EMC’s UNIFIED STORAGE AND MULTITENANCY
Technology Concepts and Business Considerations

Abstract
This white paper discusses how EMC’s leading-edge technologies are used to implement secure multitenancy in a shared infrastructure.

October 2010
# Table of Contents

**Executive summary** ........................................................................................................... 4

**Introduction** ........................................................................................................................ 4
  Audience ..................................................................................................................................... 4

**What is multitenancy?** ........................................................................................................... 5
  Why is it important? ..................................................................................................................... 5
  Four pillars of secure multitenancy .......................................................................................... 5

**Types of cloud service models** ............................................................................................ 6
  Software as a Service (SaaS) ..................................................................................................... 6
  Platform as a Service (PaaS) ..................................................................................................... 6
  Infrastructure as a Service (IaaS) .............................................................................................. 7

**Secure multitenancy pillars at the storage layer** ................................................................... 8
  Pillar #1 – Secure Separation ................................................................................................... 8
    Separation of data at rest ......................................................................................................... 8
    Address space separation ......................................................................................................... 8
    Authentication and name service separation .......................................................................... 9
    Separation of data access ....................................................................................................... 9
  Pillar #2 – Service Assurance ................................................................................................ 11
    Dedication of runtime resources .......................................................................................... 11
    QoS control ............................................................................................................................ 11
  Pillar #3 – Availability ............................................................................................................ 12
    High availability ..................................................................................................................... 12
    Local and remote data protection .......................................................................................... 12
  Pillar #4 – Management ......................................................................................................... 12
    Single end-to-end management for the service provider ....................................................... 13
    Delegated management for tenants ....................................................................................... 13

**Conclusion** ............................................................................................................................ 13

**References** ............................................................................................................................ 13
Executive summary

An increasing number of organizations are implementing private clouds to take advantage of the many benefits provided by private cloud’s shared infrastructure. A core capability of any shared infrastructure is multitenancy. Secure multitenancy allows various users to securely share IT infrastructure. Secure multitenancy can be divided into four “pillars”: Secure Separation, Service Assurance, Availability, and Management.

EMC’s unified product offerings meet or exceed the requirements for secure multitenancy. Scalable architectures and flexible provisioning strategies ensure that data remains securely separated. Unisphere™ Quality of Service Manager and dedicated hardware resources work together to meet service level objectives (SLOs). Fully redundant architectures and other protection features provide some of the most highly available systems in the industry. Finally, products like Unisphere and Ionix™ Unified Infrastructure Manager (UIM) simplify management at different management levels, including the storage level.

Because of these capabilities, EMC continues to lead the midrange marketplace’s implementation of private cloud.

Introduction

This white paper discusses different types of private clouds, and how EMC provides leading-edge hardware and software that allow you to configure your own private cloud. It includes these sections:

- **What is multitenancy?** — This term is defined and the four pillars of multitenancy are discussed.
- **Types of cloud service models**
- **Secure multitenancy pillars at the storage layer** — We take a deeper look into each of the four pillars of secure multitenancy and how they relate to the storage layer. We review the requirements of each pillar and describe how EMC addresses these requirements.

Audience

This white paper is intended for EMC customers, partners, and employees who are interested in leveraging shared storage infrastructure to support offering IT as a Service. It is assumed that the reader is familiar with EMC’s unified storage offerings, primarily Celerra® and CLARiiON® storage systems.
What is multitenancy?

To understand multitenancy, two key terms must be defined: tenant and landlord. Generally speaking, a tenant is anyone who utilizes resources provided by someone else – a landlord. In the storage world, tenants are a population of users or applications. The landlord provides and maintains the technology assets that the tenants use. Common examples of landlords include IT departments and external service providers.

Multiple tenants sharing the same resources provided by a single landlord is called multitenancy. Two common examples of multitenancy are multiple virtual machines sharing the same server hardware through the use of VMware or Hyper-V, and multiple user populations or applications using the same storage platform.

Why is it important?

Multitenancy is not a new concept; however, it has become a topic of much discussion due to the rise in popularity of deploying cloud (or IT as a Service) environments. Shared infrastructure is a core component of any cloud strategy. Properly implementing the principles of multitenancy can significantly streamline the journey to the private cloud.

