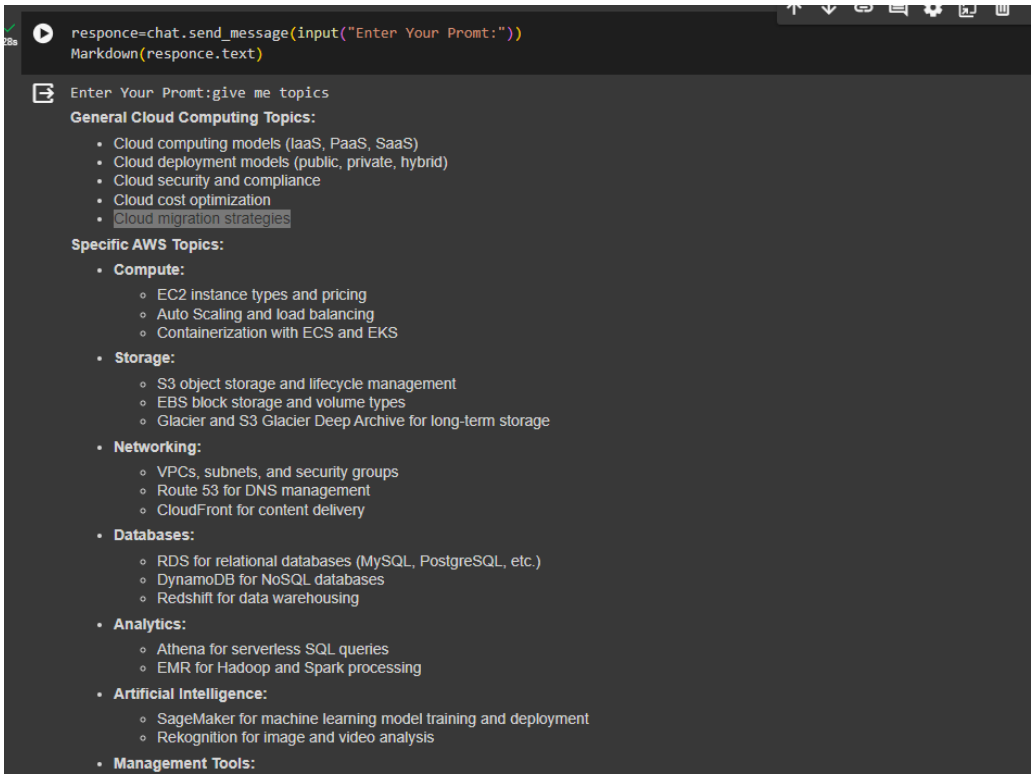
SIMPLE CHATBOT THAT READS AWS DEVELOPER GUIDE DOCUMENT AND ANSWERS OUR QUESTIONS – Sample outputs



```
prompt=input("Enter Your Prompt:")
responce=chat.send_message(f"{prompt},As per the above document")
Markdown(responce.text)
```

```
Enter Your Prompt:aws developer guide
```

AWS Developer Guide

Key Points:

- Provides comprehensive documentation and tutorials for AWS services and features.
- Covers best practices and patterns for designing, developing, and deploying applications on AWS.
- Offers code samples, reference materials, and troubleshooting tips.

Sections:

- **Getting Started:** Introduces AWS and its core concepts, including accounts, regions, and services.
- **Services:** Detailed documentation for each AWS service, including usage instructions, pricing information, and code samples.
- **Tutorials:** Step-by-step guides for common development tasks, such as creating EC2 instances, deploying web applications, and using databases.
- **Best Practices:** Guidance on designing and developing scalable, secure, and cost-effective applications on AWS.
- **Reference:** Technical specifications, data formats, and API documentation for AWS services.

Benefits:

- **Accelerated development:** Provides comprehensive resources to help developers quickly learn and use AWS services.
- **Improved code quality:** Guides developers towards best practices and patterns for building reliable and efficient applications.
- **Reduced troubleshooting time:** Offers troubleshooting tips and code samples to help developers resolve common issues.
- **Enhanced security:** Provides guidance on implementing security measures to protect applications and data on AWS.
- **Cost optimization:** Helps developers understand AWS pricing models and optimize their applications for cost-effectiveness.

