SAP 解决方案

SAP 解决方案

SAP 解决方案

概述



SAP HANA

- SAP HANA 部署指南
- SAP HANA 操作指南
- SAP HANA 备份和恢复
- SAP HANA 高可用和灾备
- SAP HANA 软件许可

SAP Business Applications

- SAP NetWeaver 规划指南
- SAP NetWeaver 部署指南
- SAP NetWeaver 操作指南
- SAP 迁移工具
- ECS Metrics Collector for SAP 部署指南

SAP Business One

- SAP B1 规划指南（英文）
- SAP B1 部署指南（英文）

SAP MaxDB

- SAP MaxDB 部署指南

- SAP MaxDB 操作指南

SAP SQL Server

- SQL Server on 阿里云（英文）

SAP Db2

- IBM Db2 for SAP 规划指南（英文版）
- IBM Db2 for SAP 部署指南（英文版）
- IBM Db2 for SAP HADR（英文版）

SAP最佳实践

- SAP S/4HANA 1709 同可用区高可用部署最佳实践
- SAP S/4HANA 1809 同可用区高可用部署最佳实践
- SAP HANA 同可用区高可用部署
- SAP HANA 跨可用区高可用部署（英文）
- SAP HANA Scale-Out 部署最佳实践
- SAP 高可用测试最佳实践
- ECS Metrics Collector for SAP 部署指南
- SAP系统云盘扩容后处理（基于LVM）
- SAP系统高可用环境维护指南

常见问题

- 操作系统使用须知

SAP HANA

SAP HANA 部署指南

- 介绍
- 云服务器 ECS 实例规格
- 阿里云服务

- 支持的 SAP HANA 版本 以及操作系统版本
- SAP HANA 部署架构
    - 单节点架构
    - 多节点架构
- 在阿里云上部署 SAP HANA
    - 准备工作
        - 阿里云账号
        - SAP HANA 安装介质
        - 选择区域和可用区
        - 账号管理
    - 部署流程
        - 配置网络
        - 创建 SAP HANA 虚拟机
        - 为 SAP HANA Studio 创建 Windows 虚拟机
    - 连接 SAP HANA
- 需要在部署后执行的任务

版本管理

版本	修订日期	变更类型	生效日期
1.0			2017/12/14
1.1	2018/7/31	1.HANA认证机型更新 2.调整和优化了部分内容	2018/7/31
1.2	2018/11/16	HANA认证机型更新	2018/11/16
1.3	2019/1/10	HANA认证机型更新	2019/1/10
1.4	2019/11/29	支持的操作系统更新	2019/11/29
1.5	2010/11/9	HANA认证机型更新	2020/11/9

介绍

SAP HANA 是一个由 SAP 开发和推广的基于内存计算的列存储关系型数据库管理系统，其作为数据库服务器的主要功能是根据应用的要求进行数据的存储和检索。此外，SAP HANA 可执行的高性能分析和实时数据处理，可以解决客户快速增长的业务分析需求。

本部署指南介绍了如何在阿里云云服务器 ECS 上规划和部署 SAP HANA 系统，包括如何配置 ECS 实例、块存储、网络和 SUSE Linux Enterprise Server (SLES) 操作系统。本指南结合了阿里云和 SAP 的最佳实践。

云服务器 ECS 实例规格

本部署指南中的采用的是运行于英特尔 Broadwell或Skylake 架构的 ECS 企业实例规格族内存优化型实例，它还支持使用 SSD 云盘和高效云盘来托管 SAP HANA 数据库的数据卷和日志。

目前支持的实例规格如下：

实例规格	vCPU	内存（GiB）	架构
ecs.r5.8xlarge	32	256	Skylake
ecs.r6.13xlarge	52	384	Cascade Lake
ecs.r5.16xlarge	64	512	Skylake
ecs.se1.14xlarge	56	480	Broadwell
ecs.re6.13xlarge	52	768	Cascade Lake
ecs.re4.20xlarge	80	960	Broadwell
ecs.re6.26xlarge	104	1536	Cascade Lake
ecs.re4.40xlarge	160	1920	Broadwell
ecs.re6.52xlarge	208	3072	Cascade Lake
ecs.re4e.40xlarge	160	3840	Broadwell
ecs.ebmre6-6t.52xlarge	208	6144	Cascade Lake

想要查看所有SAP认证的HANA机型，请点击 这里

阿里云服务

本实施指南使用的阿里云核心组件包括下表中的服务：

服务	描述
云服务器	**云服务器（ECS）是一种具有弹性处理功能的计算服务。ECS 具有比物理服务器更简单和更高效的管理模式。您可以随时创建实例，更改操作系统，以及添加或释放任何数量的 ECS 实例，以满足业务需求。**
SSD 云盘	**适用于 I/O 密集型的应用，并提供稳定和高随机读写的 IOPS 性能。**
高效云盘	**适用于中等 I/O 负载的应用场景，并为 ECS 实例提供随机读写高达3,000 IOPS 的存储性能。**
专有网络	**阿里云专有网络（VPC）是在阿里云中建立的一个私有的网络。它在逻辑上与阿里云中的其他虚拟网络隔离，VPC 使您可以在自己的专有网络中启动和使用阿里云资源。**
对象存储	**阿里云对象存储服务（OSS）是一种基于网络的数据访问服务。OSS 使您能够存储和检索结构化和非结构化数据，包括文本文件，图像，音频和视频。**

支持的 SAP HANA 版本 以及操作系统版本

目前支持的SAP HANA 及操作系统版本为：

- HANA1
  - SLES for SAP Applications / SLES 15
    - 15 SP1 (HANA 1.0 SPS12 大于等于 122.27)
    - 15 (GA) (HANA 1.0 SPS12 大于等于 122.21)
  - SLES for SAP Applications / SLES 12
    - 12 SP4 (HANA 1.0 SPS12 大于等于 122.22)
    - 12 SP3 (HANA 1.0 SPS12 大于等于 122.15)
    - 12 SP2 (HANA 1.0 SPS12)
    - 12 SP1 (HANA 1.0 SPS12)
- HANA2
  - SLES for SAP Applications / SLES 15
    - 15 SP1 (HANA 2.0 SPS04 大于等于 44)
    - 15 (GA) (HANA 2.0 SPS03 大于等于 34)
  - SLES for SAP Applications / SLES 12
    - 12 SP4 (HANA 2.0 SPS03 大于等于 35)
    - 12 SP3 (HANA 2.0 SPS02 大于等于 23)
    - 12 SP2 (HANA 2.0 SPS01 到 HANA 2 SPS03)
    - 12 SP1 (HANA 2.0 SPS00 到 HANA 2 SPS03)

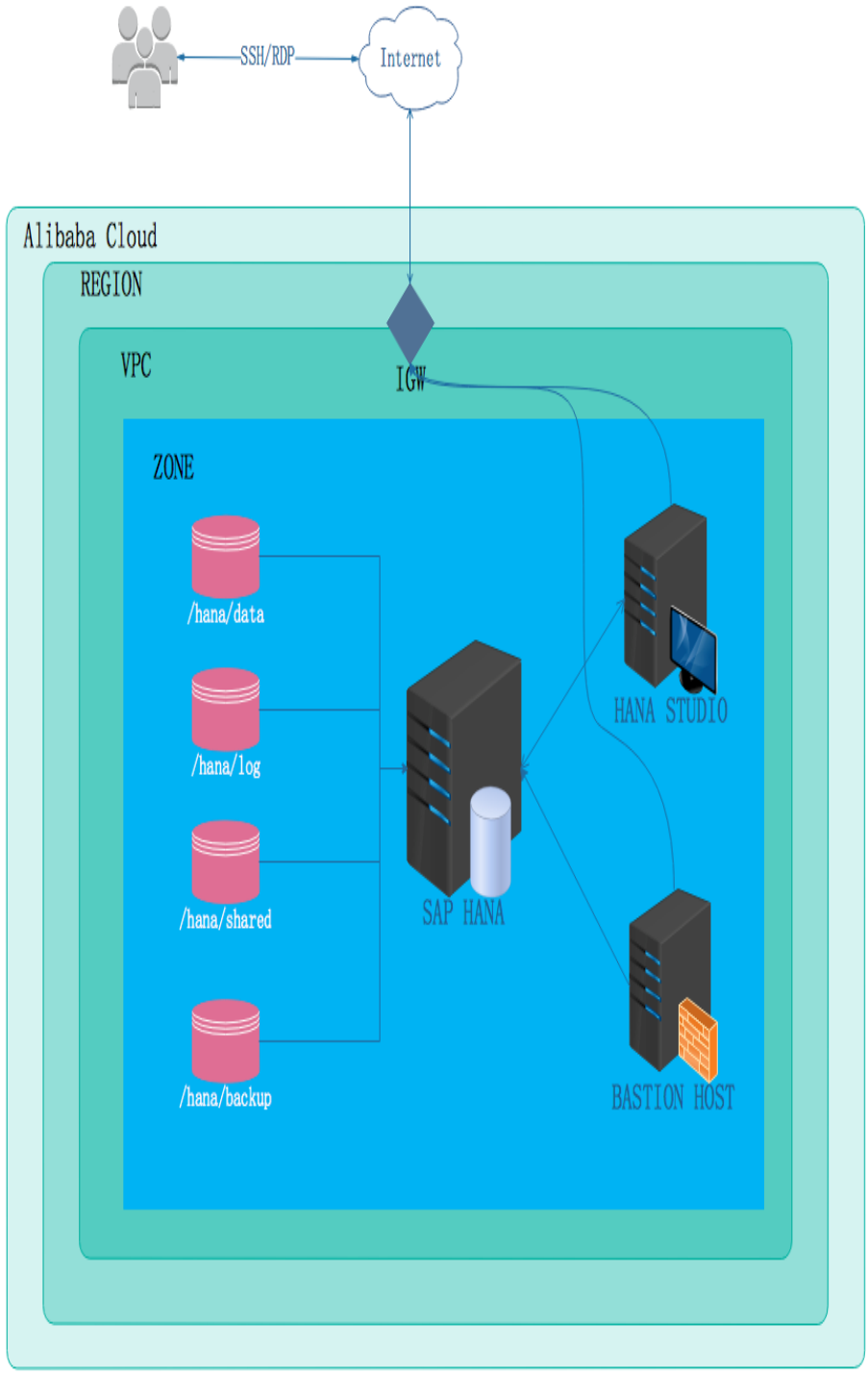
更多详细资料请查看SAP Note 2235581。

SAP HANA 部署架构

SAP HANA 支持单节点纵向扩展（scale-up）和多节点的横向扩展（scale-out）架构。

单节点架构

下图展示了 SAP HANA 的单节点体系架构，和其在阿里云中的部署设计和磁盘的布局。您可以使用 OSS 来备份存在 /hana/backup 路径下的本地备份。（此挂载点路径的容量大小应等于或大于数据卷容量）



请注意，SAP HANA 的虚拟机没有公网 IP，这意味着无法从外部网络直接访问。因此，在部署过程中需要使用堡垒机和 SAP HANA Studio 来访问 SAP HANA。SAP HANA Studio 实例和堡垒主机需要部署在与 SAP HANA 实例相同的私有网络 VPC 中。

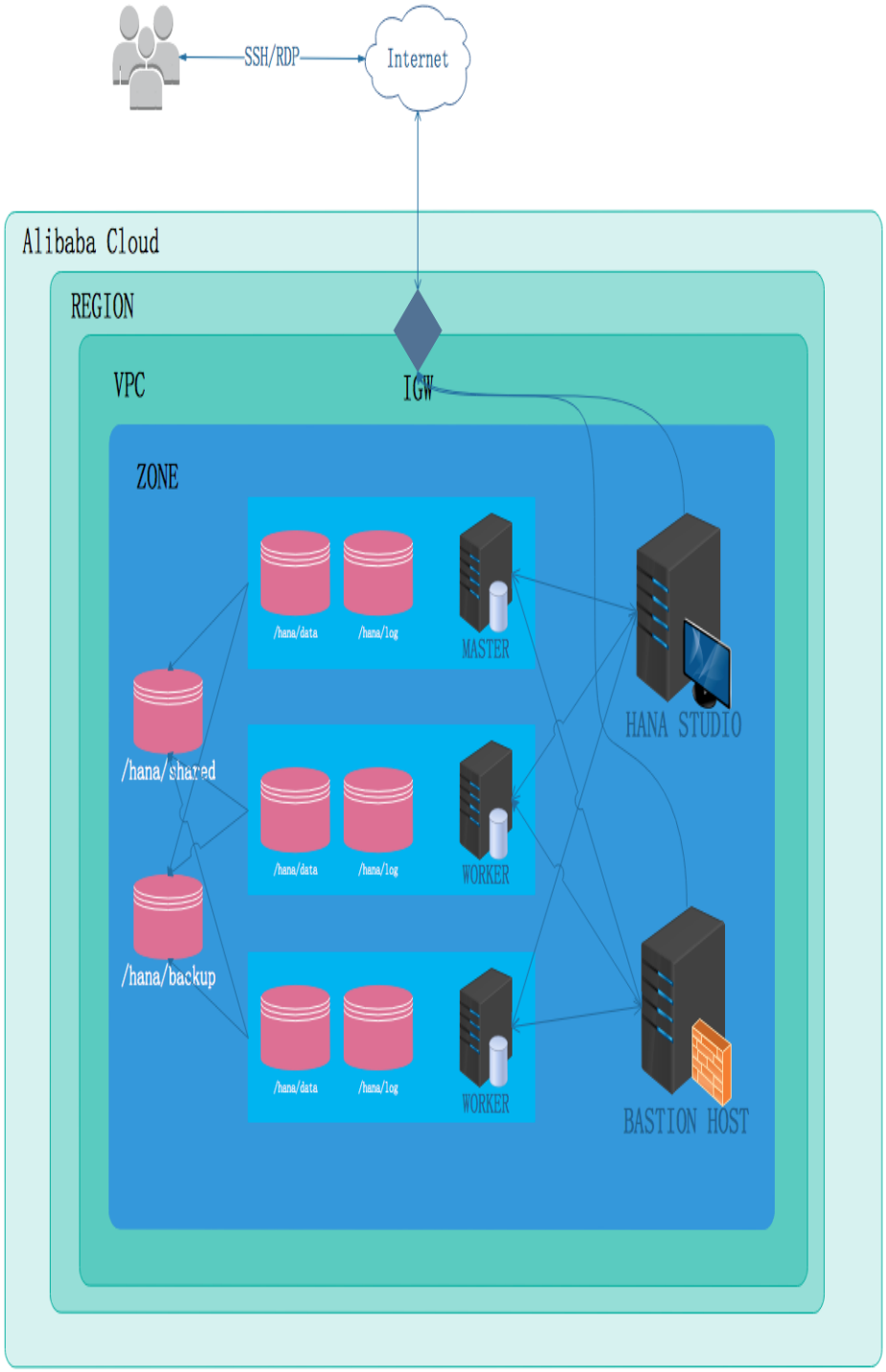
您需要提供用于安装 SAP HANA Studio 的 Windows 主机，将该主机实例放置在相同的 VPC 中，并且其防火墙策略包含使您能够从 SAP HANA Studio 连接到 SAP HANA 数据库的规则。

单节点体系架构的 SAP HANA 部署中，您将使用到以下的组件：

- SAP HANA 数据库主节点的 ECS 实例 ecs.se1.14xlarge，包括：56个 vCPU，480GB 内存，数据卷为数据量大于1.5 TB 的 SSD 云盘，日志卷和 HANA 共享卷均为大于 512GB 的 SSD 云盘。可参见本文档中 创建 SAP HANA 虚拟机 部分的第7点 - 存储配置示例。
- 您所选区域中的 VPC 具有自定义拓扑和可分配的 IP 地址范围，SAP HANA 数据库和其他 ECS 实例都会在这个 VPC 内启动。您也可以使用已存在的 VPC 来部署 SAP HANA。
- 您可以选择为您的 SAP HANA 和其他实例的公网出口配置互联网网关。本指南假定您正在使用此网关。
- ECS 安全组，用于限制实例间的访问。
- 高效云盘，使用标准为 2TB 的云盘为 SAP HANA 数据库做备份。
- ECS VM ecs.sn2.medium，配置 Windows 操作系统并托管 SAP HANA studio。
- ECS VM ecs.n1.medium，配置为堡垒机。

多节点架构

下图展示了 SAP HANA 多节点体系架构。



对于 SAP 商务应用所在的系统，您只能纵向扩展。

由于 HANA 采用无共享架构，横向扩展可以将一组小的 SAP HANA 系统连接在一起成为一个集群数据库。随着工作负载需求的增加，多节点（横向扩展）架构可以在所有节点之间进行负载均衡。

横向扩展架构由一个主节点和多个工作节点组成。它们通过容量高达10 Gbps 的网络进行互连。每个节点在 SSD 云盘上都有自己的 /hana/data 卷和 /hana/log 卷，提供一致的、高 IOPS 的 I/O 服务。主节点还用作 /hana/shared 卷和 /hana/backup 卷的 NFS 主节点，被挂载在每个工作节点上。

在多节点横向扩展体系架构的 SAP HANA 部署中，您将使用到以下的组件：

- SAP HANA 数据库**主节点**的 ECS 实例 ecs.se1.14xlarge，包括：56个 vCPU，480GB 内存，数据卷为数据量大于1.5 TB 的 SSD 云盘，日志卷和 HANA 共享卷均为大于 512GB 的 SSD云盘。同样可参见本文档中 创建 SAP HANA 虚拟机 部分的第7点 - 存储配置示例。
- SAP HANA 数据库的**多工作节点**的 ECS 实例 ecs.se1.14xlarge，包括：56个 vCPU，480GB 内存，数据卷为数据量大于1.5 TB 的 SSD 云盘，日志卷和 HANA 共享卷均为大于 512GB 的 SSD 云盘。
- 您所选区域中的 VPC 具有自定义拓扑和可分配的 IP 地址范围，SAP HANA 数据库和其他 ECS 实例都会在这个 VPC 内启动。您也可以使用已存在的 VPC 来部署 SAP HANA。
- 您可以选择为您的 SAP HANA 和其他实例的公网出口配置互联网网关。本指南假定您正在使用此网关。
- ECS 安全组，用于限制实例间的访问。
- 高效云盘，使用标准为 2TB 的云盘为 SAP HANA 数据库做备份。
- ECS VM ecs.sn2.medium，配置 Windows 操作系统并托管 SAP HANA studio。
- ECS VM ecs.n1.medium，配置为堡垒机。

在阿里云上部署 SAP HANA

本节介绍如何在阿里云上部署多节点 SAP HANA 。

准备工作

阿里云账号

如果您还没有阿里云账号，可按照如下流程进行申请

- 进入注册流程。进入阿里云首页，点击页面右上方的 免费注册 。
- 按照页面提示进行信息填写。



- 获取短信验证码，确认完成注册。

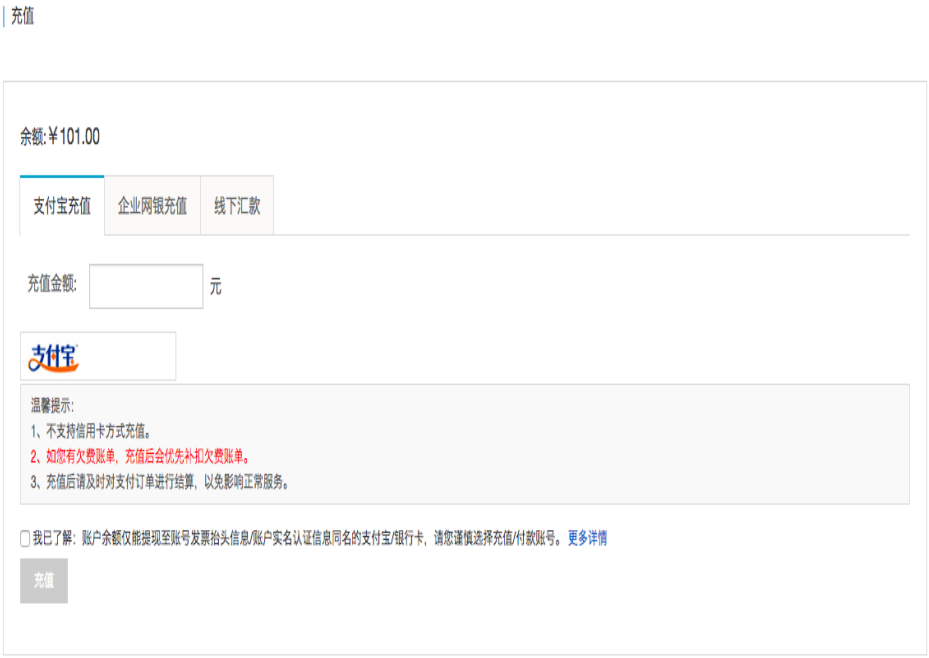


查看账户信息，确保有足够余额开通相关服务

- 登录后，进入用户中心->费用中心，点击充值，开始充值。



- 输入所需的金额，选择充值方式。



充值方式：**阿里云不支持任何方式的信用卡充值。**

- 支付宝充值（推荐）：为方便起见，推荐您使用支付宝在线充值，系统自动跳转到支付宝等待支付界面，输入相关信息，确认订单。如果没有支付宝，可以通过右侧页面创建新的支付宝账户，使用网银支付。
- 网银充值：如果您需要通过网上银行在线充值，可选择网上充值，选择**个人网银充值**或**企业网银充值**，充值成功后款项会实时充值到您的云帐号里面。
- 线下汇款：若您需要银行电汇到我方对公帐号上，您可点击“线下汇款”。阿里云线下汇款升级为招行专属账号方式；需要您先申请招行专属账号然后再通过招行专属账号进行汇款。受银行处理时间影响，采用非支付宝方式付款到账会有延误，强烈建议采用支付宝即时到账。

用户需要了解当前账号的**使用限制**，确保能够购买以下服务：

- 56 vCPU，480GB 内存规格的 ECS 实例（ecs.se1.14xlarge）
- SSD 云盘 （1.5TB X 1，512GB X 2）

- 高效云盘（2TB X 1）

若无法购买，可通过**工单方式**进行申请配额。

有关付款和帐户充值的更多细节可以参照 https://help.aliyun.com/knowledge_detail/37107.html

SAP HANA 安装介质

1.下载 SAP HANA 安装介质
请参考 SAP HANA Server Installation and Update

2.开通 OSS 服务

- 登录阿里云官网
- 点击 OSS 产品详情页 http://www.aliyun.com/product/oss/ 中的 **立即开通**
- 开通服务后，点击 **管理控制台** 直接进入 OSS 管理控制台界面

3.创建存储空间

- 进入 **OSS 管理控制台** 界面。
- 单击 **新建 Bucket**，**新建 Bucket 对话框**将弹出。
- 在 **BucketName** 框中，输入存储空间名称。存储空间的命名必须符合命名规范。所选定的存储空间名称在阿里云 OSS 的所有现有存储空间名称中必须具有唯一性。创建后不支持更改存储空间名称。有关存储空间命名的更多信息，请参阅 **OSS 基本概念介绍** 。



- 在 **所属地域** 框中，下拉选择该存储空间的数据中心。订购后不支持更换地域。如需要通过 ECS 内网访问 OSS，需要选择与您 ECS 相同的地域。更多信息请参阅 **访问域名** 。
- 在 **读写权限** 框中，下拉选择对应的权限。
    - **公共读写**：任何人（包括匿名访问）都可以对该存储空间中的文件进行读写操作，**所有这些操作产生的费用由该存储空间的创建者承担，请慎用该权限。**
    - **公共读**：只有该存储空间的创建者可以对该存储空间内的文件进行写操作，任何人（包括匿名访问）可以对该存储空间中的文件进行读操作。
    - **私有**：只有该存储空间的创建者可以对该存储空间内的文件进行读写操作，其他人无法访问该存储空间内的文件。
- 单击 **提交**。存储空间创建完成。

4.上传文件

- 进入 OSS 管理控制台界面。
- 单击您要向其中上传文件的存储空间名称，打开该存储空间管理页面。
- 单击 **Object 管理**，进入该存储空间内所有文件管理页面。



- 单击 **上传文件**，打开文件选择对话框。
- 选择 HANA 安装包，然后单击 **打开**。文件上传成功，点击 **刷新** 按钮查看已上传的文件。

选择区域和可用区

可用区（Zone）

- 可用区是指在同一地域内，电力和网络互相独立的物理区域。同一可用区内的 ECS 实例网络延时更小。
- 在同一地域内可用区与可用区之间内网互通，可用区之间能做到故障隔离。是否将云服务器 ECS 实例放在同一可用区内，主要取决于对容灾能力和网络延时的要求。
- 如果您的应用需要较高的容灾能力，建议您将 ECS 实例部署在同一地域的不同可用区内。
- 如果您的应用在实例之间需要较低的网络时延，则建议您将 ECS 实例创建在相同的可用区内。

地域介绍

阿里云数据中心目前提供华东 1、华东 2 、华北 1 、华北 2 、华北 3、华南 1 、香港、美国西部 1、美国东部 1、亚太东南 1、亚太东北 1、欧洲中部 1、中东东部 1 等地域。

- 华东 1、华东 2、华北 1 、华北 2、华北 3、华南 1 地域数据中心提供多线 BGP 骨干网线路，网络能力覆盖中国各省市，实现稳定高速中国大陆地域访问。
- 香港地域数据中心提供国际带宽访问，覆盖香港、东南亚等地域。
- 亚太东南 1 数据中心合作伙伴为 SingTel（新加坡电信），是东南亚优势运营商，公司业务能力、成熟度各方面非常可靠，可以满足周边用户需求。
- 亚太东南 2 数据中心位于澳大利亚的悉尼。
- 亚太东北 1 数据中心位于日本东京。
- 美国西部 1 地域数据中心位于美国西部硅谷，通过 BGP 线路直接接连多家美国运营商骨干网，可覆盖全美，同时可以很好的辐射南美洲和欧洲大陆。
- 美国东部 1 地域数据中心位于美国东部弗吉尼亚。
- 欧洲中部 1 数据中心位于德国法兰克福。
- 中东东部 1 数据中心位于阿联酋的迪拜。

如何选择地域

中国大陆地域

一般情况下建议选择和您目标用户所在地域最为接近的数据中心，可以进一步提升用户访问速度。不过，在基础设施、BGP 网络品质、服务质量、云服务器操作使用与配置等方面，阿里云中国大陆地域数据中心没有太大区别。中国大陆 BGP 网络可以保证全国地域的快速访问。

国际地域

国际地域提供国际带宽，主要面向非中国大陆地区用户。如果您在中国大陆，访问延迟可能稍高，不建议您使用。

- 对香港、东南亚有需求的用户，可以选择香港地域或亚太东南 1 地域。
- 对日、韩有需求的用户，可以选择亚太东北 1 地域。
- 对澳大利亚地区有需求的用户，可以选择亚太东南 2 地域。
- 对美洲有需求用户，可以选择美国地域。
- 对欧洲大陆有需求的用户，可以选择欧洲中部 1 地域。
- 中东用户，可以选择中东东部 1 地域。

不同地域之间的阿里云产品，内网不互通

- 不同地域的云服务器 ECS、关系型数据库 RDS、开放存储服务 OSS 内网不互通。
- 不同地域之间的云服务器 ECS 和其他云资源，如 RDS、OSS 等内网不互通 。
- 不同地域之间的云服务器 ECS 不能跨地域部署负载均衡，即在不同的地域购买的 ECS 实例不支持跨地域部署在同一负载均衡实例下。
- 单个 VPC 只能部署在一个区域，不同区域的 VPC 之间默认无法通信，用户可以根据自己的实际运行环境进行选择。

账号管理

SAP HANA 账号

SAP HANA 安装时需要指定 SID，HANA 安装过程中会使用<sid>adm作为该HANA的系统账号（非 HANA 数据库账号），如账号不存在，HANA 则会默认创建该账号。在个人使用过程中，需要避免使用以 adm 结尾的用户，以免出现账号与 HANA 重复导致账号下信息被 HANA 强制修改的情况。此外，在 scale out 场景中，所有的节点均需要使用同样的<sid>adm并且保证 uid，gid 一致。

系统内部账号

阿里云不会在系统内预创建任何账号，Linux 系统默认只有 root 用户。在系统的使用过程中，用户可以在满足操作系统要求情况下随意创建或删除用户账号。如 Linux 下可通过 useradd 和 userdel 来管理账号。

创建用户：useradd –u <uid> -g <gid> username
删除用户：userdel username

部署流程

配置网络

创建 VPC 和交换机

- 登录专有网络管理控制台。
- 在左侧导航栏，单击专有网络。
- 在专有网络列表页面，选择专有网络的所属地域，然后单击创建专有网络。
- 在创建专有网络对话框，输入专有网络名称并选择专有网络的网段。

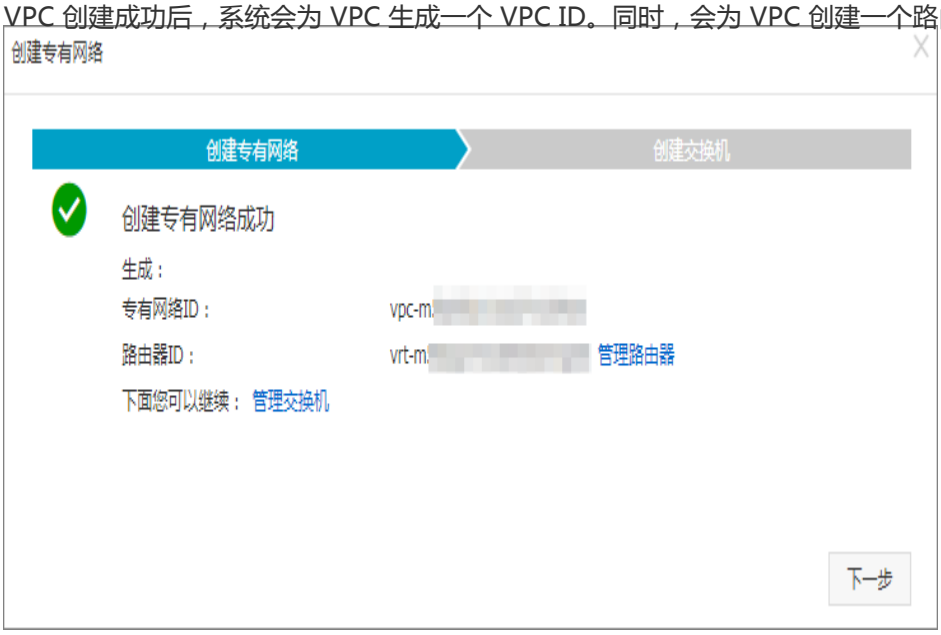
您可以选择以下三个标准私网网段。专有网络创建后，网段无法修改。建议使用较大的网段，尽量避免后续扩容。

```
10.0.0.0/8（10.0.0.0 - 10.255.255.255）
172.16.0.0/12（172.16.0.0 - 172.31.255.255）
192.168.0.0/16（192.168.0.0 - 192.168.255.255）
```



单击 **创建VPC**。

VPC 创建成功后，系统会为 VPC 生成一个 VPC ID。同时，会为 VPC 创建一个路由器。



单击 **下一步** 创建交换机。

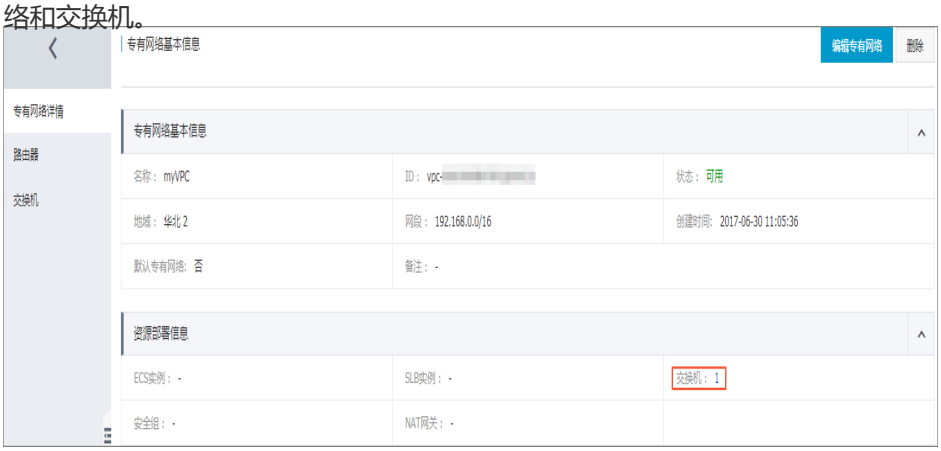
在 **创建交换机** 页签，输入以下信息，然后单击 **创建交换机**。
名称：指定交换机的名称。
可用区：选择交换机的可用区。
网段：指定交换机的网段。

交换机的网段可以和其所属的 VPC 网段相同或者是其 VPC 网段的子网；交换机的网段的大小在16位网络掩码与29位网络掩码之间。

注意：如果您的交换机网段和所属 VPC 网段相同，您只能在该 VPC 下创建一台交换机。

单击 **完成**

返回实例列表页面，单击创建的专有网络的ID链接，进入专有网络详情页面，查看专有网络和交换机。



配置安全组

安全组介绍

安全组是一个逻辑上的分组，这个分组是由同一个地域（Region）内具有相同安全保护需求并相互信任的实例组成。每个实例至少属于一个安全组，在创建的时候就需要指定。同一安全组内的实例之间网络互通，不同安全组的实例之间默认内网不通。可以授权两个安全组之间互访。

安全组是一种虚拟防火墙，具备状态检测包（SPI：Stateful Packet Inspection）过滤功能。安全组用于设置单台或多台云服务器的网络访问控制，它是重要的网络安全隔离手段，用于在云端划分安全域。

- **安全组限制**
    - 单个安全组内的实例个数不能超过 1000。如果您有超过 1000 个实例需要内网互访，可以将他们分配到多个安全组内，并通过互相授权的方式允许互访。
    - 每个实例最多可以加入 5 个安全组。
    - 每个用户的安全组最多 100 个。
    - 对安全组的调整操作，对用户的服务连续性没有影响。
    - 安全组是有状态的。如果数据包在 Outbound 方向是被允许的，那么对应的此连接在 Inbound 方向也是允许的。
    - 安全组的网络类型分为经典网络和专有网络。
        - 经典网络类型的实例可以加入同一地域（Region）下经典网络类型的安全组。
        - 专有网络类型的实例可以加入同一专有网络（VPC）下的安全组。
- **安全组规则**
    - 安全组规则可以允许或者禁止与安全组相关联的云服务器 ECS 实例的公网和内网的入出方向的访问。
    - 您可以随时授权和取消安全组规则。您的变更安全组规则会自动应用于与安全组相关联的 ECS 实例上。
    - 在设置安全组规则的时候，安全组的规则务必简洁。如果您给一个实例分配多个安全组，则该实例可能会应用多达数百条规则。访问该实例时，可能会出现网络不通的问题。
    - **安全组规则限制**
        - 每个安全组最多有 100 条安全组规则。

安全组配置方法

- 登录 ECS控制台。
- 在左侧导航中，单击 **安全组**。
- 选择您需要创建安全组的地域。
- 点击 **创建安全组**。在显示的对话框中，输入如下信息：



- 点击确认，选择配置规则。



- 根据相应的说明来完成规范设置，建议只保留远程访问所需的端口。



端口配置参考

在 SAP HANA 部署过程中，我们选择使用专有网络 VPC，只需要设置出方向和入方向的规则，无需区分公网和私网。默认情况下，安全组规则为空。所以在新建 ECS 实例时，请确保所选安全组开放包含 22（Linux）或者 3389（Windows）端口，否则无法远程登录 ECS。

HANA Studio Windows 虚拟机

入方向			
协议类型	端口范围	授权对象	备注
TCP	3389	外网 IP	需要访问 HANA Studio 的所有 IP

出方向			
TCP	1	0.0.0.0/0（所有虚拟机）	允许从 Windows 虚拟机访问任何其他虚拟机

堡垒机

入方向			
协议类型	端口范围	授权对象	备注
TCP	22	外网 IP	需要访问堡垒机的所有 IP
出方向			
TCP	22	0.0.0.0/0（所有虚拟机）	允许从堡垒机访问任何其他虚拟机

更多有关于 SAP 需要访问的特定端口和相应安全组规则，请参见 SAP 官方文档

创建 SAP HANA 虚拟机

注意：在您创建实例和存储磁盘之前，请在阿里云支持门户网站提交一个工单，来获取在部署 SAP HANA 时 SSD 云盘的特殊支持。阿里云支持专家将与您联系，并介绍更多的细节。

