Large-scale NAT

Guide for deploying and configuring NetScaler for large-scale NAT

CITRIX®

Table of Contents

Large-scale network address translation (NAT), or LSN, which is, also referred to as carrier-grade NAT (CGN), is a technology that has been implemented by several telecom companies and Internet service providers across the globe in order to extend the lifespan of IPv4 addresses before the world moves to IPv6. Unlike traditional NAT, which achieved the same purpose but on a limited scale, LSN is designed for very large networks typical in the telecom/service provider environment.

This guide explains how NetScaler can be deployed and configured to meet all these requirements. It presents use cases focused on telecom network operations. It describes the logging capabilities of NetScaler as well as typical logging infrastructure topology. Finally, the document provides all the configuration commands needed to implement the NetScaler features discussed.

What is large-scale NAT (LSN)/carrier-grade NAT (CGN)?

In most regions, the IPv4 address space has been totally exhausted. There are no more new IPv4 addresses that can be allocated to new entities or devices wanting to connect to Internet. Meanwhile, the number of devices coming online is increasing every day. With new technologies like the Internet of Things, the need for new IP addresses will grow exponentially in the future. That is why IPv6 has been created.

Transitioning all legacy IPv4 networks and endpoints to IPv6 will take time. During this phase, the limited set of existing IPv4 addresses must to be leveraged to enable connectivity across all these networks and endpoints. Hence, to allow a large number of users to connect using a limited set of IPv4 addresses, sharing of these IPv4 addresses by multiple users is necessary.

Telecom companies and service providers have developed the LSN technology to meet this requirement. LSN allows a single public IPv4 address to be shared by a large number of internal or private network subscribers. LSN has been discussed thoroughly in the below specifications.

- RFC 6888 (Common requirements for LSN)
- RFC 5382 (NAT behavioral requirements for TCP)
- RFC 5508 (NAT behavioral requirements for ICMP)
- RFC 4787 (NAT behavioral requirements for UDP)

NetScaler supports all the above specifications in addition to its existing features of optimization, security and availability.

NetScaler support for LSN

NetScaler is the most advanced application delivery controller (ADC) for datacenter and enterprise needs. It has innovated many industry-leading technologies and has provided unmatched performance over the years. Now, NetScaler has begun supporting LSN, which is a core technology for all telecom operators and service providers. With NetScaler TriScale technology for scaling up, out and in, customers enjoy great flexibility during infrastructure refreshes. Below are the details for NetScaler LSN support.

The NetScaler features supporting LSN are available on builds from 10.5-51.1017.e onwards. Customers seeking this feature set must license the NetScaler Enterprise or Platinum Edition. The LSN feature set is supported on all form factors of NetScaler, i..e., physical (MPX), virtual (VPX) and multi-tenant platform (SDX).

The LSN features can be used standalone as well as in conjunction with other NetScaler capabilities such as load balancing, audit logging, traffic domains, etc.

LSN deployment topology

Below is the generic LSN topology used by telecom operators and service providers. The topology consists of three main sections – subscribers, telco core network and Internet (see Figure 1). Subscriber traffic passes through the telco core network before it reaches the Internet. The responses from the Internet take the reverse path.

