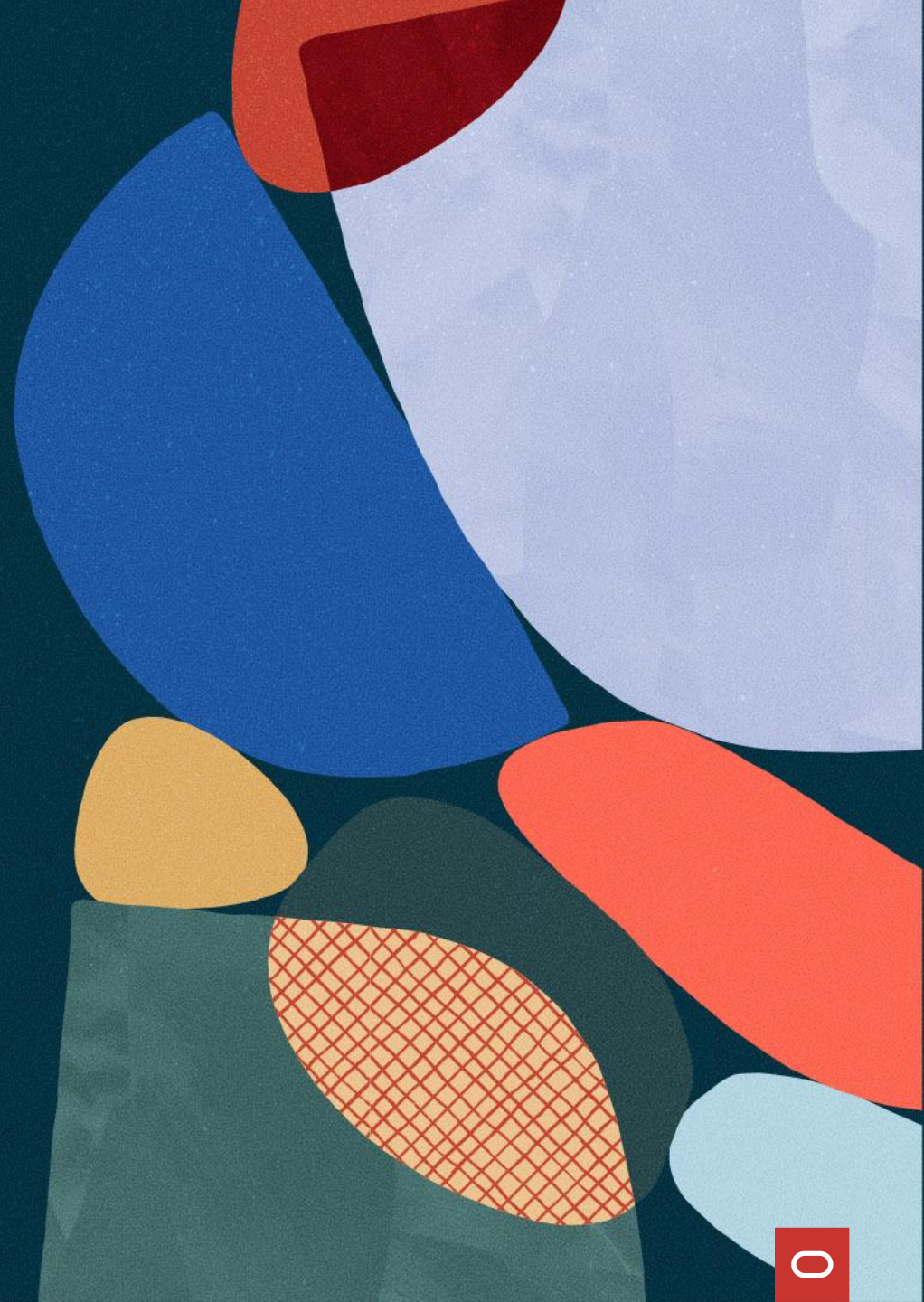
ORACLE

Build With Oracle AI Database and ORDS MCP Servers

Derrick Cameron, Master Principal Cloud Architect
Steven Nichols, Master Principal Cloud Architect

Virtual Code Innovate Team

September 2026



Agenda

- ✓ Overview of Oracle AI Database MCP ServersHow MCP Server Fits in with Other ADB AI Services
- ✓ OCI Managed MCP Server configuration and user experienceMCP Client Configuration
- ✓ ORDS MCP Server configuration and user experience
- ✓ Code Innvovate Program