进入阿里云云服务器 ECS 产品购买页面

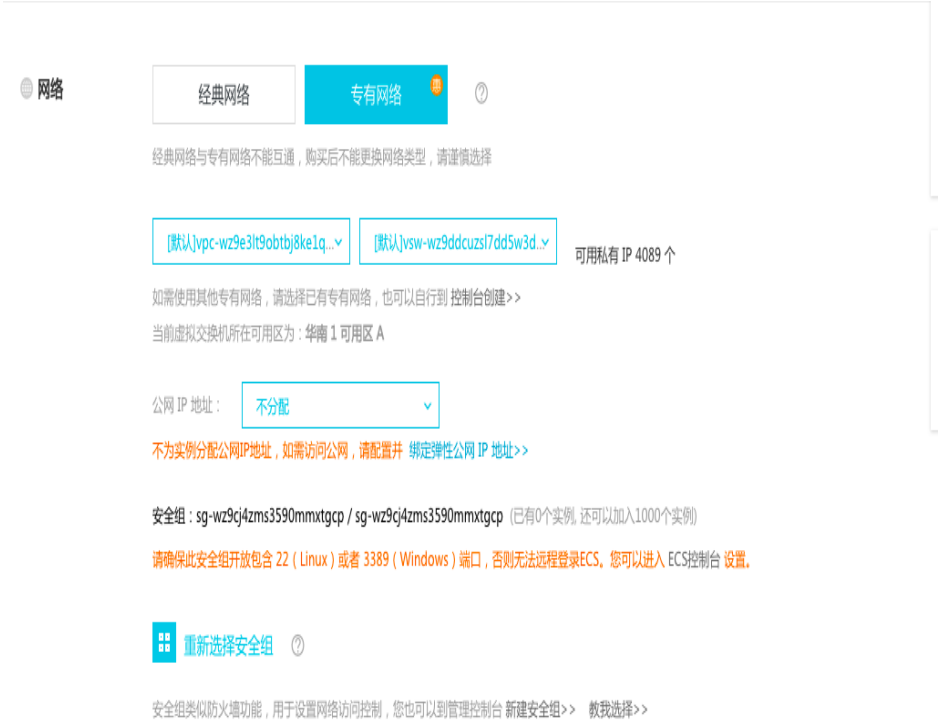
选择付费方式 **包年包月**

选择对应区域和可用区

根据之前的考虑选择对应的区域，如果有配置交换机信息，同时需要选择可用区。

网络类型选择专有网络

选择专有网络类型后，需要填写之前创建或者已有的 VPC 和交换机信息。在该多节点架构中，SAP HANA 不直接对外提供服务，因而选择不分配公网 IP。



选择实例规格

选择通过 SAP HANA 认证的实例类型，即系列III - 内存型 se1 实例规格族中的 56 vCPU 480GB规格（ecs.se1.14xlarge）。



选择操作系统镜像

认证的操作系统为 SUSE Linux Enterprise Server 12 SP1 for SAP Applications，相关镜像可在镜

像市场选取。



如果您对 SAP HANA 的性能有特殊的要求，建议您使用为运行 SAP HANA 定制的 SLES for SAP Applications 阿里云优化版，它包括 Linux 内核和 KVM 的修改。这个修正版本将由阿里云支持，在用户体验方面与标准的 SLES for SAP Applications 一致。请参考 操作系统使用说明 获取更多细节。

如果客户使用了阿里云的优化版本，在部署过程中遇到了问题，阿里云将直接解决问题或将客户运行环境转化为标准的 SLES for SAP Applications 操作系统，无需额外的费用。

当您使用这个修改后的版本，您需要确保默认参数 GRUB "nohz = off idle = dynamic" 不被删除或修改。

除此之外，这些修改是开源的在 GPL 的许可下。所有的变更阿里云已提交给 Linux 社区，将纳入 SLES 的新版本中。

配置存储磁盘

建议按如下配置选择存储磁盘：



配置初始化信息

设置好初始密码后，选择创建，需要等待几分钟来等待实例初始化完成

创建堡垒主机

类似上述步骤，在同一个可用区的同一个 VPC 内创建 1 vCPU / 2GB / 无额外存储 的堡垒主机。

配置堡垒主机网络

目前有多种配置公网 IP 的方式，这里以 EIP 配置为例。

弹性公网 IP（Elastic IP Address，简称 EIP），是可以独立购买和持有的公网 IP 地址资源，它能动态绑定到不同的 ECS 实例上，绑定时和解绑时无需实例停机。

- 登录弹性公网 IP 管理控制台
- 单击申请弹性公网 IP。
- 在购买页面，选择 EIP 的所属地域、带宽峰值和计费方式，然后单击立即购买并完成支付。
- 注意：EIP 的地域必须和要绑定的 ECS 实例的地域相同。
- 返回 EIP 列表页面，选择 EIP 的所属地域，单击刷新，查看已创建的 EIP 实例。
- 单击绑定。



- 在绑定弹性公网 IP 对话框，选择已经创建的 ECS 实例，然后单击确认。
- 绑定完成后，在 EIP 列表页面，单击刷新，查看 EIP 实例状态。
- 当 EIP 实例的状态变成已分配时，绑定了 EIP 的 ECS 实例就可以进行公网访问了。



- 登录 ECS 实例，运行以下命令，测试公网访问。

  ping www.aliyun.com



登录虚拟机

由于当前 HANA 虚拟机未配置公网，我们需要从堡垒主机上跳转到 HANA 虚拟机。

安装 SAP HANA 数据库

- 创建 /hana/data，/hana/log，/hana/shared 以及 /hana/backup 四个目录
- 按照 步骤7 中申请的磁盘规格和关系，对四个数据盘进行格式化和挂载
- 将 OSS 中的 SAP HANA 安装文件下载到本地 /hana/shared 目录
- 解压 SAP HANA 安装文件并进行安装，需要注意安装过程中的目录选择，以下是 master 节点安装的一个示例。

```
master:/hana/shared/122.05 # ./hdblcm
SAP HANA Lifecycle Management - SAP HANA 1.00.122.05.1481577062
************************************************************
Scanning Software Locations...
Detected components:
SAP HANA Database (1.00.122.05.1481577062) in /hana/shared/122.05/server
Choose installation
Index | System | Database Properties
-----------------------------------------------
1 | Install new system |
```

```
| |
2 | Extract components |
3 | Exit (do nothing) |
Enter selected system index [3]: 1 --> 新部署节点
Enter Installation Path [/hana/shared]: --> 选择共享目录
Enter Local Host Name [master]: --> 确保 hostname 可以访问
Do you want to add additional hosts to the system? (y/n) [n]: n
Enter SAP HANA System ID: AL1 --> 输入系统标示
Enter Instance Number [00]: 00 --> 输入实例号

Index | Database Mode | Description
-------------------------------------------------------------------------------------------
1 | single_container | The system contains one database
2 | multiple_containers | The system contains one system database and 1..n tenant databases

Select Database Mode / Enter Index [1]:

Index | System Usage | Description
-------------------------------------------------------------------------------
1 | production | System is used in a production environment
2 | test | System is used for testing, not production
3 | development | System is used for development, not production
4 | custom | System usage is neither production, test nor development

Select System Usage / Enter Index [4]:
Enter Location of Data Volumes [/hana/data/AL1]:
Enter Location of Log Volumes [/hana/log/AL1]:
Restrict maximum memory allocation? [n]:
Enter Certificate Host Name For Host 'master' [master]:
Enter SAP Host Agent User (sapadm) Password:
Confirm SAP Host Agent User (sapadm) Password:
Enter System Administrator (al1adm) Password: --> 输入用户密码
Confirm System Administrator (al1adm) Password:
Enter System Administrator Home Directory [/usr/sap/AL1/home]:
Enter System Administrator Login Shell [/bin/sh]:
Enter System Administrator User ID [1000]:
Enter ID of User Group (sapsys) [79]:
Enter Database User (SYSTEM) Password: --> 输入数据库用户密码
Confirm Database User (SYSTEM) Password:
Restart system after machine reboot? [n]:
Summary before execution:
=========================
SAP HANA Components Installation
Installation Parameters
Remote Execution: ssh
Installation Path: /hana/shared
Local Host Name: master
SAP HANA System ID: AL1
Instance Number: 00
Database Mode: single_container
System Usage: custom
Location of Data Volumes: /hana/data/AL1
Location of Log Volumes: /hana/log/AL1
Certificate Host Names: master -> master
System Administrator Home Directory: /usr/sap/AL1/home
System Administrator Login Shell: /bin/sh
```

```
System Administrator User ID: 1000
ID of User Group (sapsys): 79
Software Components
SAP HANA Database
Install version 1.00.122.05.1481577062
Location: /hana/shared/122.05/server

Do you want to continue? (y/n): y

Installing components...
Installing SAP HANA Database...
```

以上步骤为单节点 HANA 搭建流程，若需要搭建 scale-out 环境，需要继续进行下列步骤：

- 上述创建的 HANA 为 master 节点，在该节点上配置 NFS 服务，将 /hana/shared 和 /hana/backup 配置为共享目录
- 重复步骤 1-8，在同一个 VPC 内创建 worker node（工作节点）虚拟机，注意 worker node 的存储只需配置 /hana/data 和 /hana/log 两个磁盘
- 将 master 节点上的 /hana/shared 和 /hana/backup 目录挂载到 worker node 上
- 配置所有节点的 /etc/hosts 文件，确保可以解析所有节点的 hostname 和 ip 对应关系
- 在 master 节点上执行 hdblcm 来添加 worker node

为 SAP HANA Studio 创建 Windows 虚拟机

1. 参考上个过程中的步骤 1-8，来创建 SAP HANA Studio 虚拟机需注意以下几点：
    - 不需要配置额外存储空间
    - 镜像方面需要 Windows 镜像
    - 采用不分配公网 IP 的策略
2. 重复上个过程中步骤 10，为虚拟机配置公网 IP
3. 通过公网 IP 连入虚拟机
4. 安装SAP HANA Studio

为什么需要使用 堡垒机 和 SAP HANA Studio ?

SAP HANA 的虚拟机没有公共 IP，需要使用堡垒机和 SAP HANA Studio 来访问 SAP HANA。SAP HANA Studio 实例和堡垒机部署在与 SAP HANA 实例相同的 VPC 中，所以它们可以直接相互访问。

通常堡垒机是 Linux 操作系统，用于 SSH 访问；而 SAP HANA Studio 部署在 Windows 操作系统，是用于管理 HANA。Linux 虚拟机难以直接访问 Windows 虚拟机，因此我们将 Windows 虚拟机配置公用网络 IP，这样我们就可以通过互联网登录 SAP HANA Studio。

连接 SAP HANA

请注意，由于以上部署不会为你的 SAP HANA 实例配置公网 IP，所以您只能通过堡垒机使用 SSH 或通过部署在 Windows 虚拟机上的 SAP HANA Studio 连接到 SAP HANA 实例。

- 要通过堡垒机实例连接到 SAP HANA，请使用您选择的 SSH 客户端连接到堡垒机，然后再连接到 SAP HANA 实例。
- 要通过 SAP HANA Studio 连接到 SAP HANA 数据库，请使用远程桌面客户端连接到 Windows 虚拟机实例。连接后，手动安装 SAP HANA Studio 并开始访问 SAP HANA 数据库。

需要在部署后执行的任务

在使用 SAP HANA 实例之前，我们建议您执行以下部署后步骤（另见 SAP HANA 安装和更新指南）。

- 使用为 SAP 应用程序定制的 SUSE Linux Enterprise Server 作为 SAP HANA 实例的操作系统，需确保 Linux 内核版本至少为 3.12.74-60.64.40，以避免在某些情况下 HANA 性能下降。如果内核版本低于 3.12.74-60.64.40，请将内核升级为最低需求版本。请参阅 SAP Notes 2205917。
- 如果您使用的是为 SAP 应用程序定制的，并且内核已被阿里云优化的 SUSE Linux Enterprise Server 操作系统，请注意当您计划更新内核或给内核打补丁时，请查阅操作系统使用说明。
- 更新 SAP HANA 软件至最新版本。
- 安装其他额外的组件，如应用函数库（AFL）或智能数据访问（SDA）。
- 配置和备份您的新 SAP HANA 数据库，请参阅 在阿里云上的 SAP HANA 备份和恢复指南。

SAP HANA 操作指南

- 管理你的 SAP HANA 系统
    - 启动和停止你的 ECS 实例
    - 创建你的 SAP HANA 自定义镜像
    - 复制你的 SAP HANA 系统
- 管理你的账号
- 网络设置
    - 安全隔离
    - 访问公网
    - VPN 连接
    - 安全组
- 设置 SAProuter 接入 SAP 技术支持
- 安全配置
    - 资源访问控制
    - 安骑士（服务器安全）
    - 安全消息通知
    - 必要的配置变更
    - 停用某些 SAP HANA 服务
- 高可用性以及灾备
- 备份与恢复

- 附录：如何创建 NAT 网关

本文档着重介绍对于部署在阿里云云服务器 ECS 上的 SAP HANA 系统的推荐使用方法以及注意事项，更多 SAP HANA 使用方法，请参考 SAP 的官方文档。

管理你的 SAP HANA 系统

本节介绍对于部署在云服务器 ECS上 的 SAP HANA 系统，如何进行典型的系统管理任务，如系统启动、系统暂停、系统复制等。

启动和停止你的 ECS 实例

你可以在任何时候停止一个或者多个 SAP HANA 主机，但是作为建议，请尽量先将 SAP HANA 停止运行，然后再将其所在云服务器 ECS 实例停止。当该实例重新启动之后，其 IP 地址、网络和存储配置等保持不变。

创建你的 SAP HANA 自定义镜像

云服务器 ECS 允许用户根据现有的 ECS 实例创建自定义镜像，使用自定义镜像能够帮助用户快速创建多个操作系统和运行环境配置相同的 ECS 实例，以满足客户灵活扩容的需求。你可以通过云服务器 ECS 控制台来为你现有的 ECS 实例创建自定义镜像，具体信息和操作步骤请参见文档 使用实例创建自定义镜像。

你可以使用自定义镜像

- 创建一个完整的 SAP HANA 系统离线备份，包括操作系统、HANA 程序 /usr/sap、共享程序和文件 /hana/shared、以及数据、日志和备份文件；
- 创建新的 ECS 实例 或者 更改 ECS 实例的系统盘；
- 跨地域移动一个 SAP HANA 系统：用户可以对已有 ECS 实例创建自定义镜像，然后在另一个地域使用该镜像创建新的 ECS 实例，复制过程请参见文档 复制镜像；镜像复制可以使得用户在跨地域部署应用时轻松达成部署环境的一致性；
- 复制 SAP HANA 系统：用户可以为已有 SAP HANA 系统创建镜像，并用它来复制出一个完全相同的 SAP HANA 系统，下节会具体进行介绍。

> 注意：为了保证创建的自定义镜像与 SAP HANA 系统保持一致的状态，你需要在创建镜像之前先停止你的 SAP HANA 实例，或者按照 SAP Note 1703435 来操作。

复制你的 SAP HANA 系统

单节点系统 – 克隆一个单节点的 SAP HANA 系统，可以通过在同一个可用区之内创建该系统的自定义镜像，镜像中既包含操作系统也包含安装好的 SAP HANA 软件。

多节点系统 – 多节点的 SAP HANA 系统虽然无法通过直接克隆得到，但是可以通过备份与恢复的方法创建出多个节点，如以下步骤:

- 创建一个与克隆目标配置一样的 SAP HANA 系统
- 在源系统上做数据备份
- 在新系统上恢复备份数据

管理你的账号

管理你在阿里云上的 SAP HANA 系统，需要3类管理员账户

- **阿里云账户** – 在使用任何阿里云产品和服务之前，需要先创建你的阿里云账号。使用该账号，你可以管理你的云服务器，对网络进行配置，管理你的系统镜像和磁盘快照等。
- **云服务器 ECS 实例的管理员账户** – 在云服务器 ECS 实例创建后，你需要在该实例的操作系统中创建一个管理员账户。Linux 系统默认的管理账户是 root。作为管理员，你可以按照操作系统的要求来创建和删除用户账户。
- **HANA 数据库管理账户** – 在 SAP HANA 安装过程中，需要指定一个系统 ID（SID），而且 HANA 会使用 [sid]adm 作为 HANA 管理员用户，并且默认在操作系统上创建该用户。此外需要说明的是，在横向扩展（scale-out）场景中，所有节点都会使用相同的管理员账户 [sid]adm，并且确保 UID 与 GID 一致。

网络设置

我们强烈推荐你使用专有网络 VPC 作为你在阿里云云服务器 ECS 上搭建你的 SAP HANA 系统时使用的默认网络类型。专有网络 VPC（Virtual Private Cloud）是基于阿里云构建的一个隔离的网络环境，专有网络之间逻辑上彻底隔离。你能够在自己定义的虚拟网络中使用阿里云资源。

你可以完全掌控自己的虚拟网络，例如选择自己的 IP 地址范围、划分网段、配置路由表和网关等，从而实现安全而轻松的资源访问和应用程序访问。更多产品信息，请参考文档 专有网络VPC。你也可以通过专线或 VPN 等连接方式将你的专有网络与传统数据中心相连，形成一个按需定制的网络环境，实现应用的平滑迁移上云和对数据中心的扩展。

安全隔离

- 不同用户的云服务器部署在不同的专有网络里。
- 不同专有网络之间通过隧道 ID 进行隔离。专有网络内部由于交换机和路由器的存在，所以可以像传统网络环境一样划分子网，每一个子网内部的不同云服务器使用同一个交换机互联，不同子网间使用路由器互联。
- 不同专有网络之间内部网络完全隔离，只能通过对外映射的 IP（弹性公网 IP 和 NAT IP）互联。
- 由于使用隧道封装技术对云服务器的 IP 报文进行封装，所以云服务器的数据链路层（二层 MAC 地址）信息不会进入物理网络，实现了不同云服务器间二层网络隔离，因此也实现了不同专有网络间二层网络隔离。
- 专有网络内的 ECS 使用安全组防火墙进行三层网络访问控制。

访问公网

如果用户的企业安全策略要求所有的虚拟机要位于企业私网环境之内，这时对于必要的访问公网能力可以通过以下方式达到：

- 在用户私网中搭建 NAT 网关，提供 NAT 代理为私网环境提供一个公网流量的出入口。在 NAT 网关中配置对应的路由即可使你的虚拟机能够访问公网。关于 NAT 网关的搭建，请参考 附录：如何创建 NAT 网关
- 由于用户不允许使用 SSH 直接连接私网中的虚拟机，因此你需要搭建一台堡垒机。该堡垒机具有公网 IP 地址，并可以对 SSH 运维协议的数据流进行全程记录,堡垒机可以作为你连通私网中虚拟机的通道。搭建堡垒机的具体步骤，请参见 阿里云上 SAP HANA 实施指南

VPN 连接

阿里云也提供了 VPN 网关（VPN Gateway）服务，它是一款基于 Internet，通过加密通道将企业数据中心和阿里云专有网络（VPC）安全可靠连接起来的服务。

安全组

安全组是一个逻辑上的分组，这个分组是由同一个地域（Region）内具有相同安全保护需求并相互信任的实例组成。每个实例至少属于一个安全组，在创建的时候就需要指定。同一安全组内的实例之间网络互通，不同安全组的实例之间默认内网不通。可以授权两个安全组之间互访。安全组是一种虚拟防火墙，具备状态检测包（SPI：Stateful Packet Inspection）过滤功能。安全组用于设置单台或多台云服务器的网络访问控制，它是重要的网络安全隔离手段，用于在云端划分安全域。

更多信息，请参见 安全组介绍，ECS 安全组实践（一），ECS 安全组实践（二），ECS 安全组实践（三）。

设置 SAProuter 接入 SAP技术支持

SAProuter 是一个用来远程连接客户网络和 SAP 网络的软件。由于在某些情况下，SAP 技术支持工程师需要访问你在阿里云上的 SAP HANA 系统来进行必要的问题诊断，这时需要借助 SAProuter 来完成访问连接。而使用 SAProuter 的一个先决条件是用户和 SAP 之间的网络连接可用。

你可以认为 SAProuter 是一条在 SAP 和阿里云云服务器 ECS 之间的技术支持连接通道，配置 SAProuter 请参见如下步骤：

- 启动安装有 SAProuter 软件的云服务器 ECS 实例。由于该实例位于用户的私有网络（VPC）中，用户需要购买弹性公网 IP (EIP）并动态绑定到该 ECS 实例上。绑定过程无需重新启动 ECS 实例。
- 创建并配置一个安全组，该安全组仅允许该 SAProuter 实例和 SAP 技术支持网络之间的，通过3299 TCP 端口的入站和出站访问
- SAProuter 的安装指南，请参见 SAP Note 1628296，安装过程中还需要创建一个命名为 saprouttab 的文件。
- SAProuter 所需要的公网连接需要使用安全的网络通信（Secure Network Communication），更

多信息请参见 SAP Remote Support – Help 。

安全配置

对于一个运行在阿里云上的 HANA 系统，阿里云会负责云基础设施层面上的安全防护，而用户需要负责他们使用的云资源、HANA 数据库和其它相关应用的安全防护。

除了你常用的 SAP HANA 系统安全防护方法之外，阿里云还提供了下列一些额外的安全防护能力：

资源访问控制

RAM (Resource Access Management) 是阿里云为客户提供的用户身份管理与资源访问控制服务。使用 RAM，你可以创建、管理用户账号（比如员工、系统或应用程序），并可以控制这些用户账号对你名下资源具有的操作权限。你可以通过访问控制安全地将阿里云资源的访问及管理权限按需分配给你指定的企业成员或者合作伙伴，从而降低您的企业信息安全风险。更多信息请参见 访问控制。

安骑士（服务器安全）

安骑士是一款主机安全软件，通过安装在云服务器上轻量级的软件和云端安全中心的联动，为您提供漏洞管理、基线检查和入侵告警等功能。安骑士可以实时监控并精准捕获服务器上各种安全事件，并对入侵和异常行为进行警告和提供解决方案。更多信息，请参见文档 安骑士。

安全消息通知

用户可以在阿里云消息中心中设置自己的消息订阅渠道，可以选择邮件或者短信通知。请确保在安全消息中选择接收云盾安全信息通知，你将收到服务器安全和基础 DDoS 防护相关的安全通知。如果你购买了高级 DDoS 防护、Web 应用防火墙等服务，你也会收到相应的通知。

必要的配置变更

请参考推荐的安全设置来配置你的 SAP HANA 系统和你所使用的操作系统。例如，确保仅有必须使用的网络端口被加入访问限制白名单，对运行 SAP HANA 的操作系统进行安全防护加固，等等。

以下 SAP note 供你参考:

- 1944799: Guidelines for SLES SAP HANA installation
- 1730999: Recommended configuration changes
- 1731000: Unrecommended configuration changes

停用某些SAP HANA服务

SAP HANA的某些可选服务，在无需使用时可以停用，比如 HANA 扩展应用服务（HANA Extended

Application Services）。

请参考 SAP Note 1697613: Remove XS Engine out of SAP HANA database 了解具体操作步骤。在该服务被停用后，请将对该服务开放的所有 TCP 端口从安全组设置中移除。

更多与安全防护相关的信息，请参见 SAP HANA 在阿里云上的安全指南。

高可用性以及灾备

对于运行在阿里云上的 SAP HANA 进行高可用方案和灾备方案搭建，更多细节和最佳实践请参见 SAP HANA 在阿里云上的高可用和灾备指南。

备份与恢复

备份对于保护你的系统数据至关重要。SAP HANA 作为内存数据库，你可以为它创建定期的数据备份，其中备份时间点可以根据你的业务情况，选择在工作负载量较小的时候进行备份。这样当遇到意外的系统故障时，你可以从容恢复你的数据。

更多细节和最佳实践请参见 SAP HANA 在阿里云上的备份和恢复指南。

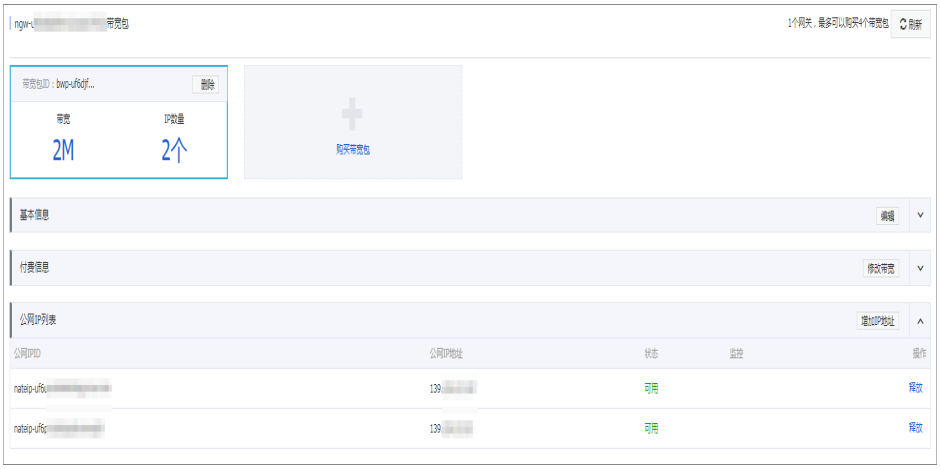
附录：如何创建 NAT 网关

NAT 网关（NAT Gateway）是一款企业级的 VPC 公网网关，提供 NAT 代理（SNAT、DNAT）、10Gbps 级别的转发能力、以及跨可用区的容灾能力。NAT 网关与共享带宽包配合使用，可以组合成为高性能、配置灵活的企业级网关。

1. 登录 VPC 管理控制台。
2. 在左侧导航栏，单击 NAT 网关。
3. 单击创建 NAT 网关。
4. 选择地域、VPC、规格和计费周期配，单击立即购买，完成创建。
5. NAT 网关创建成功后，系统会自动为 NAT 网关创建一张端口转发表和 SNAT 表。



6. 单击购买带宽包链接。
   注意：如果 NAT 网关已经配置了带宽包，则单击管理，然后在左侧导航栏选择带宽包。
7. 在带宽包页面，再次单击购买带宽包。
8. 配置带宽包，配置公网 IP 个数、带宽、计费方式。
9. 单击立即购买，完成创建。
10. 带宽包创建后，系统会根据指定的 IP 个数分配公网 IP 供 NAT 网关使用。



11. 返回 NAT 网关页面，单击端口转发表，设置 DNAT，然后单击创建端口转发条目。
12. 配置端口转发条目, 选择一个可用的公网 IP，指定要映射的专有网络 EC S实例的私网 IP，选择映射方式。
    - 所有端口：该方式属于 IP 映射，等同于为所选的 ECS 实例配置了一个弹性公网 IP。该 ECS 实例可以接收来自公网任何端口、任何协议的请求。
      选择所有端口后，无需再配置公网端口、私网端口和协议类型。
    - 具体端口：该方式属于端口映射。配置后，NAT 网关会将收到的指定协议的 [私网 IP:私网端口] 的数据发向指定的 [公网 IP:公网端口]，并将来自 [公网 IP:公网端口] 指定协议的数据发送给指定的 [私网 IP:私网端口]。
      选择具体端口后，需要配置公网端口、私网端口和协议类型。
13. 单击确定，完成配置。
    端口转发条目列表中会新增添加的转发规则，显示状态为配置中。单击刷新，当转发条目的状态显示为可用，则表示该端口转发规则创建成功。



SAP HANA 备份和恢复

- 使用阿里云服务支持 SAP HANA 数据库的备份与恢复
  - 对象存储 OSS
  - 云服务器 ECS
  - 访问控制 RAM
- SAP HANA 数据库备份在阿里云上的最终存放地
- 备份文件的权限管理

- 关于备份与恢复的一些要点
  - SAP HANA 备份和存储快照
  - 针对多节点 SAP HANA 系统的文件系统备份
  - 恢复
- 非生产系统的 SAP HANA 数据库的备份与恢复
  - 备份方式
  - 恢复方式
- 生产系统 SAP HANA 数据库的备份与恢复
  - 备份方式
  - 备份示例
  - 恢复方式
  - 恢复示例

对于 SAP HANA 数据库的备份与恢复，建议请先阅读以下 SAP 官方文档

相关文档
SAP Note 1642148 FAQ SAP HANA Database Backup & Recovery
SAP Note 2091951 Best Practice: SAP HANA Backup & Restore
SAP HANA Administration Guide

使用阿里云服务支持 SAP HANA 数据库的备份与恢复

对象存储 OSS

对象存储服务 Object Storage Service（简称 OSS），是阿里云提供的海量、安全、低成本、高可靠的云存储服务。您可以在任何时间、任何地点上传和下载数据，也可以通过 Web 控制台对数据进行简单的管理。OSS 按实际容量付费。OSS 在阿里云上 SAP HANA 数据库的备份与恢复中扮演一个关键角色。关于 OSS 更详细的介绍，请查阅阿里云 OSS 的相关文档 https://help.aliyun.com/product/31815.html

云服务器 ECS

云服务器 Elastic Compute Service（简称 ECS）是阿里云提供的一种基础云计算服务。使用云服务器 ECS 就像使用水、电、煤气等资源一样便捷、高效。您无需提前采购硬件设备，而是根据业务需要，随时创建所需数量的云服务器实例，并在使用过程中，随着业务的扩展，对云服务器进行扩容磁盘、增加带宽。如果不再需要云服务器，也可以方便的释放资源，节省费用。

ECS的主要能力:

- **ECS实例**

云服务器 ECS 实例是一个虚拟的计算环境，包含了 CPU、内存、操作系统、磁盘、网络等最基础的服务器组件，是 ECS 提供给每个用户的操作实体。一个实例就等同于一台虚拟机，您对所创建的实例拥有管理员权限，可以随时登录进行使用和管理。您可以在实例上进行基本操作，如挂载磁盘、创建快照、创建镜像、部署环境等。

- **镜像**

镜像是指 ECS 实例可选择的运行环境模板，一般包括操作系统和预装的软件。镜像可以仅包含基本的操作系统，也可以在此基础上整合具体的软件环境。用户基于镜像来创建 ECS 实例，从而获得与镜像一致的系统环境。

- **地域与可用区**

地域是指物理的数据中心。

可用区是指在同一地域内，电力和网络互相独立的物理区域。同一可用区内的 ECS 实例网络延时更小。

在同一地域内可用区与可用区之间内网互通，可用区之间能做到故障隔离。是否将云服务器 ECS 实例放在同一可用区内，主要取决于对容灾能力和网络延时的要求。

- **块存储（Block Storage）— 云盘**

块存储（Block Storage），是阿里云为云服务器 ECS 提供的低时延、持久性、高可靠的数据块级随机存储。块存储支持在可用区内自动复制您的数据，防止意外的硬件故障导致数据不可用，以保护您的业务免于组件故障的威胁。就像对待硬盘一样，您可以对挂载到 ECS 实例上的块存储做格式化、创建文件系统等操作，并对数据持久化存储。根据不同应用场景的需要，我们提供三种类型的块存储选项（SSD 云盘/高效云盘/普通云盘）。

- **云盘快照**

为磁盘创建的数据还原点，包含特定时刻磁盘的数据，可以用于还原磁盘数据或创建自定义镜像。

更多 ECS 详细介绍，请查阅阿里云 ECS 相关文档 https://help.aliyun.com/product/25365.html

访问控制 RAM

访问控制 RAM (Resource Access Management) 是阿里云提供的资源访问控制服务。通过 RAM，您可以在您的云账户下创建多个 RAM 用户，并给这些用户分配相应的资源操作权限；这样，您就可以集中管理您的用户（比如员工、系统或应用程序），以及控制用户可以访问您名下资源的权限。

当您使用 OSS 来保存 SAP HANA 数据库的备份文件的时候，您可以通过 RAM 来授权特定的用户访问备份文件。关于更多 RAM 的相关信息，请访问阿里云 RAM 相关文档
https://help.aliyun.com/product/28625.html

SAP HANA 数据库备份在阿里云上的最终存放方式

在传统的物理机上备份 SAP HANA 数据库，与阿里云上最大的不同是：备份存放的最终目的地。传统物理机上数据库备份的最终存放地通常是磁带；而在阿里云上，则是 OSS。将 SAP HANA 数据库的备份存放在 OSS 上有诸多好处：OSS 默认会自动存放3份数据拷贝在不同地点来保证 99.999999999% 数据可靠性；可以提供企业级多层次安全防护、多用户资源隔离机制，支持异地容灾机制，提供多种鉴权和授权机制及白名单、防盗链、主子账号功能等。

SAP HANA 数据库的备份，首先会被保存在 ECS 实例挂载的数据云盘中的 /hana/backup 目录，接着用户需要将云盘中的备份文件拷贝到 OSS 中做长期保存。

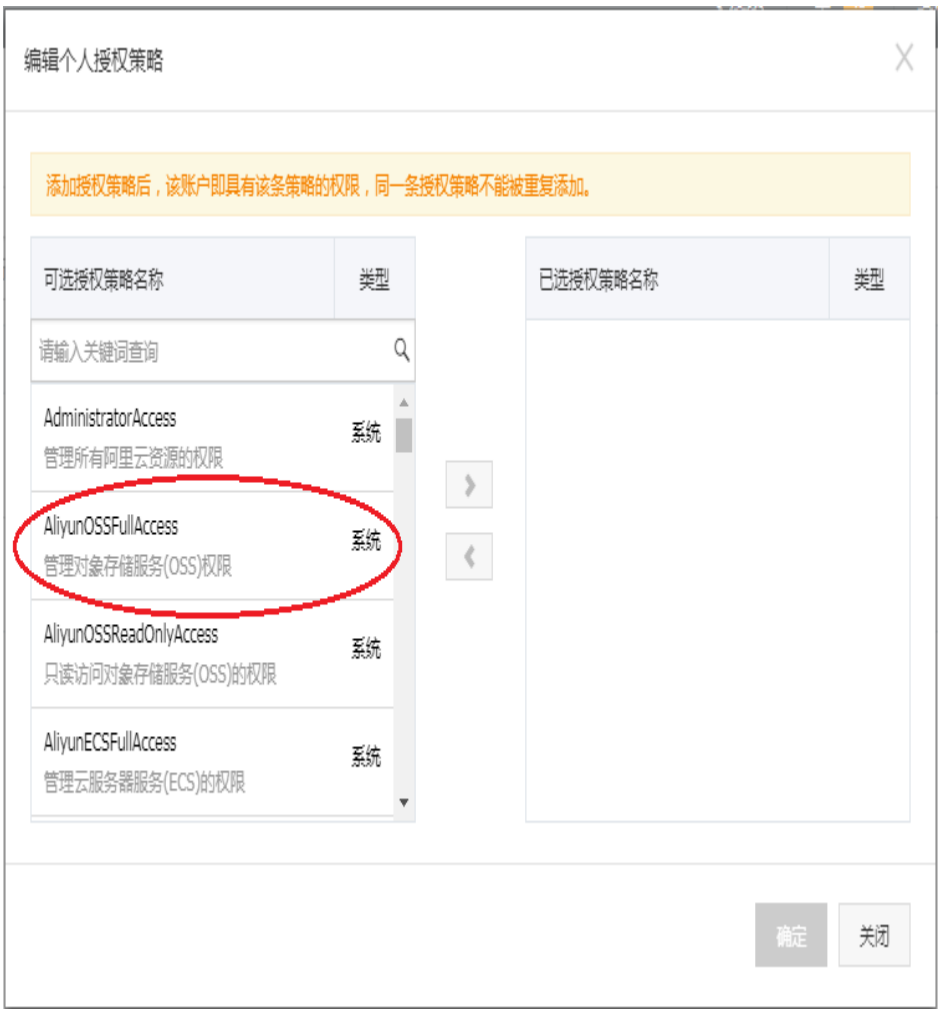
备份文件的权限管理

为了授权用户访问 OSS Bucket 中存放的 SAP HANA 备份文件，您需要在 RAM 工作台中配置用户访问规则，具体步骤如下：

选择需要访问 OSS 的用户，并且点击“授权”

