ALIBABA CLOUD

阿里云

云存储网关

最佳实践

文档版本：20220629

阿里云

法律声明

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

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

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

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

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

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

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

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

目录

1.阿里云裸金属环境部署线下网关

本文介绍如何在裸金属环境部署线下网关。

在裸金属环境部署线下网关的最佳实践，请参见本地数据中心基于SMB或NFS协议访问对象存储。

2.云存储网关操作审计日志说明

阿里云云存储网关已与阿里云ActionTrail集成，您可以在ActionTrail中查看和检索用户行为日志，同时通过ActionTrail将日志投递到日志服务Logstore或指定的OSS Bucket中，满足实时审计、问题回溯分析等需要。

> **说明**
>
> 可查询范围为2020年11月28日之后的操作审计日志。

查看操作日志步骤

1. 登录云存储网关控制台。
2. 在左侧导航栏，选择**操作审计**。
3. 单击需要查看操作日志前的+图标。

ActionTrail中记录的云存储网关操作日志

云存储网关的操作审计日志主要包含的是API事件，其中OpenAPI事件在ActionTrail中记录的eventType取值为ApiCall。

另外部分API事件目前尚未包含在上述的API说明文档中，主要涉及的这些事件的含义参考如下：

事件类型	事件名称	事件含义
ApiCall	StartElasticGateway	启动弹性网关
ApiCall	StopElasticGateway	停止弹性网关
ApiCall	SetElasticGatewayDataPolicy	设置弹性网关数据策略
ApiCall	ModifyGatewayStorageTarget	修改弹性网关存储目标
ApiCall	ModifyElasticGatewaySpec	修改弹性网关最大吞吐量
ApiCall	DescribeGatewayStorageTargets	描述弹性网关存储目标
ApiCall	DeleteGatewayStorageTarget	删除弹性网关存储目标
ApiCall	CreateGatewayStorageTarget	创建弹性网关存储目标
ApiCall	CreateElasticGateway	创建弹性网关

事件类型	事件名称	事件含义
ApiCall	DescribeGatewayMonitorData	描述弹性网关性能指标

云存储网关的日志样例

如下示例展示了一个ActionTrail中记录的云存储网关实例创建日志，该条日志记录了云存储网关CreateGateway操作记录的详细信息：

```
{
    "eventId":"D334EC86-****-****-****-34D49A613994",
    "eventVersion":"1",
    "responseElements":{ // API响应的数据
        "RequestId":"D334EC86-****-****-****-34D49A613994",
        "Message":"successful",
        "GatewayId":"gw-0001**********rk08",
        "Code":"200",
        "Success":true
    },
    "eventSource":"sgw.cn-hangzhou.aliyuncs.com",
    "requestParameters":{ // API请求的输入参数
        "AcsHost":"sgw.cn-hangzhou.aliyuncs.com",
        "Category":"Aliyun",
        "PublicNetworkBandwidth":5,
        "RequestId":"D334EC86-****-****-****-34D49A613994",
        "VSwitchId":"vsw-bp1c********ea7",
        "StorageBundleId":"sb-000a**********wrb2",
        "HostId":"sgw.cn-hangzhou.aliyuncs.com",
        "GatewayClass":"Basic",
        "Name":"test",
        "Type":"File",
        "ReleaseAfterExpiration":false,
        "AcsProduct":"sgw",
        "AcceptLanguage":"zh-CN",
        "PostPaid":true,
        "RegionId":"cn-hangzhou",
        " charset":"UTF-8",
        "Location":"Cloud"
    },
    "sourceIpAddress":"192.168.1.1", // 事件发起的源IP地址
    "userAgent":"sgwnew.console.aliyun.com",
    "eventType":"ApiCall",
    "referencedResources":{ // 事件影响的资源列表
        "ACS::CloudStorageGateway::Gateway":[
            "gw-0001**********rk08"
        ]
    },
    "userIdentity":{ // 请求者的身份信息
        "sessionContext":{
            "attributes":{
                "mfaAuthenticated":"false"
```

```
            }
        },
        "accountId":"106**********811", // 阿里云主账号ID
        "principalId":"106**********811", // 当前请求者的ID
        "type":"root-account", // 阿里云主账号
        "userName":"root"
    },
    "serviceName":"CloudStorageGateway", // 事件相关的云服务名称
    "additionalEventData":{
        "Scheme":"https"
    },
    "apiVersion":"2018-05-11",
    "requestId":"D334EC86-****-****-****-34D49A613994",
    "eventTime":"2020-11-18T11:14:05Z", // 事件的发生时间（UTC格式）
    "acsRegion":"cn-hangzhou",  // 阿里云地域
    "eventName":"CreateGateway"  // 事件名称
}
```

3.账号访问控制

本文介绍如何使用访问控制RAM（Resource Access Management）在账号级别上控制对云存储网关资源的访问，具体通过创建RAM用户（组）并授予特定权限策略实现。

背景信息

访问控制RAM是阿里云提供的资源访问控制服务，使用RAM还可以让您避免与其他用户共享云账号密钥（AccessKey），按需为用户分配最小权限，从而降低您的企业信息安全风险。更多详情，请参见什么是访问控制。

- 用户：如果您创建了多个云存储网关，您的组织里有多个用户需要使用这些网关，您可以创建一个策略允许部分用户使用这些网关。避免了将同一个AccessKey泄露给多人的风险。
- 用户组：您可以创建多个用户组，并授予不同权限策略，起到批量管理的效果。

