ORACLE
AI Database

Beyond the Hype: Practical AI for Your Oracle AI Database

MCPs, Skills, & Schema Enrichment

Kris Rice
Senior Vice President, Oracle AI Database R&D

Jeff Smith
Product Management Architect, Database Tools



Model Context Protocol (MCP) Overview



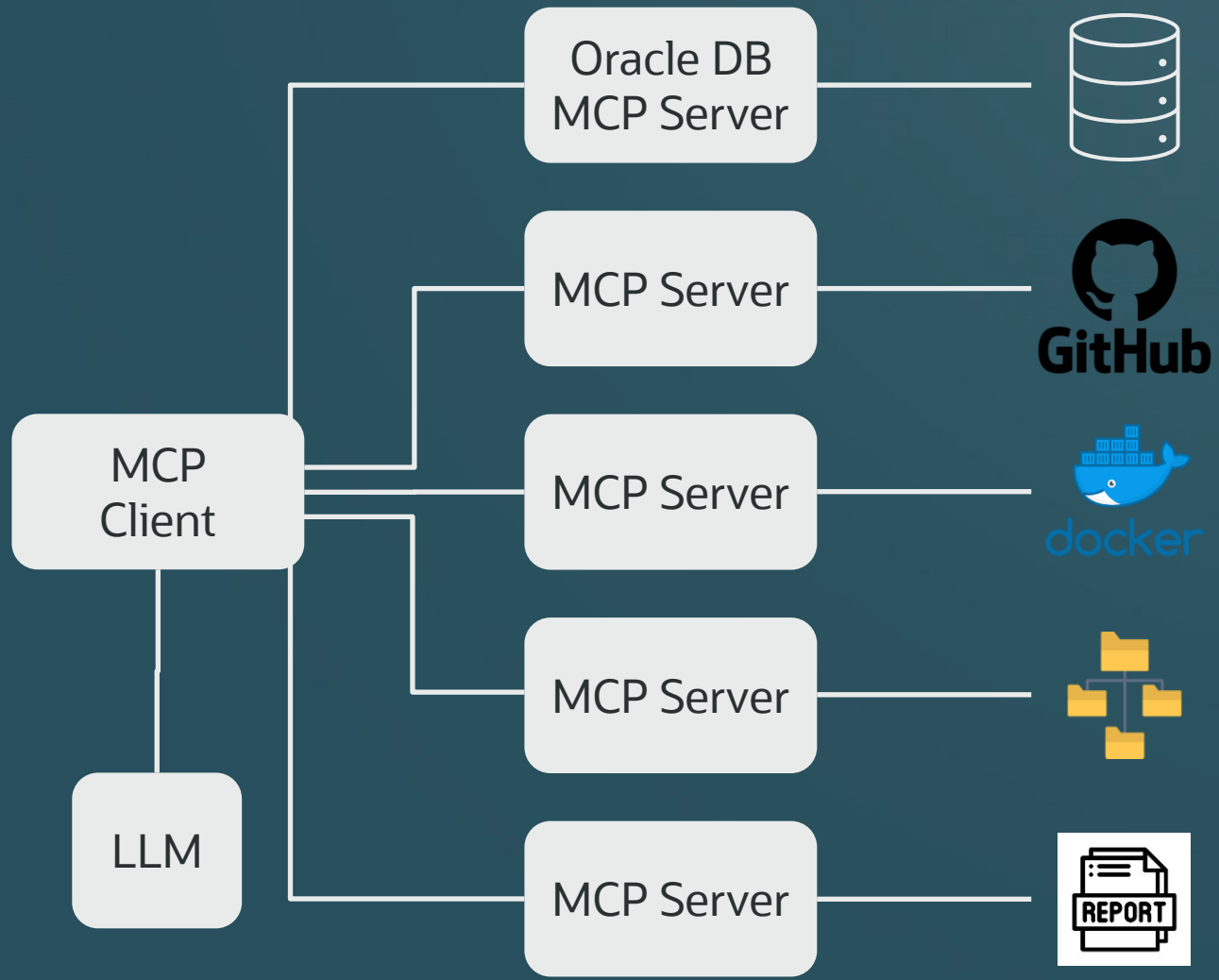
Copyright © 2026, Oracle and/or its affiliates

Model Context Protocol

- Launched Nov 2024 by Anthropic
- Donated to Linux Foundation in 2025
  Agentic AI Foundation (MCP, AGENTS.md, …)
- Marketed as “USB-C for AI applications”
- Singular interface to standard interactions with database, files, business apps, developer tools…
- Simplification hides the complexity of the Server implementation.

An Introduction:

modelcontextprotocol.io/introduction



Copyright © 2026, Oracle and/or its affiliates

Model Context Protocol Servers

- MCPs deliver:
  - 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
- MCP 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

Use Cases: LLMs can think. MCP lets them do.

DevOps / DBA

- Diagnose performance problems
  - Analyze AWR,
  - Trace Files,
  - Explain Plans
- Suggest/Implement indexing schemes
- Debug, fix, test PL/SQL errors
- Explain the latency we're seeing between our Data Guard primary and standby instances.

Business Support

- NL2SQL
  - How many accounts did we open last quarter, by region, by zipcode?
  - Correlate overdraft fees with accounts being closed.
  - Where should we invest in more local branches?
- NL2Data
  - Instead of generating SQL, your LLM chooses from curated SQL Reports!

Generative AI

- Generate data model
- … test data
- … full stack applications
- … low-code APEX apps
- … REST APIs
- … security policy, hide EMPLOYEE data for anyone outside my direct management chain.

Copyright © 2026, Oracle and/or its affiliates

Oracle AI Database MCP Servers

- **SQLcl** a *local, STDIO* MCP server that runs on the user's machine, easy to configure, up and running in minutes, included with SQL Developer for VS Code
- **Oracle REST Data Services** enterprise-ready *remote streaming HTTPS* MCP Server, ties into customer's preferred identify management
- **OCI Managed MCP Service** simply define your MCP Tools and roles, we will run your *streaming HTTPS* MCP Server for you, for any Oracle AI Database running in your cloud tenancy



Copyright © 2026, Oracle and/or its affiliates

Before bringing AI to your database: Prioritize Security

- AI/LLM/MCP amplify that security is more important than ever.
- **Least privilege principle**: use CONNECTIONs tied to database USERs having only the privs to view the data you want to share, and perform the actions you want an Agent to do on your behalf
- **Segregated environments**: use databases that have sanitized data, such as development and testing instances. PRODUCTION use should be strictly Monitored
- **Do not trust, always verify**: use only AI assistants that ask for access to the SQLcl MCP Tools, and always review requested actions before approving them. NEVER enable 'auto-approve'

Copyright © 2026, Oracle and/or its affiliates



Oracle SQLcl

Copyright © 2026, Oracle and/or its affiliates

Oracle SQLcl: Local STDIO MCP Server

Database Availability

- any edition, including FREE
- *any version* (19c, 21c, 26ai)
- any deployment
  (on-premises, Cloud, containers, etc.)

Technology stack

- *included* with database
- existing, proven product
- runs locally, STDIO
- JSON-RPC communication

```
SQLcl: Release 26.2.0 Production on Mon July 6 10:35:35
2026

Copyright (c) 1982, 2026, Oracle.  All rights reserved

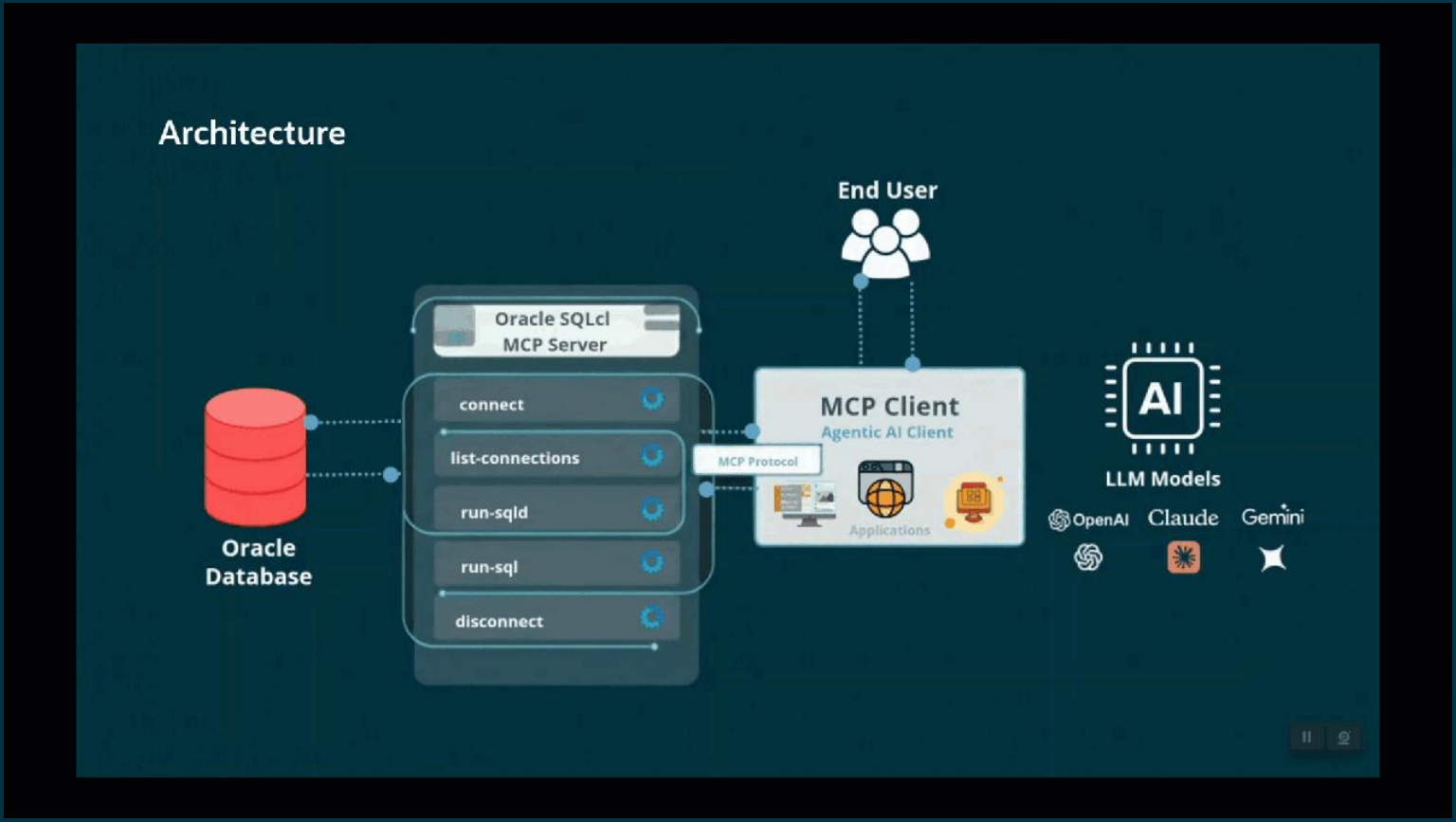
Connected to:
Oracle Database 26ai Free Release 23.26.3.0 - Develop,
Learn, and Run for Free


SQL> cm list
.
├── Cloud
│   └── 0 Autonomous Reporting
└── Local
    ├── EMS $
    └── ERP

SQL>
viins ¦ 1:0 ¦ OE¦ ERP
```