Copyright © 2025, Oracle and/or its affiliates

Previous Webinars Related To These Topics

- February 2022 – Database Access with IAM Credentials and Security Policies to Access Data
- May 2026 – ADB MCP Server

Copyright © 2025, Oracle and/or its affiliates



Model Context Protocol (MCP) Overview

Copyright © 2026, Oracle and/or its affiliates

Model Context Protocol Servers

- Model Context Protocol Servers provide
  - Resources – Static items such as documents, images, files
  - **Tools** – Essentially a function call with input/output arguments
  - Prompts – Prompts to give to the LLM for use

- Server Architectures
  - Local
  - Remote
  - STDIO vs HTTPS

- Oracle Reference MCP Servers:
  https://github.com/oracle/mcp/tree/main/src

Resource

```
{
  contents: [
    {
      uri: string;        // The URI of the resource
      mimeType?: string;  // Optional MIME type

      // One of:
      text?: string;      // For text resources
      blob?: string;      // For binary resources (base64 encoded)
    }
  ]
}
```

Prompt

```
{
  name: string;              // Unique identifier for the prompt
  description?: string;      // Human-readable description
  arguments?: [              // Optional list of arguments
    {
      name: string;          // Argument identifier
      description?: string;  // Argument description
      required?: boolean;    // Whether argument is required
    }
  ]
}
```

Tool

```
{
  name: string;          // Unique identifier for the tool
  description?: string;  // Human-readable description
  inputSchema: {         // JSON Schema for the tool's parameters
    type: "object",
    properties: { ... }  // Tool-specific parameters
  },
  annotations?: {        // Optional hints about tool behavior
    title?: string;      // Human-readable title for the tool
    readOnlyHint?: boolean;    // If true, the tool does not modify it
    destructiveHint?: boolean; // If true, the tool may perform destru
    idempotentHint?: boolean;  // If true, repeated calls with same ar
    openWorldHint?: boolean;   // If true, tool interacts with externa
  }
}
```

Copyright © 2026, Oracle and/or its affiliates

Four MCP Deployment Models

	SQLcl	ADB	OCI Managed	ORDS
What it is	A local, STDIO MCP server that runs on the user's machine that is included with SQL Developer for VS Code.	A streaming HTTPS MCP server connected to your AI Database	A streaming HTTPS MCP server that allow a user to define MCP Tools and roles for any Oracle AI Database running in your cloud tenancy	A streaming HTTPS MCP Server that ties into a customer's preferred identify management.
Best fit	Devs, dbas, power users – people already working directly with your databases	Business users, analysts, support teams, shared AI agents, developers	Business users, analysts, support teams, shared AI agents, developers	Dev, DBAs, power users
Ideal workflow	Local database exploration, dev, or troubleshooting	Easiest way to expose AI Agent tools	Governed natural language access to approved databases, validated reports, and sql tools	Governed natural language access to approved databases, and sql tools
Tools	List connections, connect, run-sql, run-sqlcl, schema info	AI agent tools (none OOTB)	Built in tools (sql-run, Schema Information, custom), reporting tools, and custom tools	sql, pl/sql, schema discovery, database discovery
Access model	DB credentials avail to the local OS user	OAuth2/token as database user	OAuth2, OCI Identity, federated users, IAM groups, MCP roles	OAuth2, JWT with scopes or roles from your identity provider of choice

OCI Managed MCP Servers

A fully managed, HTTPS MCP endpoint built into the OCI Database Tools Service. Serverless, no patching, full Oracle Premier Support — business users can **chat with their Oracle AI Database in plain language** via any MCP-compatible AI client. Validated named SQL Reports enables governed, repeatable results.