创建RAM用户

1. 使用主账号登录 RAM访问控制台。
2. 在左侧导航栏中，选择**人员管理 > 用户**，单击**新建用户**。
3. 配置用户账号信息。
4. 配置访问方式，勾选**控制台登录密码**或**编程访问**。
5. 勾选**自定义登录密码**，输入一个初始密码，并勾选**用户在下次登录时必须重置密码**。
6. （可选）启动多因素认证设备，单击**确定**。
7. 保存生成的账号、密码、AccessKeyID和AccessKeySecret。

> **说明** 请及时保存该 AccessKey 信息，并妥善保管。

创建用户组

如果您需要创建多个RAM用户，您可以选择通过创建用户组对职责相同的RAM用户进行分类并授权，从而更方便地管理用户及其权限。

1. 使用主账号登录 RAM访问控制台。
2. 在左侧导航栏中，选择**人员管理 > 用户组**，单击**新建用户组**。
3. 填写用户组名称和显示名称，单击**确认**。

为RAM用户/用户组分配授权策略

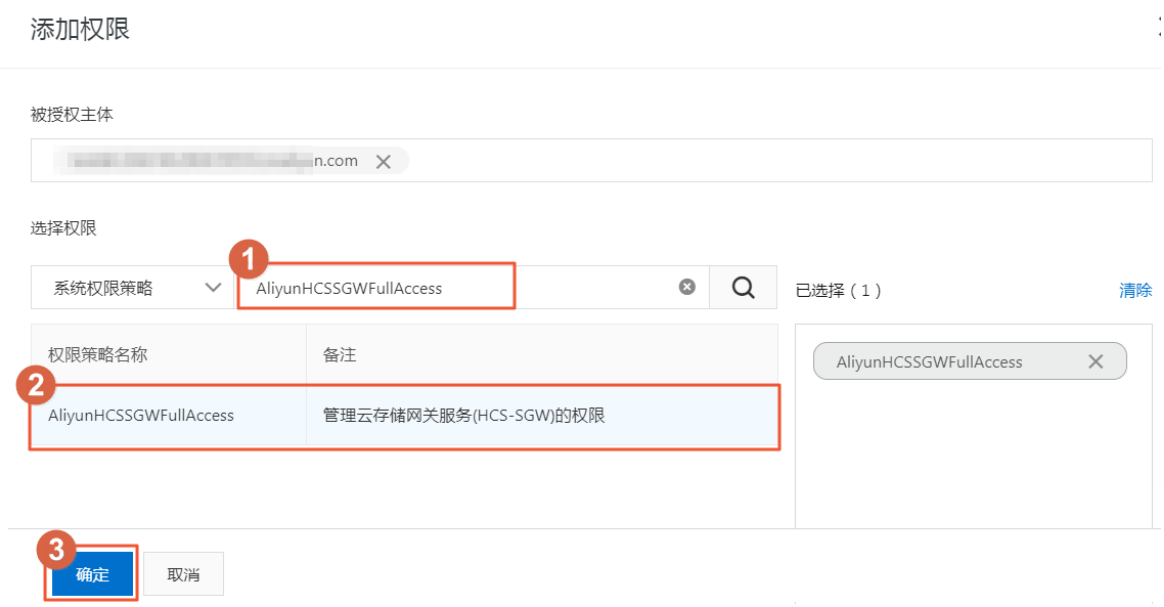
新建的RAM用户/用户组默认没有任何操作权限，只有在被授权策略之后，才能通过控制台和API操作资源。此处以RAM用户为例，介绍授权操作步骤。

1. 在**用户**页面，选择要授权的子账号，单击**添加权限**。
2. 在**添加权限**页面，添加如下权限，为子账号授权。

   云上网关需添加如下4种权限，本地网关只需添加AliyunHCSSGWFullAccess和AliyunOSSFullAccess权限。

   - AliyunHCSSGWFullAccess：管理云存储网关服务（HCS-SGW）的权限
   - AliyunOSSFullAccess：管理对象存储服务（OSS）权限
   - AliyunVPCFullAccess：管理专有网络（VPC）的权限

- AliyunECSFullAccess：管理云服务器服务（ECS）的权限



4.归档管理

通过设置OSS Bucket的生命周期规则和自动归档操作，实现文件网关中的文件自动归档。

前提条件

- 已创建标准类型或低频访问类型的OSS Bucket，详情请参见创建存储空间。

  > **说明** 云存储网关支持标准（Standard）类型、低频访问（IA）类型和归档存储类型的OSS Bucket。

- 已创建共享。

  > **说明**
  > - 只支持自动归档NFS协议文件网关中的文件。创建共享时，**协议**需配置为**NFS**。
  > - 创建共享时，**用户映射**需配置为**none**。
  > - 创建共享时，**归档管理**需配置为**是**。

  - 如果是云上文件网关，详情请参见创建共享。
  - 如果是本地文件网关，详情请参见管理NFS共享。

背景信息

从1.0.44版本开始，支持文件网关中的文件自动归档存储到OSS Bucket。

对于标准类型或者低频访问类型OSS Bucket内的文件，文件网关提供了文件系统端配置自动归档文件，解冻归档文件，查询文件归档状态的功能，不需要跳转到OSS控制台针对某个文件进行生命周期管理。

> **说明** 自动归档文件时，需要先在OSS控制台设置生命周期规则，解冻归档文件或查询归档状态时，无需设置。

步骤一：设置生命周期规则

您可以通过生命周期规则来批量转换OSS Bucket内对象（Object）的存储类型。

1. 登录OSS管理控制台。
2. 在左侧存储空间列表中，单击目标存储空间名称，进入该存储空间概览页面。
3. 单击**基础设置**页签，找到**生命周期**区域，单击**设置**。
4. 在**生命周期**页面，单击**创建规则**。
5. 在**生命周期创建规则**页面，配置如下参数。

