用，请切换到对应区域进行创建或者使用区域性密钥。有关副本密钥的区域说明，请参见**功能总览**。

- 其他参数根据具体情况选择。

5. 单击“确定”，在页面右上角弹出“创建密钥成功”，则说明密钥创建完成。用户可在密钥列表上查看已完成创建的密钥，密钥默认状态为“启用”。

创建非对称密钥

1. **登录管理控制台**。单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。
2. 单击界面右上角“创建密钥”。
3. 进入“创建密钥”页面，填写以下参数。
   - 密钥算法选择“RSA-2048”。

     创建的密钥只能在当前选择的区域使用，如需在其它区域使用，请切换到对应区域进行创建或者使用区域性密钥。有关副本密钥的区域说明，请参见**功能总览**。
   - 其他参数根据具体情况选择。
4. 单击“确定”，在页面右上角弹出“创建密钥成功”，则说明密钥创建完成。用户可在密钥列表上查看已完成创建的密钥，密钥默认状态为“启用”。

云服务加密

当前KMS服务对接OBS、EVS等服务，实现实例加密，具体原理介绍以及操作步骤可参见以下示例。

- **ECS服务端加密**
- **OBS服务端加密**
- **EVS服务端加密**
- **IMS服务端加密**
- **RDS数据库加密**
- **DDS数据库加密**

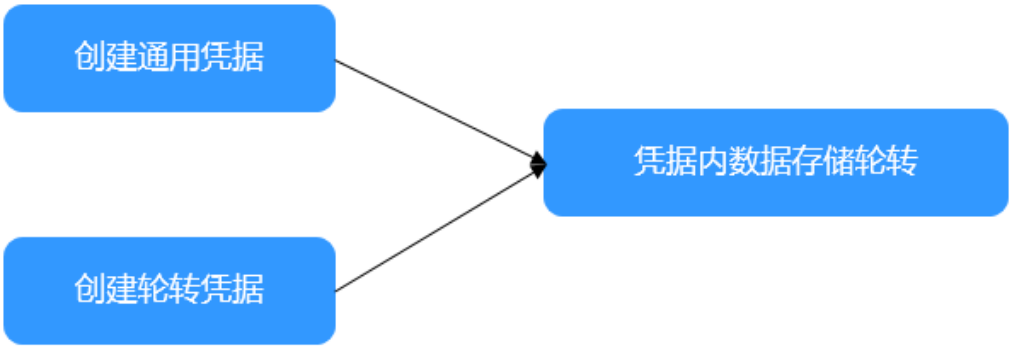
2 创建凭据进行数据存储轮转

应用系统中存在大量的敏感凭据信息，且分散到不同业务部门及系统，管理混乱，缺乏集中管理工具。通过凭据管理服务对敏感凭据进行统一的存储、检索、使用等全生命周期管控。

操作流程

本章节以通用凭据、轮转凭据为示例介绍创建凭据操作以及数据轮转，流程如**图 创建密钥以及云服务加密**所示。

图 2-1 创建凭据以及数据存储轮转



操作步骤	说明
准备工作	注册华为账号、开通华为云，为账户充值、赋予CSMS权限。
• **创建通用凭据** • **创建轮转凭据**	创建凭据，选择凭据类型等。
数据轮转	创建凭据后，通过函数工作流服务设置即可完成凭据内数据轮转。

准备工作

1. 在创建密钥之前，请先注册华为账号并开通华为云。具体操作详见**注册华为账号并开通华为云**。

   如果您已开通华为云，请忽略此步骤。
2. 购买实例前需要确保账户有足够金额，请参见**账户充值**。
3. 已创建KMS加密密钥。
   - 可选择默认密钥“csms/default”。
   - 选择在KMS创建的自定义密钥，具体操作请参见**创建密钥**。
4. 使用轮转凭据前，需完成创建对应数据库实例以及数据库账号。
   - RDS凭据：创建RDS实例，具体操作请参见**购买RDS for MySQL实例**。
   - TaurusDB凭据：仅支持TaurusDB实例，实例创建请参见**购买TaurusDB实例**。

创建通用凭据

1. **登录管理控制台**。单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。
2. 在左侧导航栏选择“凭据管理 > 凭据列表”，单击界面左上角“创建凭据”。
3. 进入“创建凭据”页面，填写以下参数。
   - 凭据类型选择“通用凭据”。

     创建的凭据只能在当前选择的区域使用，如需在其它区域使用，请切换到对应区域进行创建。有关凭据管理的区域说明，请参见**功能总览**。
   - KMS列表选择默认密钥或者已创建的密钥。
   - 其他参数根据具体情况选择。
4. 单击“确定”，凭据创建完成。用户可在凭据列表查看已完成创建的凭据，凭据默认状态为“启用”。

创建轮转凭据

1. **登录管理控制台**。单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。
2. 在左侧导航栏选择“凭据管理 > 凭据列表”，单击界面左上角“创建凭据”。
3. 进入“创建凭据”页面，填写以下参数。
   - 凭据类型选择“RDS凭据”或“TaurusDB凭据”。