Copyright © 2026, Oracle and/or its affiliates

SQLcl MCP Architecture



- SQLcl sits on user's local machine
- Agent SQLcl STDIO, JSON RPC
- Agent invokes LLM for planning, generating code
- Agent makes Tool request
- SQLcl takes tool request, executes, returns token-optimized results

Copyright © 2026, Oracle and/or its affiliates

SQLcl MCP Tools

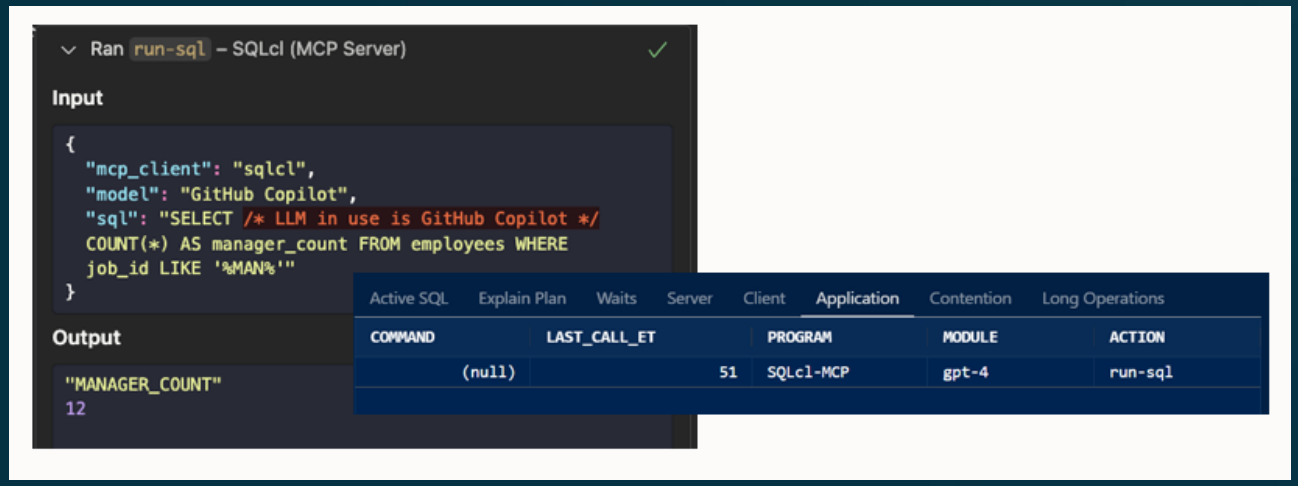
- list-connections
  Retrieves list of named, stored connections available for MCP
- connect
  Establishes requested by name, connection
- run-sql
  Runs SQL command, SQL script, or PL/SQL block
- run-sqlcl
  Runs SQLcl command (load, ddl, info, datapump, etc.)
- schema-information
  Retrieves metadata and annotations to assist with NL2SQL
- disconnect
  Ends database session, closes connection.

Copyright © 2026, Oracle and/or its affiliates

SQLcl MCP Security

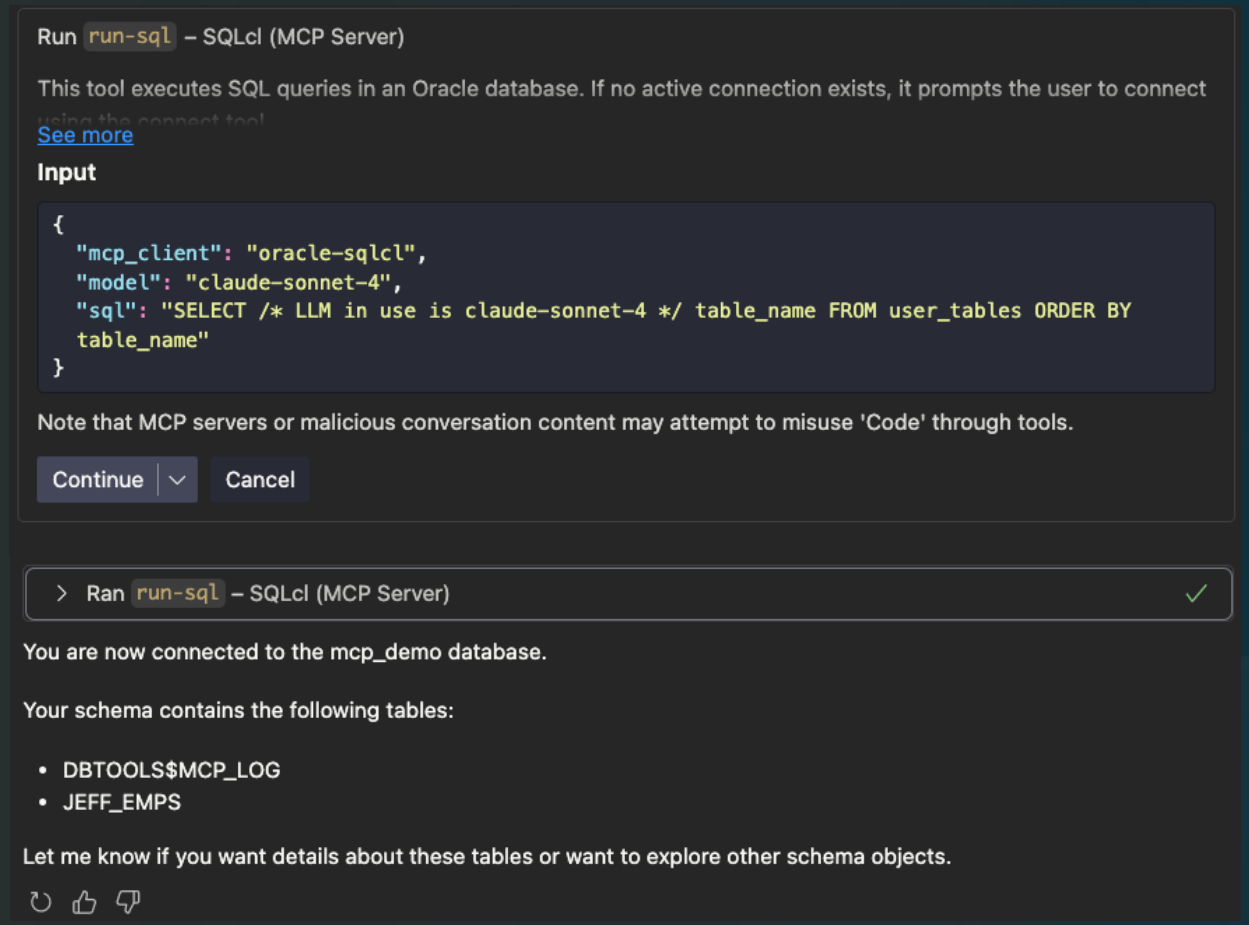
- Agent/LLM does not work with database, everything goes though SQLcl
- Passwords never shared with the agent, locally encrypted (.SSO)
- SQLcl can be configured to
  - Restrict allowed commands, prevent access to local OS
  - Use a separate list of connections from normal SQLcl runtime

- SQLcl creates db conn/session with:
  - Program (SQLcl-MCP)
  - Module (LLM)
  - Action (MCP Tool)



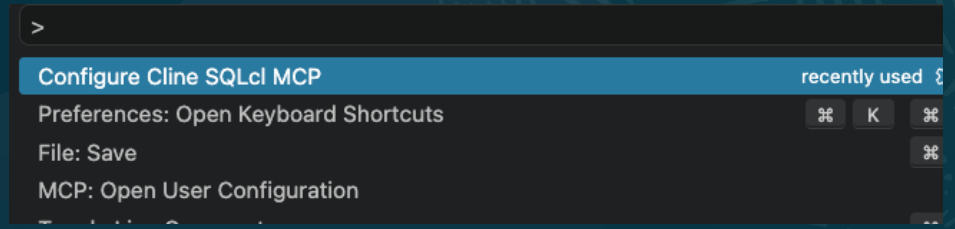
Copyright © 2026, Oracle and/or its affiliates

SQLcl MCP auto-config for VS Code Copilot



- Install SQL Developer extension
- Create at least one connection
- Start your AI chat!

- Optionally – invoke via Command Palette

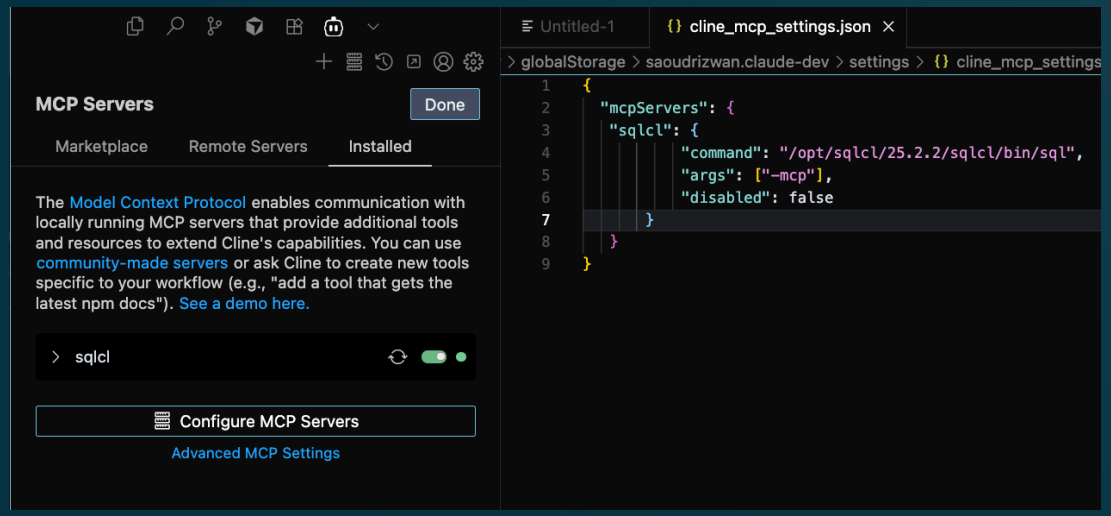


Generates JSON for SQLcl MCP you can add to your local Agent config file

Copyright © 2026, Oracle and/or its affiliates

SQLcl Installations

curl –O https://download.oracle.com/otn_software/java/sqldeveloper/sqlcl-latest.zip
brew install sqlcl
yum install sqlcl
Included with SQL Developer for VS Code