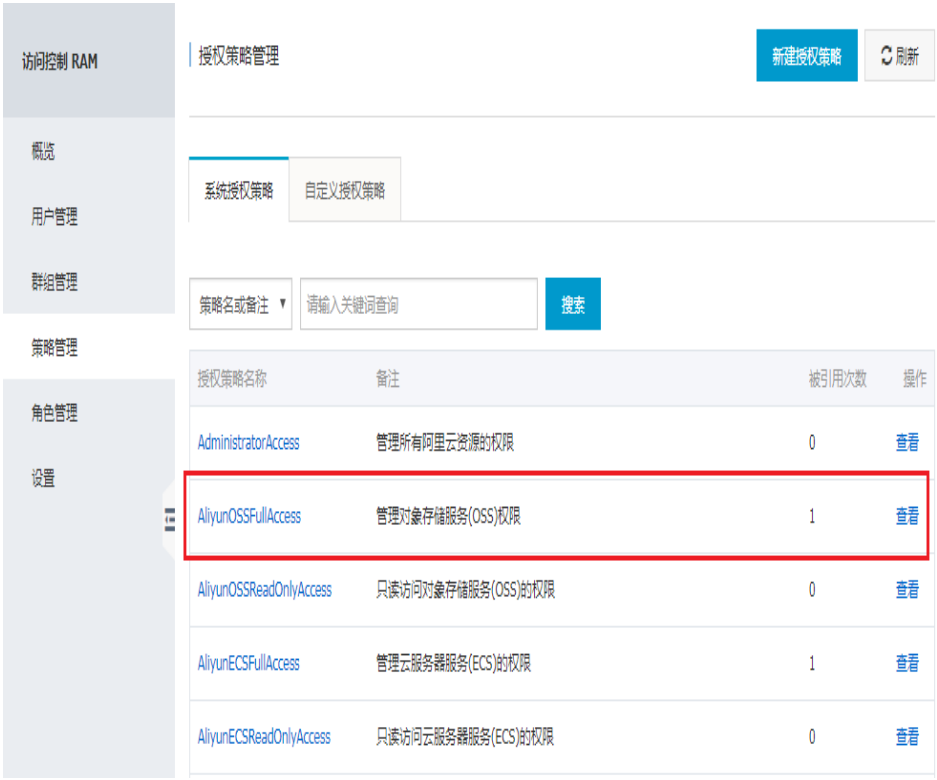


选择授权规则



作为阿里云账户的所有人，您会被要求输入验证码（验证码会发送到您注册的手机）

在验证码输入通过之后，您可以在授权规则面板检查和设置用户相应的访问授权



在授权规则面板，您也可以创建定制化的授权规则。关于权限管理的更多内容，请参见 RAM 授权策略管理

关于备份和恢复的注意事项

在您开始为您在阿里云上的 SAP HANA 系统准备相应的备份策略之前，您应该了解以下关于备份（这里指文件系统备份）、存储快照（云盘快照）、以及恢复的一些要点。

为 SAP HANA 数据库的文件、数据、日志等进行文件系统备份，是 SAP HANA 数据安全的主要措施之一。您还可以通过阿里云 ECS 云盘的快照功能，定期为 SAP HANA 的日志和数据文件系统所在的数据盘进行快照备份。

SAP HANA 备份和存储快照

- 默认情况下，SAP HANA 数据库的备份文件，会保存在/hana/backup中。
- 采用存储快照作为备份方式，在阿里云上也是支持的。
- 数据和日志只能支持在 SAP HANA 数据库联机时被备份（当所有配置的服务正在运行）。
- 当正在创建数据备份、日志备份和存储快照时，数据库可照常使用。
- 在完成初始数据备份或存储快照之前，日志模式“覆盖”是激活的。在日志模式为覆盖时，不会产生日志备份。
- 不能备份和恢复单个数据库对象，备份和恢复始终适用于整个数据库。
- 使用数据备份，只备份真实数据；不备份数据库中未使用的空间。数据备份包括恢复数据库所需的所

有数据结构，数据备份不包括客户特殊的配置。
- 存储快照获取在一个特定的时间点上的 SAP HANA 的全部数据区的内容。

针对多节点 SAP HANA 系统的文件系统备份

- 在整个系统中，数据和日志备份的配置目标路径必须是有效的，而不仅仅是针对特定主机。
- 如果您使用的是基于文件备份的方式来备份多节点的 SAP HANA 系统，强烈建议使用对于集群所有节点都可用的共享存储来进行备份。

恢复

- 恢复 SAP HANA 数据库，数据库需要关闭。在恢复过程中，数据库不能被最终用户或应用程序访问。
- SAP HANA 数据库无法恢复到比其现有版本低的任何版本。用于恢复的 SAP HANA 数据库软件版本必须是相同或高于创建备份的 SAP HANA 数据库的版本。
- 在恢复开始前，至少需要准备好一个数据备份或至少一个存储快照。
- 在恢复开始时，所有数据和日志备份必须是可通过文件系统或第三方备份工具访问。假如您通过一个存储快照恢复数据库，则该存储快照必须在数据区中可用。
- 您不能暂停和重新继续一个数据库恢复。
- 您可以取消正在运行的恢复，不过，取消恢复会使数据库状态不一致。
- 如果恢复失败，需要重新执行一遍完整的恢复过程。
- 在日志恢复期间，不能执行增量合并操作。
- 在恢复过程中，您在目标系统中的主机数量不受限制，但条件是，源系统和目标系统双方的主机的数量和其所提供的服务的类型是一致的。

非生产系统的 SAP HANA 数据库的备份与恢复

本节提供了对于非生产系统的 SAP HANA 数据库的几种备份选项。非生产系统主要包括：

- 演示系统
- 培训系统
- 沙盒系统
- PoC 验证系统

非生产系统的 SAP HANA 数据备份与恢复的典型要求：

- 备份不频繁
- 不要求恢复到 Point-in-Time
- 简单、低成本

云盘快照 为满足非生产系统的 SAP HANA 数据库备份与恢复要求，提供了简单而低成本的解决方案。快照服务可以有非常灵活的策略，用户可以在任何时候制作云盘快照，一天制作多次云盘快照，用户可以通过配置快

照相关策略，选定某一天，让系统自动在该天制作云盘快照。用户也可以配置云盘快照保留时间，或者将云盘快照保存为永久有效。

对于云盘快照更详细的信息，请参见 阿里云云盘快照。

备份方式

用户可以定期对安装有 SAP HANA 的 ECS 实例的 SAP HANA 系统盘（/usr/sap），数据盘（/hana/data）和日志盘（/hana/log）做快照，来实现对非生产系统的 SAP HANA 数据库的备份。

恢复方式

用户可以使用安装有 SAP HANA 的 ECS 实例的 SAP HANA 系统盘（/usr/sap），数据盘（/hana/data）和日志盘（/hana/log）的云盘快照，来手动恢复整个非生产系统的 SAP HANA ECS 实例。

生产系统的 SAP HANA 数据库的备份与恢复

生产系统的 SAP HANA 数据库备份与恢复的典型要求：

- 经常地、定期地进行备份，并有相应计划
- Point-in-time 数据库恢复

备份方式

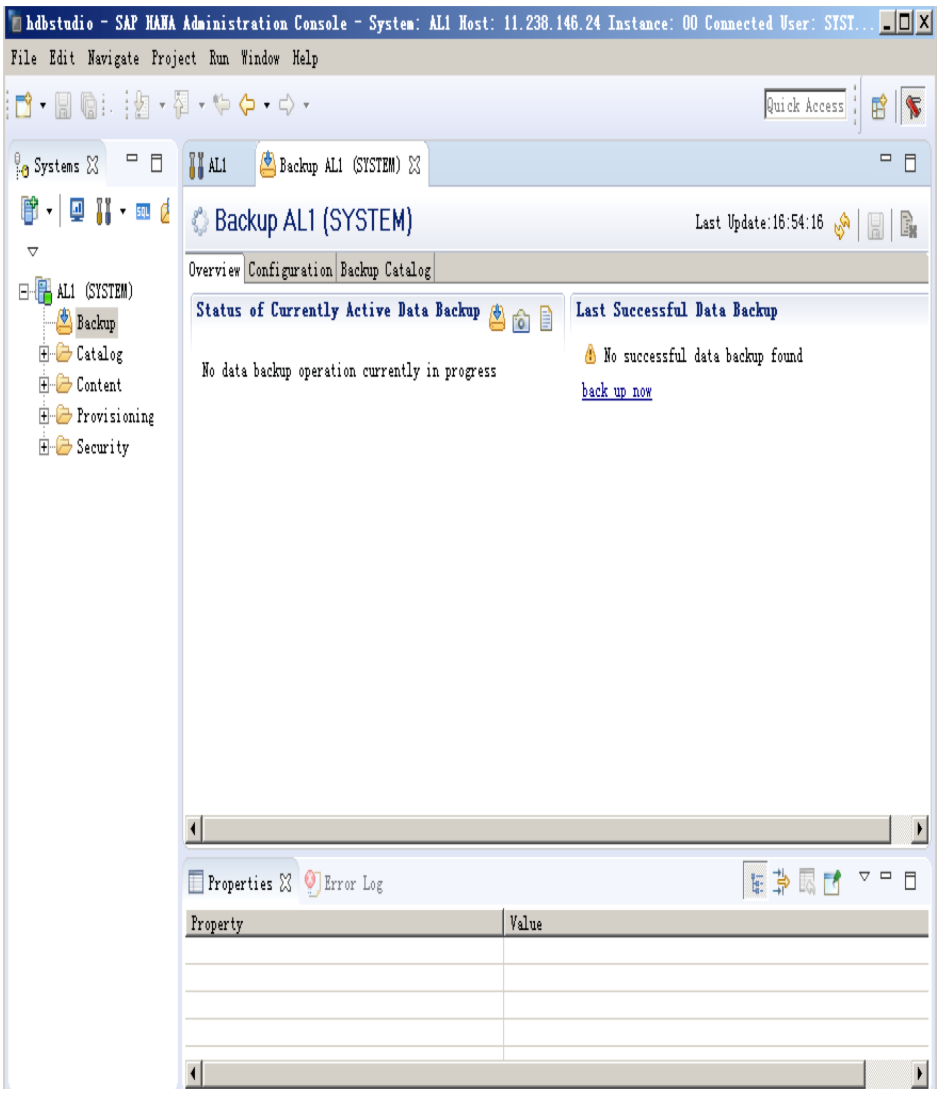
- 默认情况下，在阿里云上，SAP HANA 数据库备份文件的初始备份目的地是挂载在 ECS 实例上的本地云盘。
- 用户可以通过使用 SAP HANA Studio，SQL命令，或者 SAP DBA Cockpit 来启动和安排一次 SAP HANA 数据库备份。除非手动设置禁止，日志文件会被自动备份。
- 用户需要定期将本地云盘上的 SAP HANA 备份文件保存到 OSS bucket 中来做长期保存。
- 如果需要跨地域数据冗余，保存在 OSS bucket 中的 SAP HANA 备份文件，可以根据用户的设置，被复制到阿里云不同的区域保存。

备份示例

下面是一个典型备份任务中可能需要的步骤：

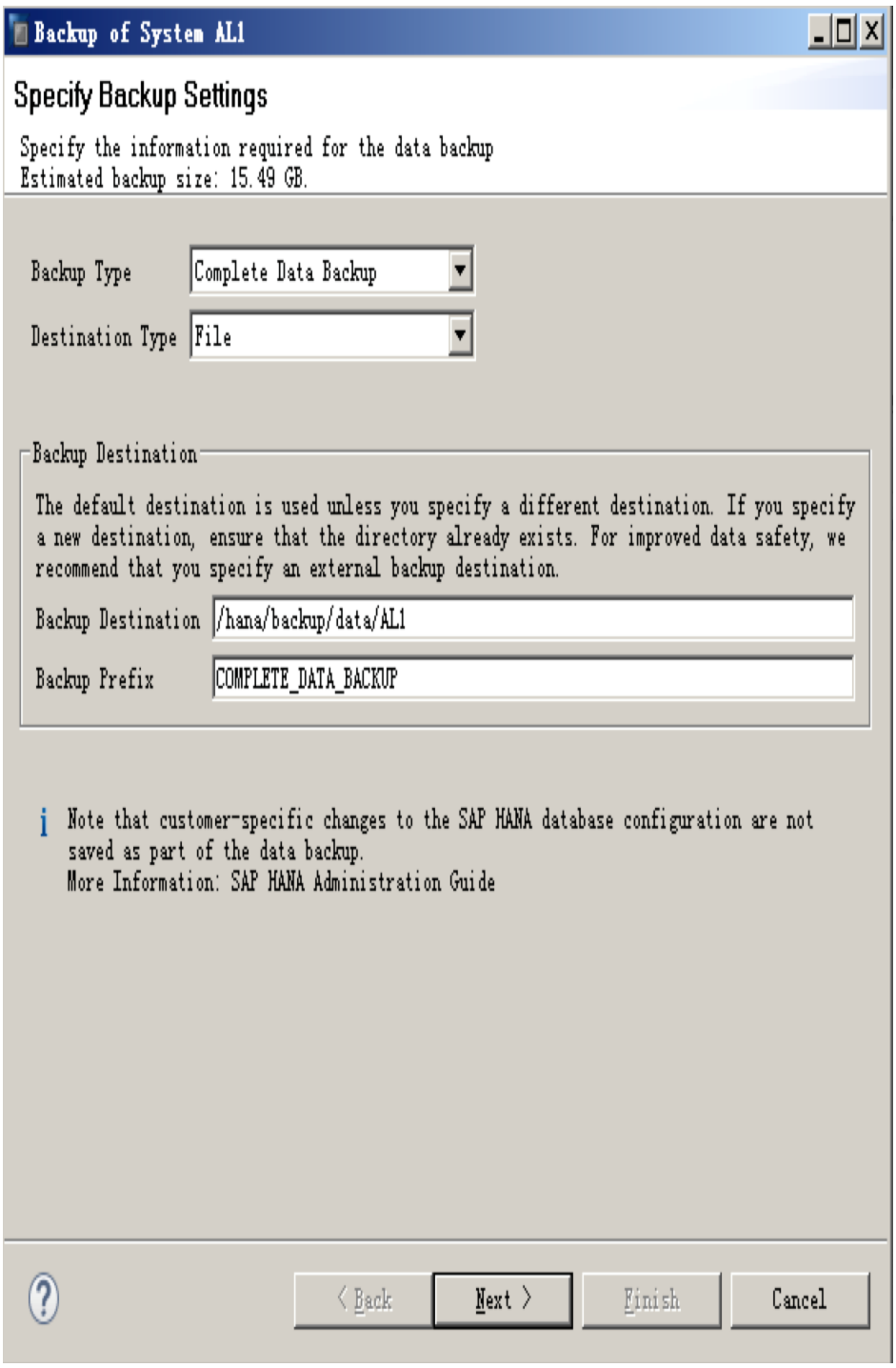
在 SAP HANA 备份编辑器中，选择打开备份向导。您也可以通过右键单击要备份的系统并选择备份

打开备份向导。

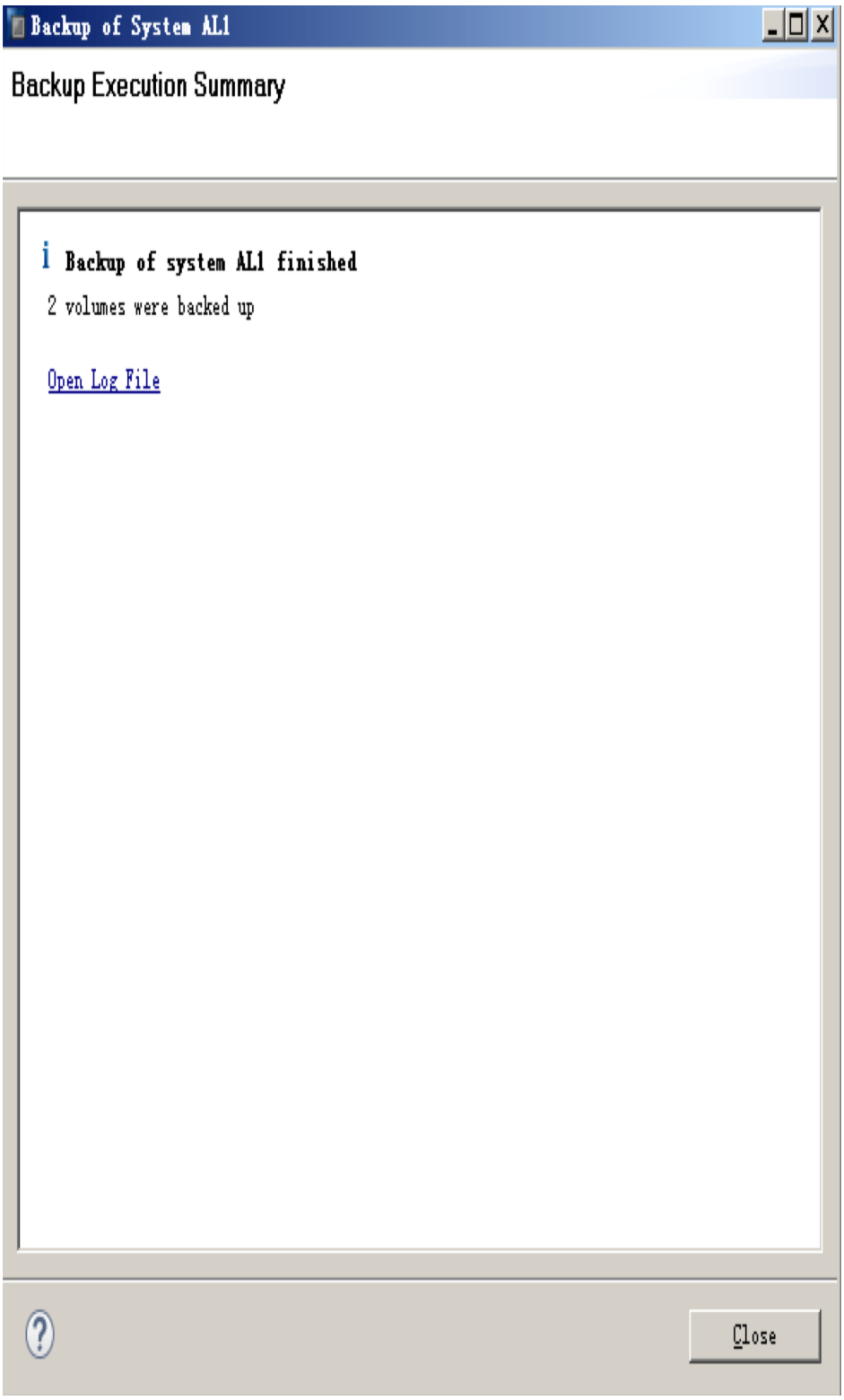


选择目标文件类型，将数据库备份到指定的文件系统中的文件

指定备份路径/hana/backup/data/[SID]和备份的前缀



单击Next，然后完成。备份完成时会出现一条确认消息



确认备份文件在操作系统层面可用

```
master:/hana/backup/data/AL1 # pwd
/hana/backup/data/AL1
master:/hana/backup/data/AL1 # ll
total 16335016
-rw-r----- 1 al1adm sapsys      155648 Jul 22 01:08 COMPLETE_DATA_BACKUP_databackup_0_1
-rw-r----- 1 al1adm sapsys    83894272 Jul 22 01:08 COMPLETE_DATA_BACKUP_databackup_1_1
-rw-r----- 1 al1adm sapsys 16643006464 Jul 22 01:09 COMPLETE_DATA_BACKUP_databackup_3_1
master:/hana/backup/data/AL1 #
```

下一步是将备份文件从/hana/backup复制到 OSS bucket 中。

3. 检查备份文件是否已复制到 OSS。

恢复方式

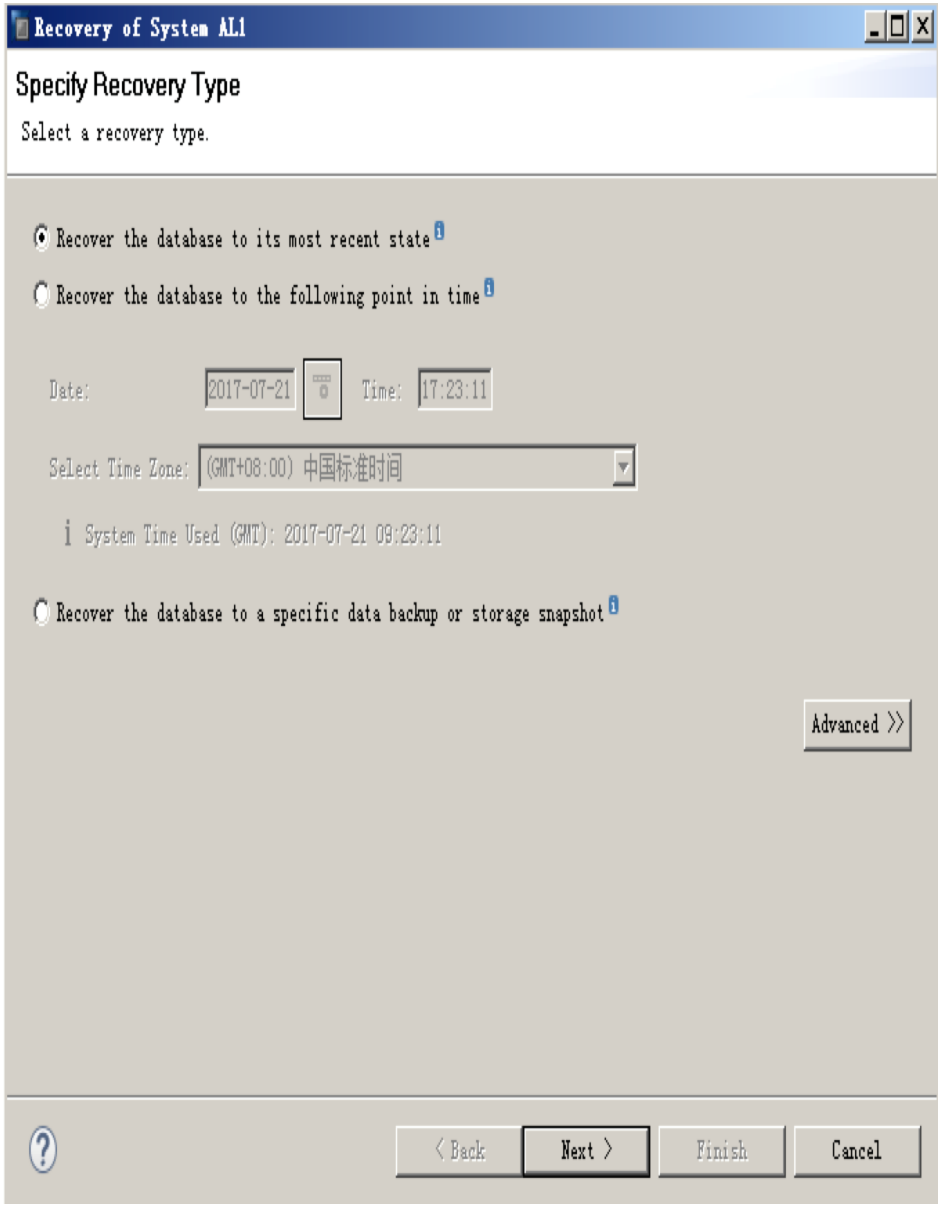
- 将 OSS bucket 中保存的 SAP HANA 备份文件拷贝到运行 SAP HANA 的 ECS 实例所挂载的云盘中的备份目录下。
- 通过运行 SAP HANA 的 ECS 实例所挂载的云盘中的备份目录下的备份文件，对 SAP HANA 数据库进行恢复。

恢复示例

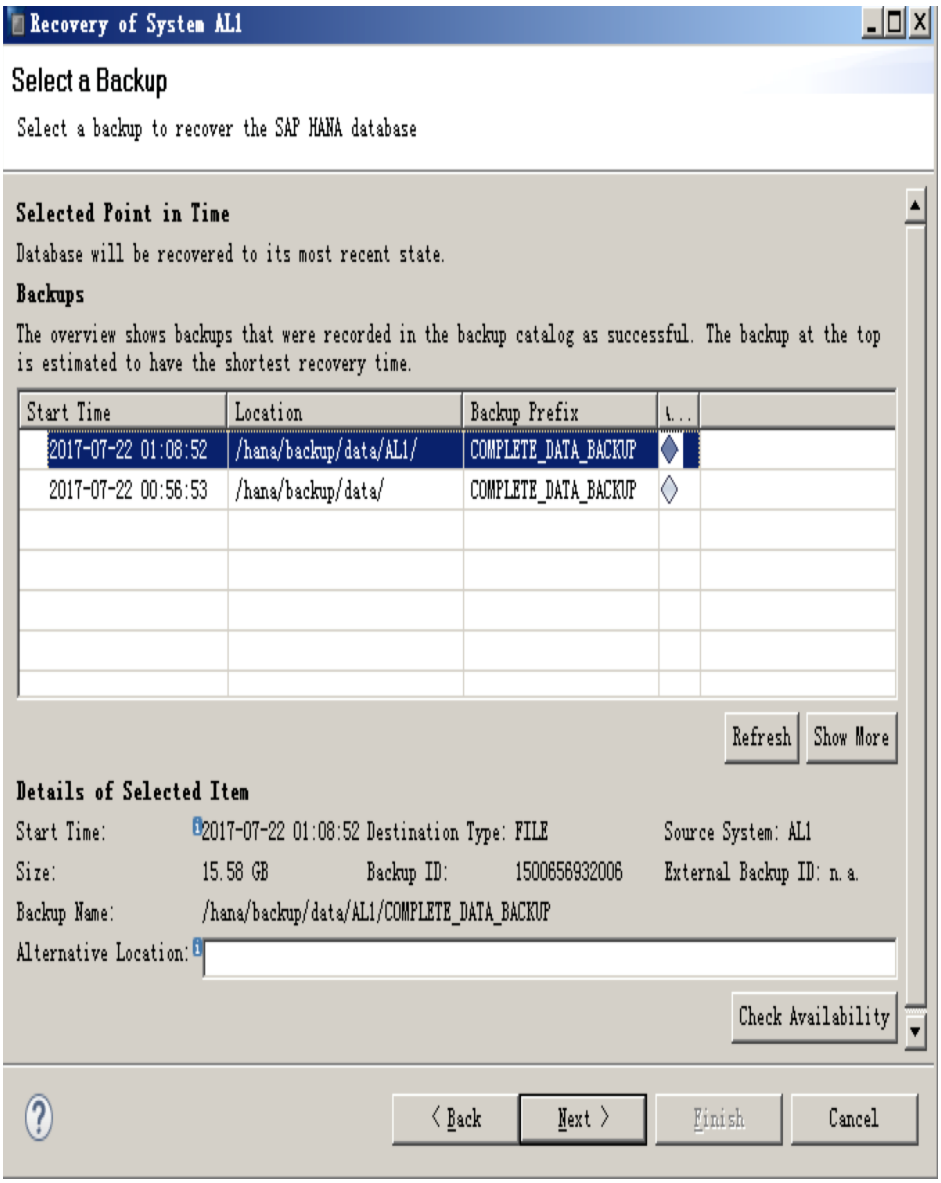
当您需要从备份中恢复您的 SAP HANA 数据库，您可以采取以下步骤：

如果备份文件没有存在于文件系统目录/hana/backup中，但是存在于阿里云的对象存储 OSS 中，请先将备份文件复制到文件系统目录/hana/backup中。

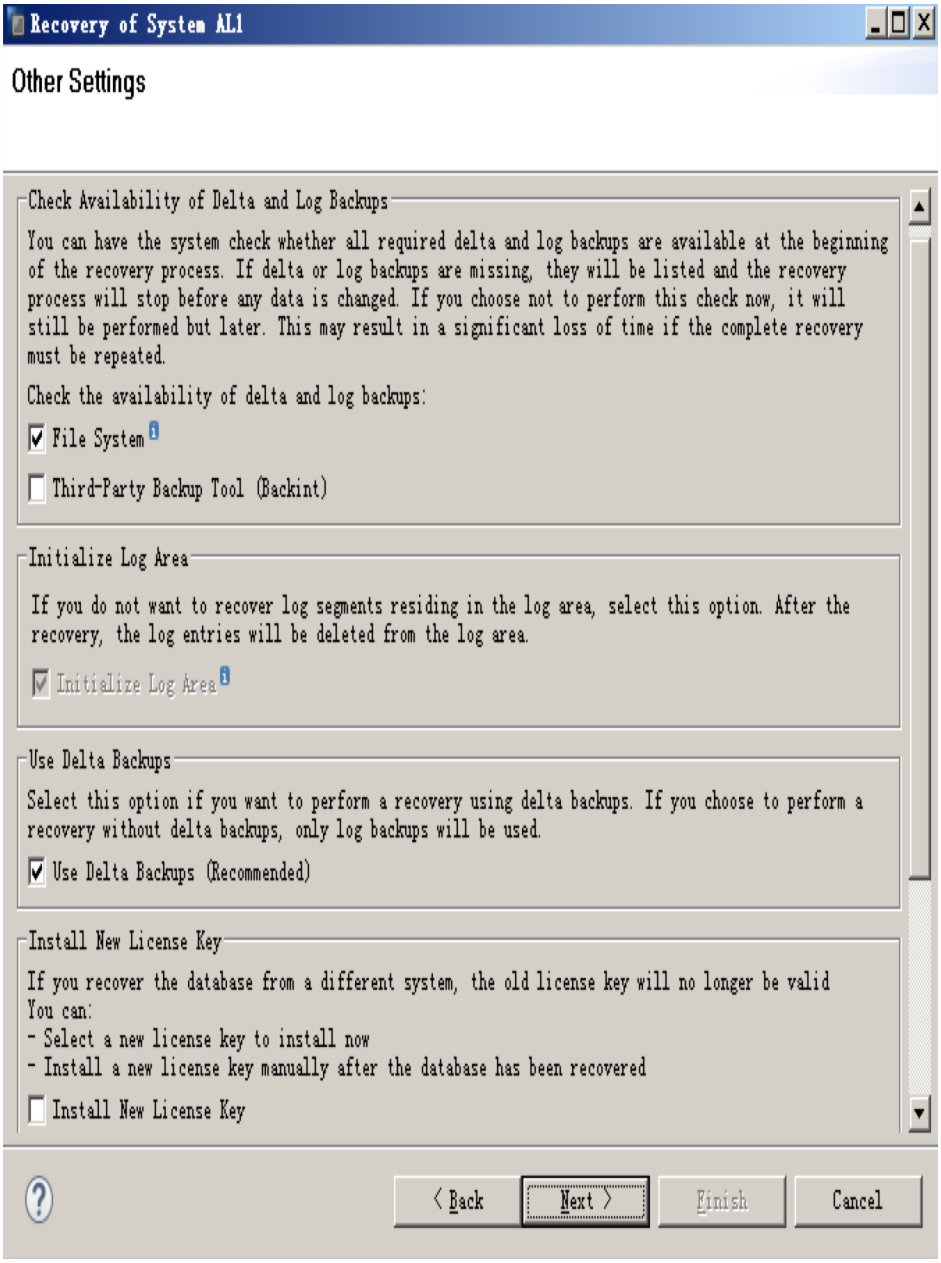
使用恢复向导恢复 SAP HANA 数据库。



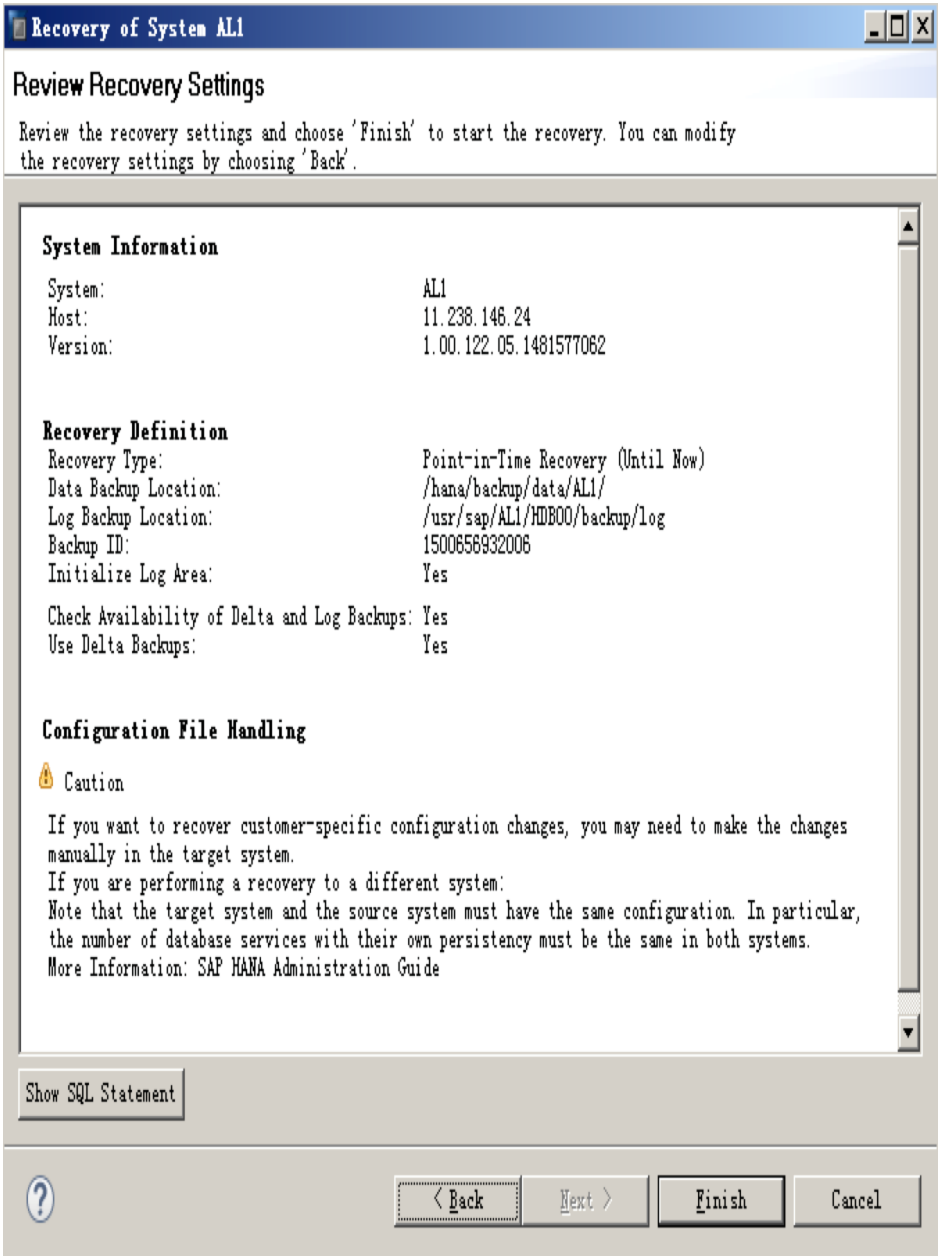
从备份集中选择正确的时间和要恢复的路径。



仔细确认将文件指定为目标类型。



检查汇总摘要并单击“完成”开始 HANA 数据库恢复。



当恢复完成后，您可以继续正常的操作并从/hana/backup/[SID]/*目录中清理备份文件。

SAP HANA 高可用和灾备

- 阿里云服务的高可用性
    - 全球基础设施
    - 计算

    - 存储
    - 宕机自动迁移
- 阿里云上支持的 SAP HANA 原生高可用性方案
    - SAP HANA 服务自动重启（Auto-Restart Service）
    - SAP HANA 节点失效自动切换（Host Auto-Failover）
    - SAP HANA 系统复制（HANA System Replication）
    - SAP HANA 备份与恢复
    - 关于存储复制的说明
- 阿里云上的 SAP HANA 高可用性和容灾方案
    - ECS 宕机自动迁移
    - SAP HANA 系统复制
    - SAP HANA 系统复制 + 备用节点作为开发和测试环境
    - SAP HANA 系统复制 + 备用节点数据预加载
    - ECS 宕机自动迁移 + SAP HANA 备份与恢复
- 节点失效时触发接管程序
- SAP HANA 客户端重定向
- 更多参考文档

阿里云服务的高可用性

全球基础设施

地域和可用区

阿里云基础设施分布在全球许多不同的地域和可用区。**地域（Region）**是指全球某个部署有阿里云基础设施的物理地点；绝大多数情况下，在该地点，我们会有多个可用区。您可以选择离您的用户最近的阿里云基础设施来部署您的SAP系统，从而满足法律和其他业务需求。地域之间的基础设施相互独立；阿里云不会自动的对您在不同地域的基础设施中的资源之间进行同步。

可用区（Zone）是指在同一地域内，电力和网络互相独立的数据中心。可用区让您在阿里云上运行的生产系统与数据库拥有更高的可用性、更强的容错能力和更好的可扩展能力。

阿里云目前在全球范围内运行有14个地域和29个可用区。关于阿里云地域和可用区的更详细信息，请访问 **阿里云全球基础设施**。

通过多个可用区来实现高可用性

阿里云过去多年提供云计算服务的经验告诉我们：对应用程序高可用性和性能更关注的客户，可以通过把应用程序部署在同一地域的不同可用区来实现更好的容错能力和更低的网络时延。

在同一地域内，可用区与可用区之间内网互通，可用区之间能做到故障隔离；这样的架构能够让您通过将应用程序部署在同一地域的不同可用区中，来实现应用程序遇到问题时候，系统自动在不同的可用区之间进行故障切换，而无需人工参与。

通过跨地域数据同步来提高系统的持续性

在阿里云上，块存储（云盘）会在可用区内自动复制您的业务数据，防止意外的硬件故障导致数据不可用，以保护您的业务免于组件故障的威胁。除此之外，您还可以选择将业务数据存放在对象存储（OSS）中，在不同的地域之间进行同步来达到进一步的数据冗余。

计算

云服务器 ECS 是阿里云最核心的服务之一。它让您可以在短短几分钟内，通过部署一个 ECS 实例，实时的满足您的计算需求：不同的CPU、内存、操作系统、IP 地址等等。

