SCTE® CABLE-TEC EXPO®
FAST FORWARD 2021

ATLANTA, GA
OCTOBER 11-14

SCTE®
a subsidiary of CableLabs®

UNLEASH THE POWER OF LIMITLESS CONNECTIVITY

2021 Fall
Technical Forum
SCTE® • NCTA • CABLELABS®

Converged Networks and Mobility

Cable and Wireless Subscriber Management Convergence: A common approach to identity management

Pablo Stalteri

Master Solution Architect
HPE Communications Technology Group

Silo approach when deploying OSS platforms for different BUs

Cable & Wireless Operators

- **Different access technologies & BUs need** resulted in the deployment of dedicated systems
- **Wireline, Broadband, Cable TV, IPTV or wireless services, for residential or enterprise customers** led to multiple Billing, CRM, subscriber and identity management systems
- **Technology evolution and tactical execution** methodologies to launch new services contributed to:
  - Different subscriber identification flows for authN & authZ to access each service
  - Plethora of subscriber DBs and data sources

End State:

- Managing and maintaining multiple systems performing similar functions
- Increased OPEX
- Offer different experience to the end customer depending on the service to be used

Subscriber Management Convergence Solution

Increasing flexibility and fast integration with legacy data sources

- Abstracts data models from external applications, offering dedicated views to each of them
- Supports entitlement queries for all type of subscribers: cable, wireline and wireless
- Flexible business logic enabling sequential and/or parallel requests to data sources
- Easy integration with legacy data bases and platforms, with more than 100 protocols available
- No need of data consolidation or data migration
- [illegible]

Challenge

- Integrate Subscriber's Data and Entitlements of all users, from cable, wireline and wireless into a **single platform**
- Changes done on legacy systems (such as Product catalogue QoS upload/download bytes, etc) must **be immediately available** to external applications