Four pillars of secure multitenancy

Security is of primary concern in any shared-service (or cloud) deployment. Secure multitenancy means that no tenant can access another tenant’s data. To ensure this fundamental tenet is achieved, all deployments should adhere to the following four pillars of secure multitenancy:

- Secure Separation
- Service Assurance
- Availability
- Management

The first pillar, Secure Separation, enables data path separation across various tenants in a multitenant environment. Without proper separation, there is no multitenancy.

The second pillar, Service Assurance, plays an important role in providing an SLO that can be unique to each tenant. Consistent and reliable service levels are integral to secure multitenancy. With secure multitenancy, consistent SLOs can be delivered across the compute, network, and storage layers.

Availability is the third pillar. High availability ensures a resilient architecture that provides fault tolerance and redundancy. Availability is the one of the most important design requirements since it is critical to have application and data availability for business continuity. This is especially true when IT infrastructure is shared by multiple tenants as the impact of any outage is magnified.
The fourth, and final, pillar is **Management**. One goal of secure multitenancy is to simplify management across all the various products and provide the functionality to provision, monitor, and troubleshoot so that the user can easily manage their environments from end to end. This includes provisions that allow a landlord to manage basic infrastructure while delegating management responsibilities to tenants for the resources that they interact with day to day. Simplified management reduces time managing and translates into reduced total cost of ownership (TCO).

### Types of cloud service models

There are numerous service models that can be implemented when building out a cloud deployment. The following are three examples as defined by the National Institute of Standards and Technology (NIST). The major difference between each model is how deep in the stack the tenant separation lies.

**Software as a Service (SaaS)**

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (for example, web-based email). The consumer does not manage or control the underlying cloud infrastructure including the network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Figure 1 displays the stack as defined by the SaaS model.

![Software as a Service (SaaS) stack](image)

**Platform as a Service (PaaS)**

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including the network, servers, operating systems, or storage, but has control over the deployed applications and possibly application-
hosting environment configurations. Figure 2 displays the stack as defined for a PaaS model.

![Figure 2. Platform as a Service (PaaS) stack](image)

**Infrastructure as a Service (IaaS)**

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications, and possibly has limited control of select networking components (for example, host firewalls). Figure 3 displays the stack as defined for an IaaS model.

![Figure 3. Infrastructure as a Service (IaaS) stack](image)

As demonstrated by these figures, IaaS requires the separation of tenants at more levels than SaaS or PaaS, all the way down the stack to the storage level.
Secure multitenancy pillars at the storage layer

Each of the four pillars can be broken down into specific requirements for the storage layer. The following sections detail what those requirements are, and how EMC's unified offerings fulfill them.

Pillar #1 – Secure Separation

As stated earlier, the fundamental principle that makes multitenancy secure is that no tenant can access another's data. The Secure Separation pillar is essential to reaching this goal. At the storage layer, this pillar can be divided into four basic requirements: separation of data at rest, address space separation, authentication and name service separation, and separation of data access.

Separation of data at rest

Today, most deployments treat physical storage as a shared infrastructure. However, in some cases, it is necessary to ensure that a specific dataset does not share spindles with any other dataset. This separation could be required between tenants or even within a single tenant's dataset. Business reasons for this could be competitive companies using the same shared service, and governance/regulatory requirements. Both Symmetrix® and CLARiiON provide flexible RAID and volume configurations that allow spindles to be dedicated to LUNs or storage pools. Celerra allows the creation of tenant specific storage pools that can be used to dedicate specified spindles to particular tenants.

Address space separation

In an ideal implementation of secure multitenancy, each tenant is completely unaware of any and all other tenants. However, without proper mitigation there is the potential for address space overlap. Fibre Channel World Wide Names (WWN) and iSCSI device names are globally unique. There is no possibility of contention in either area. IP addresses, however, are not globally unique and may conflict. To remedy this situation, the landlord can assign infrastructure-wide IP addresses within a service offering. Each Celerra X-Blade or CLARiiON storage processor (SP) supports one IP address space. However, an X-Blade can support multiple logical IP interfaces and both SPs and X-Blades support VLAN tagging. VLAN tagging allows multiple networks to access resources without the risk of traversing address spaces. In the event of an IP address conflict, the server log file logs any duplicate address warnings. IP addressing conflicts can be addressed in higher layers of the stack. This is most easily accomplished at the compute layer. Figure 4 displays a graphical representation of how VMware’s vSphere can be used to separate each tenant's address space.
Authentication and name service separation

