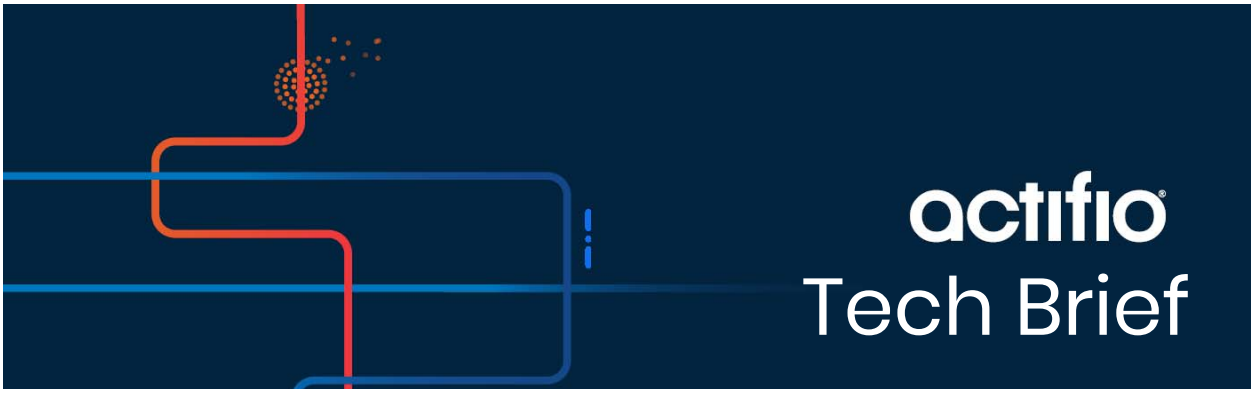

Multi-Tenancy with Actifio

Executive Summary

This paper gives a detailed overview of how Actifio solutions should be deployed in a multi-tenant environment. Multi-tenancy is a reference to the mode of operation and a deployment model of software and hardware where multiple independent instances of one or multiple applications operate in a shared environment. In this deployment model, the tenants are logically isolated, but physically integrated. Multi-tenancy is a core deployment model for a cloud service provider or managed service provider to reduce resource cost by increasing infrastructure utilization and to make it easier to chargeback customers. Multi-tenancy in enterprise datacenters is also becoming a deployment model of choice as private and hybrid clouds take hold with internal business divisions identified as tenants that share the common IT infrastructure.

Purpose of this document

This document is intended to provide details of how Actifio appliances and related management tools can be deployed in a multi-tenant model with the following characteristics:

- Logical separation of data traffic flow from customer datacenter to a CSP datacenter
- Logical and physical separation of data storage
- Tenant UI separation and access models
- Tenant specific resource usage reporting
- Developing portals and extensions using Foresight APIs in a multi-tenant deployment model

Intended audience

- Cloud Provider IT infrastructure executives who make technology decisions
- Cloud operations administrators who integrate and automate vendor platforms with services infrastructure

Prerequisites

A basic familiarity with Actifio products is assumed. For more information on that, please consult Actifio documentation. It is beneficial but not required to have an overall understanding of how Actifio is deployed in a single tenant model.

Overview

Multi-tenancy encompasses multiple aspects, from management and reporting through data separation at storage and networking. An Actifio environment is managed using Actifio Global Manager (AGM), and that where management separation is defined, using organizations that have users and resources associated with them. The data virtualization and handling is done on Actifio appliances, managed by AGM.

The simplest approach to multi-tenancy would be to use separate appliances for each tenant, managed by one AGM, thereby achieving data separation in combination with streamlined management. This enables a service provider, for example, to manage data across all customers, while providing the strictest and clearest operational separation. This is the most common model used today, especially leveraging the flexibility that the Actifio Sky virtual appliance provides to match appliance size with a customer's data capacity.

In some situations, especially with tenants that have small amounts of data, it is not economical to dedicate an appliance to each tenant. Actifio appliances can support multi-tenancy within an appliance, using organizations and separation of physical resource pools.