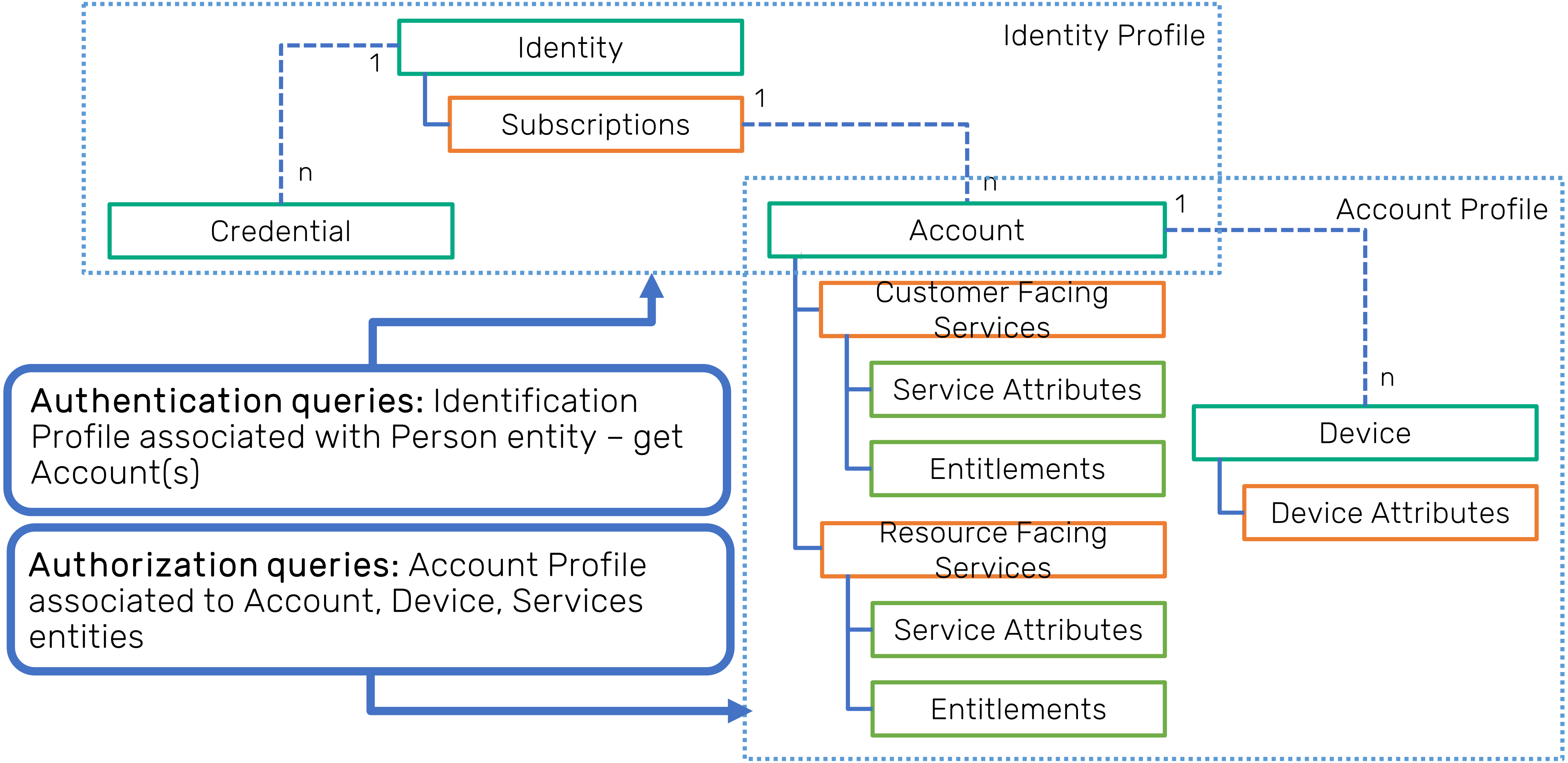
Solution

- Data Federation allows applications to query account, subscriber, service and device information from a set of downstream data sources, being the main one Universal Identity Repository LDAP (ID values)
- Federates external data sources via different protocols, to build a **consolidated XML response**
- Supports AuthN and AuthZ for premium content (Entitlements)

Outcome

- Rapid adaptation to new business cases
- The data federation **abstracts query requests** so that applications do not need to care about data models and/or where data is retrieved
- Reduce implementation and maintenance costs: single platform
- When legacy IDs are maintained, service catalogue **changes** are

Universal Identity Repository (UIR): Subscriber Profile Data



Authentication queries: Identification Profile associated with Person entity – get Account(s)

Authorization queries: Account Profile associated to Account, Device, Services entities

Layered Architecture

API Broker Layer

Logical component that hosts one or more API broker components. It provides the HTTPS/REST based interfaces to which North Bound applications can authenticate, connect and query