     创建的凭据只能在当前选择的区域使用，如需在其它区域使用，请切换到对应区域进行创建。有关凭据管理的区域说明，请参见**功能总览**。
   - KMS列表选择默认密钥或者已创建的密钥。
   - 凭据值设置为已创建数据库账号、密码。
   - 其他参数根据具体情况选择。
4. 单击“下一步”，进入“选择轮转周期”页面，开启自动轮转开关并根据具体情况选择轮转周期。
5. 选择创建轮转函数，输入自定义轮转函数名称并勾选“我已知晓风险”，单击“下一步”。

6. 单击“确定”，凭据创建完成。用户可在凭据列表查看已完成创建的凭据，凭据默认状态为“启用”。

数据轮转

通用凭据需要通过函数工作流服务进行数据轮转，具体使用场景请参见如下章节。

- **通过函数工作流轮转IAM凭证**
- **如何使用凭据管理服务自动轮转安全密码**

3 绑定密钥对并使用私钥登录弹性云服务器

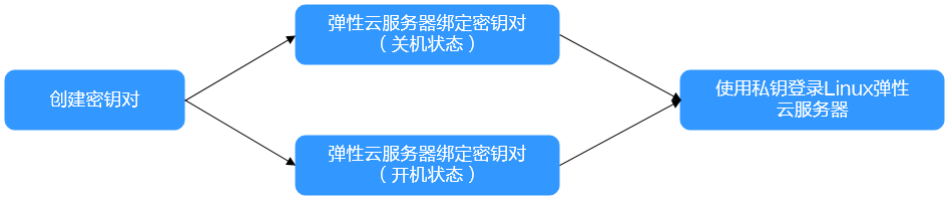
密钥对是通过加密算法生成的一对密钥，包含一个公钥和一个私钥，公钥自动保存在KPS中，私钥由用户保存在本地。如果用户将公钥配置在Linux云服务器中，则可以使用私钥登录Linux云服务器，提高登录安全性。

本章节介绍如何绑定密钥对并使用私钥登录弹性云服务器。

操作流程

本章节以“SSH_RSA_2048”密钥对为示例介绍创建密钥对并登录弹性云服务器，流程如**图 创建密钥对并登录弹性云服务器**所示。

图 3-1 创建密钥对并登录弹性云服务器



操作步骤	说明
准备工作	注册华为账号、开通华为云，为账户充值、赋予KPS权限。
步骤一：创建密钥对	创建密钥对，选择密钥对类型等。
• **步骤二：弹性云服务器绑定密钥对（关机状态）** • **步骤二：弹性云服务器绑定密钥对（运行中状态）**	为弹性云服务器绑定密钥对。
步骤三：使用私钥登录弹性云服务器	绑定密钥对后，通过私钥登录该弹性云服务器。

准备工作

1. 在创建密钥之前，请先注册华为账号并开通华为云。具体操作详见**注册华为账号并开通华为云**。

   如果您已开通华为云，请忽略此步骤。
2. 已完成弹性云服务器创建，具体操作请参见**创建ECS弹性云服务器**。

   弹性云服务器安全组SSH端口（默认22）需对网段100.125.0.0/16提前放通。具体端口及网段放通操作请参见**Linux云服务器SSH登录的安全加固**。
3. 已创建KMS加密密钥。
   - 可选择默认密钥“kps/default”。
   - 选择在KMS创建的自定义密钥，具体操作请参见**创建密钥**。

步骤一：创建密钥对

1. **登录管理控制台**。单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。
2. 在左侧导航栏选择“密钥对管理”，选择“私有密钥对”页签，单击界面左上角“创建密钥对”。
3. 进入“创建密钥对”页面，填写以下参数。
   - 选择密钥对类型为“SSH_RSA_2048”。
   - 勾选“我同意将密钥对私钥托管”。
   - KMS列表选择默认密钥或者已创建的密钥。
   - 勾选“我已阅读并同意《密钥对管理服务免责声明》”
4. 单击“确定”，浏览器自动执行下载任务，下载私钥文件，并弹出页面提示，用户自行保存私钥文件。

步骤二：弹性云服务器绑定密钥对（关机状态）

1. **登录管理控制台**。单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。
2. 在左侧导航栏选择“密钥对管理”，选择“云服务器列表”页签，选择目标ECS实例（处于关机状态），单击绑定。
3. 进入“绑定密钥对”页面，填写以下参数。
   - 选择目标密钥对。
   - 勾选“关闭密码登录方式”。
   - 勾选“我已阅读并同意《密钥对管理服务免责声明》”。
4. 单击“确定”，完成密钥对绑定操作。

步骤二：弹性云服务器绑定密钥对（运行中状态）

1. **登录管理控制台**。单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。
2. 在左侧导航栏选择“密钥对管理”，选择“云服务器列表”页签，选择目标ECS实例（处于运行中状态），单击“绑定”。

