BROADCOM SOFTWARE

What's new in Layer7 API Gateway 11.1 GA?

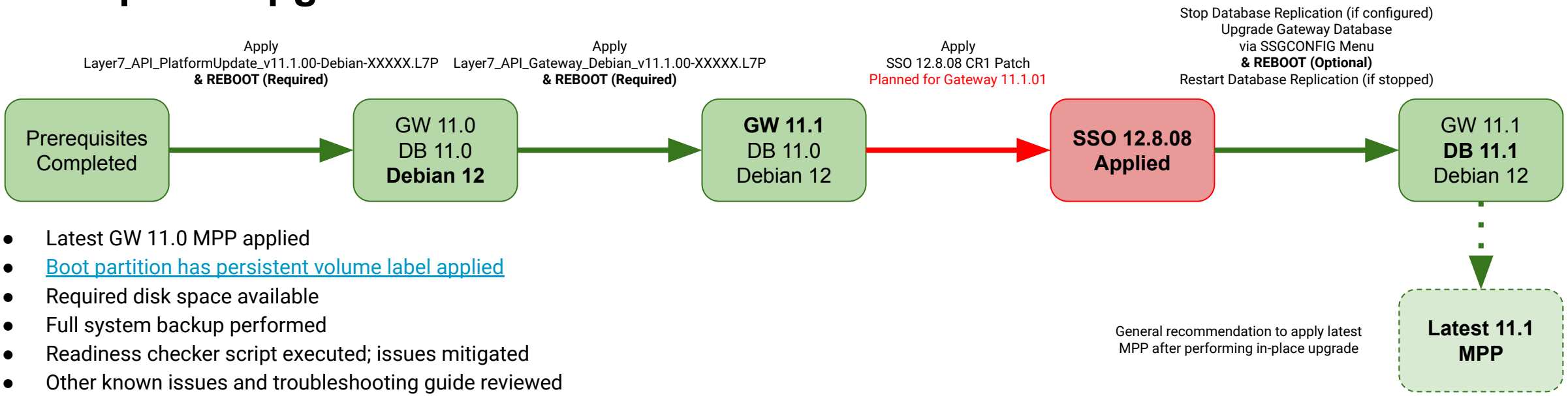
April 2024

Agenda

- Debian 12 Upgrade
- JDK 17 Upgrade
- ESXi 8 Support
- MySQL Enterprise with Group Replication Support
- Percona XtraDB Clusters Support
- OpenTelemetry (Preview)
- Graphman Enhancements (Preview)
- Policy as Code (Preview)
- Throughput Quota Assertion Enhancements for Redis (Preview)
- Require and Introspect OAuth Token Assertion (Preview)
- Key Value Storage Assertion (Preview)
- WebSockets via Shared HTTP Port (Preview)
- Deprecations
- Upgrade Paths
- Other

Debian 12 Upgrade

- Upgrade from Debian 11 to Debian 12
- Supported for Gateway v11.1 standard lifetime
- Improved reliability and security in general
- OVA for virtual appliance; no ISO for hardware appliance
- **In-place Upgrade!!!**



- Latest GW 11.0 MPP applied
- Boot partition has persistent volume label applied
- Required disk space available
- Full system backup performed
- Readiness checker script executed; issues mitigated
- Other known issues and troubleshooting guide reviewed

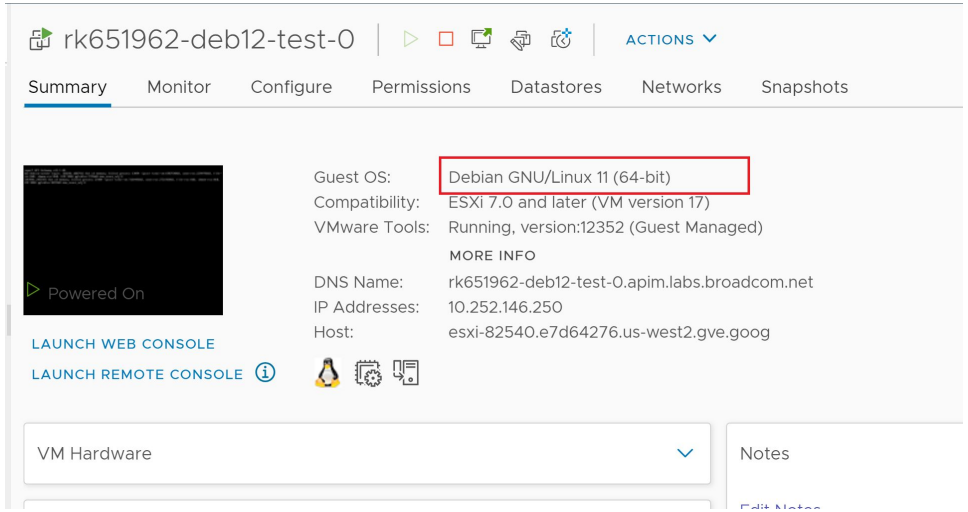
BROADCOM SOFTWARE

JDK 17 Upgrade

- Upgrade from JDK 11 to JDK 17
- Improved reliability and security
- Improved performance
  - Garbage collection is about 15% faster which contributes to overall 13% throughput and 12% average response time improvements (during controlled testing; actual mileage may vary)
- Some weak EC algorithms removed
- Some weak algorithms not selected by default (but can be selected by users)
  - Effects default cipher sets; not customized cipher sets
- Luna and nShield HSM clients require upgrades (seperate from in-place upgrade)
- Should use Policy Manager v11.1 with Gateway v11.1

ESXi 8 Support

- Debian 12 technically requires ESXi 8+ and virtual hardware version 20+
- We have tested against and will provide back support for our Debian 12 appliance on ESXi 7 and virtual hardware version 17
  - ESXi 7 will report the guest OS is Debian 11 even when it's actually Debian 12



