How to setup client-side HTTP/2 on NetScaler successfully?

Use Case

How to setup client-side HTTP/2 on NetScaler successfully.

Introduction

HTTP/2 is binary protocol which is more compact on the wire. HTTP/2 much less error-prone, compared to textual protocols like HTTP/1.x

HTTP/2 is defined for both HTTP URIs (i.e. without encryption) and for HTTPS URIs (over TLS, where TLS 1.2 or newer is required). Although the standard itself does not mandate usage of encryption, most client implementations (Firefox, Chrome, Safari, Opera, IE, Edge) have stated that they will only support HTTP/2 over TLS, which makes encryption de facto mandatory.

Cipher suites supported for HTTP/2 handshake:

RFC 7540 mandates to use TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 cipher with P-256 curve. Other ciphers suite which can be used are:

1. TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
2. TLS1.2-DHE-RSA-AES256-GCM-SHA384
3. TLS1.2-DHE-RSA-AES128-GCM-SHA256
4. TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384
5. TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256

All the NetScaler appliances have support for these cipher suites at client-side. Find the required build number for your NetScaler appliance here – http://docs.citrix.com/en-us/netscaler/12/ssl/cipher_protocl_support_matrix.html

When will NetScaler not upgrade to HTTP/2 protocol?

If NetScaler virtual server has none of the above-mentioned ciphers bound, then NetScaler will not upgrade to HTTP/2 and further communication will happen on existing HTTP/1.x protocol only.

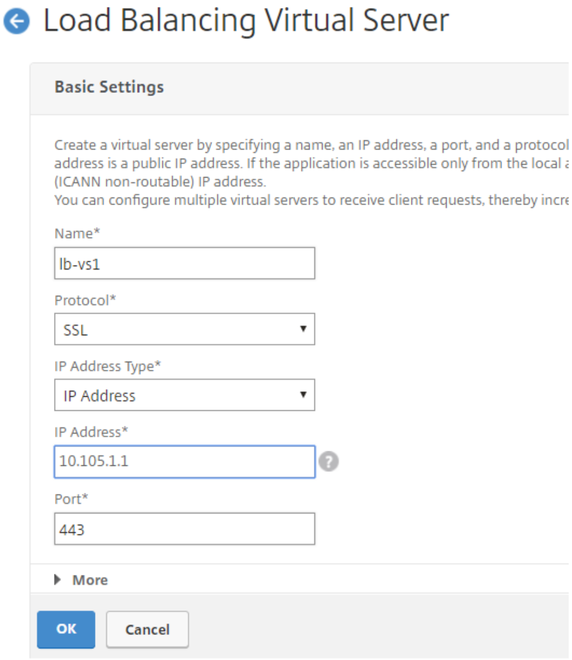
E.g. Let's say during TLS handshake, if client browser has support for cipher suite – TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 and TLS_RSA_WITH_AES_256_CBC_SHA and NetScaler virtual server has support for cipher suite – TLS_RSA_WITH_AES_256_CBC_SHA then client and server will negotiate on cipher suite – TLS_RSA_WITH_AES_256_CBC_SHA. So as per the RFC specifications if negotiation is happening for unsupported cipher suite, protocol upgradation will not happen and further communication will be on HTTP/1.x protocol.

For more details about unsupported cipher suite, see https://tools.ietf.org/html/rfc7540#page-83

How to setup HTTP/2 on NetScaler:

Following screenshots will guide you to setup HTTP/2.

1. Add SSL type Load Balancing virtual server



Load Balancing Virtual Server

Basic Settings

Create a virtual server by specifying a name, an IP address, a port, and a protocol
address is a public IP address. If the application is accessible only from the local a
(ICANN non-routable) IP address.
You can configure multiple virtual servers to receive client requests, thereby incre

Name*
lb-vs1

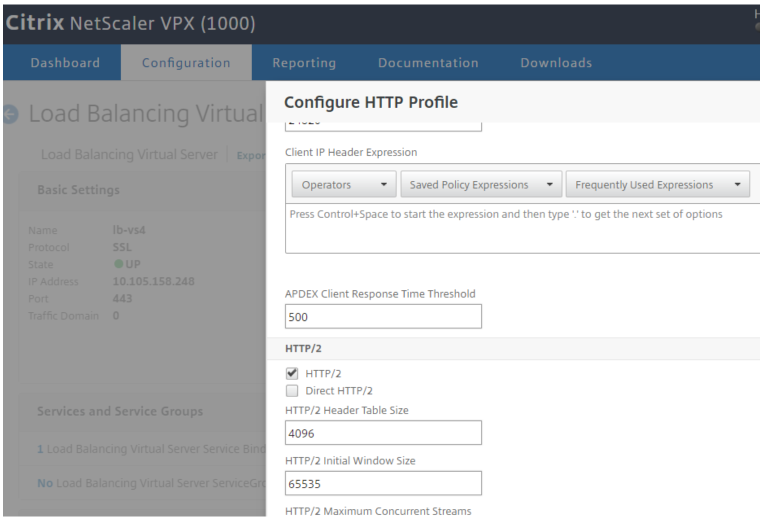
Protocol*
SSL

IP Address Type*
IP Address

IP Address*
10.105.1.1

Port*
443

2. Configure HTTP profile and tick mark the HTTP/2 check box.



Basic Settings

Name	lb-vs4
Protocol	SSL
State	● UP
IP Address	10.105.158.248
Port	443
Traffic Domain	0