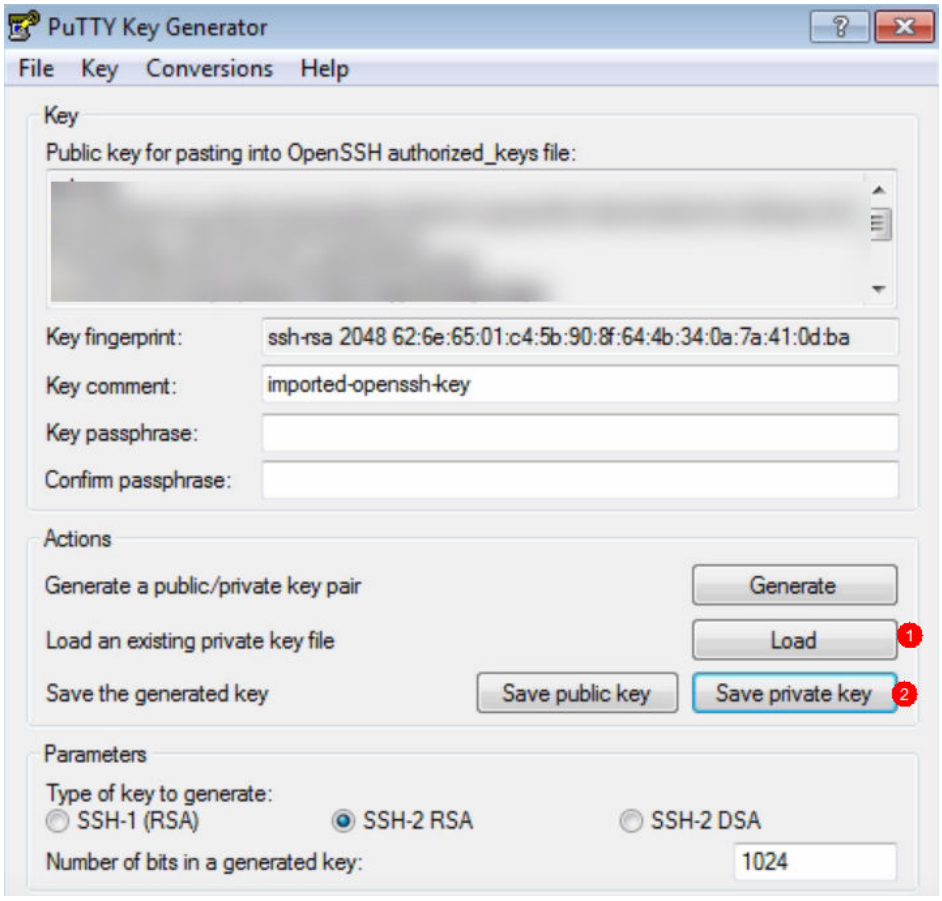
3. 进入“绑定密钥对”页面，填写以下参数。
   - 选择目标密钥对。
   - 输入root密码。
   - 端口参数默认22。
   - 勾选“关闭密码登录方式”。
   - 勾选“我已阅读并同意《密钥对管理服务免责声明》”。
4. 单击“确定”，完成密钥对绑定操作。

步骤三：使用私钥登录弹性云服务器

1. 判断私钥文件是否是.ppk格式。
   - 是，直接登录ECS服务器。
   - 否，执行以下操作转换私钥文件格式后，执行登录ECS服务器。

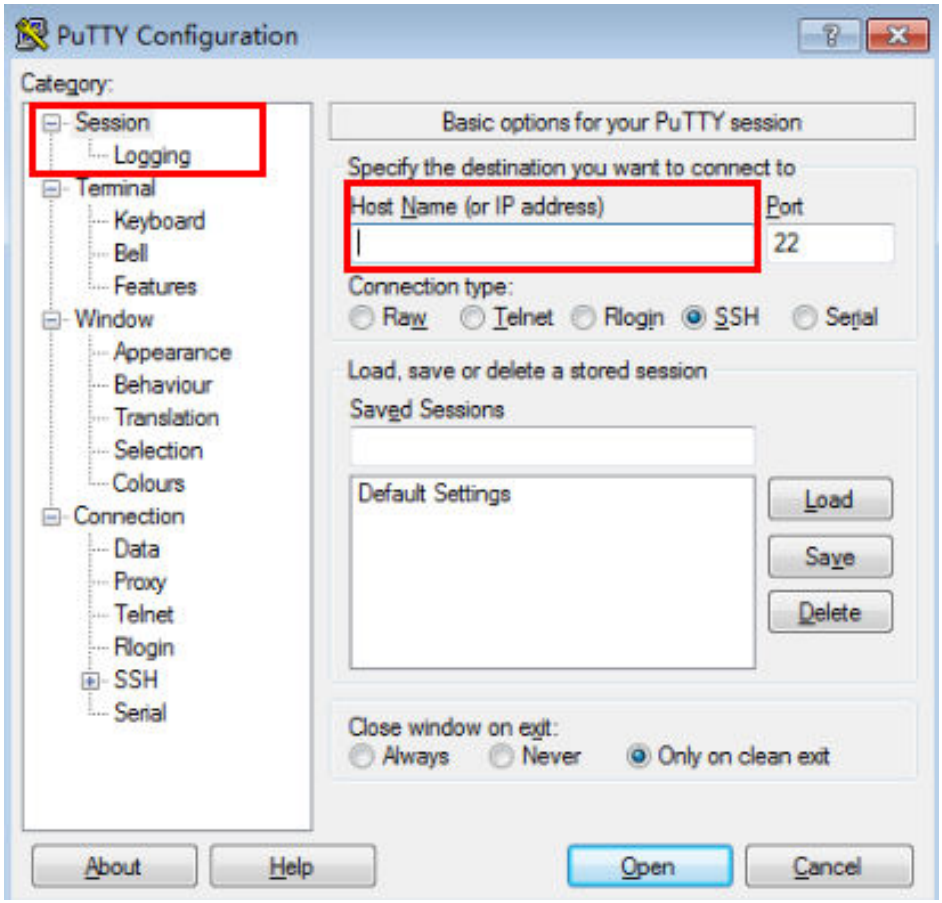
     打开第三方PuTTY工具，将.pem格式私钥文件导入后，导出转换后的.ppk格式私钥文件。