Enterprise Security

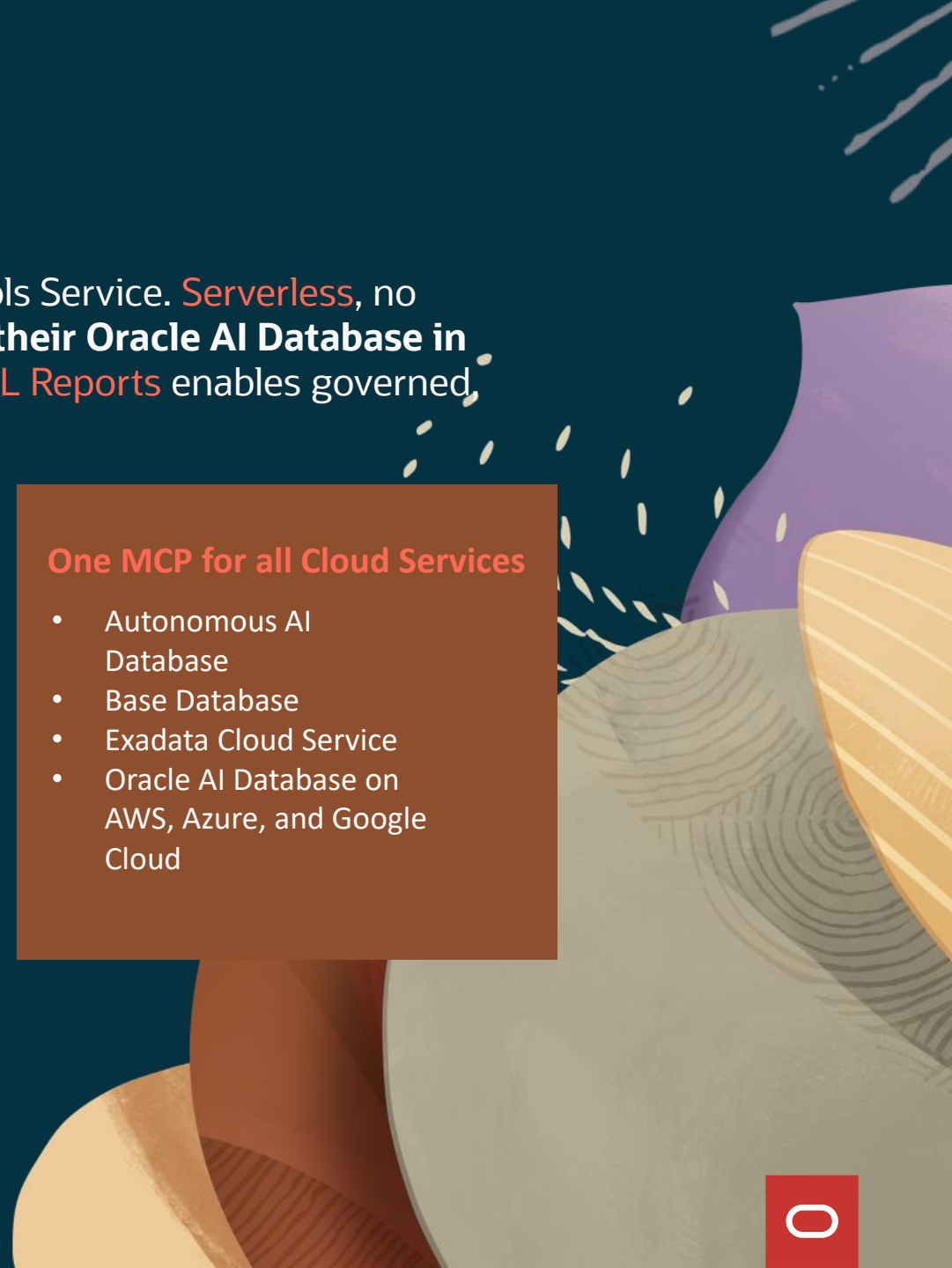
- OCI IAM auth via OAuth2
- Federate Azure Entra ID, Okta, etc
- Application roles control exactly who can run what

Easy to Deploy

- Enable it in the OCI Console.
- Built on the existing DBTools Connection
- Pay only for the database resources you consume.

One MCP for all Cloud Services

- Autonomous AI Database
- Base Database
- Exadata Cloud Service
- Oracle AI Database on AWS, Azure, and Google Cloud



Copyright © 2026, Oracle and/or its affiliates

MCP Server Toolsets – you have complete choice!

You can deploy any one or combination of these tools.

Built-in SQL tools

Ad-hoc, NL2SQL focused, allows an Agent to execute any Oracle SQL or PL/SQL code it has generated.