Connections

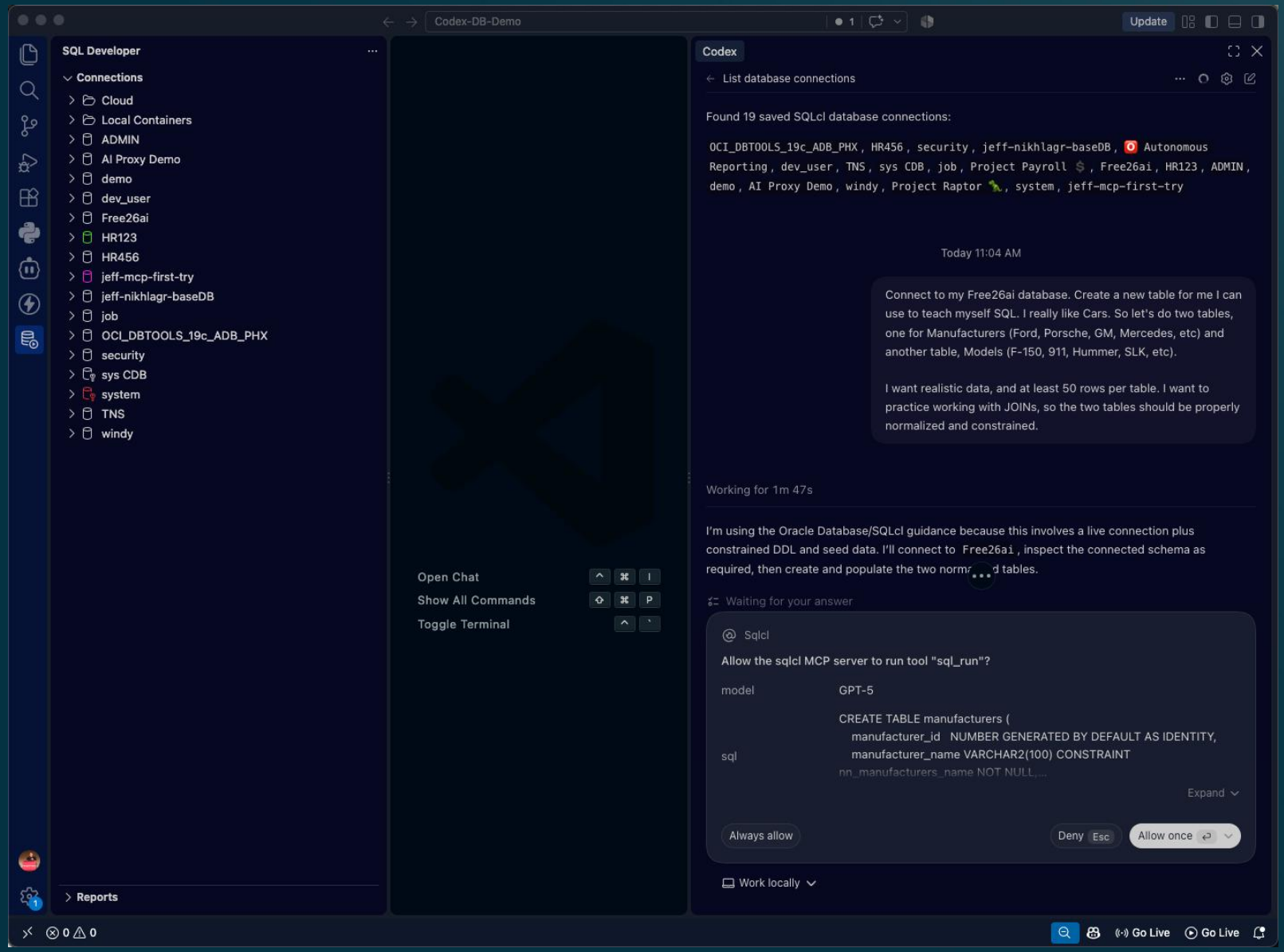
Create/Save one or more connections with passwords saved
SQLcl connections shared with SQL Developer for VS Code

```
SQL> conn -save mcp_demo -savepwd jeff/xyzabc@localhost1521/freepdb1
```


Copyright © 2026, Oracle and/or its affiliates

DEMO

- MCP
  SQLcl MCP
- Agent
  Codex Extension for VS Code
- LLM
  5.6 Luna Extra High
- Database
  FreeSQL.com hosted 26ai



Copyright © 2026, Oracle and/or its affiliates

Is SQLcl right for me?



	SQLcl MCP
Best fit	Devs, dbas, power users – people already working directly with your databases
Ideal workflow	**Local** database exploration, dev, or troubleshooting
Transport	STDIO
Connection model	**locally** managed connections, stateful
Access model	DB credentials avail to the **local** OS user
Tools	List connections, connect, run-sql, run-sqlcl, schema-information, disconnect
Operational model	Lightweight **local** setup
Database reach	Oracle databases with a network path from the **local** machine

Copyright © 2026, Oracle and/or its affiliates



OCI Database Tools MCP Servers

Copyright © 2026, Oracle and/or its affiliates

Developer Services

Database Tools

Database Developer Portal
Connections
Private Endpoints
Model Context Protocol Servers
SQL Reports
Database API Gateway Configurations
Database Actions
SQL Worksheet

Database Developer Portal

Your central workspace for building, connecting, and managing Oracle databases. Quickly create new environments, run SQL, load data, and access essential developer tools—all in one place.

Overview | Databases | Connections

Database tools

One-click access to essential utilities.

SQL worksheet
A command interface for running SQL and PL/SQL code directly against the database.
SQL worksheet

MCP Servers
Managed multi-tenant gateway letting MCP clients reach Oracle AI Database via Model Context Protocol and offering built-in and custom SQL/PL/SQL tools.
Create MCP server

VS Code
Provides the configuration needed to use Visual Studio Code for database dev
Download VS Code configuration

MCP Servers
Managed multi-tenant gate
offering built-in and custom
Create MCP server

Favorites

Search and Filter

Applied filters: Compartment All

Name	State	Resource type	Compartment	Created
jeff-nikhlagr-baseDB	Active	Connection	dbtools-mcp	Apr 16, 2026, 7:21:49 PM UTC

Page 1 of 1 (1 - 1 of 1 total items)

Quick actions

Single-click shortcuts to instantly provision new cloud databases (ADB, MySQL) or establish connections to existing ones.

Create ADB
Provisions a new Autonomous Database (ADB) instance, and Oracle Cloud service, for immediate use.
Create Autonomous AI Database

Create MySQL
Sets up a new MySQL Database Service instance, providing a fully managed, highly available MySQl environment.
Create MySQL DB system

Connect to database
Establishes a network connection to an existing database by configuring nece connection details.
Create connection

Copyright © 2026, Ora

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 via OCI Console.
- Powered via 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

It All Starts with an OCI Database Connection

What it is

- A managed, secure link between OCI and your Oracle AI Database
- Stores credentials, wallet, and endpoint centrally — not on each user's machine
- One connection can back multiple MCP Servers
- Defined once by an administrator, consumed by everyone

Why it matters for security

- The database user tied to the connection is the ultimate security backstop
- Oracle AI Database security rules apply in full — roles, object grants, VPD, all of it
- The MCP layer inherits those controls automatically — no duplication needed
- A read-only database user means read-only AI access. Full stop.

OCI controls who can reach the MCP layer – Oracle AI Database controls what they can see

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.

- **sql_run**
- **request_status**
- **schema_information**

Reporting tools

Curated, parameterized queries published as governed, callable tools.

- **report_list**
- **report_sql**
- **report_execute**

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

No new credential silos — OCI Identity Management handles it all

Authentication

- Users authenticate via OAuth2 via OCI IAM
- Federate Azure Entra ID, Okta, or Active Directory
- No separate MCP credentials to manage or rotate
- SSO experience:
  users sign in once
  grant OBO access for their clients
  clients retrieve access tokens as necessary

Authorization

User access determined by Group membership/policies

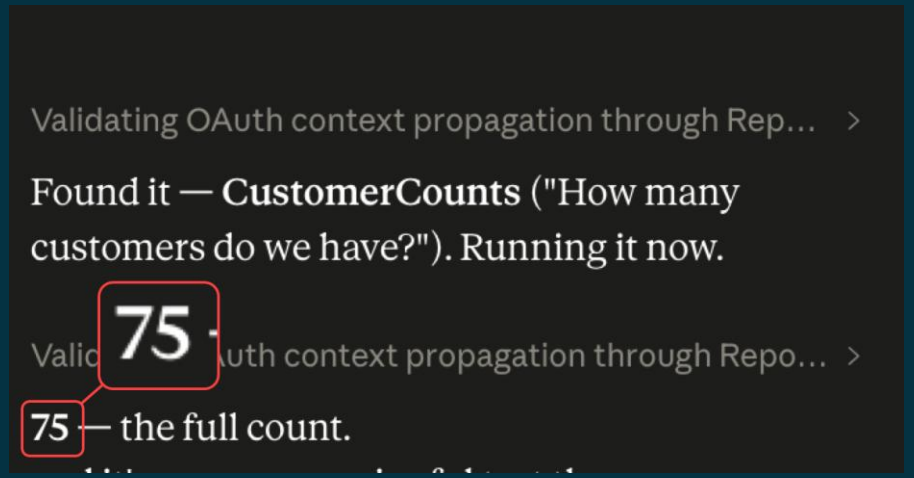
IAM Group
- 🔒 DBTools Connections
- 🔒 MCP Servers
- 🔒 Toolsets & Reports

Copyright © 2026, Oracle and/or its affiliates

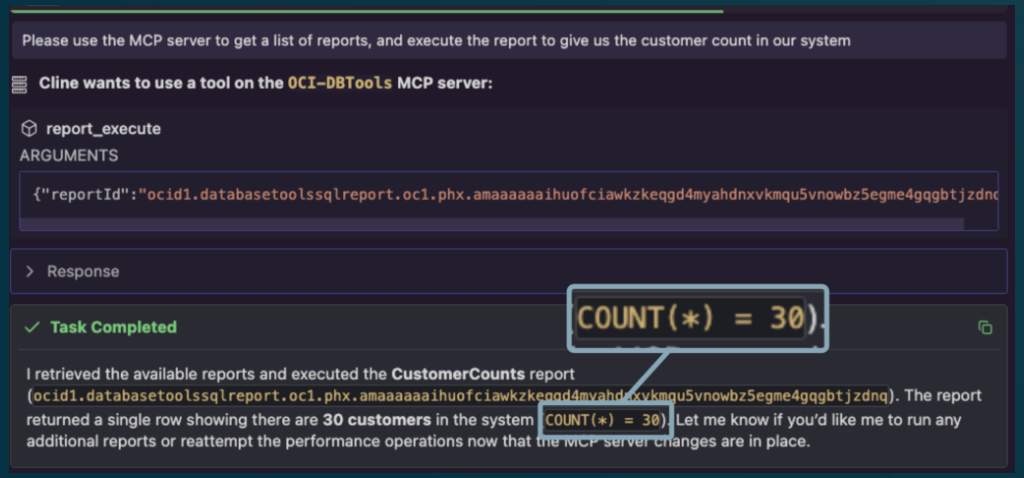
One Identity, From Client to the Database