参数	说明
状态	选择**启用**。

参数	说明
策略	选择**配置到整个Bucket**，使生命周期规则应用到整个存储空间。 **说明** 选择**配置到整个Bucket**只允许配置一条生命周期规则。
标签	勾选**标签**并配置正确的标签，可以让规则针对拥有指定标签的对象生效。 ○ **键**设置为**AutoArchive**。 ○ **值**设置为**enabled**。
文件过期策略	设置文件过期时间，选择**过期天数**或**过期日期**。
转换到归档存储	勾选**转换到归档存储**并设置过期天数或过期日期。本文以设置过期天数1天为例。 ○ 过期天数：指定一个过期天数N。对象会在其最后修改时间的N天后过期，并执行归档操作。例如设置为1天后归档，最后修改日期为2019-10-1的对象会在2019年10月2号被后端程序扫描转换为归档存储。 **说明** 存储类型转换后的计量计费规则，请参见基于最后一次修改时间的生命周期规则介绍。 ○ 过期日期：指定一个过期日期，最后修改时间在该日期之前的对象全部过期，并执行归档操作。例如设置为2019-10-1归档，最后修改日期为2019-10-1之前的对象会被后端程序扫描转换为归档存储。

6. 单击**确定**。

注意
- 生命周期规则配置完成后即会被执行，请确认无误后再保存规则。
- 更多关于生命周期规则的介绍请参见基于最后一次修改时间的生命周期规则介绍。

步骤二：归档管理配置

1. 登录主机（Linux系统）。
2. 获取网关归档管理工具sgw_archive_util。
3. 添加网关归档管理工具的执行权限。

```
sudo chmod a+x sgw_archive_util
```

4. 使用归档管理工具，自动归档文件。

```
sgw_archive_util -a /path/file
```

/path/file为本地文件的绝对路径，请根据实际情况替换。

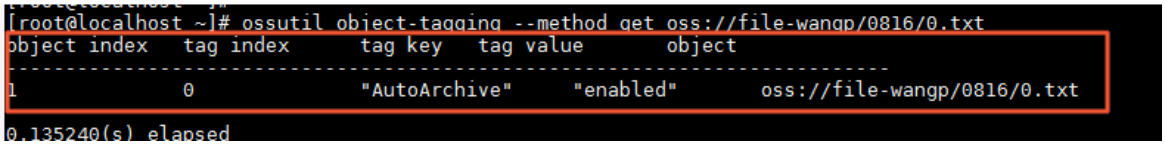
5. 执行以下命令，验证归档结果。

```
ossutil object-tagging --method get oss://file-wanqp/0816/0.txt
```

oss://file-wanqp/0816/0.txt为文件在OSS Bucket的路径，请根据实际情况替换。

在步骤一：设置生命周期规则中以设置过期天数1天为例，所以1天后，文件将自动归档存储。

如果显示如下信息，则表示自动归档成功。



相关操作

- 使用归档管理工具，自动解冻文件。

```
sgw_archive_util -r /path/file
```

/path/file为本地文件的绝对路径，请根据实际情况替换。

- 使用归档管理工具，查询归档状态。

```
sgw_archive_util -q /path/file
```

/path/file为本地文件的绝对路径，请根据实际情况替换。

5.网络配置

5.1. 通过Classiclink联通经典网络和云存储网关服务

本文介绍如何通过专有网络的ClassicLink功能联通经典网络和云存储网关服务。

背景信息

云存储网关是一款可以将本地应用程序、基础设施、数据存储与阿里云无缝集成的存储服务。通过可在本地数据中心和阿里云部署的兼容行业标准存储协议的虚拟设备，将现有的存储应用程序和工作负载连接阿里云存储服务，无缝对接阿里云的存储和计算服务。

云存储网关服务可自动部署网关和配置资源，自动适配专有网络内的ECS实例。由于阿里云公网里有大量存量的经典网络ECS实例，无法自动匹配云存储网关。您可以通过专有网络的ClassicLink功能打通经典网络和云存储网关服务，ClassicLink功能可以使经典网络ECS实例和专有网络中的云资源通过内网互通。

配置专有网络和云存储网关

1. 配置专有网络。
   i. 登录专有网络管理控制台。
   ii. 创建专有网络，详情请参见搭建专有网络。

   建议创建一个172.16.0.0/12网段的专有网络，便于配置。如果已有可用的专有网络，请跳过此步骤。

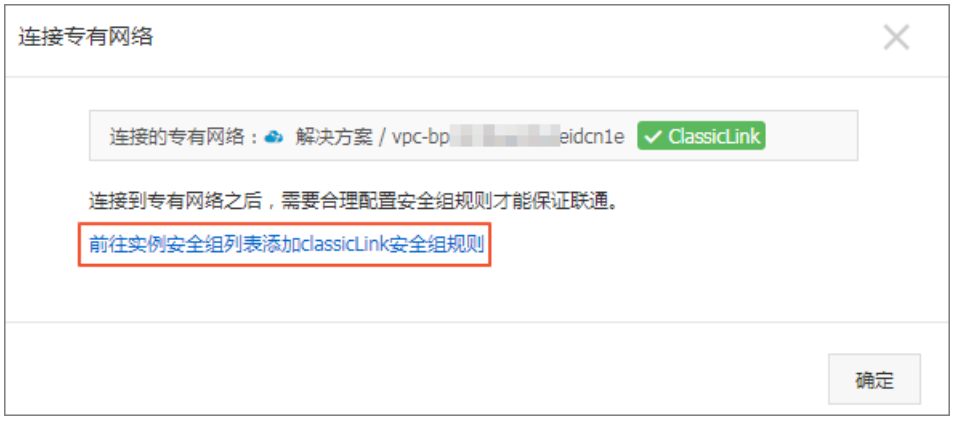
   iii. 找到并单击目标专有网络，单击**开启ClassicLink**。
2. 创建云存储网关。
   i. 登录云存储网关控制台。
   ii. 创建云存储网关。