- dbtools_execute_sql
- dbtools_get_tool_request
- dbtools_schema_information

Reporting tools

Curated, parameterized queries published as governed, callable tools.

- dbtools_list_reports
- dbtools_execute_report
- dbtools_get_report_sql

Available reports controlled by authenticated user's Group membership.

Custom Tools

Predefined, parameterized SQL or PL/SQL scripts to implement your database operations.

- your_tool_name

Want your Agent to be able to cancel any query, reset a password, or run your favorite script? Build your own tool!

Copyright © 2026, Oracle and/or its affiliates

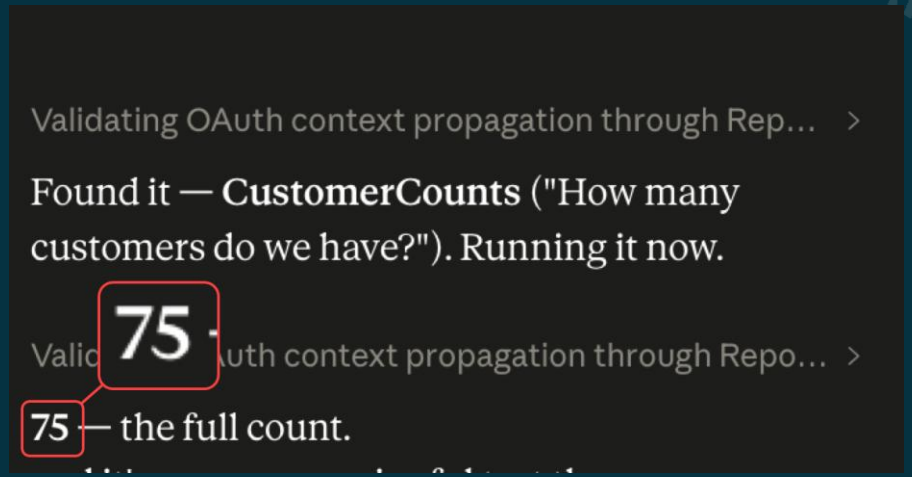
One Identity, End to End

MCP Server propagates the OAuth2 client/user's information to the Database (V$SESSION, Session Contexts)

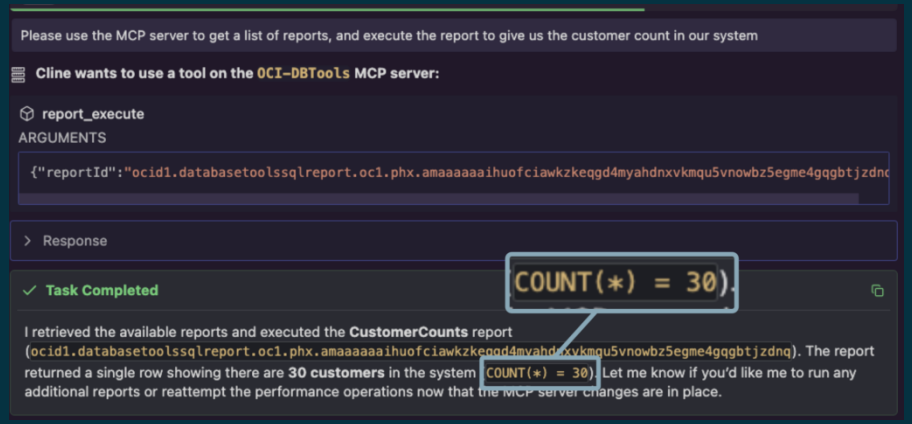
1. Database connection requested
   a. MCP server creates conn, w/USERENV & CLIENTCONTEXT populated
   b. Includes OAUTH info, including user & client details
2. Database security policy defined for schema and appropriate tables
3. Database automatically filters out PII

The database knows that DB userX is connected, and that the end user jeff.d.smith@oracle is running queries via AI Agent Y.