A tenant’s environment dictates the methods it uses to authenticate before accessing their data. CLARiiON and Celerra storage systems provide support for several different protocols. Each Celerra X-Blade can participate in one UNIX “name services” domain UID/GID scope and one iSCSI iSNS domain at a time. Therefore, tenants that share the same UNIX “name services” domain, or iSNS domain, may share an X-Blade. If more domains are required, Celerra systems can scale to a maximum of eight X-Blades¹ providing support for up to eight domains. Each CLARiiON can participate in a single iSCSI iSNS domain. CIFS servers can be instanced on a Celerra X-Blade providing support for many simultaneous Windows domains. This allows tenants from different Windows domains to share an X-Blade and maintain authentication domain separation.

Separation of data access

Separation of data access ensures that one tenant cannot see or access any other tenant’s data. The way this is accomplished depends on the data access protocol in use. Figure 5 displays the access protocols, and their respective protocol stack, that can be used to access data resident on a unified system.

¹ Maximum limit varies by Celerra model.
Figure 5. Protocol stack

CIFS
The pillar Secure Separation of data access begins at the bottom of the CIFS stack on the IP network with the use of Virtual Local Area Networks (VLANs) to separate individual tenants. The VLAN tagging model can then be extended into the unified system by VLAN tagging the individual IP interfaces so they understand the tags being used, and honor them. IP packet reflection guarantees that any traffic sent from the storage system in response to a client request will go out over the same physical connection, and VLAN, on which the request was received. The Virtual Data Mover is a logical configuration container that wraps around a CIFS file sharing instance. Above the Virtual Data Mover resides the CIFS server. CIFS shares are built upon the CIFS servers. At the top of the stack is a Windows feature named Access Based Enumeration (ABE). ABE shows a user only the files that he/she has permission to access, thus extending the separation all the way to end users if desired. Throughout the CIFS stack Secure Separation is maintained at each layer.

NFS
The NFS stack is very similar to the CIFS stack. All the same separation measures are in place until the Virtual Data Mover layer. There is no concept of a Virtual Data Mover when using NFS. NFS exports are the next layer in the NFS stack and these can be associated with specific VLANs. NFS export hiding tightly controls which users access the NFS exports. NFS export hiding enhances standard NFS server behavior by preventing users from seeing NFS exports that they do not have access-level permission for. To each tenant, it now looks as if they each have their own individual NFS server.
iSCSI

Much like both CIFS and NFS, the iSCSI stack begins by separating the physical IP network into VLANs and tagging the IP interfaces accordingly. Access then flows through an iSCSI portal, to a target device, where it is ultimately addressed to a LUN. LUN masking is a feature for block-based protocols that ensures that LUNs are only viewed and accessed by those SAN clients with the appropriate permissions. At the top of the stack the data itself is protected thorough the use of EMC PowerPath® Encryption software.

Fibre Channel over Ethernet/Fibre Channel

The lower layers of the Fibre Channel stack looks quite different because it is not an IP-based protocol. FC zoning controls which FC/Fibre Channel over Ethernet (FCoE) interfaces can communicate with each other within the fabric. Virtual Storage Area Networks can be used to further sub-divide individual zones without the need for physical separation. From the target layer on, the higher layers of the FC/FCoE stack are identical to those in the iSCSI stack.

Pillar #2 – Service Assurance

Now that the Secure Separation pillar of each tenant’s data and path to that data has been achieved, the next priority is predictable and reliable access that meets the tenant’s SLO. Furthermore, in a service-provider chargeback environment, it may be important that tenants do not get more performance than they paid for simply because there is no contention for shared storage resources. The pillar of Service Assurance ensures that SLOs are met at appropriate levels through the dedication of runtime resources and quality-of-service (QoS) control.

Dedication of runtime resources

Celerra’s X-Blades each have dedicated CPUs, memory, front-end, and back-end networks. An X-Blade may be dedicated to a single tenant or shared between several. To further ensure the dedication of runtime resources, X-Blades can be clustered into active/standby groupings. From a hardware perspective, dedicating pools, spindles, and network ports to a specific tenant or application can further ensure adherence to SLOs.