     图 3-2 私钥文件格式转换



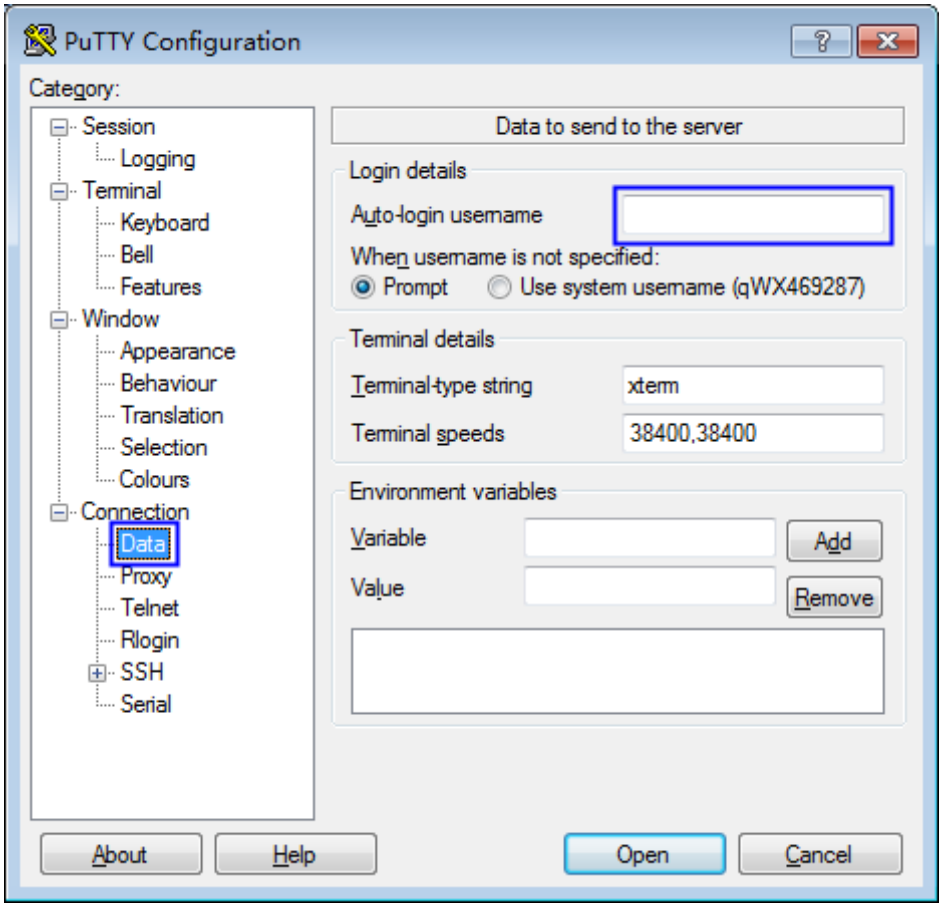
2. 打开PuTTY工具，登录ECS服务器。
   - 输入弹性云服务器IP地址，默认使用22端口。