BROADCOM SOFTWARE

MySQL Enterprise with Group Replication Support

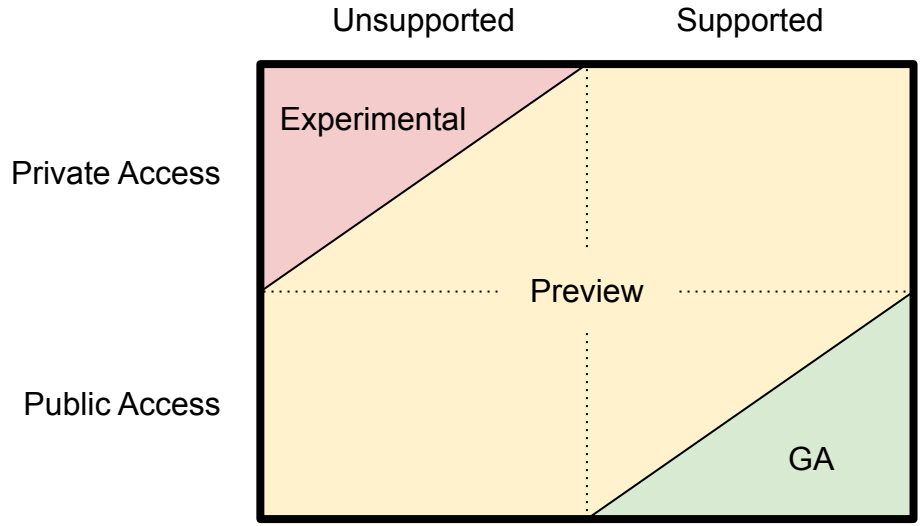
- Support for MySQL Enterprise as self managed alternative for ssg database
- Support for group replication as alternative to master-master replication
  - Single primary mode only (multi-primary mode not supported)
- Primary keys added to support group replication
  - Gateway only (does not include OTK/MAG/Portal databases)
- Expects gateway connection via a proxy (e.g. MySQL Router, HAproxy, etc.)
  - Proxy handles fail over
- MySQL Enterprise and proxy not provided by Layer7

Percona XtraDB Clusters (PXC) Support

- Support for PXC as self managed alternative for ssg database
- Support for Galera cluster as alternative to master-master replication
- Primary keys added to support strict mode
  - Gateway only (does not include OTK/MAG/Portal databases)
- Expects gateway connection via a proxy (e.g. HAproxy, etc.)
  - Proxy handles fail over
- PXC and proxy not provided by Layer7

Progressive Delivery Model

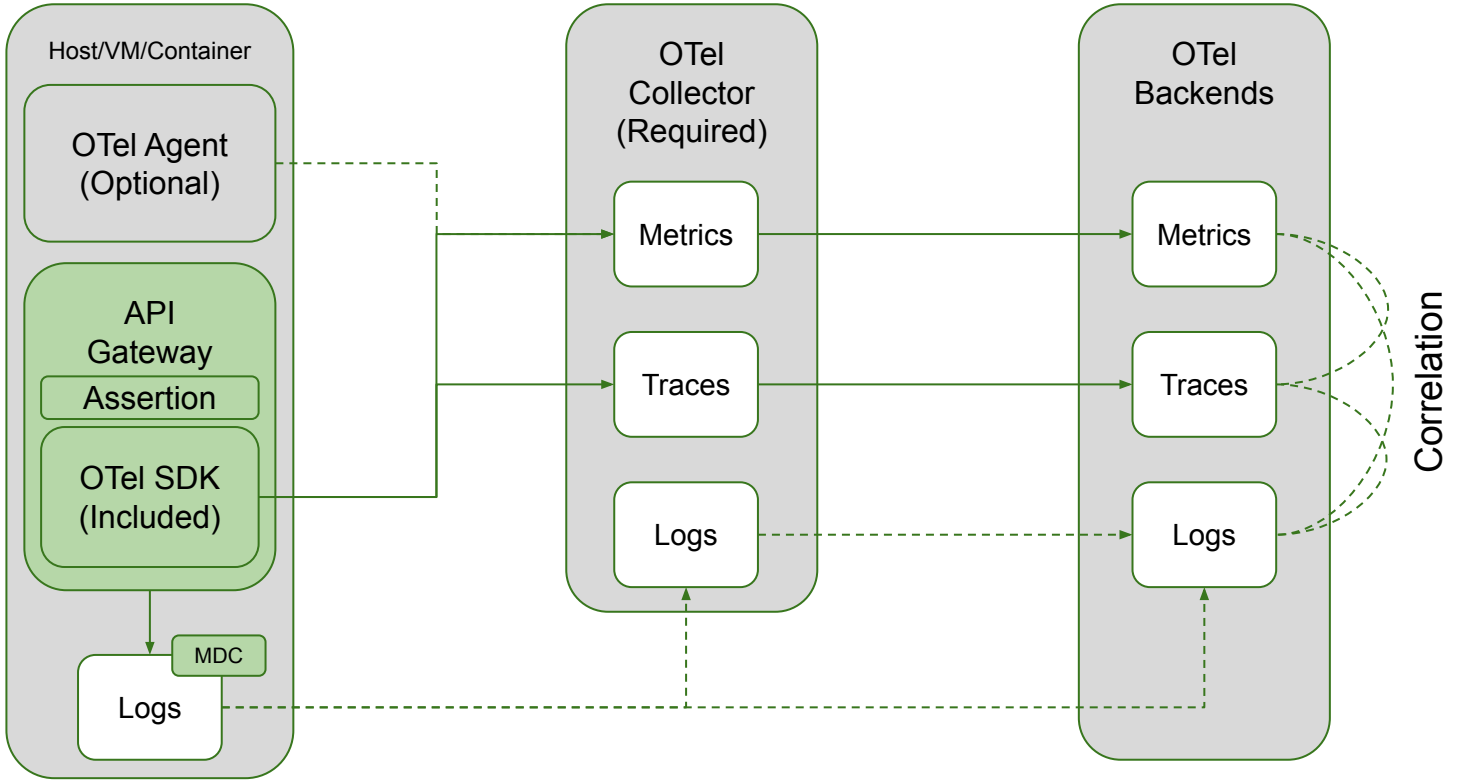
- **[Experimental] -** Limited testing; distributed in ***non-official releases***; no tech docs; only community portal supported; non-prod use only
- **[Preview]** - Nearly complete feature; distributed in ***official releases***; possible feature flag; tech docs; generally community portal supported; *customers wanting full Broadcom support of a preview feature in production environments must request Layer7 product team approval via a Broadcom support case*
- **[General Availability]** - Available to all customers with full support for production environments



BROADCOM SOFTWARE

OpenTelemetry (Preview)