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

Administrator asks question, routed to report



Biz Analyst asks same question, via same report



1. Database MCP Tool invoked
   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 sensitive or unauthorized data

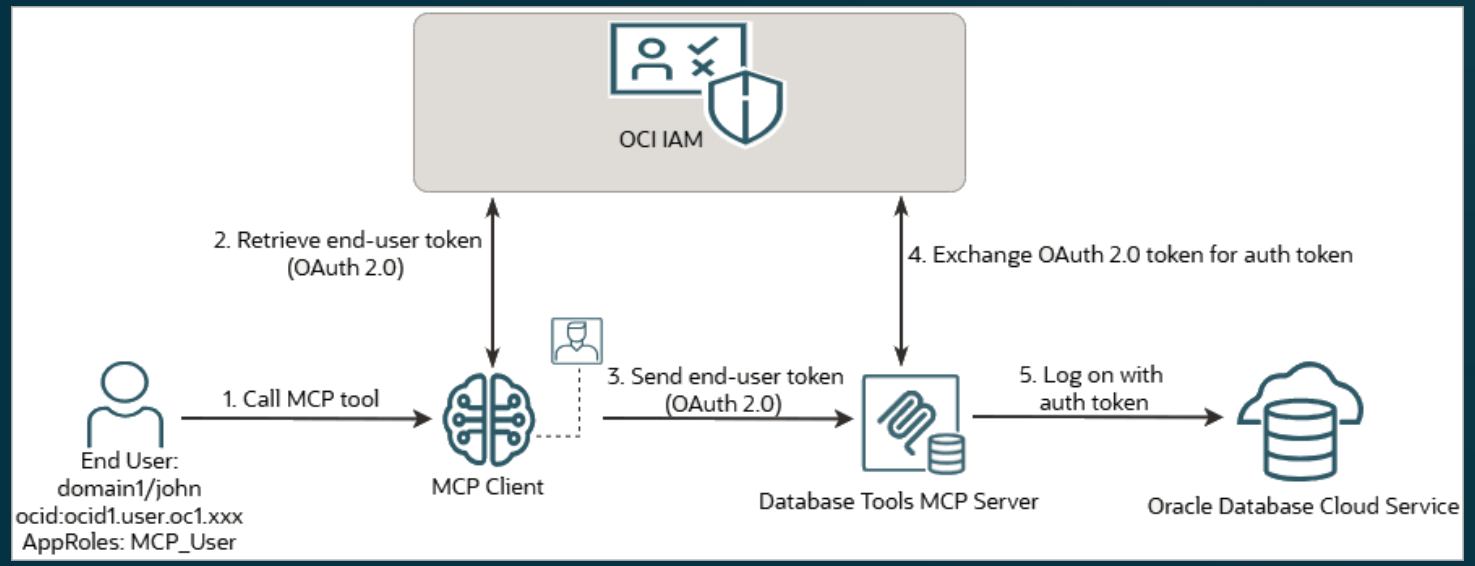
Copyright © 2026, Oracle and/or its affiliates

Deep Data Security: Fine Grained Access Control in the DB for the SSO User

Managers can SELECT all columns except SSN, can only UPDATE SALARY for their direct reports.

Now available!

- minVer Oracle AI Database 23.26.3
- Uses OCI IAM auth tokens
- Deep Data Security Integration Use Case Docs



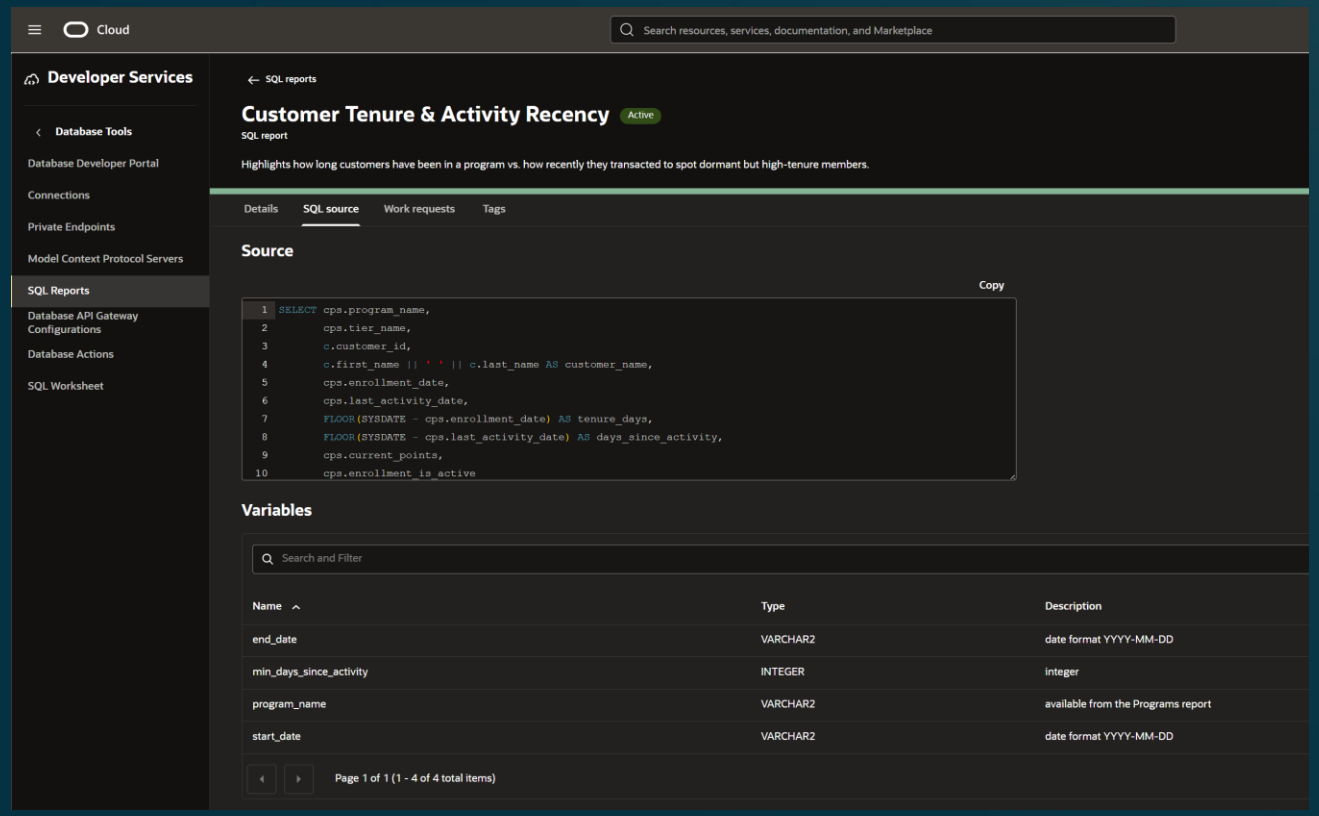
Copyright © 2026, Oracle and/or its affiliates

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. Reports are OCI Resources
   - 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 invokes reports
4. Consistent SQL

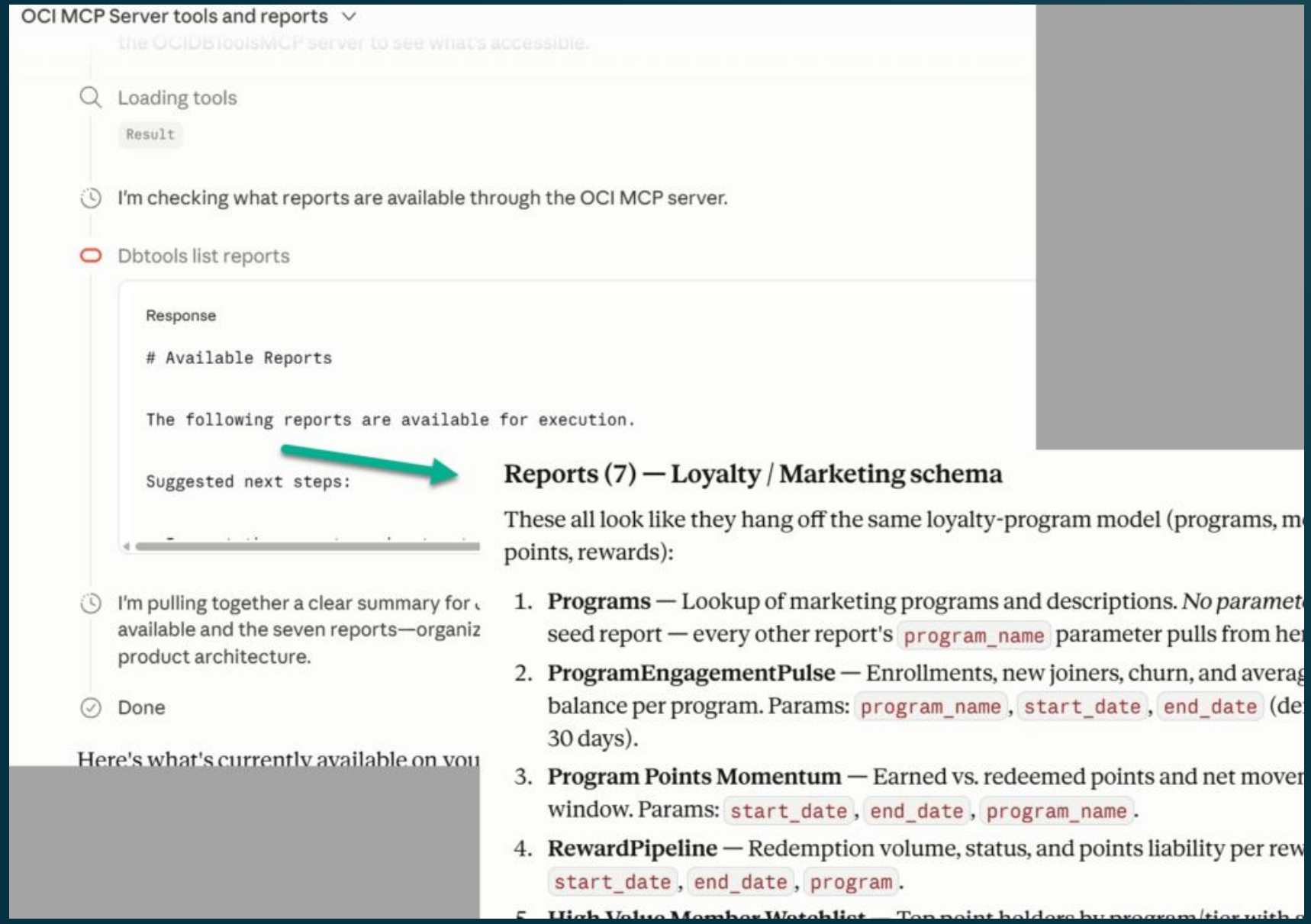


Your organization already has many of these reports, now they can be utilized via AI.

