EXPRESS CONNECT: JOINED-UP THINKING FROM ALIBABA CLOUD

Alibaba Cloud
Worldwide Cloud Services Partner

AT A GLANCE

Express Connect from Alibaba Cloud is a subscription product that allows intranet-like communication between virtual private clouds (VPCs) in cases such as:

» Two VPCs in different hosting regions, via Alibaba Cloud's infrastructure

» Two VPCs on different hosting accounts, via Alibaba Cloud's infrastructure

» A VPC and an on-premises data center, via a leased line

BENEFITS

HIGH-SPEED INTERCOMMUNICATION

Powered by the very high-speed infrastructure of Alibaba Cloud's global network, Express Connect allows the connection of different network environments, so both sides can communicate with each other directly through the intranet and bypass public networks. Even when the connected sites are far away from each other, you benefit from low network latency and high bandwidth communication as if the two connected data centers, whether physical or virtual, were part of the same intranet.

Connections of up to 256MB per second are available, for access to large amounts of data at high speed. The very low latency allows for cases where a database server may remain on-site in an existing data center but the databases themselves have been migrated to the cloud in order to cope with the very large data volumes that need to be stored.

Express Connect can be used on a permanent basis to provide a stable, fixed connection between two points. Alternatively, it can be used for a relatively short period of a few hours, days or weeks in order to facilitate a migration to one or more cloud-based servers from on-site services.

> Express Connect can be used on a permanent basis to provide a stable, fixed connection between two points.

STABLE AND RELIABLE

Powered by Alibaba Group's state-of-the-art infrastructure, Express Connect ensures that connections are stable and reliable. A formal Service Level Agreement (SLA) operates, and customers receive a 25 percent refund if availability drops below 99 percent during any month. Other levels also apply for shorter periods of unavailability.

SECURE NETWORKS

Express Connect performs inter-network communication over the network virtualization layer, meaning all data is transmitted through Alibaba Cloud's own facilities. This removes the need for access to public networks and achieves multi-tenant isolation, reducing the risk of data theft during transmission. Where a link between a customer's existing data center and Alibaba Cloud infrastructure is required, use of a leased line helps guarantee the security of data in transit.

FLEXIBLE

Express Connect is designed for use in many common corporate IT scenarios. For example, multi-center deployment, hybrid networks, one-off migration tasks, or the provision of fault tolerance or disaster recovery services. The service can be configured from scratch in just a few minutes.

EASE OF USE

Express Connect replaces complex physical network configurations with a few simple operations. At the same time, you will have complete control over the communication bandwidth, operation status, and route configurations on both sides.

PURCHASE ON-DEMAND

A diverse range of specifications are available, providing different data transmission speeds. You can purchase only what is needed for your business, in order to minimize costs. Prices as at January 2018 start at less than USD $200 per month for a 1.25MB per second connection, depending on the location of the two sites being bridged.

CONTENTS

INTRODUCTION

Businesses are using the cloud like never before. But it's very rarely one-business-one-cloud. It is instead commonplace for organizations to deploy a mix of services from different cloud providers, to host with one provider in multiple regions and to mix onsite clouds with offsite clouds.

And this raises the challenge of how to safely and securely connect different cloud environments.

This whitepaper explores some of the issues and presents the Alibaba Cloud Express Connect network service, which provides a fast, stable, secure and private or dedicated network communication between different cloud environments. This network service includes VPC intranet intercommunication and dedicated leased line connections across regions and between users.

> Businesses are using the cloud like never before. But it's very rarely one-business-one-cloud.
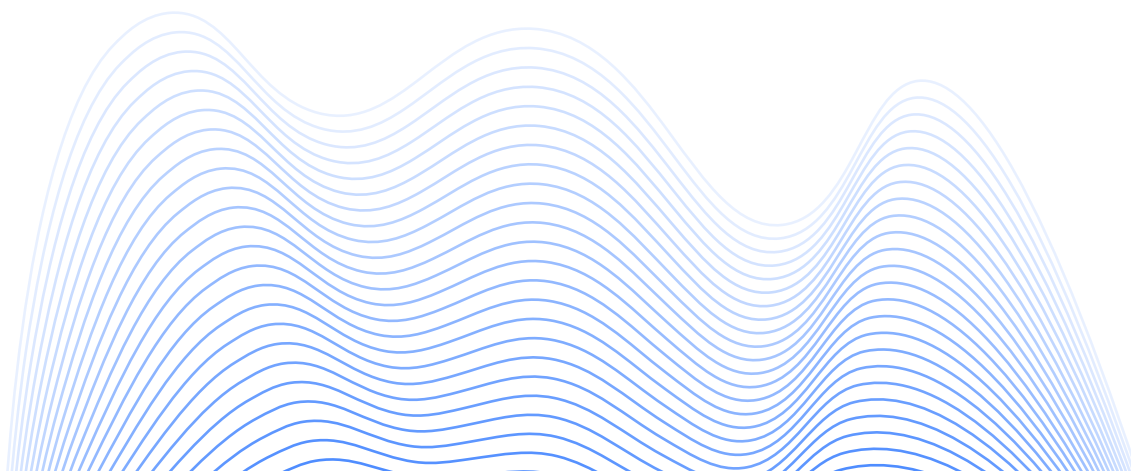
CONNECTIVITY AND SECURITY