图 3-3 弹性云服务器 IP 地址



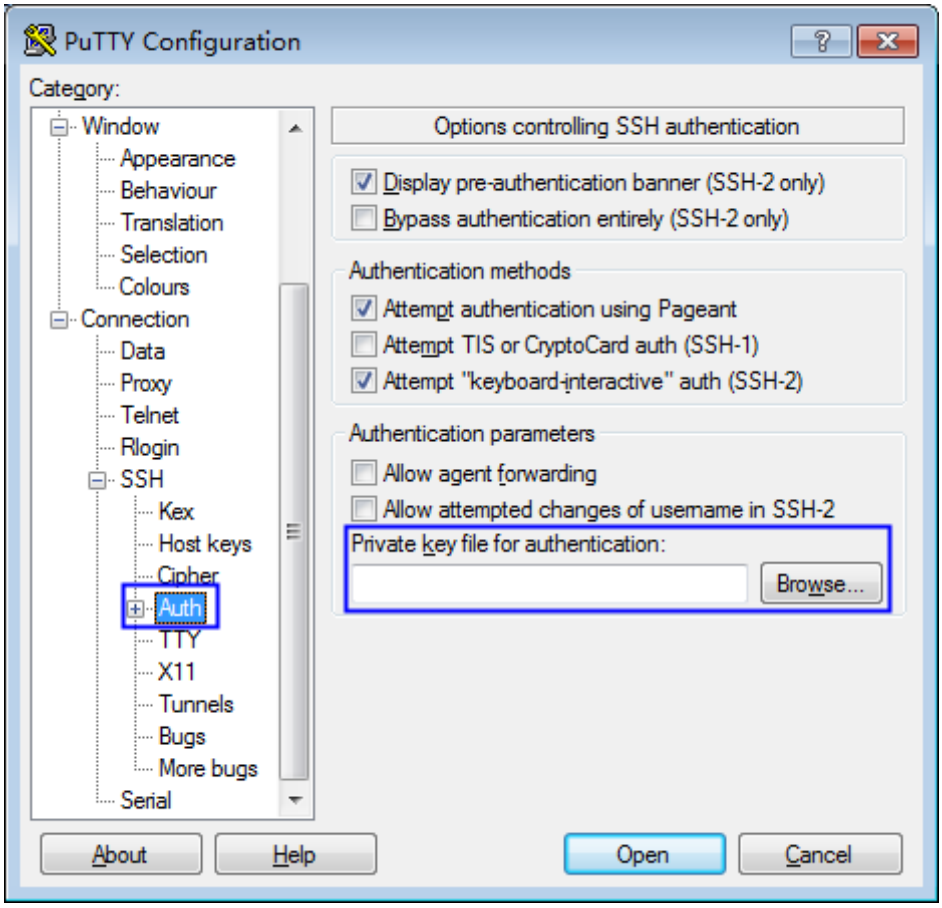
- 输入弹性云服务器镜像的用户名。

图 3-4 镜像用户名



- 上传.ppk格式私钥文件。

图 3-5 上传私钥文件



- 单击“Open”，完成云服务器登录操作。

4 使用密钥进行 OBS 服务端加密

数据加密服务（Data Encryption Workshop）是一个综合的云上数据加密服务。它提供的密钥管理（Key Management Service，KMS）是一种安全、可靠、简单易用的密钥托管服务，帮助用户集中管理密钥，保护密钥安全。

您可以通过KMS创建密钥，并使用创建的密钥将OBS服务端中上传的文件进行加密。

步骤一 准备环境

1. 登录**登录管理控制台**，在控制台页面中选择“存储 > 对象存储服务”。
2. 单击“创建桶”，创建一个桶，用于存储上传的文件。

步骤二 创建密钥

1. 在控制台页面中，选择“安全 > 数据加密服务”，进入密钥管理页面。
2. 在密钥管理列表页面，单击右上角的“创建密钥”。
3. 在弹出的“创建密钥”对话框中，输入密钥的别名和描述信息，并单击“确定”。

说明

您也可以根据自己的需要将自己的密钥导入到KMS，由KMS统一管理。关于如何导入密钥，请参见**导入密钥材料**获取。

步骤三 上传文件到 OBS 桶

1. 在控制台页面中选择选择“存储 > 对象存储服务”，单击桶的名称，进入桶的详细信息页面。
2. 单击“对象 > 上传对象”。
3. 选择待上传的文件，并选择“SSE-KMS加密”，选择“加密密钥类型”后，单击“上传”，完成文件上传。

5 使用私钥登录 Linux 弹性云服务器

数据加密服务（Data Encryption Workshop）是一个综合的云上数据加密服务。它提供的密钥对管理（Key Pair Service，KPS）一种安全、可靠、简单易用SSH密钥对托管服务。SSH密钥对，简称为密钥对，是为用户提供的远程登录Linux云服务器的认证方式，是一种区别于传统的用户名和密码登录的认证方式。

密钥对是通过加密算法生成的一对密钥，包含一个公钥和一个私钥，公钥自动保存在华为云中，私钥由用户保存在本地。用户也可以根据自己的需要将私钥托管在华为云中，由华为云统一管理。

本指南以创建的密钥对登录Linux弹性云服务器为例，指导您快速上手密钥对管理服务。

步骤一 准备环境

1. 登录**登录管理控制台**。
2. 在控制台页面中选择“计算 > 弹性云服务器”，创建一台弹性云服务器（ECS），用于绑定密钥对。

步骤二 创建密钥对

1. 登录**登录管理控制台**，选择“安全 > 数据加密服务”。
2. 在左侧导航树中，单击“密钥对管理”，进入密钥对管理页面，单击“创建密钥对”。

   说明

   - 您可以根据自己的需要是否将私钥托管到华为云。
   - 为保证云服务器安全，未进行私钥托管的私钥只能下载一次，请妥善保管。已授权华为云托管的私钥可在您需要时导出使用。

步骤三 绑定密钥对

1. 在密钥对管理页面，单击“云服务器列表”，进入云服务器列表页面。
2. 单击弹性云服务器所在行的“绑定”，在弹出的“绑定密钥对”对话框中，完成配置后，单击“确定”。

