Maximizing Multi-tenancy with Citrix NetScaler

Learn why NetScaler is the most flexible and effective application delivery solution for building high-density, multi-tenant data centers and cloud services.
Over the last few years, organizations have increasingly been shifting their data centers to a cloud-based model. This transition has been built upon virtualization, automation and orchestration of IT resources—mainly server, storage and switching infrastructure. The goal is to increase agility and reduce the costs of deploying and managing resources to support business applications.

Introduction
There are other concerns when it comes to supporting applications. In its report, “Cloud Service Strategies: North American Enterprise Survey, January 15, 2014,” Infonetics Research found that 79 percent of respondents want to improve application performance, 78 percent want to respond more quickly to business needs, 77 percent want to speed up application deployment and increase scalability, and 73 percent expect to reduce costs with cloud services.

As the transition to cloud-based data centers marches on, it is becoming apparent that organizations need to keep going after they virtualize their server, storage and switching infrastructure. To maximize device consolidation and increase flexibility and agility in deploying resources, other components instrumental to the security, performance and availability of the organization’s computing services need to take part in the transformation.

This white paper explains how the Citrix® NetScaler® application delivery controller (ADC) provides unmatched support for building high-density, cloud-based data centers by offering infrastructure teams multiple, powerful options for architecting a multi-tenant solution for application performance management. With NetScaler SDX™ in particular, IT teams can take advantage of multi-tenancy capabilities, including:

- Implementing multiple hard-walled ADC instances on a single physical platform.
- Sub-dividing any individual ADC instance into multiple admin partitions, with complete management isolation and soft-walled separation of underlying system resources.
- Treating a single physical platform as a “pool” of instances, admin partitions and system resources that can be reallocated as needed to meet changing business conditions.
- Leveraging a metering and bursting capability to dynamically share idle bandwidth/capacity across ADC instances.

These capabilities result in an unsurpassed degree of flexibility that ensures a best-fit alignment for the broadest set of multi-tenant requirements and use cases for enterprises and cloud service providers alike. NetScaler enables the adoption of optimal configurations for management or resource isolation and maximizes the consolidation that can be achieved.
Multi-tenancy and the shift to cloud-based data centers
In addition to streamlining operations and delivering a more flexible and adaptable computing environment, the transformation to cloud-based data centers delivers a significantly consolidated infrastructure footprint and a corresponding reduction in data center TCO. The key to the TCO benefit is the shift from dedicated to shared infrastructure enabled by virtualization and other related technologies. This shift allows multiple different applications (or separate instances of the same application) to be served by the same physical compute, storage and networking resources in a way that makes it appear as if they have dedicated resources. Put another way, the key to success is all about multi-tenancy.

Multi-tenancy is clearly a powerful, even transformative, capability. Maximizing returns on data center transformation, however, depends upon realizing and accounting for two key factors in the multi-tenancy architecture.

The first factor to consider is that not all tenants are created equal. Most data centers are complex environments designed to meet the needs of numerous constituents, be they user groups, business units or, in the case of service providers, customers. Consequently, most organizations have a broad spectrum of use cases to accommodate, each with its own set of requirements and priorities. This situation points to the need for solutions that provide multiple options for achieving multi-tenancy. Instead of being confined to a single approach, architects and customers need to weigh tradeoffs—for example, between tenant density and the extent of isolation—as they select, implement and configure the best-fit options for each constituent and scenario that they need to support.

The second factor to consider is that although some multi-tenancy is a good thing, consistent and pervasive multi-tenancy is necessary for a complete solution. In particular, embracing virtualization technologies that enable multi-tenant server, storage and switching infrastructure is only a starting point. If other data center components fail to provide multi-tenant capability, the result will be unrealized potential for consolidation and increased complexity as IT is left to “map” between and maintain a patchwork of multi-tenant and non-multi-tenant solutions. Given the crucial role that they play in ensuring the availability, performance and security of key computing services, ADCs should be viewed as the top candidates for the second wave of virtualization and multi-tenancy that organizations pursue.

