

本地专用集群

产品简介



腾讯云

【 版权声明 】

©2013–2024 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或 95716。

文档目录

产品简介

产品概述

产品优势

应用场景

访问管理

访问管理概述

可授权的资源类型

授权策略语法

访问管理示例

产品简介

产品概述

最近更新时间：2023-07-13 20:36:31

腾讯云本地专用集群（Cloud Dedicated Cluster，CDC）是全新推出的托管型基础设施类产品，目的是将中心化的公有云服务延伸为可在用户机房落地的近场服务。融合公有云与本地 IDC 的双重优势，用户可以基于本地化的时延和数据安全来使用公有云的丰富能力。

CDC 通过一体化机柜的形式在用户机房部署本地化算力，资源就近接入临近公有云地域实现统一管理，用户可通过公有云现有工具（控制台、API 等）来管理 CDC 资源。

产品优势

最近更新时间：2023-07-14 11:05:02

快速标准化交付

腾讯云本地专用集群（Cloud Dedicated Cluster，CDC）采用与腾讯云自有数据中心相同的采购及交付标准，在交付速度、性价比及软硬件可用性方面都精益求精。

完全一致的服务

CDC 完全同步腾讯云新技术和服务，包含星星海服务器、裸金属云服务器及超高性能云盘。用户可以基于 CDC 快速搭建超级计算集群，也可以利用容器服务 TKE、弹性伸缩 AS 等云产品构建大规模 Web 服务后台。

一致的混合云体验

用户可以使用与公有云完全一致的方案管理在 CDC 上的资源，包括但不限于控制台、API、SDK、腾讯云可观测平台等方式。真正实现混合云的同构管理及无差别调度。

运维与托管共担

不同于一般的设备售卖模式，腾讯云将为 CDC 设备和软件提供运营、升级、保障等服务。通过清晰的责任共担机制，既可保证用户的本地安全和隐私，也可使用户脱离繁琐的维保工作。

应用场景

最近更新时间：2023-07-13 20:36:31

工业自动化

工业制造过程控制系统（例如 SCADA）需要在工厂设备附近运行应用程序以保证系统毫秒级延迟。腾讯云本地专用集群（Cloud Dedicated Cluster，CDC）可以提供应用的运行环境，同时可与云中心区域的服务无缝集成。

基因生物

基因分析行业有大量数据分析和存储需求，使用 CDC 可以快速构建本地高性能计算和存储系统，帮助企业在竞争中取得优势。

媒体与娱乐

图形处理、音频和视频渲染需要使用靠近用户的本地位置实现低延迟的实时计算和存储服务。CDC 将帮助企业以更低成本、更快速度交付系统以满足市场变化的需求。

医疗保健

CDC 可以帮助医疗行业各级机构从任何地点向用户提供检查、诊断及分析等过程相关的信息服务，同时还可以满足敏感信息必须本地保留的安全需求。

访问管理

访问管理概述

最近更新时间：2023-10-09 17:24:31

如果您在腾讯云中使用到了本地专用集群（Cloud Dedicated Cluster，CDC）等服务，这些服务由不同的人管理，但都共享您的云账号密钥，将存在以下问题：

- 您的密钥由多人共享，泄密风险高。
- 您无法限制其他人的访问权限，易误操作造成安全风险。

此时，您可以通过子账号实现不同的人管理不同的服务，来规避以上的问题。默认情况下，子账号没有使用 CDC 的权利或 CDC 相关资源的权限。因此，我们就需要创建策略来允许子账号使用他们所需要的资源或权限。

访问管理（Cloud Access Management，CAM）可以帮助您安全、便捷地管理对腾讯云服务和服务资源的访问。您可以使用 CAM 创建子用户、用户组和角色，并通过策略控制其访问范围。CAM 支持用户和角色 SSO 能力，您可以根据具体管理场景针对性设置企业内用户和腾讯云的互通能力。

您最初创建的腾讯云主账号，拥有整个账号全部腾讯云服务和服务资源的完全访问权限，建议您保护好主账号的凭证信息，日常使用子用户或角色进行访问，并开启多因素校验和定时轮换密钥。

