
ORACLE®

Oracle REST Data Services

CON6667 Securing Your RESTful Services

Colm Divilly
Consulting Member of Technical Staff
Oracle, Database Tools

October 03 2017

ORACLE OPEN WORLD

October 1–5, 2017
SAN FRANCISCO, CA

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Oracle Database Exadata Express Cloud Service

Cloning & Lifecycle Management

ORACLE OPEN WORLD

October 1–5, 2017
SAN FRANCISCO, CA

Tuesday, 3:45-4:30
Moscone West,
Room #3012

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

CON6667 - Securing your RESTful Services - Agenda

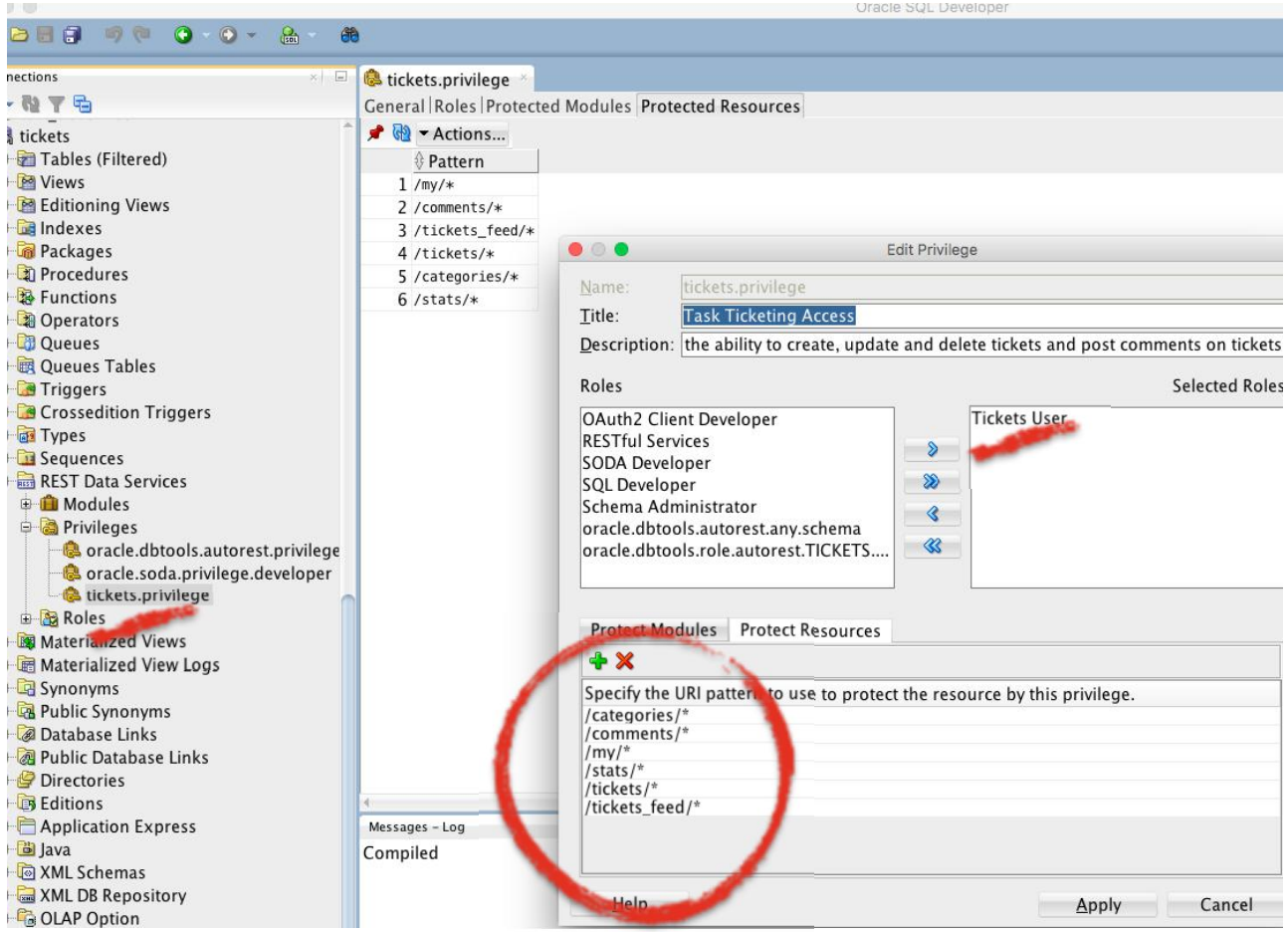
1. Protecting ORDS RESTful Services with Privileges and Roles
2. Integrating ORDS with your Enterprise security solution
3. ORDS out of the box security solutions
4. Using HTTPS with ORDS
5. One more thing... ;-)

