Optimizing Government Data Centers for Cloud adoption with Citrix NetScaler

Learn why NetScaler is the most flexible and effective application delivery solution for building software-centric, multi-tenant data centers and cloud services.

Over the last few years, Government agencies have increasingly been shifting their data centers to a software-defined, 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 mission critical 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 agencies 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 agency's computing services need to take part in the transformation.

A recent Federal mandate – the Data Center Optimization Initiative (DCOI) is aimed at making Data Centers more efficient, partic`ularly in the area of energy consumption. DCOI encourages shared services models, such as cloud computing using FedRAMP certified clouds.

State and Local Governments have similarly spent the last few years consolidating data centers and are now looking at how to best optimize them and adopt Cloud for further efficiencies.

What is an ADC?

This white paper explains how the Citrix® NetScaler® application delivery controller (ADC) provides unmatched support for building high-density, software-defined, cloud-based data centers by offering infrastructure teams 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.
- Treating a single physical platform as a "pool" of instances, 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 Government agencies and cloud shared 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 equally. Most data centers are complex environments designed to meet the needs of numerous constituents, be they user groups, agency departments or service providers' customers. Consequently, most agencies have a broad spectrum of use cases to accommodate, each with its own set of requirements and priorities. The ability to support multi-tenant use cases is key factor in datacenter design. Architects need flexibility when creating instances that are not rigidly bound by the architecture of the hardware supporting each tenant.

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 an ADC plays 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 agencies 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 and instances.

Devices

Although inconsistent with consolidation objectives, there may be situations where specific tenants need separate physical ADCs. Super-critical 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 and high-availability pairs. Separate, shared ADCs deployed in parallel would be used to meet the needs of any other tenants.

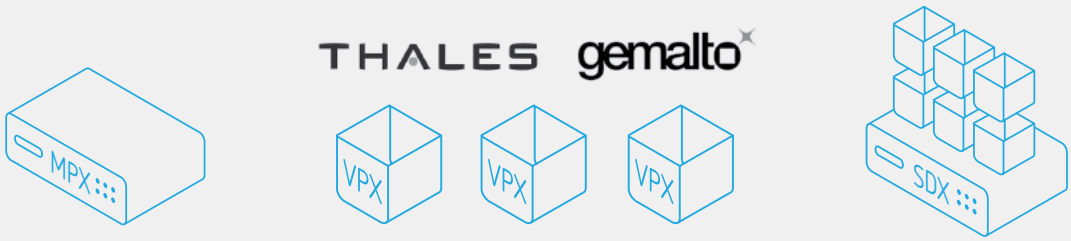
FIPS 140-2 Level 1 imposes limited security requirements. Hardware components must be production grade without any obvious security flaws

FIPS 140-2 Level 2 includes requirements for physical "tamper proof" components and role-based authentication

Applicable platform options that support this scenario include NetScaler MPX™ FIPS purpose-built single instance hardware appliances and NetScaler VPX™ virtual appliances running on general-purpose server hardware.

- NetScaler MPX FIPS edition appliances contain an on-board FIPS 140-2 Level 2 Certified Hardware Security Module (HSM). This allows for the utmost security and performance for the most mission critical applications.
- NetScaler VPX are a virtual edition of the same NetScaler appliance running on general purpose server hardware. Our integration with FIPS 140-2 Level 1 certified Hardware Security Modules from both Thales and SafeNet allow any virtual environment to meet FIPS level security requirements.

Figure 1. Device choices – dedicated NetScaler MPX FIPS HA pair for Tenant 1, NetScaler VPXs cluster for Tenant 3 and NetScaler SDX FIPS serving Tenants 3-N



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 FIPS. Designed from the outset as a multi-tenant solution, NetScaler SDX FIPS enables up to 25 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.

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.

Figure 2: NetScaler SDX FIPS edition—delivering secure SSL isolation across instances while providing FIPS 140-2 Level 2 validated security