NetScaler support for multi-tenant data centers and cloud services
NetScaler is an all-in-one ADC. Deployed in thousands of networks around the globe, NetScaler optimizes, secures and controls the delivery of all enterprise and cloud services while ensuring a high-performance experience for all, including those using mobile clients. Complementing its many strengths, NetScaler includes an unmatched set of multi-tenancy features and options that make it the ideal application delivery solution for enterprises and service providers that are architecting, building and operating high-density cloud data centers.
Core multi-tenancy options with NetScaler
The core NetScaler building blocks for multi-tenant designs are devices, instances and admin partitions.

Devices
Although inconsistent with consolidation objectives, there may be situations where specific tenants need separate physical ADCs. Super-critical, revenue-generating applications and semi-independent enclaves with ultra-rigorous security requirements are two examples. The overriding motivation is to remove any potential for operations in support of less-important tenants to degrade, compromise or otherwise interfere with the delivery services being provided to high-profile tenants. The general approach in these cases is to serve the high-profile tenants with their own individual devices, high-availability pairs or NetScaler clusters. Separate, shared ADCs deployed in parallel would be used to meet the needs of any other tenants. Applicable platform options that support this scenario include NetScaler MPX™ purpose-built hardware appliances and NetScaler VPX™ virtual appliances running on general-purpose server hardware.

Instances
The second NetScaler multi-tenancy building block is the instance. With instances, administrators can configure a single physical appliance to operate as multiple independent NetScaler ADCs. Think of server virtualization technology where multiple virtual machines are able to run side-by-side on a single physical server. NetScaler instances work essentially the same way.

The primary platform option for deploying instances is NetScaler SDX. Designed from the outset as a multi-tenant solution, NetScaler SDX enables up to 80 independent instances to operate on a single, purpose-built hardware platform. The degree of independence, or isolation, provided with this approach is extensive, minimizing the opportunity for the operation of one instance to interfere with that of any other instances running on the same platform. In addition to allocating its own, dedicated system-level resources—including CPU cores, memory, bandwidth and SSL capacity—to each instance, complete network and administrative isolation is maintained down to the level of separate IP stacks, routing tables, configuration files and event logs.
Admin partitions

Another NetScaler option for supporting multi-tenant operations is the admin partition. This capability provides a second way to provision multiple logical ADCs using a single physical hardware platform. Compared to instances, however, there are two key differences. First, the degree of isolation provided is not as extensive. For example, partitions running within the same instance are constrained to a single version of the NetScaler firmware. In addition, there is no way to dedicate CPU cores or SSL processing capacity to an individual partition. Instead, admins can only set rate and maximum usage limits—for example, for connections, bandwidth and memory—as a way to moderate usage of the underlying system resources. In comparison, however, relatively robust isolation is still maintained both for networking and administration, resulting in support for overlapping IPs and completely separate configuration and event management.

The second major difference between instances and admin partitions is the level at which they are applied. Specifically, instances are a device-level feature, whereas admin partitions are an instance-level feature. Think of it as another layer of subdivision, where instances are used to subdivide devices and admin partitions are used to subdivide instances. The net result is an exponential increase in the number of logical ADCs that can be provisioned within a single physical device. In addition, feature parity is maintained. Each admin partition supports the full spectrum of service delivery capabilities, from server load balancing, global server load balancing and lower-level traffic management and optimization features to AAA and application firewallsing functionality.
To demonstrate how admin partitions might be employed, consider the scenario where different business units within an organization have their own set of applications that require ADC services. To address everyone’s needs with a minimum footprint, a single NetScaler SDX is first subdivided into multiple instances, with each business unit receiving its own dedicated instance. Next, each instance is subdivided into multiple admin partitions, with one for each application needed by the corresponding business unit.