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Protecting REST Services with Privileges and Roles

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Defining Resource Privileges



- Using SQL Developer you can view the **Privileges** defined for a schema
- You can also query the underlying views: **USER_ORDS_PRIVILEGES**, **USER_ORDS_PRIVILEGE_MAPPINGS**, **USER_ORDS_PRIVILEGE_ROLES**
- Similarly you can create/update/delete privileges using SQL Developer or **PL/SQL API**
- A user must have **at least one of the required roles** to be granted access

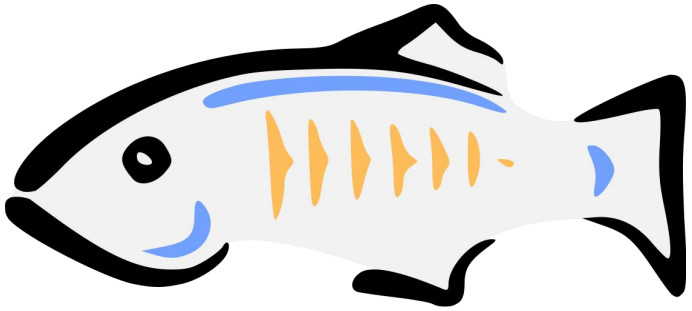
Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Integrating with Enterprise Security Solutions

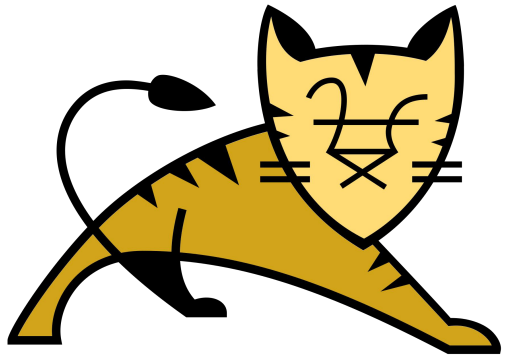
Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The Preferred Solution

Delegate to the Application Server



ORACLE
WebLogic



- Application Servers have a wealth of security solution integrations
- ORDS has built in support for retrieving the user identity from Apache Tomcat, Oracle Glassfish and Oracle WebLogic
- Challenges: No one size fits all solution, multitude of approaches, not clear which is best choice. Integrations often require expertise to configure

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Enterprise Intergration - Case Study

Oracle Database Cloud

- Oracle Database Cloud **Schema as a Service** and **Exadata Express** products are web based cloud databases, with ORDS powering the web interface
- Need to integrate ORDS with the Cloud security solution, **Oracle Identity Manager**
- **OHS, WebGate and WebLogic** all sit in front of ORDS and take care of all authentication of users
- All that is required on ORDS side is to configure ORDS to enable WebLogic to propagate user identity to ORDS

```
java -jar ords.war oam-config
```

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The Alternative Integration Option

Use Custom HTTP Request Headers to share user identity with ORDS

- Assume there is some **middleware** sitting in front of ORDS. The purpose of this middleware is to authenticate and identify user and their roles.
- When user is succesfully authenticated then it must **add additional headers to the request** that indicate to ORDS the user's identity and roles
- Middleware **must be locked down to prevent an attacker spoofing these headers!**
- We call this feature **External Session Authentication**

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Configuring External Session Authentication

- Add 3 settings to defaults.xml:
  - *security.externalUserHeader* - The name of the header that identifies the user
  - *security.externalRolesHeader* - The name of the header that identifies user roles (comma delimited)
  - *security.externalSessionTrustedOrigins* - The set of Origins trusted to make cross-origin requests to this server

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Out of the Box Security

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Out of the Box Security Functionality

Built in Security Functionality that Oracle REST Data Services provides

- **OAuth 2.0** Support
  - Client Credentials
  - Implicit Grant
  - Authorization Code
- **HTTP Basic** (over HTTPS) support - use strongly discouraged
- **Cookie** based first party app authentication
  - Stateless encrypted cookie for the same Origin that ORDS is hosted on
- Deep Cross Origin Request Sharing (**CORS**) Support

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Using HTTPS

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Using HTTPS

HTTPS is now ubiquitous, and required

- If you don't know about **LetsEncrypt**, you should! Provides automated **free** HTTPS certs to any public Internet connected web-site. **No more $$$ for HTTPS certs**
- Any REST API endpoint **MUST** use HTTPS to keep data secure
- ORDS **Standalone Mode** supports **user provided certs** and **auto generated self signed certs**