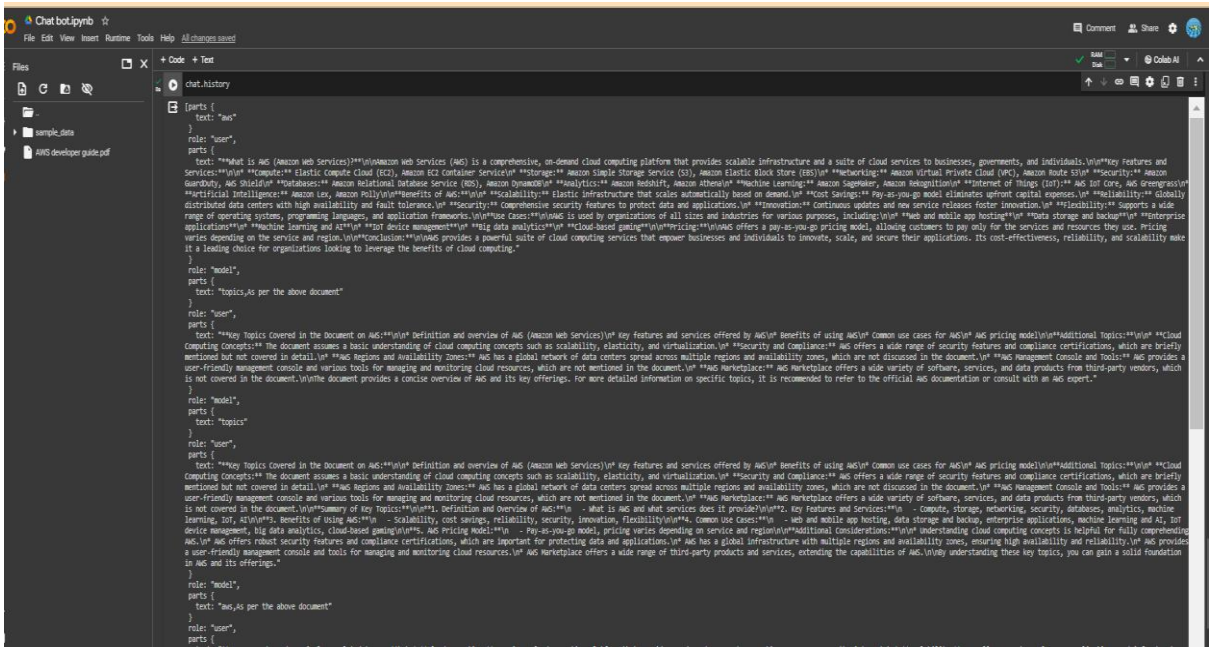
Use Cases:

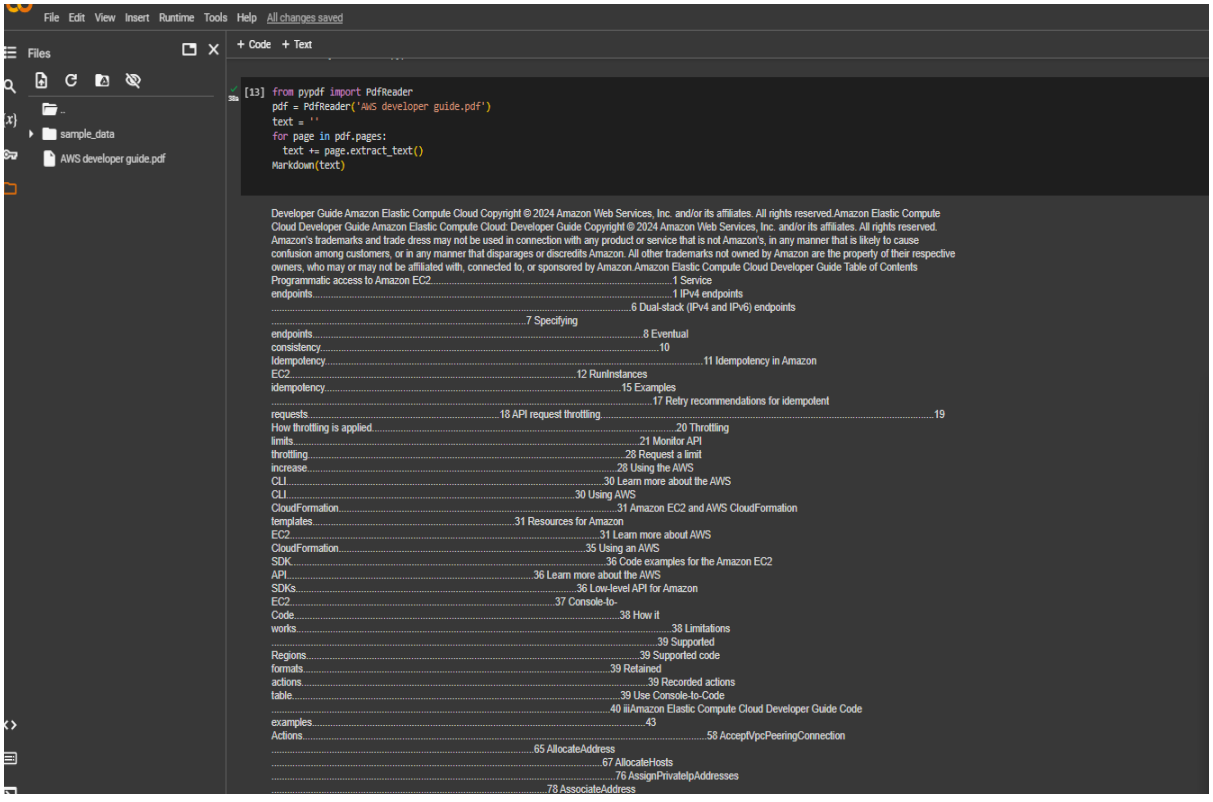
- Developers building new applications on AWS
- Developers migrating existing applications to AWS
- Developers looking to improve the performance and security of their AWS applications
- Developers preparing for AWS certifications