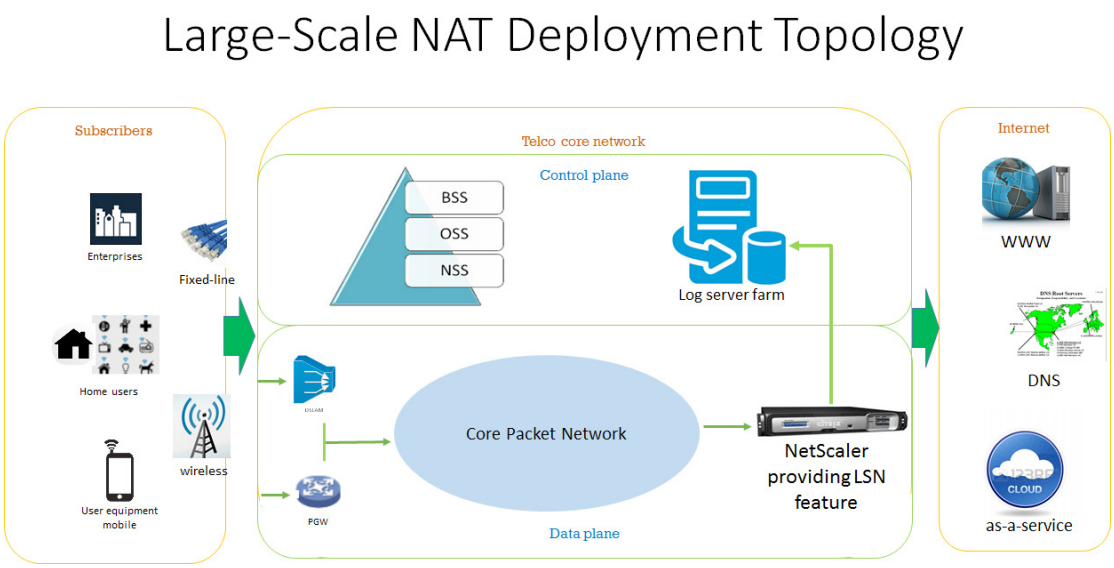

Figure 1. LSN deployment

The subscribers consist of all end users connecting to a telecom provider's network through wireless mode (e.g., RAN) as well as wired mode (e.g., broadband). The Internet section consists of all elements as we know – DNS infrastructure, web services, cloud-based services and content service providers/OTT-apps.

The key section in the above topology is the telco core network, which can be broadly divided into two sub-sections: control plane and data plane. The control plane consists of all the management functions needed to control subscriber traffic through the core network. These functions include billing, traffic management, logging, subscriber profile management, etc. The data plane consists of traffic forwarding functions such as routing devices, DSLAM, P-GW and services. This layer takes input from the control plane and decides how to handle the subscriber traffic.

NetScaler sits in the data plane and performs the LSN function.

Configure a simple LSN

The simple, straightforward use case for LSN is to perform NAT operation on subscriber traffic to allow subscribers to communicate with services on the Internet. Configuring NAT operation on NetScaler in an LSN deployment is an easy, three-step process. This section covers the complete Layer 2/3, high-availability and LSN configuration of NetScaler.

Note: Before proceeding to configuration, familiarize yourself with the following LSN terminology so that the rest of the document is easy to follow.

- **LSN client:** The LSN client entity refers to a set of subscribers on the private telecom network. LSN operation would be performed on subscriber traffic identified using the LSN client entity.
- **LSN pool:** The LSN pool entity defines the set of public NAT IP addresses available on NetScaler. NetScaler uses public IP addresses defined in the LSN pool to perform NAT operation on subscriber traffic.
- **NAT IP:** This represents the public IP on the LSN device. These public IPs are owned by the telecom service provider and are used to communicate with the rest of the Internet.
- **LSN group:** The LSN group entity represents the set of LSN client and LSN pool. Few parameters can be defined at the group level. The group-level parameters are discussed in the "Configure advanced LSN features" section.
- **LSN mapping:** LSN mapping represents the association of subscriber private IP+port info with public NAT IP+port info. The mapping can be dynamic or static.
- **LSN session:** An LSN session represents a subscriber's active mapping and all the associated parameters (e.g., timeout) applicable for this session. The destination tuple (IP, port) is part of the session information.
- **LSN traffic profile:** The LSN traffic profile is used to define various timeouts and limits for different protocols (TCP, UDP and ICMP). The traffic profile can be bound to the LSN group so the parameters define the traffic behavior for all subscribers in that group.
- **LSN application profile:** An LSN application profile defines the LSN mapping and LSN filtering controls for a given protocol and for a set of destination ports. The application profile also can be bound to a LSN group.

Figure 2 shows the relationship among all these configuration entities and the recommended sequence of configuration.