简洁的阿里云控制台让您轻松选择不同操作系统来运行应用程序，并且管理网络访问的权限。在控制台中，您可以也使用各种最新的存储功能，如：自动快照。**自动快照** 让您可以迅速拷贝和复制一个云服务器，对于您测试新的功能与操作系统非常有效。更多详细信息，请访问 云服务器 ECS。

存储

块存储（云盘），是阿里云为云服务器 ECS 提供的低时延、持久性、高可靠的数据块级随机存储。您可以为一个 ECS 实例挂载多个云盘来持久地保存数据。您可以对挂载到 ECS 实例的云盘进行格式化、创建文件系统，并且在上面存放数据。由于不同业务场景对于 I/O 性能有完全不同需求，阿里云提供了不同类型的云盘，让您可以单独或者组合使用不同类型的云盘，来满足相应需求。在同一可用区内，云盘上的数据都会有3份副本被自动保存在不同的位置，来帮助您最大程度的保护数据安全。与此同时，您也可以使用云盘快照来保存和恢复您的云盘。您也可以按照您的意愿，对云盘配置自动快照策略。更多详细信息，请访问 块存储。

对象存储（OSS），是阿里云提供的一种使用简单、价格低廉的存储服务。OSS 能够用来在阿里云上，长期保存备份和归档数据。存放在 OSS 中的文件，可以在全球任何一个地方被安全的访问。OSS 可以达到 99.99999999% 数据可靠性，非常适合全球团队和国际项目的数据存储。OSS 提供跨地域数据复制功能，允许您将数据在不同地域之间进行实时同步。对于 SAP 解决方案，OSS非常适合用来长期保存数据库备份文件、SAP 归档文件等。更多详细信息，请访问 对象存储 OSS。

宕机自动迁移

宕机自动迁移 功能是云服务器 ECS 的一个提高云服务器高可用性的功能。当部署在物理机上的云服务器 ECS 由于底层物理机性能出现异常或者其他原因导致物理机宕机时，ECS 实例会启动保护性迁移，将受影响的 ECS 实例迁移到性能正常的物理机上，ECS 实例的实例 ID、私有 IP 地址、弹性公网 IP 地址及实例的元数据等都不变。

同时，阿里云会发送宕机迁移短信通知受影响的用户。为了有效利用云服务器 ECS 的宕机自动迁移功能来提高 SAP HANA 运行环境的高可用性，我们推荐您将 ECS 实例内部的 SAP HANA 设置为开机自动启动。关于云服务器 ECS 宕机迁移的更多细节，请访问相关文档 云服务器 ECS 宕机迁移 FAQ。

注意：宕机自动迁移功能只对挂载云盘的 ECS 实例有效。对于使用本地磁盘的 ECS 实例，当系统发送了宕机短信通知之后，阿里云服务专家将会联系客户一起决定下一步操作。

阿里云上支持的 SAP HANA 原生高可用性方案

SAP HANA 服务自动重启（Auto-Restart Service）

当 SAP HANA 的服务，如 Index Server、Name Server 等，由于程序奔溃，或者管理员的人工干预导致停止运行时，SAP HANA 会通过自动重启监控进程发现被停止的服务，并且将其重启。在重启过程中，服务会将数据装载进内存并且恢复它的相关功能。服务自动重启在恢复数据安全的同时，也需要相应的时间。

SAP HANA 服务自动重启，在阿里云平台上与其他平台上运行没有区别。

SAP HANA 节点失效自动切换（Host Auto-Failover）

SAP HANA 节点失效自动切换是 SAP 提供的一个 N+m 节点宕机恢复解决方案。一台或多台节点可以被配置为待命状态，加入到一个单节点或者分布式的 SAP HANA 系统中；系统中处于待命状态的节点，不会存放任何数据，也不会接受任何请求和查询。

当一个工作节点不可用时，系统中的一个待命节点会自动接管它的工作。因为待命节点可能接管系统中任何一个工作节点的工作，因此它必须可以访问所有数据库的数据。这个需要通过共享网络存储（NFS）或者存储连接接口（storage connector API）实现。

阿里云建议您可以充分利用阿里云 ECS 的宕机自动迁移功能，即当您的 ECS 实例所在的物理机出现问题的时候，ECS 实例被自动移动到同一可用区内另一个没有问题的物理机上。本质上，该功能让您可以在无需任何额外费用的情况下，即可拥有一个高可用的 ECS 实例。在新的物理机上恢复的 ECS 实例，和原实例完全相同，包括：存储、各种配置、IP 地址、ECS 实例 ID。同时，我们建议您将 SAP HANA 配置为开机自动启动，以便在您的 SAP HANA ECS 实例发生宕机自动迁移之后，HANA 服务会自动恢复。另一方面，重启之后，将数据加载到内存也需要一定的时间，具体所需要的时间，会因为 HANA 数据量不同而不同。

SAP HANA 系统复制（HANA System Replication）

SAP HANA 系统复制（HANA System Replication， 简称 HSR）是 SAP HANA 提供的高可用和容灾解决方案。通常，经过 HSR 设置，备用节点系统被配置为主节点的一个完全拷贝。

备用节点可以被放置在主节点附近，来构建一个快速的故障切换解决方案，用来解决计划内宕机，或者主节点存储系统损坏及其他本地错误；备用节点也可以被安装在远端（通常是异地），用来构架容灾解决方案。根据您对于恢复时间目标（RTO）和数据库的恢复点目标（RPO）的不同要求，HSR 允许您有完全多种不同的设置：内存同步、同步、异步。关于 HSR 的更多详细信息，请参见 SAP 的官方文档 How to Perform System Replication for SAP HANA。

SAP HANA 系统复制在阿里云上完全支持，而且您可以将 HSR 和阿里云的可用区有效结合来更好地保护您的数据安全。通常，同一地域的同一可用区内的网络速度会更加快，我们会建议内在同一可用区内配置的 HSR 设置为同步；而不同的地域的 HSR，我们建议配置为异步。

SAP HANA 备份与恢复

虽然 SAP HANA 是内存数据库，但为了在例如突然停电时，能够恢复数据并确保数据不丢失，所有数据修改都会被 SAP HANA 保存在持久存储系统中。为了在灾难发生后，能够恢复数据，还必须定期将持久存储系统中的数据和数据库日志备份到远端。关于 SAP HANA 数据库更多的备份和恢复细节，请参见 SAP 官方文档 Backup and Recovery - SAP HANA。

您在阿里云上进行 SAP HANA 数据库的备份和恢复，和在其他平台上没有任何区别。而且您还能利用对象存储 OSS 安全、持久、高度可扩展、性价比高的优势，将 HANA 备份文件放到 OSS bucket 中长期保存，或者通过对存放 HANA 备份文件的云盘做快照的方式来实现灾备。

关于存储复制的说明

SAP HANA 硬件合作伙伴为 SAP HANA 灾备提供了存储系统级别的系统复制解决方案，来将 SAP HANA 数据库的相关数据、日志或者文件系统等同步到远端的联网的存储系统上，得以实现灾难过后，在尽可能短的恢复时间目标（RTO）内恢复 SAP HANA 数据库。

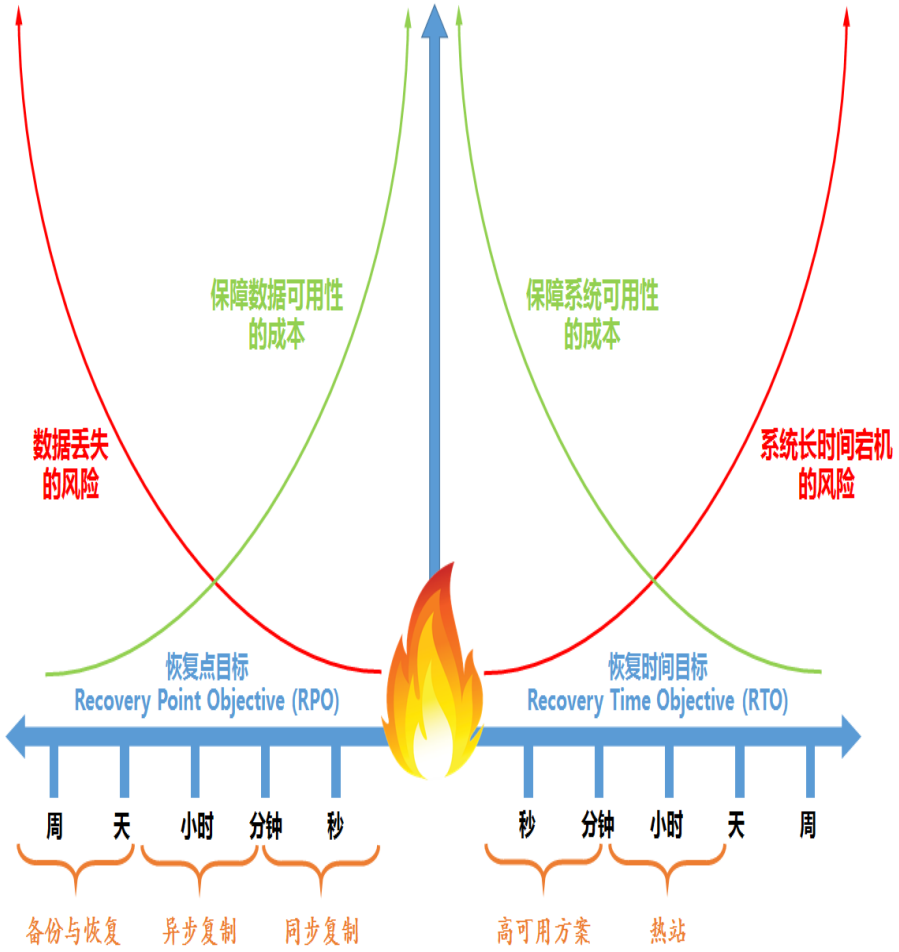
但是，阿里云上无法提供存储级别的复制（Storage Replication）。

阿里云上的 SAP HANA 高可用性和容灾方案

您需要结合您的业务场景和业务关键程度，来选择在阿里云上为您的 SAP HANA 系统选择合适的高可用性和容灾方案。作为最核心的两个考量因素：

- Recovery Point Objective (RPO) = 恢复点目标，主要考量有多少数据丢失
- Recovery Time Objective (RTO) = 恢复时间目标，主要考量服务不可用时间有多长

相关概念，可参考下图



对于各方案的 RPO、RTO、以及成本的简单比较

方案	成本	RPO	RTO
SAP HANA 系统复制	￥￥	低	中
SAP HANA 系统复制 + 备用节点作为开发和测试环境	￥￥￥	低	中
SAP HANA 系统复制 + 备用节点数据预加载	￥￥￥	低	低
ECS 宕机自动迁移 + SAP HANA 备份与恢复	￥	中	高

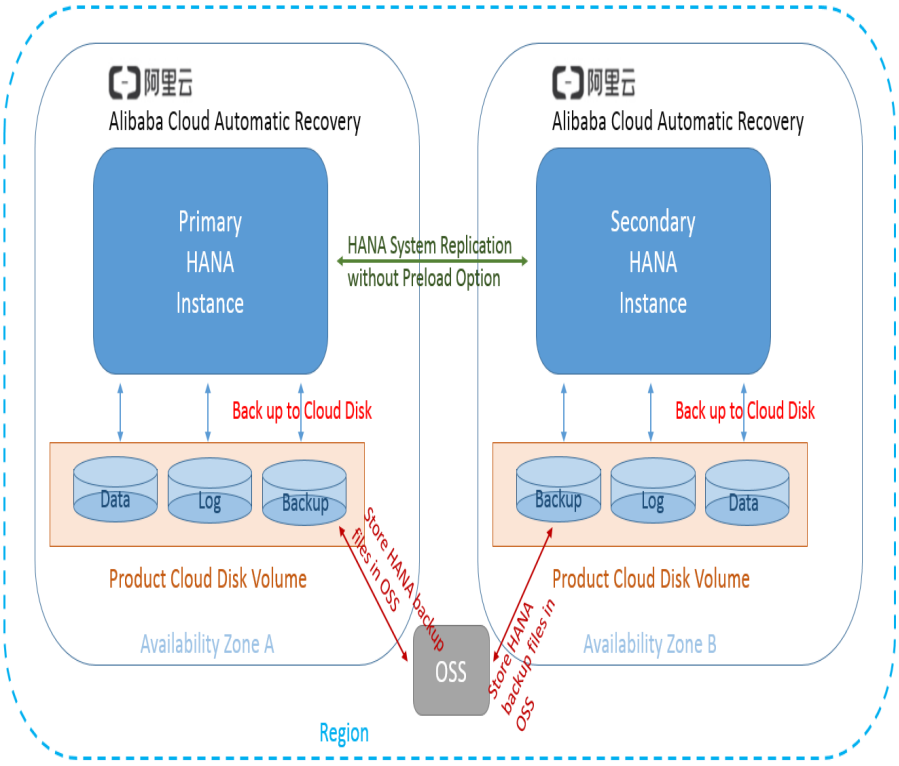
ECS 宕机自动迁移

通常情况下，云服务器 ECS 宕机自动迁移功能可以帮助您在 ECS 实例所在底层物理硬件发生故障的时候，自动将您的 SAP HANA ECS 实例恢复到 **同一可用区** 内的另外一台物理机上运行。而当整个可用区出现故障的时候，您可以参考以下 **跨可用区方案** 来帮助您保护 SAP HANA 数据库中的数据。

SAP HANA 系统复制

您将 SAP HANA 主节点部署在可用区 A，备用节点部署在可用区 B，两个节点之间配置了 HSR。因为使用了 HSR，SAP HANA 主节点上的数据变化，会被持续地复制到备用节点上。当可用区 A 内的主节点不可用时，您可以立刻在可用区 B 内的备用节点上恢复整个 HANA 实例。

注意：在这个场景中，您需要将 HSR 配置异步同步，这样主节点不需要因为等待备用节点的同步反馈而产生性能影响。



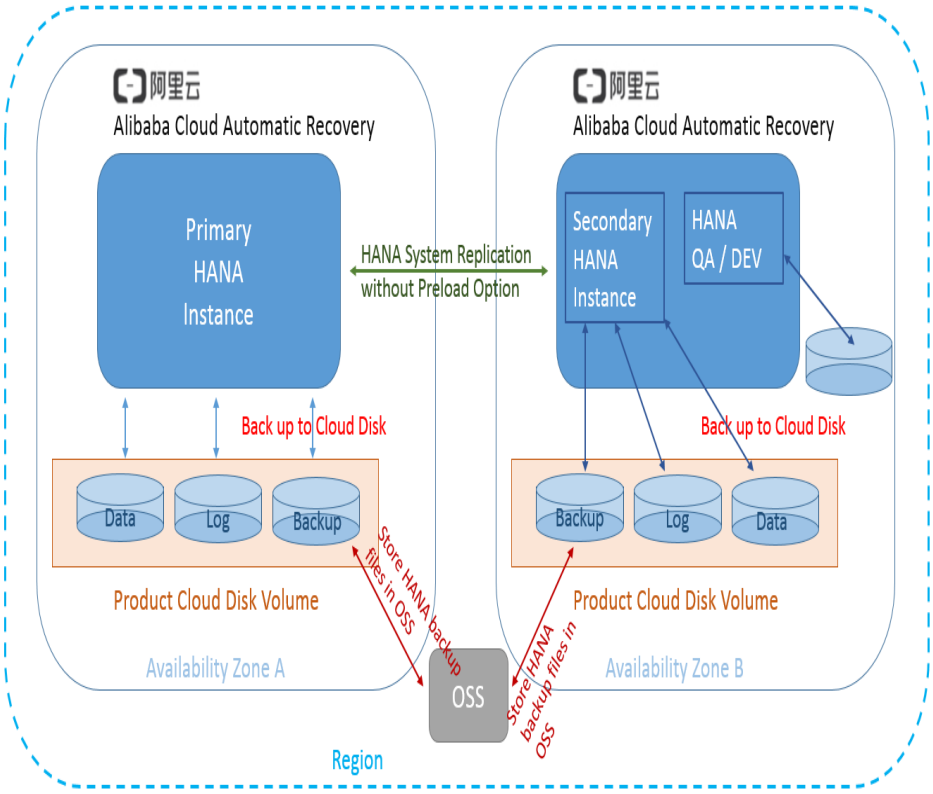
这里需要说明一下，HSR 有一个配置选项：**备用节点预加载**

如果该预加载选项被关闭，同步到备用节点的数据不会被加载到备用节点的内存中。这也意味着对于备用节点，您可以选择相对较低配置的 ECS 实例，从而降低总的运行成本。在故障切换的过程中，您可以将备用节点的 ECS 实例配置调整为与主节点 ECS 实例配置相同。当 SAP HANA 系统在备用节点上被完全恢复起来之后，您再将客户端的 HANA 访问重新定向到备用节点。

SAP HANA 系统复制 + 备用节点作为开发和测试环境

基于 SAP HANA 的 HSR 方案，你还可以更加充分地利用您的备用节点，降低总的运维成本。通常，您选用的备用节点的 ECS 实例配置和主节点的完全相同。而在备用节点的 ECS 实例中，除了配置 HANA HSR 备用节点，还可以安装您的 HANA 开发和测试环境。

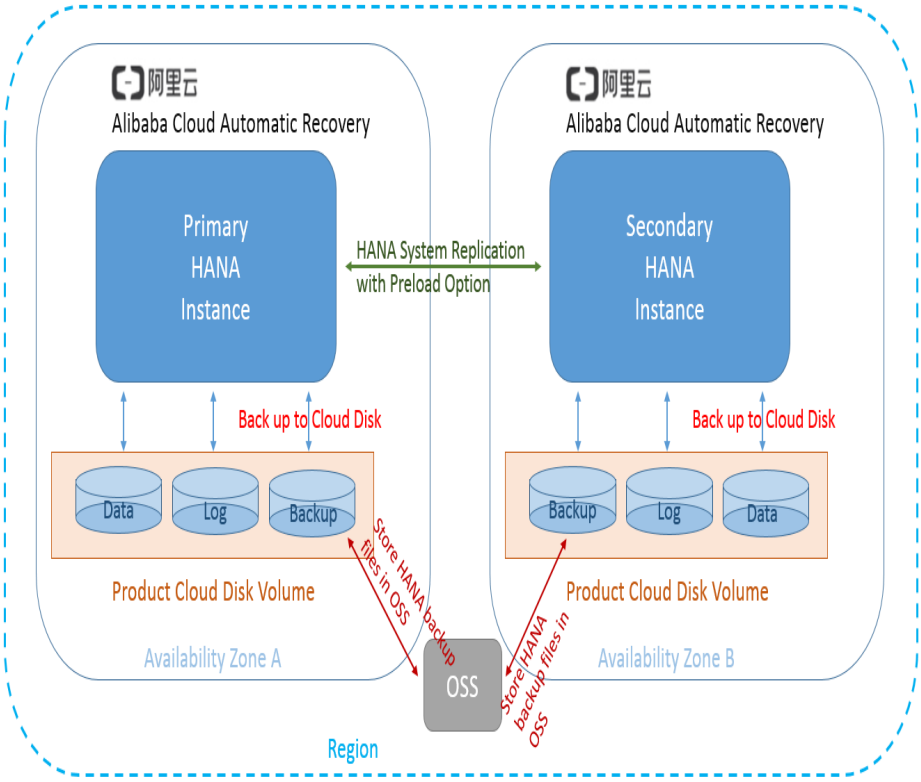
当系统发生故障切换时，备用节点的 HANA 实例将提供整个 HANA 数据库服务，这时您必须将备用节点上的 HANA 开发和测试环境关闭，将其占用的资源释放出来给 HANA 生产环境使用。当备用节点上的 SAP HANA 运行正常后，您就可以将客户端的 HANA 访问重新定向到备用节点。



SAP HANA 系统复制 + 备用节点数据预加载

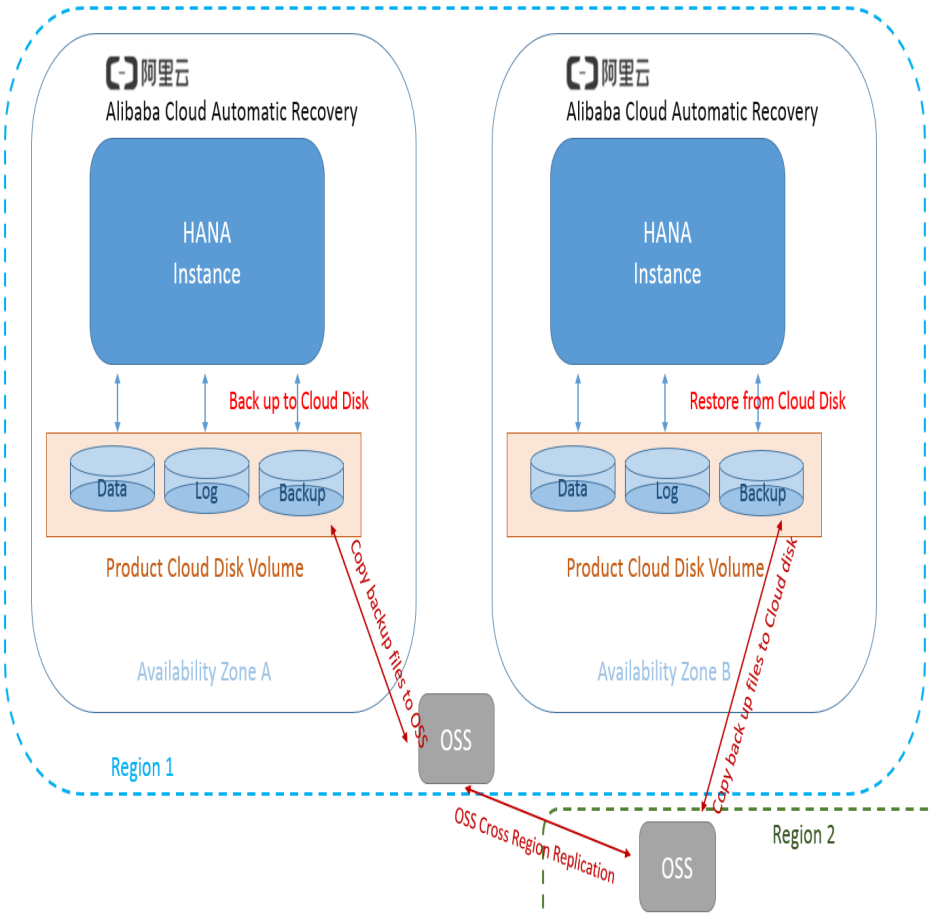
前面提到 HSR 的配置选项 **备用节点预加载**。

如果该预加载选项被开启，这意味着同步到备用节点的数据会在第一时间被加载到备用节点的内存中。这样的好处是，您的备用节点需要更少的时间就可以将 HANA 系统投入正常运行。不过使用这种方案要求备用节点的 ECS 实例配置必须和主节点的始终保持一致。



ECS 宕机自动迁移 + SAP HANA 备份与恢复

您可以通过自定义镜像，在另外一个可用区（比如下图中的可用区 B）重新搭建一个和原来配置一样的 ECS 实例，并且将保存在别的地域的 OSS bucket 中的 SAP HANA 数据库备份文件，拷贝到新的 ECS 实例所挂载的云盘。一旦备份文件拷贝到了 ECS 实例挂载的云盘，您就可以通过 SAP HANA 的恢复功能，在新的实例上恢复 SAP HANA 数据库。当 SAP HANA 数据库在新的 ECS 实例上正常运行后，您可以将客户端的 HANA 访问切换到新的 ECS 实例来。



SAP HANA 数据库的恢复点（RPO），依赖于您备份 SAP HANA 数据库的频率和将备份文件拷贝到 OSS 中的频率。

节点失效时触发接管程序

为了启动容灾功能，您还需要考虑如何触发 SAP HANA 系统复制的备用节点的接管程序。具体c操作，请参考 HSR 官方文档 How to Perform System Replication for SAP HANA 中系统接管流程 (Takeover) 的章节。

此外，在 SAP Note 2063657 中也提供了 SAP 官方的指导方针，帮助您决定备用节点接管是否是一个最佳选择。

SAP HANA 客户端重定向

在 SAP HANA 的备用节点接管工作最后，您需要确保 SAP HANA 的各类客户端应用（例如： NetWeaver 应用服务器、JDBC 链接、ODBC 连接等）能够在故障切换完成后，和新的 SAP HANA 服务器节点之间建立连接。然后您可以通过更新客户端的 SAP HANA 数据库的 IP 地址或者 DNS 来完成重定向。

关于 SAP HANA 故障切换后，客户端访问重定向的更详细解释，请参见 SAP HANA Administration Guide 中 “Client Connection Recovery” 章节。

更多参考文档

- High Availability for SAP HANA
- How to perform System Replication for SAP HANA
- SAP Notes:
    - 1999880 - FAQ: SAP HANA System Replication
    - 2057595 - FAQ: SAP HANA High Availability
    - 2063657 - HANA System Replication takeover decision guideline
    - 1913302 - HANA: Suspend DB connections for short maintenance tasks

SAP HANA 软件许可

软件许可

阿里云为您提供了运行您的 SAP HANA 和相关数据库应用所需的基础环境，而您在阿里云上使用 SAP HANA 软件和运行 SAP HANA 系统则需要相应的软件许可。您需要使用您的软件许可在 SAP 软件下载中心 来下载你所需要的软件。

目前阿里云支持以下两种 SAP HANA 的软件许可：

您自有的软件许可（BYOL）

您可以将已有的 SAP HANA 软件许可或者购买新的 SAP HANA 软件许可用于您的生产系统或者非生产系统。

支持场景：

- SAP HANA 数据库应用
- 基于 SAP HANA 数据库的数据仓库、数据分析和商务智能应用
- SAP HANA Scale-out（横向扩展）多节点架构
- BW/4 HANA

软件许可获取方式：

- Bring Your Own License (BYOL)

支持内存规模：

- 纵向扩展至 1920 GB
- 横向扩展至 13440 GB

SAP HANA One

按实际使用需求，按月订阅软件许可的 SAP HANA One。详细信息，请参见 阿里云云市场

支持场景：

- SAP HANA 数据库应用
- 基于 SAP HANA 数据库的数据仓库、数据分析和商务智能应用

软件许可获取方式：

- 用户在阿里云云市场购买的 SAP HANA One 镜像，已附带 SAP HANA One 软件许可

支持内存规模：

- 64 GB

克隆实例时 HANA License Key 的处理方法

在您克隆您的 HANA 实例时，请确保执行以下步骤：

1. 如果 HANA 服务已经停止，或者尚未启动
   - su -- <SIDADM>
   - 打开配置文件
     /usr/sap/<instance ID>/SYS/global/hdb/custom/config/nameserver.ini
   - 删除参数id的那一行
   - 执行 Linux 命令 hdbnsutil –convertTopology
   - 启动 HANA
2. 确保您的 HANA 处于“license lockdown mode” （许可锁定模式）
   - 安装新的 License Key

示例

在 HANA 实例被克隆之前

检查 HANA 数据库状态

```
hanaZlicenseZ:~ # su -l alladm
alladm@hanaZlicenseZ:/usr/sap/AL1/HDB00> HDB info
USER       PID  PPID %CPU    VSZ   RSS COMMAND
alladm    8214  8213  1.0  14840  3588 -sh
alladm    8278  8214  0.0  13196  1804  \_ /bin/sh /usr/sap/AL1/HDB00/HDB info
alladm    8305  8278  0.0  26668  1348      \_ ps fx -U alladm -o user,pid,ppid,pcpu,vsz,rss,
alladm    7188     1  0.0  21028  1688 sapstart pf=/hana/shared/AL1/profile/AL1_HDB00_hanazli
alladm    7196  7188  0.0 592152 295720  \_ /usr/sap/AL1/HDB00/hanazlicensez/trace/hdb.sapAL1
alladm    7212  7196  0.6 16697556 1435204      \_ hdbnameserver
alladm    7304  7196  5.5 3529288 779172       \_ hdbcompileserver
alladm    7306  7196 61.7 8094716 5467840       \_ hdbpreprocessor
alladm    7340  7196 31.5 13726992 10333452       \_ hdbindexserver
alladm    7342  7196  1.8 4486848 1259832       \_ hdbxsengine
alladm    7668  7196  0.4 3309140 652184       \_ hdbwebdispatcher
alladm    7103     1  0.2 491636 25752 /usr/sap/AL1/HDB00/exe/sapstartsrv pf=/hana/shared/AL1
alladm@hanaZlicenseZ:/usr/sap/AL1/HDB00>
```

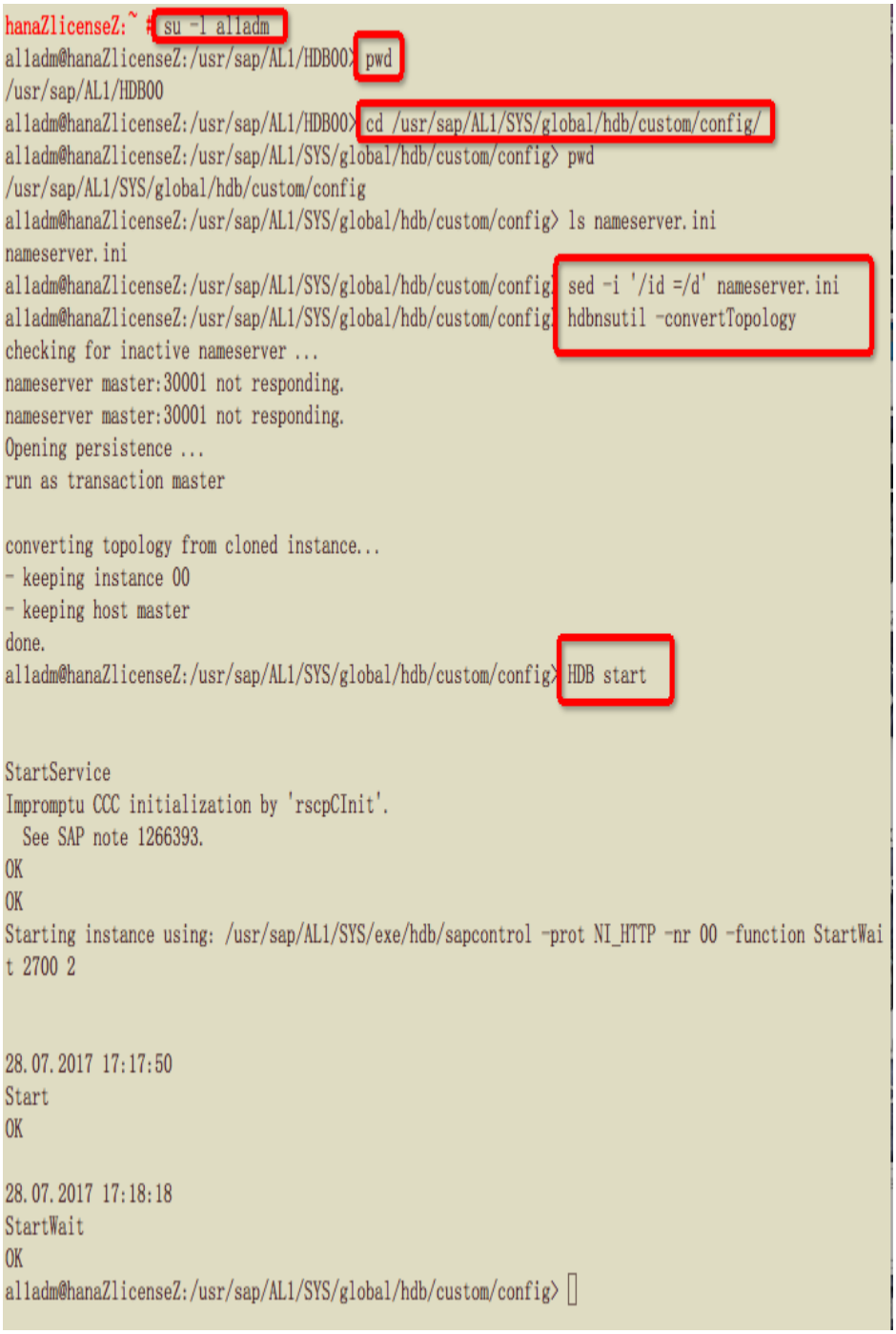
检查 Landscape ID

```
alladm@hanaZlicenseZ:/usr/sap/AL1/SYS/global/hdb/custom/config> pwd
/usr/sap/AL1/SYS/global/hdb/custom/config
alladm@hanaZlicenseZ:/usr/sap/AL1/SYS/global/hdb/custom/config> cat nameserver.ini
[landscape]
id = 595c910a-5272-1b4b-e200-b7a73061749a
master = hanazlicensez:30001
worker = hanazlicensez
roles_hanazlicensez = worker
active_master = hanazlicensez:30001
alladm@hanaZlicenseZ:/usr/sap/AL1/SYS/global/hdb/custom/config>
```

检查 SQL 执行结果

```
alladm@hanaZlicenseZ:/usr/sap/AL1> cat test.sql
select count(*) from sys.tables
alladm@hanaZlicenseZ:/usr/sap/AL1> hdbsql -n localhost:30015 -u SYSTEM -p manager -I ./test.s
ql -o test.out
alladm@hanaZlicenseZ:/usr/sap/AL1> cat test.out
COUNT(*)
564
alladm@hanaZlicenseZ:/usr/sap/AL1>
```

克隆的实例第一次启动后，执行本节描述的处理方法



HANA 重启后

检查 HANA 数据库状态

```
alladm@hanaZlicenseZ:/usr/sap/AL1> HDB info
USER       PID  PPID %CPU    VSZ   RSS COMMAND
alladm   10709 10708  0.0  14840  3776 -sh
alladm   11754 10709  0.0  13196  1804  \_ /bin/sh /usr/sap/AL1/HDB00/HDB info
alladm   11781 11754  0.0  26668  1348      \_ ps fx -U alladm -o user,pid,ppid,pcpu,vsz,rss,
alladm   11133     1  0.0  21028  1688 sapstart pf=/hana/shared/AL1/profile/AL1_HDB00_hanazli
alladm   11141 11133  0.6 592152 295376  \_ /usr/sap/AL1/HDB00/hanazlicensez/trace/hdb.sapAL1
alladm   11157 11141  3.4 12468172 1360928      \_ hdbnameserver
alladm   11246 11141 18.9 3267144 600580      \_ hdbcompileserver
alladm   11248 11141  1.4 3002684 391924      \_ hdbpreprocessor
alladm   11280 11141 47.4 7307384 3881480      \_ hdbindexserver
alladm   11282 11141  5.5 4538628 1218308      \_ hdbxsengine
alladm   11659 11141  3.3 3307984 631756      \_ hdbwebdispatcher
alladm    7103     1  0.0 623740 26084 /usr/sap/AL1/HDB00/exe/sapstartsrv pf=/hana/shared/AL1
alladm@hanaZlicenseZ:/usr/sap/AL1>
```

检查 Landscape ID

```
alladm@hanaZlicenseZ:/usr/sap/AL1/SYS/global/hdb/custom/config> pwd
/usr/sap/AL1/SYS/global/hdb/custom/config
alladm@hanaZlicenseZ:/usr/sap/AL1/SYS/global/hdb/custom/config> cat nameserver.ini
[landscape]
master = hanazlicensez:30001
worker = hanazlicensez
active_master = hanazlicensez:30001
id = 595c90f4-6d9c-2a98-e200-90520e7f6aca
roles_hanazlicensez = worker
alladm@hanaZlicenseZ:/usr/sap/AL1/SYS/global/hdb/custom/config>
```

检查 SQL 执行结果

```
alladm@hanaZlicenseZ:/usr/sap/AL1> cat test.sql
select count(*) from sys.tables
alladm@hanaZlicenseZ:/usr/sap/AL1> hdbsql -n localhost:30015 -u SYSTEM -p manager -I ./test.s
ql -o test.out
* 437: only commands for license handling are allowed in current state SQLSTATE: HY000
* 437: only commands for license handling are allowed in current state SQLSTATE: HY000
alladm@hanaZlicenseZ:/usr/sap/AL1> cat test.out
* 437: only commands for license handling are allowed in current state SQLSTATE: HY000
* 437: only commands for license handling are allowed in current state SQLSTATE: HY000
alladm@hanaZlicenseZ:/usr/sap/AL1>
```

确认实例处于许可锁定模式

此时，可以开始安装新的 HANA License Key

SAP Business Applications

SAP NetWeaver 规划指南

- 阿里云概览
    - 阿里云 SAP NetWeaver 概览
    - 两层架构
    - 三层架构（SAP NetWeaver 应用服务器横向扩展）
    - 高可用性
- 阿里云 ECS
    - ECS 实例类型
    - 镜像
    - 地域和可用区
    - VPC
    - 部署 ECS 实例
    - 访问 ECS 实例
- 数据库
    - SAP HANA
    - 数据库备份和恢复
- 存储
    - 块存储（云盘）
    - 对象存储服务 (OSS)
- 网络和安全
    - 安全组
    - SSH 密钥对
    - 路由器配置
    - 堡垒机
    - NAT 网关
    - VPN 网关
    - 安全文档
- 系统拷贝和迁移
- SAP NetWeaver 监控和支持
- 许可
    - SAP 许可证
    - Linux 许可证