   创建云存储网关时，请选择步骤 1中创建的专有网络。

   - 如果您要创建云上文件网关，详情请参见创建文件网关。
   - 如果您要创建云上块网关，详情请参见创建块网关。

配置经典网络的ECS实例

1. 登录云服务器管理控制台。
2. 选择目标ECS实例所在地域。
3. 在**实例**页面，找到需要联通云存储网关服务的ECS实例，单击**更多 > 网络和安全组 > 设置专有网络连接状态**。
4. 在弹出的对话框中选择目标专有网络，单击**确定**并单击**前往实例安全组列表添加classicLink安全组规则**。



5. 单击**添加ClassicLink安全组规则**，根据以下信息配置ClassicLink安全组规则，并单击**确定**。

参数	说明
经典网络安全组	显示经典网络安全组的名称。
选择专有网络安全组	此处需选择云存储网关所对应的安全组。
授权方式	选择一种授权方式。 ○ （推荐）经典网络 <=> 专有网络：相互授权访问。 ○ 经典网络 => 专有网络：授权经典网络类型ECS实例访问专有网络内的云资源。 ○ 专有网络 => 经典网络：授权专有网络内的云资源访问经典网络类型ECS实例。
协议类型	选择授权通信的协议，例如自定义TCP。
端口范围	端口的输入格式为xx/xx，比如授权80端口，则输入80/80。 不同协议对应的端口不同，请根据业务需求进行配置。 ○ HTTPS：443 ○ NFS：111（TCP、UDP），875（TCP、UDP），892（TCP、UDP），2049（TCP、UDP），32888（TCP、UDP），32889（TCP、UDP） ○ SMB：137（UDP），138（UDP），139（TCP），389（TCP），445（TCP、UDP），901（TCP） ○ iSCSI：860（TCP）、3260（TCP）
优先级	设置该规则的优先级。数字越小，优先级越高。例如：1。
描述	输入安全组描述。

6. 返回**实例**页面，查看连接结果。

   如果**连接状态**显示**已连接**，则表示经典网络类型ECS实例成功连接到专有网络。

使用云存储网关

- 文件网关
  - 如果您使用的是Linux客户端，详情请参见访问NFS共享目录。
  - 如果您使用的是Windowsx客户端，详情请参见访问SMB共享目录。
- 块网关
  - 如果您使用的是Linux客户端，详情请参见在Linux系统上使用卷。
  - 如果您使用的是Windowsx客户端，详情请参见在Windows系统上使用卷。