当您使用 CAM 的时候，可以将策略与一个用户或一组用户关联起来，策略能够授权或者拒绝用户使用指定资源完成指定任务。有关 CAM 策略的更多相关基本信息，请参见 [策略语法](#)。有关 CAM 策略的更多相关使用信息，请参见 [策略](#)。

说明

若您不需要对子账号进行 CDC 相关资源的访问管理，您可以跳过此章节。跳过这些部分不会影响您对文档中其余部分的理解和使用。

入门

CAM 策略必须授权使用一个或多个 CDC 操作或必须拒绝使用一个或多个 CDC 操作。同时还必须指定可以用于操作的资源（可以是全部资源，某些操作也可以是部分资源），策略还可以包含操作资源所设置的条件。

CDC 部分 API 操作支持资源级权限，意味着对于该类 API 操作，您不能在使用该类操作的时候指定某个具体的资源来使用，而必须要指定全部资源来使用。

任务	参考文档
了解策略基本结构	策略语法
在策略中定义操作	CDC 的操作
在策略中定义资源	CDC 的资源路径
使用条件来限制策略	CDC 的条件密钥

CDC 支持的资源级权限	CDC 支持的资源级权限
访问管理示例	访问管理示例

可授权的资源类型

最近更新时间：2023-07-13 20:36:32

资源级权限指的是能够指定用户对哪些资源具有执行操作的能力。本地专用集群（Cloud Dedicated Cluster，CDC）部分支持资源级权限，即表示针对支持资源级权限的 CDC 操作，控制何时允许用户执行操作或是允许用户使用特定资源。

在访问管理（Cloud Access Management，CAM）中可授权的资源类型如下：

资源类型	授权策略中的资源描述方法
本地专用集群“站点”相关	<code>qcs::cdc:\$region::site/*</code>
本地专用集群“集群”相关	<code>qcs::cdc:\$region::cluster/*</code>

本地专用集群“站点”相关、本地专用集群“集群”相关 分别介绍了当前支持资源级权限的 CDC API 操作，以及每个操作支持的资源和条件密钥。设置资源路径时，您需要将 `$region`、`$account` 等变量参数修改为您实际的参数信息，同时您也可以使用 `*` 通配符。

注意

表中未列出的 CDC API 操作即表示该 CDC API 操作不支持资源级权限。针对不支持资源级权限的 CDC API 操作，您仍可以向用户授予使用该操作的权限，但是策略语句的资源元素必须指定为 `*`。

本地专用集群“站点”相关

API 操作	资源路径	条件密钥
CreateSite	<code>qcs::cdc:\$region:\$account:site/*</code>	<code>cdc:region</code>
DeleteSites	<code>qcs::cdc:\$region:\$account:site/*</code> <code>qcs::cdc:\$region:\$account:site/\$siteId</code>	<code>cdc:region</code>
DescribeSites	<code>qcs::cdc:\$region:\$account:site/*</code> <code>qcs::cdc:\$region:\$account:site/\$siteId</code>	<code>cdc:region</code>
DescribeSitesDetail	<code>qcs::cdc:\$region:\$account:site/*</code> <code>qcs::cdc:\$region:\$account:site/\$siteId</code>	<code>cdc:region</code>

本地专用集群“集群”相关

--	--	--

API 操作	资源路径	条件密钥
CreateDedicatedCluster	qcs::cdc:\$region:\$account:cluster/*	cdc:region
CreateDedicatedClusterOrder	qcs::cdc:\$region:\$account:cluster/* qcs::cdc:\$region:\$account:cluster/\$clusterId	cdc:region
DeleteDedicatedClusters	qcs::cdc:\$region:\$account:cluster/* qcs::cdc:\$region:\$account:cluster/\$clusterId	cdc:region
DescribeDedicatedClusterInstanceTypes	qcs::cdc:\$region:\$account:cluster/* qcs::cdc:\$region:\$account:cluster/\$clusterId	cdc:region
DescribeDedicatedClusterOrders	qcs::cdc:\$region:\$account:cluster/* qcs::cdc:\$region:\$account:cluster/\$clusterId	cdc:region
DescribeDedicatedClusters	qcs::cdc:\$region:\$account:cluster/* qcs::cdc:\$region:\$account:cluster/\$clusterId	cdc:region