QoS control

EMC has several software tools available that organize the dedication of runtime resources. At the storage layer, the most powerful of these is Unisphere Quality of Service Manager (UQM). This software allows CLARiiON resources to be managed based on service levels. UQM utilizes policies to set performance goals for high-priority applications, set limits on lower-priority applications, and schedule policies to run on pre-defined time-tables. These policies direct the management of any or all of the following performance aspects: response time, bandwidth, and throughput. UQM allows the landlord to control these policies through a simple user interface. This control is completely invisible to the tenant and can ensure that the activity of one tenant does not impact that of another.
Pillar #3 – Availability

The pillar of Availability goes hand in hand with Service Assurance. While Service Assurance directs resources at the tenant level, Availability secures resources at the landlord level. Availability ensures that resources are available for all tenants utilizing the landlord’s infrastructure by meeting the requirements of high availability and local and remote data protection.

High availability

High availability (HA) systems are the foundation upon which any enterprise-class multitenancy environment is built. EMC’s unified storage offerings are among the most reliable in the industry, offering five 9s availability (99.999 percent uptime). HA systems are designed to be fully redundant with no single point of failure. Additional availability improving features in EMC’s unified products include:

- Dual-ported drives
- Redundant FC loops
- Battery-backed mirrored write cache
- Dual SPs
- Asymmetrical Logical Unit Access (ALUA)
- Dual paths to storage
- N+M X-Blade failover clustering
- Network link aggregation
- Fail-Safe Network devices

Local and remote data protection

It is important to ensure that data is protected for the entirety of its lifecycle. Local replication technologies, such as snapshots and clones, allow users to roll back to recent points in time in the event of corruption or accidental deletion. Local replication technologies include SnapSure™ for Celerra and SnapView™ for CLARiiON. NDMP backup to deeply efficient storage platforms, such as Data Domain®, can be used for restoration of data from a point further back in time. Remote replication is a key to the protection user data from site failures. RecoverPoint is EMC’s enabling software for remote replication between EMC's unified storage systems. To ease the management of replication and ensure consistency between replicas, users are encouraged to utilize Replication Manager. For more information on any of the products referenced in this section, please visit Powerlink®.

Pillar #4 – Management

The fourth and final pillar is Management. This pillar ties the other pillars into a simple administrator experience that improves each tenant’s interaction, while
simplifying the management of both tenants and resources for the landlord. The core requirements of the Management pillar are single end-to-end management for the service provider and the ability to delegate day-to-day management to tenants.

Single end-to-end management for the service provider

With FLARE® release 30 and DART release 6.0, EMC introduced Unisphere, a unified element management interface for NAS, SAN, replication, and more. Unisphere offers a single pane of glass through which the landlord can manage all aspects of the storage layer. Those users who need to manage the entire stack (compute, network, and storage), should consider Ionix Unified Infrastructure Manager (UIM). These two products mark a paradigm shift in the way infrastructure is managed.

Delegated management for tenants

With landlords managing more resources and tenants, it is advantageous to delegate appropriate management tasks to individual tenants. Tenants can manage their CIFS domain for CIFS services on Celerra using native Windows management tools such as Microsoft Management Console (MMC) and Group Policy Objects (GPOs).

Conclusion

Through the use of secure multitenancy, cloud deployments can successfully realize a shared infrastructure, a core component of any cloud deployment. However there are several key areas of technology that must be in place for secure multitenancy to be truly “secure.” These areas are secure tenant data separation, service level assurance, high availability, and simple management. All of these are available from EMC’s unified storage offerings and software portfolios.

References

For more information, consult the following white papers on EMC.com and Powerlink:

- **EMC CLARiiON SnapView Clones — A Detailed Review**
- **CLARiiON SnapView Snapshots and Snap Sessions Knowledgebook — A Detailed Review**
- **EMC Replication Manager and EMC RecoverPoint — Applied Technology**
- **Introducing EMC Unisphere: A Common Midrange Element Manager — A Detailed Review**
- **Introduction to EMC Celerra Unified Storage — A Detailed Review**
- **Introduction to the EMC CLARiiON CX4 Series Featuring UltraFlex Technology — Applied Technology**