

Databricks: Agent Bricks – Agentic AI, narzędzia i governance

Szkolenie Databricks: Agent Bricks – Agentic AI to praktyczny kurs projektowania i budowy agentów AI w Databricks. Program koncentruje się na agencie, który sam wybiera i wywołuje narzędzia: wyszukiwanie w AI Search, funkcje Unity Catalog lub kontrolowane zapytania SQL, przy zachowaniu kontroli nad tym, do jakich danych i działań ma dostęp.

Uczestnicy przechodzą przez cały proces: od decyzji, czy problem wymaga agenta, czy wystarczy RAG, przez zdefiniowanie narzędzi i budowę agenta, po analizę jego działania w MLflow Tracing, testy niepożądanych wywołań i projekt uprawnień. Dzięki temu szkolenie kończy się prototypem agenta z ograniczoną listą narzędzi oraz planem jego bezpiecznego wdrożenia. Ćwiczenia opierają się na danych i dokumentach RetailOps (fikcyjna firma handlowa, na której danych realizujemy wszystkie ćwiczenia).



Odbiorcy szkolenia

Szkolenie jest przeznaczone dla osób technicznych, które chcą budować agentów AI działających na danych i narzędziach firmowych w Databricks.

W szczególności kurs sprawdzi się dla:

- inżynierów AI i ML, którzy mają doświadczenie z RAG i chcą przejść do agentów,
- programistów budujących asystentów wykonujących działania w systemach firmowych,
- architektów rozwiązań AI odpowiedzialnych za bezpieczeństwo i uprawnienia,
- zespołów, które planują produkcyjne wdrożenie agentów i potrzebują sposobu ich testowania.

Szkolenie będzie szczególnie wartościowe dla organizacji, które chcą korzystać z agentów, ale potrzebują jasnych zasad, do czego agent ma dostęp i jak sprawdzić jego zachowanie.



Korzyści

- RAG czy agent – dowiesz się, kiedy agent jest uzasadniony i jak ograniczyć jego autonomię do potrzeb przypadku użycia.
- Narzędzia agenta – nauczysz się udostępniać agentowi AI Search, funkcje Unity Catalog i kontrolowane zapytania SQL z jasnym kontraktem.
- Budowa agenta – zbudujesz własnego agenta z wywoływaniem narzędzi (tool calling) w Agent Bricks, platformie Databricks do tworzenia agentów w kodzie.
- Uprawnienia i bezpieczeństwo – poznasz zasadę najmniejszych uprawnień dla agenta i sposób ograniczania dostępu do danych przez Unity Catalog.
- Testowanie i ocena – nauczysz się analizować działanie agenta w MLflow Tracing, oceniać jego odpowiedzi i testować niepożądane zachowania.
- Droga do produkcji – poznasz opcje wdrożenia agenta i przygotujesz plan kolejnych kroków.



Program szkolenia

1. Moduł – RAG czy agent: wybór architektury

Cel modułu: uczestnik wie, czym agent różni się od RAG i kiedy warto go zbudować.

- Agent – model językowy, który sam decyduje, jakie narzędzie wywołać (wyszukiwarkę, zapytanie do bazy, funkcję biznesową), żeby wykonać zadanie
- Poziomy rozwiązań – prosty łańcuch, RAG, agent z narzędziami, kilka współpracujących agentów; rosnące możliwości, ale też koszt i ryzyko
- Granice autonomii – co agent może zrobić sam, a co wymaga zatwierdzenia przez człowieka
- Agent bez programowania (Genie Agent) a własny agent pisany w kodzie (Agent Bricks); dotychczasowe Knowledge Assistant i Supervisor Agent mają od października 2026 status legacy
- Wybór modelu – które modele potrafią wywoływać narzędzia
- Lab: uczestnik dobiera architekturę dla trzech przypadków użycia RetailOps

2. Moduł – Narzędzia agenta

Cel modułu: uczestnik przygotowuje narzędzia, z których agent może bezpiecznie korzystać.

- Funkcje Unity Catalog jako narzędzia – np. „sprawdź status zamówienia”, zapisane w SQL lub Python, z kontrolą uprawnień
- Wyszukiwanie w dokumentach (AI Search) jako narzędzie agenta
- Genie Agent (wcześniej Genie space) jako narzędzie do pytań o dane w tabelach (pokaz)
- Kontrolowane zapytania SQL – agent podaje tylko parametry do przygotowanego wcześniej zapytania (pokaz)
- Opis narzędzia – nazwa, opis i parametry decydują, czy model wybierze właściwe narzędzie

- Lab: uczestnik tworzy dwie funkcje (status zamówienia, zasady zwrotów) i sprawdza, jak agent z nich korzysta

3. Moduł – Budowa agenta

Cel modułu: uczestnik buduje działającego agenta i rozumie, jak podejmuje on decyzje.

- Pętla działania agenta – model wybiera narzędzie, otrzymuje wynik i decyduje o kolejnym kroku lub odpowiedzi
- Projekt agenta w Agent Bricks – szablon tworzony przez Agent Bricks CLI (Beta), lista narzędzi i ich uprawnień w pliku agent.toml, serwer agenta DurableAgentServer
- Biblioteki do budowy agentów: LangGraph, OpenAI Agents SDK (krótkie porównanie)
- Podłączenie funkcji Unity Catalog jako narzędzi agenta
- Testowanie agenta w AI Playground i w notebooku
- Lab: uczestnik buduje agenta z jednym narzędziem i analizuje jego decyzje

4. Moduł – Warsztat 1: agent z wyszukiwaniem i funkcją biznesową

Cel modułu: uczestnik łączy kilka narzędzi w jednym agencie.