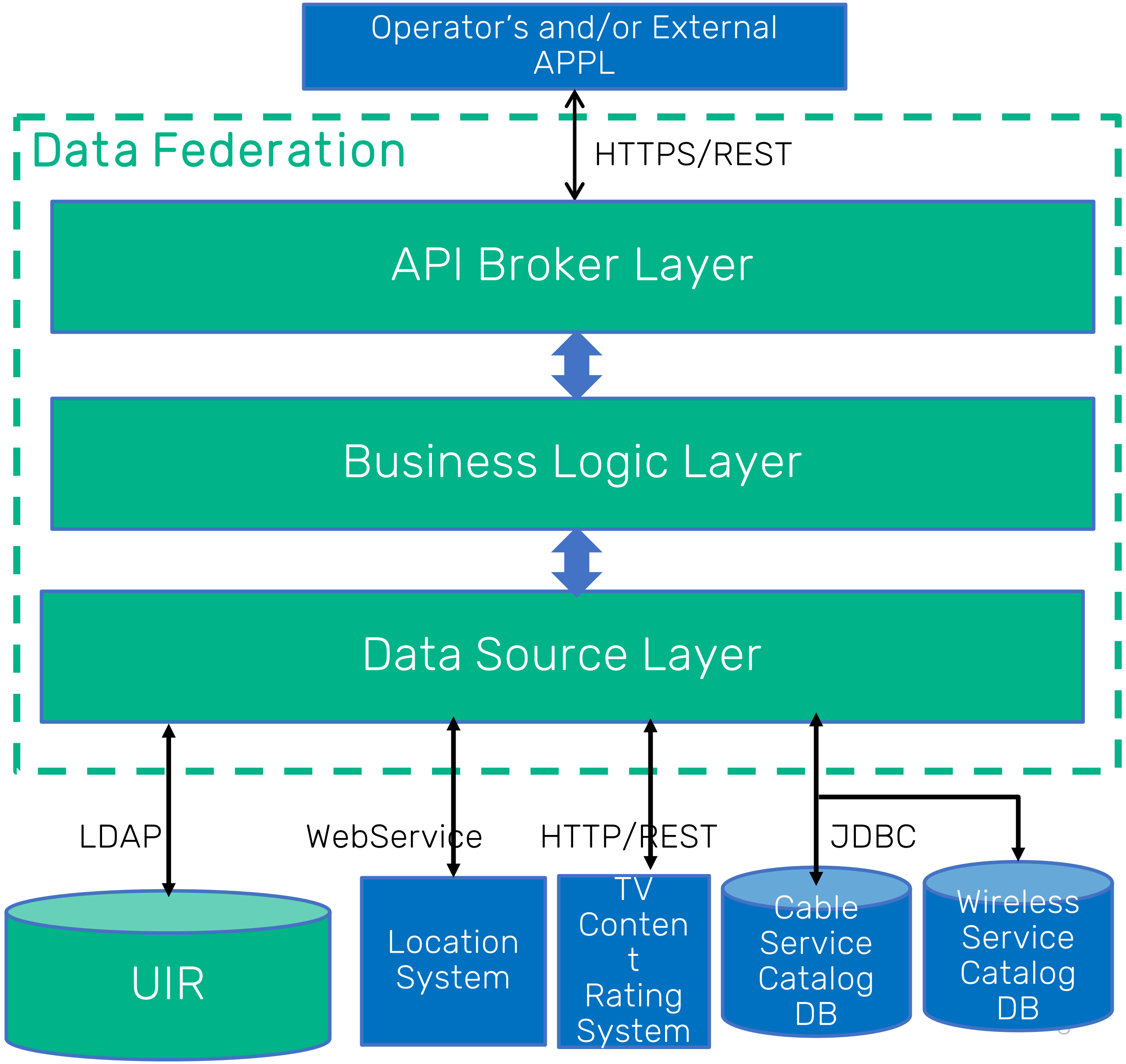
Business Logic Layer

Based on API request triggers the flow selecting the Data Sources to consolidate the dedicated response:

1. Flow execution order in which each corresponding query needs to be executed according to business logic
2. Query in parallel / sequential for Data Sources/protocols
3. Receive response from all Data Sources and keep them in memory
4. Compose all answers into a virtual data model to create the XML response (Payload)

Data Source Layer

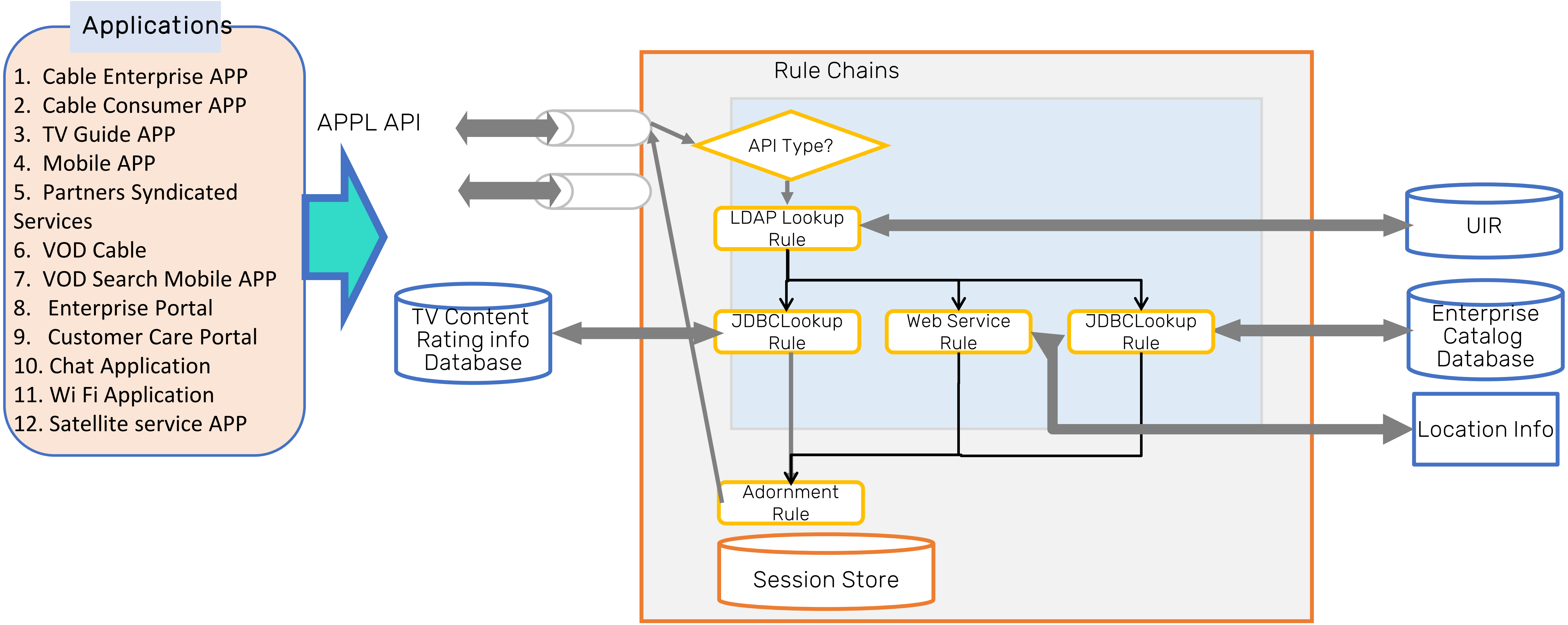
Set of out of the box connectors to interface with each Southbound DataSources (ex. LDAP, JDBC, WebServices, HTTP/REST, SOAP/XML, etc) to acquire relevant information