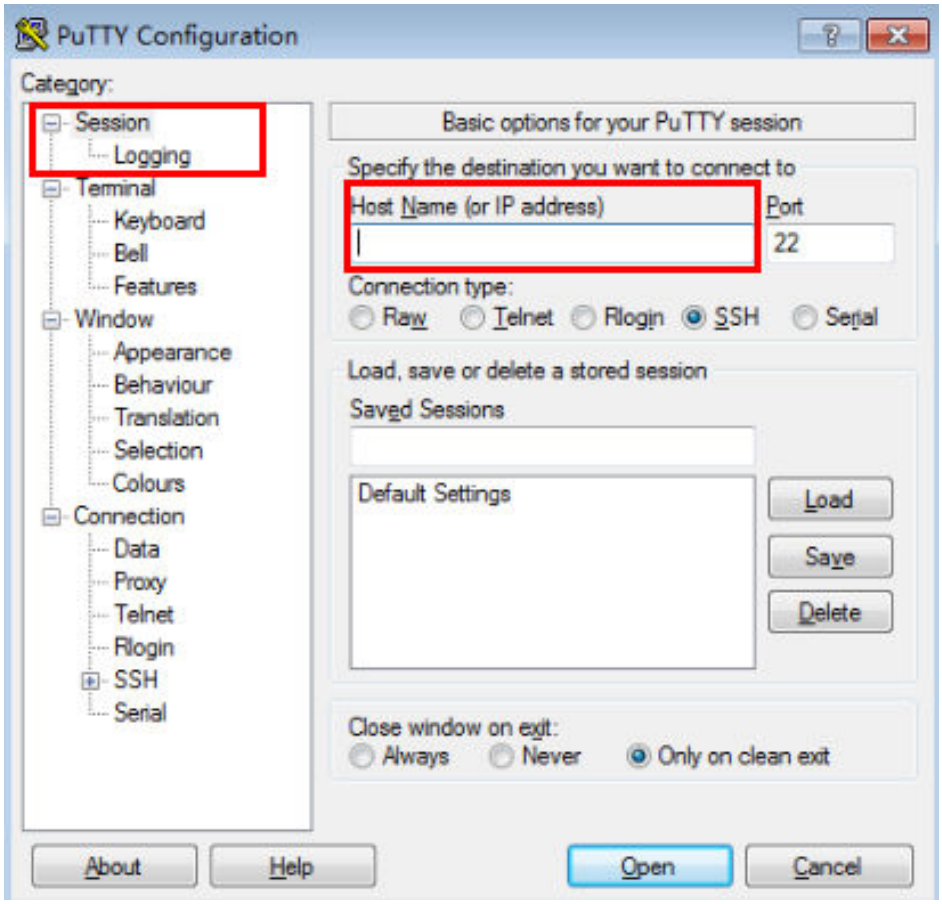
说明

- 若您已有弹性云服务器的“root密码”，可直接输入root密码，直接进行密钥对绑定操作。
- 若您没有弹性云服务器的“root密码”，可将弹性云服务器关机，在弹性云服务器关机状态执行密钥对绑定操作。