- Warsztat: agent RetailOps, który przeszukuje dokumentację i sprawdza dane zamówień przez funkcję Unity Catalog. Efektem jest agent, który wykonuje kilka kroków i uzasadnia odpowiedź źródłami.
- Analiza nieudanych wywołań i poprawa opisów narzędzi

5. Moduł – Tożsamość, uprawnienia i granice danych

Cel modułu: uczestnik projektuje uprawnienia agenta tak, żeby nie miał dostępu do więcej, niż potrzebuje.

- W czym imieniu działa agent – na koncie technicznym (service principal) czy na uprawnieniach pytającego użytkownika (autoryzacja użytkownika, wcześniej on-behalf-of-user – Public Preview)
- Zasada najmniejszych uprawnień – dostęp tylko do potrzebnych funkcji, tabel i indeksów
- Filtry wierszy i maskowanie kolumn w Unity Catalog – jak wpływają na odpowiedzi agenta
- Unity Gateway – kontrola dostępu do modeli i serwerów MCP, limity, budżety, śledzenie użycia i kosztów (GA); zasady ochronne (service policies), np. filtry treści i wykrywanie danych wrażliwych (Beta) – omówienie
- Prompt injection – ochrona przed instrukcjami ukrytymi w dokumentach i danych
- Lab: uczestnik projektuje uprawnienia agenta i sprawdza jego odpowiedzi z drugiego konta, jeśli środowisko zapewnia drugie konto testowe; w przeciwnym razie pokaz trenera

6. Moduł – Ocena jakości i testy bezpieczeństwa

Cel modułu: uczestnik potrafi sprawdzić, czy agent działa poprawnie i bezpiecznie, zanim trafi do użytkowników.

- Śledzenie działania (MLflow Tracing) – które narzędzia zostały wywołane, z jakimi parametrami, ile to trwało i kosztowało (znajomość z DBX-RAG zakładamy, skupiamy się na wywołaniach narzędzi)
- Automatyczna ocena – poprawność odpowiedzi, wybór właściwego narzędzia, zgodność z zasadami firmy
- Testy niepożądanych zachowań (red teaming) – próby obejścia instrukcji, pytania o dane spoza zakresu
- Zachowanie awaryjne – odmowa, przekazanie sprawy człowiekowi, limit liczby kroków
- Warsztat 2: uczestnik uzupełnia przygotowany zestaw 10 przypadków testowych, uruchamia ocenę i

analizuje przebieg działania agenta. Efektem jest raport jakości i lista poprawek.

7. Moduł - Wdrożenie i dalsze kroki

Cel modułu: uczestnik wie, jak udostępnić agenta użytkownikom i monitorować go po wdrożeniu.

- Wdrożenie agenta poleceniem `agentbricks deploy` w Agent Runtime na Databricks Apps (zalecane dla nowych agentów); wdrożenie jako endpoint Model Serving ma status legacy - kiedy je spotkamy i jak migrować
- Monitorowanie po wdrożeniu - zapis zapytań i odpowiedzi, ocena jakości na rzeczywistym ruchu
- MCP - standard podłączania narzędzi do agentów; serwery MCP dostarczane przez Databricks i zewnętrzne, kontrolowane w Unity Gateway (serwer Genie One MCP - GA, pozostałe - Beta) - pokaz
- Pamięć agenta - historia rozmowy i fakty zapamiętywane między rozmowami (agent memory and sessions w Lakebase, Beta) - omówienie; plan kolejnej wersji rozwiązania



Oczekiwane przygotowanie uczestnika

- Ukończone szkolenie DBX-RAG (GenAI: RAG z AI Search) lub równoważne doświadczenie z AI Search, modelami językowymi i MLflow
- Znajomość Python na poziomie funkcji i skryptów
- Podstawowa znajomość Unity Catalog (uprawnienia; filtry wierszy i maskowanie krótko przypominamy)

Dla zwiększenia komfortu pracy oraz efektywności szkolenia zalecamy skorzystanie z dodatkowego ekranu. Brak dodatkowego ekranu nie jest przeciwwskazaniem do udziału w szkoleniu, ale w znaczący sposób wpływa na komfort pracy podczas zajęć

Informacje oraz wymagania dotyczące uczestniczenia w szkoleniach w formule zdalnej dostępne na: <https://www.altkomakademia.pl/jak-dzialamy/o-szkoleniach/?distance-learning>



Szkolenie obejmuje

* dostęp do portalu słuchacza AltKom Akademii

Metoda szkolenia:

- przygotowane środowisko Databricks z indeksem AI Search, endpointem modelu i danymi scenariusza RetailOps na czas szkolenia
- noteboki i materiały do ćwiczeń w formie elektronicznej

Uwaga: W trakcie wybranych szkoleń Akademia zapewnia Uczestnikom dostęp do płatnych narzędzi i usług niezbędnych do realizacji programu szkolenia (w szczególności usług Azure, oraz innych zasobów chmurowych). Uczestnik zobowiązany jest do korzystania z udostępnionych zasobów wyłącznie w zakresie wynikającym z agendy szkolenia oraz zgodnie z poleceniami trenera. Wykorzystywanie tych zasobów w sposób wykraczający poza zakres szkoleniowy, w szczególności do realizacji projektów

prywatnych, testowania dodatkowych usług, modyfikowania konfiguracji środowiska lub podejmowania działań generujących koszty niezwiązane z realizacją ćwiczeń – skutkować będzie obciążeniem Uczestnika kosztami przekraczającymi przewidziany limit, na podstawie wydatków poniesionych przez Akademię (<https://www.altkomakademia.pl/ogolne-warunki-uczestnictwa-w-szkoleniach/>)



Czas trwania

1 dni / 7 godzin

Język

Wykład: polski

Materiały: angielski