Tenant logical resource isolation using organizations

Actifio Organizations are the main means for logically separating multiple tenants within an Actifio environment. Organizations associate users with objects or physical resources to control who can view and act on what.

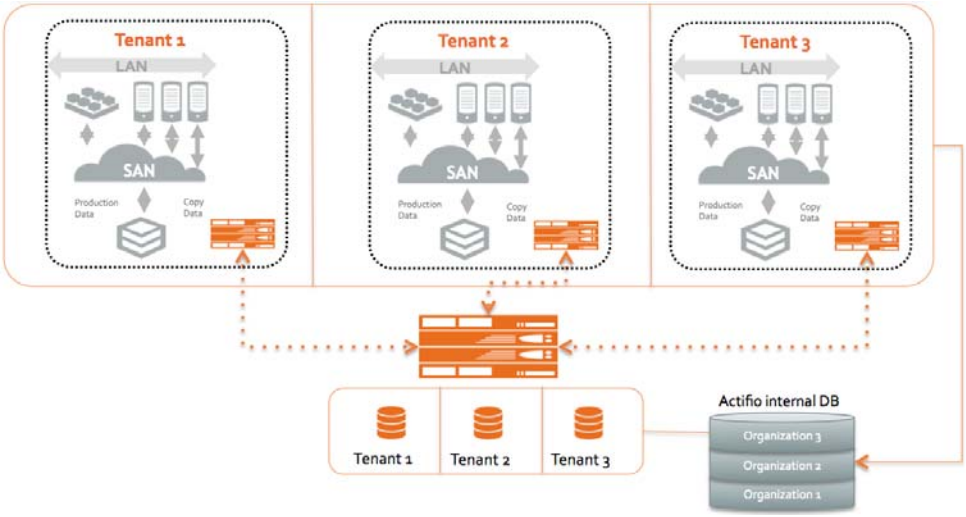

Figure 1 Resource Logical Separation in an Organization

Entities that can be logically separated includes storage pools, hosts and applications (with their images/backups), SLA templates, and resource profiles.

Organizations can be created in a hierarchy, so that a tenant sub organization's resources can also be isolated. For instance, PepsiCo could have Frito-Lay hosts placed under a separate organization to simplify their chargeback model.

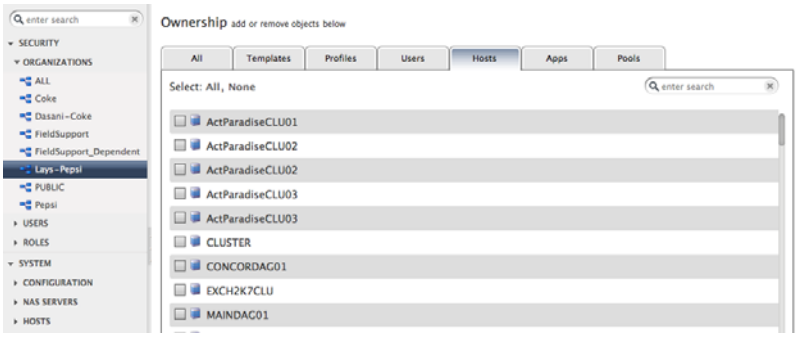

Figure 2 A Sub-organization within a Tenant

Tenant resource access separation with role-based access control

For a service provider, or a private enterprise operating in a service provider model, it is important to create separate users with clear separation of control responsibilities for different tenants. Actifio's Role-Based Access Control (RBAC) mechanism provides fine-grained access privileges for specific parts of the system using roles and their associated rights. There are a variety of predefined roles and it is easy to define new roles with appropriate rights. For example, a storage administrator can have access privilege for creating and maintaining a set of storage pools, and at the same time she might only have viewing privileges for hosts. Even within the context of one tenant, the administrator of all the tenant's resources can restrict who can access which service features in the product. For example, an administrator responsible for creating and maintaining SLA policies need not have access to storage and hosts. Figure 3 outlines how a tenant's user co-exists with other tenants in the same environment.