5.2. 云企业网版配置实践

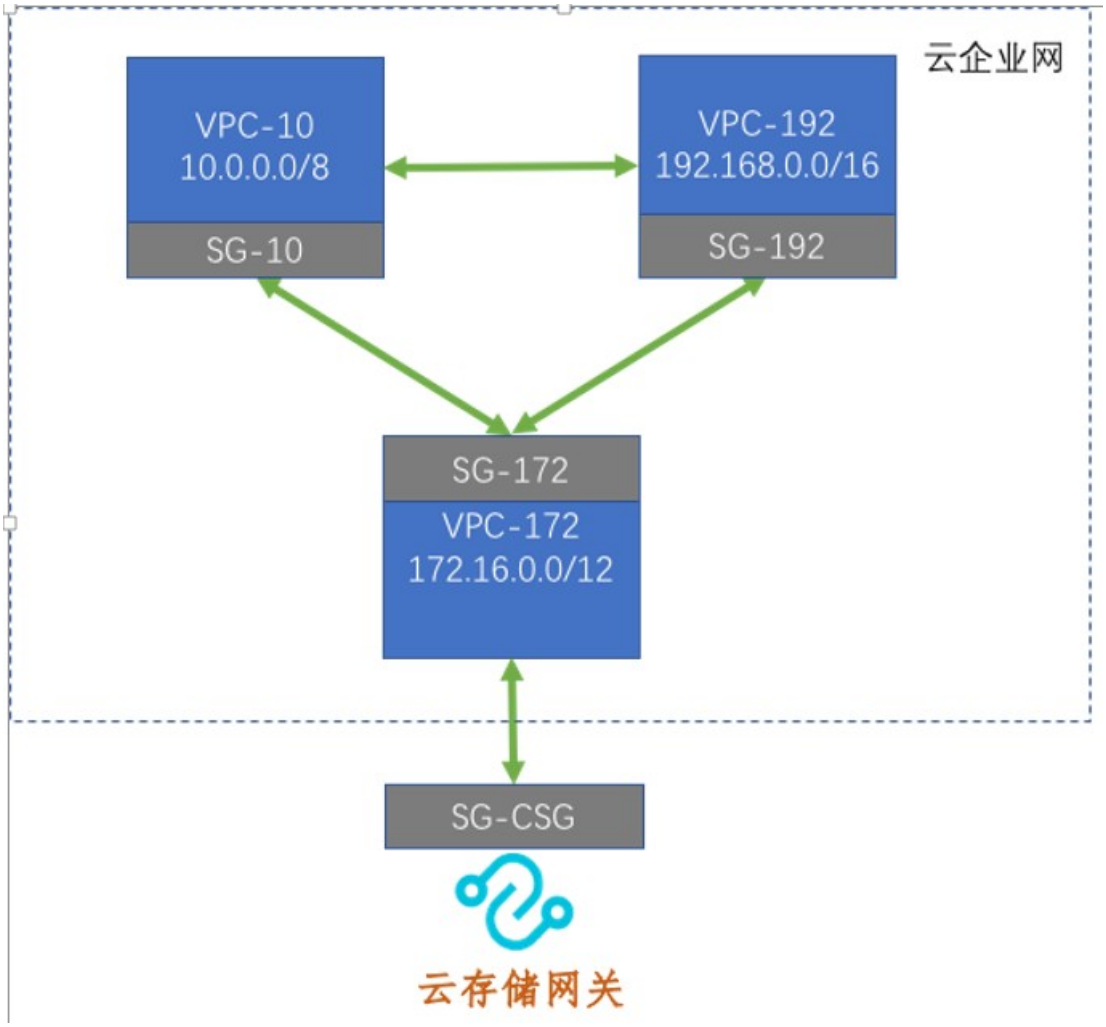
本文介绍如何通过云企业网实现多个专有网络ECS实例访问云存储网关。

背景信息

云存储网关是一款可以将本地应用程序、基础设施、数据存储与阿里云无缝集成的存储服务。通过可在本地数据中心和阿里云部署的兼容行业标准存储协议的虚拟设备，将现有的存储应用程序和工作负载连接阿里云存储服务，无缝对接阿里云的存储和计算服务。

由于阿里云公网里有大量的企业客户采用多个专有网络互联的方式支持大规模ECS集群，而1.0.31及之前版本的云存储网关只支持单个专有网络ECS实例连接，不支持多个专有网络互联。云存储网关服务从1.0.32版本开始，支持多个VPC网段：192.168.0.0/16、 172.16.0.0./12、10.0.0.0/8。而，

本案例介绍在三个专有网络互联的场景下，如何配置云企业网、安全组使得三个专有网络ECS实例都可以访问云存储网关。



- SG表示安全组。
- VPC表示虚拟网络，172.16.0.0/12等表示支持的IP地址网段。

配置云企业网

1. 登录云企业网管理控制台。
2. 创建云企业网实例。具体操作，请参见步骤二：创建CEN实例。
3. 加载网络实例。具体操作，请参见步骤三：加载网络实例。

   将三个专有网络加入同一个云企业网。

配置安全组策略

通过配置云存储网关的安全组实现整个云企业网可以共享同一个云存储网关，此处需配置安全组SG-10和SG-192。

1. 登录云服务器管理控制台。
2. 选择**网络与安全 > 安全组**。
3. 找到**安全组列表**页面，找到目标安全组，单击**配置规则**。
4. 在**安全组规则**页面，单击**创建安全组规则**。
5. 在**添加安全组规则**页面，配置相关信息。

其中**授权类型**选择**IPv4 地址段访问**，关于其他参数配置，请参见添加安全组规则。

如果需要使用LDAP和AD，则在安全组中配置端口（TCP 53/636和UDP 53/636）即可。

通过配置安全组规则，在云企业网里的ECS实例可以轻松访问云存储网关提供的NFS/SMB/iSCSI的协议转换功能，对接海量的OSS存储，帮助您轻松应对存储扩容、跨地域共享和数据分发、适配传统应用和备份数据归档转存等场景。更多信息，请参见云存储网关场景。

使用云存储网关

- 文件网关
  - 如果您使用的是Linux客户端，详情请参见访问NFS共享目录。
  - 如果您使用的是Windowsx客户端，详情请参见访问SMB共享目录。
- 块网关
  - 如果您使用的是Linux客户端，详情请参见在Linux系统上使用卷。
  - 如果您使用的是Windowsx客户端，详情请参见在Windows系统上使用卷。

5.3. 高速通道版配置实践

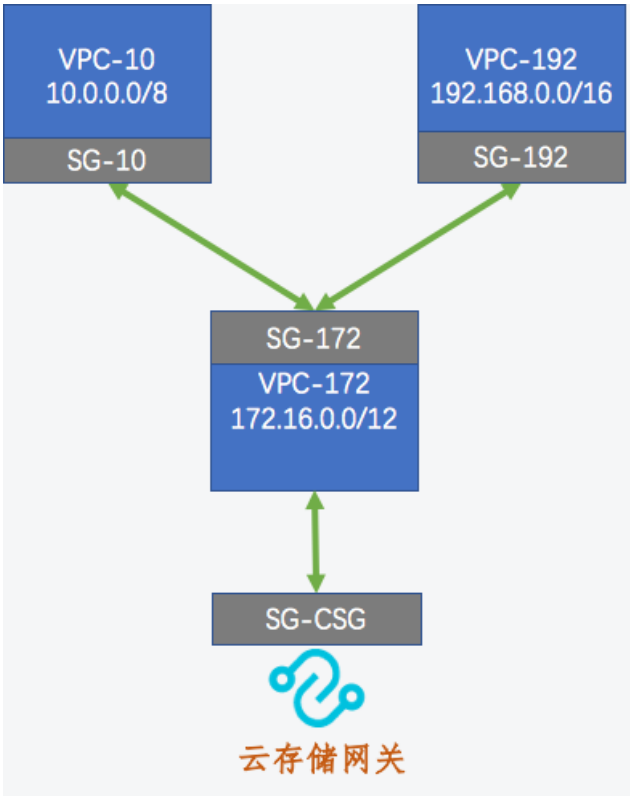
本文介绍如何通过高速通道实现多个专有网络ECS实例访问云存储网关。

背景信息

云存储网关是一款可以将本地应用程序、基础设施、数据存储与阿里云无缝集成的存储服务。通过可在本地数据中心和阿里云部署的兼容行业标准存储协议的虚拟设备，将现有的存储应用程序和工作负载连接阿里云存储服务，无缝对接阿里云的存储和计算服务。

