Configuring Databricks on AWS US East / West for FedRAMP Compliance

Version 2.0 - September 11, 2023

databricks

Table of Contents

1. Introduction

This page describes customer responsibilities under the Databricks’ FedRAMP Moderate authorization in AWS Commercial (US-East-1 and US-West-2 regions), and aligns with the Databricks FedRAMP SSP Version 2.0. Customers must implement the below outlined customer responsibilities in order to ensure the use of Databricks meets all of the FedRAMP requirements.

2. Databricks FedRAMP Authorization Package

The complete Databricks on AWS US East/West FedRAMP authorization package is located on https://max.omb.gov (Package ID #: FR1834740315). Government agencies may request access to the entirety of the Databricks authorization package, including the SSP and the Control Implementation Summary/Customer Responsibility Matrix (CIS/CRM), by submitting a Package Access Request Form to the FedRAMP PMO.

3. Databricks on AWS US East/West FedRAMP Moderate AWS Shared Responsibility Model

The Databricks on AWS US East/West FedRAMP Moderate Shared Responsibility Model outlines the responsibilities of both Databricks and the customer in meeting security and compliance requirements set forth by FedRAMP.

#	Category	Customer Responsibility	Applicable Controls
1	Workspace configuration	Enable the *compliance security profile*.	Various

2	Databricks audit logging and monitoring	Customers are responsible for configuring Databricks Audit Log Delivery, including granting the appropriate s3:GetBucketLocation permissions, log storage capacity configurations, and for monitoring log activity including but not limited to account creation, modification, enabling, disabling, and removal; access to the Databricks workspace; the use of accounts; and anti-virus alerts.	AC-2(g)
			AC-2(4)
			AC-2(12)(b)
			AC-11(a)
			AC-17(1)
			AU-4
			AU-5(a)
			AU-5(b)
			AU-6(b)
			AU-6(c)
			AU-6(1)
			AU-6(3)
			AU-7(a)
			AU-12(b)
			CM-7(2)
			CM-7(5)(a)

#	Category	Customer Responsibility	Applicable Controls

			CM-7(5)(b)
			CM-7(5)(c)
			CM-8(3)(b)
			CM-11(a)
			CM-11(b)
			CM-11(c)
			RA-5(11)
			SC-7(a)
			SC-7(b)
			SC-7(c)
			SC-13(b)
			SI-3(c)
			SI-3(d)
			SI-4(a)
			SI-4(c)
			SI-4(1)
			SI-4(2)
			SI-4(4)(a)
			SI-4(4)(b)
			SI-4(5)
			SI-6(c)
			SI-6(d)

3	Databricks classic compute host monitoring	Customers are responsible for ingesting and responding to Capsule8 alerts delivered to the customer's S3 bucket.	CM-7(2)
			CM-7(5)(a)
			CM-7(5)(b)
			CM-7(5)(c)
			CM-8(3)(b)
			CM-11(a)
			CM-11(b)
			CM-11(c)
			SI-3(c)
			SI-3(d)
			SI-4(a)

4	Databricks IP Access Restrictions	Customers are responsible for configuring IP access lists if they would like to further restrict access to their Databricks instance.	AC-4
			AC-14(a)
			AC-14(b)
			AC-17(a)
			AC-17(b)
			AC-20(a)
			AC-20(1)(a)
			SC-7(3)

#	Category	Customer Responsibility	Applicable Controls

5	Identity Management	Customers are responsible for selecting an identity provider which accepts FICAM-approved third-party credentials including the acceptance and verification of PIV credentials. Customers are responsible for configuring their single sign-on solution to initiate session timeouts, session terminations, disabling inactive accounts, and displaying a system use notification prior to redirecting users to the Databricks web application using their single sign-on solution and ensuring their access to Databricks meets applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance on cryptographic module authentication. Customers are also responsible for ensuring that single sign-on requires the use of multifactor authentication (MFA). (https://docs.databricks.com/administration-guide/users-groups/single-sign-on/index.html).	AC-2(1)
			AC-2(2)
			AC-2(3)(d)
			AC-7(a)
			AC-7(b)
			AC-8(a)
			AC-11(b)
			AC-11(1)
			AC-12
			AC-20(a)
			AC-20(1)(a)
			IA-2
			IA-2(1)
			IA-2(2)
			IA-2(6)(a)
			IA-2(6)(b)
			IA-2(8)
			IA-2(12)
			IA-4(a)
			IA-4(b)
			IA-4(c)
			IA-4(d)
			IA-4(4)
			IA-5(a)
			IA-5(b)
			IA-5(c)
			IA-5(d)
			IA-5(e)
			IA-5(f)
			IA-5(g)
			IA-5(h)
			IA-5(i)
			IA-5(1)(a)
			IA-5(1)(b)
			IA-5(1)(c)
			IA-5(1)(d)
			IA-5(1)(e)
			IA-5(6)
			IA-5(7)
			IA-7
			IA-8
			IA-8(1)
			IA-8(2)(a)
			IA-8(2)(b)
			IA-8(4)