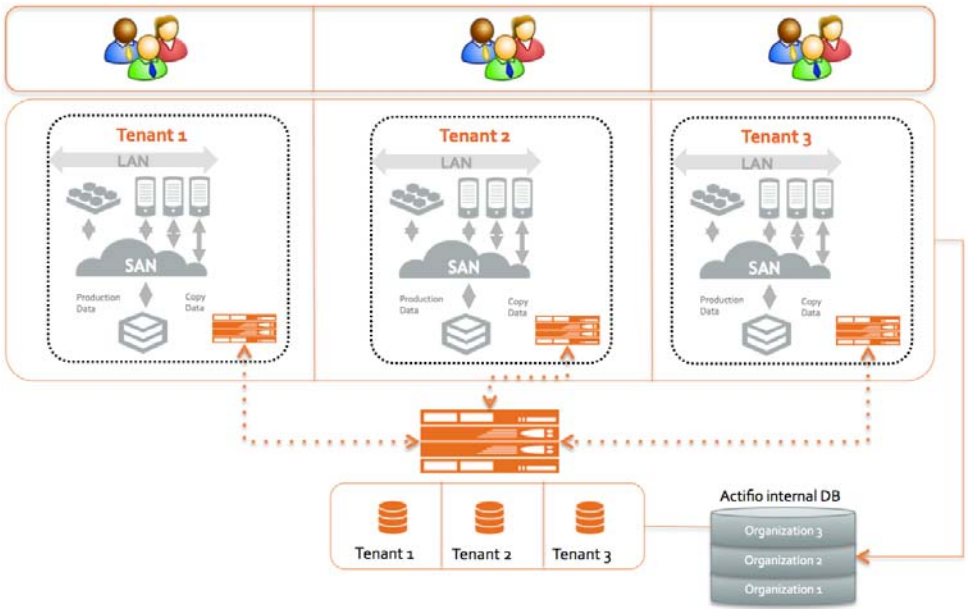

Figure 3 Role-Based Access Control per Tenant

Actifio provides several levels of rights for dealing with resources within the system. The most basic level is viewing a resource, whereas the most complete level is managing it (creating, modifying, deleting). Some resources have more levels in between - for example a user might be given a right to view SLA templates and assign them to applications, but not the right to manage the templates. Figure 4 provides an example of some of these access rights.

To summarize, a user is limited to performing specific actions (based on their role and associated rights) on specific resources (limited by the organizations to which they belong). A user cannot see resources that are not within their organizations.