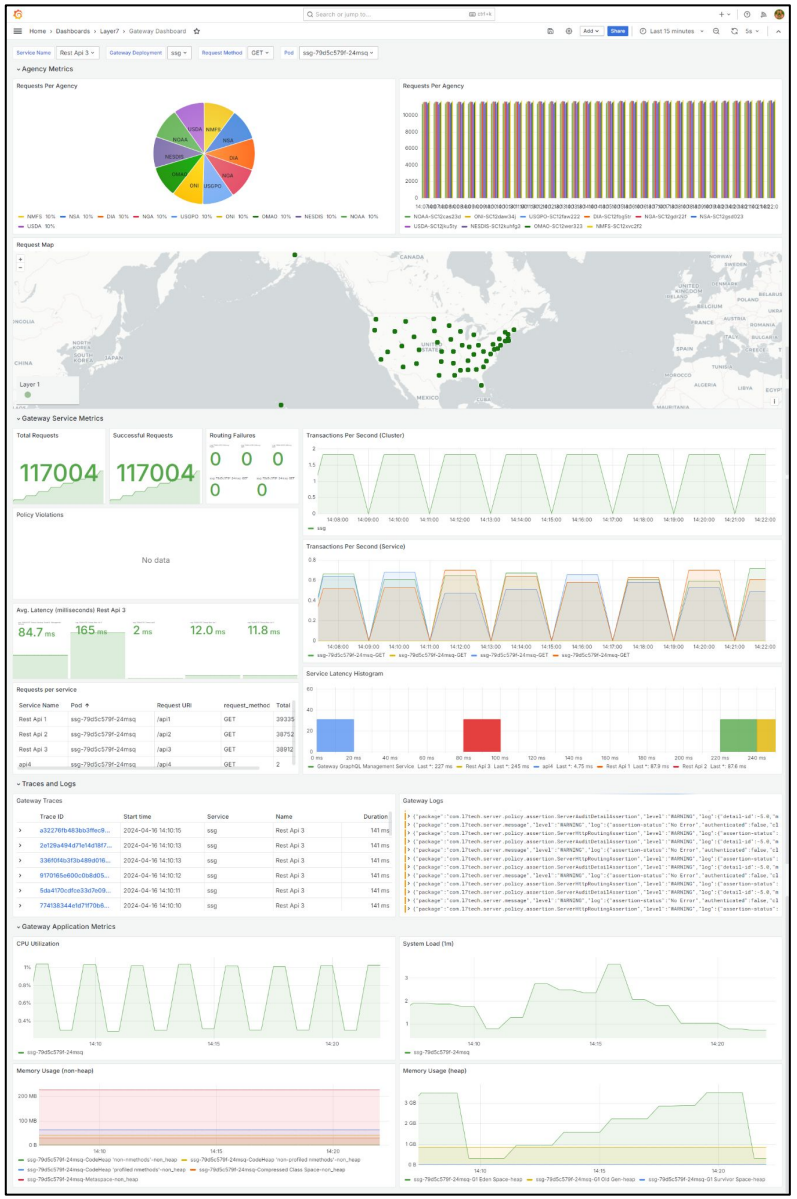
- An Observability framework and toolkit designed to create and manage telemetry data such as traces, metrics, and logs.
- Supported by many vendors
- Standard including:
  - Specification
  - Protocol
  - Semantics
- OTel SDK (v1.35)
- OTel Agent (v1.33+, v2.1.0+)
- OTel Collector
- Telemetry Metric Assertion



BROADCOM SOFTWARE

OpenTelemetry (Preview) - Metrics

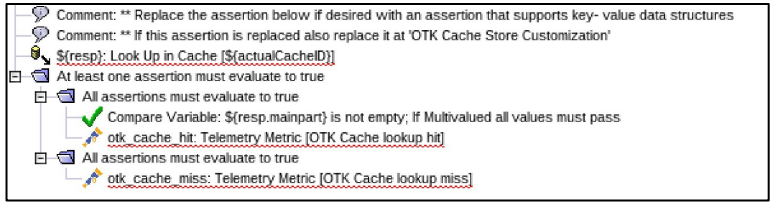
- Gateway Service Metrics
  - service_attempted
  - service_policy_violations
  - service_routing_failures
  - service_success
  - service_latency
  - service_routing_latency
- Attributes
  - l7_operation (SOAP Operation)
  - l7_serviceName
  - l7_goid
  - l7_serviceUri
  - l7_method

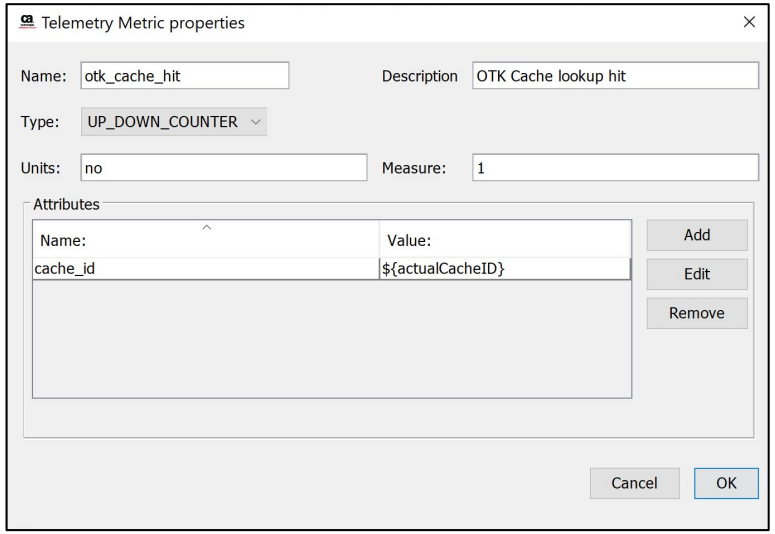


BROADCOM SOFTWARE

OpenTelemetry (Preview) - Telemetry Metric Assertion

- Emit custom metrics in policy
- Supported types:
  - Counter
  - Up Down Counter
  - Gauge
  - Histogram
- Counters reset on gateway restart
  - Includes service metrics; expected; should be handled by backend
- Attributes attached as metadata of metric; can be used to filter metrics in collector and backend solutions
  - Its highly discouraged to have attributes having high cardinality. (Eg. timeStamp) It will impact the backend system storage requirements.