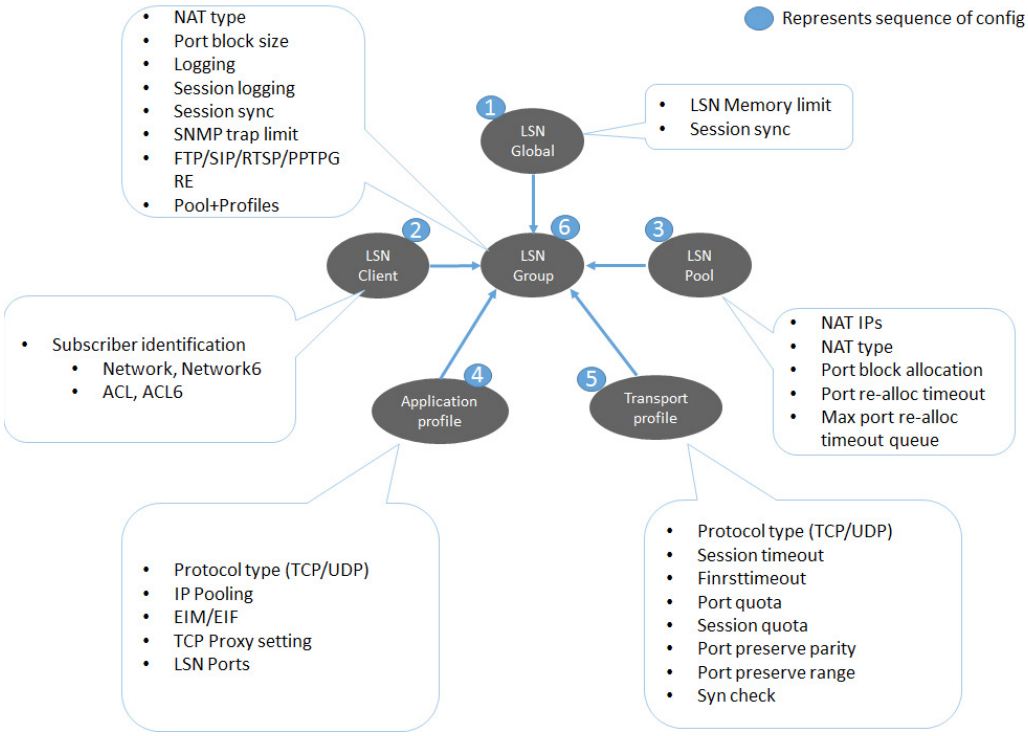

Figure 2. LSN config entities on NetScaler

Configure basic setup of NetScaler

Before looking into configuration of the NetScaler LSN feature, the basic setup of the appliance should be made ready. This basic setup includes configuration of management IP and VLANs, link-aggregation to upstream and downstream switching gear, and configuration of high-availability and packet-forwarding settings.

Initial setup

To configure the management IP and subnet IP (SNIP) on an out-of-the-box, brand-new NetScaler appliance, complete the power cabling and switch on the device. Then, by accessing the configuration command-line interface through the serial console, execute the following commands:

ns> set ns config –ipAddress <management-ip> -netmask <subnet-mask>
ns> add ns ip <ip-address> <netmask> -type <type>
ns> set system user <username> -password <password>
ns> save ns config
ns> reboot

Note: Subnet IP (SNIP) is an IP on NetScaler used to initiate communication with the server-side network. For example, to initiate communication with log servers, SNIP will be used as the source IP address from NetScaler.

Configure NSVLAN

NSVLAN is a VLAN to which the NetScaler management IP (NSIP) address's subnet is bound. The NSIP subnet is available only on interfaces associated with NSVLAN. By default, NSVLAN is VLAN-1, but you can designate a different VLAN as NSVLAN. If you do so, you must reboot the NetScaler appliance for the change to take effect. After the reboot, NSIP subnet traffic is restricted to the new NSVLAN.

ns> set ns config –nsvlan <vlan-id> -ifnum <slot/port> [-tagged (Yes/No)]
ns> save ns config
ns> reboot

Configure high availability

NetScaler supports active-passive mode in a high-availability (HA) setup. It is highly recommended to install NetScaler in HA mode because NetScaler operates on the critical path in the LSN deployment.

In HA setup, NetScaler modes (primary and secondary) exchange heartbeats to monitor the status of each other. The heartbeats should be disabled on all interfaces that are unused.

ns> add HA node <id> <ip-address-of-the-peer-HA-node>
ns> set interface <id> -haMonitor OFF [on all interfaces not used for HA heartbeat exchange]
ns> show HA node

Prerequisites for HA:

- Symmetric RSS key
- Once the RSS key is synced to secondary, force sync (recommended) and warm reboot of secondary should be executed

Configuration for symmetric RSS and sync:

1. On primary:
   a. Set RSS key to symmetric
   b. Force failover
   c. Set node –hasync disabled
   d. Saveconfig/reboot
      /* At this point, primary came up with symmetric key */
2. On secondary, after primary comes up
   a. Force failover
3. On primary:
   a. Set node – hasync enabled
   b. Enable NetScaler LSN feature
   c. Force sync
      /* Secondary synced with symmetric key of N1 */
4. On secondary:
   a. Saveconfig/reboot
   /* Symmetric key is applied to N2 */

Configure data VLAN

In an LSN deployment, NetScaler is installed at the boundary of the telecom core network. Its Internet-facing side that peers with a BGP node and routes packets to the Internet. The inside-facing or telco core network-facing side of NetScaler carries all subscriber traffic that require LSN capabilities to reach the Internet.

NetScaler needs VLANs on each of these two sides. On NetScaler, VLANs can act as L3-VLANs, which means subnet IPs also can be bound to VLANs.

ns> add vlan <id> [-aliasName <string>]
ns> bind vlan <id> -ifnum <slot/port>
ns> bind vlan <id> -IPAddress <IPAddress> <netmask>

Note: In HA setup, ensure that both the devices have similar interface numbering because the VLAN configurations will be synchronized across the HA pair.