由于阿里云公网里有大量的企业客户采用多个专有网络互联的方式支持大规模ECS集群，而1.0.31及之前版本的云存储网关只支持单个专有网络ECS实例连接，不支持多个专有网络互联。云存储网关服务从1.0.32版本开始，支持多个VPC网段：192.168.0.0/16、172.16.0.0./12、10.0.0.0/8。

本案例介绍在三个专有网络互联的场景下，如何配置网络、高速通道和安全组使得三个专有网络ECS实例都可以访问云存储网关。



- SG表示安全组。
- VPC表示虚拟网络，172.16.0.0/12等表示支持的IP地址网段。

创建云存储网关

1. 登录云存储网关控制台。
2. 选择需要创建文件网关的地域。
3. 在**网关列表**页面，创建云存储网关。

   创建云存储网关时，请选择VPC-172（172.16.0.0./12）网段下的专有网络。
   - 如果您要创建云上文件网关，具体操作，请参见创建文件网关。
   - 如果您要创建云上块网关，具体操作，请参见创建块网关。

配置专有网络和高速通道

1. 登录高速通道管理控制台。
2. 在**VPC互联**页面，单击**创建对等连接**。
3. 在**高速通道-对等连接（预付费）**页面，配置相关信息。具体操作，请参见同账号VPC互连。

   以VPC-172作为发起端，分别创建VPC-172到VPC-10和VPC-172到VPC-192的对等连接。
4. 建立对等连接后，为互连的专有网络添加路由。
   i. 找到并单击发起端实例。
   ii. 在**基本信息**页面，单击**添加对端路由**。
   iii. 输入要连接的专有网络或其交换机的网段，单击**确定**。

   此处输入对端专有网络的网段：192.168.0.0/16（VPC-192），10.0.0.0/8（VPC-10）。

iv. 配置完成后，请检查高速通道的连通性。

VPC-172下的ECS实例可以PING通VPC-192下的ECS实例和VPC-10下的ECS实例。

配置安全组策略

通过配置云存储网关的安全组实现整个云企业网可以共享同一个云存储网关，此处需配置安全组SG-10和SG-192。

1. 登录云服务器管理控制台。
2. 选择**网络与安全 > 安全组**。
3. 找到**安全组列表**页面，找到目标安全组，单击**配置规则**。
4. 在**安全组规则**页面，单击**创建安全组规则**。
5. 在**添加安全组规则**页面，配置相关信息。

   其中**授权类型**选择**IPv4 地址段访问**，关于其他参数配置，请参见添加安全组规则。

   如果需要使用LDAP和AD，则在安全组中配置端口（TCP 53/636和UDP 53/636）即可。

通过配置安全组规则，在高速通道里的ECS实例可以轻松访问云存储网关提供的NFS/SMB/iSCSI的协议转换功能，对接海量的OSS存储，帮助您轻松应对存储扩容、跨地域共享和数据分发、适配传统应用和备份数据归档转存等场景。更多信息，请参见云存储网关场景。

使用云存储网关

- 文件网关
  - 如果您使用的是Linux客户端，详情请参见访问NFS共享目录。
  - 如果您使用的是Windowsx客户端，详情请参见访问SMB共享目录。
- 块网关
  - 如果您使用的是Linux客户端，详情请参见在Linux系统上使用卷。
  - 如果您使用的是Windowsx客户端，详情请参见在Windows系统上使用卷。

6.功能特性

6.1. 使用Windows权限控制功能实现基于访问权限的枚举

本文通过一个操作实例说明如何使用云存储网关的Windows权限控制功能实现基于访问权限的枚举。

前提条件

- 已经创建了SMB共享并开启了Windows权限控制功能。详细步骤请参见开启Windows权限控制。
- 已经创建了Windows系统的ECS实例作为客户端，该ECS实例必须与云存储网关处于同一专有网络中。详细步骤请参见创建ECS实例。
- 域控制器里已有三个域用户：Administrator、user1和user2。

背景信息

在Windows文件系统中，即使用户没有权限对某个文件或文件夹进行操作，该文件或文件夹对用户依然默认可见。开启云存储网关的Windows权限控制功能后，挂载至客户端的共享目录可以启用基于访问权限的枚举，使用户只能看到自身有权限操作的文件或文件夹。

本文中ECS实例的操作系统为Windows Server 2012 R2数据中心版。

添加用户权限

1. 登录云存储网关控制台。
2. 选择目标文件网关所在的地域，然后在**网关列表**页面，找到并单击目标文件网关。
3. 选择**共享**页签，在目标SMB共享右侧的**操作**列中单击**设置**。
4. 在**SMB共享设置**对话框中，将创建好的Administrator、user1和user2加入**读写权限用户**中。
5. 单击**确认**。