Copyright © 2026, Oracle and/or its affiliates

DEMO

- MCP
  OCI Database Tools
- Agent
  Claude Desktop
- LLM
  5.6 Luna Extra High
- Database
  OCI Base VM 26ai



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	run-sql, schema-information,list reports, run reports, custom
Operational model	Oracle Managed 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

Copyright © 2026, Oracle and/or its affiliates

Oracle REST Data Services (ORDS): Remote Streaming HTTPS

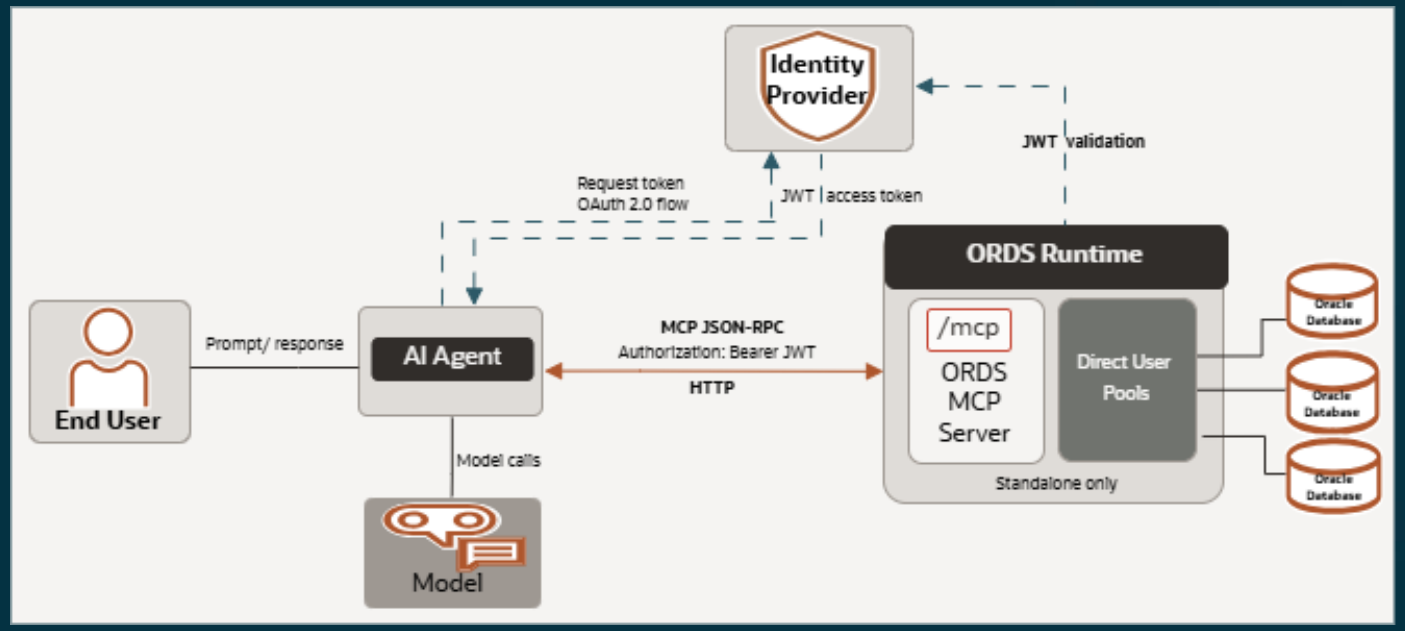
- Established, well-known mid-tier solution, debuted in 2010
- Supports every version of Oracle, for EVERY environment
- FREE
- 📢 **/mcp** endpoint available, minVer 26.2
- ALSO serves up -

  Database REST APIs
  - Oracle APEX applications
  - SQL Developer Web
  - Oracle Backend for Firebase (BaaS)
  - Database API for MongoDB
  - Vector DB / AI Vector Search APIs



Copyright © 2026, 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)
- Bring your own Identity Provider (JWT)
- Fully OAuth compliant to MCP Spec
  - Supports dynamic client registration!
- Stateless

Copyright © 2026, Oracle and/or its affiliates

ORDS MCP Server Tools

Included Tools

- database_list
- run_sql
- schema_information

What is database_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

Coming Soon

- Reports (list-reports, run-report)
- Custom Tools
- Deep Data Security

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

Active Directory Example

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

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

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

Copyright © 2026, Oracle and/or its affiliates

JWT Identity Propagation & Audit Trail

End-user identity travels from the MCP token through ORDS into the database
— no identity is lost behind the pool

OAUTH_PRINCIPAL

User principal from the JWT

OAUTH_CLIENT_NAME

Name of the MCP client application

OAUTH_SUB

JWT subject (sub) claim — unique user identifier

REQUEST_ECID

Execution Context ID — links ORDS logs to database audit

OAUTH_ISSUER

JWT issuer (iss) — which IdP issued the token

OAUTH_APP_ROLES

Roles from the JWT (role mode)

OAUTH_MODE

scope or role — which authorization model is active

OAUTH_APP_SCOPES

Scopes from the JWT (scope mode)

Agent with Keycloak Auth info is available in the database

```
Called ords-querystuff-demo (ctrl+o to expand)

● That's a much richer picture:
```

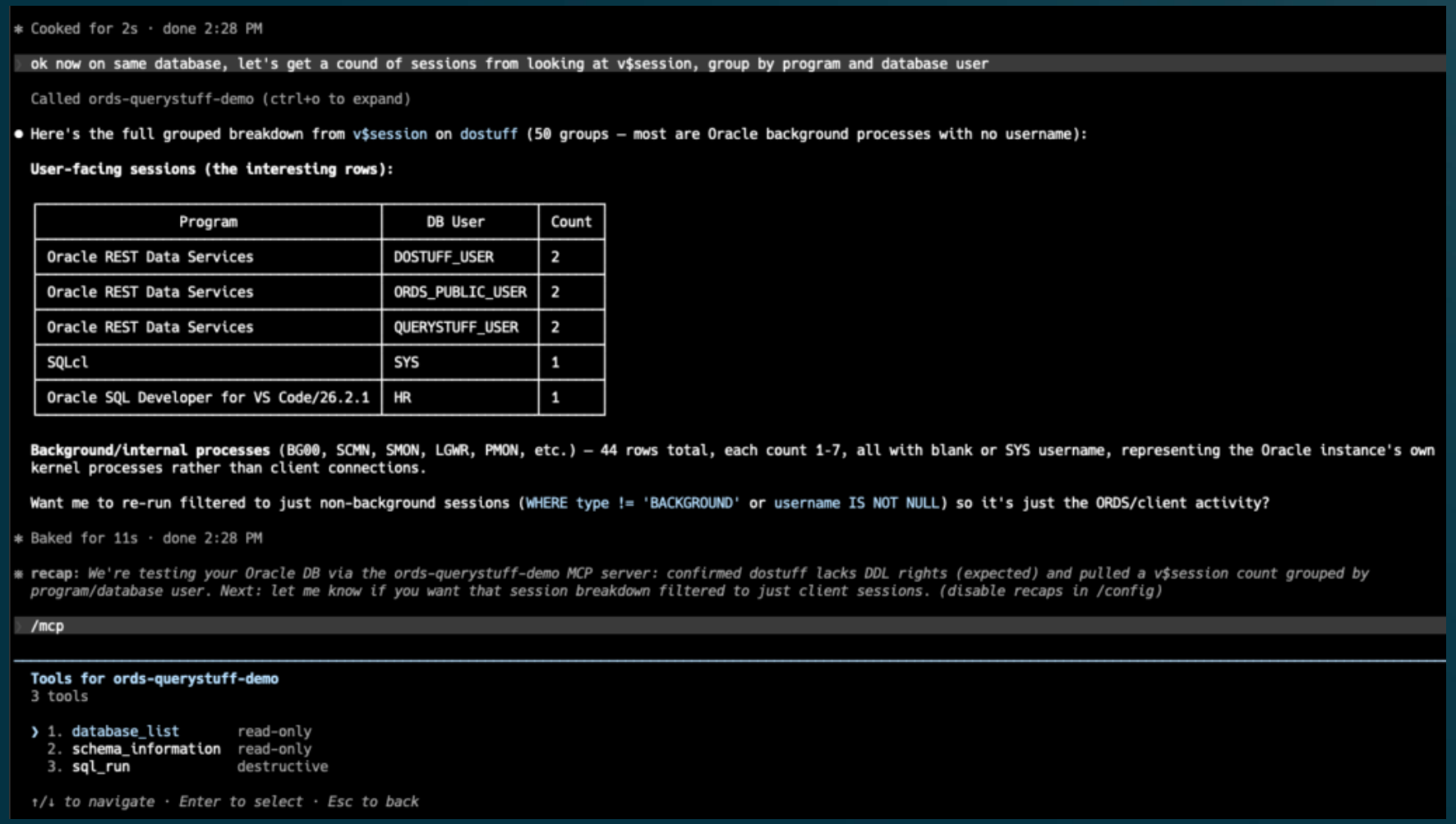
Attribute	Value
OAUTH_ISSUER	http://localhost:8080/realms/ords-mcp-demo
OAUTH_PRINCIPAL	951dad24-4aa0-458f-b2d7-c32b7a401c69
OAUTH_APP_ROLES	DoStuff default-roles-ords-mcp-demo offline_access uma_authorization QueryStuff
OAUTH_SUB	951dad24-4aa0-458f-b2d7-c32b7a401c69

```
So the Keycloak token does carry both DoStuff and QueryStuff roles for your identity — that's likely exactly why database_list
sometimes only querystuff: it's not a permissions difference between two separate users, it's the same principal with both rol
depends on which roles happened to be present/recognized in whatever token was active on a given reconnect. Worth checking if
issuance/refresh (offline_access refresh flow) rather than being enforced consistently server-side.
```


Copyright © 2026, Oracle and/or its affiliates

DEMO

- MCP
  ORDS
- Agent
  Claude Code
- LLM
  Sonnet 5
- Database
  On Premises 26ai EE



✻ Cooked for 2s · done 2:28 PM

ok now on same database, let's get a cound of sessions from looking at v$session, group by program and database user

Called ords-querystuff-demo (ctrl+o to expand)

● Here's the full grouped breakdown from v$session on dostuff (50 groups — most are Oracle background processes with no username):

User-facing sessions (the interesting rows):

Program	DB User	Count
Oracle REST Data Services	DOSTUFF_USER	2
Oracle REST Data Services	ORDS_PUBLIC_USER	2
Oracle REST Data Services	QUERYSTUFF_USER	2
SQLcl	SYS	1
Oracle SQL Developer for VS Code/26.2.1	HR	1

Background/internal processes (BG00, SCMN, SMON, LGWR, PMON, etc.) — 44 rows total, each count 1-7, all with blank or SYS username, representing the Oracle instance's own kernel processes rather than client connections.