Data Federation

SCTE. CABLE-TEC EXPO
ATLANTA, GA > OCTOBER 11-14

API Sample

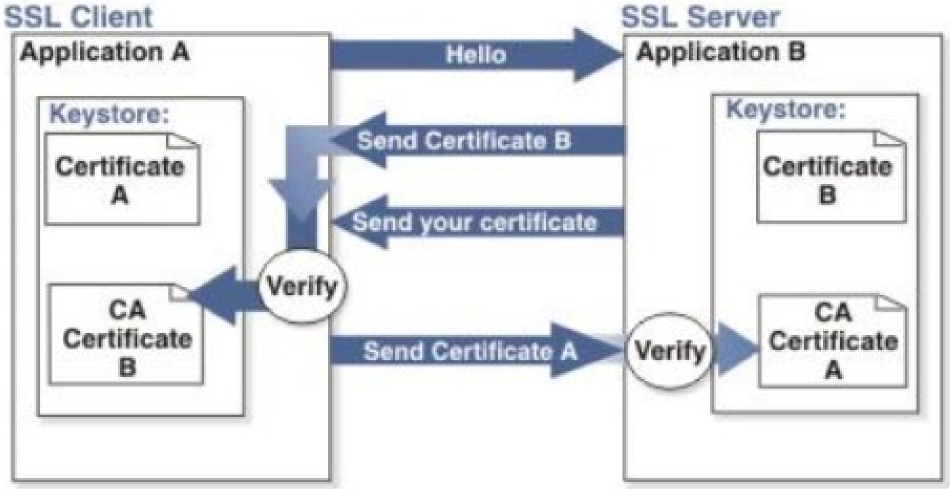


Data Federation Key Features

- Real Time Protocols for both Northbound and Southbound interface: HTTPS, REST, SOAP, JDBC, LDAP, Diameter, RADIUS client/server/proxy with advanced access control, TLS support
- Messaging format supported: XML, JSON, HTML
- Supports synchronous and asynchronous requests
- Onboarding of Consumer Applications: Who access What attribute with What API
- OOB GUIs: Data Modelling Studio, Configuration Editor, File Service Workflow, Rule Chain Visualization, App Deployment Visualization, Operations Console, Deployment Manager, O&AM Workflow, Common Codec Framework
- NFV ready and cloud scalability: Level 3 Scale in/out
    - Dataless Micro service architecture, paving the way to 5G and Wi-Fi 6
    - VNF Manager (new component for NFV/MANO integration) and O&AM Workflow
    - EMS Management enhancement: NFV Templates and Operations Console Extensibility
    - Load Balancer for Real Time
- Management enhancement: statistics threshold with alarm, resource utilization chart, SNMP v2c and v3 support, Management HA support
- Reference Data Manager and Services enhancement: extend control for admin to manage reference data that drives business logic, advanced querying and caching

Data Federation: Access Control Logic Feature

- Allows only **trusted clients/applications** to access UIR DF by providing mutual authentication using HTTPS Two-Way SSL
- Authenticates and Authorizes the users accessing UIR DF by checking against its LDAP database where user information, credentials and user's **access control list** (user, roles and privileges objects) data is stored
- Provides **secure communication channel** between the clients and UIR Data Federation platform: TLS 1.2