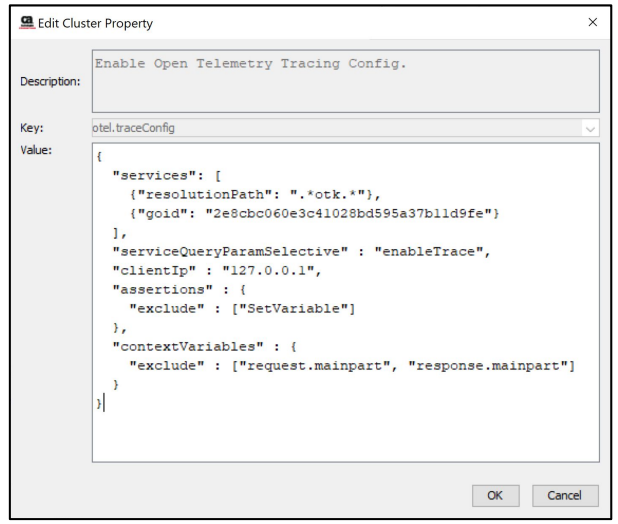


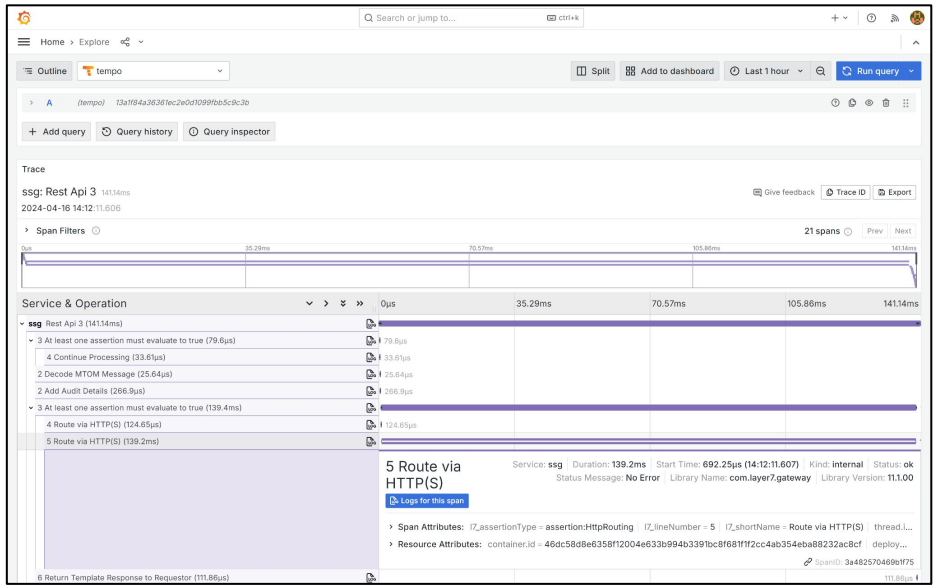


BROADCOM SOFTWARE

OpenTelemetry (Preview) - Traces

- Service, policy and assertion level transaction tracing
- Optionally tracks changing context variable values
- Context propagation - HTTP(S)(/2) only
- Supports filtering (via CWP)
- Supports head & tail sampling (via collector)
- New context variables
  - otel.traceId
  - otel.spanId

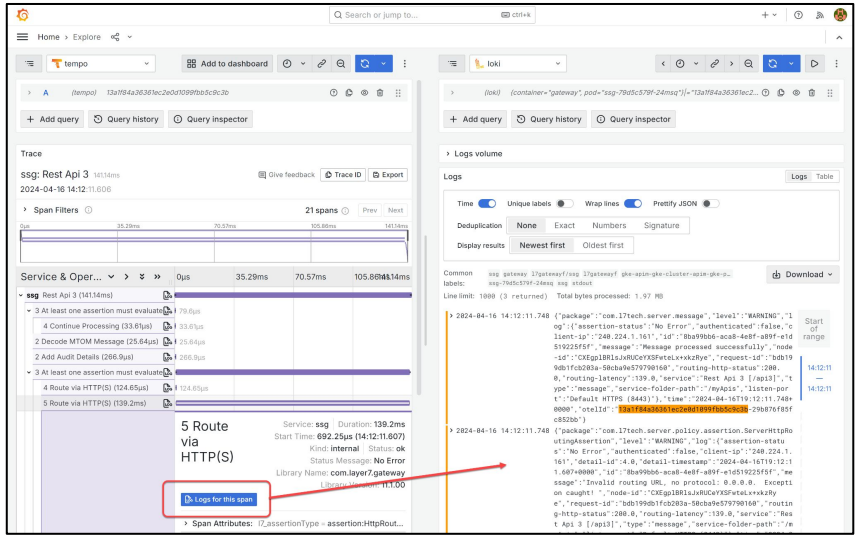


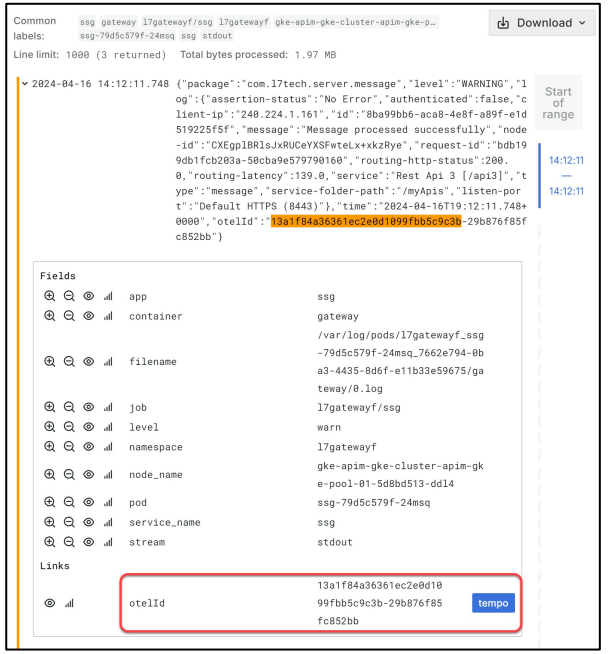


BROADCOM SOFTWARE

OpenTelemetry (Preview) - Logs

- ***traceId-spanId*** injected into transaction log events (not system or audit log events)
- OTel, in general, and tracing, specifically, must be enabled
- Other log configuration applies
- Works differently for different log formatters
  - ConfigurableLogFormatter
  - JsonLogFormatter
  - SingleLineLogFormatter
- Works with all log sinks (including console, file and syslog)
- Customer must collect and forward logs to target system






```
2024-02-13T10:56:36.716-0800 WARNING 314 c2d42717035b45761d7892fb7c056b9f-428f4d0f831735ca com.l7tech.server.policy.assertion.ServerAuditDetailAssertion: -5
2024-02-13T10:56:36.760-0800 INFO    315 c2d42717035b45761d7892fb7c056b9f-747807f1be8b3290 com.l7tech.traffic: 2024-02-13T18:56:36.753Z, , , 200
2024-02-13T10:56:36.762-0800 INFO    315 c2d42717035b45761d7892fb7c056b9f-747807f1be8b3290 com.l7tech.server.message: Processing request for service: test2
2024-02-13T10:56:36.762-0800 WARNING 315 c2d42717035b45761d7892fb7c056b9f-747807f1be8b3290 com.l7tech.server.policy.assertion.ServerAuditDetailAssertion: -5
2024-02-13T10:56:36.762-0800 WARNING 315 c2d42717035b45761d7892fb7c056b9f-747807f1be8b3290 com.l7tech.server.message: Message processed successfully
2024-02-13T10:56:36.767-0800 INFO    314 c2d42717035b45761d7892fb7c056b9f-28013d2a0fb4a6b9 com.l7tech.traffic: 2024-02-13T18:56:36.670Z, , , 200
```