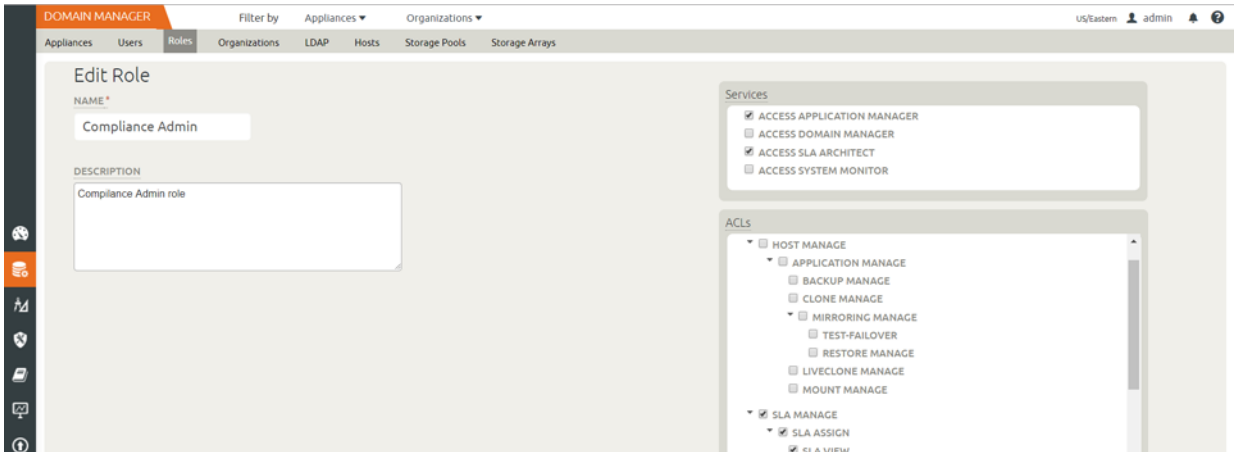

Figure 4 Roles and Rights within a Tenant Role

Data storage tenant isolation

In a multi-tenant environment, customers of Cloud Service Providers might require data storage isolation. An Actifio appliance can completely isolate tenant storage in different snapshot pools that use storage from separate RAID groups or even different storage arrays. These snapshot pools can have different performance characteristics with unrelated disk groups. They may even be from different vendors.

Similarly, multiple OnVault pools can be created, within one cloud account or object storage array or on different accounts and arrays. These pools provide data storage isolation among tenants for long-term retention on object storage. Note that OnVault can be configured with multiple appliances writing into the same object storage bucket, and when importing images from that bucket into a new Actifio appliance all images in that bucket will be available to the importing user. Different buckets should be used to ensure data separation. In addition, organization information is not written to OnVault so organizational separation must be re-established after importing images, if needed.

When storing data in dedup pools, storage separation requires using separate appliances, since each appliance manages one global dedup pool where all the data managed by that appliance is deduplicated.

Figure 5 illustrates a deployment model of a Cloud Service Provider with a private cloud tenant co-located within the cloud provider facility and another tenant located outside of the CSP's facility.

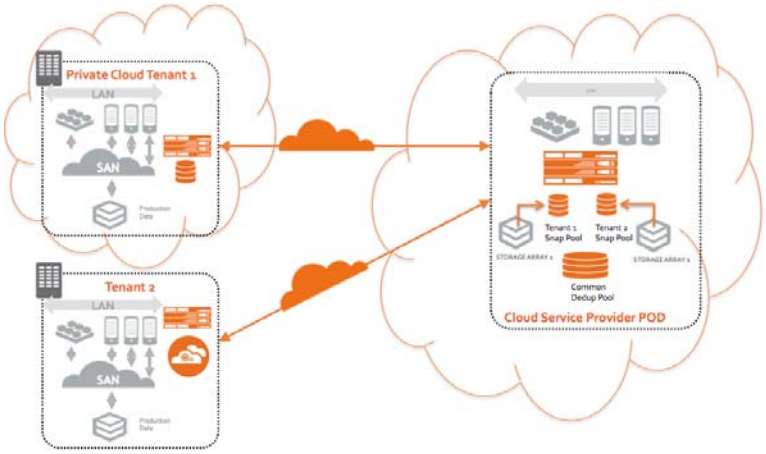

Figure 5 Data Storage Isolation with Actifio VDP

When replicating data from an on-prem (or colo) tenant appliance into a service provider appliance using Dedup-Async or StreamSnap replication, the service provider can control the target snapshot pool based on the source appliance, to ensure continued data storage separation.

Isolating data traffic per tenant

In addition to providing for data storage separation, service provider clouds require the ability to deal with data traffic isolation in the form of VLAN tags or the ability to deal with overlapping IP ranges when different customers replicate data over to CSP clouds. Actifio appliances provide basic support for network traffic separation with different network interfaces. From a Cloud Service Provider point of view, network separation is important between network edges up until where data touches the Actifio appliance replication interfaces. Data traffic between a customer datacenter and the CSP datacenter could be handled as mixed traffic or isolated using dedicated Virtual Private Networks. These VPN networks could also handle tagged VLAN traffic if customer networks are on a trusted domain. In a mixed data traffic environment such as over the Internet, IPSec VPNs can be configured to encrypt different tenants' data to avoid security problems. These mixed traffic environments can be terminated at the CSP using appropriate firewalls and routers. The following diagrams present different approaches on how Actifio appliances can be configured with various network isolation mechanisms.