步骤四 使用私钥登录弹性云服务器

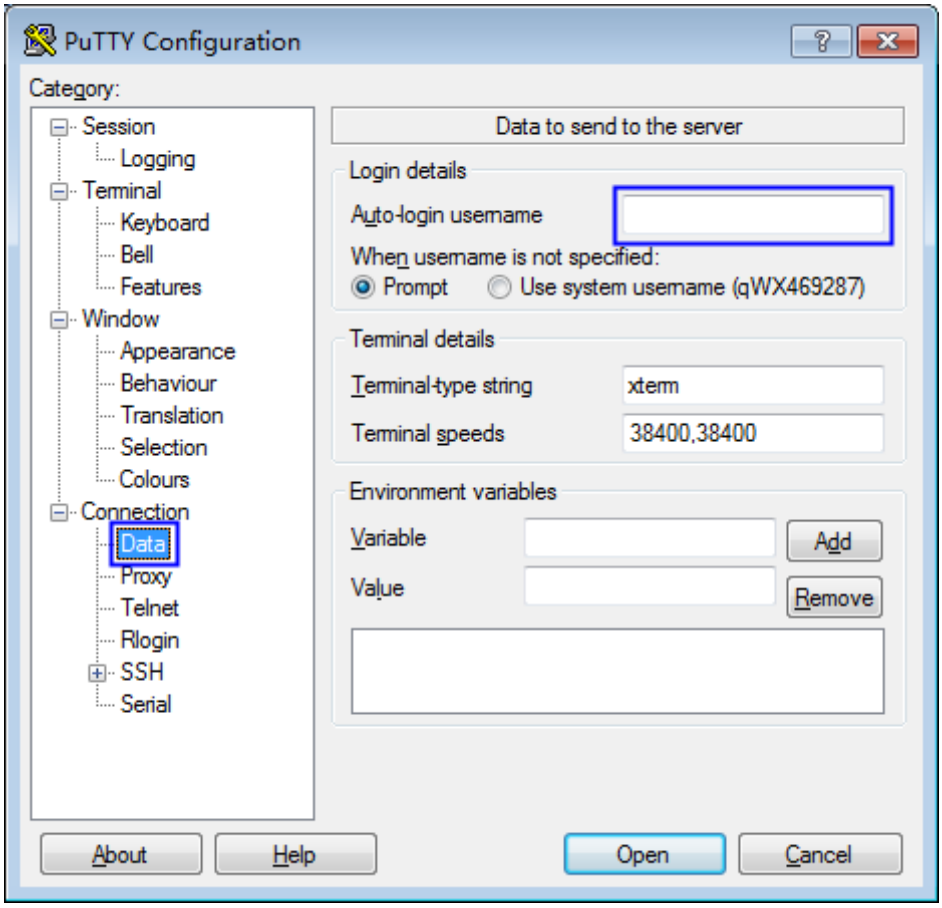
1. 打开第三方工具PuTTY。

图 5-1 弹性云服务器 IP 地址



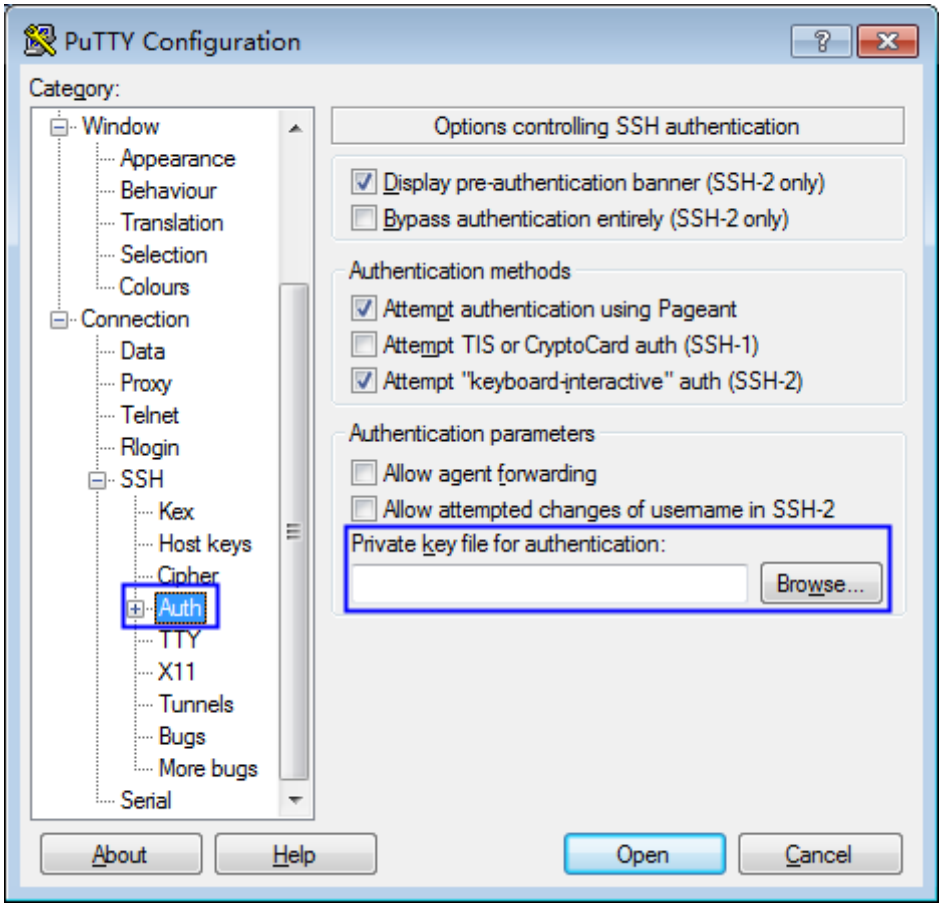
2. 输入弹性云服务器镜像的用户名。

图 5-2 镜像用户名



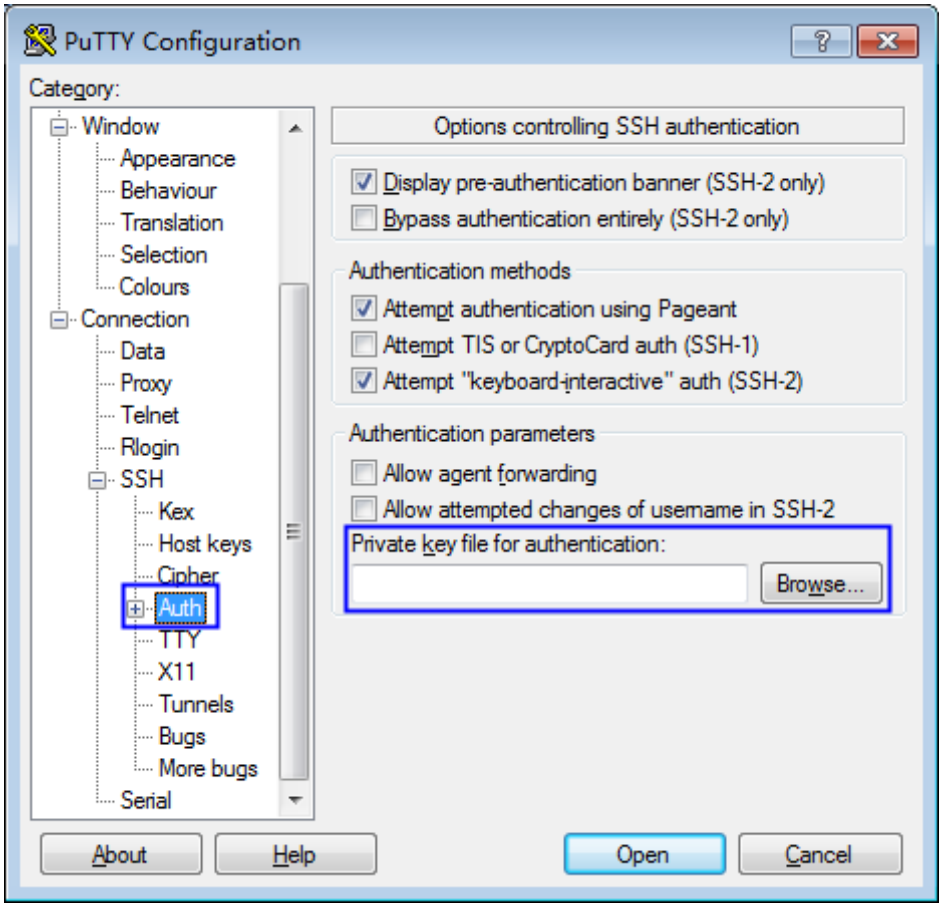
3. 上传“.ppk”格式的私钥文件。

图 5-3 上传私钥文件



4. 输入弹性云服务器的弹性IP地址。

图 5-4 上传私钥文件



说明

- 若是“CoreOS”的公共镜像，镜像的用户名为“core”；若是“非CoreOS”的公共镜像，镜像的用户名为“root”。
- 上传的私钥文件格式需要是“.ppk”格式文件，若不是“.ppk”格式，需要将私钥文件格式转换为“.ppk”格式。