BROADCOM SOFTWARE

OpenTelemetry (Preview) - Performance

- Emphasis on no performance impact when OTel is completely disabled
- Light testing to verify that gateway doesn't fall down under some load when OTel is enabled
- Significant performance impact with OTel fully enabled with no head/tail sampling
- Customer mileage will vary
  - Customers should perform their own performance tests
  - Customers should make their own performance cost vs. observability benefit assessment
- We welcome feedback, and we may plan future OTel performance optimizations that will benefit common customer scenarios

Graphman Enhancements (Preview)

- Policy Revision Support
  - New policy (L7Policy) and service (L7Service) types added
  - Policy revisions only supported for new types; old types deprecated but not removed
  - L7Policy
    - FRAGMENT (***@deprecated*** PolicyFragment)
    - GLOBAL (***@deprecated*** GlobalPolicy)
    - INTERNAL
    - POLICY_BACKED_IDP
    - POLICY_BACKED_OPERATION
    - POLICY_BACKED_BACKGROUND_TASK (***@deprecated*** BackgroundTaskPolicy)
    - POLICY_BACKED_SERVICE_METRICS
  - L7Service
    - WEB_API (***@deprecated*** WebApiService)
    - SOAP (***@deprecated*** SoapService)
    - INTERNAL_WEB_API (***@deprecated*** InternalWebApiService)
    - INTENAL_SOAP (***@deprecated*** InternalSoapService)
  - Policy revisions cannot be queried directly; only through L7Policy and L7Service
  - Mutations allow setting the active policy revision of an L7Policy or L7Service by its ordinal

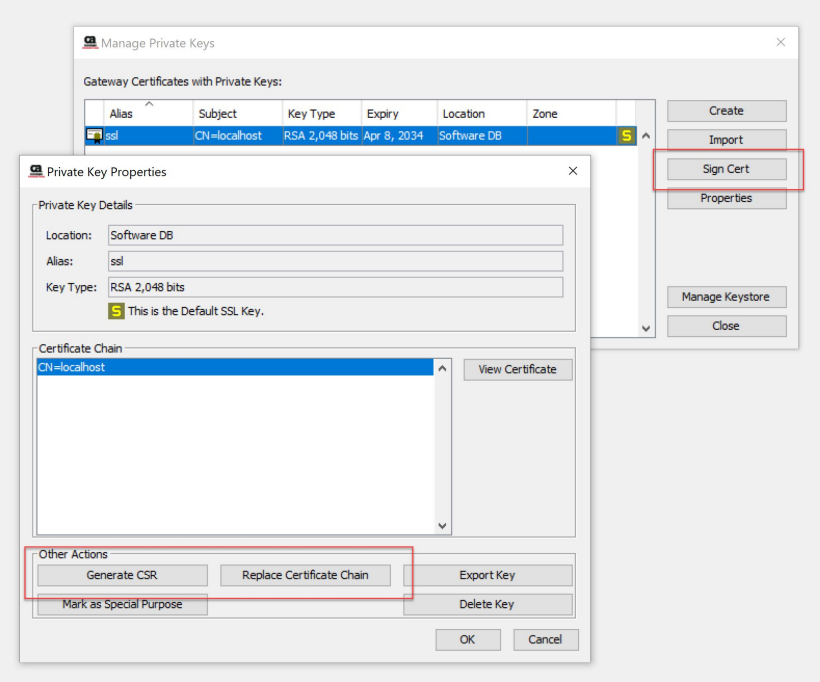
```
policyByName(name: “some-policy”) {
    goid
    guid
    name
    policyRevision {ordinal active comment time xml}
}

serviceByResolutionPath(resolutionPath: “/some-service”) {
    goid
    guid
    name
    policyRevision {ordinal active comment time xml}
}
```

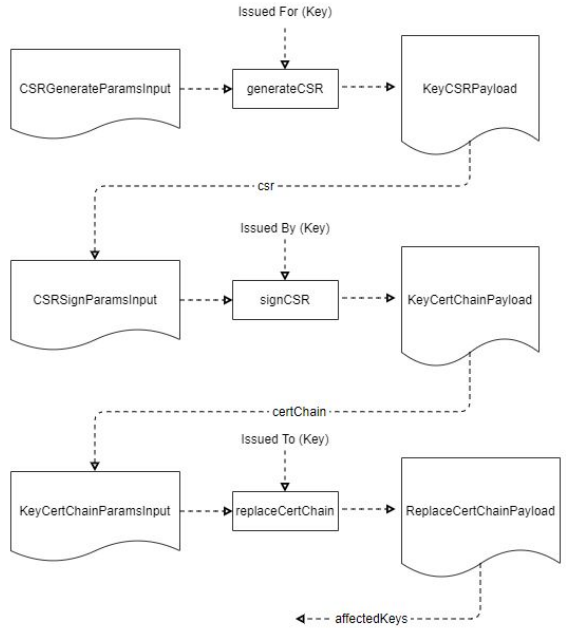
```
Query:
updateRevisions($policies: $[L7Policy!]!, $services: $[L7Service!]!) {
  updatePoliciesRevision($policies, activate: 'true', comment: 'v1.1-patch') {
    detailedStatus {status description source {name value} target {name value}}
  }

  updateServicesRevision($services, activate: 'true', comment: 'v1.1-patch') {
    detailedStatus {status description source {name value} target {name value}}
  }
}

Variables:
{
  "policies": [
    {
      "name": "some-policy",
      "policyRevision": {
        "ordinal": 3
      }
    }
  ],

  "services": [
    {
      "name": "some-webapi-service",
      "serviceType": "WEB_API",
      "resolutionPath": "/webapi-1",
      "policyRevision": {
        "ordinal": 3
      }
    },
    {
      "name": "some-soap-service",
      "serviceType": "SOAP",
      "resolutionPath": "/soap-1",
      "policyRevision": {
        "ordinal": 5
      }
    }
  ]
}
```


BROADCOM SOFTWARE

Graphman Enhancements (Preview)

- Key Cert Management Support
  - generateCSR(alias: String!, params: CSRGenerateParamsInput!) : KeyCSRPayload
  - signCSR(alias: String!, params: CSRSignParamsInput!) : KeyCertChainPayload
  - replaceCertChain(alias: String!, params: KeyCertChainParamsInput!) : ReplaceCertChainPayload





BROADCOM SOFTWARE

Graphman Enhancements (Preview)