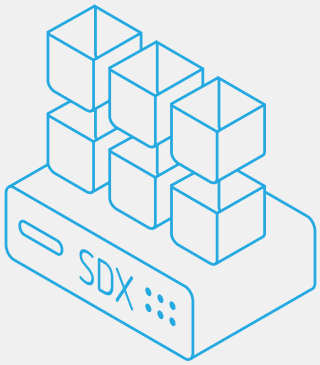
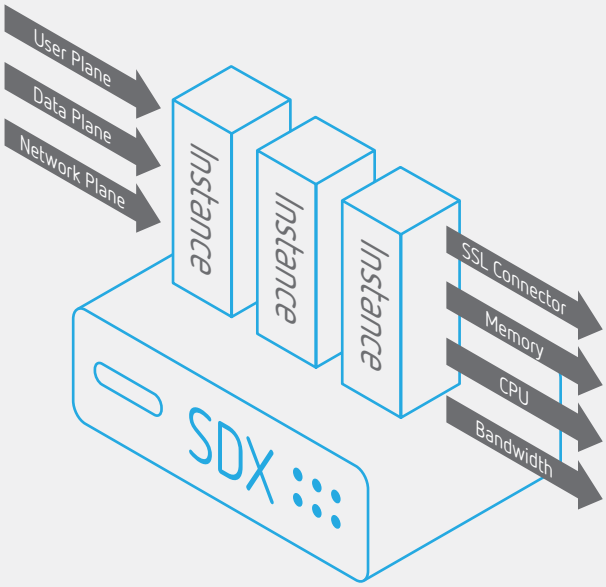


Figure 3: Metering and bursting options for NetScaler instances



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. Agencies 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 agencies that must comply with various privacy and security regulations that include the following:
  - Payment Card Industry Data Security Standard (PCI DSS)
  - National Institute of Standards and Technology (NIST)
  - Criminal Justice Information Services (CJIS)
  - Health Insurance Portability and Accountability Act (HIPAA)

- 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?

- FIPS-compliant SSL Key isolation. How are SSL Certificates and keys stored? How are they accessed across multiple tenants? Do administrators have access to all SSL keys on the platform?

Having physically separate ADC appliances for different tenants clearly provides the greatest degree of isolation. However, this approach incurs the greatest upfront cost and on-going maintenance.

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:

- Hardware type/capabilities. Purpose-built NetScaler MPX FIPS and NetScaler SDX FIPS platforms eliminate hardware selection challenges, offer greater multi-tenant functionality and deliver proven performance up to 80 Gbps. In comparison, using general-purpose servers introduces the flexibility of being able to leverage existing, available hardware resources.

- IT and Government mandates. Mandates for consolidation and data center automation tip the scales away from numerous per-tenant systems in favor of SDX multi-tenant platforms. For businesses with an extremely low tolerance for risk, however, the scales will be tipped in exactly the opposite direction.

Key use cases

The power and flexibility of NetScaler multi-tenant capabilities enable IT departments to meet whatever combinations of requirements they encounter, both currently and as conditions change in the future. Potential implementation scenarios include:

- Simplify Operations and Maintenance. Maintenance downtimes are painful — especially for critical applications and services such as an agency's ERP, Lync, Exchange or other mission critical application. By isolating each critical application along with their associated delivery functions (HA, Encryption, App Firewall, Authentication, Optimization), agencies can eliminate the risk of downtime of one application impacting another. This model has helped immensely during maintenance windows requiring upgrades to comply with constantly evolving security mandates (SSL, TLS, etc).

- Cloud Migration. As applications move to the cloud, migrating their associated delivery functions (HA, Encryption, App Firewall, Authentication, Optimization) should be a key part of any cloud adoption strategy. Leveraging the power of a Software-first platform, NetScaler ADC can easily be migrated from on-prem data centers to public clouds, speeding the transition of critical applications and services to the cloud.

- Migrating from Cisco ACE. For agencies migrating due to the platform's EOL, NetScaler SDX provides 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. https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/seamlessly-integrate-application-intelligence-on-cisco-nexus-series-switches-with-citrix-netscaler.pdf

- Multi-tenancy for multiple environments. Using NetScaler SDX, IT can allocate an individual instance for each business-critical application environment. Development, Staging, Test and Production environments can each be allocated a separate NetScaler instance for complete isolation with zero downtime.

- Crossing multiple-networks. Agencies are moving rapidly to software-defined and virtual networks where physical separation of networks is becoming a thing of the past in certain environments. NetScaler SDX allows for deployment of instances across multiple networks and VLANs while providing true hardware isolation using SR-IOV. This would allow instances to be deployed in separate logical network segments and remain isolated.

- FIPS/CJIS/PCI 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 other instances may not be. 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 full-featured, virtually private ADCs (where each customer gets its own instances), to 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 FIPS platform, which is purpose-built for highly secure multi-tenancy, government agencies gain unmatched flexibility that ensures a best-fit alignment for several of their use cases.

Benefits of using NetScaler SDX FIPS 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 hardware footprint.

CITRIX®

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000
US Public Sector Sales | 301-280-0800

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309 United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054 United States