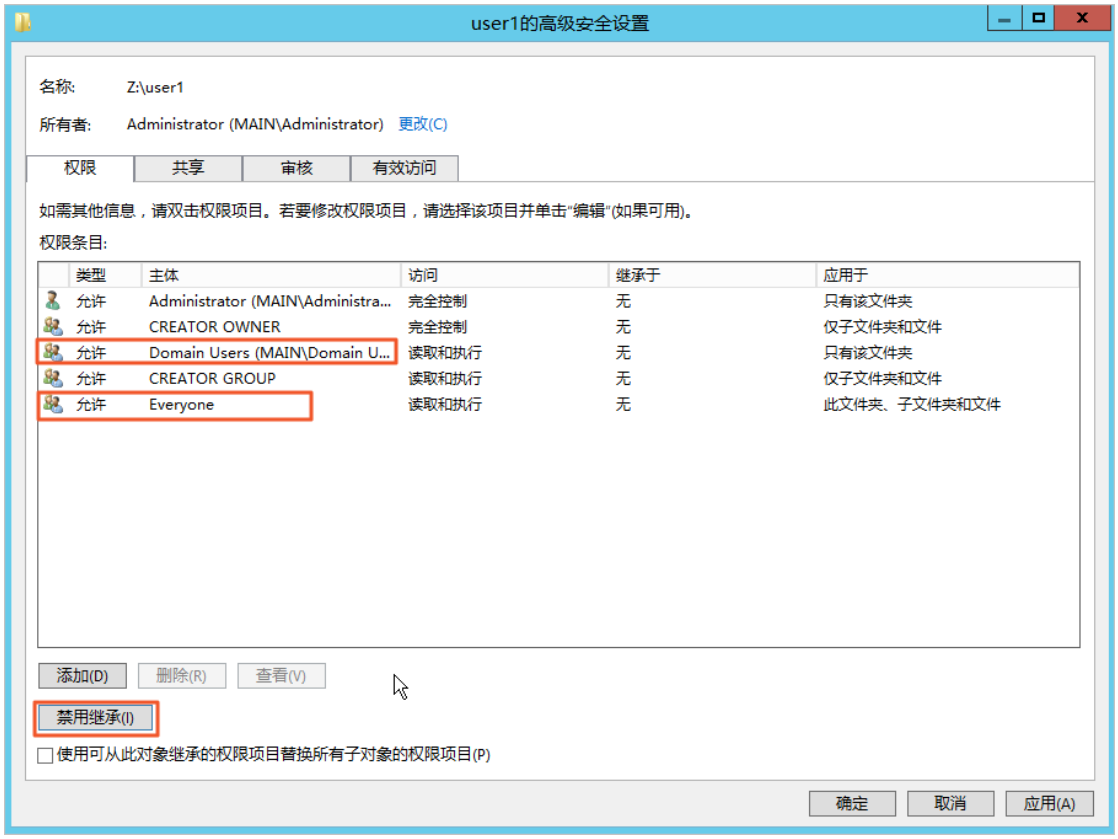
挂载共享目录并设置文件夹权限

1. 登录创建好的Windows系统ECS实例。
2. 打开**计算机**，单击**映射网络驱动器**。
3. 选择驱动器，在**文件夹**框中输入云存储网关的挂载点，然后单击**完成**。

   您可以在云存储网关控制台中找到目标云存储网关，并在其**共享**页面查看挂载点。
4. 在**Windows安全**对话框中，输入Administrator及其密码，单击**确定**。

   输入用户名时，需要在前面添加AD域名，格式为：<AD域名>\Administrator。
5. 进入挂载后的共享目录，创建两个新文件夹：*user1*和*user2*。
6. 右键单击*user1*文件夹，单击**属性**，选择**安全**页签。
7. 按照以下步骤设置*user1*文件夹的权限，使得只有Administrator和user1对该文件夹有操作权限。

i. 单击**高级**，在**权限**页签，单击**禁用继承**，然后删除Everyone和Domain Users权限，单击**应用**并**确定**。



ii. 单击**编辑**，在权限对话框中单击**添加**，输入user1并单击**检查名称**。

iii. 在**Windows安全**对话框中，输入user1及其密码，单击**确定**。

输入用户名时，需要在前面添加AD域名，格式为：<AD域名>\user1。

8. 按照步骤7中的方法设置*user2*文件夹的权限，使得只有Administrator和user2对该文件夹有操作权限。

验证Windows权限控制功能

1. 在**这台电脑**中，右键单击挂载的共享目录，单击**断开**。
2. 刷新后，按照挂载共享目录并设置文件夹权限中的步骤2与步骤3重新挂载共享目录。
3. 分别使用user1、user2和Administrator连接并进入挂载后的共享目录。
   结果如下：
   - user1只能看到*user1*文件夹。
   - user2只能看到*user2*文件夹。
   - Administrator能够看到*user1*和*user2*文件夹。