- Identity Provider Updates
  - Added support for InternalIdp, SimpleLdapIdp, PolicyBackedIdp
  - Updated FederatedIdp (***@deprecated*** Fip), LdapIdp (***@deprecated*** Ldap)
    - Renamed (and deprecated old) types, queries and mutations
  - Updated InternalUser, InternalGroup, FederatedUser (***@deprecated*** FipUser), FederatedGroup (***@deprecated*** FipGroup)
    - Renamed (and deprecated old) ***some*** types, queries and mutations
- Graphman Encryption Updates
  - Cluster passphrase used for crypto by default (previously used master passphrase)
  - New HTTP encryption header, x-l7-passphrase (***@deprecated*** l7-passphrase & encpass); base64 encoded; custom passphrase (cluster passphrase
  - System property, com.l7tech.bootstrap.graphmanBundles.passphrase, can be encrypted with cluster passphrase (for decrypting bundles bootstrapped on startup)
    - Use custom passphrase to secure bundle; use cluster passphrase to secure custom passphrase
  - OpenSSL encryption friendly

```
# to encrypt the secrets
echo -n "<clear text secret>" | openssl enc -e -aes-256-cbc -md sha256 -pass pass:<passphrase> -a

# to decrypt the secrets
echo -n "<cipher text secret>" | openssl enc -d -aes-256-cbc -md sha256 -pass pass:<passphrase> -a
```


BROADCOM SOFTWARE

Policy as Code (Preview)

- Dev & DevOps friendly alternative to policy authoring using Policy Manager
- Supported by Graphman (exports/imports)
- Represent policy as XML, JSON and YAML strings; or JSON object (code)
  - Should be one; can be all three; precedence xml > json > yaml > code
- Some embellishments (e.g. shorter names, less base64 encoding, etc.)
- Emphasis on short list of assertions; mileage varies for others
  - Add Comment to Policy
  - Set Context Variable
  - Encapsulated Assertions
  - All assertions must evaluate to true
  - At least one assertion must evaluate to true
  - Include Policy Fragment

BROADCOM SOFTWARE

Policy as Code (Preview)(cont.)

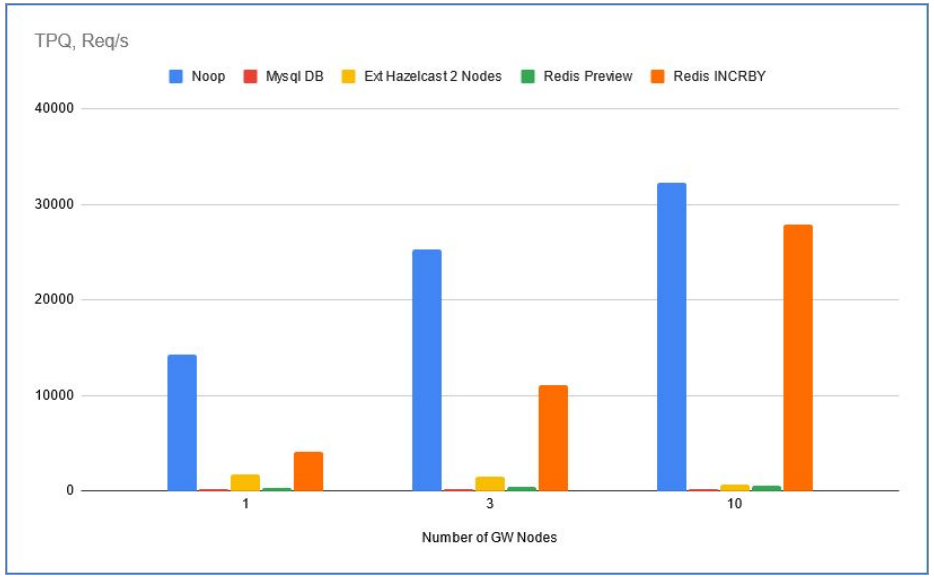
```
<wsp:Policy xmlns:L7p="http://www.layer7tech.com/ws/policy" xmlns:wsp="http://schemas.xmlsoap.org/ws/2002/12/policy">
    <wsp:All wsp:Usage="Required">
        <wsp:OneOrMore wsp:Usage="Required">
            <wsp:All wsp:Usage="Required">
                <L7p:AuditAssertion/>
                <L7p:CommentAssertion>
                    <L7p:Comment stringValue="Hello"/>
                </L7p:CommentAssertion>
            </wsp:All>
            <L7p:CommentAssertion>
                <L7p:Comment stringValue="World!"/>
            </L7p:CommentAssertion>
        </wsp:OneOrMore>
        <wsp:OneOrMore wsp:Usage="Required">
            <L7p:SetVariable>
                <L7p:Base64Expression stringValue="MTIzNA=="/>
                <L7p:DataType variableDataType="int"/>
                <L7p:VariableToSet stringValue="some-variable"/>
            </L7p:SetVariable>
            <L7p:TrueAssertion/>
            <L7p:assertionComment>
                <L7p:Properties mapValue="included">
                    <L7p:entry>
                        <L7p:key stringValue="LEFT.COMMENT"/>
                        <L7p:value stringValue="This is left comment"/>
                    </L7p:entry>
                </L7p:Properties>
            </L7p:assertionComment>
        </wsp:OneOrMore>
        <wsp:OneOrMore wsp:Usage="Required">
            <L7p:Include>
                <L7p:PolicyGuid stringValue="111-12356-789-123"/>
                <L7p:PolicyName stringValue="some-policy"/>
            </L7p:Include>
            <L7p:Encapsulated>
                <L7p:EncapsulatedAssertionConfigGuid stringValue="222-12356-789-123"/>
                <L7p:EncapsulatedAssertionConfigName stringValue="some-encass"/>
                <L7p:Parameters mapValue="included">
                    <L7p:entry>
                        <L7p:key stringValue="some-param1"/>
                        <L7p:value stringValue="some-value1"/>
                    </L7p:entry>
                    <L7p:entry>
                        <L7p:key stringValue="some-param2"/>
                        <L7p:value stringValue="some-value2"/>
                    </L7p:entry>
                </L7p:Parameters>
            </L7p:Encapsulated>
            <L7p:SetVariable>
                <L7p:Base64Expression stringValue="SGVsbG8sIFdvcmxkIQ=="/>
                <L7p:Enabled booleanValue="false"/>
                <L7p:VariableToSet stringValue="some-variable"/>
            </L7p:SetVariable>
        </wsp:OneOrMore>
    </wsp:All>
</wsp:Policy>
```

```
{
  "All": [
    {
      "OneOrMore": [
        {
          "All": [
            {
              "Audit": {}
            },
            {
              "Comment": "Hello"
            }
          ]
        },
        {
          "Comment": "World!"
        }
      ]
    },
    {
      "OneOrMore": [
        {
          "SetVariable": {
            "expression": "1234",
            "dataType": "int",
            "variable": "some-variable"
          }
        },
        {
          "True": {}
        }
      ],
      ".properties": {
        ".left.comment": "This is left comment"
      }
    },
    {
      "OneOrMore": [
        {
          "Include": {
            "policyGuid": "111-12356-789-123",
            "policyName": "some-policy"
          }
        },
        {
          "Encapsulated": {
            "encassGuid": "222-12356-789-123",
            "encassName": "some-encass",
            "parameters": {
              "some-param1": "some-value1",
              "some-param2": "some-value2"
            }
          }
        },
        {
          "SetVariable": {
            "expression": "Hello, World!",
            "variable": "some-variable"
          },
          ".properties": {
            ".enabled": false
          }
        }
      ]
    }
  ]
}
```


