Use Cases

Two categorical use cases are presented in defining this system solution:

- Business Use Case, page 2-1
- Technology Use Cases, page 2-2

Business Use Case

The joint solution delivered by Cisco ACI and Citrix NetScaler technologies is ideal for enterprise deployments of Microsoft SharePoint Server 2013. The solution allows IT administrators to configure efficient and agile application services for enterprise collaboration. Whether SharePoint is deployed within a private enterprise cloud or from a cloud service provider, Cisco ACI and Citrix NetScaler create an application-driven solution that fosters data security, responsive performance, and high service levels.

Cisco ACI enables a scalable, efficient cloud infrastructure that is application-centric. ACI technology combines the benefits of Software-Defined Networking with centralized policy control, allowing data centers to automate, virtualize, and pool infrastructure and network resources and provision them based on application requirements. Cisco ACI supplies the critical link between business-based requirements for application services and the enterprise infrastructure that delivers them. As a result, data centers gain speed and flexibility when deploying applications as well as the ability to consolidate resources, secure data, and reduce costs.

Citrix NetScaler intelligently directs application traffic between the Cisco ACI fabric and the available infrastructure. It is the only Application Delivery Controller that fully integrates into Cisco’s unified ACI fabric. This integration reduces deployment complexity and aligns applications to infrastructure using automation, saving deployment time and increasing flexibility.

This joint solution enables enterprise IT organizations to simplify application-driven control of Layer 4 to Layer 7 network services. Cisco ACI is supported on Cisco Nexus 9000 series switches and is managed through a centralized policy controller, the Application Policy Infrastructure Controller (APIC). APIC automates network provisioning—including production-ready NetScaler configurations—based on application requirements and defined traffic management policies. APIC is a comprehensive and unified management framework that can orchestrate NetScaler instances based on APIC-configured service policies.
Enabling an Efficient, Secure, and Reliable Architecture

Much of the potential promise of enterprise cloud architectures stems from cost savings and efficiencies that are gained through consolidation. Sharing infrastructure and networking components can yield management efficiencies as well as savings in CAPEX and OPEX. At the same time, cloud architectures require strict separation between shared resources including servers, enterprise networks, and data streams. Because SharePoint application services enable collaboration between different end-user and business entities (including suppliers, customers, and line-of-business organizations), secure multi-tenancy is an underlying requirement to isolate traffic and protect data.

For networking components (such as Application Delivery Controllers), supporting multi-tenancy has historically involved the ability to carve a single device into multiple logical partitions. This approach allows different sets of policies to be implemented for each tenant or application without the need for many separate devices. However, on some ADC devices, this approach is inadequate because the degree of isolation is limited.

The NetScaler SDX appliance—because it supports multiple, fully isolated virtualized instances—overcomes the challenge of enabling consolidation while providing strict isolation. Since the NetScaler SDX supports ADC instances that run as separate virtual machines, it enables tenant segregation for consolidated SharePoint workloads. Clustering NetScaler instances, along with best practices for designing a highly available SharePoint deployment, facilitates the high service levels and protection needed for strategic SharePoint services.

Technology Use Cases

This system solution constructs a fully functional Microsoft SharePoint farm on a Cisco ACI fabric. NetScaler instances on the fabric direct SharePoint client requests to physical and virtualized infrastructure resources, forwarding traffic to infrastructure servers. While doing so, it applies Layer 4 through Layer 7 services.

In addition to redundant SharePoint servers in the farm, this enterprise-ready deployment relies on Microsoft SQL Server 2012 clustering and failover for high availability. To optimize performance and availability, traffic is load-balanced across multiple SharePoint and SQL servers. NetScaler and the ACI fabric provide enterprise-grade security and data protection for SharePoint and SQL client requests as well as general web traffic.

NetScaler Services

NetScaler instances in this system solution are specifically configured to perform these operations:

- Web traffic inspection, identifying destinations, ports, and protocols.
- Load balancing of web traffic using load-balancing virtual IPs (LB VIPs). NetScaler instances perform Layer 4 (TCP and UDP) through Layer 7 (FTP, HTTP, and HTTPS) traffic management and load balancing.
- SSL offloading using built-in NetScaler hardware acceleration. In this system solution, SSL offloading is performed for generic traffic as well as for SharePoint web traffic.
- Content (or Layer 7) switching for SharePoint web and Database traffic. Content switching provides fast packet switching based on application-specific information (such as a URL, a cookie, or an SSL session ID). In this deployment, content switching allows traffic to be directed to different
SharePoint or SQL servers based on application layer criteria. The packet is forwarded from a Content Switching (CS) VIP to an LB VIP and in this way load-balanced across SharePoint or SQL servers in the farm.

- Layer 7 application firewall for SharePoint web traffic. This is in addition to the ACI fabric’s firewall capabilities—ACI acts inherently as a network firewall since it allows only configured traffic to pass between fabric endpoints. (By default, communication between endpoints is denied. ACI policies define the TCP/UDP ports that are opened to allow communication between endpoints.) NetScaler devices provide complementary firewall capabilities at the application layer.

- Global server load balancing (GSLB). GSLB extends the concept of load balancing across the end-to-end enterprise, distributing client requests across multiple data centers based on proximity, load, or availability. In this way, the NetScaler instances improve response time and support disaster recovery for SharePoint services.