#	Category	Customer Responsibility	Applicable Controls
			SA-4(10)

6	User Access Management	Customers are responsible for assigning customer users access to Databricks services, verifying the identity of their users, and administering permissions by employing the principle of least privilege and separation of duties through limiting access to privileged functions.
		- User Entitlements:
		https://docs.databricks.com/administration-guide/users-groups/users.html#manage-user-entitlements
		- Group Entitlements:
		https://docs.databricks.com/administration-guide/users-groups/groups.html#manage-a-groups-entitlements
		- Groups:
		https://docs.databricks.com/administration-guide/users-groups/groups.html
			AC-2(e)
			AC-2(f)
			AC-2(h)
			AC-2(7)(a)
			AC-2(7)(b)
			AC-2(7)(c)
			AC-2(7)(d)
			AC-2(9)
			AC-2(12)(a)
			AC-3
			IA-2
			IA-2(5)
			IA-4(a)
			IA-4(b)
			IA-4(c)
			IA-4(d)
			IA-4(4)
			IA-5(a)
			IA-5(b)
			IA-5(c)
			IA-5(d)
			IA-5(e)
			IA-5(f)
			IA-5(g)
			IA-5(h)
			IA-5(i)
			IA-5(1)(a)
			IA-5(1)(b)
			IA-5(1)(c)
			IA-5(1)(d)
			IA-5(1)(e)
			IA-5(7)
			IA-6
			IA-8

7	Security Awareness Training	Customers are responsible for providing basic security awareness training, including training on recognizing and reporting potential indicators of insider threats, as part of onboarding, at least annually after initial training is provided, and whenever a significant change occurs. Additionally, the customer is responsible for providing role-based security training to personnel with assigned security roles and responsibilities. The customer is responsible for documenting, monitoring, and retaining security training records for their users.	AT-2(a)
			AT-2(b)
			AT-2(c)
			AT-2(d)
			AT-2(2)
			AT-2(3)
			AT-3(a)
			AT-3(b)
			AT-3(c)
			AT-4(a)

#	Category	Customer Responsibility	Applicable Controls
			AT-4(b)

8	Disaster Recovery	Customers are responsible for establishing necessary agreements with AWS and implementing a disaster recovery environment for Databricks that includes the availability of customer's data sources. (https://docs.databricks.com/administration-guide/disaster-recovery.html)	CP-2(8)
			CP-6(b)
			CP-6(1)
			CP-6(3)
			CP-7(a)
			CP-7(b)
			CP-7(c)
			CP-7(1)
			CP-7(2)
			CP-7(3)
			CP-8
			CP-8(1)(a)
			CP-8(1)(b)
			CP-8(2)
			CP-9(a)
			CP-9(d)
			CP-9(1)
			CP-10

9	Customer AWS Account & Infrastructure	Customers are responsible for managing the networking of their AWS account. Customers are responsible for managing connections to/from their Databricks workspace including, but not limited to the following: • IP access lists to further restrict access to their Databricks instance.	AC-4 SC-7(3)

10	Library Usage	Customers are responsible for controlling the software they import (Libraries).	CM-8(3)(b)
			SC-7(3)

11	Data Sources	Customers are responsible for mounting their data sources and protecting the confidentiality and integrity of data sources.	AC-4
			AC-20(1)(b)
			SC-7(3)

12	Data Sharing	Customers are responsible for using Databricks workspace access controls (https://docs.databricks.com/security/access-control/workspace-acl.html) when sharing folders and notebooks.
		
		Customers are responsible for acting as a “Data Provider” when using Delta Sharing (https://docs.databricks.com/delta-sharing/recipient.html).
			AC-21(a)
			AC-21(b)

13	Incident Reporting	Customers are responsible for reporting incidents to Databricks preferably by filling out a support ticket, but alternatively via the Report an Issue form at databricks.com/trust.	IR-6(b)

14	Data Exfiltration	The customer is responsible for protecting their data from exfiltration, such as mechanisms described in the following	SC-7(12)
			SI-4(18)

#	Category	Customer Responsibility	Applicable Controls
		link: https://www.databricks.com/blog/2021/02/02/data-exfiltration-protection-with-databricks-on-aws.html.	

15	Encryption	Customers are responsible for configuring and supporting their cryptographic keys.
		
		Customers are responsible for allowing Databricks to GetBucketLocation to ensure Databricks uses the FIPS AWS S3 endpoint for Audit Log Delivery.
			SC-13(a)
			SC-13(b)

16	Network Configuration	Customers are responsible for using Customer-managed VPC (https://docs.databricks.com/administration-guide/cloud-configurations/aws/customer-managed-vpc.html) and ensuring the Databricks data plane components request and perform data origin authentication and data integrity verification on the name/address resolution responses for the system receives from authoritative sources.	SC-21
17	Data Confidentiality and Integrity	Customers are responsible for protecting the confidentiality and integrity of their data sources, such as Google BigQuery, MongoDB, Amazon Redshift, CSV files, images, JSON files, MLflow experiments, Parquet files, XML files, and Zip files. (https://docs.databricks.com/data/data-sources/index.html)	SC-28(1)