这样，我们就通过云存储网关的Windows权限控制功能实现了共享目录中基于访问权限的枚举。

6.2. 云监控集成

本文介绍如何在云监控控制台上查看文件网关及块网关的监控信息。

前提条件

已创建云存储网关，请参见在云控制台上使用文件网关。

背景信息

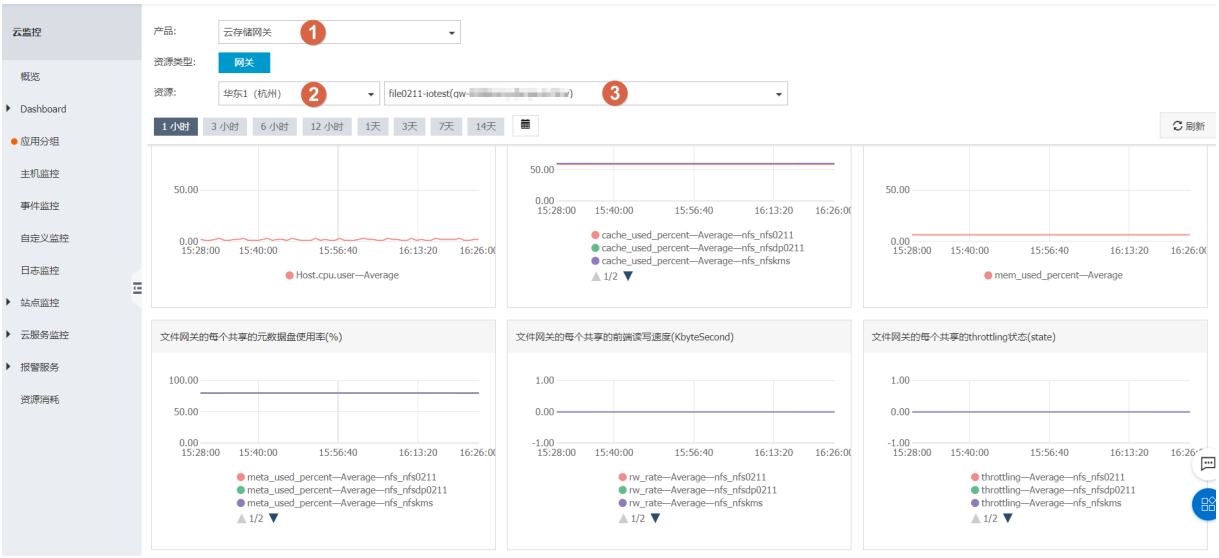
从1.3.0版本开始云存储网关支持云监控控制台的集成监控功能。

- 文件网关监控信息包括：网关cpu用户态空间使用率、每个共享的缓存使用率、网关内存使用率、每个共享的元数据盘使用率、每个共享的前端读写速度、每个共享的throttling状态、每个共享的数据上云速度。
- 块网关监控信息包括：网关cpu用户态空间使用率、网关内存使用率、每个卷的缓存使用率。

> **注意** 云监控集成功能只支持云上的存储网关。

查看监控信息

1. 登录云监控控制台。
2. 选择**Dashboard > 云产品监控**。
3. 在**云产品监控**页面，选择云存储网关及对应的地域和网关ID，查看监控图表。



相关操作

应用场景不同，您可以选择不同的时间粒度，也可以进行自定义时间粒度。

配置项	说明
监控时间粒度	可选项：1小时、3小时、6小时、12小时、1天、3天、7天、14天。
自定义时间粒度	30天内的查询提供分钟粒度的数据，最多连续查询7天数据。

6.3. 云存储文件网关缓存扩容

本文介绍了如何扩容云存储网关缓存盘。

在实际使用中，由于初期对使用场景和文件容量估算不准确，造成对云存储网关的本地缓存容量设置偏小。随着应用负载增加，缓存容量无法满足负载，此时需要对缓存盘进行扩容。目前云存储网关的缓存盘暂时不支持在线的热扩容，需要进行手动配置。下面分别以云控制台和本地网关控制台为例介绍如何手动升级网关缓存。云存储文件网关缓存设置有推荐计算公式，详情请参见使用须知。

扩容前的检查

由于扩容的时候需要临时解绑文件系统，所以需要保证在操作过程中没有IO写入，确保所有的NFS/SMB客户端的读写都已经停止。同时在所有的客户端上解除对云存储网关的挂载，并且等待文件网关的共享详情页面的缓存状态为“同步完成”，具体见下图。

云控制台：

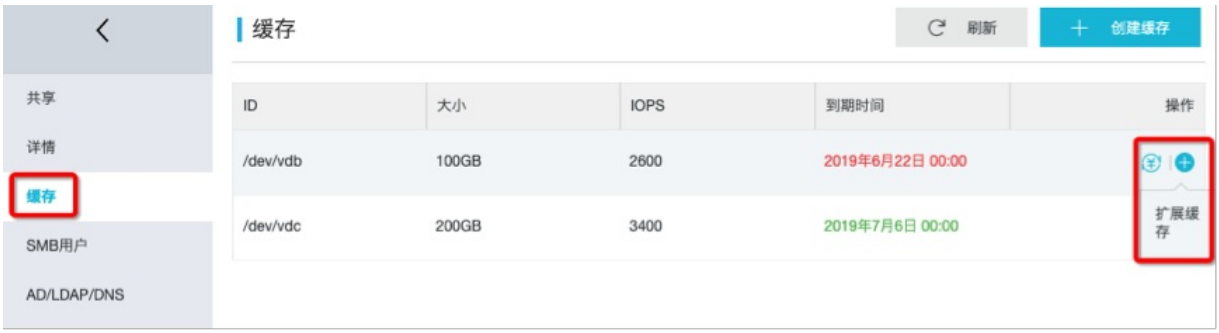
本地网关控制台：

删除需要扩容的共享

记录下当前的云存储网关的配置（bucket、共享名、访问控制列表及高级选项），然后从云控制台或者网关控制台上删除对应的共享。此时缓存盘不会被直接释放，只是解除了本地缓存和OSS存储桶之间的绑定关系。由于缓存是同步完成状态，此时所有的数据已经都上传到OSS bucket，删除共享不会造成数据丢失。

缓存物理扩容

在云控制台对现有的缓存进行扩容操作，具体如下。



点击“扩展缓存”按钮以后，会弹出下列窗口。

此时输入计算好的新的容量，就可以进行扩容，注意扩容的最小单位为1GB。点击确定后，会需要对新增容量做一次付费操作，完成购买操作后物理扩容会自动完成，在云控制台上会看到扩容后的物理容量。

当使用线下的云存储网关是，缓存的物理扩容需要在对应的vsphere/VHD/KVM的管理界面上进行操作，请参考对应的软件的操作手册。

重建共享

按照之前的共享名和配置重建共享，在重建过程时选择之前物理扩容的数据盘。此时新的共享就会显示新的缓存容量。