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

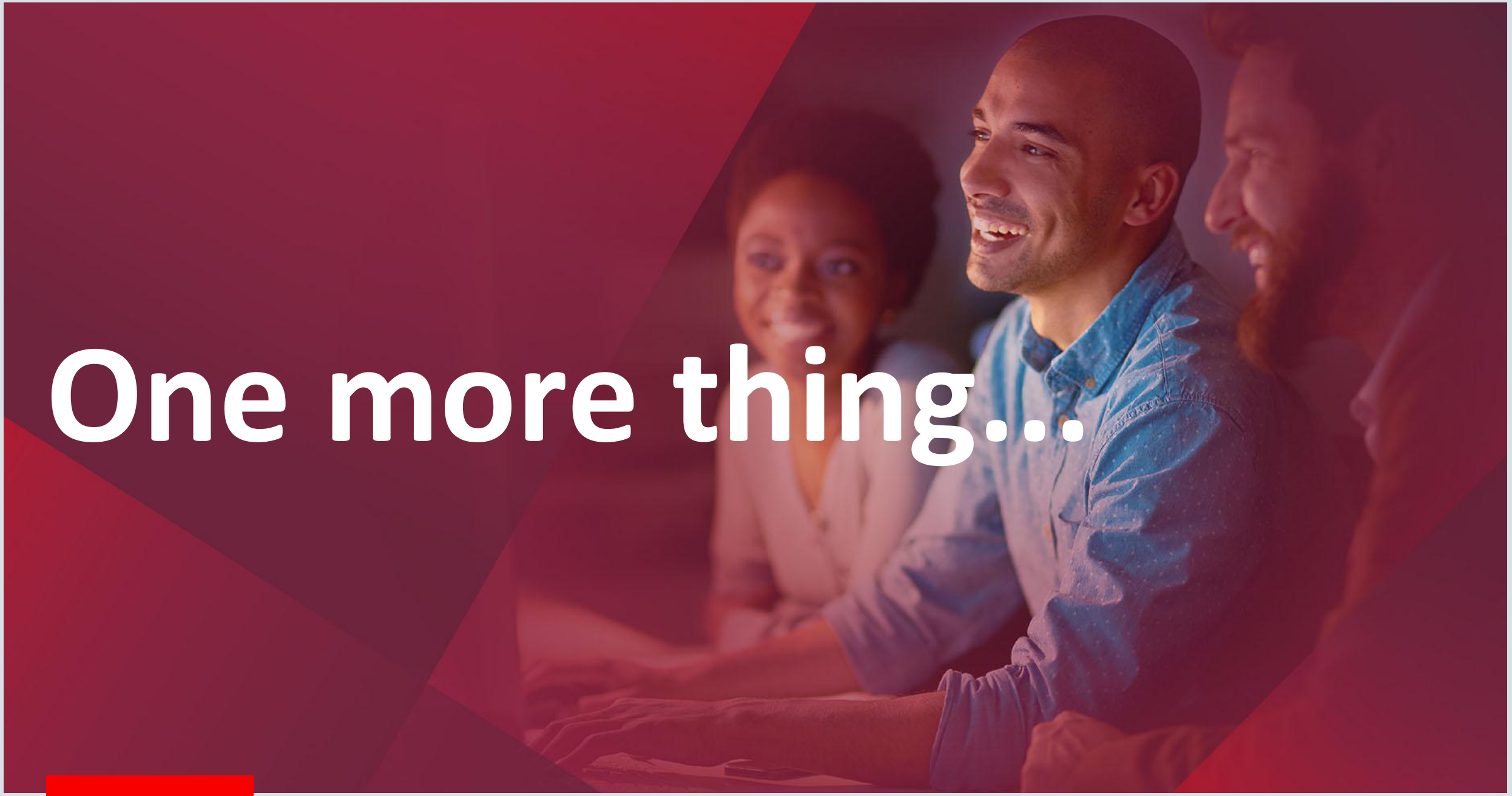
Standalone Mode & HTTPS Support

User defined certificate

- Need PEM encoded Certificate file and unencrypted PKCS8 PEM encoded private key
- Place both files in a suitable location. Use file permissions to restrict access
- Either:
  - Specify location when prompted during setup
  - Pass the locations via Java System properties
    - -Dssl.cert=/path/to/host.crt, -Dssl.cert.key=/path/to/host.key