- 安装介质
- SAP Router 和 Solution Manager

阿里云概览

阿里云 SAP NetWeaver 概览

阿里云构建于全球基础设施之上，可提供各种类型的 IaaS 产品和服务。客户可以在全球不同的地域使用阿里云服务。在阿里云运行 SAP NetWeaver 之前，必须充分了解以下基础知识：

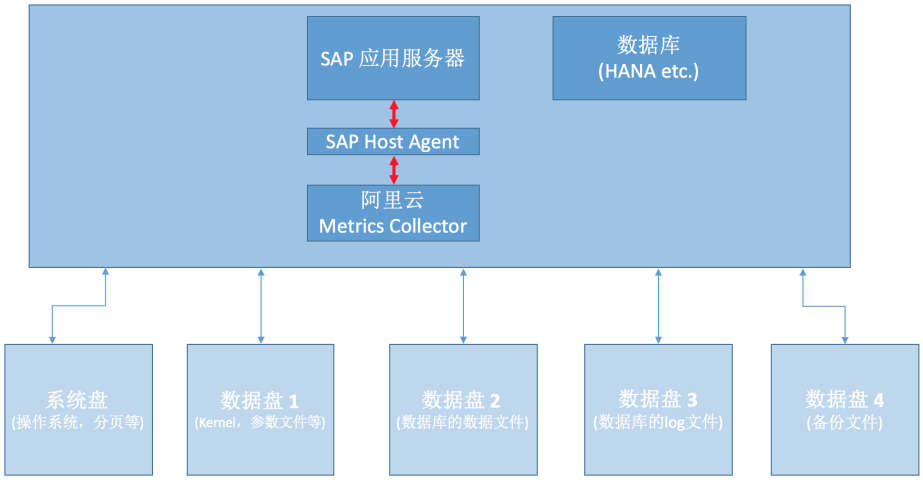
- **阿里云云服务器 (ECS)**
  阿里云云服务器 (ECS) 是一项 Web 服务，可在云中提供缩放式计算能力。简单的 Web 服务接口使您能够轻松获得和配置计算能力。随着计算需求的变化，您可以快速扩展和缩减计算能力，而您只需按实际需求付费。
- **阿里云块存储（云盘）**
  阿里云块存储（云盘）可为运行在阿里云平台上的阿里云 ECS 实例提供永久块级存储卷。云盘存储卷具有一致性和低时延性能，可满足您的工作负载运行需要。借助云盘，您可以在几分钟内增加或降低使用量，而所有这一切只需按实际使用支付低廉的费用。
- **阿里云对象存储 (OSS)**
  阿里云对象存储服务 (OSS) 是一种易于使用的服务，让您能够在云上存储、备份和归档大量数据。OSS 作为加密的中央存储库，允许人们从世界各地安全地访问文件。OSS 能够保证高达 99.9999% 的可用性，堪称全球团队和国际项目管理的完美选择。
- **专有网络 (VPC)**
  专有网络 (Virtual Private Cloud, VPC) 可为阿里云的用户构建一个隔离的网络环境。您可以选择 IP 地址范围，划分网络，配置路由表和网关。

SAP NetWeaver 和阿里云服务共同携手，以特定方式为我们的客户提供合而为一的企业应用和基础设施能力。

- SAP NetWeaver 系统及数据库组件使用阿里云 ECS 实例存储服务以及专有网络服务。
- SAP Host Agent/SAPOSCOL 可随 SAP NetWeaver 标准安装部署，能够调用阿里云提供的监控代理组件。
- 阿里云 ECS Metrics Collector 是一款监控代理程序，可以收集所需的 CPU\内存\磁盘\网络监控数据，并且可以将这些监控项提供给 SAP 应用程序使用。

两层架构

下图给出了运行于阿里云之上的两层架构的一些细节：



在此架构中，所有组件都运行在单个 ECS 实例上。该 ECS 实例挂载有 3 个磁盘，每个磁盘都扮演了特定角色。这些角色包括：

- **系统盘**：包含 ECS 实例的操作系统和分页文件。
- **数据盘 1**：包含 SAP NetWeaver 安装和配置文件以及数据库安装和配置文件
- **数据盘 2**：包含用于维护数据一致性的数据库数据文件。注意：数据盘 2 应当使用 SSD 云盘，以保证数据库性能。
- **数据盘 3**：包含用于维护数据一致性的数据库日志文件。注意：数据盘 3 也应当使用 SSD 云盘，以保证数据库性能。
- **数据盘 4**：包含用于数据库备份的文件；

有关阿里云 SAP HANA 部署架构的更多信息，请参阅“HANA 部署指南”：https://www.alibabacloud.com/help/doc-detail/57229.htm。

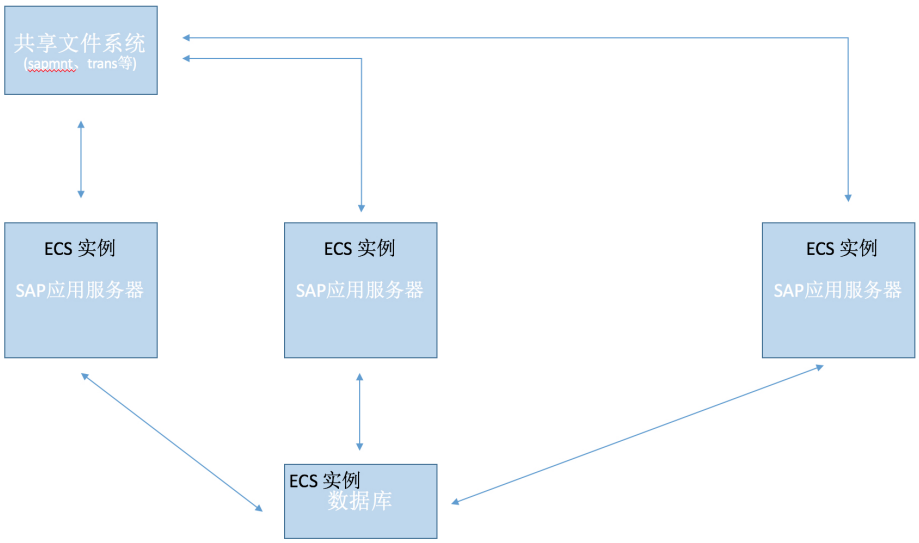
关于 SAP HANA 的两层部署，请参阅 SAP 官方说明：1953429 - SAP HANA and SAP NetWeaver AS ABAP on one Server。

三层架构（SAP NetWeaver 应用服务器横向扩展）

面对更高的工作负载，SAP 支持按需使用多个应用服务器的横向扩展架构。

在横向扩展配置中，各节点必须访问同一个共享文件系统。对于 Linux，请使用“网络文件系统”(NFS) 作为中央系统的 NetWeaver 二进制文件/配置文件磁盘的文件共享系统（/sapmnt/[SID]，其中 [SID] 是系统 ID）。更多详细信息，请参阅 SAP 标准文档。

下图给出了运行于阿里云之上的三层横向扩展架构的一些细节：



在此架构中，SAP NetWeaver 系统可将工作负载分配给托管于多个 ECS 实例上的多个 NetWeaver 应用服务器 (AS)。所有 NetWeaver AS 节点共享同一个数据库，该数据库托管在一个单独的 ECS 实例上。

所有 NetWeaver AS 节点都安装并访问一个共享文件系统，该文件系统中托管有 SAP NetWeaver 二进制文件和配置文件。对于 Linux，请使用“网络文件系统”(NFS) 作为中央系统的 NetWeaver 二进制文件/配置文件磁盘的文件共享系统（/sapmnt/[SID]，其中 [SID] 是系统 ID）。更多详细信息，请参阅 SAP 标准文档。

在本文的示意图中，该共享文件系统位于一个与 SAP Central Services 一起挂载至 ECS 实例 1 的云盘中。

高可用性

关于在阿里云平台上为 SAP 解决方案规划和设置高可用性的指南和最佳实践，我们将尽快提供此类文档。

阿里云 ECS

ECS 实例类型

阿里云 ECS 提供了多种实例类型（虚拟机规格）以部署 SAP 解决方案。每一种实例类型提供不同的 CPU、内存和 I/O 能力。您只能在通过 SAP 认证的 ECS 实例上运行 SAP 应用程序。有关通过 SAP 认证的可用于 SAP NetWeaver 的实例类型的列表，请参考以下内容；最新信息请参阅 SAP 说明 2552731 - SAP Applications on Alibaba Cloud: Supported Products and IaaS VM types

实例类型	vCPU	内存（GiB）
ecs.sn2ne.large	2vCPUs	8GiB
ecs.sn2ne.xlarge	4vCPUs	16GiB
ecs.sn2ne.2xlarge	8vCPUs	32GiB
ecs.sn2ne.3xlarge	12vCPUs	48GiB
ecs.sn2ne.4xlarge	16vCPUs	64GiB

ecs.sn2ne.6xlarge	24vCPUs	96GiB
ecs.sn2ne.8xlarge	32vCPUs	128GiB
ecs.sn2ne.14xlarge	56vCPUs	224GiB
ecs.r5.large	2vCPUs	16GiB
ecs.r5.xlarge	4vCPUs	32GiB
ecs.r5.2xlarge	8vCPUs	64GiB
ecs.r5.3xlarge	12vCPUs	96GiB
ecs.r5.4xlarge	16vCPUs	128GiB
ecs.r5.6xlarge	24vCPUs	192GiB
ecs.r5.8xlarge	32vCPUs	256GiB
ecs.g5.large	2vCPUs	8GiB
ecs.g5.xlarge	4vCPUs	16GiB
ecs.g5.2xlarge	8vCPUs	32GiB
ecs.g5.3xlarge	12vCPUs	48GiB
ecs.g5.4xlarge	16vCPUs	64GiB
ecs.g5.6xlarge	24vCPUs	96GiB
ecs.g5.8xlarge	32vCPUs	128GiB
ecs.g6.large	2vCPUs	8GiB
ecs.g6e.large	2vCPUs	8GiB
ecs.g6.xlarge	4vCPUs	16GiB
ecs.g6e.xlarge	4vCPUs	16GiB
ecs.g6.2xlarge	8vCPUs	32GiB
ecs.g6e.2xlarge	8vCPUs	32GiB
ecs.g6.3xlarge	12vCPUs	48GiB
ecs.g6.4xlarge	16vCPUs	64GiB
ecs.g6e.4xlarge	16vCPUs	64GiB
ecs.g6.6xlarge	24vCPUs	96GiB
ecs.g6e.6xlarge	24vCPUs	96GiB
ecs.g6.8xlarge	32vCPUs	128GiB
ecs.g6e.8xlarge	32vCPUs	128GiB
ecs.r6.large	2vCPUs	16GiB
ecs.r6e.large	2vCPUs	16GiB
ecs.r6.xlarge	4vCPUs	32GiB

ecs.r6e.xlarge	4vCPUs	32GiB
ecs.r6.2xlarge	8vCPUs	64GiB
ecs.r6e.2xlarge	8vCPUs	64GiB
ecs.r6.3xlarge	12vCPUs	96GiB
ecs.r6.4xlarge	16vCPUs	128GiB
ecs.r6e.4xlarge	16vCPUs	128GiB
ecs.r6.6xlarge	24vCPUs	192GiB
ecs.r6e.6xlarge	24vCPUs	192GiB
ecs.r6.8xlarge	32vCPUs	256GiB
ecs.r6e.8xlarge	32vCPUs	256GiB
ecs.c6.large	2vCPUs	4GiB
ecs.c6e.large	2vCPUs	4GiB
ecs.c6.xlarge	4vCPUs	8GiB
ecs.c6e.xlarge	4vCPUs	8GiB
ecs.c6.2xlarge	8vCPUs	16GiB
ecs.c6e.2xlarge	8vCPUs	16GiB
ecs.c6.3xlarge	12vCPUs	24GiB
ecs.c6.4xlarge	16vCPUs	32GiB
ecs.c6e.4xlarge	16vCPUs	32GiB
ecs.c6.6xlarge	24vCPUs	48GiB
ecs.c6e.6xlarge	24vCPUs	48GiB
ecs.c6.8xlarge	32vCPUs	64GiB
ecs.c6e.8xlarge	32vCPUs	64GiB

有关 ECS 实例类型的详细介绍，请查看阿里云官方网站。

每个经过 SAP 认证的 ECS 实例类型均使用 SAP 的“标准应用销售和分销”(SD) 基准工具包来确定规格。关于各个 SAP 认证实例的 SAPS 评级，请参阅 SAP 说明 2552731 - SAP Applications on Alibaba Cloud: Supported Products and IaaS VM types

镜像

创建 ECS 实例时，您使用的是包含预先安装的基本操作系统的镜像。阿里云与操作系统合作伙伴合作，为您提供最新的、经过优化的操作系统镜像。有多种方法可以为您的 ECS 实例指定镜像。

公共镜像

公共镜像的操作系统许可证费用已包含在 ECS 实例收费价格中。您无需提供您自己的操作系统许可证。下列各项是公共镜像列表中可用的 SAP NetWeaver 所需的操作系统：

Linux

- SUSE Linux Enterprise Server 12 SP2 (SLES12) 以及更高
- Red Hat Enterprise Linux 7.4 (RHEL7) 以及更高

Windows

- Microsoft Windows Server 2012 R2, 2016 以及 2019

有关支持的操作系统的最新信息，请参阅 SAP 说明 2552731 - SAP Applications on Alibaba Cloud: Supported Products and IaaS VM types.

地域和可用区

阿里云基础设施是围绕地域和可用区而建立的。地域是指地球上某个具体的物理位置，大多数情况下，我们有多个地域。可用区由一个或多个分散的机房组成，每个机房都有冗余的电源、网络和连接功能，并位于单独设施中。这些可用区为您提供了运行生产环境应用程序和数据库的能力，相比单个机房具有更高的可用性、容错性和可扩展性。阿里云在全球 14 个地域运营着 29 个可用区。

VPC

专有网络 (Virtual Private Cloud, VPC) 允许您在阿里云中构建出一个专用的、隔离的网络环境，您可以在自己定义的虚拟网络中运行 IaaS 资源。借助 VPC，您可以定义一个与自己的机房所在的传统运营网络极其相似的虚拟网络拓扑。此外，您可以在您的企业机房与阿里云 VPC 之间建立连接，并利用阿里云作为您企业机房的扩展。

部署 ECS 实例

您可以使用标准的阿里云方法，在阿里云平台上部署您的 ECS 实例，其中包括 ECS 控制台（云平台控制台 Web UI）和 REST API。您可以阅读以下页面获取更多有用信息。

- 创建 ECS 实例
- 启动和查看 ECS 实例

有关在 ECS 上部署 SAP NetWeaver 系统的详细信息和分步说明，请参阅阿里云 SAP NetWeaver 实施指南。

访问 ECS 实例

对于基于 Linux 的 ECS 实例，用户能够使用 SSH 功能，可以通过基于 SSH 的工具（如 PuTTY）访问 ECS 实例。例如，您可以借助 PuTTY 从跳板机访问 ECS 实例。

对于基于 Windows 的 ECS 实例，用户可以通过远程桌面协议 (RDP) 访问 ECS，只要公网 IP 地址能够访问 ECS 实例。

数据库

对于阿里云 SAP NetWeaver，您可以使用 SAP HANA。

SAP HANA

SAP HANA 目前仅支持用于 SUSE Linux Enterprise Server。有关受支持的 ECS 实例类型和操作系统的更多信息，请参阅 SAP HANA 部署指南。

有关 SAP HANA 的更多信息，请参阅 SAP HANA 操作指南和 SAP 文档。

要获得 SAP HANA 的规格准则和建议，请查看 SAP 官方网站的相关信息。

数据库备份和恢复

由于大多数 SAP NetWeaver 系统都用于任务关键型工作负载，因此客户必须具有数据备份和恢复计划，以确保在最坏情况发生时可以恢复其系统和数据库。

有关 SAP HANA 备份和恢复的信息，请参阅阿里云 SAP HANA 操作指南，具体如下：

- 操作指南，https://www.alibabacloud.com/help/doc-detail/57886.htm
- 备份和恢复，https://www.alibabacloud.com/help/doc-detail/57886.htm

存储

默认情况下，每个 ECS 实例都有一个包含操作系统的小型系统盘（高效云盘或 SSD 云盘）。您可以添加额外的数据盘，并将它们挂载到 ECS 实例，以充当您系统不同组件的存储盘。

块存储（云盘）

阿里云块存储（云盘）可提供与阿里云 ECS 实例配合使用的永久块级存储卷。您可以根据您的需求选择不同的云盘类型：

云盘类别	普通云盘	高效云盘	SSD 云盘
单盘最大容量	2 TB	32.768 TB	32.768 TB
单盘最大 IOPS	300+ IOPS	3,000 IOPS	20,000 IOPS
单盘最大吞吐量	20~40 MBps	80 MBps	300 MBps
访问时延	5.0~10.0 ms	1.0~3.0 ms	0.5~2.0 ms

典型应用场景	数据不被经常访问或者低 I/O 负载的应用场景。	- 中小型数据库。 - 开发和测试。 - 云服务器日志记录。	- I/O 密集型应用。 - 大中型关系数据库。 - NoSQL 数据库。

对于**数据可靠性**，凭借采用三重存储系统的阿里云分布式存储技术的优势，这三种类型的云盘都可以保证 99.9999999% 的数据完整性。 |

一般来说，我们推荐以下磁盘布局：

磁盘布局	使用情况	云盘类型
系统盘	操作系统	高效云盘
数据盘 1	NetWeaver、数据库的执行文件、配置文件等	SSD 云盘
数据盘 2	数据库的数据文件	SSD 云盘
数据盘 3	数据库的日志文件	SSD 云盘

对于 SAP HANA 数据库，我们推荐使用 SSD 云盘。有关如何为 SAP HANA 设置存储系统的更多信息，请参阅阿里云 SAP HANA 操作指南。

对象存储服务 (OSS)

阿里云对象存储服务是面向任何类型或格式的文件的对象存储；它具有几乎无限的存储空间，您无需担心容量限制或扩容问题。

通常做法是使用 OSS 长期存储备份文件。

网络和安全

安全组

安全组功能类似于虚拟防火墙，用于为一个或多个 ECS 实例设置网络访问控制。创建实例时，您必须选择一个安全组。您还可以添加安全组规则，来控制安全组中所有 ECS 实例的流出和流入网络访问。

SSH 密钥对

阿里云提供两种远程登录 ECS 实例的鉴权方式：

- **密码登录**：使用管理员密码的标准鉴权方式。它适用于 Windows 实例和 Linux 实例。
- **SSH 密钥对登录**：此方法仅适用于 Linux 实例。如果您运行在 Linux 之上，建议您选择此鉴权方式来保护 ECS 实例的安全。

SSH 密钥对是由加密算法生成的一对密钥：一个对外界公开，称为公钥；另一个您自己保留，称为私钥。

阿里云将默认为您创建 2048 位的 RSA 密钥对。您也可以导入由其他密钥对生成工具生成的密钥对的公钥。更多详细信息，请访问以下链接了解阿里云 SSH 密钥对：https://www.alibabacloud.com/help/doc-detail/51792.htm。

如果您将公钥放在 Linux 实例中，则可以使用私钥通过 SSH 命令或相关工具从本地计算机或其他实例登录此实例，而无需输入密码。

路由器配置

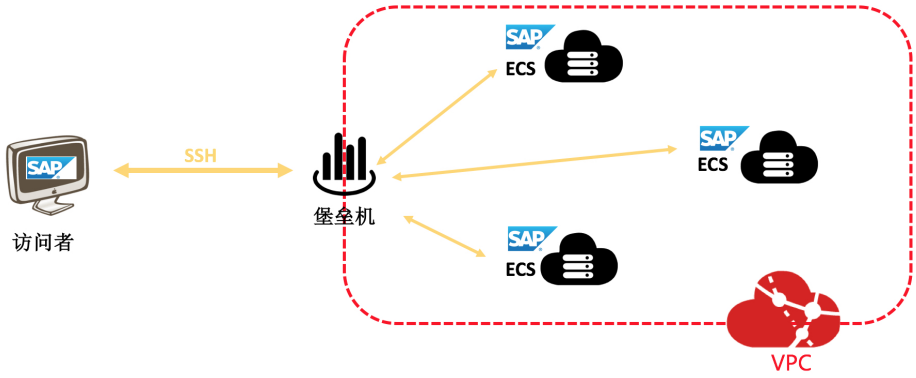
在阿里云创建 VPC 网络时，系统会在 VPC 创建后自动创建路由器和路由表。您不能直接创建或删除它们。VPC 删除后，这些路由器和路由表将自动删除。您可以将路由条目添加到路由表，以路由网络流量。

路由表中的每个条目都用于引导网络流量的方向。创建 VPC 时，系统会默认添加一条目标 CIDR 网段为 100.64.0.0/10 的路由条目。您可以为您的 VPC 添加自定义路由条目。

如果 VPC 中不含外部 IP 地址的 ECS 实例想要访问外网，则需要 NAT 网关。可以通过以下链接查看有关 NAT 网关的更多详细信息：https://www.alibabacloud.com/product/NAT。

堡垒机

堡垒主机提供进入包含专有网络虚拟机的 VPC 网络的外部入口点。该主机可提供单点防御或审计，可以启动和停止该功能，以启用或禁用来自外网的流入 SSH 通信。



通过先连接到堡垒主机，可以实现对没有外部 IP 地址的虚拟机的 SSH 访问。

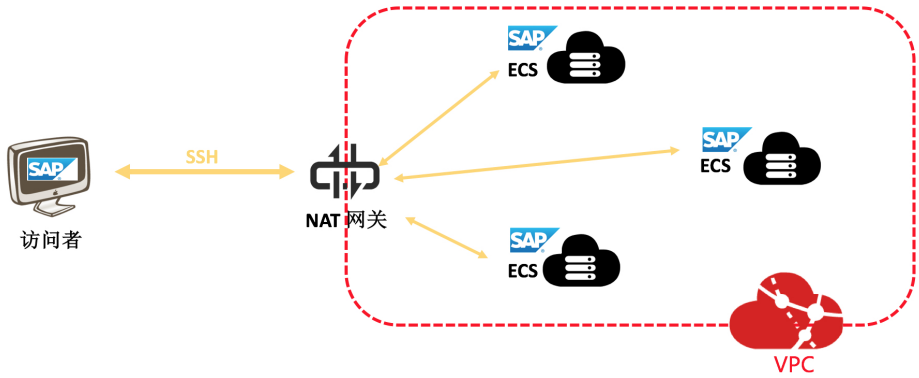
使用堡垒主机时，首先登录堡垒主机，然后通过基于 SSH 的工具（如 PuTTY）登录至目标专有 ECS 实例。

NAT 网关

如果一个 ECS 实例创建于 VPC 内部，并且没有分配外部 IP 地址，那么它不能直接连接到外部服务。

要允许这些 ECS 实例访问外网，您可以设置并配置 NAT 网关。NAT 网关可以代表 VPC 中的任何 ECS 实例进行流量路由。每个 VPC 都应当有一个 NAT 网关。

在部署 SAP 解决方案时，必须为 VPC 配置一个含有 SNAT 的 NAT 网关。有关此配置的更多详细信息，请参阅实施指南。

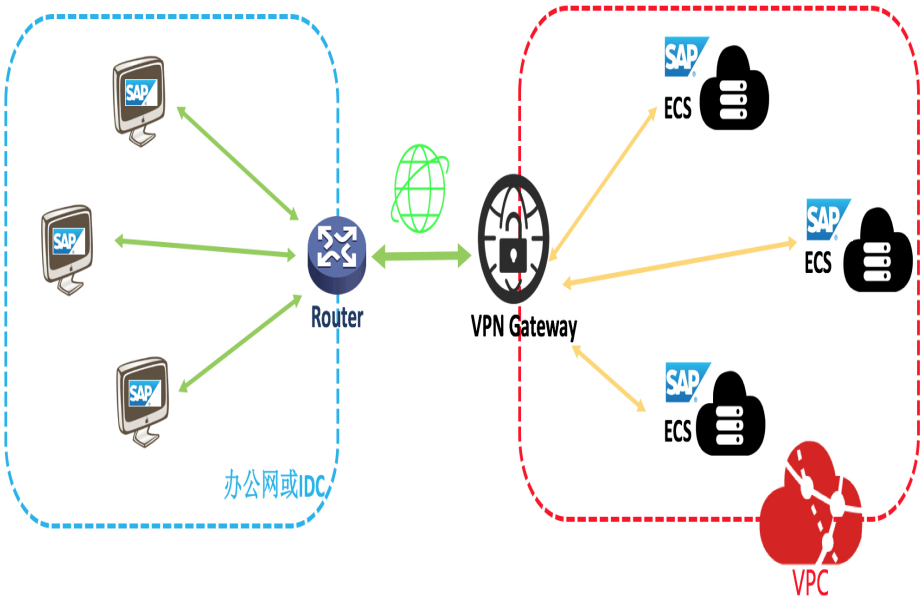


关于 NAT 网关的更多详细信息，可查阅阿里云官方网站，如下所示：
https://www.alibabacloud.com/product/NAT

如果您想允许从外网访问您的 SAP 系统，建议您使用 NAT 网关。

VPN 网关

您可以在阿里云中通过 VPN 网关和 VPN 连接（使用 IPSec）将您现有的 IDC 和阿里云专有网络 (VPC) 安全地连接起来。两个网络之间的流量传输由一个 VPN 网关加密，然后由另一个 VPN 网关解密。这可以保护您在外网中的数据传输。欲了解更多信息，请查阅阿里云官方网站。



关于 VPN 网关的更多详细信息，可查阅阿里云官方网站，如下所示：
https://www.alibabacloud.com/product/vpn-gateway

如果您只想从本地机房或办公室局域网访问您的 SAP 系统，建议您通过 VPN 网关将您的本地机房和办公室局域网与阿里云专有网络连接起来。

安全文档

以下附加资源可帮助您从安全性和合规性的角度进一步了解阿里云中的 SAP 环境：

- 安全合规中心
- 云盾白皮书

系统拷贝和迁移

请首先参阅 SAP 官方文档“系统拷贝和迁移指南”：http://support.sap.com/sltoolset -> System Provisioning -> System Copy Option。

SAP 通过 Software Provisioning Manager 1.0 提供系统拷贝和迁移服务，使您能够创建 SAP 系统的一致副本

- 如果源系统和目标系统采用相同的操作系统和数据库系统，需要使用 **同构系统复制。**
  对于同构系统复制，您可以有以下选项：
  - 使用数据库独立进程 (R3load / JLoad)；
  - 数据库还原/恢复；（使用数据库还原和恢复可以最大限度地降低系统停机时间。特别是将这种方法与某种日志传送结合起来时更为有效）；
- 如果源系统和目标系统采用不同的操作系统或数据库系统，需要使用 **异构系统复制**
  - 可以通过以下链接找到系统拷贝指南：https://help.sap.com/viewer/nwguidefinder
  - 对于异构 SAP 系统复制，需要咨询具有 SAP 迁移认证的顾问。

有关 SAP 系统拷贝和迁移最佳实践的详细信息，请参阅此链接：
https://wiki.scn.sap.com/wiki/display/SL/System%2BCopy%2Band%2BMigration

SAP NetWeaver 监控和支持

云环境中的 SAP 应用程序运行在虚拟环境下安装的客户操作系统 (Guest OS) 上。SAP Host Agent 可收集 SAP 监控所需的全部信息，并将其提供给 SAP NetWeaver 本地监控和 Solution Manager，以用于分析和显示。客户或 SAP 技术支持人员可通过 SAP 事务代码 ST06 访问 SAP 工具，无论是通过本地 ABAP 监控系统，还是通过 SolutionManager（用于阿里云中运行的受管系统）。

除此之外，阿里云与 SAP 共同合作，为运行在阿里云上的 SAP NetWeaver 构建了一款监控代理程序 - ECS Metrics Collector。ECS Metrics Collector 负责从底层的阿里云基础设施和虚拟化平台收集有关配置和资源（CPU\内存\磁盘\网络）利用率的信息，并将其提供给 SAP Host Agent。

有关如何安装 ECS Metrics Collector 的详细信息和分步说明，请参阅“阿里云 SAP NetWeaver 实施指南”；有关其生命周期和操作的详细信息，请参阅“阿里云 SAP NetWeaver 操作指南”。

许可

SAP 许可证

在阿里云运行 SAP 需要您自行拥有许可证 (BYOL)。

有关 SAP 许可证的更多信息，请联系 SAP。

Linux 许可证

在阿里云中，有两种获得 SUSE Linux 许可证的方式：

- 按量付费许可模式：阿里云提供 SLES 11 SP4 和 SLES 12 SP2 作为公共镜像，SLES 许可证费用包含在 ECS 实例价格中
- BYOL 模式：客户可以购买自己的 SLES 许可证，并导入 SLES 操作系统作为自定义镜像。

安装介质

将 SAP 安装介质复制到 ECS 实例主要有两种选择：

- 直接从 SAP Service Marketplace 下载到 ECS 实例。从您的 ECS 实例连接到 SAP Service Marketplace 并下载所需的安装介质。此选项很可能是在阿里云中获取 SAP 安装介质的最快方法，因为 ECS 实例与外网的连接速度非常快。您可以创建专用的 ECS 实例，以下载和存储 SAP 安装介质。
- 从您的网络复制到 ECS 实例。如果您已经将所需的 SAP 安装介质下载到您网络中的某个位置，则可以将该介质从您的网络直接复制到 ECS 实例。

SAP Router 和 Solution Manager

以下部分介绍了在阿里云运行 SAP 解决方案时，SAP Solution Manager 和 SAProuter 的相关选项。

混合架构 - 一部分 SAP 解决方案在云端，一部分 SAP 解决方案在本地 IDC
如果将阿里云用作 IT 基础设施的扩展，您可以使用您在本地机房运行的现有 SAP Solution Manager 系统和 SAProuter，来管理运行在阿里云专有网络中的 SAP 系统。

纯阿里云架构
在阿里云中设置 SAP 环境时，您需要设置 SAP Solution Manager 系统和 SAProuter 并连接至 SAP 支持网络，就像部署在任何基础设施上一样。

设置 SAProuter 和 SAP 支持网络连接时，请遵循以下准则：

- 要在其中安装 SAProuter 软件的实例必须启动到阿里云专有网络的公共子网中，并为其分配弹性公网 IP 地址 (EIP)。
- 需要为 SAProuter 实例创建一个特定的安全组，其中配置必要的规则以允许对 SAP 支持网络进行所需的流入和流出访问。
- 您应当使用安全网络通信 (SNC) 类型的外网连接。有关更多信息，请参阅

https://support.sap.com/en/tools/connectivity-tools/remote-support.html

SAP NetWeaver 部署指南

- 部署 SAP 系统
    - 前提条件
        - 帐户设置
        - 创建专有网络 (VPC)
        - 创建安全组
        - 从外网连接 ECS 实例
        - RAM 服务角色设置
    - 创建和配置实例
        - 打开 ECS 购买页面
        - 选择计费方式
        - 选择机房地域和可用区
        - 选择实例类型
        - 选择镜像
        - 供应和配置存储
        - 安全设置
    - 实例配置后
        - 连接至 SAP ECS 实例
        - 操作系统安全加固
        - 更改主机名
        - RAM 角色配置
        - 准备 SAP 安装介质
        - ECS Metrics Collector 安装和验证
        - 检查操作系统
        - 创建操作系统镜像
    - 安装 SAP 解决方案
        - 启动 SWPM
        - 升级 SAP kernel
        - 检查 Host Agent 版本
        - 升级 Host Agent
        - 安装横向扩展系统
        - 安装单一节点系统
    - 安装后
        - 创建 SAP 实例镜像
- SAP 系统迁移
    - VM 导入/导出工具
    - SAP 同构和异构系统复制

- 第三方工具

本指南提供了有关部署您自己的基于 SAP NetWeaver 的系统以及将现有 SAP 系统迁移至阿里云的说明。

部署 SAP 系统

前提条件

对于在传统基础设施上部署和运行 SAP 系统方面经验丰富的 SAP 管理员，以下前提条件知识可帮助您在开始为 SAP 创建 ECS 实例以及部署 SAP 系统之前，了解一些公共云特定的任务。

帐户设置

- 注册阿里云帐户
- 添加支付信息
- 实名登记，只有在位于中国大陆境内的地域创建 ECS 实例时才需要

创建专有网络 (VPC) 和交换机

1.登录**专有网络控制台**。

2.在左侧导航窗格中，单击**专有网络**。

3.选择专有网络的所属地域。

4.单击右上角的**创建专有网络**。

5.在弹出的对话框中，输入专有网络名称，并以无类域间路由网段的格式选择专有网络的 IP 地址范围。

对于 IP 地址范围，使用以下的标准 CIDR 网段格式之一。专有网络创建后，CIDR 网段将无法修改。关于更多详细信息，请参阅**创建专有网络**。

- 10.0.0.0/8 (10.0.0.0 - 10.255.255.255)
- 172.16.0.0/12 (172.16.0.0 - 172.31.255.255)
- 192.168.0.0/16 (192.168.0.0 - 192.168.255.255)


创建专有网络
如何搭建专有网络
专有网络
地域
华东 1
名称
0/128
目标网段
192.168.0.0/16
一旦创建成功，网段不能修改
描述
0/256
交换机
名称
0/128
可用区
请选择
创建专有网络
如何搭建专有网络
专有网络
地域
华东 1
名称
0/128
目标网段
192.168.0.0/16
一旦创建成功，网段不能修改
描述
0/256

6.单击**创建专有网络**。

专有网络VPC（Virtual Private Cloud）是基于阿里云构建的一个隔离的网络环境，专有网络之间逻辑上彻底隔离。专有网络是您自己独有的的云上私有网络。您可以完全掌控自己的专有网络，例如选择IP地址范围、配置路由表和网关等。具体详细信息和文档请参考 产品文档.