Because it is an instance-level feature, the admin partition capability is applicable to all NetScaler platforms (i.e., MPX, VPX and SDX). It is with multi-instance platforms such as NetScaler SDX, however, that IT teams can realize the full flexibility (and consolidation potential) of NetScaler support for multi-tenant environments.

**Additional multi-tenancy features of NetScaler SDX**

Two multi-tenancy features specific to NetScaler SDX are role-based administration (RBA) for the NetScaler service virtual machine (SVM) and an innovative metering and bursting capability.

**RBA at the SVM level**

Root SVM admins have read-write privileges across an entire NetScaler SDX platform, including root privileges for all instances and admin partitions. NetScaler SDX SVM RBA capabilities make it possible to set up second-tier admins with a sphere of influence limited to a designated subset of instances. This feature is particularly useful for enterprises where a NetScaler SDX platform is being “shared” by two or more groups, each of which is looking to operate multiple ADC instances. In this scenario, the administrators for each group can only see and/or manipulate the configurations, events and logs applicable to the instances owned by that group.

**Metering and bursting**

When instances are initially created, they are allocated a portion of system-level resources, such as CPU cores, memory, bandwidth and SSL processing capacity. Administrators have the ability to manually adjust these allocations to account for changing business conditions that result in changes in demand. They also have the option of using an innovative metering and bursting capability to dynamically share idle bandwidth capacity across instances. With this feature, administrators set a guaranteed minimum bandwidth, burstable maximum bandwidth and priority parameter for each instance. On a priority basis, highly utilized instances can tap into excess bandwidth capacity up to their burst limit. Organizations implementing a chargeback scheme can use an associated metering function to keep track of the bandwidth used by each instance.
Factors to consider when selecting an approach

There are several factors to consider when determining which multi-tenancy and platform option(s) are the best fit for a given scenario, including the extent of isolation, tenant density and performance requirements that need to be supported.

The many dimensions and degrees of isolation

Different multi-tenancy options deliver different degrees of separation, or isolation, in terms of which resources are shared and to what extent. Several aspects of isolation to consider when making a selection include:

- Fault isolation. Does a process failure for one tenant impact the availability of services for other tenants?
- Performance isolation. Does one tenant’s consumption of system resources have the potential to impact the performance of other tenants, or is there hard-walled separation, for example, for CPU, memory and SSL processing capacity?
- Data isolation. If and how one tenant’s data is kept separate from another’s is especially relevant for organizations that must comply with various privacy and security regulations, such as the Payment Card Industry Data Security Standard (PCI DSS).
- Functional isolation. Can different tenants run different firmware versions? What if one tenant needs to run the latest version of application firewalling to obtain access to new functionality? Is it possible to accomplish that without forcing all other tenants to upgrade to the latest software version as well?
- Administrative isolation. To what extent can management functions—especially configuration, monitoring, reporting and logging—be separated (and delegated) for different tenants?

Having physically separate ADC appliances for different tenants clearly provides the greatest degree of isolation. However, this approach also incurs the greatest cost and, therefore, will typically be used sparingly—for example, only for an organization’s most critical applications and security- or performance-sensitive business units. Otherwise, the decision comes down to instances, admin partitions, or—since they are not mutually exclusive—some combination of the two. Figure 5 provides a quick reference guide for the isolation-oriented differences between instances and admin partitions.
Other factors

Although the degree of isolation provided is an appropriate starting point, there are a handful of other factors that also deserve consideration when selecting the combination of multi-tenancy and platform options for a given scenario:

- Tenant density. Although a single NetScaler SDX appliance can support up to 80 instances, there are some use cases where even that number may not be sufficient. For example, for cloud service providers offering server load balancing as a service—or any other subset of application delivery capabilities as a service—the ability to offer compelling price points may depend upon supporting hundreds of customers per hardware platform. To address such a requirement, admin partitions need to be brought into the mix to divide instances.