Want me to re-run filtered to just non-background sessions (WHERE type != 'BACKGROUND' or username IS NOT NULL) so it's just the ORDS/client activity?

✻ Baked for 11s · done 2:28 PM

※ **recap:** *We're testing your Oracle DB via the ords-querystuff-demo MCP server: confirmed dostuff lacks DDL rights (expected) and pulled a v$session count grouped by program/database user. Next: let me know if you want that session breakdown filtered to just client sessions. (disable recaps in /config)*

/mcp

Tools for ords-querystuff-demo
3 tools

❯ 1. database_list read-only
  2. schema_information read-only
  3. sql_run destructive

↑/↓ to navigate · Enter to select · Esc to back

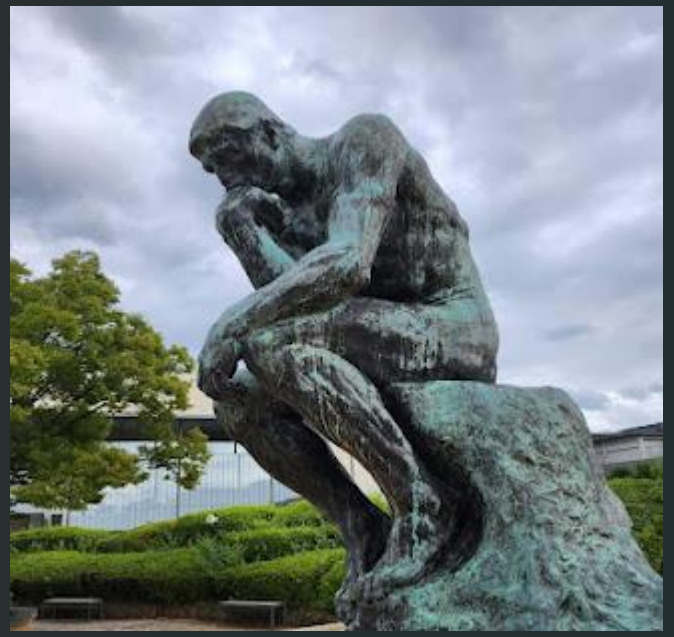
Copyright © 2026, Oracle and/or its affiliates

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**
Tools	List databases, run-sql, schema-information
Operational model	**Customer managed** mid-tier
Database reach	**On-premises**

Copyright © 2026, Oracle and/or its affiliates



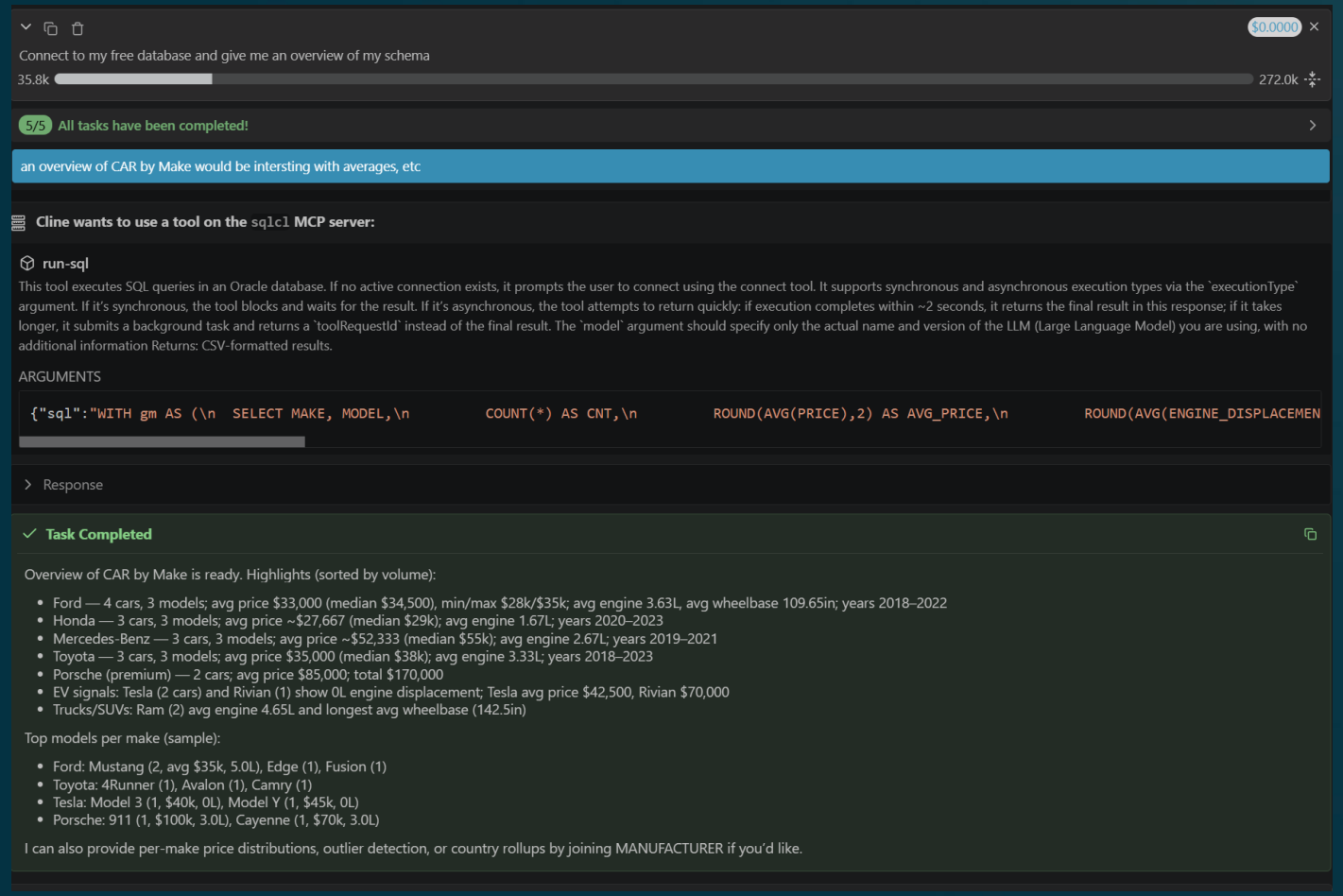
Some Practical thoughts, musings, observations

Copyright © 2026, Oracle and/or its affiliates

Step 1: Start Chatting!

Day 0 / Getting Started

- Connect
- Explore
- Summarize Existing
- Learn Tools / Agent Flow
- Understand security model



Copyright © 2026, Oracle and/or its affiliates

The promise is real. The steering wheel is still yours.

> **Be the Pilot. I'm not a passenger on this magical plane ride my Agent is taking me on. I'm in charge.**

Vibe coding is not "turn off your brain."
It is "move faster because you are actively directing the work."

Copyright © 2026, Oracle and/or its affiliates

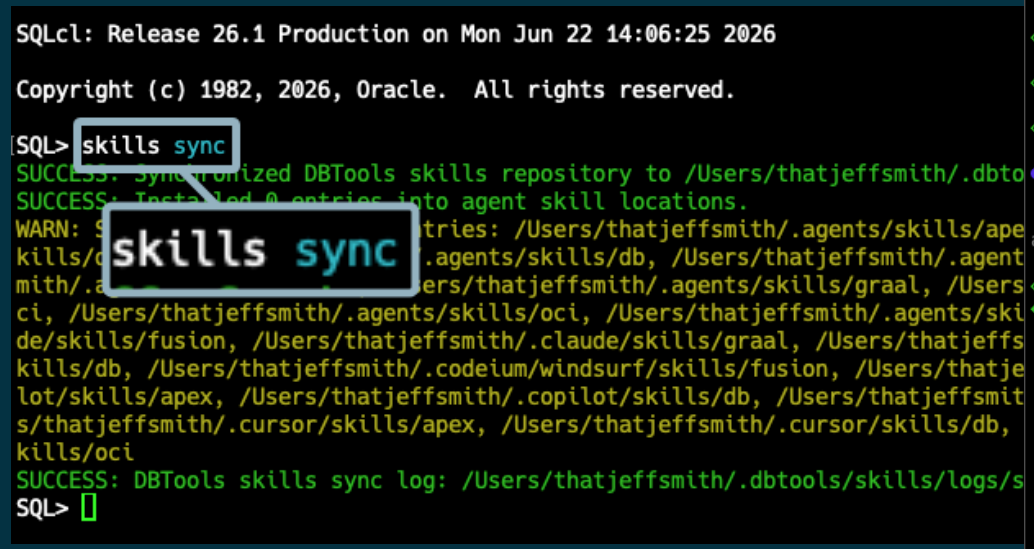
Live demo vibe coding is hard, but if you want that...