Monitoring VLANs

To verify the configuration of VLANs or to check the statistics related to VLAN traffic, the following commands will be useful.

ns> show vlan
ns> stat vlan

Configure link aggregation

In LSN deployments, NetScaler handles very high volumes of traffic. Hence, using link aggregation is more useful than single interfaces. NetScaler supports link aggregation by using LACP as well as manual channel configuration. Since LACP support is available on almost all of the switch/router gear, LACP can be used for aggregation.

To configure LACP on NetScaler, execute below command on all interfaces that would be part of the LACP channel.

ns> set interface <id> [-lacpMode <lacpMode>] [-lacpKey<positive_integer>] [-lacpPriority <positive_integer>] [-lacpTimeout (LONG | SHORT)]
ns> show interface <id>

Note: In an HA configuration, LACP configurations are neither propagated nor synchronized.

Configure L2L3 packet-forwarding mode

NetScaler supports a variety of packet-forwarding modes. NetScaler can act as a simple switch or router based on the mode settings. In an LSN deployment, the packet-forwarding modes should be set as described below.

ns> disable ns mode l2
ns> enable ns mode l3
ns> disable ns mode mbf
ns> enable ns mode USNIP

Installing license files

The NetScaler ADC supports three types of license editions – Standard, Enterprise and Platinum. The license edition determines the set of features available for use on the NetScaler ADC. For a detailed list of feature sets associated with each license edition, please refer to the NetScaler data sheet.

http://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet.pdf

The LSN feature is available on NetScaler Enterprise and Platinum Editions. The process to install licenses on NetScaler is the same for all editions. Before proceeding to LSN configurations, install the license files on NetScaler. License files should be copied to the /nsconfig/license/ directory and the device should be rebooted.

ns> shell
root@ns# cd /nsconfig/license/
root@ns# cp <license-file-location> /nsconfig/license/
root@ns# reboot

LSN configuration

Configuring the LSN feature on NetScaler is a simple and easy process. The LSN module consists of one set of global parameters. Global implies that these parameters are applicable to all LSN traffic passing through the NetScaler device. Then, there are LSN clients and LSN pools that define LSN behavior for a specific set of subscribers or applications or protocols. The behavior for each specific set of subscribers or protocols can be further fine-tuned by using LSN profiles (traffic profile or application profile).

Configure LSN global parameters

At a global level, memory limit and session synchronization behavior can be set as needed. This step is needed for all the use cases discussed below.

ns> set lsn parameter [-memLimit <MBytes>] [-sessionSync (ENABLED | DISABLED)]

Configure simple LSN client and pool

If there is a simple requirement of one subscriber network and one public NAT IP, the configuration is one LSN client and one LSN pool.

ns> add lsn client <client-name>
ns> add lsn client <client-name> -network <IPAddress> -netmask <netmask>
ns> add lsn pool <pool-name>
ns> bind lsn pool <pool-name> <public-NAT-IP>
ns> add lsn group <group-name> -clientname <client-name>
ns> bind lsn group <group-name> -poolname <pool-name>

Using ACLs for subscriber identification, range of public NAT-IPs

The subscriber network can be identified using access control lists (ACLs) on NetScaler as well. Using ACLs provides lot of flexibility because they support identification using IP, VLAN, interface and other parameters.

ns> add ns acl <acl-name> ALLOW –srcIP <startIP-endIP>
ns> apply acl
ns> add lsn client <client-name>
ns> bind lsn client <client-name> -aclname <acl-name>
ns> add lsn pool <pool-name>
ns> bind lsn pool <pool-name> <NATIP1-NATIPx>
ns> add lsn group <group-name> -clientname <client-name>
ns> bind lsn group <group-name> -poolname <pool-name>

LSN configuration with multiple client networks and NAT IP pools

Using application profiles and transport profiles, LSN behavior can be controlled per each protocol or application. The application or transport profiles can be bound to the LSN group. All LSN clients in this group will be subject to the settings configured in the profiles.

In the following example, we also show how to share resources (pool IP) and how to add a large set of subscribers to the LSN client.

ns> add lsn client <client-name>
ns> bind lsn client <client-name> -network 192.0.4.0 -netmask 255.255.255.0
ns> bind lsn client <client-name> -network 192.0.5.0 –netmask 255.255.255.0
ns> bind lsn client <client-name> -network 192.0.6.0 –netmask 255.255.255.0
ns> add lsn pool <pool-name>
ns> bind lsn pool <pool-name> 200.100.50.10-200.100.50.20
ns> bind lsn pool <pool-name> 200.100.50.40-200.100.50.50
ns> bind lsn pool <pool-name> 200.100.50.80-200.100.50.100
ns> add lsn group <group-name> -clientname <client-name>
ns> bind lsn group <group-name> -poolname <pool-name>

Verify configuration

All the LSN configurations executed on NetScaler can be verified using the command lines below. Save the configuration after verification to retain the changes after reboots.

ns> show lsn parameter
ns> show lsn client [<client-name>]
ns> show lsn pool [<pool-name>]
ns> show lsn group [<group-name>]
ns> show lsn appsprofile
ns> show lsn transportprofile

Configure advanced LSN features

Several advanced LSN features are supported on NetScaler, including deterministic NAT, EIM/EIF, hair-pinning, user quotas, ALGs, etc. The configurations required for each of these use cases are discussed below.