授权策略语法

最近更新时间：2023-07-14 10:49:41

策略语法

CAM 策略：

```
{
  "version": "2.0",
  "statement": [
    {
      "effect": "effect",
      "action": ["action"],
      "resource": ["resource"],
      "condition": {"key": {"value"}}
    }
  ]
}
```

参数说明如下：

- **版本 version**：必填项，目前仅允许值为**2.0**。
- **语句 statement**：是用来描述一条或多条权限的详细信息。该元素包括 effect、action、resource、condition 等多个其他元素的权限或权限集合。一条策略有且仅有一个 statement 元素。
 - **影响 effect**：必填项，描述声明产生的结果是**允许**还是**显式拒绝**。包括 allow（允许）和 deny（显式拒绝）两种情况。
 - **操作 action**：必填项，用来描述允许或拒绝的操作。操作可以是 API（以 name 为前缀描述）或者功能集（一组特定的 API，以 permid 为前缀描述）。
 - **资源 resource**：必填项，描述授权的具体数据。资源是用六段式描述。每款产品的资源定义详情会有所区别。有关如何指定资源的信息，请参阅您编写的资源声明所对应的产品文档。
 - **生效条件 condition**：非必填项，描述策略生效的约束条件。条件包括操作符、操作键和操作值组成。条件值可包括时间、IP 地址等信息，有些服务允许您在条件中指定其他值。

CDC 的操作

在 CAM 策略语句中，您可以从支持 CAM 的任何服务中指定任意的 API 操作。对于 CDC，请使用以 name/cdc: 为前缀的 API。例如：name/cdc:CreateDedicatedCluster。

如果您要在单个语句中指定多个操作的时候，请使用逗号将它们隔开，如下所示：

```
"action":["name/cdc:action1","name/cdc:action2"]
```

您也可以使用通配符指定多项操作。例如，您可以指定名字以单词 **Describe** 开头的的所有操作，如下所示：

```
"action":["name/cdc:Describe*"]
```

如果您要指定 CDC 中所有操作，请使用 * 通配符，如下所示：

```
"action": ["name/cdc:*"]
```

CDC 的资源路径

每个 CAM 策略语句都有适用于自己的资源。

资源路径的一般形式如下：

```
qcs:project_id:service_type:region:account:resource
```

- **project_id**: 描述项目信息，仅为了兼容 CAM 早期逻辑，无需填写。
- **service_type**: 产品简称，如 CDC。
- **region**: 地域信息，如 bj。
- **account**: 资源拥有者的根账号信息，如 uin/164256472。
- **resource**: 各产品的具体资源详情，如 cluster/cluster_id1 或者 cluster/*。

例如，您可以使用特定实例 (i-15931881scv4) 在语句中指定它，如下所示：

```
"resource":["qcs::cdc:bj:uin/164256472:cluster/cluster-7yq5m7bl"]
```

您还可以使用 * 通配符指定属于特定账户的所有实例，如下所示：

```
"resource":["qcs::cdc:bj:uin/164256472:cluster/*"]
```

您要指定所有资源，或者如果特定 API 操作不支持资源级权限，请在 Resource 元素中使用 * 通配符，如下所示：

```
"resource": ["*"]
```

如果您想要在一条指令中同时指定多个资源，请使用逗号将它们隔开，如下所示为指定两个资源的例子：

```
"resource":["resource1","resource2"]
```

下表描述了 CDC 能够使用的资源和对应的资源描述方法。

在下表中，\$为前缀的单词均为代称。

- 其中，region 指代的是地域。
- 其中，account 指代的是账户 ID。

资源	授权策略中的资源描述方法
站点	qcs::cdc:\$region:\$account:site/\$siteId
集群	qcs::cdc:\$region:\$account:cluster/\$clusterId

CDC 的条件密钥

在策略语句中，您可以选择性指定控制策略生效时间的条件。每个条件都包含一个或多个密钥值对。条件密钥不分大小写。

- 如果您指定了多个条件或在单一条件中指定了多个密钥，我们将通过逻辑 AND 操作对其进行评估。
- 如果您在单一条件中指定了一个具有多个值的密钥，我们将通过逻辑 OR 操作对其进行评估。必须匹配所有条件才能授予权限。