创建VPC，本示例如下：



规划业务网段，本示例如下:



创建安全组

安全组是一个逻辑上的分组，这个分组是由同一个地域（Region）内具有相同安全保护需求并相互信任的实例组成。每个实例至少属于一个安全组，在创建的时候就需要指定。同一安全组内的实例之间网络互通，不同安全组的实例之间默认内网不通。可以授权两个安全组之间互访。

安全组是一种虚拟防火墙，具备状态检测包过滤功能。安全组用于设置单台或多台云服务器的网络访问控制，它是重要的网络安全隔离手段，用于在云端划分安全域。

一台ECS实例必须至少属于一个安全组。具体详细信息和文档请参考**安全组**。

新建安全组，选择刚才创建的专有网络，本示例如下：



添加安全组规则

找到刚才创建的安全组，在“操作”栏中单击“配置规则”。

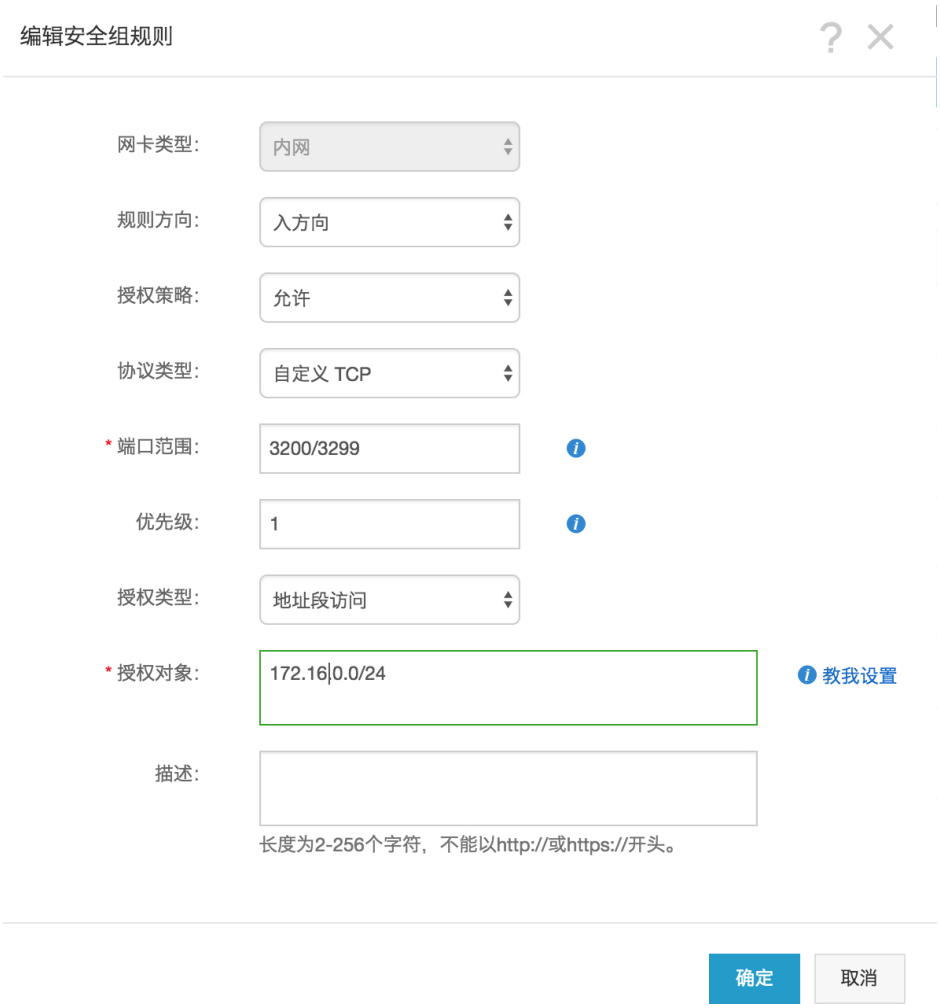
在“安全组规则”页面上，单击“添加安全组规则”。

端口范围的设置受选择的协议类型影响。SAP 系统要求访问某些端口，因此需添加防火墙规则以允许访问关于SAP系统使用的端口请参考 SAP系统端口概述。下表给出了常用端口示例。

协议类型	端口范围	应用场景
全部	显示为 -1/-1，表示所有端口。	应用场景： - **对流出调用没有限制；** - 两种应用相互完全信任。
RDP	显示为 3389/3389，默认 RDP 端口为 3389。	显示为 3389/3389，默认 RDP 端口为 3389。
SSH	显示为 22/22，默认 SSH 端口为 22。	用于远程连接到 Linux 实例。
TELNET	显示为 23/23。	用于通过 Telnet 远程登录实例。
HTTP	显示为 80/80。	实例作为网站或 Web 应用的服务器。
HTTPS	显示为 443/443。	实例作为支持 HTTPS 协议的网

		站或 Web 应用的服务器。
MS SQL	显示为 1433/1433。	实例作为 MS SQL 服务器。
Oracle	显示为 1521/1521。	实例作为 Oracle SQL 服务器。
SAP Dispatcher	范围为 3200-3299	SAP GUI 在 Windows 和 Java 环境下使用。
SAP Gateway	范围为 3300-3399	用于 CPIC 和 RFC 通信。
SAP Message server	范围为 3600-3699	用于 SAP 消息服务器通信。

示例：允许172.16.0.0/24网段通过32xx端口访问到本示例中专有网络”SAP_Network”下的ECS服务器，创建规则如下：



从外网连接 ECS 实例

VPC 是在阿里云中创建的一种专有网络。VPC 在逻辑上与阿里云中的其他虚拟网络隔离开。您可以使用 NAT 网关或 EIP（弹性公网 IP）从外网连接至 ECS 实例。

NAT 网关是一款企业级公共网关，提供 NAT 代理服务（SNAT 和 DNAT）、高达 10 Gbps 的转发能力以及跨可用区灾难恢复能力。作为一个公网网关，NAT 网关需要配置公网 IP 和带宽。NAT 网关上的公网 IP 被归类为“共享带宽包”抽象组。

EIP 地址是 NAT IP 地址的一种类型。它位于阿里云的公共网关上，通过 NAT 方式映射到了被绑定 ECS 实例的专有网卡 (NIC) 上。因此，绑定了 EIP 地址的 ECS 实例可以与外网通信，却不会暴露 NIC 的 EIP 地址。

对于运行 SAP 应用的每个 ECS 实例，均需要安装 ECS Metrics Collector。因此，出于 SAP 系统性能数据收集的需要，您的 SAP ECS 实例还需要能够访问外网。有两种方式可以实现这种访问，您可以将一个 EIP 直接绑定到 ECS 实例，或者您可以使用一个 NAT 网关，为您的 ECS 实例配置 SNAT。

有关NAT网关的详细说明和使用，请参考 NAT网关

有关EIP的详细说明和使用，请参考 EIP弹性IP

创建弹性公网 IP (EIP)

弹性公网 IP (Elastic IP，简称 EIP) 是可以独立购买和持有的公网 IP 地址资源。EIP 可动态绑定到 VPC ECS 实例，而无需重启该 ECS 实例。

1.在控制台点击“专有网络VPC”-》“弹性公网 EIP”，点击“申请弹性公网IP”

2.在购买页面上，选择 付费方式、EIP 地址的地域、带宽和购买数量，然后点击“立即购买”。



3.完成付款。

4.EIP绑定ECS实例

返回EIP控制台点击“刷新”，将刚才创建的EIP绑定到指定ECS实例，本示例如下：



选择实例类型“ECS”和对应的ECS实例



EIP 地址绑定到 ECS 实例后，ECS 实例便可以和外网进行通信。确保配置的安全组规则不会阻止外网访问。

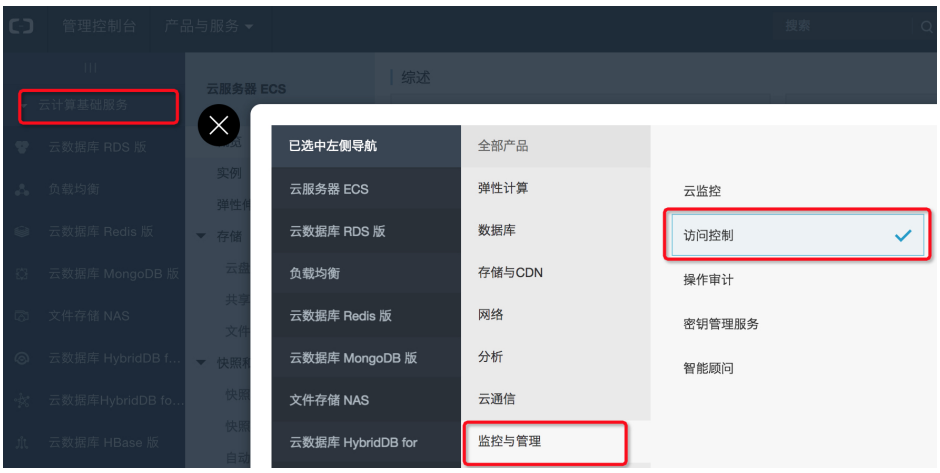
RAM 服务角色设置

监控代理 **ECS Metrics Collector**（专为在阿里云基础设施上运行的 SAP 系统而设计）需要特定的 RAM 服务角色设置。请注意，这只是一次性工作，因为它在您的帐户级别始终有效。有关 RAM（访问控制）角色设置的更多信息，请参阅如何通过控制台使用实例 RAM 角色。

1.登录 ECS 控制台。

2.在左侧导航窗格中，单击“访问控制”。

如果左侧导航栏没有“访问控制”，请修改导航配置，“监控与管理”，勾选“访问控制”



确认开通



3.打开访问控制服务控制台，选择**角色**选项卡，然后单击**创建角色**



4.在**选择角色类型**步骤中，选择**服务角色**



5.在**填写类型信息**步骤中，选择 **ECS云服务器**



6.在**配置基本信息**步骤中，您必须定义一个角色名称。例如，您可以添加 **ecs-metrics-collector** 作为角色名称

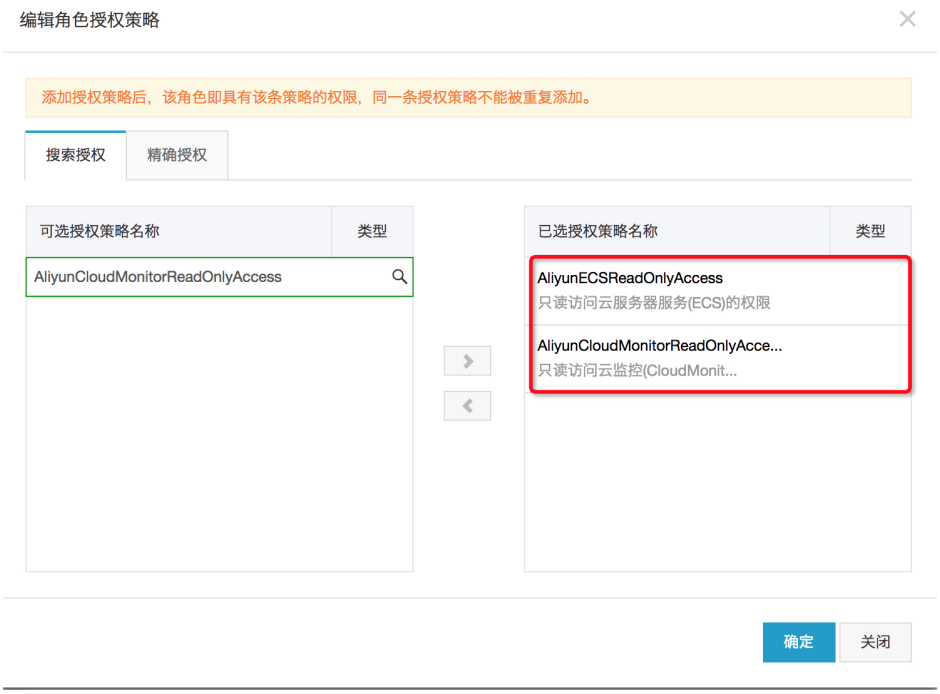


。然后单击**创建**

7.服务角色创建成功。单击**授权**进入后续步骤



8.单击**编辑授权策略**。选择策略名称 AliyunECSReadOnlyAccess和AliyunCloudMonitorReadOnlyAccess 并将其分配给您的 RAM 服务角色



9.单击**确定**，完成策略分配。



创建和配置实例

要创建一个 ECS 实例用于在阿里云部署 SAP NetWeaver，请执行以下步骤：

打开 ECS 购买页面

- 登录 ECS 控制台。
- 在左侧导航窗格中，单击**实例**。

- 在**实例列表**页面，单击**创建实例**。

选择计费方式

您可以选择**包年包月付费**或者**按量付费**，作为您实例的计费方式。

请参见 ECS 产品定价和价格计算器，计算产品价格。

选择机房地域和可用区

通常情况下，所有 SAP 应用程序（SAP ERP、CRM、SRM 等）及系统（SAP DB、SAP 应用服务器）建议部署在同一个可用区中。实例创建之后，不能更换地域和可用区。在选择地域和可用区时，您需要考虑几个因素：

- 通常情况下，如果您的实例所在地域与您的客户较为接近，那么客户在使用您的服务时，可以有较低的网络时延和更快的下载速度。
- 某些功能（如可用区数量、实例类型、存储类型和网络服务定价）因地域而异。选择一个恰当的地域，以满足您的业务需求。
- 中国大陆以外地域的 ECS 实例不支持 Linux 系统之间的交换。
- 如果要为 SAP 系统创建多个实例：
    - 如果您需要较低的网络时延，我们建议您在相同的可用区内创建实例。
    - 如果对灾难恢复有更高要求，我们建议您在同一地域的不同可用区内创建实例。
- 不同地域的实例之间无法通过内网互相通信。

选择实例类型

实例类型的可用性因地域而异。请参见“产品说明”中的实例规格系列，了解各实例类型的应用场景。

> 注意：如果您选择了“按量付费”计费方式，您将无法从实例类型中购买所有 ECS 实例。如果您需要的实例不在列表中，您可以向阿里云支持提交工单进行购买。

阿里云 ECS 实例提供了大量实例类型（虚拟机规格）。建议使用通过 SAP 认证的 ECS 实例上运行 SAP 应用程序。有关通过 SAP 认证的可用于生产环境的实例类型的列表，请参阅以下内容：

实例类型	系列	vCPU	内存 (GiB)
ecs.sn2ne.large	sn2ne	2	8
ecs.sn2ne.xlarge	sn2ne	4	16
ecs.sn2ne.2xlarge	sn2ne	8	32
ecs.sn2ne.4xlarge	sn2ne	16	64
ecs.sn2ne.8xlarge	sn2ne	32	128
ecs.sn2ne.14large	sn2ne	56	224
ecs.r5.large	r5	2	16.0

ecs.r5.xlarge	r5	4	32.0
ecs.r5.2xlarge	r5	8	64.0
ecs.r5.3xlarge	r5	12	96.0
ecs.r5.4xlarge	r5	16	128.0
ecs.r5.6xlarge	r5	24	192.0
ecs.r5.8xlarge	r5	32	256.0

更多信息请参阅 SAP Note 2552731 - SAP Applications on Alibaba Cloud: Supported Products and IaaS VM types.

选择镜像

公共镜像：内含阿里云官方提供的操作系统镜像。最重要的是，您需要根据您的具体要求，安装相关软件并配置应用环境。建议使用SUSE Linux Enterprise Server for SAP，用以运行 SAP应用系统和数据库：

从镜像市场选择，选择“SUSE linux for SAP-12SP2”镜像



供应和配置存储

您必须选择云盘作为系统盘和数据盘。阿里云为您的 ECS 实例提供了灵活、经济高效且易于使用的数据存储选项。

- **系统盘**是必需的。它用于安装操作系统。
  - 本地、临时和基于实例的存储。
  - 存储在实例存储卷上的数据将保持不变，直到 ECS 实例被释放。
  - 对于系统盘，我们推荐使用高效云盘；您可以选择 SSD 云盘获取更出色的性能。
- 您在此处添加的**数据盘**将随实例一起释放，不能从实例中分离。您可以独立创建云盘。

    - 永久块级存储卷，配合 ECS 实例使用。
    - 对于数据盘，我们推荐 SAP 非生产环境使用高效云盘，SAP 生产环境使用 SSD 云盘。
  - 每个用户帐户最多可同时拥有 250 个云盘，单盘最大容量为 32768 GB。
  - 根据业务需求，最多可添加 16 个数据盘，可以是空白或来自快照。

云盘类型因地域而异。请参见云盘参数和性能测试，了解云盘功能差异。云盘有三种不同的卷类型，每种类型具备独特的性能和持久性组合。

  - SSD 云盘
    适用于 I/O 密集型应用，提供稳定的高随机 IOPS 性能。
  - 高效云盘
    适用于具有中等 I/O 负载的应用场景，可为 ECS 实例提供最高 3000 个随机 IOPS 的存储性能。
  - 普通云盘
    适用于具有低 I/O 负载的应用场景，可为 ECS 实例提供数百个 IOPS 的 I/O 性能。

对于您的 SAP 生产环境，建议的存储选项如下所示：

目录	磁盘类型
SAP 软件	SSD 云盘
DB 数据文件	SSD 云盘
DB 日志文件	SSD 云盘
数据库的备份文件	高效云盘
SAP 数据归档	高效云盘

对于 SAP HANA，我们推荐所有环境均使用 SSD 云盘。有关 HANA 存储配置的更多信息，请参阅阿里云 SAP HANA 部署指南。

目录	磁盘类型
HANA 共享文件	SSD 云盘
HANA 数据文件	SSD 云盘
HANA 日志文件	SSD 云盘
数据库的备份文件	高效云盘

安全设置

您可以基于操作系统设置鉴权方式。

操作系统	鉴权方式
Linux	SSH 密钥对或密码

  - 您有两种选择：现在设置或以后设置鉴权方式。

- 如果您想以后再设置鉴权方式，则在创建实例后，在 ECS 控制台中重置密码或绑定 SSH 密钥对。

安装后配置

连接至 SAP ECS 实例

一般情况下，如果您的 SAP ECS 实例不使用外部 IP，则只能使用 SSH 通过堡垒实例连接至 SAP 系统实例。

要通过堡垒实例连接到 SAP 系统，请使用您所选择的 SSH 客户端连接到堡垒主机，然后再连接到 SAP 系统 ECS 实例。

要从堡垒主机通过 SWPM 安装或维护 SAP 系统，您应当在 Windows 操作系统上安装堡垒主机。使用 GUI 或浏览器启动 SWPM。

要通过 SAP HANA Studio 连接到 SAP HANA 数据库，请使用远程桌面客户端连接到 Windows Server 实例。建立连接后，手动SAP HANA Studio Installation and Update Guide 并访问您的 SAP HANA 数据库。

操作系统安全加固

在创建实例之后，为了实例的安全性，我们建议您对以下项目执行安全合规性检查和配置：

- Linux 实例：参见安全公告中的 Linux 操作系统加固。

更改主机名

ECS 实例默认命名为实例 ID，运行 SAP 软件的主机的命名必须遵循一般标准和某些 SAP 特定限制，例如 SAP rel. 4.6 或更高版本的主机名长度限定为最多 13 个字符。请参考 SAP Note 611361 - Hostnames of SAP servers 了解更多详细信息。

对于您运行在 SUSE Linux 系统上的 SAP 系统，要在 SuSe Linux Enterprise Server 中永久设置主机名：Edit /etc/HOSTNAME

#vi /etc/HOSTNAME

或

echo newhostname > /etc/HOSTNAME

这将永久更改主机名。

重新启动服务器并在 SAP 安装之前进行验证。

RAM 角色配置

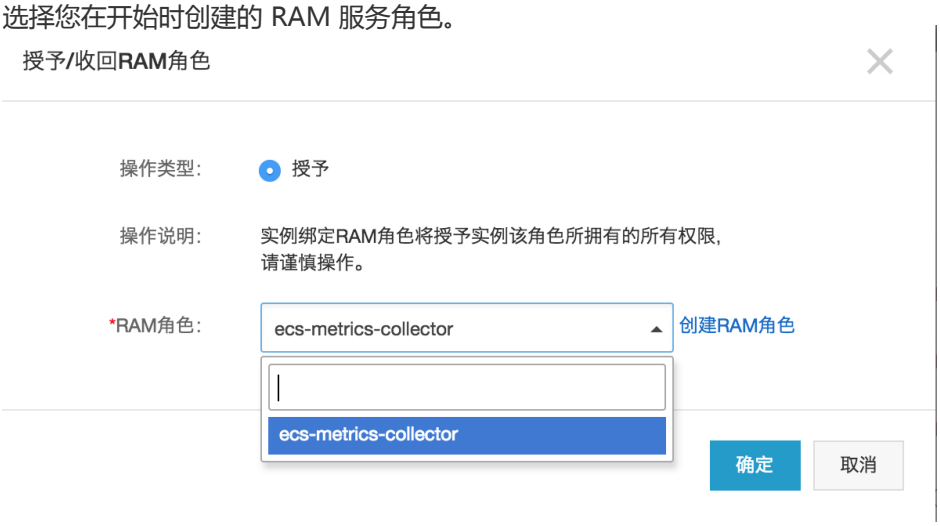
将您创建的 RAM 服务角色挂载至您的 SAP ECS 实例。

打开 ECS 控制台，转到**实例**选项卡，找到您的 ECS 实例

在**更多**操作的下拉列表中选择**绑定/解绑 RAM 角色**



选择您在开始时创建的 RAM 服务角色。



点击“确定”以挂载角色。

关于绑定/解绑 RAM 角色的更多信息，请参考如何通过控制台使用实例 RAM 角色。

准备 SAP 安装介质

通常，您会从 SAP 获得安装介质（作为安装包的一部分）。然而，您也可以通过 SAP Software Distribution Center 下载安装介质，网址为 http://support.sap.com/swdc。要将 SAP 安装介质复制到阿里云的 ECS 实例，主要有两种选择：

直接从 SAP Service Marketplace 下载到阿里云的 ECS 实例

从您的阿里云 ECS 实例中，连接到 SAP Service Marketplace 并下载所需的安装介质。此选项很可能是在阿里云获取 SAP 安装介质的最快方法，因为阿里云实例与外网的连接速度非常快。您可以创建

专用的阿里云 OSS 存储卷以存储安装介质，然后根据需要将存储卷挂载到不同的实例。您还可以创建阿里云存储卷的快照，并创建多个存储卷，并且并行挂载到多个实例。

从您的网络复制到阿里云的 ECS 实例

如果您已经将所需的 SAP 安装介质下载到您网络中的某个位置，则可以将该介质从您的网络直接复制到阿里云的 ECS 实例中。

ECS Metrics Collector 安装和验证

ECS Metrics Collector 是一款监控代理程序，使得 SAP 监控工具能够从 SAP ECS 实例和底层主机环境收集所需的系统信息。对于运行 SAP 应用程序的每个 ECS 实例，都需要安装该监控代理程序。

安装 ECS Metrics Collector

第 1 步：使用具有 root 权限的用户帐户登录您的 SAP ECS 实例。

为使用 root 权限，您需要使用 sudo，因此您的用户必须属于 sudo 组。

第 2 步：根据以下步骤，通过云助手安装 ECS Metrics Collector：

metrics collector工具需要python支持，如果你的ECS还没有安装pip，需要先安装

```
wget https://bootstrap.pypa.io/get-pip.py
python get-pip.py
pip -V #查看pip版本
```

```
aliyun_installer -i ecs-metrics-collector
```

在选择package_id的时候，填写最新版的id，示例中当前最新版是8

```
hana01:/usr/local/share/aliyun-assist # aliyun_installer -i ecs-metrics-collector
package_id      name    version arch    publisher
5       ecs-metrics-collector   0.2     x64     aliyun-inc
6       ecs-metrics-collector   0.3     x64     aliyun-inc
8       ecs-metrics-collector   0.4     x64     aliyun-inc
Please input the package_id you want to install.
8
The package_id you input is 8.
The package you want to install is ecs-metrics-collector.
Downloading...
Check MD5
Unzip
Installing...
see details in installation log file: /var/log/ecs_metrics_collector/install.log

[DEBUG] prepare_env
[DEBUG] account_check
[DEBUG] distro_check
[DEBUG] init_system_check
[DEBUG] system_restraint_check
[DEBUG] package_check
[DEBUG] python_env_check
[DEBUG] install_collector
[DEBUG] install_watchmen
[DEBUG] install_service

Installation success !
```

验证 ECS Metrics Collector 的安装

第 3 步：通过以下操作验证 ECS Metrics Collector 服务是否正常：

```
systemctl status ecs_metrics_collector
```

```
hana01:/usr/local/share/aliyun-assist # systemctl status ecs_metrics_collector
● ecs_metrics_collector.service - ECS Metrics Collector for SAP
   Loaded: loaded (/etc/systemd/system/ecs_metrics_collector.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2018-05-24 19:56:39 CST; 4min 45s ago
  Process: 5412 ExecStartPost=/usr/local/sbin/ecs_metrics_collector_watchmen --set (code=exited, status=0/SUCCESS)
  Process: 5405 ExecStart=/usr/local/sbin/ecs_metrics_collector -d (code=exited, status=0/SUCCESS)
 Main PID: 5410 (python)
    Tasks: 2 (limit: 512)
   CGroup: /system.slice/ecs_metrics_collector.service
           └─5410 python /usr/local/sbin/ecs_metrics_collector -d

May 24 19:56:39 hana01 systemd[1]: Starting ECS Metrics Collector for SAP...
May 24 19:56:39 hana01 systemd[1]: ecs_metrics_collector.service: Supervising process 5410 which is not our child. We'll most lik...t exits.
May 24 19:56:39 hana01 systemd[1]: Started ECS Metrics Collector for SAP.
Hint: Some lines were ellipsized, use -l to show in full.
```

第 4 步：使用以下命令，验证在 crontab 中是否已配置保护任务和自动更新任务以及运行日志

```
cat /etc/cron.d/ecs_metrics_collector
cat /var/log/ecs_metrics_collector/watchmen.log
```

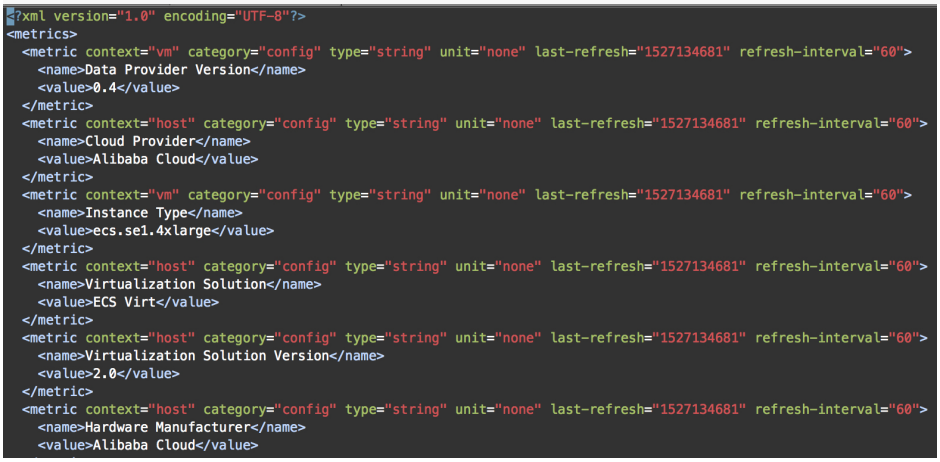
```
hana01:/usr/local/share/aliyun-assist # cat /etc/cron.d/ecs_metrics_collector
*/1 * * * * root /usr/local/sbin/ecs_metrics_collector_watchmen --watching >& /dev/null
*/5 * * * * root /usr/local/sbin/ecs_metrics_collector_watchmen --update >& /dev/null
hana01:/usr/local/share/aliyun-assist # cat /var/log/ecs_metrics_collector/watchmen.log
[Thu May 24 19:56:39 CST 2018] [watchmen] [INFO] register watchmen
[Thu May 24 19:57:01 CST 2018] [watchmen] [INFO] detect collector running, pid 5410
[Thu May 24 19:58:01 CST 2018] [watchmen] [INFO] detect collector running, pid 5410
[Thu May 24 19:59:01 CST 2018] [watchmen] [INFO] detect collector running, pid 5410
[Thu May 24 20:00:01 CST 2018] [watchmen] [INFO] check_update
[Thu May 24 20:00:02 CST 2018] [watchmen] [INFO] detect collector running, pid 5410
[Thu May 24 20:01:01 CST 2018] [watchmen] [INFO] detect collector running, pid 5410
[Thu May 24 20:02:01 CST 2018] [watchmen] [INFO] detect collector running, pid 5410
[Thu May 24 20:03:01 CST 2018] [watchmen] [INFO] detect collector running, pid 5410
[Thu May 24 20:04:01 CST 2018] [watchmen] [INFO] detect collector running, pid 5410
[Thu May 24 20:05:01 CST 2018] [watchmen] [INFO] detect collector running, pid 5410
[Thu May 24 20:05:02 CST 2018] [watchmen] [INFO] check_update
[Thu May 24 20:06:01 CST 2018] [watchmen] [INFO] detect collector running, pid 5410
hana01:/usr/local/share/aliyun-assist #
```

在 ECS Metrics Collector 安装过程中，这两个任务将自动添加至 crontab。自动更新任务每 5 分钟自动在云助手服务器上检查一次 ECS Metrics Collector 的最新版本，一旦有新版本可用将自动升级。

检查收集的监控项数据

第 5 步：验证收集的数据：

```
curl localhost:8888 | vim -
```



```
<?xml version="1.0" encoding="UTF-8"?>
<metrics>
  <metric context="vm" category="config" type="string" unit="none" last-refresh="1527134681" refresh-interval="60">
    <name>Data Provider Version</name>
    <value>0.4</value>
  </metric>
  <metric context="host" category="config" type="string" unit="none" last-refresh="1527134681" refresh-interval="60">
    <name>Cloud Provider</name>
    <value>Alibaba Cloud</value>
  </metric>
  <metric context="vm" category="config" type="string" unit="none" last-refresh="1527134681" refresh-interval="60">
    <name>Instance Type</name>
    <value>ecs.se1.4xlarge</value>
  </metric>
  <metric context="host" category="config" type="string" unit="none" last-refresh="1527134681" refresh-interval="60">
    <name>Virtualization Solution</name>
    <value>ECS Virt</value>
  </metric>
  <metric context="host" category="config" type="string" unit="none" last-refresh="1527134681" refresh-interval="60">
    <name>Virtualization Solution Version</name>
    <value>2.0</value>
  </metric>
  <metric context="host" category="config" type="string" unit="none" last-refresh="1527134681" refresh-interval="60">
    <name>Hardware Manufacturer</name>
    <value>Alibaba Cloud</value>
```

更多操作命令

有关metrics collector更多的命令，可以通过aliyun_installer --h查询

检查操作系统

启动 ECS 后，请参阅相关的 SAP 安装说明，并确保您的系统包含指定的软件组件：

- 1310037 - SUSE LINUX Enterprise Server 11: Installation notes
- 1984787 - SUSE LINUX Enterprise Server 12: Installation notes

创建操作系统镜像

在启动 SAP ECS 实例并获得 SAP 安装介质时，您应当执行以下操作通过快照创建自定义镜像：

登录 ECS 控制台。

在左侧导航栏中，单击**快照** > **快照**。

选择所需地域。

选择一个磁盘属性为**系统盘**的快照，然后单击**创建自定义镜像**。

注意：数据盘不能用于创建自定义镜像。



您可以在显示的对话框中查看快照 ID。为自定义镜像输入名称和描述。

（可选）单击**添加数据盘快照**，为镜像选择数据盘的多个快照。

注：如果快照磁盘容量为空，系统将会创建一个默认容量为 5 GB 的空磁盘。如果您选择了可用的快照，系统会创建与这些快照的大小相同的磁盘。



单击**创建**。自定义镜像已成功创建。

（可选）要查看已经创建的镜像，可在左侧导航栏中选择**镜像**。

安装 SAP 解决方案

一旦您在阿里云供应并配置了所需的 ECS 实例，就可以开始安装 SAP 解决方案了。在此之前，请参阅以下 SAP 官方指南。

System Provisioning Guide

查看 [Installation Guides - Application Server Systems] 部分，找到 [Installing SAP Systems Based on SAPNetWeaver 7.1 and Higher - Using Software Provisioning Manager 1.0]，确定适合您的数据库、SAP 产品版本、操作系统和技术资源栈。

关于所有受支持技术（ABAP、Java，或 ABAP 和 Java）组合、数据库和操作系统的具体安装指南，请访问：http://support.sap.com/sltoolset

启动 SWPM

Software Provisioning Manager (SWPM) 选择具有最大可用空间的磁盘驱动器作为每个组件的安装建议。在 SWPM 对话框中，请务必将这些磁盘分配给正确角色。

您可以根据 SAP Note 1680045下载最新版本的 SWPM。

注：在运行 SWPM 以执行安装时，如果要使用浏览器连接到 SWPM，则需要使用 root 用户。所以即使客户选择通过证书连接，也必须设置 root 密码。

安装完成后，如果需要保护系统，客户可以在 SSH 配置中禁用密码登录。

更新 SAP kernel

SAP NetWeaver 安装完成后，请确保根据《安装指南》的说明应用最新 kernel，或者将 SAP kernel 更新到最低支持补丁。

除此之外，还请确保它包含最低 SAP kernel 补丁级别，如以下说明所述：SAP Note 2533233 - Linux on Alibaba Cloud (IaaS): Adaption of your SAP License。

检查 Host Agent 版本

SAP Host Agent 是一款代理工具，可以完成多项生命周期管理任务，如操作系统监控、数据库监控、系统实例控制和供应。通常 SAP Host Agent 会在操作系统启动时自动启动。您也可以使用 saphostexec 程序进行手动控制。

您在阿里云的 Linux ECS 实例中运行 SAP，并希望在云环境下配置 SAP 所需的增强监控。此外您需要参考 SAP Note 2564176

请按照以下步骤检查 SAP Host Agent 版本：

以 root 身份登录，因为 [sidadm] 不具备执行 SAP HOST AGENT 命令的权限

cd /usr/sap/hostctrl/exe 导航至 SAP Host Agent 的安装目录

执行命令 ./saphostexec –version

用于增强监控的 SAP Host Agent 最低版本是 Release 7.21 补丁级别 32。为了在 SAP 增强监控中包含阿里云性能数据，SAP 增强了 SAP Host Agent 及其监控事务 ST06。

关于所需的 SAP NetWeaver 支持包级别，请查看 SAP Note 1102124。

升级 Host Agent

请确保所运行的 SAP Host Agent 版本不低于阿里云环境所需的最低版本。我们建议在 SAP 实例之外独立升级 SAP Host Agent，可以手动完成，也可以配置自动升级。

要默认定期更新 SAP Host Agent，请参见 SAP Note 1473974 - Using the SAP Host Agent Auto Upgrade Feature。

安装横向扩展系统

在三层扩展 SAP 系统中，您应当将多个 ECS 实例部署为不同的 SAP 实例。

ASCS：ABAP Central Services Instance，您可以将 ASCS 安装在包含入队服务器和消息服务器的独立 ECS 实例上。SAP 系统中只能有一个这样的实例，并且可以将其变为高可用性实例。

SCS：SAP Central Services，在 Java 系统中，Central Services 称为 SCS。

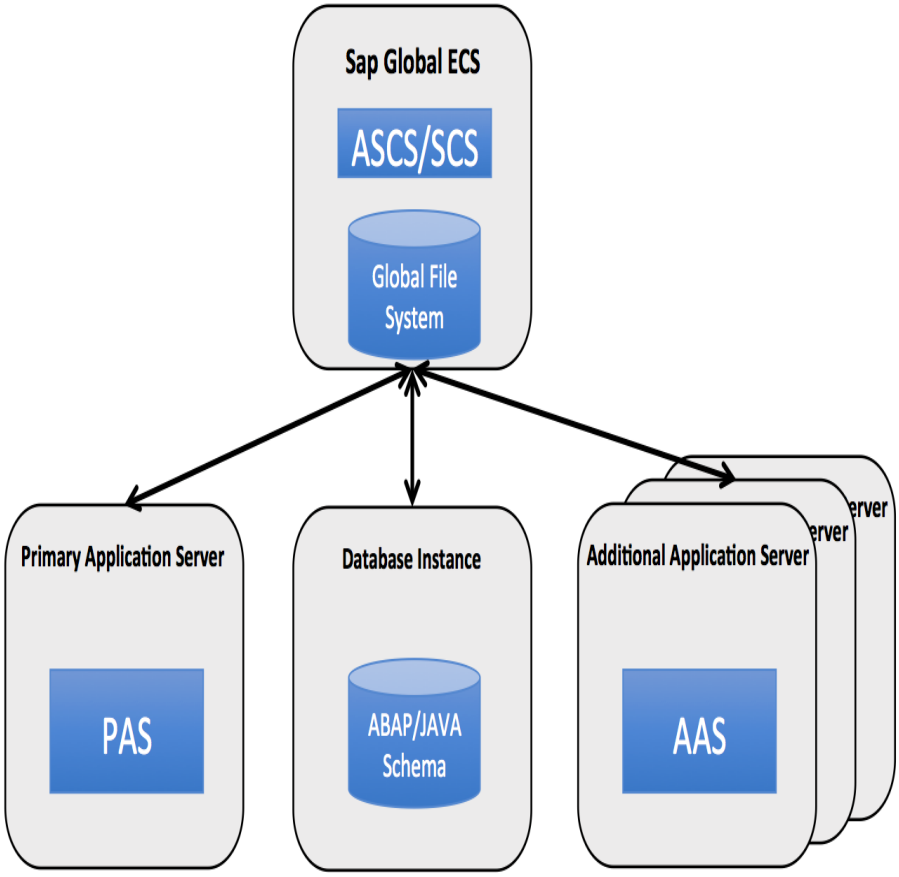
PAS：Primary Application Server Instance，这是运行 SAP NetWeaver 应用服务器 (AS) 的主 ECS 实例，此 ECS 实例还托管了包含共享配置文件的共享文件系统，运行相同 SAP SID 各部分的每个 ECS 实例都必须可以访问该实例。如果它还用于传输共享，则必须使用相同的传输目录以便与所有 SAP SID 共享。

您也可以在此主 ECS 实例上安装 ASCS 或 SCS。

AAS：Additional Application Server Instances，这是运行 AS 的一些额外虚拟机，用于扩展目的。

DB 实例：专用于中央数据库的 ECS 实例。

全部内容都需要运行在同一个可用区。



主要步骤如下：

- DB 实例：创建托管数据库的 ECS 实例，然后安装数据库实例。
- PAS：
  - 在要运行 SAP NetWeaver 的 ECS 实例上运行 SWPM。
  - 安装 Central Services、ASCS 或 SCS。
  - 安装 AS ABAP 或 AS JAVA。
  - 连接到现有的数据库实例。
- AAS：
  - 在要运行 SAP NetWeaver 的每个附加 ECS 实例上运行 SWPM。
  - 安装 AAS。
  - 连接到现有的数据库实例。
  - 指向包含有配置文件并且由主实例管理的网络共享。

安装单节点系统

在 Linux 上以 2 层架构配置来部署 SAP NetWeaver 的步骤，与设置 3 层架构配置的步骤非常相似。对于 2 层架构配置：

- SAP NetWeaver 和数据库实例都安装在单个 ECS 实例中。

- 在安装 SAP NetWeaver 之前，先安装数据库实例。
- 对于基于 SAP HANA 的系统，SAP NetWeaver ABAP 系统的系统 ID 必须与 SAP HANA 系统的系统 ID 不同。参见 SAP Note 1953429 - SAP HANA and SAP NetWeaver AS ABAP on One Server。该说明附有安装指南。