Deterministic NAT

NetScaler supports two methods of assigning NAT IPs to subscribers – dynamic and deterministic. The default method is dynamic. Deterministic NAT is useful in reducing logging information because subscriber-to-NATIP+port mapping is pre-determined.

Administrators can choose the deterministic NAT option by following the configuration below.

ns> add lsn client <client-name>
ns> bind lsn client <client-name> -network <IPaddress> -netmask <netmask>
ns> add lsn pool <pool-name> -nattype DETERMINISTIC
ns> bind lsn pool <pool-name> <NATIP1-NATIPx>
ns> add lsn group <group-name> -clientname <client-name> -nattype DETERMINISTIC –portblocksize 1000
ns> bind lsn group <group-name> -poolname <pool-name>

Note: DETERMINISTIC NAT type can be specified in the “add lsn pool” command as well.

EIM/EIF

Endpoint-independent mapping (EIM) and endpoint-independent filtering (EIF) are very important features of LSN. EIM controls the behavior of LSN mapping. Below is a brief explanation of each EIM option.

ENDPOINT-INDEPENDENT: Current LSN mapping is used for traffic sent from same subscriber IP address? and port (X:x) to any external IP address? and port

ADDRESS-DEPENDENT: Current LSN mapping is used for traffic sent from same subscriber IP address and port (X:x) to same external IP address (Y), regardless of external port

ADDRESS-PORT-DEPENDENT: Current LSN mapping is used for traffic sent from same subscriber IP address and port (X:x) to same external IP address and port (Y:y)

Note: The default setting is ADDRESS-PORT-DEPENDENT.

EIF controls the way external hosts access any internal host by using an existing mapping session. EIF also supports all the above options.

ns> add lsn client <client-name>
ns> bind lsn client <client-name> -network <IPAddress> -netmask <mask>
ns> add lsn pool <pool-name>
ns> bind lsn pool <pool-name> <NATIP1-NATIPx>
ns> add lsn group <group-name> -clientname <client-name>
ns> bind lsn group <group-name> -poolname <pool-name>
ns> add lsn appsprofile <apps-profile-1-name> TCP –mapping ENDPOINT-INDEPENDENT
ns> bind lsn appsprofile <apps-profile-1-name> <port-range>
ns> add lsn appsprofile <apps-profile-2-name> TCP –filtering ADDRESS-DEPENDENT
ns> bind lsn group <group-name> -appsprofilename <apps-profile-1-name>
ns> bind lsn group <group-name> -appsprofilename <apps-profile-2-name>

User quotas

User quotas enable the administrator to restrict the maximum number of simultaneous NAT sessions each subscriber is allowed to use, thereby maintaining a fair distribution of the resources across the entire subscriber base.

Quotas can be defined in two ways – either by restricting the number of ports available for each subscriber or by restricting the total number of simultaneous NAT sessions allowed for each subscriber.

ns> add lsn client <client-name>
ns> bind lsn client <client-name> -network <IPAdress> -netmask <mask>
ns> add lsn pool <pool-name>
ns> bind lsn pool <pool-name> <NATIP1-NATIPx>
ns> add lsn group <group-name> -clientname <client-name>
ns> bind lsn group <group-name> -poolname <pool-name>
ns> add lsn transportprofile <transport-profile-1-name> TCP –portquota 1000
ns> bind lsn group <group-name> -transportprofilename <transport-profile-1-name>
ns> add lsn transportprofile <transport-profile-2-name> UDP –portquota 20
ns> bind lsn group <group-name> -transportprofilename <transport-profile-2-name>
ns> add lsn transportprofile <transport-profile-3-name> TCP –sessionquota 50
ns> bind lsn group <group-name> -transportprofilename <transport-profile-3-name>

How does the administrator decide on the port quota? Let's walk through an example. Let's say the LSN device is serving a subscriber base of X and there are Y public IP addresses available. Then, the theoretical number of ports for each subscriber can be calculated using the formula

(65535 * Y) / (X)

Note: Well-defined ports (1-1024) on any IP would not be used for subscribers. Hence, the administrator should deduct these ports from the available range.

