white paper

dimension data

Private Cloud for Every Organization

Leveraging the community cloud

As more organizations today seek to gain benefit from the flexibility and scalability of cloud environments, many struggle with business and regulatory constraints that keep them from being good candidates for public or private cloud offerings. Perhaps they operate within a highly regulated space that takes public cloud off the table, but don't have the internal resources to set-up or administer suitable private cloud infrastructure. Or maybe they have specific industry requirements for performance that aren't readily available in the public cloud and would be expensive to build out for a single organization.

These might seem like hard-luck cases, but fortunately there is another option that could still put the cloud within the reach of these organizations. Called community cloud, this option makes it possible to set up a private cloud in a limited multi-tenant environment that is designed for similar organizations that have in common very specific technical and regulatory requirements. Typically administered by some sort of underlying industry organization or, in the case of government entities, some sort of overarching agency, these community clouds convey the benefits of the cloud while still giving organizations the power to meet needs that the open market can't cater to.

Defining 'Community'

For the purpose of this paper, a "community" is a group of companies or legal entities that share a common risk profile or may have the same funding source and could be part of the same legal entity. Examples include a group of community hospitals that are part of a larger non-profit health care provider; independent realtors that are part of a consortium to leverage advertising and other business services; or franchise holders for a retail chain.

TechTarget Custom Media

Community Cloud Use Cases

The 'community' in a community cloud can be made up of organizations with a range of relationships with one another, but at very least they'll probably share a common risk profile. They may be tightly coupled in other ways, for example, sharing the same funding source or even being part of the same entity. Some examples of communities that could benefit from a community cloud:

- A group of community hospitals that are part of a larger non-profit health care provider
- Independent realtors that are part of a consortium to leverage advertising and other business services
- Franchise holders for a retail chain
- A group of companies in a buyer's club that's already placing orders for goods and services as a group to leverage better pricing
- Holding company—the members of the holding company are loosely related but are part of one legal entity with typically centralized IT policies and processes
- Agencies of a county or city government
- Members of an association like federal credit unions

Whatever the community, they typically have specialized cloud needs that fall under three common use case scenarios.

The first commonality many communities share is data governance requirements. Government agencies—and sometimes contractors that handle sensitive government information—often must satisfy these requirements, making them excellent candidates for community clouds. Not only are they frequently required by law to keep all of their data within the country the agency resides in, but they typically have to provide for additional data security requirements that are difficult to achieve in a shared public cloud. For example, data may require at-rest encryption not only for the data store, but also the entire operating system with encryption keys maintained outside of the purview of the cloud provider's operational team. The most sensitive data also requires physical destruction of hard drives, as with the DOD's degaussing requirements. While public cloud providers may be able to address some of these requirements, fulfilling all government data security requirements on public cloud is nearly impossible. A single government entity could administer a community cloud for sub-agencies, departments or offices based on its most stringent data security requirements and support all data security requirements.

Another trait frequently shared by entities that could take advantage of community clouds are unique performance requirements. Certain industries might require hardware or compute power not typically supported in the average cloud environment.

For example, organizations in analytical-heavy industries that run high data volumes might need high-performance clustering not available in most public cloud infrastructure, which might be cost prohibitive to build out a single private cloud infrastructure to support. Similarly, some organizations could need close physical proximity to the infrastructure due to low-latency requirements for apps commonly used across the industry.

Instead of separate companies going out to purchase and maintain their own hardware, they might be able to band together through an underlying industry association to build out a community cloud. This affords them some of the benefits of scale that are typically associated with public cloud, while still meeting those technical performance requirements.

The third most common shared attribute among these potential community cloud members are special compliance concerns that may prohibit public cloud use. Highly regulated industries like healthcare and finance often cannot take advantage of public cloud due to security concerns around personally identifiable information (PII). While rare, mutli-

tenancy security concerns such as VLAN hopping and virtual machine (VM) escape vulnerabilities create just enough doubt to make public cloud deployment too risky. For example, the VENOM vulnerability impacts multiple hyper-visors and reveals the ability to execute code on another guest VM. If the cloud tenants all follow the same strict security adherence and industry guidelines, the risk is mitigated. An organization such as a financial holding company that owns loosely related sub-companies or an industry association may be able to serve as a community cloud provider so that separate entities run off of a cloud with other trusted entities. That way the cloud is maintained according to industry standards and is still at its root a less risky private cloud.