- Hardware type/capabilities. Purpose-built NetScaler MPX and NetScaler SDX platforms eliminate hardware selection challenges, offer greater multi-tenant functionality and deliver proven performance up to 120 Gbps. In comparison, using general-purpose servers introduces the flexibility of being able to leverage existing, available hardware resources.

- IT and corporate objectives. Mandates for consolidation and data center automation tip the scales away from numerous per-tenant systems in favor of both SDX multi-tenant platforms and admin partitions. For businesses with an extremely low tolerance for risk, however, the scales will be tipped in exactly the opposite direction.
Sample scenarios
The power and flexibility of NetScaler multi-tenant capabilities enable IT departments to meet whatever combinations of requirements they encounter across their organization, both currently and as conditions change in the future. Potential implementation scenarios include:

• Migrating from Cisco ACE. For organizations looking to migrate subsequent to EOL of ACE, NetScaler admin partitions provide a functionally equivalent option to the widely used “context” capability of the Cisco product. NetScaler is the only ADC to integrate with Nexus switches using Cisco RISE technology so that it can act as a module on the Nexus.
• Multi-tenancy with multi-tier applications. Using NetScaler SDX, IT can allocate its own instance to each business-critical application. Application owners can then set up admin partitions to provide logical separation between the tiers of their applications—for example, creating separate admin partitions for the web frontend, application and database servers.
• Enterprises with a mix of critical and non-critical applications. An appropriate approach for this scenario is to allocate one or more dedicated instances for each critical application, along with a separate, shared instance (or two) for the non-critical applications. The shared instance(s) would subsequently be subdivided, with each non-critical application receiving its own admin partition.
• Basic and advanced SMBs. A redundant pair of either NetScaler MPX hardware appliances or NetScaler VPX virtual appliances, configured with multiple admin partitions, are typically sufficient to meet the needs of most small and mid-size businesses (SMBs). Alternately, SMBs that are subject to regulatory compliance, have substantial SSL processing requirements or need to support numerous tenants with varying degrees of sensitivity/criticality will find NetScaler SDX a better fit due to the greater degree of performance and administrative isolation it delivers.
• PCI DSS (or other) compliance. Having RBA at the SVM level enables IT to deploy a single NetScaler SDX appliance where one subset of the provisioned instances is subject to security and privacy mandates, but all other instances are not. Details for a PCI DSS validated configuration supporting this specific scenario can be obtained here: https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/pci-dss-success-achieving-compliance-and-increasing-web-application-availability.pdf

Cloud services for application delivery. By leveraging the full set of multi-tenant capabilities available with NetScaler SDX, cloud service providers can devise and deploy an entire portfolio of application delivery capabilities as a service. Options range from inexpensive, high-density server load balancing services (where each customer gets its own admin partition) to full-featured, virtually private ADCs (where each customer gets its own instances), or even dedicated, fully private ADCs (where each customer gets its own NetScaler VPX, MPX or SDX appliances).
No matter which options are selected for a given scenario, the same code base across NetScaler MPX, VPX and SDX ensures consistent functionality and the flexibility to easily accommodate changes as an organization’s needs evolve.

**Conclusion**

The transformation to cloud-based data centers and full realization of related benefits hinge on the ability to execute a shift from dedicated to shared infrastructure. Moreover, this shift needs to occur not only for servers, storage and networks, but also for other major components of the data center, including ADCs. Featuring a powerful set of multi-tenancy capabilities, the market-leading Citrix NetScaler ADC is uniquely positioned to be a key part of the transformation to cloud data centers. With the NetScaler SDX platform, which is purpose-built for multi-tenancy, enterprises and cloud service providers obtain unmatched flexibility that ensures a best-fit alignment for their many use cases. Benefits of using NetScaler SDX include increased adaptability and reduced data center TCO, as a single application delivery solution can be used to fully meet all of an organization’s requirements for application services in multi-tenant environments while minimizing the ADC footprint.