Application Layer Gateway

There are certain protocols that use the IP/port information in the payload as well for their functionality. For example, FTP inserts the IP and port info in the payload. These applications would have an impact in case the traffic is traversing through a NAT device. Typically, NAT devices modify the IP and port info in the L3/L4 headers only. NAT device does not parse the payload of the traffic. Hence, a NAT device might impact the protocols, and hence applications, that use IP and port info in the payload.

Application Layer Gateway is a functionality on NAT device that enables the device to parse the payload as well and modify the IP and port info. By performing ALG operation, the protocols (applications) are not impacted even with the NAT device in the path.

NetScaler supports ALG functionality for the below set of protocols. After extensive customer studies, the below protocols were the only set that have real-world use cases.

File Transfer Protocol (FTP)
Trivial File Transfer Protocol (TFTP)
Internet Control Message Protocol (ICMP)
Session Initiation Protocol (SIP)
Real-time Streaming Protocol (RTSP)
Point-to-Point Tunneling Protocol - GRE (PPTP-GRE)

Below is a sample configuration for enabling SIP and RTSP ALGs.

ns> add lsn client <client-name>
ns> bind lsn client <client-name> -network <IPAdress> -netmask <mask>
ns> add lsn pool <pool-name>
ns> bind lsn pool <pool-name> <NATIP1-NATIPx>
ns> add lsn group <group-name> -clientname <client-name>
ns> bind lsn group <group-name> -poolname <pool-name>
ns> add lsn appsprofile <app_profile_name> TCP -ippooling PAIRED -mapping ENDPOINT-INDEPENDENT -filtering ENDPOINT-INDEPENDENT
ns> add lsn appsprofile <app_profile_name> UDP -ippooling PAIRED -mapping ENDPOINT-INDEPENDENT -filtering ENDPOINT-INDEPENDENT

ns> bind lsn appsprofile <app_profile_name> 1-65535
ns> bind lsn appsprofile <app_profile_name> 1-65535
ns> add lsn sipalgprofile <sipalgprofile_name> -sipdstportrange 5060 -sipTransportProtocol UDP -rport DISABLED
ns> add lsn sipalgprofile <sipalgprofile_name> -sipdstportrange 5060 -sipTransportProtocol TCP -rport DISABLED
ns> add lsn group <group-name> -clientname <client_name> -sipalg ENABLED
ns> bind lsn group <group-name>-poolname <pool_name>
ns> bind lsn group <group-name>-appsprofilename <app_profile_name>
ns> bind lsn group <group-name>-appsprofilename <app_profile_name>
ns> bind lsn group <group-name>-sipalgprofilename <sipalgprofile_name>
ns> bind lsn group <group-name>-sipalgprofilename <sipalgprofile_name>
ns> add lsn rtspalgprofile rtspalgprofiledefault -rtspIdleTimeout 100 -rtspportrange 554
ns> add lsn group <group-name> -clientname <client-name> -nattype DETERMINISTIC -portblocksize 512 -rtspalg ENABLED

Hair-pinning

The hair-pinning feature enables communication between two internal subscribers or internal hosts using the NATIP. This feature is enabled by default on NetScaler and cannot be disabled.

Static mapping

NetScaler supports static mapping capability. A customer can choose to provide a static manual mapping between a subscriber IP:port and a NAT IP:port. This configuration ensures that traffic from a specific subscriber IP address and port always gets the same NAT IP address and port. The other use case is if the subscriber is hosting any service on the internal network. This mapping enables Internet hosts to reach this internal service.

ns> add lsn static <static-map-name> <TCP/UDP> <subscrIP> <subscrPort> <natIP> [<natPort>]

IP pooling

IP pooling determines how the NATIP is allocated to the subscriber traffic. There are two options for IP pooling.

1. Paired: Same NATIP is used for all sessions of a subscriber. If no more ports are available on this NATIP, new connections from the subscriber are dropped.
2. Random: NATIP is assigned randomly from the pool of available IPs.

The default method of IP pooling is random. To change the method to paired, use LSN Appsprofile.

ns> add lsn client <client-name>
ns> bind lsn client <client-name> -network <IPAddress> -netmask <mask>
ns> add lsn pool <pool-name>

ns> bind lsn pool <pool-name> <NATIP1-NATIPx>
ns> add lsn group <group-name> -clientname <client-name>
ns> bind lsn group <group-name> -poolname <pool-name>
ns> add lsn appsprofile <apps-profile-1-name> TCP –ippooling paired
ns> bind lsn group <group-name> -appsprofilename <apps-profile-1-name>

Logging configuration

NetScaler supports logging of all LSN activity on both internal and external log servers. Telecom companies can choose to send operational logs to the local log server and session- and traffic-related logs to external log servers. NetScaler supports the Auditlog framework, which is based on the TCP protocol. In Auditlog, the server component is also provided by NetScaler and can be installed on Windows/Linux/FreeBSD/Mac platforms.