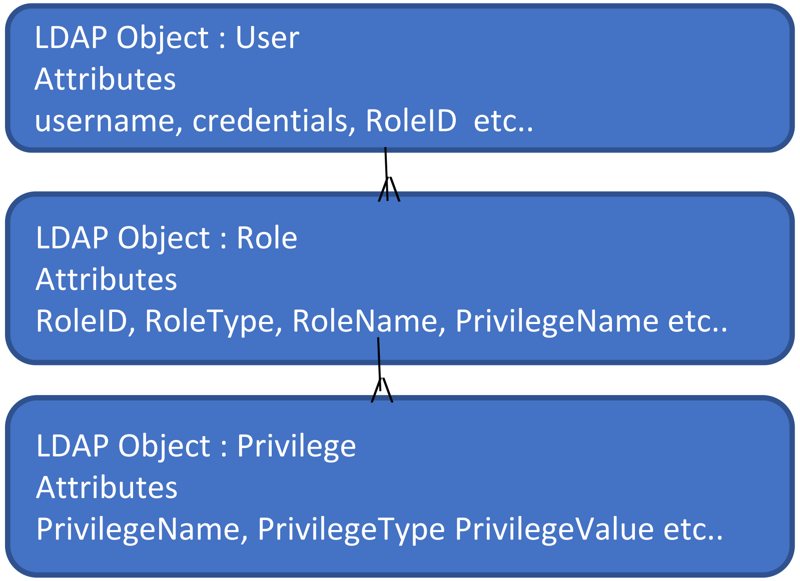
Details

○ Data Federation leverages UIR LDAP Database where the Access Control List (ACL) for a User is stored

○ ACL consists of UserRole, its Privileges and other artifacts

○ Data Federation will provide only those information elements to user based on Access Control List

○ All client applications accessing Data Federation must provide user credentials in HTTP Authenticate Header as per RFC 2617



LDAP Object : User
Attributes
username, credentials, RoleID etc..

LDAP Object : Role
Attributes
RoleID, RoleType, RoleName, PrivilegeName etc..

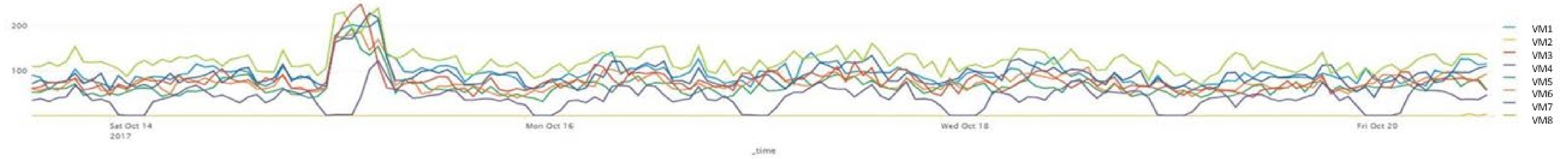
LDAP Object : Privilege
Attributes
PrivilegeName, PrivilegeType PrivilegeValue etc..

Performance Metrics: Operator with 3M Subscribers - Payload

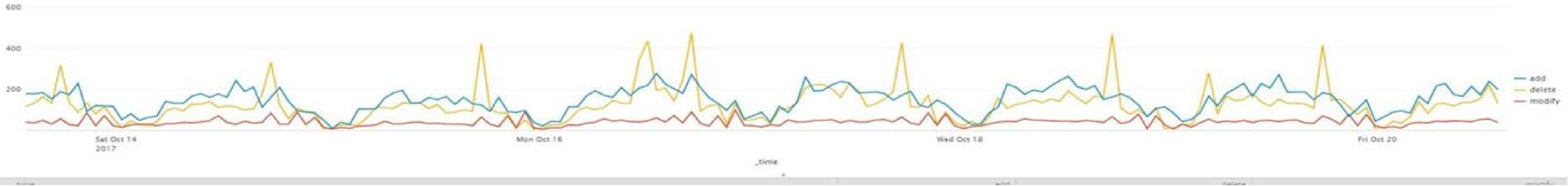
View	Average TPS	Max TPS	Average Response Time (ms)	Payload size
Account Lite View	5	80	75	Average – 405KB
Account View	19	300	200	Max- 3.3MB
Person View	7	20	10	Average – 1KB Max- 30KB
Mobile App View	4	73	188	Average – 2.5KB Max- 8KB
TV Guide View	9	290	200	Average – 18KB Max- 224KB
VOD Auth View	24	47	140	Average – 3.5KB Max- 17KB
Wifi View	2	26	2	Average – 1.3KB Max- 5KB
TOTAL	**70**	**500**		