There's no doubting that the only way is up for cloud computing. Almost unheard of at the start of the 21st Century, it's now on the lips of every IT manager in the world as they look to optimize or eliminate in-house data centers.

Consumers, too, are nowadays quite comfortable storing, backing up and editing documents and images online. The days of desktop PCs being supplied with massive amounts of local storage might be drawing to an end. A small drive and a fast Internet connection is more flexible and arguably more secure.

According to a 2017 survey[1] carried out among 350,000 members of an online security community, 76 percent of responding organizations are piloting, implementing or already operating in the cloud.

The stated benefits provide a compelling explanation for the current exodus of in-house IT. In the survey, 47 percent cited flexible capacity and scalability as the primary benefits, 43 percent said improved availability and business continuity, and 36 percent mentioned cost reduction. But head further into the survey report, under the category of cloud adoption barriers, and a common presumption turns out to be a proven truth. Security risks is the biggest adoption barrier, at 33 percent, followed by lack of staff resources, and issues with integrating existing systems with cloud-based ones.

When specifically asked whether they were concerned about cloud security, 81 percent of responders said that they were moderately, extremely or very concerned. And when you look more closely at the figures for the type of data that companies are moving to the cloud, it's not hard to see why. Email, customer data, and employee data each score around 40 percent. Coming in at around 30 percent are sales and marketing data, contracts and invoices, and financial corporate data.

SECURITY RISKS IS THE BIGGEST CLOUD ADOPTION BARRIER AT 33%

Alibaba Cloud is acutely aware that security is the #1 concern to our customers and indeed to the reputation of our own services. IT managers have historically been rightly protective of their in-house networks and don't relinquish control unless there is a clear benefit. For them, a server that's out of sight is rarely out of mind.

Cloud providers invest significant amounts of effort and money into ensuring that their services remain secure, regardless of the multitude of uses to which their infrastructure gets put. And because cloud providers' customers have such a wide variety of demands in terms of computing power and connectivity, this isn't always easy.

"
Alibaba Cloud is acutely aware that security is the #1 concern to our customers and indeed to the reputation of our own services.
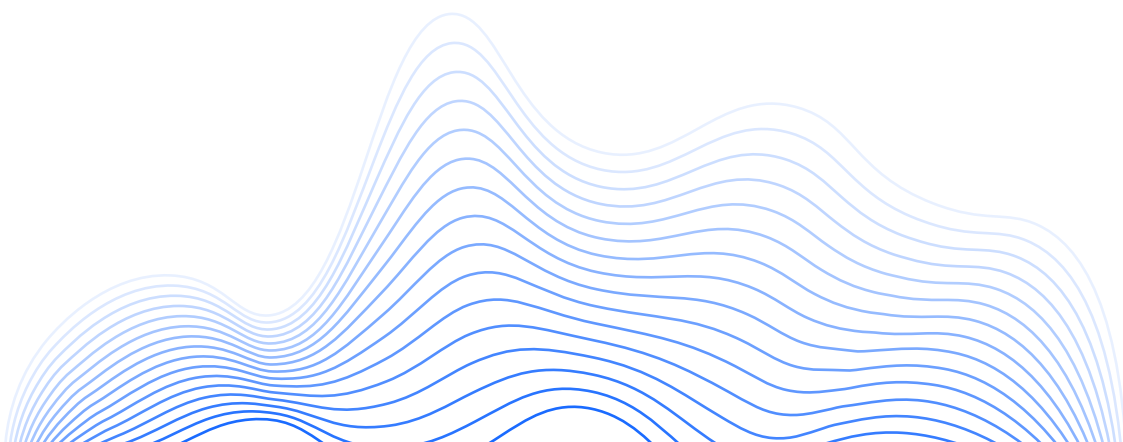
THE VPC

Although it's possible to start off with a cloud presence that consists merely of a single server or even a shared web hosting account, the basic building block of any serious cloud presence for a company looking to move its servers off-site is a Virtual Private Cloud (VPC). A VPC is a "network in the cloud" running on a cloud provider's infrastructure, which typically consists of one or more routers, switches, and servers. In the case of Alibaba Cloud, the switches are known as VSwitches and each server is an Elastic Compute Service (ECS) instance.