BROADCOM SOFTWARE

Throughput Quota Assertion Enhancements for Redis (Preview)

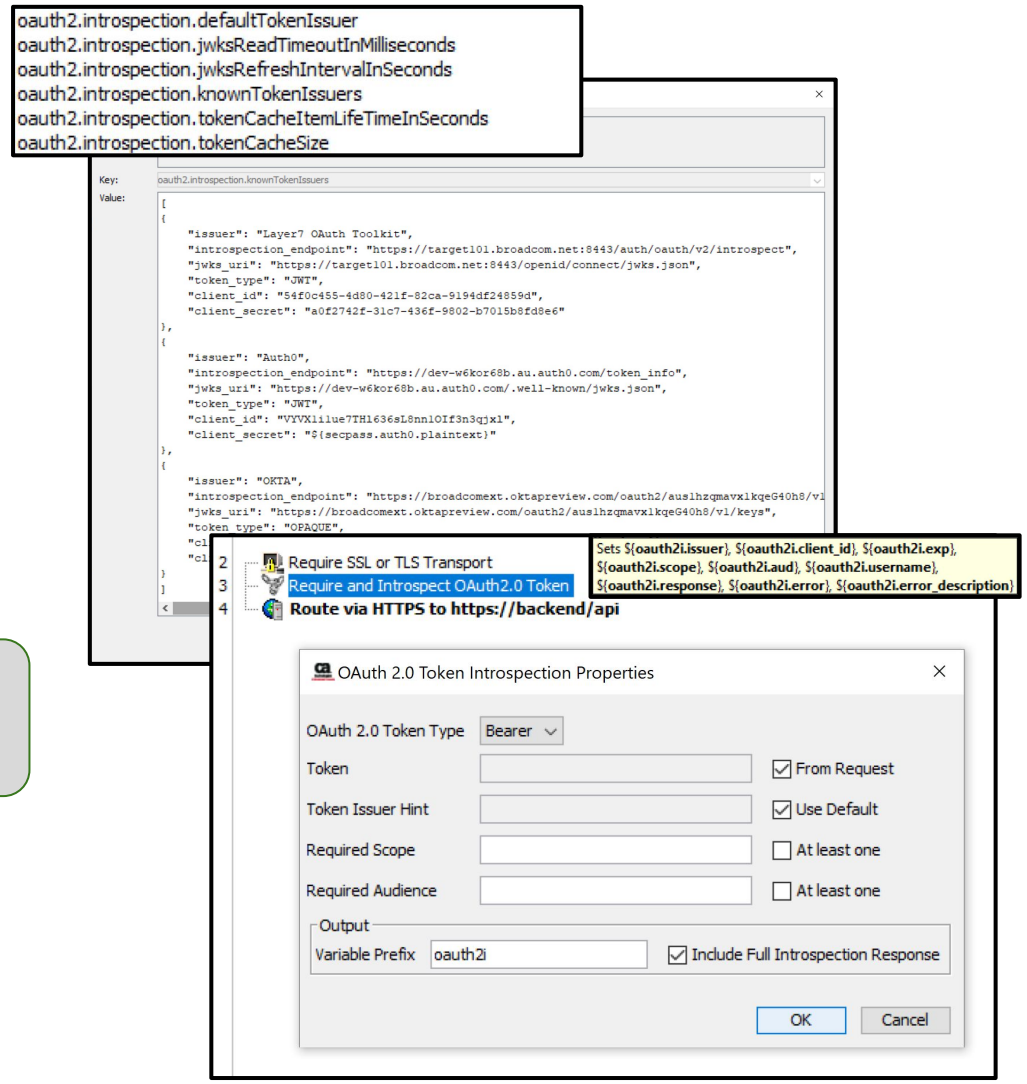
- Shared counters across one or more gateway clusters; and/or cluster-less gateways
- **Within a region** using Lua script with **Redis OSS (Standalone or Sentinel)**
- Across region using active-active enterprise Redis support targeted for 11.1 CR1
- Significantly improved performance (near no op) and accuracy (no leakage or errors; unlike database/Hazelcast when configured for consistency) at scale

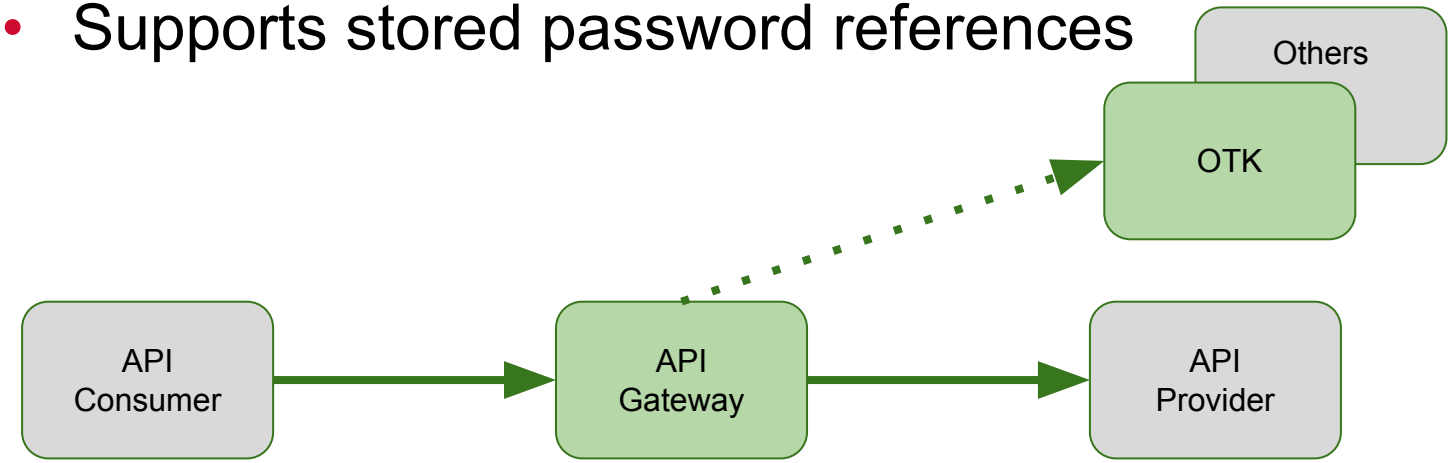


BROADCOM SOFTWARE

Require and Introspect OAuth Token Assertion (Preview)