Performance Metrics: Operator with 3M Subscribers – LDAP

LDAP Reads: Peak 1,202 TPS



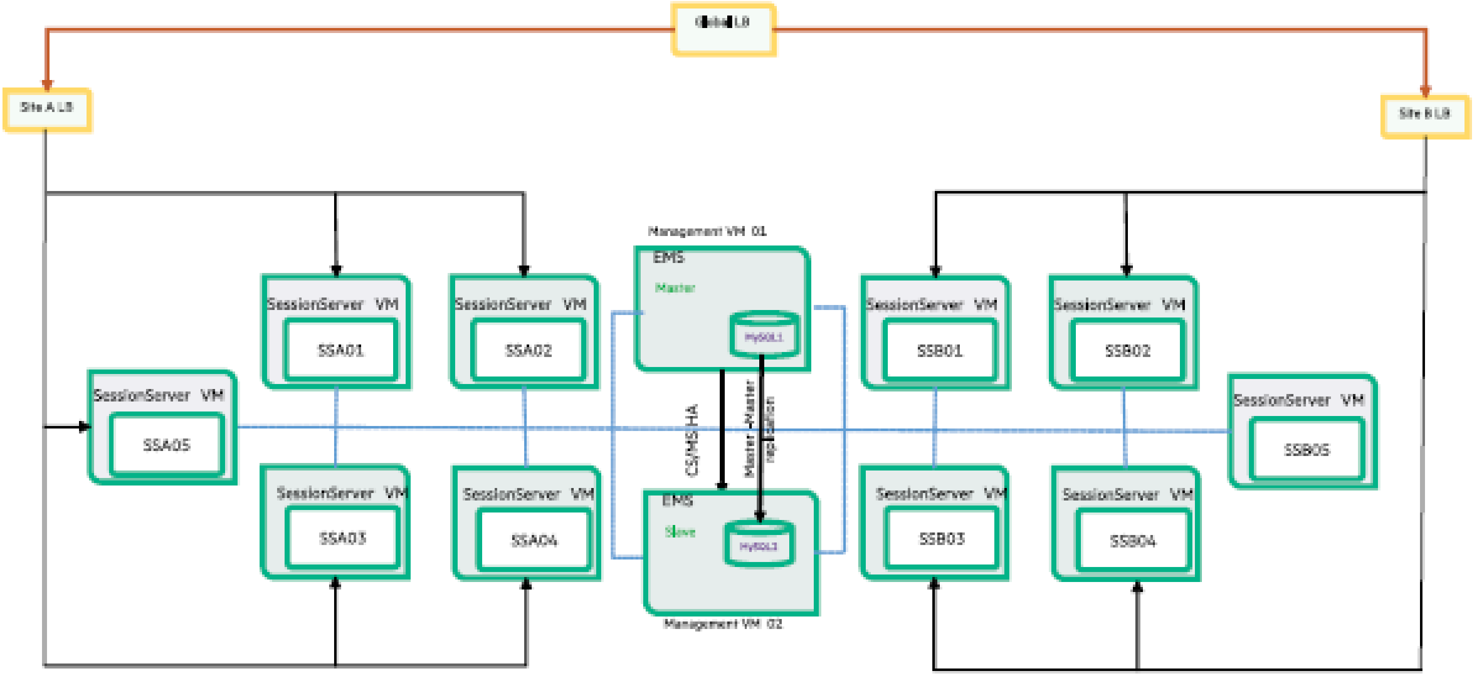
LDAP Writes: Peak 800 TPS (400TPS DEL + 300TPS ADD + 100TPS MODIFY)



Sample Production Deployment: Operator with 3M Subscribers

- Two identical sites
- Each site with 5 Session Servers VMs and 1 EMS VM, supporting up to 500TPS query
- Each VM with one Session Server containing the 3 layers: API Broker, Business Logic and Data Source Layer

	vCPU	vRAM (GB)	Disk (GB)
VM supporting 100 TPS	8	16	200
OS	RHEL 7.5 (x86-64)		
Hypervisor	VMWare		



- Multi site deployment is achieved with built in HA, that is, there is no need for third party clustering software (i.e. Red Hat Clustering)

- EMS: Single Config Server (CS) and Management Server (MS) run on HA mode with a replicated master-master MySQL database

Thank You!

Pablo Stalteri (pablo.stalteri@hpe.com)

Master Solution Architect
HPE Communications Technology Group