Within a VPC, one or more servers can be grouped into a single unit known as a cluster, in order to provide a more scalable and resilient environment. A cluster can also house a containerized environment using Alibaba Cloud's Docker-based[2] infrastructure known as Container Service. A cluster of just one ECS instance can be used to start deploying containers, with new servers being added (or decommissioned) as the need arises (or budgets dictate) for more or less power within the cluster.

By its very nature, a virtual private cloud is a very secure and closed system. Communication channels between the virtual devices in the VPC are fully under your control, and you can allow or deny them as you wish. Communication with a device outside of the VPC, or outside of an ECS instance, requires firewall ports being opened, Virtual Private Networks (VPNs) possibly being established, and use of the Internet for the data transfer to take place.

In certain cases, however, this isn't ideal. Allowing a VPC to talk to another VPC via the Internet can sometimes be a security risk, and can also often fall foul of specific industry regulations. A similar situation arises if a comms link is required between a cloud-based VPC and a traditional in-house data center. A VPN will probably work, but there's a security risk to the data in transit and the quality of the link is reliant on the Internet Service Provider (ISP) being used.

> By its very nature, a virtual private cloud is a very secure and closed system.

This can be a real issue in certain instances. Perhaps your web server and domain controllers are in the cloud, but the email and file servers are still on-premises. Or the SQL Server box is on-premises but the databases themselves are not.

Cloud providers employ what are known as hosting regions. Alibaba Cloud, for example, has hosting regions in the north, east and south of China, Singapore, Hong Kong, Sydney, Japan, Kuala Lumpur, Dubai, Mumbai, Frankfurt, Silicon Valley and Virginia. So you can host in the location that's most suitable for your business and its needs.

Many organizations host in multiple regions, and this is another reason why inter-VPC communications may be required. Multi-region hosting is good for resilience and also means that you can have more of a perceived presence in your key markets. There may be other reasons too. A U.S.-based company considering expansion into China will probably want to host its new China-facing services within the country itself, while probably leaving existing U.S.-facing systems in situ.

Not all company or corporate structures are straightforward, especially after a period of mergers, acquisitions or expansion. There may be two branches of the company, each with their own Alibaba Cloud account that contains one or more VPCs. Or maybe a company with its own Alibaba Cloud account and VPC wants to allow limited access to their resources by a trusted third-party, such as a reseller, strategic partner or auditor. Again, this presents a need for communications between VPCs.

BEYOND VPN

While a VPN might be considered the obvious choice to support communication between VPCs and with in-house kit, it's important to keep in mind the question of security and resilience. A VPN connection uses the Internet, which will be insufficiently secure for some types of operations or where regulations prohibit its use. In addition, Internet bandwidth is not always guaranteed, which can lead to problems such as latency issues in database connections.

That's where Alibaba Cloud's Express Connect comes in. As with other aspects of Alibaba Cloud's service, it's available to all customers via the web-based admin console.

Express Connect is available in two forms. For inter-VPC connections, within one hosting region or between two, Express Connect relies on Alibaba Cloud's own infrastructure rather than using the Internet. For a connection between a VPC and a location outside of Alibaba Cloud, a leased line is used. You can arrange the line through the independent carrier of your choice or work with one of the company's telecoms partners. At least two connection points are available at all Alibaba Cloud hosting locations.

Express Connect offers the facility, unique among public cloud providers, for fast, secure and dedicated links between servers in China and those elsewhere in the world. This is a compelling reason why a company looking to outsource IT operations to the cloud, and which has a presence in China or is considering one, might wish to strongly consider Alibaba Cloud as their cloud provider.

" run intranet-like services in the cloud...

...but with speed and latency figures at the same levels as if the servers were on the premises. "

SETTING UP EXPRESS CONNECT

If you have two VPCs in different regions and you want the VPCs to communicate with each other, you can use Express Connect to establish an intranet connection between them. Express Connect enables private network communication between VPCs in any region, avoiding unstable public networks and reducing the risk of data theft during transmission.

Setting up Express Connect is quick and easy, and can be performed from the admin console. Let's look at an example of what's required. There are three main steps involved.