6 入门实践

当用户完成了创建密钥、创建密钥对、创建凭据等基本操作后，可以根据自身的业务需求使用DEW提供的一系列常用实践。

表 6-1 常用最佳实践

实践		描述
数据保护	**加解密小量数据**	当有少量数据（例如：口令、证书、电话号码等）需要加解密时，用户可以通过密钥管理服务（Key Management Service，KMS）控制台使用在线工具加解密数据，或者调用KMS的API接口使用指定的用户主密钥直接加密、解密数据。
	加解密大量数据	当有大量数据（例如：照片、视频或者数据库文件等）需要加解密时，用户可采用信封加密方式加解密数据，无需通过网络传输大量数据即可完成数据加解密。
	使用加密SDK进行本地文件加解密	加密SDK提供了数据的加解密、文件流加解密等功能，用户只需调用加解密接口即可轻松实现海量数据加解密。当出现大型文件、图片等数据通过HTTPS请求到KMS服务进行保护时会消耗大量网络资源，加密效率低的问题时，可以使用加密SDK进行本地文件加解密。
	跨Region容灾加解密	当单Region加解密出现服务侧故障时，无法再对数据进行加解密操作，用户可以通过密钥管理服务（Key Management Service，KMS）实现跨Region容灾加解密，保证业务不中断。
	如何使用KMS对文件进行完整性保护	当有大量文件（例如：镜像、电子保单或者重要文件等）需要在传输或者存储时确保安全性，用户可以使用KMS对文件摘要进行签名，再次使用时可以重新计算摘要进行验签。确保文件在传输或者存储过程中没有被篡改。

实践		描述
云服务使用KMS加密	ECS服务端加密	KMS支持对ECS服务进行一键加密，弹性云服务器资源加密包括镜像加密和数据盘加密。 • 在创建弹性云服务器时，用户如果选择加密镜像，弹性云服务器的系统盘会自动开启加密功能，加密方式与镜像保持一致。 • 在创建弹性云服务器时，用户也可以对添加的数据盘进行加密。
	OBS服务端加密	当用户启用OBS服务端加密功能时： • 在上传对象时，数据会在服务端加密成密文后存储。 • 在下载加密对象时，存储的密文会先在服务端解密为明文，再提供给用户。 在OBS服务中需要上传的对象可以通过KMS提供密钥的方式进行服务端加密。
	EVS服务端加密	当用户由于业务需求需要对存储在云硬盘的数据进行加密时，EVS服务与KMS集成，通过KMS提供的密钥实现磁盘数据的加密。
	IMS服务端加密	用户创建私有镜像时，可以通过选择KMS加密的方式，使用KMS提供的密钥对镜像进行加密，确保镜像数据安全性。
	RDS数据库加密	用户在创建RDS数据库实例和扩容磁盘并启用加密功能后，磁盘数据会在服务端加密成密文后存储。用户下载加密对象时，存储的密文会先在服务端解密为明文，再提供给用户。
	DDS数据库加密	用户在创建DDS数据库实例和扩容磁盘并启用加密功能后，磁盘数据会在服务端加密成密文后存储。用户下载加密对象时，存储的密文会先在服务端解密为明文，再提供给用户。
凭据加密	如何使用凭据管理服务替换硬编码的数据库账号密码	用户在日常访问应用程序的过程中，通常会嵌入凭据直接访问程序。在需要更新凭据时，除了创建新的凭据以外，还需要花费一些时间更新应用程序以使用新的凭据。需要使用华为云凭据管理服务更便捷高效、高安全性的进行凭据管理。
	如何使用凭据管理服务解决AK&SK泄露问题	通过统一身份认证服务（Identity and Access Management，IAM ）对弹性云服务器（Elastic Cloud Server，ECS）的委托获取临时访问密钥来保护AK&SK。
	如何使用凭据管理服务自动轮转安全密码	通过函数工作流和凭据管理服务，定期生成和轮转强安全密码，以满足用户安全合规的密码生成、托管、以及定期自动轮换的要求。

实践		描述
	单用户凭据轮换策略	单用户凭据轮换是指一个凭据中更新一个用户所保存的信息，这是最基础的凭据轮换策略，适用于大多数日常使用场景。
	双用户凭据轮换策略	双用户轮换策略是指在一个凭据中更新两个用户所保存的信息。为防止在修改用户密码和更新凭据时出现访问失败的情况，需要使用双用户凭据轮换策略确保应用程序的高可用性。
	通过函数工作流轮转IAM凭证	使用函数工作流模板，通过凭据管理服务轮转IAM凭证。
API调用	使用指数退避方法对DEW服务请求错误进行重试	当用户调用API时，收到返回的错误信息，可参照使用指数退避方法对请求错误进行重试。