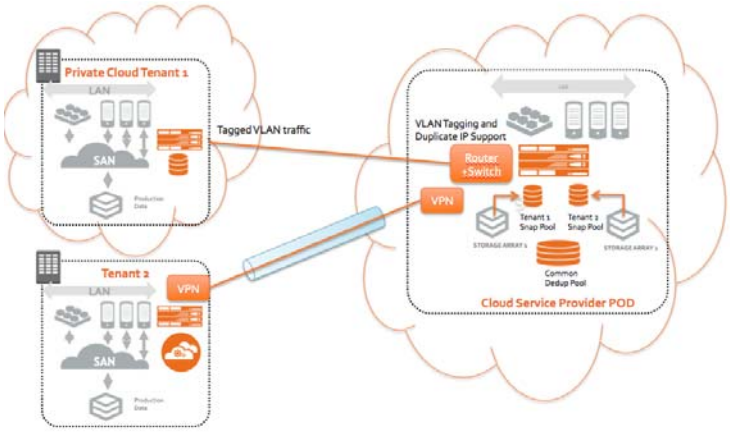

Figure 6 Data Traffic Isolation for Tenants

Tenant specific reporting for chargeback

A critical component of Cloud Service Provider business model relies on proper chargeback to customers. Actifio Report Manager provides the ability to measure resource utilization across multiple customer deployments and Actifio appliances, leveraging organization information. The following reports are typically used in such an environment for tenant chargeback and other reporting:

- SLA reports per tenant
- MDL consumption report that gives the total amount of Managed Data License consumed per tenant
- Storage Pool and other resource consumption details such as VDisks per tenant's application
- Job success and failures per tenant
- Historical data on storage pool consumption
- Replication reports, including bandwidth consumption per appliance/Tenant

Note: *As of standalone Report Manager 9.0.5, not all organizational information is synchronized between AGM and the appliances for reporting purposes. If Report Manager is a component of AGM (runs in the same VM), it will use the organization membership information from AGM instead of that provided by the appliances. In this case, the report will have correct data.*