Take the case of a company that currently has two VPCs as follows:

Configuration	VPC-A	VPC-B
VPC ID	vpc-12345678	vpc-87654321
Region	China North 2 (Beijing)	China East 1 (Hangzhou)
VPC CIDR Block	192.168.0.0/16	172.16.0.0/12
VSwitch CIDR Block	192.168.100.0/24	172.16.100.0/24

For this example we'll assume that VPC-A is in Beijing and VPC-B is in Hangzhou. In reality, the VPCs could be located in any Alibaba Cloud hosting location including Australia, Japan, Dubai, India, Germany, the U.S., China or Hong Kong.

For the first of the three steps we need to set up two virtual routers, or VRouters, one in each of our VPCs.

Region A Custom router:
172.16.0.0/12->RouterInterface1

VPC1 — VRouter1 — 192.168.00/16
RouterInterface1

ECS Instance1
192.168.0.100

Region B Custom router:
192.168.0.0/16->RouterInterface2

VPC2 — VRouter2 — 172.16.00/12
RouterInterface2

ECS Instance2
172.16.0.10

KEY ⟷ Interconnection between router interfaces
⟷ Intercommunication data flow
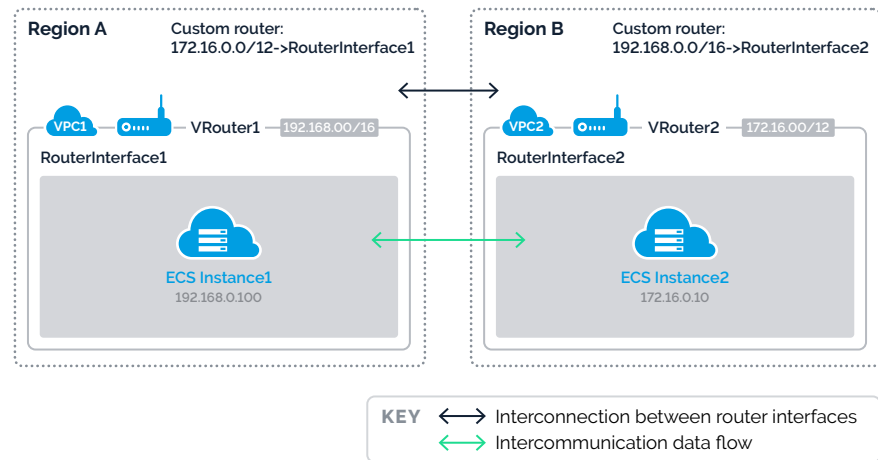
To start, we log into Alibaba Cloud, and specifically the Express Connect section. We then opt to create a new router interface as shown in the screenshot:

When setting up Express Connect there are two scenario options, namely VPC Interconnect and Physical Access. In this case we are connecting two VPCs across Alibaba Cloud's infrastructure without the need for a separate leased line, hence the choice of VPC Interconnect.

We then specify that we want to set up both sides of the connection, which are known as the initiator and receiver.

The communication link is bidirectional and there is no difference between the initiator and receiver. For a link between two VPCs on the same account, the process starts automatically when required. When the link is between VPCs on two separate accounts, you have to manually initiate a connection between the initiator router interface and the receiver router interface.

We specify the two regions involved, and the two VPC ID's. We also specify the size of the connection required. This needs to be decided at the point of purchase as it will obviously impact the price, and there is a Purchase Plan setting that allows the customer to choose between monthly and annual payment. It is recommended that new connections use a monthly plan so that the size of the connection can be adjusted at a later date if required.

Pricing is obviously an important factor, and the figures for Express Connect are straightforward. As at January 2018, A connection between two VPCs starts at around USD $170 per month, depending on the two locations being connected. This is for the "small.1" service level, which allows for maximum transmission of 1.25MB per second (that is 4.5GB per hour or 108GB per day).

There are currently eight service levels in total, with the most powerful one (known as "large.2") providing for an astonishing 256MB per second. That is 900GB per hour or 21.6TB per day.

As already mentioned, each end of the connection is designated either as the initiator or receiver. For charging purposes, only the data sent from the initiator is charged. The receiver does not pay again. Depending on which of the two Alibaba Cloud accounts will be responsible for making the payment on behalf of the organization, this may affect your choice in deciding which end is given which designation.

With the specification chosen and the purchase made, the second and third of the three steps involves configuring routes within each VPC. These are simple to achieve. Simply log into the console and, for each VPC, select the relevant region from the Router Interface List, choose the Route Configuration option and then choose Add Route Entry. You then need to specify the destination Classless Inter-Domain Routing (CIDR) block.

The connection is then activated and is available to use immediately, with an intranet-like communication channel now in operation between the two VPCs, even if their cloud hosting regions are tens of thousands of miles apart. The whole process can typically be set up in 15 minutes or so, and all from a web-based console.

