

HTTP/S Object Storage Protocol Suite

The industry's premiere validation system for
Object Storage, Web Service and Application Delivery

Overview

The HTTP/S protocol suite allows equipment manufacturers, service providers and enterprises to model complex RESTful transactions at scale simulating end users activities and cloud storage interfaces such as Amazon S3, OpenStack Swift and SNIA CDMI. Bottlenecks in the service delivery chain that extend through security appliances and application delivery controllers can be pinpointed prior to deployment avoiding live data center outages. Client authentication emulation supports both Pre-emptive and Passive modes and schemes from Basic to the widely used NTLM/Kerberos to find the capacity limits of access management infrastructure.

Amazon S3, OpenStack Swift, SNIA CDMI and proprietary Object storage server infrastructure can be validated against functional and performance acceptance criteria. A robust HTTP data verification capability helps users ensure that information sent through a variety of proxies and caching points passes through intact. Negative testing also helps users verify that data that should be scrubbed doesn't make it through gateway access points.

IT organizations and service providers can use these features and many others to do performance and capacity assessments to ensure clients and servers are configured and tuned optimally for maximum performance.

Highlights

- Pre-built commands and dedicated stats for OpenStack Swift and SNIA CDMI
- Broad authentication schemes
- Unique Load DynamiX HTTP Dynamic Parsing feature
- User defined certificates uploads
- Gain full support of all major SAN, NAS and Object protocols

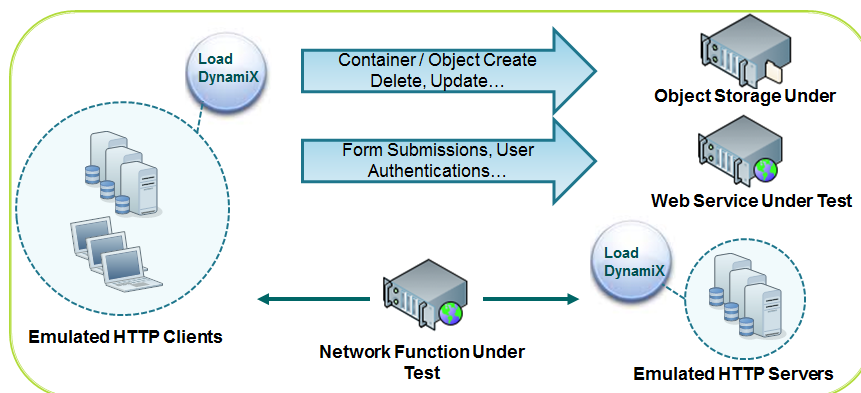


Illustration 1. Load DynamiX HTTP client-only and client / server emulation.

Key Features

<p>Client Emulation Realism</p>	<ul style="list-style-type: none"> ▪ Realistic emulation of HTTP clients with the ability to emulate multiple scenarios from a single interface ▪ HTTPS support with user-defined certificates and configurable cipher advertisement (SSL 2.0/3.0, TLS 1.0/1.1/1.2) ▪ HTTP request header and message body content extraction/insertion for stateful RESTful API and Object storage validation ▪ Dynamic HTTP message bodies with content insertion can be used for form submissions and user authentication ▪ Configurable network options supporting VLAN tagging, IPv4, IPv6 and MAC address assignment with increment schemes for emulation of millions of unique clients
<p>HTTP Authentication</p>	<ul style="list-style-type: none"> ▪ Test authentication mechanisms including Basic, Digest, Amazon S3, NTLM, Kerberos leveraging both Passive and Pre-Emptive options
<p>Test Modeling</p>	<ul style="list-style-type: none"> ▪ Flexible scenario modeling with looping constructs, user parameter files, and functions for unique parameter usage such as creating complex URI structures ▪ Set independent, iterative load profile objectives for each parallel scenario to assess scalability including: concurrent scenarios, new scenarios per second, concurrent actions, new actions per second, concurrent connections, new connections per second, and throughput
<p>Content Creation / Data Verification</p>	<ul style="list-style-type: none"> ▪ Create complex container nesting with varying object sizes for object storage ▪ Support for reading and writing large files ▪ Data verification options to ensure the integrity of data written to target storage
<p>Commands</p>	<ul style="list-style-type: none"> ▪ HTTP command sequencing control within scenarios to emulate any complex workload that represents browser, application and device behaviors. Supported commands include: <ul style="list-style-type: none"> - HTTP 1.0/1.1: CONNECT, GET, PUT, POST, HEAD, DELETE, OPTIONS, TRACE
<p>Object Storage Protocol APIs</p>	<ul style="list-style-type: none"> ▪ OpenStack Swift ▪ SNIA CDMI
<p>Client/Server Support</p>	<ul style="list-style-type: none"> ▪ End-to-end client and server emulation for validation of content-aware network functions including Firewalls, Unified Threat Management, Intrusion Detection/Prevention, Application Delivery Controllers and Content Switching

Statistics

Commands	HTTP Action counts or Actions/sec (average for all or individual Actions)
Details	HTTP command transmission/receipt OK/Fail/Drop in packets/sec or kilobits/sec
Authentications	HTTP Authentication Attempts (Passive, Preemptive), Ignored/Succeeds, Failures (Cred. Denied, Access Forbidden, Server Error, Reset by Server, Disabled by Client), Aborts
HTTP Response Time	HTTP command response time (average, minimum, maximum)
HTTP Throughput	HTTP packet or byte throughput on per command or All basis
TCP Connection Time	Connection Time (Avg. Duration, Time-to-1 st -Byte, Closing Time)
TCP Connections	Attempts, Opened, Closed, Failed, Reset, Timeout (Open, Data, Idle, ARP, SYN), SYN Rejected
TCP Throughput	TCP packet throughput on per command or All basis
TCP Details	Tx (OK, Retransmissions, Out-of-Sequence,), Rx (Ok, Length Error, Drop, Duplicate, Out-of-Sequence, Rejected, Invalid Destination)
Data Verification	HTTP data verification operations attempts, successes, failures

Supported Platforms

Load DynamiX 1G Series Appliances
 Load DynamiX 10G Series Appliances