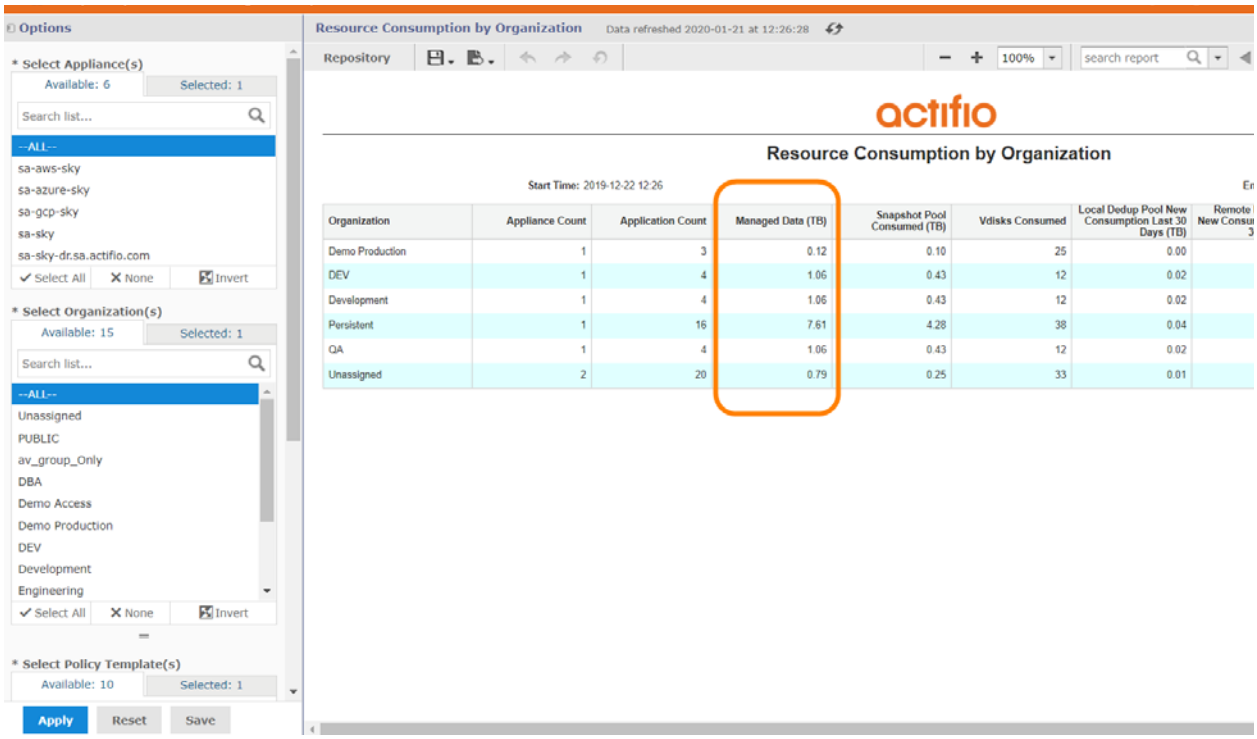

Figure 7 MDL Consumption by Organization/Tenant

Writing multi-tenant cloud portals using Actifio Foresight APIs

The Actifio Foresight platform allows third party portal development to customize and manage an Actifio environment at service providers. Capabilities to manage storage pools, resource profiles, SLA definition and management, data capture, manage and use lifecycle, replication pairing of appliances, users and their roles and rights are all exposed using a fine grained API which can be used from any RESTful capable portal development system at the service provider. Some service providers might want to even extend the Actifio organization capabilities in their portal system to better manage tenants as part of their IaaS infrastructure provisioning.

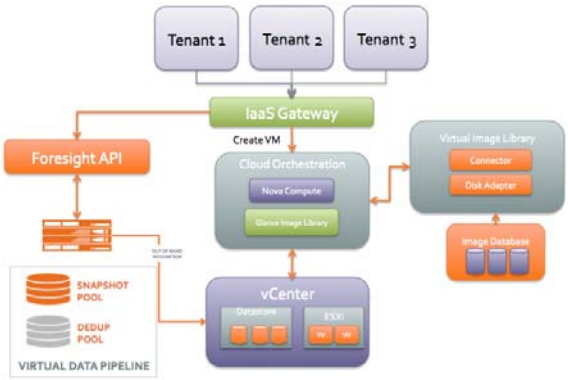

Figure 8 Integrating Foresight Into a Multi-tenant Portal

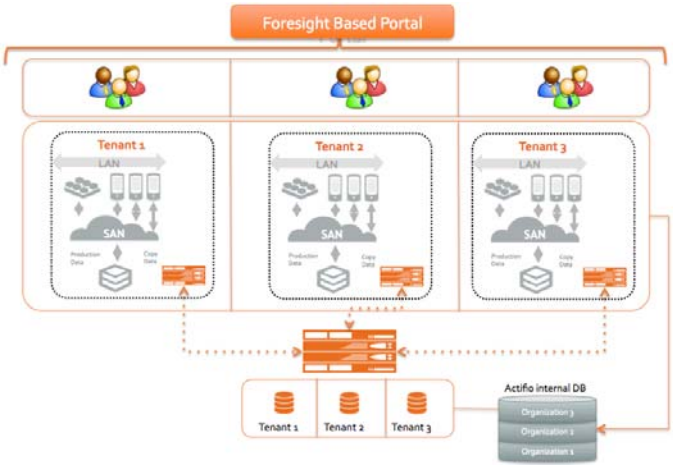

Figure 9 Managing Multiple Tenants using the Foresight Platform

Summary

Today's Cloud Service Provider (CSP) deployments are architecturally demanding. CSPs on the one hand want to deploy flexible solutions that satisfy many of their customers needs but on the other hand need an easier chargeback mechanism. Actifio offers a flexible architecture depending on the requirements of the CSPs as well as their end customers. Actifio enables multiple levels of tenant isolation and separation; isolation at the storage layer; separation of access per tenancy; filtering of reports per tenant for chargeback; and has the capabilities to adapt to different customer network demands.

CSPs need to go through a decision process to evaluate the best deployment architecture depending on their customer data size, their use cases, network capabilities as well as CSP datacenter and operations capabilities. Actifio Solution Architects can help in that process, sharing Actifio's experience and best practices.