Steps for Setting Up a Community Cloud

Setting up a community cloud can be an extremely successful endeavor for the community members, but it'll require planning and preparation to pull off well. The following steps can help make certain that initial set-up goes smoothly.

1. **Ensure there's an underlying organization to administer the cloud.**
   This underlying entity could be a government agency, a holdings company with interests in the member organizations, or an industry association or non-profit. It could even be a consulting group that services a specific industry. This underlying organization is different than an MSP or other service provider that might do something similar while layering in a mark-up on the services. Regardless, there needs to be a trusted organization that will administer the cloud on behalf of all the other user organizations.

2. **Establish requirements of the group.**
   Before building out a community cloud on behalf of a number of different businesses or agencies, the leader in charge of the effort at the underlying organization will need to establish crystal clear requirements from members. This includes clarifying what type of capacity member organizations will need. It also means fully threshing out the common technical and compliance specifications that are banding everyone together in favor of the community cloud in the first place.

Communicate clearly what's being offered.
Finally, once the underlying organization establishes requirements and builds out its technical plan for the cloud, it must communicate back to member organizations a clear plan of what will be offered through the community cloud.

Everything needs to be laid out in advance because in order to make it scale there can be no special customization for member organizations—so it is critical that members agree on what the standard configuration will be.

Best Practices for Administering a Community Cloud

Once the community cloud is established, it will be up to the underlying organization to administer the cloud so that it feels like a seamless IT environment to each member of the community. This will require adhering to some administrative best practices.

First among them is sorting out user account management. The underlying organization will have to establish roles for who is going to manage the user account structure for administration accounts and how that's going to be replicated to the architecture. It must be able to isolate users from a management, security and privacy perspective. Similarly, the organizer of the cloud must find a way to set up a secure network connection—there must be some way to arrange for securely passing network organizations to the community cloud.

Also critical is the issue of billing. There must be a mechanism to bill all of the member organizations separately for their specific usage

of cloud compute. And, finally, the organizer must consider support needs. It will need to figure out if it has the in-house capability to handle tech support or if the member organizations will need so much support that a trusted third party will have to be brought in to offer additional tech support.

Conclusion

Whatever the trusted entity is that will be organizing the formation of a community cloud, chances are it will need help with the technical details. Many organizations are adept enough to set up a private cloud but may still find it difficult to sustain 24/7 operational support. Services such as capacity management, release upgrades, user account maintenance and usage tracking for billing all represent major challenges. If an organization is not a managed service provider whose core mission is to provide IT assets, the ongoing support and upkeep of the service offering can suffer. Fortunately, Dimension Data offers the technical resources to simplify the creation and ongoing management of a community cloud. Dimension Data offers an OpEx model to provide a pay-as-you-go service, and brings together all of the technical components necessary with the help of an orchestration engine called Cloud Control. This platform provides vendor-level account management with sub-administration accounts to segregate member entities within the cloud. In addition, Dimension Data offers an enablement program to ensure the community partner is equipped with the necessary sales and technical training to support its community.

dimension data

MIDDLE EAST & AFRICA

ALGERIA · ANGOLA
BOTSWANA · CONGO · BURUNDI
DEMOCRATIC REPUBLIC OF THE CONGO
GABON · GHANA · KENYA
MALAWI · MAURITIUS · MOROCCO
MOZAMBIQUE · NAMIBIA · NIGERIA
RWANDA · SAUDI ARABIA
SOUTH AFRICA
TANZANIA · UGANDA
UNITED ARAB EMIRATES · ZAMBIA

ASIA

CHINA · HONG KONG
INDIA · INDONESIA · JAPAN
KOREA · MALAYSIA
NEW ZEALAND · PHILIPPINES
SINGAPORE · TAIWAN
THAILAND · VIETNAM

AUSTRALIA

AUSTRALIAN CAPITAL TERRITORY
NEW SOUTH WALES · QUEENSLAND
SOUTH AUSTRALIA · VICTORIA
WESTERN AUSTRALIA

EUROPE

BELGIUM · CZECH REPUBLIC
FRANCE · GERMANY
ITALY · LUXEMBOURG
NETHERLANDS · SPAIN
SWITZERLAND · UNITED KINGDOM

AMERICAS

BRAZIL · CANADA · CHILE
MEXICO · UNITED STATES

For contact details in your region please visit www.dimensiondata.com/globalpresence

www.dimensiondata.com