The Auditlog framework is a client-server model. The server component runs on the external log server. In the auditlog.conf file, the IP address of the NetScaler appliance must be specified. Then, the server component establishes a TCP connection to NetScaler. Similarly, on NetScaler, Auditlog action and policies must be configured to specify the log server IP, log level, log severity etc.

Below are the steps required to setup the logging on NetScaler.

1. Configure Auditlog action and policy on NetScaler
2. Bind Auditlog policy to global level
3. Install Auditlog server component on the external log server specified in the Auditlog action
4. Configure the Auditlog server component to point to NetScaler
5. Verify that Auditlog server is able to communicate with NetScaler
6. Start LSN traffic and verify that all sessions are logged on the external log server

Enabling LSN logging

NetScaler logs LSN mapping entries and the LSN sessions created or deleted for each LSN group. You can control logging of LSN information for an LSN group by using the logging and session logging parameters of the LSN group. These are group-level parameters and are disabled by default. The NetScaler ADC logs LSN sessions for an LSN group only when both logging and session logging parameters are enabled.

A log message for an LSN mapping entry consists of the following information:

- NSIP address of the NetScaler App Delivery Controller
- Time stamp
- Entry type (MAPPING)
- Whether the LSN mapping entry was created or deleted
- Subscriber's IP address, port and traffic domain ID
- NAT IP address and port
- Protocol name

- Destination IP address, port and traffic domain ID might be present, depending on the following conditions:
  - Destination IP address and port are not logged for EIM
  - Only the destination IP address is logged for address-dependent mapping. The port is not logged
  - Destination IP address and port are logged for address-port-dependent mapping

A log message for an LSN session consists of the following information:

- NSIP address of the NetScaler ADC
- Time stamp
- Entry type (SESSION)
- Whether the LSN session is created or removed
- Subscriber's IP address, port and traffic domain ID
- NAT IP address and port
- Protocol name
- Destination IP address, port and traffic domain ID

Configuration

ns> add lsn group <group-name> -clientname <client-name> [-logging (ENABLED | DISABLED)] [-sessionLogging (ENABLED | DISABLED)]
ns> set audit nslogparams –lsn ENABLED
ns> add audit nslogAction <name> <log-server-ip> -logLevel <level> -lsn ENABLED

Syslog over TCP

Logging is a very critical feature that every service provider requires. Logging is very important because of multiple reasons.

1. Logging provides evidence that service provider is meeting all the SLAs with their customers
2. Logging is mandatory by legal authorities in many countries
3. Logging can be used to gain insights into the network activity and plan for future capacity

Since logging has such high importance, most of the service providers use large log server farms to store the date for long periods. They are also looking for logging infrastructure that is reliable and scalable.

With these requirements in the scope, NetScaler now supports Syslogs over TCP. All the LSN logs that are generated in Syslog format can be exported to the external log servers over TCP. TCP is a more reliable protocol (acknowledgement feature) and supports packet recovery in case of packet loss. With this feature, NetScaler can support very large LSN deployments while maintaining reliably, all the logs of each and every LSN session.

While NetScaler can send huge amount of logs reliably using Syslog over TCP feature, the log server also must be capable of receiving such amount of logs. Since the normal log servers are not fine-tuned for receiving large amount of data in short periods, customers deploy multiple log servers and perform load balancing of these servers. NetScaler supports an build-in load balancing capability of log servers as well.

With above two features, a customer can deploy NetScaler for reliable logging (using Syslog over TCP) as well as perform load balancing of all these logs using the same device. We ensure that all the logs pertaining to one LSN session are sent to the same log server and maintain persistency.

Below given is a sample configuration for enabling Syslog over TCP feature with load balancing capabilities.

ns> add lb vserver <vname> SYSLOGTCP
ns> add server <sname1> <server_ip>
ns> add server <sname2> <server_ip>
ns> add service service1 <sname1> SYSLOGTCP 1999
ns> add service service2 <sname2> SYSLOGTCP 1999
ns> bind lb vserver <vname> service1
ns> bind lb vserver <vname> service2
ns> add syslogaction <sys_act_name> –lbvservername <vname> –logLevel all –transport TCP
ns> add syslogpolicy <sys_pol_name> ns_true <sys_act_name>
ns> bind system global <sys_pol_name>

Best practices

Citrix recommends certain NetScaler best practices as well as points to consider before proceeding with LSN configuration.