- OOTB; no OTK install required
- Works with OTK and other OAuth providers
- Works with opaque (introspection) and JWT tokens (validate via JWKS; or introspection if encrypted)
- Supports stored password references

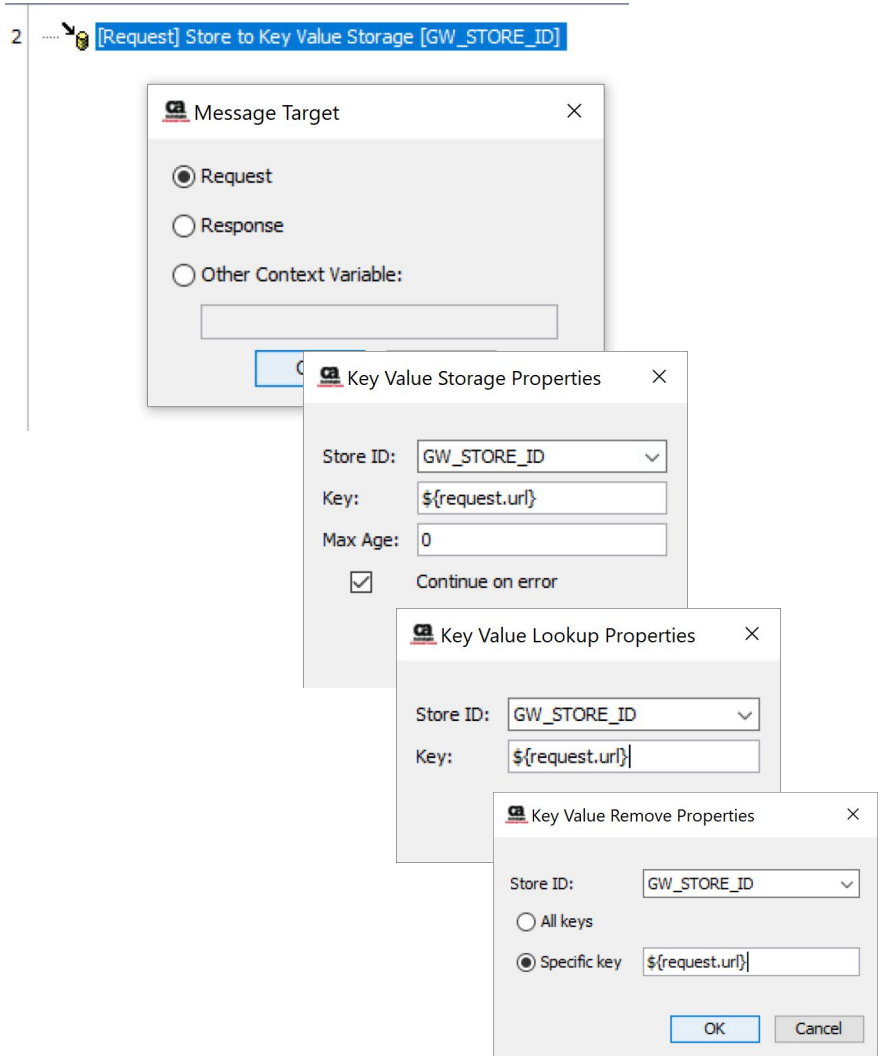




BROADCOM SOFTWARE

Key Value Storage Assertion (Preview)

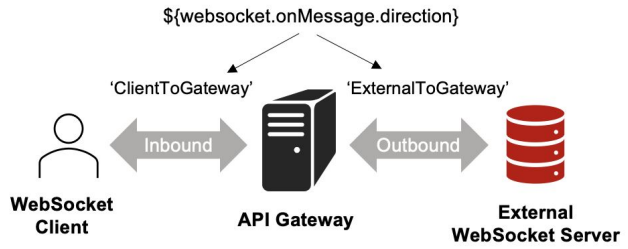
- Three assertions:
  - Store to Key Value Storage
  - Lookup from Key Value Storage
  - Remove from Key Value Storage
- Support for local or remote (Hazelcast or Redis) cache
- Message targetable
- Continue on error
- kvstorage.assertion.status variable (store only; always set)
  - 0 - Success
  - 1 - Invalid Store ID
  - 2 - Max Entries Exceeded
  - 3 - Max Entry Size Exceeded
  - 4 - Unregistered provider [not properly configured; not available]
  - 5 - Invalid key
  - 6 - Invalid max age value
  - 7 - General error (catch all)



BROADCOM SOFTWARE

WebSockets via Shared HTTP Port (Preview)

- Advanced all related features to preview status
- Including these recent experimental additions:
  - Backend (outbound) response message processing
  - Backend (outbound) WSS configuration
    - ***websocket.onUpgrade.connectToServerUseSecure (deprecated; ignored; now automatic based on URI)***
  - Backend (outbound) header manipulation
- New in 11.1:
  - Backend (outbound) client certificate authentication
  - Access headers from saved upgrade event request and response messages
  - Close WebSocket connection with custom codes and message triggers
  - Custom response handling
  - Enhanced error logging



BROADCOM SOFTWARE

Deprecations

- Deprecating, but not removing, the “second” duration of the ***Apply Throughput Quota*** assertion
- Deprecating the X7 and X8 hardware appliance gateway models
  - 11.1 will be the last major release for which hardware appliance gateways will be supported
  - X7 and X8 EOL announcement will be sent at the same time as the 11.1 EOL announcement
    - Major releases normally have a 3 year life
    - EOL announcements normally sent 18 months in advance

BROADCOM SOFTWARE

Upgrade Paths

- Software & Container Gateways
  - Must install JDK17 on software gateway host first
  - Should update PMS for JDK17 before software gateway upgrade
  - Otherwise, standard upgrades
- Appliance Gateways
  - From 10.x to 11.1 using manual expedited upgrade
  - From 11.0 to 11.1 using **in-place upgrade** (or manual expedited upgrade)
  - No new 11.1 ISO for hardware appliances; must first upgrade to 11.0 and then perform in-place upgrade to 11.1

Other

- New known issues should be reviewed in documentation
- New version and upgrade strategy
  - Subminor version number will be used in place of CRs after 11.1 GA
  - For example, our next release will be 11.1.01; ***NOT 11.1 CR1***
  - 11.0 will continue to have CR releases until EOL
  - Allows us to align more with Broadcom's preferred software versioning model
  - Gives us an opportunity to reset standard upgrade procedures to expect database upgrades and possibly platform upgrades during subminor releases
  - In turn, that allows us to remove arbitrary feature design and release limitations
- Layer7 Operator Preview Release (February 12th, 2024)

Thank you

BROADCOM SOFTWARE