AgentCore Tools

What are AgentCore Tools?

AgentCore Tools provides **secure, managed capabilities** for AI agents to execute code and interact with web resources through fully managed, built-in tools - eliminating infrastructure management while maintaining enterprise-grade security.

Learn more about AgentCore Tools

Key Components

AgentCore Tools consists of two primary tools and supporting infrastructure:

- **Code Interpreter**: A secure environment for executing code in multiple languages and processing data. Learn more about AgentCore Code Interpreter features
- **Browser Tool**: A managed service for web interactions, enabling AI agents to navigate and interact with websites. Learn more about AgentCore Browser features
- **Resource Management**: Handles configurations, permissions, and feature toggles for both tools.
- **Security Controls**: Ensures secure operations through IAM integration, session isolation,

and access restrictions.

- **Observability**: Provides monitoring and replay capabilities for both Code Interpreter and Browser Tool sessions.

How the AgentCore tools work (General Flow)

1. **Tool Resource Creation**
   - Developer configures tool settings and

   - Agent requests tool session
   - System creates isolated runtime in a dedicated microVM with isolated CPU, memory, and filesystem resources
   - Session maintains state during configurable session lifetime
3. **Tool Execution**
   - Agent invokes tool capabilities
   - Operations run in isolated environment
   - Results stream back to agent
   - Tool maintains active monitoring and logging
4. **Resource Cleanup**
   - Automatic cleanup after session timeout
   - Resources automatically released
   - Logs and metrics preserved

Labs:

AWS account access

Workshop catalog in AWS Builder Center

Content preferences

Exit event

In the following labs, you'll learn how to:

- **Lab: Advanced Data Analysis with Code Interpreter** - convert existing AWS Lambda functions into fully managed MCP servers without managing infrastructure.
- **Lab: Amazon Bedrock AgentCore Browser Tool with the Amazon Nova Act SDK and Browser-Use SDK** - build agents that leverage the AgentCore Browser Tool's secure, production-ready, and fully managed browser environment with the Amazon Nova Act SDK and Browser-Use SDK.

Previous Next