Administrator asks question, routed to report



Biz Analyst asks same question, via same report



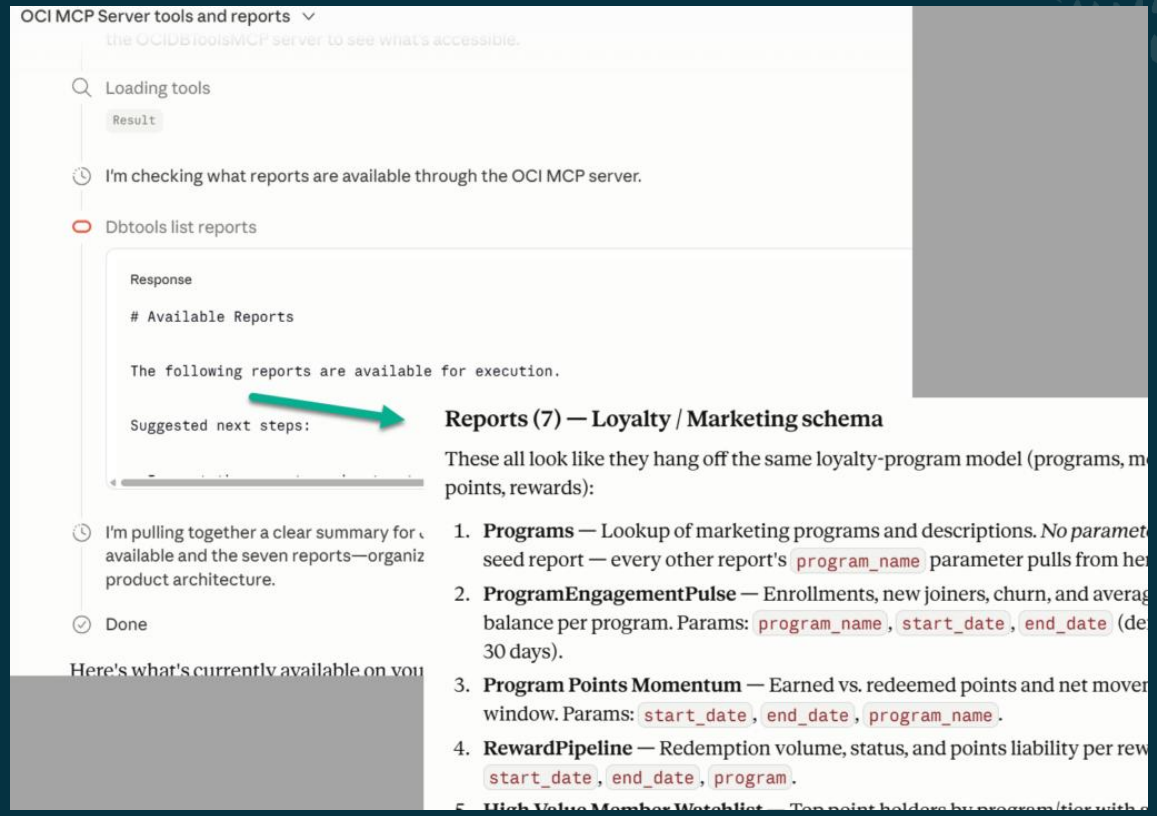
Copyright © 2026, Oracle and/or its affiliates

Reports provide reliability, trust to the Natural Language AI conversations

You no longer need to worry about the Agent/LLM generating the correct SQL, only to pick the right report!

OCI SQL Reports, accessible via MCP Tools

1. Administrator creates reports
   - Trusted, validated SQL
   - Named, documented (when to use, what questions are answered)
   - Parameterized – variables permit questions like, last X days
2. Report access via role
3. Agent gets question, peruses reports
4. Runs report, always same SQL



Your organization already has many of these reports, now they can be utilized via AI.

Copyright © 2026, Oracle and/or its affiliates

Is OCI Managed MCP right for me?



	OCI Managed MCP
Best fit	Business users, analysts, support teams, shared AI agents, developers
Ideal workflow	Governed natural language access to approved databases, validated reports, and SQL tools
Transport	Streaming HTTPS
Connection model	OCI Database Tools Connections, passwords in OCI Vaults / stateless
Access model	OAuth 2.0, OCI identity, federated users, IAM groups, MCP roles
Tools	MCP Servers, Toolsets, run-sql, list reports, run reports, SQL Reports
Operational model	Managed, serverless cloud service
Database reach	Any Oracle AI Database in OCI, Oracle @ AWS, Azure, GCP