Services and Service Groups

1 Load Balancing Virtual Server Service Bind

No Load Balancing Virtual Server ServiceGr

Configure HTTP Profile

Client IP Header Expression

Press Control+Space to start the expression and then type '.' to get the next set of options

APDEX Client Response Time Threshold
500

HTTP/2

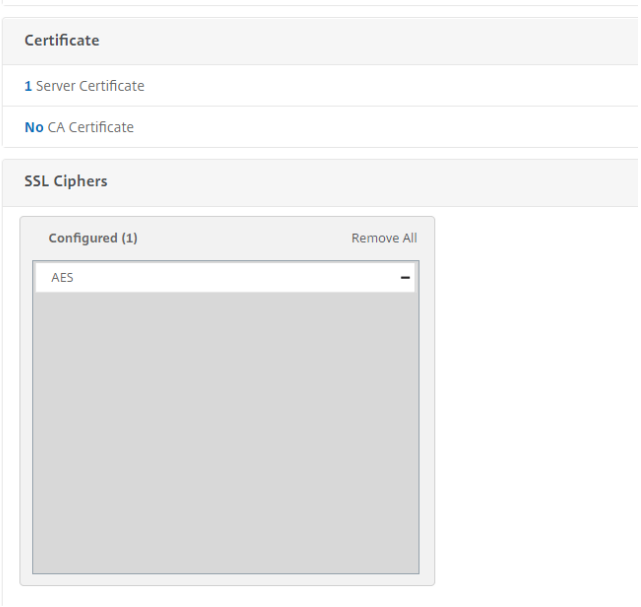
☑ HTTP/2
□ Direct HTTP/2

HTTP/2 Header Table Size
4096

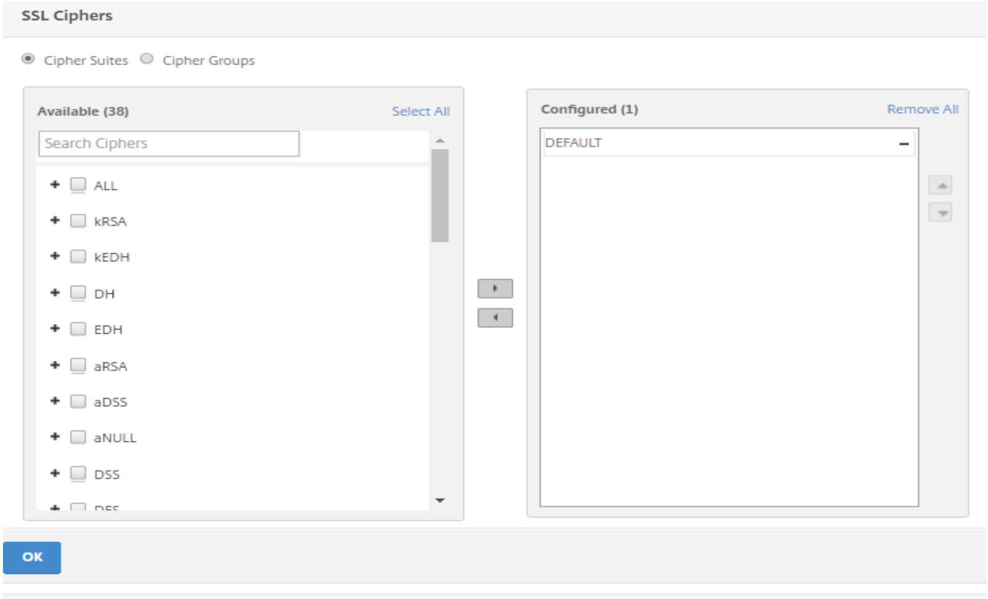
HTTP/2 Initial Window Size
65535

HTTP/2 Maximum Concurrent Streams

3. Select SSL Ciphers tab from SSL type virtual server to edit cipher suite list.



4. Shortlist recommended SSL Ciphers from drop down box and click on OK button. (Note: Default cipher suite group contains all whitelisted ciphers).



Note: 512 bits certificate key will not work for supported cipher suites. Recommended certificate key size is 2048 bits or more. Find how to create and install a 2048-bit certificate here – https://www.citrix.com/content/dam/citrix/en_us/citrix-developer/documents/Netscaler/how-do-i-setup-rsa-keys-on-netscaler.pdf

References:

- https://en.wikipedia.org/wiki/HTTP/2#Encryption
- https://tools.ietf.org/html/rfc7540
- https://http2.github.io/faq/#what-are-the-key-differences-to-http1x