下表描述了 CDC 用于特定于服务的条件键。

条件键	参考类型	键值对
cdc:region	String	cdc:region= region <ul style="list-style-type: none"> • 其中 region 指代的是地域（例如 ap-guangzhou）

访问管理示例

最近更新时间：2023-07-17 14:54:11

您可以通过使用访问管理（Cloud Access Management，CAM）策略让用户拥有在本地专用集群（Cloud Dedicated Cluster，CDC）中查看和使用特定资源的权限。本文档提供了查看和使用特定资源的权限示例，指导用户如何使用控制台的特定部分的策略。

操作示例

CDC 的全读写策略

如果您希望用户拥有创建和管理 CDC 相关实例的权限，您可以对该用户使用名称为：`QcloudCDCFullAccess` 的策略。该策略允许用户对 CDC 中所有资源都具有操作的权限。具体操作步骤如下：

您可以参见 [授权管理](#)，将预设策略 `QcloudCDCFullAccess` 授权给用户。

CDC 的只读策略

如果您希望用户拥有查询 CDC 相关数据的权限，但是不具有创建、删除的权限，您可以对该用户使用名称为：

`QcloudCDCReadOnlyAccess` 的策略。该策略允许用户具有操作 CDC 中所有以单词 **Describe** 及单词 **Inquiry** 开头的所有操作的权限。具体操作步骤如下：

参见 [授权管理](#)，将预设策略 `QcloudCDCReadOnlyAccess` 授权给用户。

授权用户拥有特定 CDC 的操作权限策略

如果您希望授权用户拥有特定 CDC 操作权限，可将特定策略关联到该用户。具体操作步骤如下：

1. 根据 [策略](#)，创建一个可以查看 CDC 控制台中的云硬盘信息，具有创建、使用云硬盘等其他权限的自定义策略。

策略内容可参考以下策略语法进行设置：

```
{
  "version": "2.0",
  "statement": [
    {
      "effect": "allow",
      "action": [
        "name/cdc:CreateSite",
        "name/cdc:CreateDedicatedCluster"
      ],
      "resource": [
        "qcs::cdc::uin/1410643447:*"
      ]
    }
  ]
}
```

```
}
```

2. 找到创建的策略，在该策略行的操作列中，单击**关联用户/组**。
3. 在弹出的**关联用户/用户组**窗口中，选择您需要授权的用户/组，单击**确定**。

授权用户拥有特定地域 CDC 的操作权限策略

如果您希望授权用户拥有特定地域的 CDC 的操作权限，可将以下策略关联到该用户。具体操作步骤如下：

1. 根据 [策略](#)，创建一个允许用户拥有对广州地域的 CDC 操作权限的自定义策略。

策略内容可参考以下策略语法进行设置：

```
{
  "version": "2.0",
  "statement": [
    {
      "action": "cdc:*",
      "resource": "qcs::cdc:ap-guangzhou:*",
      "effect": "allow"
    }
  ]
}
```

2. 找到创建的策略，在该策略行的操作列中，单击**关联用户/组**。
3. 在弹出的**关联用户/用户组**窗口中，选择您需要授权的用户/组，单击**确定**。

授权子账号拥有 CDC 的所有权限但不包括支付权限

假设，企业账号（CompanyExample，ownerUin 为12345678）下有一个子账号（Developer），该子账号需要对企业账号的 CDC 服务拥有所有管理权限（例如创建、管理等全部操作），但不包括支付权限（可下单但无法支付）。

可通过以下两种方案进行实现：

- **方案 A**

企业账号 CompanyExample 直接将预设策略 `QcloudCDCFullAccess` 授权给子账号 Developer。授权方式请参见 [授权管理](#)。

- **方案 B**

- 1.1 根据以下策略语法，创建一个自定义策略。

```
{
  "version": "2.0",
  "statement": [
    {
      "effect": "allow",
```

```
"action": "cdc:*",  
"resource": "*" }  
]  
}
```

1.2 将该策略授权给子账号。授权方式请参见 [授权管理](#)。

自定义策略

如果您觉得预设策略不能满足您的要求，可以通过创建自定义策略达到目的。

具体操作步骤请参见 [策略](#)。

更多 CDC 相关的策略语法请参见 [授权策略语法](#)。