Copyright © 2026, Oracle and/or its affiliates

Oracle REST Data Services (ORDS): Remote Streaming HTTPS

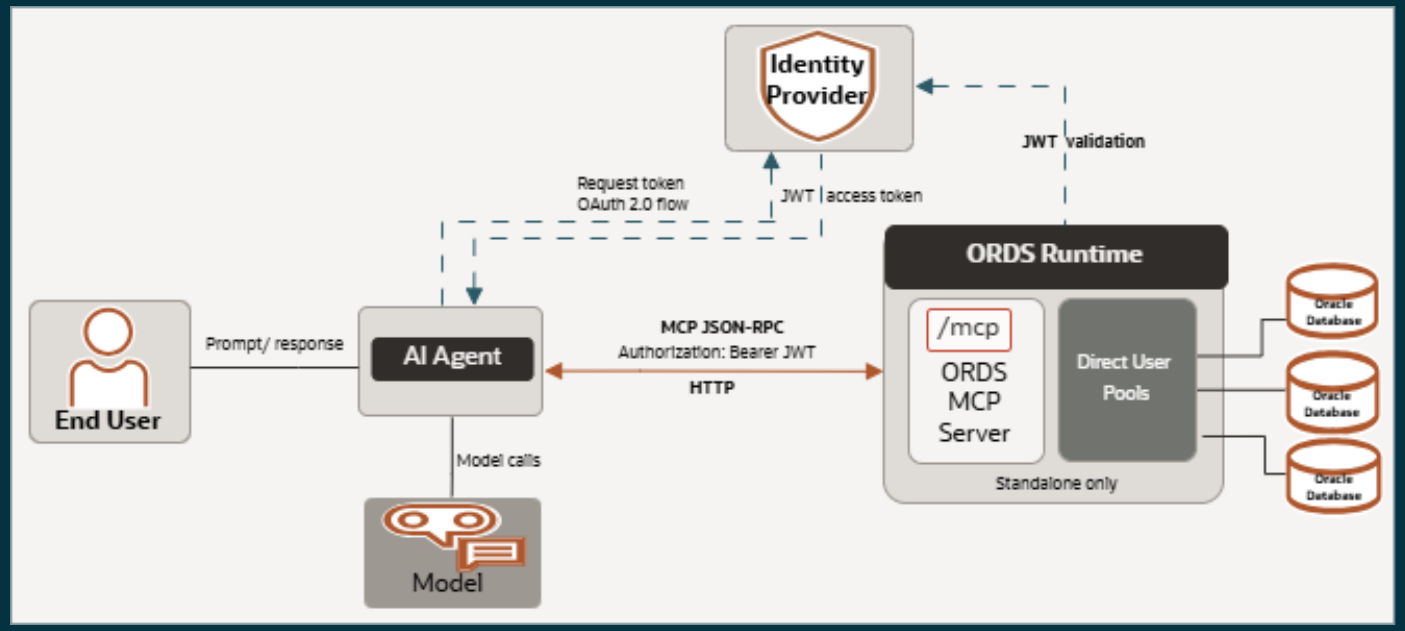
- Established, well-known mid-tier solution, debuted in 2010
- Supports every version of Oracle, for EVERY environment
- FREE
- 📢 **/mcp** endpoint available, minVer 26.2
- ALSO serves up -
  - Database REST APIs
  - Oracle APEX applications
  - SQL Developer Web
  - Oracle Backend for Firebase (BaaS)
  - Database API for MongoDB
  - Vector DB / AI Vector Search APIs



Powered by Oracle REST Data Services {ORDS}

Copyright © 2025, Oracle and/or its affiliates

ORDS serves /mcp endpoint, handles multiple databases



- ***No database install required***
- Connections are direct, not proxy (e.g. ORDS_PUBLIC_USER for REST APIS)
- MCP feature is opt-in
- Bring your own Identity Provider (JWT)
- Fully OAuth compliant to MCP Spec
  - Supports dynamic client registration!
- Stateless/Autocommit

MCP Server Tools

Built-in SQL tools

- database_list
- run_sql
- schema_information

What is databse_list ?