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

One more thing…



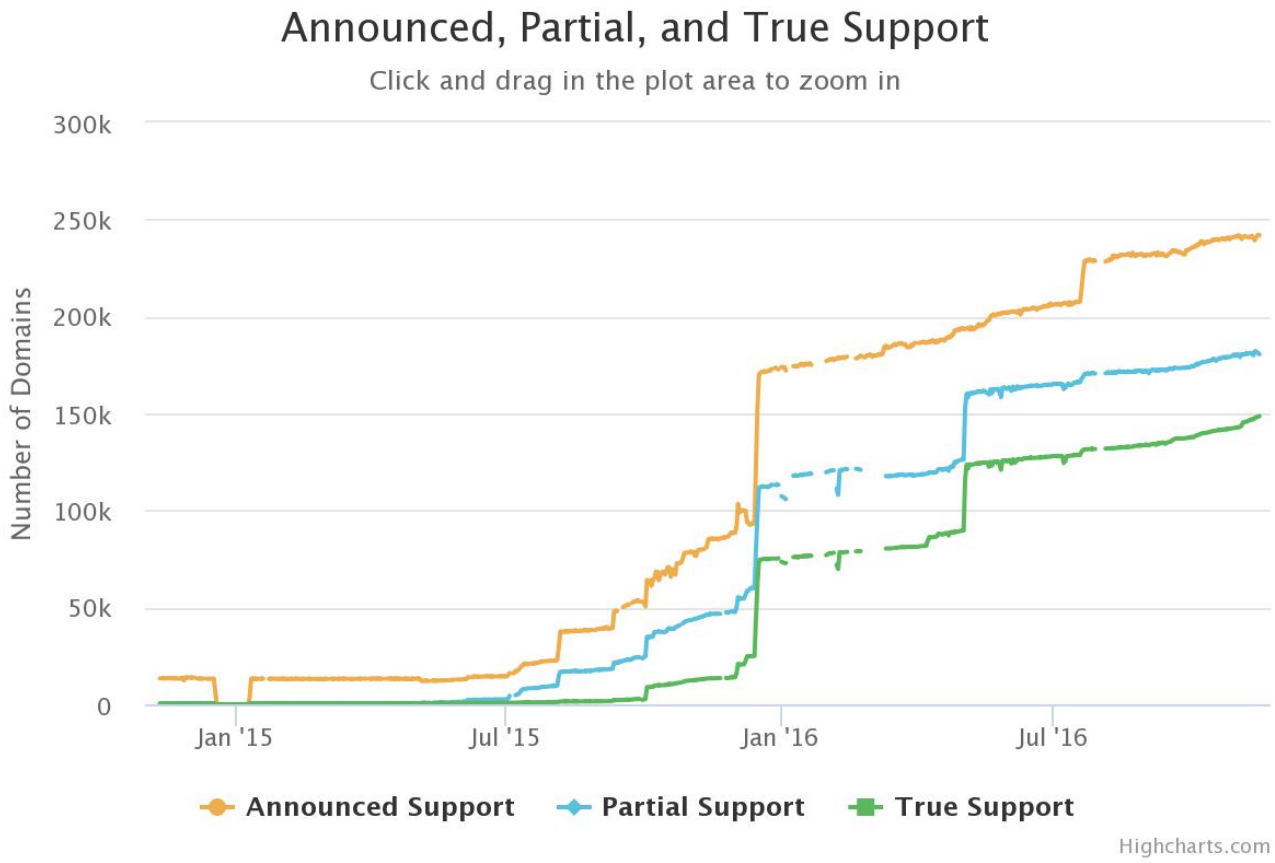
Copyright © 2017, Oracle and/or its affiliates. All rights reserved. |

HTTP/2 Support is Incoming!

The upcoming ORDS release will support HTTP/2 when running on JDK 9

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The Web never stops evolving



- **HTTP/2** is already in use with top tier sites and CDNs. Google, Facebook, Cloudflare etc.
- From 0 to 100K sites in a year
- Offers significant **performance improvements** over HTTP/1.1
- ORDS is committed to keeping pace as the Web evolves, so we are delighted to build atop the HTTP/2 support in **Java JDK 9**
- Also supports **cleartext HTTP/2** to facilitate TLS termination at **load balancer**

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

HTTP/2 Support

- HTTP/2 Support is provided for Standalone Mode.
- Just works out of the box on JDK 9
  - HTTP port will negotitate HTTP/1.1 or HTTP/2 cleartext
  - HTTPS port will negotiate HTTP/1.1 or HTTP/2 ciphertext
- Tomcat 9 and GlassFish 5 also offer HTTP/2 support, haven't had chance to test yet!
- Try it out today: Download new 17.3 Beta from https://oracle.com/rest

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Integrated Cloud

Applications & Platform Services

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.


ORACLE®