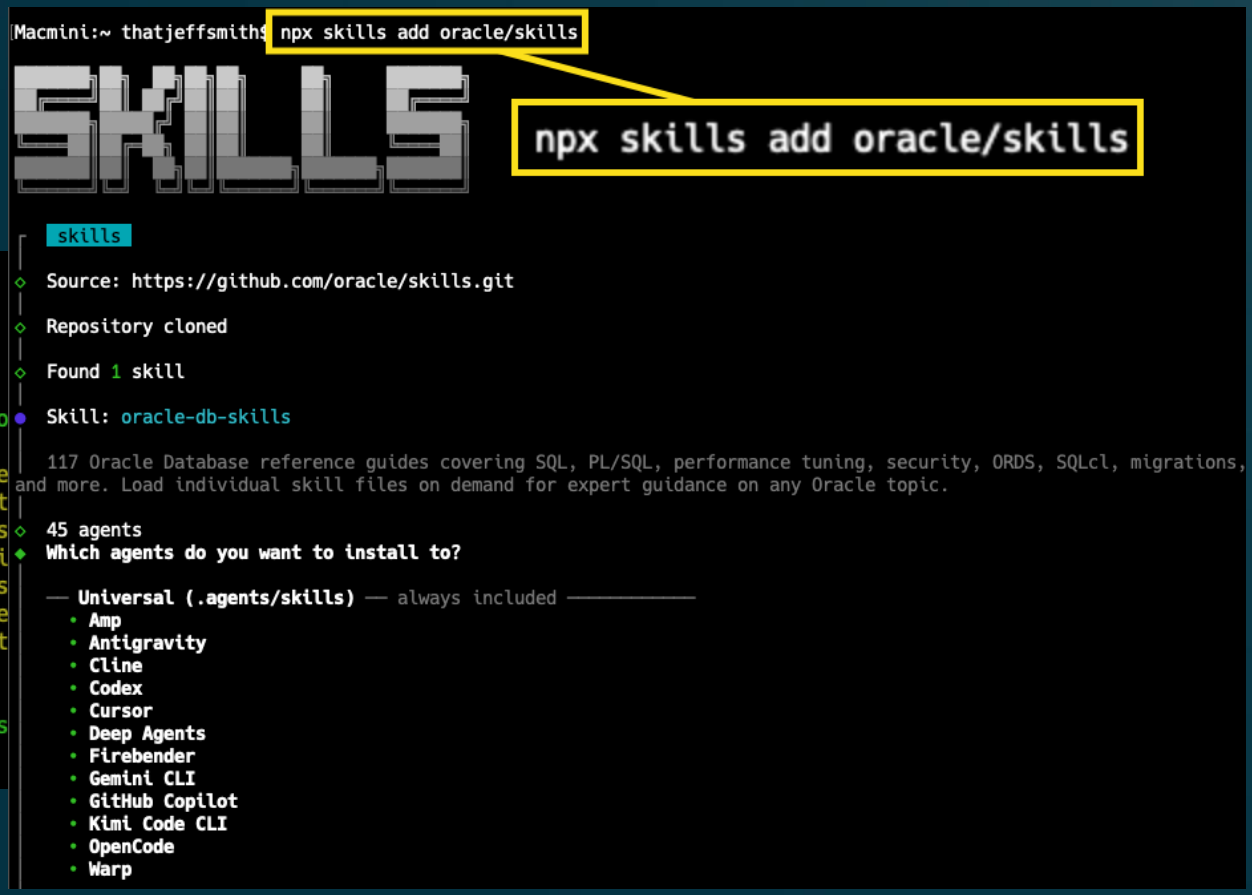


Copyright © 2026, Oracle and/or its affiliates

GIVE THE AGENT ORACLE CONTEXT

Load Oracle skills first.





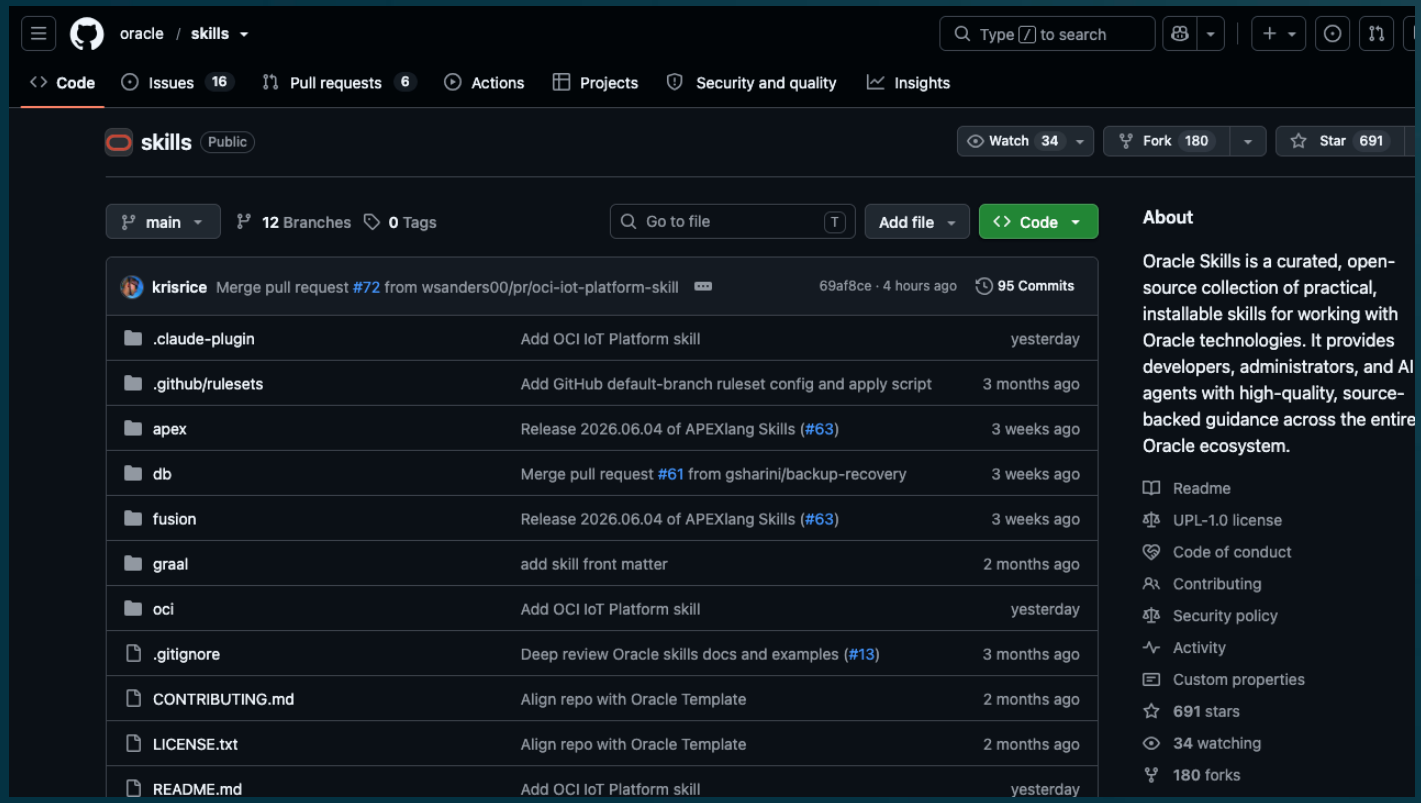
Skills are your “Oracle-aware starting point.”

Copyright © 2026, Oracle and/or its affiliates

GIVE THE AGENT ORACLE CONTEXT

AI Skills for Oracle AI Database

- 100+ doc-backed skill guides for working with the database
- Agents stop *thinking* – 'do exactly this' here's the code/sql/plsql/ddl/dml
- Less reasoning / fewer tokens / faster
- Works for ANY AI tool
- Open Source and extensible



Copyright © 2026, Oracle and/or its affiliates

AI Skills for Oracle AI Database

🤖 **Estimated savings:**

- **Tokens:** ~40–60% fewer input tokens (no need to fetch/reason through Oracle security docs)
- **Speed:** Likely 1–2 fewer tool call roundtrips, saving maybe 30–45 seconds of wall time
- **Quality:** The `oracle_maintained = 'Y'` filter and the profile hardening DDL came directly from the skill — I might have gotten there eventually but could have used a less precise exclusion pattern

Copyright © 2026, Oracle and/or its affiliates

AGENTS SHOULD THINK BEFORE THEY ACT

Plan first. Debate it. Amend it. Only then, GO.

01

Ask

State outcome, constraints, and what “done” means.

02

Review

Challenge the plan: objects, blast radius, rollback, tests.

03

Execute

Approve bounded steps — not an unlimited adventure.

A good plan is a contract you can negotiate before it becomes a transaction.

Copyright © 2026, Oracle and/or its affiliates

PROMPT LIKE A DOMAIN EXPERT

Specificity buys you useful output. Vagueness buys you… vibes.

Weak ask

“Build me an app for sales.”

Outcome: an impressive-looking guess.

Strong ask

“Create a local ORDS app for account managers to review open orders. Use these APIs, roles, and acceptance tests. Do not deploy.”

Outcome: a bounded proposal you can judge.

Copyright © 2026, Oracle and/or its affiliates

PROMPT LIKE A DOMAIN EXPERT

Example: here's a prompt I used to build ORDS REST APIs

Connect to my Raptor database, and for my Spotify data, construct an ORDS REST API, GET Handler, that returns a collection of artists with a summary of the total number of tracks and total overall time spent listening

You will need to generate some SQL to provide for the GET handler definition in the ORDS PL/SQL API.

Implement the ORDS REST API using the ORDS.CREATE_SERVICE plsql program.

The module base path should be 'claude-apis' and the template should be called 'spotify-summary'

Here is a simple example -

```
begin
  ORDS.create_service(
        p_module_name => 'day_zero',
          p_base_path => 'day0',
            p_pattern => 'greeting/',
             p_method => 'GET',
        p_source_type => 'json/item',
             p_source => 'select ''Hello!'' from dual',
             p_status => 'PUBLISHED',
    p_module_comments => 'see if we can create a module',
  p_template_comments => 'see if we can create a template',
   p_handler_comments => 'see if we can say Hello!');
COMMIT;
END;
```



ORDS REST API Created Successfully! 🎵

API Details:

- **Module Name:** `claude_apis`
- **Base Path:** `/claude-apis`
- **Template:** `spotify-summary/`
- **Method:** `GET`
- **Full Endpoint:** `/ords/[your-schema]/claude-apis/spotify-summary/`

What the API Returns:

The API returns a JSON collection of artists with the following statistics for each artist:

- **artist_name**: The name of the artist
- **total_tracks**: Number of unique tracks played
- **total_plays**: Total number of times any track was played
- **total_ms_played**: Total milliseconds of listening time
- **total_minutes_listened**: Total listening time in minutes (rounded to 2 decimals)
- **total_hours_listened**: Total listening time in hours (rounded to 2 decimals)
- **avg_seconds_per_play**: Average seconds per play session

Sample Output:

Based on your data, top artists include:

1. **Puscifer**: 59 tracks, 16.02 hours total listening time
2. **Def Leppard**: 48 tracks, 15.75 hours total listening time
3. **Kix**: 25 tracks, 11.78 hours total listening time
4. **Metallica**: 45 tracks, 9.01 hours total listening time

The API is now **PUBLISHED** and ready to use. The results are automatically sorted by total listening time (descending), so you'll always see your most-listened-to artists first!

To access the API, you would typically use:

```
GET http://[your-server]/ords/[your-schema]/claude-apis/spotify-summary/
```

The API will return the data in JSON format, perfect for integration with web applications or data visualization tools.