- The Cisco Application Policy Infrastructure Controller (APIC) provides an intuitive and easy configuration process, allowing NetScaler functions to be intelligently chained together (such as the combination of content switching, SSL offloading, and load balancing for SharePoint client requests). APIC uses the concept of a service graph to represent the sequence of traffic management functions. As shown in later configuration procedures, service graphs (and associated Layer 4 to Layer 7 parameters) for NetScaler functions can be defined in APIC using the graphical user interface (GUI) or Python-interpreted XML files.

- APIC also supplies comprehensive management visibility into the fabric and NetScaler operations. It supplies a centralized view of configuration parameters as well as the ability to manage and observe traffic, events, and performance.

An overview describing the integration of Cisco ACI and Citrix NetScaler technologies is available in the architecture guide, “Implementing Cisco Application Centric Infrastructure with Citrix NetScaler Application Delivery Controllers.”

### Optimizing Security, Performance, and Availability

This system solution documents how Citrix NetScaler instances integrate with the fabric to meet enterprise-level architectural goals, including:

- Securing SharePoint application delivery for multiple tenants
- Optimizing SharePoint performance
- Enabling high availability and failover for SharePoint services and associated databases

### Use Case—Securing SharePoint Traffic Delivery

SharePoint deployments control access to company and customer-sensitive data, so client requests on the fabric must be protected against data loss and compromise. This implementation of NetScaler provides critically important application security, network/infrastructure security, and identity and access management capabilities.

NetScaler provides robust multi-tenancy capabilities, running completely independent NetScaler instances with separate policies. Separate IP addressing simplifies deployment into the ACI fabric. NetScaler completely isolates traffic, helping to meet compliance requirements.
NetScaler enables application-layer protections, including a full-featured application firewall, data loss protection, and countermeasures for thwarting denial-of-service (DoS) and other Layer 7 attacks. Layer 7 application firewall (AppFW) capabilities examine bi-directional traffic, including SSL-encrypted packets, to safeguard against a range of security threats. At the application layer NetScaler can also perform HTTP protocol validation to protect against DoS attacks.

NetScaler also incorporates several network and infrastructure-oriented security capabilities, including SSL-based encryption, DNS security, and Layer 4 attack protection. To protect against Layer 4 DoS attacks, NetScaler controls the allocation of back-end resources until it establishes a legitimate client connection and a valid request has been received.

For SharePoint traffic, SSL offloading can be applied pervasively beyond HTTPS. A simple SSL offloading scheme decrypts SSL records in HTTPS and then forwards HTTP traffic in clear text to back-end web servers. To safeguard against HTTP compromise, an end-to-end SSL offloading approach applies SSL offloading to re-encrypt the clear text for communications with the back-end web servers. To facilitate fast SSL operations, NetScaler supports both 2048 and 4096 bit keys in hardware.

In addition to load balancing internal DNS servers, NetScaler can also be configured to operate as an authoritative DNS (ADNS) server to directly handle name and IP resolution requests. This capability can be implemented in conjunction with GSLB to balance load across multiple data centers that support SharePoint Server 2013.

Use Case—Optimizing Responsiveness and Performance

For SharePoint workloads, NetScaler instances are used to load balance both edge and content servers. Intelligent load balancing distributes user requests for content across multiple SharePoint servers in the farm. Load balancing can be used to manage user requests, prevent poor performance and outages, and ensure that users can access protected applications. Load balancing—within a single data center as well as GSLB across multiple data centers—means that SharePoint services are continuously accessible and responsive.

NetScaler compression, caching and load balancing features also help to conserve bandwidth. ACI defines network Quality of Service (QoS) service classes for traffic, permitting bandwidth allocation based on tenant requirements. Since NetScaler offloads CPU-intensive tasks such as SSL processing, caching, and compression from SharePoint servers, these servers can process greater load and scale more efficiently. NetScaler also acts as a SQL proxy, offloading connection management from the SQL servers, and performs Database optimizations. This conserves SQL server resources, which helps to improve performance and scalability.

Use Case—Enabling Resiliency and Failover

This system solution defines a highly available architecture for deploying SharePoint. It leverages the Cisco Intercloud DC ACI 1.0 Architecture (the Silver Cloud Consumer Model) and includes redundant SharePoint servers and AlwaysOn Availability Groups in Microsoft SQL Server 2012. (Refer to Microsoft Tech Note: “Failover Clustering and AlwaysOn Availability Groups: SQL Server”.) NetScaler DataStream technology performs intelligent monitoring of Microsoft SQL Server, detecting which AlwaysOn node is the master so that NetScaler load-balancing services direct traffic appropriately.

To support NetScaler failover, NetScaler instances are configured as an Active/Standby pair. All instance configuration changes are synced from the Primary HA node (Active instance) to the Secondary HA node (Standby instance). A health check or “heartbeat” monitors the status of the primary node. During a failover, the Standby instance takes over as Active.
NetScaler load balancing promotes high availability for on-demand SharePoint services. Within a single data center, if a SharePoint server in the farm or an SQL Server is unavailable, the NetScaler instance will direct application requests to the remaining servers. Across multiple enterprise data centers, NetScaler GSLB functionality can be configured to distribute SharePoint client requests across data centers. Various criteria for GSLB distribution can be used, such as least connection, static proximity, or dynamic proximity. If a link to a data center goes down, NetScaler can redirect traffic to an available data center.

This system solution includes configuration details deploying NetScalers in the ACI fabric to achieve a resilient SharePoint deployment. Later sections cover how to configure NetScaler instances from APIC to optimize application service levels and enable service failover.