- EIM and EIF are disabled by default. Citrix recommends enabling these options for proper functioning of VoIP and peer-to-peer (P2P) applications.
- Logging the LSN information on external log servers instead of on the NetScaler ADC facilitates optimal performance when the ADC creates large numbers (millions) of LSN log entries.
- Citrix recommends configuring the LSN feature in an HA deployment of two NetScaler ADCs for uninterrupted and seamless operation of all LSN sessions.
  - Set the SYNC VLAN parameter for dedicating a VLAN for all HA-related communication
  - Synchronize the symmetric RSS key of the primary node to the secondary node for stateful synchronization of a large number of LSN mappings and sessions
- LSN takes precedence over RNAT. If a packet from a specified LSN subscriber also matches a RNAT rule, the packet is translated according to the LSN configuration.
- Forwarding of packets related only to the LSN sessions is based on the NetScaler ADC's routing table.
- Unlike with subnet IP addresses, selection of an LSN NAT IP address for a subscriber's connection is not based on the routing entry for the destination IP address.
- For inbound packets, static LSN mappings take precedence over dynamic LSN mappings.

- For outbound packets, LSN application profiles take precedence over static mapping.
- The L2 connection parameter of a load balancing virtual server does not work with the LSN feature.
- MAC-based vorwarding (MBF) does not apply to packets related only to the LSN sessions.
- To reduce the amount of active memory allocated to the LSN feature, you must warm restart the NetScaler ADC after changing the configured-memory setting. Without a warm restart, you can only increase the amount of active memory.

Conclusion

With the impending depletion of IPv4 address space and the challenges of adopting IPv6, there is an immense need to extend the usage of limited IPv4 addresses. Telecom providers are impacted the most because these service providers enable millions of subscribers to connect to Internet. Because of this large scale, the solution to extend IPv4 address usage should be robust, delivering high stability, high performance and agility while providing the required functionality.

NetScaler, the world's most advanced ADC, now offers a comprehensive set of LSN features that enable telecom providers to effectively leverage their IPv4 address space. NetScaler supports all the required features for LSN deployment and has an unparalleled record of delivering very high performance. It is also a very mature technology that offers exceptional stability and three-dimensional scalability. Overall, NetScaler is the best solution for delivering the LSN features required by telecom companies and service providers to meet subscriber needs during the transition to IPv6.

Appendix

Command reference

> set lsn parameter [-memLimit <MBytes>] [-sessionSync (ENABLED | DISABLED)]
> add lsn client <clientname>
> bind lsn client <clientname> ((-network <ip_addr> [-netmask <netmask>] [-td <positive_integer>]) | -aclname <string>)
> add lsn pool <poolname> [-nattype (DYNAMIC | DETERMINISTIC)] [-portblockallocation (ENABLED | DISABLED)] [-portrealloctimeout <secs>] [-maxPortReallocTmq <positive_integer>]
> bind lsn pool <poolname> <lsnip>
> add lsn appsprofile <appsprofilename> <transportprotocol> [-ippooling (PAIRED | RANDOM)] [-mapping <mapping>] [-filtering <filtering>] [-tcpproxy (ENABLED | DISABLED)] [-td <positive_integer>]
> bind lsn appsprofile <appsprofilename> <lsnport>
> add lsn transportprofile <transportprofilename> <transportprotocol> [-sessiontimeout <secs>] [-finrsttimeout <secs>] [-portquota <positive_integer>] [-sessionquota <positive_integer>] [-portpreserveparity (ENABLED | DISABLED)] [-portpreserverange (ENABLED | DISABLED)] [-syncheck (ENABLED | DISABLED)]
> add lsn group <groupname> -clientname <string> [-nattype (DYNAMIC | DETERMINISTIC)] [-portblocksize <positive_integer>] [-logging (ENABLED | DISABLED)] [-sessionLogging (ENABLED | DISABLED)] [-sessionSync (ENABLED | DISABLED)] [-snmptraplimit <positive_integer>] [-ftp (ENABLED | DISABLED)]

> bind lsn group <groupname> (-poolname <string> | -transportprofilename <string> | -appsprofilename <string>)
> add lsn static <name> <transportprotocol> <subscrIP> <subscrPort> [-td <positive_integer>] [<natIP> [<natPort>]] [-destIP <ip_addr> [-dsttd <positive_integer>]]

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

CITRIX®

About Citrix
Citrix (NASDAQ:CTXS) is leading the transition to software-defining the workplace, uniting virtualization, mobility management, networking and SaaS solutions to enable new ways for businesses and people to work better. Citrix solutions power business mobility through secure, mobile workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. With annual revenue in 2014 of $3.14 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.