THE PROCESS CAN BE SET UP IN 15 MINUTES - ALL FROM A WEB-BASED CONSOLE

One major consideration when joining VPCs, or indeed when joining a VPC to an on-premises data center, is the issue of Internet Protocol (IP) address conflicts. It clearly helps if the two VPCs were initially set up to use different ranges. If there are issues here, or if you have a device in a VPC that needs to use an address that is normally reserved, a ticket raised to Alibaba Cloud support services will normally get it sorted.

Using Express Connect to bridge the connection between VPCs, or between customer premises and a VPC, brings a number of benefits. Perhaps the most important is high-speed intercommunication. Because it's part of the Alibaba Cloud infrastructure, Express Connect can bridge different network environments so both sides can communicate directly through the intranet and bypass public networks. Furthermore, Express Connect offers features typically associated with intranet communication, such as low latency and high bandwidth, across long distances. So a hybrid network in which, say, your database server is in-house but the storage is in the cloud, will perform as if everything is still local. You can thus run intranet-like services in the cloud, but with speed and latency figures at the same levels as if the servers were on the premises.

Because everything runs within one infrastructure, this helps to ensure stability and reliability. There's a formal SLA for the Express Connect product, full details of which are on the Alibaba Cloud website. In essence, if uptime drops below 99.95 percent for any given month, you'll receive 10 percent of your fees back as a credit. Below 99 percent uptime, the credit figure rises to 25 percent.

Express Connect is not only easy to configure, it's also easy to reconfigure. This is important to consider when you're shopping around for connectivity services and providers. From the standard web-based control panel, complex physical network configurations can be undertaken with just a few clicks.

SUMMARY

While cloud is definitely here to stay, hybrid IT and on-premises servers aren't going to completely disappear anytime soon. It is therefore vital for any company's cloud migration plans to include the ability to communicate quickly and securely between existing in-house locations and cloud servers, and also between multiple cloud-based VPCs.

Express Connect from Alibaba Cloud provides that service worldwide, and its connectivity in Mainland China is unrivaled. Express Connect should be of particular interest to any organization which currently has operations in China or which might do so in the future.
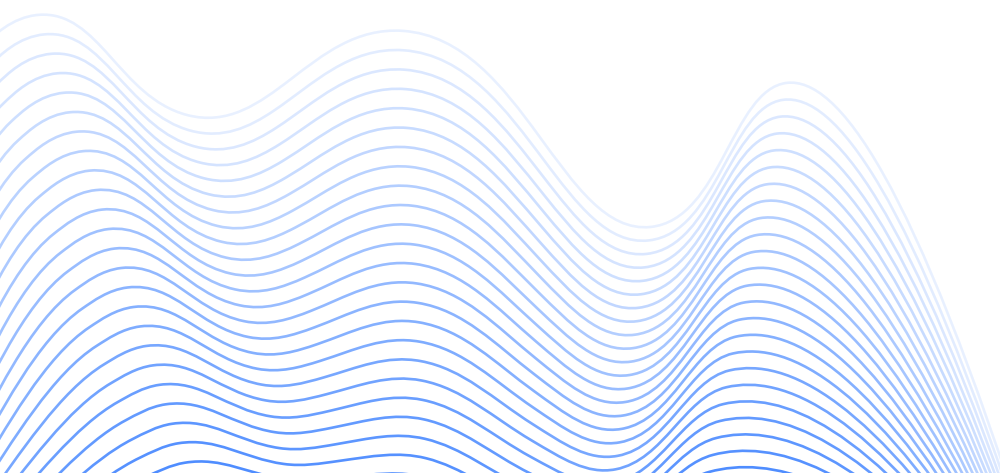
REFERENCES

1. The "Cloud Security 2017 Spotlight Report" published by Crowd Research Partners available at https://pages.cloudpassage.com/cloud-security-survey-2017.html

2. Docker and the Docker logo are trademarks or registered trademarks of Docker, Inc. in the United States and/or other countries. Docker, Inc. and other parties may also have trademark rights in other terms used herein.

ABOUT

Established in September 2009, Alibaba Cloud is the cloud computing arm of Alibaba Group and develops highly scalable platforms for cloud computing and data management.

It provides a comprehensive suite of cloud computing services available from www.alibabacloud.com to support participants of Alibaba Group's online and mobile commerce ecosystem, including sellers and other third-party customers and businesses.

Alibaba Cloud is a business within Alibaba Group which is listed on the New York Stock Exchange (NYSE) under the symbol BABA.

www.alibabacloud.com/contact-sales