- ORDS maintains connection pools, serving either REST or MCP
- MCP pools are retrieved along with descriptions
- Agents discover what databases are available, name included on subsequent tool requests

Copyright © 2026, Oracle and/or its affiliates

ORDS and MCP Auth

ORDS acts as an OAuth-protected resource server for /mcp — auth and audit extend all the way into the database

OAuth-Protected Resource

- ORDS validates JWTs
- Bearer token required for all /mcp calls
- Unauthenticated calls receive 401 + discovery hint

Enterprise IDP Integration

- RFC 9728 protected-resource metadata at /.well-known/…
- Supports any IdP that issues standard JWTs
- Dynamic Client Registration reduces admin overhead

End-to-End Audit Trail

- JWT identity propagated to CLIENTCONTEXT
- Calls written to DBTOOLS$MCP_LOG
- REQUEST_ECID links DB evidence back to ORDS logs

📢 One ORDS instance can serve multiple MCP database connection pools. ORDS can be clustered, front-ended with a load balancer, supports Data Guard for high availability and failover.

Copyright © 2026, Oracle and/or its affiliates

ORDS MCP Authorization via JWT claims

Every connection resolves through two configurable layers — a global default, refined per connection pool

LAYER 1 — GLOBAL APPLICATION SETTING

Applies to every connection pool, unless overridden below.

`jwt.profile.role.claim.name` set?

YES → use named role claim

NO → fall back to scopes

LAYER 2 — POOL-LEVEL OVERRIDE

Set a tighter requirement for specific connection pool — three equivalent ways to express it:

CUSTOM SCOPE

`mcp.scope=pools:sales`

Scope minted specifically for this pool

GLOBAL SCOPE

`mcp.scope=urn:oracle:dbtools; ords.mcpserver:all`

Accept the broad, server-wide scope

REQUIRED ROLE

`mcp.role=POOL.SALES`

Match a named role claim instead

Active Directory Example

AD group **`SALES_DBA`** →
AD FS / Entra ID issues role claim →
`mcp.role=POOL.SALES` →
pool access granted

No new infrastructure — reuses the customer's existing AD group-to-role mapping and audit trail!

Is ORDS MCP right for me?



	ORDS
Best fit	Devs, dbas, power users
Ideal workflow	Governed natural language access to approved databases, and SQL tools
Transport	Streaming HTTPS
Connection model	Local ORDS, direct user connection pools / stateless
Access model	OAuth 2.0, JWT with scopes or roles from your identity provider of choice
Tools	List databases, run-sql, schema-information
Operational model	Customer managed mid-tier
Database reach	Oracle databases reachable from the mid-tier

Copyright © 2026, Oracle and/or its affiliates

Code Innovate Program



Copyright © 2025, Oracle and/or its affiliates

Code Innovate Experience



Bring your use cases

We work on your use cases instead of showing canned demos of our offerings.



Rapid Knowledge Share

Oracle Engineers work with your team.



Build a First Pass Prototype

Our Engineers help build a first pass working prototype of your use case solution.

Copyright © 2025, Oracle and/or its affiliates

What is a **Virtual Code Innovate?**

- Hands on Introduction to OCI Cloud Services
- 1 Week / Monday – Friday / 4 hours a day
- Our Engineers Work Online with Your Team
- Facilitates Rapid Knowledge Sharing
- Leverages Your Use Cases
- No cost - if minimum requirements are met



Copyright © 2025, Oracle and/or its affiliates

Requirements



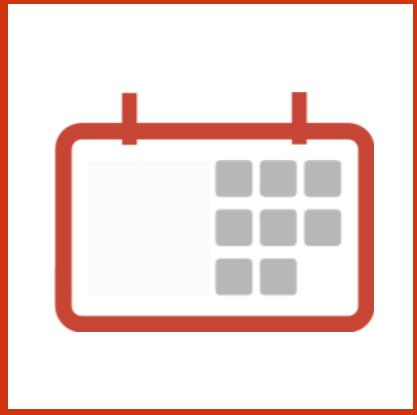
4 or more
Developers



Time Commitment
5 days / 4 hours day
(20 hours total)



Bring your Use
Case(s)



~3 Weeks
Lead Time

Copyright © 2025, Oracle and/or its affiliates

Contact Us to Schedule Your Event
codeinnovate_us_grp@oracle.com

Code Innovate – Timeline



Event Date Confirmed



Pre-Event Virtual Setup



Structured Learning and Tenancy Configuration



Virtual Code Innovate

Copyright © 2025, Oracle and/or its affiliates

Thank you

Copyright © 2025, Oracle and/or its affiliates