Copyright © 2026, Oracle and/or its affiliates

Example: I didn't like the SQL it used, so I fixed it

```
select /* LLM in use is claude-opus-4-1-
20250805 */ artistname,
       count(distinct trackname) as
total_tracks,
       count(*) as total_plays,
       sum(msplayed) as total_ms_played,
       round(
          sum(msplayed) / 1000 / 60,
          2
       ) as total_minutes,
       round(
          sum(msplayed) / 1000 / 60 / 60,
          2
       ) as total_hours
  from spotify_streaming
 where artistname is not null
 group by artistname
 order by total_ms_played desc
```

Copyright © 2026, Oracle and/or its affiliates

PROMPT LIKE A PRODUCT MANAGER

I noticed you are summing the milliseconds and dividing it out multiple times to get the hours, minutes, and seconds played we're connected to a 23ai database, this is much easier now, we can simply SUM the PLAYING_TIME column, which is an interval, which will return the time spent represented as Days, Hours, Minutes, and Seconds, and even fractions of a second up to 6 digits of precision let's refactor our REST API to do that instead -

we can keep the interval type

we do not need to drop and recreate the module, we can simply define the module again, and it will overrite or replace the existing api



You're absolutely right Let's refactor the REST API to use the INTERVAL column directly, which is much cleaner in Oracle 23ai. We'll just redefine the module and it will replace the existing one.

Run-sql

I see - we need to update the existing handler. Let me use the ORDS.define_handler approach instead to update just the handler:

Run-sql

Perfect! The API has been refactored successfully. Now let's test the output to verify the INTERVAL format:

Run-sql

Excellent! The API has been successfully refactored to use Oracle 23ai's INTERVAL data type directly. Let me update the curl test commands to reflect this change:

ORDS API Test Commands
Document • Version 2

Get Top 5 Artists Only (using jq)

```bash
curl -s -X GET http://localhost:8080/ords/hr/claude-apis/spotify-summary/ | jq
```

Extract Just Artist Names and Hours (using jq)

```bash
curl -s -X GET http://localhost:8080/ords/hr/claude-apis/spotify-summary/ | \
  jq '.items[] | {artist: .artist_name, hours: .total_hours_listened}'
```

Windows PowerShell Alternative

```powershell
Invoke-WebRequest -Uri "http://localhost:8080/ords/hr/claude-apis/spotify-summa
```

Expected Response Structure (Refactored with INTERVAL)

The API now returns a JSON response using Oracle 23ai's INTERVAL data type:

```json
{
  "items": [
    {
      "artist_name": "Puscifer",
      "total_tracks": 59,
      "total_plays": 295,
      "total_time_played": "+000000000 16:00:47.000000000",
      "avg_time_per_play": "+000000000 00:03:15.413559322"
    },
    {
```

Copyright © 2026, Oracle and/or its affiliates

TREAT MCP APPROVALS LIKE A CHANGE REVIEW

Never auto-approve database tool calls.

Tool approval is the moment to ask:

01 What exact connection/account?

02 Read, write, DDL, or OS access?

03 What is the object and scope?

04 Can I explain the SQL/PLSQL?

05 What proves success — and what undoes it?

Good approval behavior

✓ Review the call
✓ Reject surprises
✓ Reduce scope
✓ Ask for dry-run output
✓ Keep credentials & privilege boundaries intact

Copyright © 2026, Oracle and/or its affiliates

SANDBOX BEFORE PRODUCTION

Build a safe place to be wrong.

Local Docker sandbox

Fast prototypes
Disposable test data
Repeatable setup
No production surprises

Purpose-built “vibe” account

Least privilege
No DBA role
Only the schemas, objects, packages, and operations required
Auditable connection identity

Keep “can the agent do this?” separate from “should it be allowed to do this here?”

Copyright © 2026, Oracle and/or its affiliates

DOMAIN KNOWLEDGE IS STILL THE QUALITY GATE

If you can’t judge it, you probably can’t keep it.

> **Just because the code compiles, we don’t ship it. Just because the chart has pretty colors, doesn’t mean we present it to the CEO.**

A very sensible rule for both apps and databases

Research the business domain. Understand the data. Be able to spot the “looks right” answer that is wrong.

Copyright © 2026, Oracle and/or its affiliates

GIVE IT A MAP, NOT A FLASHLIGHT

Use schema-information. Be stubborn.

Preferred path

schema-information
→ structured metadata
→ focused SQL
→ fewer round trips

The common detour

dictionary query
dictionary query
more probing
sample rows “just to see”

Prompt it explicitly: “Use schema-information for metadata. Do not run dictionary queries unless I ask.”

Copyright © 2026, Oracle and/or its affiliates

ANNOTATIONS ARE PROMPT ENGINEERING THAT EVERYONE CAN REUSE

Teach the database what its own objects mean.

Old schema reality:

- cryptic names
- missing comments
- unclear relationships
- business meaning trapped in people's heads

AI Schema Enrichment

Group objects. Annotate tables, views, columns, and APIs. Put the "what this really means" context beside the data.

One bit of homework; every human and agent benefits.

Copyright © 2026, Oracle and/or its affiliates

ASK FOR A SUMMARY, THEN TURN IT INTO A SKILL

Turn a good run into institutional memory.

After a successful task, ask the agent to capture:

Trigger	When should this skill be used?
Procedure	What does it inspect, decide, and execute?
Guardrails	What can go wrong and how is it verified?

Real-world example

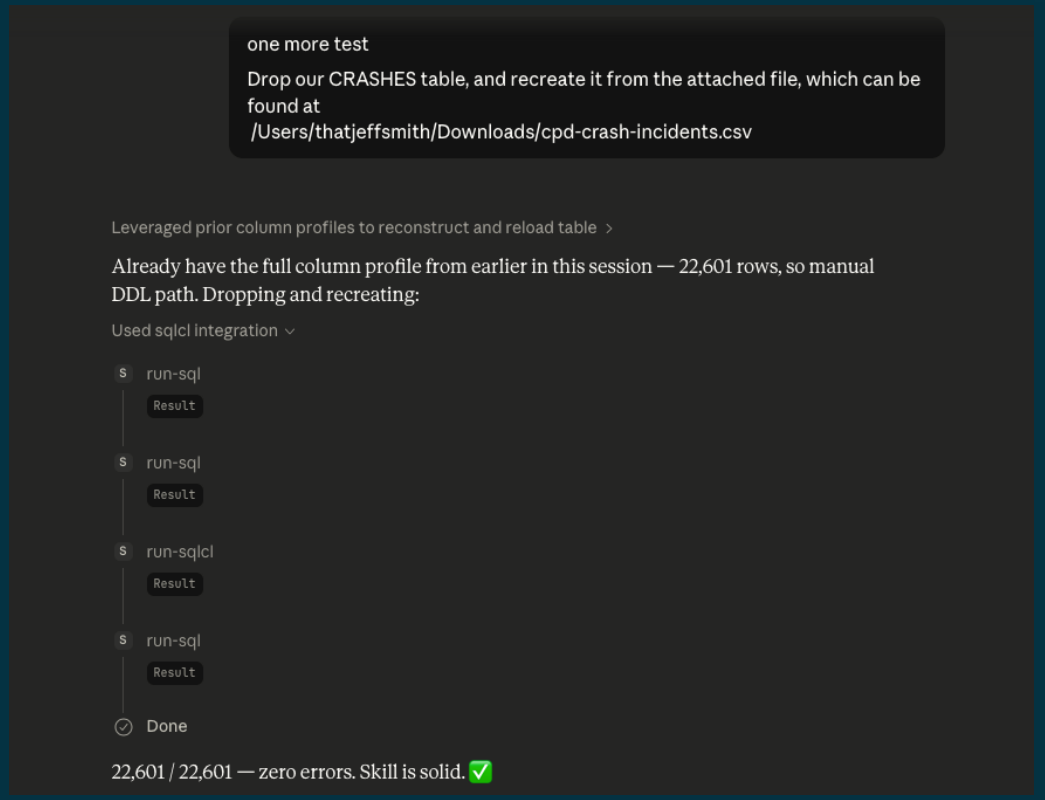
ETL / CSV load skill

The agent learned how to inspect data, choose settings, load it, check row counts, then improve the skill across runs.

Copyright © 2026, Oracle and/or its affiliates

ASK FOR A SUMMARY, THEN TURN IT INTO A SKILL

Turn a good run into institutional memory.





Copyright © 2026, Oracle and/or its affiliates

REQUIRE PROOF

“It generated code” is not the finish line.

Every code-generation request should also ask for:

- ✓ A test script / harness
- ✓ Happy-path test data
- ✓ Negative & edge-case coverage
- ✓ Expected results
- ✓ Cleanup / rollback steps

My favorite prompt add-on

“Generate the tests that prove this works — and show me the expected output before executing anything.”

Copyright © 2026, Oracle and/or its affiliates

REQUIRE PROOF

“The SQL is faster” is not the finish line.

Every SQL-tuning request should also ask for:

- ✓ A test script / harness
- ✓ Happy-path test data
- ✓ Negative & edge-case coverage
- ✓ Expected results
- ✓ Cleanup / rollback steps

My favorite prompt add-on

“Run some load tests before we implement this new index, and then again afterwards.

Compare.

Copyright © 2026, Oracle and/or its affiliates

PUT THIS NEXT TO YOUR AGENT

The “before you approve” checklist.

- ☐ Oracle skills loaded?
- ☐ Plan reviewed and agreed?
- ☐ Dedicated low-privilege account?
- ☐ Sandbox / Docker where possible?
- ☐ schema-information used?
- ☐ Scope and SQL understood?
- ☐ Tests + expected output ready?
- ☐ Good work summarized as a skill?

High expectations. Thoughtful prompts. Verify everything.

Copyright © 2026, Oracle and/or its affiliates

Takeways

1. You can bring your own LLM to your Oracle Database today via our MCP Server

2. This is free, secure, and supported via our database tools.

3. Today's agents & LLMs are amazing problem solvers – think BIG & TOMORROW.

Copyright © 2026, Oracle and/or its affiliates

Next Steps

Explore and learn more about our MCP Servers.

LiveLabs

Get hands-on with Oracle's products and technologies.
Always Free. Always Available. Always For Everyone.



FreeSQL

[Explore the MCP LiveLab]

Step-by-Step tutorials for getting started, including prompts to guide you on your Agentic AI development experience with the Oracle AI Database.

[Download SQLcl]

Get started with our local MCP Server for the Oracle Database.

Alternatively download our SQL Developer Extension for VS Code, which includes SQLcl.

[Try FreeSQL.com]

Oracle's free online portal for learning SQL and data management. Run in your browser or connect from your favorite development and query IDEs – perfect for exploring with your local agent via our MCP Server!

Copyright © 2026, Oracle and/or its affiliates

Upcoming Events & Feedback

Discover more developer events

Plug in virtually, or attend in-person, these upcoming events are just for developers:

oracle.com/developer/events/

Your feedback is important to us!

Tell us what you think. Please take our survey so we can keep improving our events:

bit.ly/your-feedback-090226

Thank you

Jeff blogs AI and MCP at

https://www.thatjeffsmith.com

Kris shares insight and news at

https://linkedin.com/in/krisrice



Copyright © 2026, Oracle and/or its affiliates


ORACLE