安装后

创建 SAP 实例镜像

完成 SAP 安装步骤后，建议您创建一个 ECS 实例的镜像，以保存您所做的所有安装工作。请参考以下步骤创建自定义的 SAP 实例镜像。

1.登录 ECS 控制台。2.在左侧导航窗格中，单击**实例**。3.选择地域。4.选择您的 SAP ECS 实例，然后选择**更多** > **创建自定义镜像**。5.输入名称和描述。6.单击**创建**。



SAP 系统迁移

有三种方式可以将 SAP 系统迁移至阿里云的 ECS 实例。您可以使用 P2V 工具，执行 SAP 同构或异构系统复制，或者使用第三方工具。

VM 导入/导出工具

对于小型 SAP 系统的迁移，我们推荐使用 P2V 或 V2V 工具，这使您可以轻松地将现有环境中的机器镜像导入阿里云的 ECS 实例。您现有环境的系统状态和数据将会映射到一个虚拟磁盘文件中，并上传至阿里云平台。请自定义镜像，以确保 ECS 实例中运行的应用及数据与原有物理服务器一致。

更多信息请参阅阿里云网站的 P2V 迁移工具。

由于在迁移期间您的 SAP 系统的硬件密钥将发生变化，因此您应当在阿里云的目标系统中实施新的 SAP 许可

证。

您还需要手动安装 Metrics Collector。有关更多信息，请参阅本指南中有关 ECS Metrics Collector 安装的部分。

SAP 同构和异构系统复制

将 SAP 系统迁移到阿里云 ECS 实例的推荐方法是标准的 SAP 同构和异构系统复制程序。

将现有 SAP 系统迁移至阿里云的三个主要步骤如下所述：

导出

在源系统中，在导出源系统之前停止所有 SAP 应用程序实例。使用 SWPM 创建源系统的导出转储文件。

传输

将导出转储文件或数据库备份数据复制到阿里云。

网络拷贝

对于具有导出转储文件和数据库备份数据的 SAP 系统，您可以通过网络将数据直接复制至阿里云的目标 ECS 实例。传输时间取决于数据量、网络连接的速度和带宽。您可以并行加载数据以减少传输时间。

导入

进入阿里云，在 ECS 实例中安装新的 SAP 系统。在安装 DB 实例过程中，使用 SWPM 导入从源系统导出的文件。

然后，安装 SAP 应用程序实例，并执行 SAP 系统拷贝的安装后步骤。

最后，在阿里云启动 SAP 系统并提供 SAP 服务。

第三方工具

如使用未获认证的第三方工具或迁移方法，请联系供应商以获取支持。SAP 支持的系统拷贝方法在系统拷贝指南和“SAP 说明”中进行了阐述。

系统迁移后，您应当实施新的 SAP 许可证，并手动安装 Metrics Collector。

SAP NetWeaver 操作指南

- ECS 实例生命周期管理
    - ECS 实例可用性
    - 停止 ECS 实例
- 备份和恢复
    - OSS 备份
    - 磁盘快照
    - SAP NetWeaver 系统克隆
    - 自定义系统镜像
    - 在不同地域和可用区之间移动 SAP NetWeaver 系统
    - 非生产环境的备份和恢复
    - 生产环境的备份和恢复
- 数据库操作
    - HANA
- 访问控制
    - ECS 实例 RAM 角色
- 访问安全
    - SSH 密钥
- ECS Metrics Collector for SAP

ECS 实例生命周期管理

这一部分提供了如何管理 ECS 实例运行状态的信息。

ECS 实例可用性

ECS 实例自动恢复是阿里云的一项功能。它旨在增加实例可用性。如果由于底层硬件问题或故障导致 ECS 实例受损或终止，则具有相同的实例 ID、专有 IP 地址、弹性公网 IP 地址和所有实例元数据的相同实例将在不同的硬件上恢复。恢复过程中用户将收到一封电子邮件。更多信息请参考 ECS 实例宕机迁移 FAQ。

启动和停止 ECS 实例

您可以随时停止一个或多个 SAP NetWeaver 主机。停止 ECS 实例意味着关闭该实例，您可以通过 ECS 控制台执行此操作。启动或停止实例。确保您应当先停止 SAP NetWeaver，然后再停止实例。

注意：实例停止后，分配给该 ECS 实例的专有 IP 地址不会被释放，因此当您再次启动该实例时，它将以与之前相同的专有 IP 地址、网络和存储配置进行启动。

备份和恢复

这一部分介绍了阿里云的功能，可以帮助您处理需要保存系统状态的应用场景。

OSS 备份

阿里云对象存储 (OSS)是一种易于使用的服务，让您能够在云上存储、备份和归档大量数据。OSS 作为加密的中央存储库，允许人们从世界各地安全地访问文件。

OSS 存储空间可用于存储磁盘快照、自定义镜像和系统副本。

磁盘快照

您可以为挂载到 ECS 实例的云盘随时创建快照，以生成磁盘状态的时间点副本。快照对于以下用例很有用：

1.更改您的云盘类型例如，您希望将当前的云端硬盘类型从高效云盘更改为 SSD 云盘；2.将 SAP NetWeaver 系统从一个地域（或可用区）移至另一个地域（或可用区）您可以通过以下方式来实现： 1.创建自定义镜像，包括挂载到 ECS 实例的磁盘的所有快照； 2.使用自定义镜像在另一个地域或可用区创建新的 ECS 实例，这种方式下，移动 NetWeaver 之后您需要更新 SAP 许可证。

1. 高效率、低成本地备份非生产系统；对于托管了非生产系统的 ECS 实例，您可以为挂载到该实例的所有云盘创建快照。

要获得具有一致性的快照，您必须阻止 SAP NetWeaver 或数据库向文件系统写入数据。

要创建快照，您可以参照阿里云网站的官方指南创建快照进行操作。

SAP NetWeaver 系统克隆

要在阿里云克隆您的 SAP NetWeaver 系统，请遵循标准的 SAP 导出-导入过程：

1.使用 Software Provisioning Manager (SWPM) 导出源系统。2.将从系统和数据库导出的数据复制到您的阿里云 OSS 存储空间；3.将导出的数据从 OSS 存储空间复制到您的目标 ECS 实例；4.使用 SWPM 创建新的目标系统，并将从源系统导出的数据导入其中。

自定义系统镜像

要捕获挂载到您 ECS 实例的系统盘的状态，您可以创建一个自定义镜像。镜像与备份不同。镜像可用于创建新的 ECS 实例，而备份不能。除非您使用系统盘的备份来创建自定义镜像，然后使用此自定义镜像创建 ECS 实例。

在部署步骤结束时，您应当已经创建了一个或多个镜像。但是，在对系统做出重要更改（如安装 SAP NetWeaver 二进制文件更新或升级 SAP NetWeaver 版本）之后，您可能需要创建新的镜像。

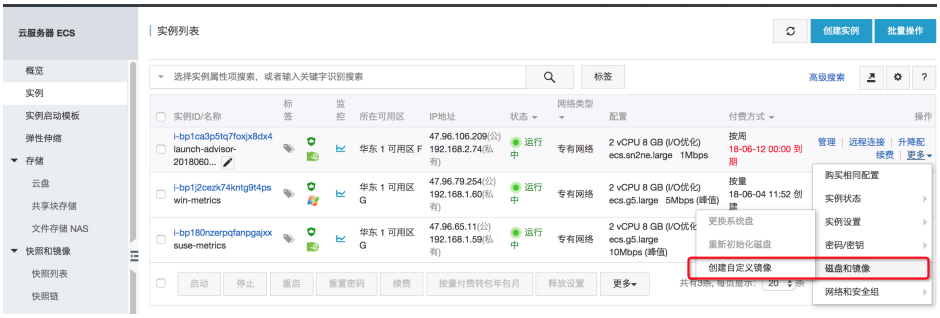
请参阅以下文件了解关于镜像的更多信息

- 使用快照创建自定义镜像
- 使用实例创建自定义镜像

在不同地域和可用区之间移动 SAP NetWeaver 系统

在某些情况下，您可能需要将 SAP NetWeaver 系统从一个地域（或可用区）移动到另一个地域（或可用区）。您可以为源地域（或可用区）中托管 SAP NetWeaver 系统的整个 ECS 实例创建自定义镜像（包括快照），然后通过自定义镜像创建新的 ECS 实例，从而实现此目的。

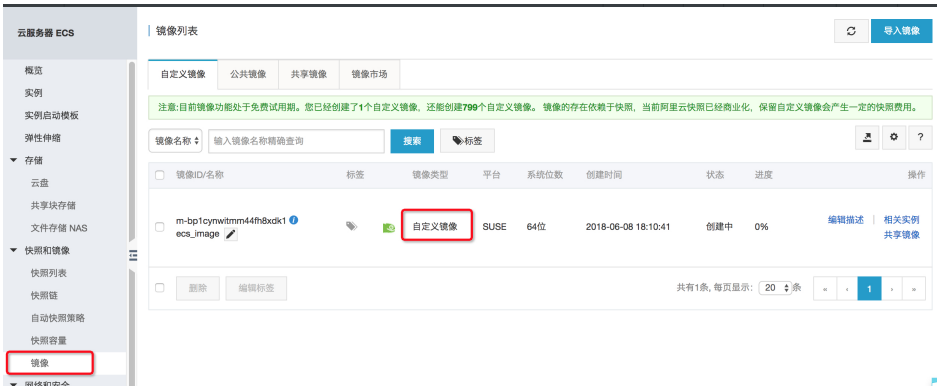
您可以从ECS 控制台创建自定义镜像，如下所示：



填写所有信息，并记下高亮部分（系统也将创建一个磁盘快照），如下所示：



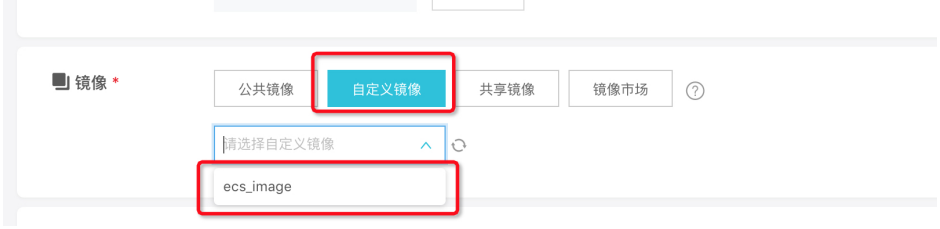
创建自定义镜像后，您可以在 ECS 控制台找到以下内容：1.自定义镜像：



2.所有相关磁盘的快照：



创建自定义镜像后，可以根据以下步骤，通过自定义镜像启动一个新的 ECS 实例，从而轻松地从一个 ECS 实例创建另一个实例 SAP NetWeaver 系统的拷贝：



请查阅阿里云 SAP NetWeaver 实施指南中的“创建和配置实例”一节，了解更多详细步骤

如果名字尚未使用，则可以在新的地域（或可用区）中保留相同的主机名。但请注意，将 ECS 实例从一个可用区移动到另一个可用区后，ECS 实例 ID 将发生变化。这意味着 SAP 硬件密钥已更改，您必须相应地导入新的 SAP 许可证。

非生产环境的备份和恢复

云盘快照提供了简单、低成本的备份服务，可以利用该服务满足非生产系统的备份要求。它具有非常灵活的快照策略，例如，用户可以在一天中的整点时刻和某几个时间点进行快照，可以选择任意星期几作为每周快照的快照日，也可以指定快照保留期限或者选择永久保留。请注意，当达到最大自动快照数时，最早的自动快照将被删除。有关云盘快照的更多信息，请查看阿里云网站。

可以使用快照手动还原非生产系统的整个 HANA ECS 实例。

生产环境的备份和恢复

对于生产系统，您应当使用数据库备份和恢复功能。

数据库操作

这一部分提供了在阿里云中管理 SAP HANA 的一般信息。

HANA

有关在阿里云运行 SAP HANA 的完整信息，请参阅阿里云 SAP HANA 操作指南。该指南涵盖了有关管理、备份和恢复、安全性、联网和其他主题的详细信息。

访问控制

控制对阿里云计算资源的访问，是保护和操作 SAP 系统部署的一个关键部分。尽管 SAP 提供了自己的用户管理系统，但是阿里云访问控制 (Resource Access Management, RAM) 服务将提供对阿里云计算资源的统一访问控制。

有时，您可能需要在 SAP 项目的不同阶段添加或删除团队成员或更改其访问权限级别。您可以通过定义哪些人对资源拥有哪些访问权限，来管理访问控制。例如，您可以控制哪些人可以在 SAP 实例上执行阿里云控制台操作，例如创建和修改 ECS 实例、VPC 设置等。

有关 RAM 的更多细节，请参阅此处。

ECS 实例 RAM 角色

ECS 实例 RAM (Resource Access Management) 角色（以下简称“实例 RAM 角色”）让 ECS 实例获得某些授权的角色，从而赋予 ECS 实例权限。

通过将一个 RAM 角色关联到 ECS 实例，您可以在 ECS 实例内部基于 STS (Security Token Service，安全令牌服务）临时凭证访问其他云服务。这样，一方面可以保证 Access Key 安全，另一方面也可以借助 RAM 实现权限的精细化控制和管理。欲了解更多详情，请查阅此处。

访问安全

SSH 密钥

阿里云提供 SSH 密钥对登录，该登录方式仅适用于 Linux 实例。如果您运行在 Linux 之上，建议您选择此鉴

权方式来保护 ECS 实例的安全。

SSH 密钥对是由加密算法生成的一对密钥：一个对外界公开，称为公钥，另一个您自己保留，称为私钥。

如果您将公钥放在 Linux 实例中，则可以使用私钥通过 SSH 命令或相关工具从本地计算机或其他实例登录此实例，而无需输入密码。有关 SSH 密钥的更多详情，请查阅此处。

用于SAP监控和支持的 ECS Metrics Collector

云环境中的 SAP 应用程序运行在虚拟环境下安装的客户操作系统 (Guest OS) 上。SAP Host Agent 可收集 SAP 监控所需的全部信息，并将其提供给 SAP NetWeaver 本地监控和 Solution Manager，以用于分析和显示。客户或 SAP 技术支持人员可以通过 SAP 事务代码 ST06 访问 SAP 工具。

除此之外，阿里云与 SAP 共同合作，为运行在阿里云上的 SAP NetWeaver 构建了一款监控代理程序 - ECS Metrics Collector。ECS Metrics Collector 负责从底层的阿里云基础设施和虚拟化平台收集有关配置和资源（CPU\内存\磁盘\网络）利用率的信息，并将其提供给 SAP Host Agent。

注意：您必须在您的 SAP ECS 实例上部署 ECS Metrics Collector，以便从 SAP 获得支持并使 SAP 能够满足其服务级别协议 (SLA)。

ECS Metrics Collector for SAP

关于ECS Metrics Collector的部署，请参考 ECS Metrics Collector for SAP部署指南

SAP迁移工具

- 概述
- 阿里云 P2V 迁移工具
    - 线上 P2V 迁移
    - 线下 P2V 迁移
    - V2V 迁移
    - P2V 迁移的其他方式

概述

P2V 即 Physical to Virtual，简称 P2V。它是指将物理服务器上的操作系统及其上的应用软件和数据迁移到阿里云平台管理的 ECS 云服务器中。

V2V 即 Virtual to Virtual，简称 V2V。它是指从其他云平台或传统虚拟化平台的虚拟主机迁移到阿里云的 ECS 云服务器，比如 VMware 迁移到阿里云，云主机（如 AWS EC2、Azure Virtual Machines 等）迁移到阿里云。

以上这两类迁移方式，主要是使用迁移工具软件，把物理服务器或虚拟主机上的系统状态和数据镜像到一个虚拟磁盘文件中，并上传至阿里云平台中，确保运行的 ECS 云服务器和原有物理服务器或者虚拟主机运行的应用及数据一致。

阿里云 P2V 迁移工具

本文中介绍的阿里云 P2V 工具对于这两类迁移方式都适用。

线上 P2V 迁移

目标场景

在线迁移工具主要是帮助用户将可访问公网的线下服务器或者其他云虚拟机的工作负载迁移到阿里云，主要适用于下述场景：

- 从 AWS / Azure / GCP / 腾讯 / 华为 等云平台上的虚拟机迁移至阿里云；
- 从可访问公网的线下服务器（物理机、虚拟机）迁移至阿里云。

适用范围

适用于市面上主流的 Windows 和 Linux 32位/64位操作系统。主要列表如下：

- Windows Server 2003/2008/2012/2016
- CentOS 5/6/7
- Ubuntu 12/14/16
- Debian 7/8/9
- Red Hat 6/7

其他不在此列的操作系统暂不保证能迁移成功，详细信息请参阅帮助文档。

迁移工具及帮助文档

迁移工具及帮助文档下载地址： http://p2v-tools.oss-cn-hangzhou.aliyuncs.com/在线P2V迁移工具.zip

线下 P2V 迁移

目标场景

线下迁移工具主要是帮助用户把线下局域网内的工作负载迁移到阿里云，主要适用于下述场景：

- 从线下局域网内的虚拟机迁移至阿里云；
- 从线下局域网内的物理机服务器迁移至阿里云。

适用范围

适用于市面上主流的 Windows 和 Linux 32位/64位操作系统。主要列表如下：

- Windows Server 2008/2012
- CentOS 5/6/7
- Ubuntu 12.04/14.04/16.04
- Debian 7/8/9
- SUSE Linux Enterprise Server 11/12
- OpenSUSE

其他不在此列的操作系统暂不保证能迁移成功，详细信息请参阅帮助文档。

- 同时，需要有一个本地 Windows 客户端来安装线下迁移工具（需要有一定的磁盘空间）。

迁移工具及帮助文档

迁移工具及帮助文档下载地址： http://p2v-tools.oss-cn-hangzhou.aliyuncs.com/P2V_Release_2017_08_23.zip

V2V 迁移

VMware 虚机迁移

方法一

- 使用格式转换工具把 vmdk 转换成 vhd。（请参阅 https://help.aliyun.com/document_detail/57187.html）
- 导入阿里云生成自定义镜像。（请参阅 https://help.aliyun.com/document_detail/25464.html）

注意：对于部分操作系统类型，可能会存在驱动的问题。

方法二

- 使用在线/离线 P2V 工具完成 V2V 迁移。

Azure 虚机迁移

方法一

- 导出 Azure vhd 文件。（请参阅 https://docs.microsoft.com/zh-cn/azure/virtual-machines/windows/download-vhd ）
- 导入阿里云生成自定义镜像。（请参阅 https://help.aliyun.com/document_detail/25464.html ）

注意：对于部分操作系统类型，可能会存在驱动的问题。

方法二

- 使用在线/离线 P2V 工具完成 V2V 迁移。

AWS 虚机迁移

- 使用在线/离线 P2V 工具完成 V2V 迁移。

P2V 迁移的其他方式

通过 VMware 迁移工具进行迁移

- 使用 VMware 的迁移工具把源机器迁移至 VMware ESXi。（请参阅 https://www.vmware.com/cn/products/converter.html ）
- 使用格式转换工具把 vmdk 转换成 vhd。（请参阅 https://help.aliyun.com/document_detail/57187.html ）

导入阿里云生成自定义镜像。（请参阅 https://help.aliyun.com/document_detail/25464.html ）

注意：对于部分操作系统类型，可能会存在驱动的问题。

SAP MaxDB

SAP MaxDB部署指南

版本管理

版本	修订日期	变更类型	生效日期
1.0			2018/7/18

概述

SAP® MaxDB™ 是由 SAP SE 开发和支持的数据库管理系统。SAP MaxDB 可在 Microsoft Windows、Linux 和 UNIX 上使用，并可用于大多数卓越的硬件平台以及公共云。有关 SAP MaxDB 的更多详细信息，请参阅 SAP 官方网站:http://maxdb.sap.com

本部署指南介绍如何在阿里云 ECS 上规划和部署 SAP MaxDB 数据库系统，包括如何配置 ECS 实例、块存储、网络和 SUSE Linux Enterprise Server (SLES) 操作系统。本指南包括阿里云和 SAP 的最佳实践。

ECS 实例规格

本部署指南介绍针对 SAP MaxDB 认证的 ECS 通用型实例族 (sn2ne)，它运行在 Intel Broadwell 架构上并属于 ECS 企业实例规格族之一。SSD 云盘和超级云盘可用于在 SAP MaxDB 数据库中托管数据卷和日志。下表列出了目前支持的 ECS 实例规格，有关更多信息，请参阅 SAP Note 2552731 - SAP Applications on Alibaba Cloud: Supported Products and IaaS VM Types

实例类型	vCPU	Memory (GiB)
ecs.sn2ne.large	2	8
ecs.sn2ne.xlarge	4	16
ecs.sn2ne.2xlarge	8	32
ecs.sn2ne.4xlarge	16	64
ecs.sn2ne.8xlarge	32	128
ecs.sn2ne.14xlarge	64	256
ecs.r5.large	2	16.0
ecs.r5.xlarge	4	32.0
ecs.r5.2xlarge	8	64.0
ecs.r5.3xlarge	12	96.0
ecs.r5.4xlarge	16	128.0
ecs.r5.6xlarge	24	192.0
ecs.r5.8xlarge	32	256.0

有关 ECS 内存实例规格族 se1 的详细信息，请转到 https://www.alibabacloud.com/help/doc-

detail/25378.htm#se1

阿里云服务

下表列出了本部署指南使用的阿里云核心组件中包括的服务。

服务	说明
云服务器ECS	ECS 是一类计算服务，它具有弹性处理功能。ECS 具有比物理服务器更简单、更高效的管理模式。您可以随时创建实例、更改操作系统以及添加或释放任意数量的 ECS 实例以满足您的业务需求。
SSD 云盘	它适用于 I/O 密集型应用，可提供稳定的高随机 IOPS 性能。
超级云盘	它适用于中等 I/O 负载应用场景，可为 ECS 实例提供高达 3,000 随机读写 IOPS 的存储性能。
专有网络 VPC	阿里云 VPC 是在阿里云上构建的专有网络。它在逻辑上与阿里云中的其他虚拟网络隔离。VPC 使您能够在自己定义的网络中启动并使用阿里云资源。
对象存储 OSS	阿里云 OSS 是基于网络的数据访问服务。OSS 使您能够存储和检索结构化和非结构化数据，包括文本文件、图像、音频和视频。

在阿里云上部署 SAP MaxDB

本节介绍如何在阿里云上部署 SAP MaxDB。

准备工作

阿里云帐户

如果您目前还没有阿里云帐户，可以按照以下过程申请一个：

- 完成注册过程。转到阿里云主页，然后单击页面右上角的“免费注册”。
- 按照注册指南，完成注册。

可用区和地域

1.可用区

- 可用区是一个地域中具有独立电网和网络的物理区域。同一可用区内的 ECS 实例的网络时延更短。
- 同一地域内的可用区与可用区之间内网互通，可用区之间能做到故障隔离。是否将 ECS 实例部署在同一可用区中取决于容灾能力和网络时延的要求。
- 如果您的应用需要较高的容灾能力，建议您将 ECS 实例部署在同一地域的不同可用区内。
- 如果您的应用在实例之间需要较低的网络时延，则建议您将 ECS 实例创建在同一可用区内。

2.地域

阿里云数据中心目前部署在以下地域：华东 1（杭州）、华东 2（上海）、华北 1（青岛）、华北 2（北京）、华北 3（张家口）、华南 1（深圳）、香港、美国西部 1（硅谷）、美国东部 1（弗吉尼亚）、新加坡、亚太 NE 1（日本）、德国 1（法兰克福）和中东地区 1（迪拜）。

- 华东 1（杭州）、华东 2（上海）、华北 1（青岛）、华北 2（北京）、华北 3（张家口）和华南 1（深圳）的数据中心提供了多线 BGP 骨干网络，覆盖中国的所有省份和城市，并在中国大陆提供稳定快速的接入。
- 香港的数据中心提供了国际带宽接入，覆盖香港和东南亚。
- 作为新加坡数据中心的合作伙伴，SingTel 是东南亚的主流运营商。该公司在业务专业知识和成熟度方面高度可靠，可很好地为该地域内的用户服务。
- 亚太 SE 2 的数据中心位于澳大利亚悉尼。
- 亚太 NE 1 的数据中心位于日本东京。
- 美国西部 1（硅谷）的数据中心通过 BGP 线路直接连接到多个美国运营商的骨干网络。除了整个美国地域外，该数据中心将其范围扩展到南美洲和欧洲大陆。
- 美国东部 1 的数据中心位于美国的弗吉尼亚。
- 德国 1 的数据中心位于法兰克福。
- 中东地区 1 的数据中心位于阿拉伯联合酋长国迪拜。

3.如何选择地域

中国大陆的地域

一般情况下，建议您选择离您的最终用户最近的数据中心以进一步加快用户访问速度。阿里云在中国大陆的各数据中心在基础设施、BGP 网络质量、服务质量以及 ECS 操作和配置方面类似。国内 BGP 网络可确保快速访问中国各地域。

国际地域

中国大陆之外的数据中心可提供国际带宽并面向中国大陆之外的区域。从中国大陆访问这些地域可能会引发高时延。因此，建议您不要使用它们。

- 如果您在香港或东南亚有业务需求，可以选择香港或新加坡。
- 如果您在日本或韩国有业务需求，可以选择亚太 NE 1（日本）。
- 如果您在澳大利亚有业务需求，可以选择亚太 SE 2（悉尼）。
- 如果您在美国有业务需求，可以选择美国西部 1（硅谷）和美国东部 1（弗吉尼亚）。
- 如果您在欧洲大陆有业务需求，可以选择德国 1（法兰克福）。

如果您在中东地区有业务需求，可以选择中东地区 1（迪拜）。

不同地域中的不同阿里云产品无法通过内网相互通信

- 不同地域中的 ECS 和 OSS 实例无法通过内网相互通信。
- 不同地域中的 ECS 实例和其他云资源（如 OSS 实例）无法通过内网相互通信。
- 无法为不同地域中的 ECS 实例部署负载均衡，也就是说，在不同地域购买的 ECS 实例无法部署在同一负载均衡实例中。
- 单个 VPC 只能部署在一个地域中。默认情况下，不同区域中的 VPC 无法相互通信。可以根据实际的运行环境选择 VPC。

SAP MaxDB 安装介质

1. 从 SAP 官方网站下载 SAP MaxDB 安装介质；
2. 将 SAP MaxDB 安装介质上传到 ECS 实例；

部署过程

配置网络

1. 创建 VPC 和交换机

- 登录 VPC 控制台。
- 在左侧导航栏中，单击“VPC”。
- 在 VPC 列表页面上，选择 VPC 所在的地域，然后单击“创建VPC”。
- 在“创建 VPC”对话框中，输入 VPC 名称，然后为 VPC 选择网段。您可以选择 VPC 的以下标准网段之一：在创建了 VPC 之后，无法修改其网段。建议您使用大网段以防止后续扩容：

```
10.0.0.0/8（10.0.0.0 - 10.255.255.255）
172.16.0.0/12（172.16.0.0 - 172.31.255.255）
192.168.0.0/16（192.168.0.0 - 192.168.255.255）
```

- 单击“创建 VPC”。在创建了 VPC 之后，会生成 VPC ID。同时会为 VPC 创建路由器。
- 单击“下一步”来创建交换机。
- 在“创建交换机”选项卡页面上，提供以下信息，然后单击“创建交换机”。

名称：指定交换机名称。
可用区：选择交换机的可用区。
网段：指定交换机的网段。交换机的网段可以与交换机所属的 VPC 的网段或 VPC 网段的子网相同。交换机的网段大小必须介于 16 位网络掩码和 29 位网络掩码之间。注意：如果交换机的网段与交换机所属的 VPC 的网段相同，则只能在 VPC 下创建一个交换机。

- 单击“完成”。返回到实例列表页面，然后单击已创建的 VPC 的 ID 链接来进入 VPC 详情页。检查页面上的 VPC 和交换机。

配置安全组

关于安全组

安全组是一个逻辑上的分组，这个分组是由同一个地域内具有相同安全保护需求并相互信任的实例组成。每个实例至少属于一个安全组，创建实例时必须指定安全组。同一个安全组中的实例可以通过网络通信，但默认情况下，不同安全组中的实例无法通过内网通信。可以授权两个安全组之间的相互访问。安全组是可提供有状态数据包检查 (SPI) 功能的虚拟防火墙。安全组用于为一个或多个 ECS 设置网络访问控制。作为一种重要的安全隔离方法，安全组用于划分云上的安全域。

- **安全组限制**
  - 单个安全组内的实例个数不能超过 1,000。如果您有超过 1,000 个实例需要内网互访，可以将它们分配到不同安全组，并通过互相授权的方式允许互访。

- 每个实例最多可以加入 5 个安全组。
- 每个用户最多可以有 100 个安全组。
- 对安全组的调整操作不会影响对用户的服务连续性。
- 安全组是有状态的。如果允许出站数据包，则也会允许对应于此连接的入站数据包。
- 安全组具有两种网络类型：经典网络和 VPC。
- 经典网络类型的实例可以加入同一地域中的经典网络上的安全组。
- VPC 类型的实例可以加入同一 VPC 上的安全组。

- **安全组规则**
- 安全组规则可设置为允许或禁止与安全组关联的 ECS 实例从入站和出站方向访问公网或内网。
- 您可以随时授权或删除安全组规则。您已更改的安全组规则将自动应用于与安全组关联的 ECS 实例。在设置安全组规则时，确保安全组规则很简单。如果您将多个安全组分配给一个实例，则可能对该实例应用数百条规则。在您访问实例时，网络可能会断开连接。
- **安全组规则限制** 每个安全组最多可以具有 100 条安全组规则。

安全组配置方法

- 登录 ECS 控制台。
- 在左侧导航栏中，单击“安全组”。
- 选择要对其创建安全组的地域。
- 单击“创建安全组”。
  在显示的对话框中，输入以下信息：



- 单击“确定”，然后单击“配置规则”。
- 按照相应说明完成规则设置。建议您仅保留远程访问端口。



端口配置参考

在 SAP MaxDB 部署过程中，使用 VPC。您只需设置出站和入站方向的规则，而无需指定公网或 VPC。默认情况下，安全组规则是空白的。在创建 ECS 实例时，请确保所选安全组包含端口 22 (Linux) 或 3389 (Windows)。否则，您无法远程登录 ECS 实例。有关 SAP 需要访问的特定端口及相关安全组规则的详细信息，请参阅 SAP 官方文档。

创建 SAP MaxDB ECS 实例

1. 登录阿里云 ECS 产品购买页面。
2. 选择“包年包月”作为付款方式。
3. 选择地域和可用区。
4. 选择“VPC”作为网络类型。
   在选择了网络类型之后，填充有关已创建或现有的 VPC 和交换机的信息。在多节点架构中，SAP MaxDB 没有直接提供外部服务。因此，将“公网 IP 地址”设置为“未分配”。
5. 选择实例规格。选择 sn2ne ECS 实例族中的实例规格。
6. 选择操作系统镜像。操作系统可以是 SUSE Linux Enterprise Server。



7. 配置存储磁盘。建议对日志和数据文件系统使用单独的 SSD 云盘，对备份文件系统使用单独的超级云盘。
8. 配置初始化信息。在设置初始密码后，单击“创建”，然后等待几分钟来完成实例初始化。
9. 创建堡垒机。按照上述步骤创建具有一个 vCPU 和 2 GB 内存且在同一可用区的同一 VPC 中没有其他存储的堡垒机。
10. 配置堡垒机的网络。目前可以使用多种方法来配置公网 IP 地址。使用弹性 IP 地址 (EIP) 配置作为示例。EIP 是可以独立购买和持有的公网 IP 地址资源。它可以动态绑定到不同的 ECS 实例或与其解除绑定，而无需停止 ECS 实例。

- 登录 EIP 控制台。
- 单击“申请 EIP”。
- 在购买页面上，为 EIP 选择地域、带宽峰值和付款方式，单击“立即购买”，然后进行付款。
- 注意：EIP 的地域必须与 EIP 所绑定到的 ECS 实例的地域相同。
- 返回到 EIP 列表页面，选择 EIP 的地域，然后单击“刷新”来检查已创建的 EIP 实例。
- 单击“绑定”。
- 在“绑定公网 EIP”对话框中，选择已创建的 ECS 实例，然后单击“确定”。
- 在绑定完成后，单击 EIP 列表页面上的“刷新”来检查 EIP 实例状态。
- 当 EIP 实例状态为“刷新”时，可通过公网访问 EIP 所绑定到的 ECS 实例。
- 登录 ECS 实例并运行以下命令来测试通过公网的访问。ping www.aliyun.com

登录实例 目前没有为 SAP MaxDB ECS 实例配置任何公网。因此，登录 SAP MaxDB ECS 实例需要堡垒机。

连接到 SAP MaxDB

由于在上述部署中不会为 SAP MaxDB 实例配置公网 IP 地址，您只能使用 SSH 通过堡垒机连接到 SAP MaxDB 实例；

- 要通过堡垒机连接到 SAP MaxDB，请将您选择的 SSH 客户端连接到堡垒机，然后再连接到 SAP MaxDB 实例。

参考

1173395 - FAQ: SAP MaxDB and liveCache configuration

1142243 - SAP MaxDB release for virtual systems

1492000 - General Support Statement for Virtual Environments

SAP MaxDB 操作指南

版本管理

版本	修订日期	变更类型	生效日期
1.0			2018/7/19

简介

本指南提供运行已部署在阿里云上的 SAP MaxDB 系统的最佳实践。请注意，本指南并不能取代任何标准 SAP 文档。

管理

本节介绍如何执行在阿里云上运行 SAP MaxDB 系统通常需要的管理任务，包括有关启动、停止和克隆系统。

启动和停止 ECS 实例

您可以随时停止任何 SAP MaxDB 主机。作为最佳实践，您应该首先停止运行在阿里云 ECS 实例上的 SAP MaxDB，然后再停止该实例。在恢复实例时，ECS 实例将自动使用与以前相同的 IP 地址、网络和存储配置启动。

创建 SAP MaxDB 系统的自定义镜像

阿里云上的自定义镜像允许您创建多个具有相同 OS 和环境数据的 ECS 实例以满足扩展需求，从而可帮助您有效运行 ECS 实例。您可以使用阿里云管理控制台基于现有实例创建自己的自定义镜像。有关更多信息，请参阅阿里文档中的“使用快照创建自定义镜像”部分。您可以按以下方式使用镜像：

- 创建（OS、/usr/sap、数据、日志、备份文件的）完整离线 MaxDB 系统备份。
- 可以使用镜像创建 ECS 实例或更改 ECS 实例的系统盘；
- 将 SAP MaxDB 系统从一个地域移动到另一个地域 – 按照阿里云文档中的说明创建现有阿里云 ECS 实例的镜像并将其移动到另一个地域。您还可以将自定义镜像复制到另一个地域，以保持环境和应用的跨多个地域一致性部署。
- 克隆 SAP MaxDB 系统 – 您可以创建现有 SAP MaxDB 系统的镜像以创建系统的精确克隆。请参阅本文档的下一节。注意：要创建具有一致状态的 SAP Max 系统的镜像，您需要先停止 SAP MaxDB 实例，然后再创建。

克隆 SAP MaxDB 系统

创建 SAP MaxDB 系统的克隆，您可以在同一可用区中的阿里云 ECS 中创建 SAP MaxDB 系统的镜像。它一般包括操作系统和预装的 SAP MaxDB 软件，以及相同的存储系统布局。

帐户管理

在阿里云上的 SAP MaxDB 系统的管理过程中，有 3 种类型的管理员帐户，如下所示：

- 阿里云帐户 - 在使用阿里云产品和服务之前，您必须先在阿里云网站上创建阿里帐户。使用此帐户，您可以从阿里云网站管理 ECS、配置 VPC 以及管理 SAP MaxDB 系统的镜像或快照。
- ECS 实例管理员帐户 - 在创建 ECS 实例时，将在 OS 级别创建管理员帐户（通常为根）。阿里云不会在操作系统中创建任何帐户；默认的 Linux 系统用户仅为根用户。在使用系统时，用户可以根据操作系统的需要创建或删除用户帐户。
- SAP MaxDB 数据库系统管理员 - 在安装 SAP MaxDB 的过程中需要指定 SID，SAP MaxDB 将使用 [sid]adm 作为系统帐户并默认创建此帐户。

联网

您通过 ECS 虚拟网络使用 ECS 预置 SAP MaxDB 系统。我们强烈建议使用 VPC 作为 SAP MaxDB 的默认网络类型。阿里云 VPC 是在阿里云中建立的私网。它在逻辑上与阿里云中的其他虚拟网络隔离。VPC 使您能够在自己的 VPC 中启动并使用阿里云资源。您可以全面控制阿里云 VPC，例如，您可以选择其 IP 地址范围，将 VPC 进一步分段为子网，以及配置路由表和网关。请参阅阿里文档中的 VPC 用户指南。另外，您可以使用物理连接或 VPN 将 VPC 与本地网络相连接以形成可按需自定义的网络环境。这样，您可以毫不费力地将应用顺利迁移到阿里云。

安全隔离

- 默认情况下，不同用户的云服务器位于不同的 VPC 中。
- 不同的 VPC 之间通过隧道 ID 进行隔离。使用虚拟交换机和虚拟路由器，您可以将 VPC 分段为子网，就像在传统网络环境中那样。同一子网中的不同云服务器使用虚拟交换机相互通信，而 VPC 中不同子网中的云服务器使用虚拟路由器相互通信。
- 不同 VPC 之间的内网完全隔离，只能通过 IP 的外部映射（弹性 IP 和 NAT IP）互联。
- 因为使用隧道 ID 封装云服务器的 IP 数据包，所以云服务器的数据链路层（两层 MAC 地址）不会传输到物理网络。因此，不同云服务器的两层网络互相隔离。换句话说，不同 VPC 之间的两层网络互相隔离。
- VPC 内的 ECS 实例使用安全组防火墙来控制网络访问。这是第三层隔离。

NAT 网关

如果您的安全策略需要真正内部的 VM，则需要在网络上手动设置 NAT 代理和相应的路由，以便 VM 可以访问外网。请务必注意，您无法使用 SSH 直接连接到完全内部的 VM 实例。要连接到此类内部虚拟机，您必须设置具有外部 IP 地址的堡垒实例，然后通过它建立隧道。有关用户如何设置堡垒实例的信息，请参阅阿里云指南上的“SAP MaxDB 部署指南”。
当 VM 没有外部 IP 地址时，它们只能由网络上的其他 VM 访问或通过托管 VPN 网关进行访问。您可以在网络中预置 VM 来充当入站连接的可信中继（称为堡垒机）或网络出口（称为 NAT 网关）。要获得没有设置此类

连接的更加透明的连接，可以使用托管 VPN 网关资源。

安全组

安全组是一个逻辑上的分组，这个分组是由同一个地域内具有相同安全保护需求并相互信任的实例组成。每个实例至少属于一个安全组，创建实例时必须指定安全组。同一个安全组中的实例可以通过网络通信，但默认情况下，不同安全组中的实例无法通过内网通信。不过，可以授权两个安全组之间的相互访问。

安全组是可提供有状态数据包检查 (SPI) 的虚拟防火墙。安全组用于为一个或多个 ECS 设置网络访问控制。作为一种重要的安全隔离方法，安全组用于划分云上的安全域。请参阅阿里文档中的“安全组用户指南”。

使用 SAProuter 允许 SAP 支持访问

SAProuter 是在客户的网络和 SAP 之间提供远程连接的软件应用。在一些情况下，可能需要允许 SAP 支持工程师访问阿里云上的 SAP MaxDB 系统。使用 SAProuter 的唯一前提条件是从客户的网络到 SAP 网络的网络连接。在设置从阿里云上的 ECS 到 SAP 的直接支持连接时，请按照以下步骤操作：

- 启动 SAProuter 软件将安装在其上的 ECS 实例，购买弹性 IP (EIP) 资源并动态绑定到 VPC ECS 实例，而无需重启 ECS 实例。
- 创建并配置特定安全组，它只允许 SAProuter 实例和 TCP 端口 3299 对 SAP 支持网络进行所需的入站和出站访问。
- 按照 SAP Note 1628296 中的说明安装 SAProuter 软件，并创建允许从 SAP 访问阿里云上的 SAP MaxDB 系统的 saprouttab 文件。
- 设置与 SAP 的连接。对于外网连接，请使用安全网络通信 (SNC)。有关更多信息，请参阅 SAP 远程支持 – 帮助。

安全

对于 IaaS 部署和 SAP MaxDB 系统实施，阿里云负责维护支持云的基础设施的安全，而客户负责确保其使用的云资源和应用的安全。
下面是可帮助您实现阿里云上的 SAP MaxDB 环境所需的安全级别的其他阿里云安全资源。

访问控制 RAM

阿里云 RAM 是一项身份和访问控制服务，使您能够集中管理用户（包括员工、系统或应用）并安全控制其通过权限级别对您的资源的访问。因此，RAM 使您能够将阿里云资源的访问权限安全地只授予所选的具有高特权的用户、企业成员和合作伙伴。这有助于确保您的云资源的安全且适当的使用，并防止对您的帐户进行任何未经请求的访问。请参阅阿里文档中的“访问控制 RAM 用户指南”。

访问通知

阿里云消息中心允许用户订阅通知和配置通知通道，包括电子邮件和短信。如果用户的服务器上有 SSH 登录，则会通知用户。

安骑士

阿里云安骑士是可提供服务器和数据库的实时监控的可靠且安全的服务。全天候监控已暴露的漏洞可确保服务和应用的最佳可用性。请参阅阿里文档中的“安骑士用户指南”。有一些登录安全措施，如下所示：

- 实时监控整个网络中的常规 Web 软件漏洞。
- 允许用户访问云盾的紧急漏洞响应功能，包括漏洞补丁（在正式补丁发布之前提供）。
- 在漏洞暴露和发布正式补丁之间的那段时间里，让用户一键修复漏洞并拦截黑客攻击。

备份与恢复

备份对于保护记录系统来说非常重要。您应该创建在 SAP MaxDB 工作负载较低时运行的定期备份，并且您可以从意外系统故障恢复。下面是有关阿里云上的备份与恢复的一些要点。

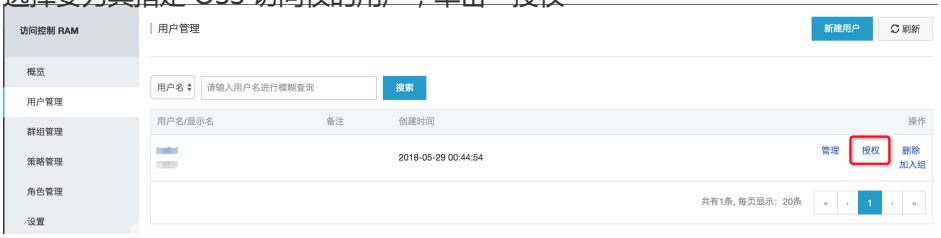
阿里云上的 SAP MaxDB 备份的最终目标

备份阿里云上的 SAP MaxDB 与备份传统本地基础设施的主要区别是最终备份目标。用于本地基础设施的典型最终备份目标是磁带。在阿里云上，备份存储在 OSS 中。与磁带相比，将备份存储在阿里云 OSS 中有许多好处，例如您可以在 OSS 存储桶中读取、写入、删除和存储无限对象；OSS 在多个位置存储您的对象的三个副本以确保 99.999999999% 的数据可靠性；内置的安全机制，包括多层安全防护、监控未授权登录尝试、DDoS 攻击防护和数据访问策略等。
默认情况下，在阿里云上，将 SAP MaxDB ECS 实例配置为使用云盘作为 SAP MaxDB 数据库的初始本地备份目标。SAP MaxDB 备份首先存储在这些本地云盘卷上，然后复制到 OSS 以进行长期存储。

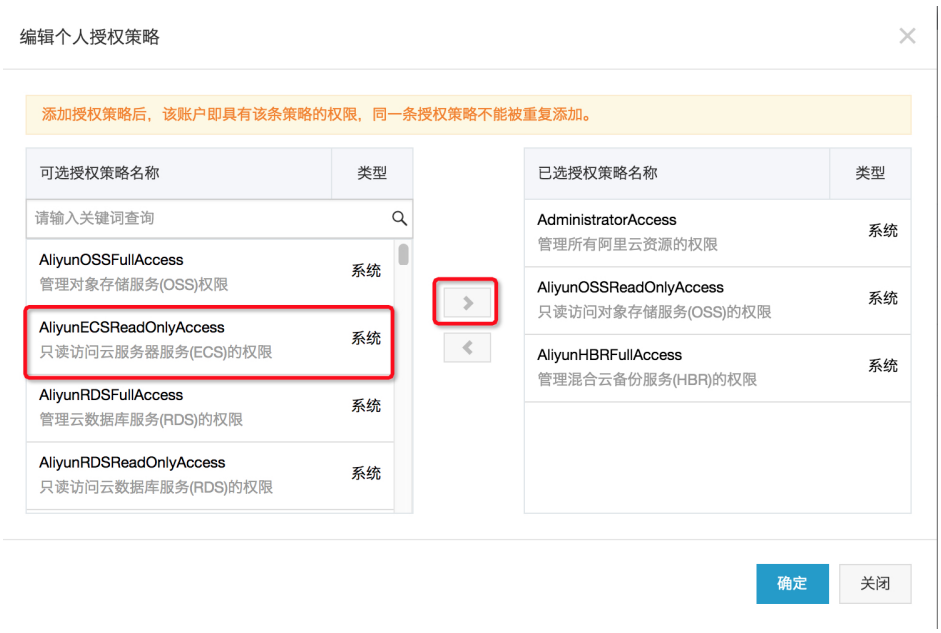
管理身份和对备份的访问

要允许访问 OSS 存储桶中的备份，您需要在 RAM 控制台中为用户配置访问规则。请参考以下步骤：

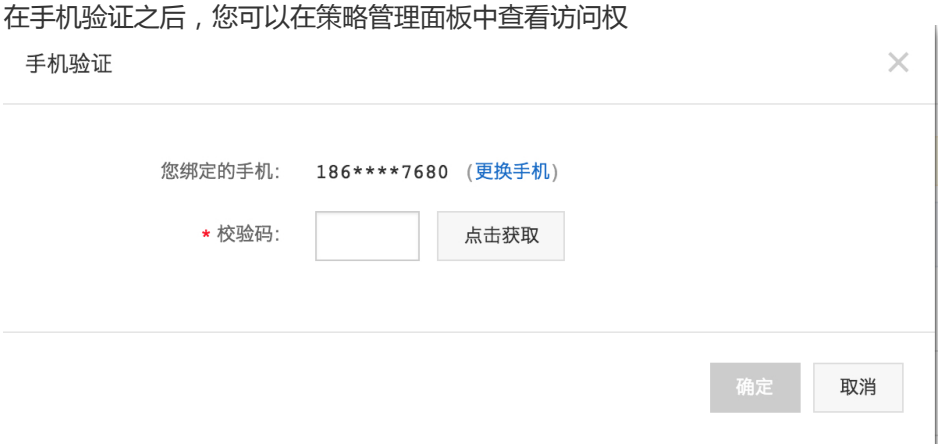
1. 选择要为其指定 OSS 访问权的用户，单击“授权”



2. 选择授权策略“AliyunOSSFullAccess”



3. 作为帐户所有者，您将需要通过手机验证输入验证码
4. 在手机验证之后，您可以在策略管理面板中查看访问权



5. 如果您要创建自定义策略，也可以从策略管理面板创建它。有关更多详细信息，请参考阿里云网站上的 RAM 策略管理文档



非生产 SAP MaxDB 数据库上的备份和恢复

本节提供了适用于非生产系统的备份选项。非生产系统的示例包括：

- 演示系统
- 培训系统
- 沙箱系统
- 概念验证系统

- 跟踪系统非生产系统的典型要求：
- 不经常备份
- 不请求时间点恢复
- 低成本

云盘快照提供了简单的低成本备份服务，可用于满足非生产系统的要求。它具有非常灵活的快照策略，例如，用户可以在整点时刻拍摄快照以及每天拍摄多次快照，用户可以选择星期几作为每周拍摄快照的重复日子，用户可以指定快照保留期或选择永久保留快照。请注意，当达到自动快照的最大数后，会删除最旧的自动快照。有关云盘快照的更多信息，请阅读阿里云网站上的文档（https://help.aliyun.com/document_detail/25391.html)。同时，在使用云盘快照执行备份之前，请查看 SAP Note 1928060 - Data backup and recovery with file system backup。在做磁盘快照之前，必须满足一些特定前提条件。

备份方法

可以配置附加到 SAP MaxDB ECS 实例的云盘卷（包括系统盘 (/usr/sap)、数据文件系统和日志文件系统的数据盘）的自动快照以定期创建快照。

还原方法

快照可用于手动还原非生产系统的整个 SAP MaxDB ECS 实例。

生产 SAP MaxDB 数据库上的备份和恢复

本节中介绍的备份选项可满足生产系统共有的以下备份要求：

- 经常按计划备份
- 时间点数据库恢复

备份方法

- 默认情况下，在阿里云平台上，在附加到 SAP MaxDB ECS 实例的云盘卷上配置 SAP MaxDB 数据库的初始本地备份目标；
- 用户可以使用 SQL 命令或 SAP DBA Cockpit 启动或计划 SAP MaxDB 数据备份。除非禁用，否则会自动写入日志备份；
- 然后，用户可以将本地云盘上的 SAP MaxDB 数据库备份文件复制到阿里云 OSS 以进行长期存储；
- 如果需要跨地域冗余，则可以将 OSS 上的备份文件配置为复制到不同地域。

还原方法

- 将 OSS 中的备份文件复制到 SAP MaxDB ECS 实例的备份目录的云盘；
- 基于备份云盘的备份文件还原并恢复 SAP MaxDB 数据库。

SAP 安全解决方案

SAP 安全解决方案

- SAP 系统安全现状
- 阿里云安全责任共担
- 阿里云安全架构
- SAP 系统网络安全规划
    - 网络隔离与规划
    - 安全策略
    - VPC 间互连
- SAP 系统安全架构
- 阿里云安全产品
    - 账户安全
    - 主机安全
    - 应用安全
    - 网络安全
    - 数据安全
    - 安全运营
    - 业务安全

本文档着重介绍对于部署在阿里云的 SAP 应用安全解决方案，通过阿里云丰富的云安全产品保障客户 SAP 系统平稳运行，降低 SAP 系统的安全风险，使客户更专注于其核心业务。

SAP 系统安全现状

根据 Onapsis 的调查报告，全世界超过25万企业因 SAP 系统中存在的一系列安全漏洞而受到影响，可能导致严重的企业数据泄露。SAP 是世界上最受欢迎的企业应用软件企业和解决方案提供商，为85%以上的全球500强企业和190个国家的282,000+家客户提供解决方案。

漏洞原因
最近在对 SAP 解决方案提供商进行的一项研究显示，超过95%的企业 SAP 存在严重的安全问题，这些问题将它们置于网络攻击风险之中并可能导致严重的数据泄露。影响包括98%的100个最有价值的品牌在内，全世界超过250000个 SAP 业务客户都因 SAP 系统中的一系列漏洞而暴露在网络攻击之下。

Onapsis 首席执行官 Mariano Nunez 说：
“最令人惊讶的是，因为 SAP 操作团队和 IT 安全团队之间的责任差距，大多数公司的 SAP 网络安全都面临着威胁。事实上，应用的大多数补丁都与安全无关、发布过迟或者引入了进一步的操作风险。”

该研究还报告说，在2014年 SAP 发布了391个安全补丁，而它们中的50%以上都被评定为高风险漏洞。

攻击方式及影响范围

针对 SAP 应用程序的主要网络攻击(也就是系统弱点)分为以下几类：

- 核心网络：执行远程功能的模块。
- 数据仓库：为了获取或修改 SAP 数据库中的信息，利用 SAP RFC网关中的漏洞执行管理员权限指令。
- 门户网站攻击：利用漏洞创建J2EE后门账户，以访问 SAP 门户和其他内部系统。

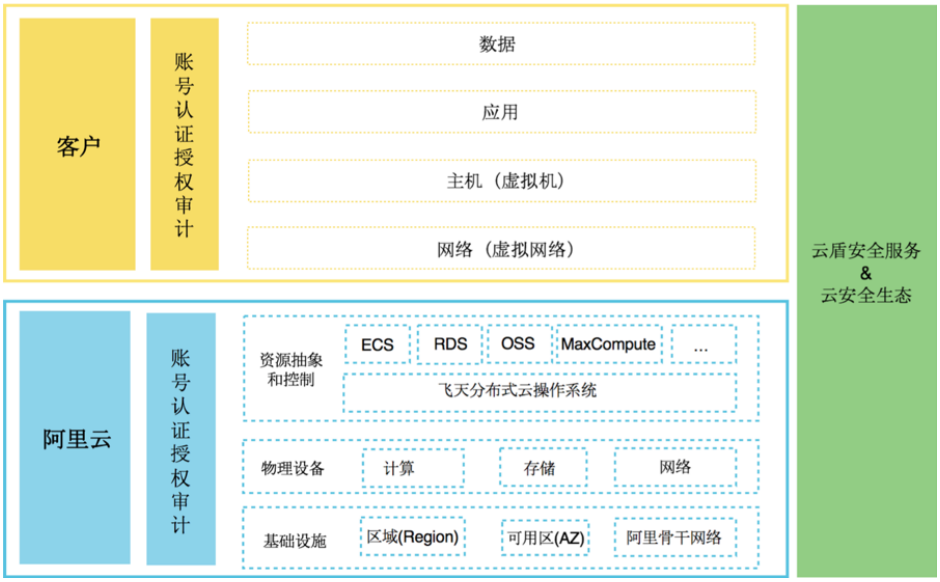
报告中提供了针对SAP系统最常见的三种网络攻击的细节信息，这些攻击向量使得黑客可以入侵SAP系统并能够访问公司数据的应用程序。经过专家研究确认，网络攻击将会严重影响以下关键业务进程：

- 在 SAP 系统之间使用 Pivoting，造成客户信息和信用卡信息泄漏。
- 客户和供应商门户攻击。
- 通过SAP私有协议对数据仓库发起攻击。

根据 Nunez 所说，SAP HANA 应该对新增加的450%的安全补丁负责：
“这一趋势不仅仅是持续的，而是随着 SAP HANA 更加恶化，因为 SAP HANA 导致新的安全补丁增加了450%。因为 SAP HANA 位于 SAP 生态系统的中心，所以存储在 SAP 平台的数据现在必须同时在云端和前端进行保护。”

阿里云安全责任共担

基于阿里云的 SAP 客户应用，其安全责任由双方共同承担：阿里云确保云服务平台的安全性，客户负责基于阿里云服务构建的应用系统的安全。



阿里云负责基础设施(包括跨地域、多可用区部署的数据中心，以及阿里巴巴骨干传输网络)、物理设备(包括计算、存储和网络设备)、天分布式云操作系统及之上的各种云服务产品的安全控制、管理和运营，从而为客户提供高可用和高安全的云服务平台。

阿里云基于阿里巴巴集团多年攻防技术积累，为客户提供云盾安全服务，保护客户的应用系统。客户负责以安全的方式配置和使用云服务器(ECS)、数据库(RDS)实例及其他云产品，基于这些云产品以安全可控的方式构建自己的应用；客户可选择使用云盾安全服务或者阿里云安全生态里的第三方安全厂商的安全产品为其应用系统提供安全防护。

安全责任共担模式之下，阿里云提供并保障基础设施的安全，能够让用户降低 IaaS 层的安全性的顾虑，安心使用阿里云 IaaS 服务，更专注于核心业务发展。

阿里云安全架构

阿里云提供了共 11 个不同层面的安全架构保障，其中包括物理安全，硬件安全，虚拟化安全，云产品安全等 4 个云平台层面的安全架构保障；以及账户安全，主机安全，应用安全，网络安全，数据安全，安全运营，业务安全等 7 个云用户层面的安全架构保障。



本文在介绍 SAP 整体安全架构时，会简要介绍各个架构层面中的关键特性，同时会覆盖多种阿里云产品，包括云盾安全产品。

SAP 系统网络安全规划

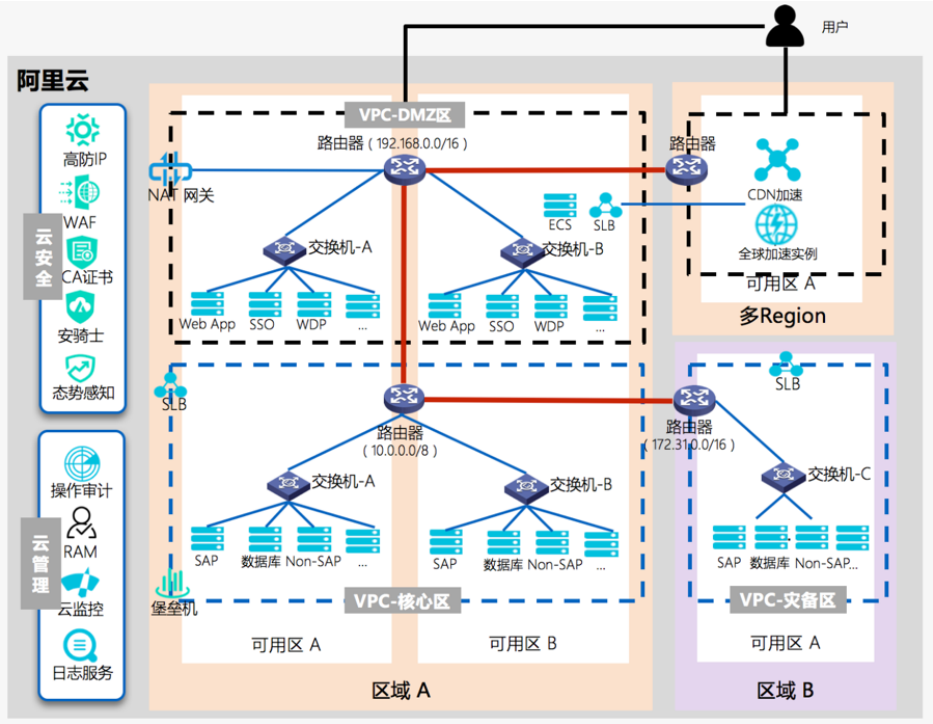
网络隔离与规划

阿里云 SAP 的解决方案中，专有网络 VPC（Virtual Private Cloud）是阿里云推荐使用的网络类型，做为企业独有的的云上专有网络，专有网络之间逻辑上彻底隔离。如果在一个地域的多个 SAP 业务系统需要通过 VPC 进行严格隔离，比如生产环境和测试环境，那么也需要使用多个 VPC。VPC 是企业用户上云第一个考虑的产品，主要是因为：

隔离的网络环境
VPC 基于隧道技术，实现数据链路层的隔离，为每个租户提供一张独立、隔离的安全网络。不同专有

网络之间内部网络完全隔离，只能通过对外映射的 IP（弹性公网 IP 和 NAT IP）互连。

可控的网络配置
您可以完全掌控自己的虚拟网络，例如选择自己的 IP 地址范围、配置路由表和网关等，从而实现安全而轻松地资源访问和应用程序访问。此外，您也可以通过专线或 VPN 等连接方式将您的专有网络与传统数据中心相连，形成一个按需定制的网络环境，实现应用的平滑迁移上云和对数据中心的扩展。



DMZ 区：介于内网（可信任区）和外网（不可信区）之间的一个中间公共访问区域（专有网络），该区域一般可以被外网用户所访问，承载公网用户以及 SAP 支持人员对业务系统的访问，在向外界提供在线服务的同时，阻止外部用户直接访问内网，以确保内部网络环境的安全。

运维管理区：DMZ 区的内部分区，部署阿里云的运维跳板机，是系统云运维人员管理其它区域云主机及系统的中转区域。

核心应用区：部署企业核心应用，如 SAP 和 非 SAP 应用，供企业内部用户接入和访问，安全级别最高，高于 DMZ 区。可按照企业 SAP 应用的安全规划，划分开发区、测试区、预生产区和生产区等。

灾备区：部署企业灾备环境，如同城灾备和异地灾备，保障系统的数据安全。通常通过网络复制技术，来实现数据库和应用级别的数据复制。

网络加速区：部署 CND 加速、全球加速实例等，提升企业应用的访问速度，满足企业的全球访问需求。

安全策略

云产品	安全域	接入规则	接出规则
SLB	DMZ	允许互联网用户访问	接出到ECS_Web 协议/端口

			：tcp/80,443,2800-3300,5000-10000,13000-14000,21234,22223,22225
堡垒机	DMZ-G1	允许VPN拨入 协议/端口: SSH/22，远程桌面（RDP）/3389	接出到ECS_Web，协议/端口：Web管理/443，SSH和SFTP/60022，RDP/63389
ECS_Web	DMZ-G2	允许SLB访问 协议/端口 ：http/https/tcp/1~65535 允许堡垒机访问 协议/端口 ：TCP/22~3389	接出到核心区ECS_APP 协议/端口 ：tcp/1~65535
ECS_APP	应用核心区-G3	允许ECS-Web访问 协议/端口：TCP/具体的应用端口	接出到灾备区 ECS_DR 协议/端口 ：tcp/1~65535
ECS_DR	灾备区	允许ECS-APP访问 协议/端口：TCP/具体的应用端口	协议/端口 ：tcp/1~65535
CND, 全球加速实例	网络加速区	允许互联网用户访问	接出到ECS_Web 协议/端口 ：tcp/80,443,2800-3300,5000-10000,13000-14000,21234,22223,22225
OSS	-	-	-

通过以上安全策略，运维路径是：

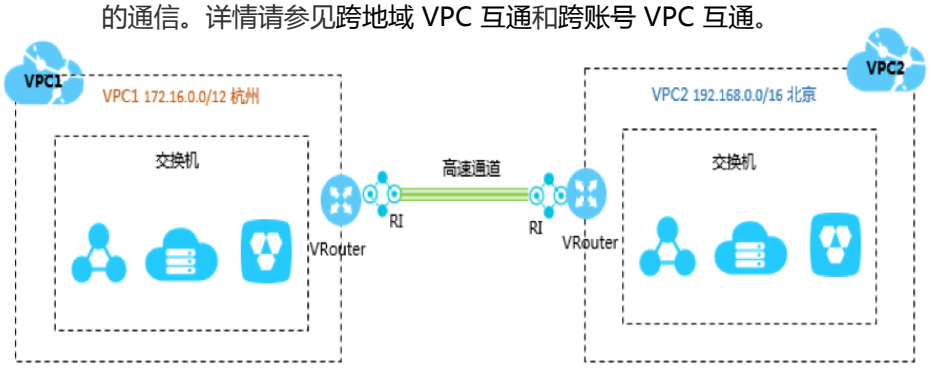
- 拨入 VPN；
- 登录 G1（跳板机或堡垒机）；
- 登录 G2（Web Server）和 G3（Business Server），堡垒机对所有 ECS 进行操作审计。

VPC 间互连

您可以在不同的地域的 VPC 内部署 SAP 应用，构建多地域服务网络，实现就近提供服务降低网络时延并相互备份提高整个系统的可靠性。
阿里云高速通道和 VPN 网关都可以实现跨地域或同地域 VPC 互连。

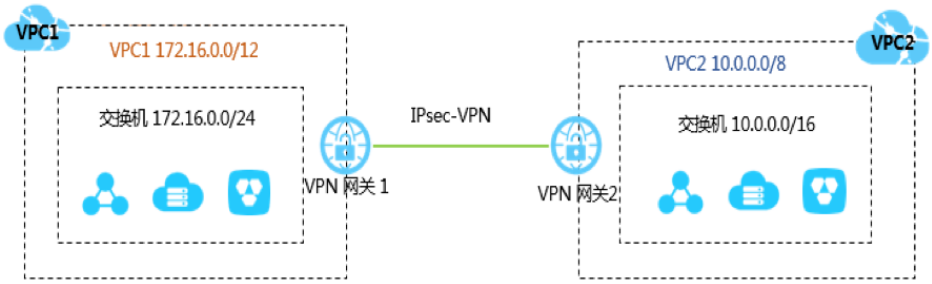
- **高速通道**
  高速通道支持同地或跨地域，同账号或跨账号的 VPC 之间的内网互通。您可以在两个 VPC 的路由器上分别创建路由器接口，基于骨干网络来搭建高速通道，轻松实现两个 VPC 之间安全可靠，方便快捷

的通信。详情请参见跨地域 VPC 互通和跨账号 VPC 互通。

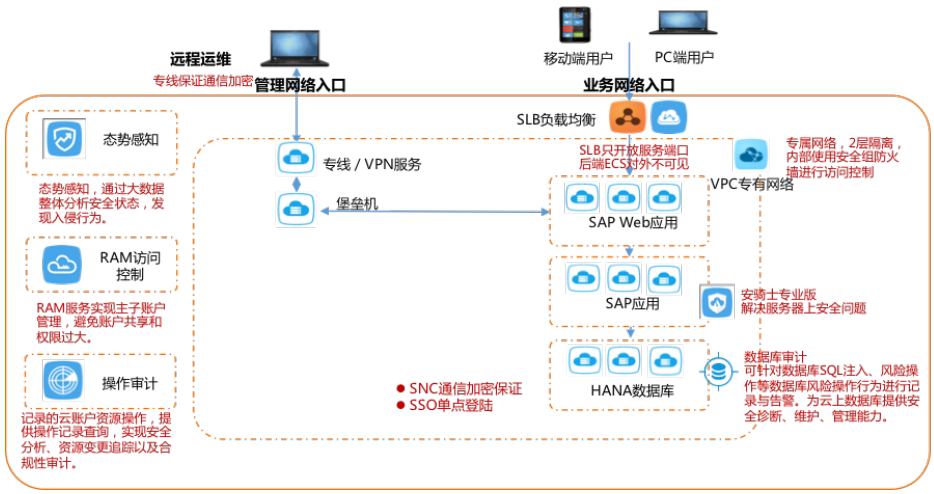


VPN 网关

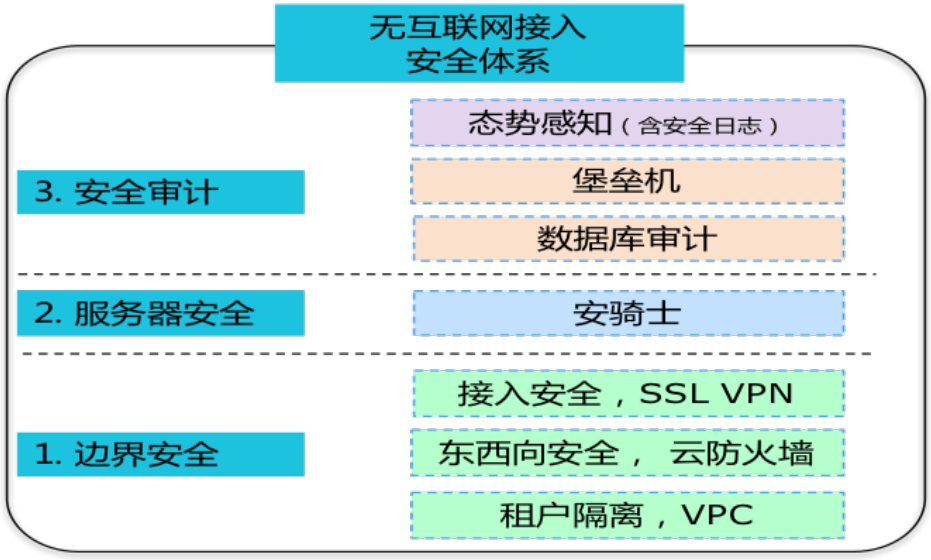
VPN 网关是一款基于 Internet，通过加密通道将企业数据中心、企业办公网络、或 Internet 终端和 VPC 安全可靠连接起来的服务。您可以通过 VPN 网关实现跨地域、跨账号 VPC 互通。您需要分别为互连的 VPC 创建两个 VPN 网关和用户网关，然后在 VPN 网关和用户网关间建立 IPsec 加密隧道进行私网通信。



SAP 系统安全架构



在 SAP 应用的基础安全体系中，基于标准的 C/S 架构的 SAP 应用，无互联网或 Internet 接入需求。阿里云推荐部署安骑士、态势感知和堡垒机，对于 SAP 核心应用的数据库，如 SAP HANA、Oracle、DB2、Sybase等，建议部署数据库审计服务产品，保障您的数据库应用安全。



基于无互联网接入的 SAP 安全体系，从边界安全、服务器安全和安全审计3个维度构建 SAP 的安全体系，保证 SAP 应用的稳定运行。



当您部署了基于 B/S 架构的 SAP 应用，或部署了多种访问类型的 SAP 应用。基于 B/S 或混合架构的 SAP 安全体系，在 C/S 架构的安全体系下，阿里云推荐增加网络漏洞扫描，Web 应用防火墙和安全管家等阿里云安全产品。

除此之外，阿里云还提供了多种的安全产品，从不同的维度保障您的应用安全，可参加章节阿里云安全产品。

阿里云安全产品

账户安全

阿里云提供多种安全机制来帮助客户保护账户安全以防止未授权的用户操作。这些安全机制包括云账户登录及 MFA 管理、创建子用户、集中管理子用户权限、数据传输加密、子用户操作审计。客户可以使用这些机制来保

护其云账户安全。

主机安全

入侵检测和漏洞管理，阿里云用户可以通过在主机上安装轻量级软件安骑士，实现与云端安全中心的联动，获取入侵检测、漏洞管理的安全能力。

镜像加固，阿里云保持对阿里云公共镜像操作系统漏洞以及三方软件漏洞的实时监测，以确保所有阿里云公共镜像高危漏洞在第一时间得到修复，阿里云公共镜像默认进行主机最佳安全实践配置，得到全面的安全保障。

自动宕机迁移，云服务器部署在宿主机(承载云服务器的物理服务器)上，宿主机可能因性能异常或者硬件原因导致故障，当检测到云服务器所在的宿主机发生故障时，系统会启动保护性迁移，把云服务器迁移到正常的宿主机上，恢复实例正常运行，保障应用的高可用性。

应用安全

Web 应用防火墙(Web Application Firewall, WAF)，基于云安全大数据能力实现，通过防御 SQL 注入、XSS 跨站脚本、常 Web 服务器插件漏洞、木上传、非授权核心资源访问等 OWASP 常攻击，过滤海量恶意访问，避免网站资产数据泄露，保障网站的安全与可用性。

代码安全，在云产品安全生命周期(SPLC)中，阿里云的安全专家在各个开发节点中都会严格审核和评估代码的安全性，从而保障阿里云提供给用户的产品的代码安全质量。

数据库审计服务，是一款专业、主动、实时监控数据库安全的审计产品。数据库审计服务将数据库监控、审计技术与公共云环境相结合，支持对阿里云平台中的 RDS云数据库、ECS自建数据库（包括 SAP HANA）进行审计，针对数据库 SQL 注入、风险操作等数据库风险行为进行记录与告警，形成对核心数据的安全防护，为您的云端数据库提供完善的安全诊断、维护、管理功能。

网络安全

网络隔离，阿里云建议对生产环境网络与非生产环境网络，以及 SAP 应用网络与非 SAP 应用网络，进行了安全隔离，各子网络之间不能直接访问任何服务器和网络设备。

VPN 网关(Virtual Pirvate Network Gateway)，是一款基于 Internet，通过加密通道将企业数据中心，企业办公网络，阿里云专有网络(VPC)安全可靠连接起来的服务。

专有网络(Virtual Private Cloud)，可以帮助用户基于阿里云构建出一个隔离的网络环境，并可以自定义 IP 地址范围、网段、路由表和网关等；此外，也可以通过专线/VPN 等连接方式实现云上 VPC 与传统 IDC 的互联，构建混合云业务。

分布式防火墙，安全组是阿里云提供的分布式虚拟化防火墙，具备状态检测和包过滤功能。使用安全组可设置单台或多台云服务器的网络访问控制，它是重要的网络安全隔离手段，用于在云端划分网络安全域。

DDoS 防御，阿里云使用自主研发的 DDoS 防护系统保护所有数据中心，提供 DDoS 攻击自动检测、调度和清洗功能，可以在 5 秒钟内完成攻击发现、流量牵引和流量清洗全部动作，保证云平台网络的稳定性。

数据安全

数据安全体系，阿里云数据安全体系从数据安全生命周期角度出发，采取管理和技术两方面的手段，进行全面、系统的建设。通过对数据生命周期(数据生产、数据存储、数据使用、数据传输、数据传播、数据销毁)各环节进行数据安全管理管控，实现数据安全目标。

全栈加密，阿里云对于数据安全提供了全栈的加密保护能力，其中包括从应用程序敏感数据加密，RDS 数据库透明加密，块存储数据加密，对象存储系统加密，硬件加密模块和网络数据传输加密。

密钥管理，阿里云提供的密钥管理服务(Key Management Service，KMS)是一款安全易用的管理类服务。用户无需花费大量成本来保护密钥的保密性、完整性和可用性。

安全运营

态势感知，利用大数据技术，从攻击者的角度，有效捕捉高级攻击者使用的 0day 漏洞攻击、新型病毒攻击事件、和正在发生的安全攻击行为有效的展示，帮助云上租户实现云上业务安全可视和可感知。

操作审计，阿里云 ActionTrail 为客户提供统一的云资源操作安全日志管理，记录账户下的用户登录及资源访问操作，包括操作人、操作时间、源 IP 地址、资源对象、操作名称及操作状态。

应急响应，阿里云组建了专的安全应急团队来应对云平台上可能的安全威胁，并对异常事件积极的进行响应和处理。

安全众测，阿里云建有先知平台，提供私密的安全众测服务。先知可以帮助企业全面发现业务漏洞和险信息。

业务安全

业务安全服务，是基于阿里大数据控能力，通过海量险数据和机器学习模型，解决账号注册、认证、交易、运营等关键业务环节存在的各种险问题，保障企业业务健康发展。