Additional Resources:

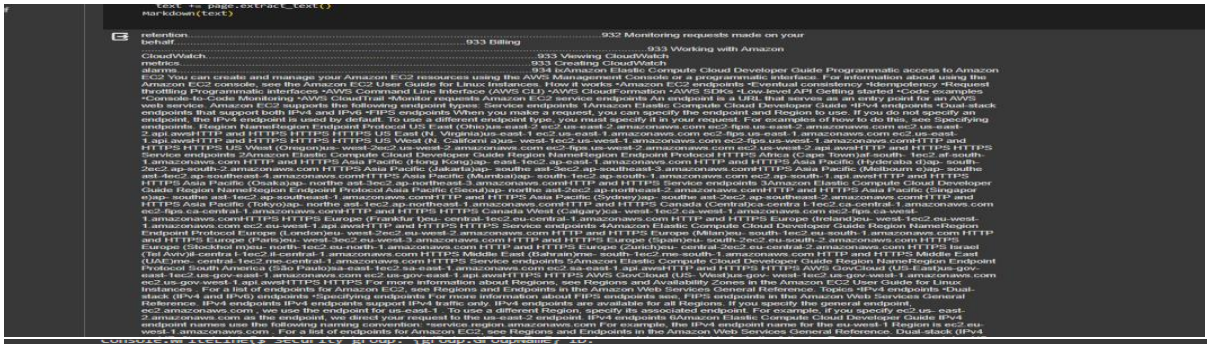
- AWS Developer Guide
- AWS Documentation
- AWS Code Samples
- AWS Forums

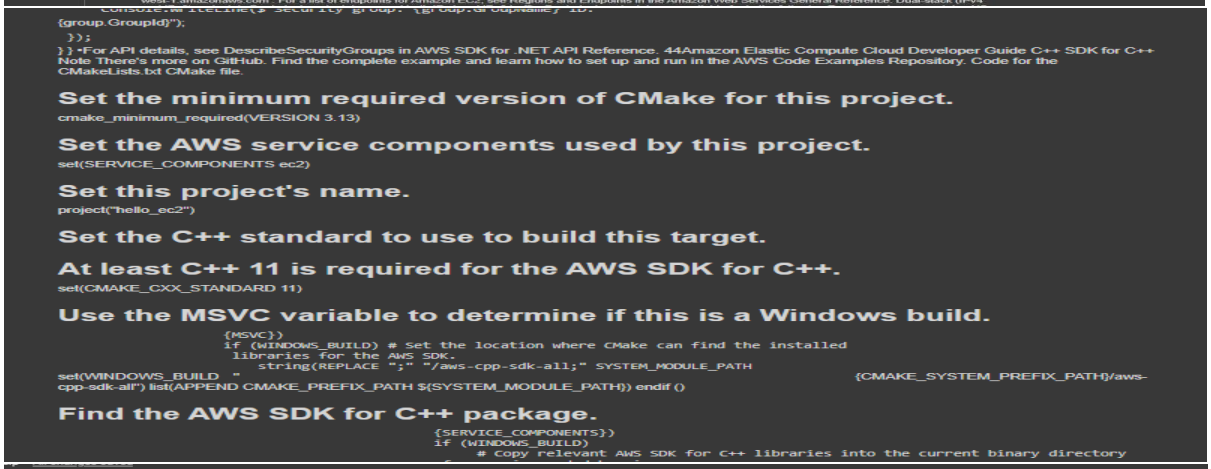

```
AWS offers a wide range of services, including compute, storage, networking, security, databases, analytics, machine learning, IoT, and AI.\n* **Pay-as-you-go Pricing:** AWS follows a pay-as-you-go pricing model, where you only pay for the services and resources you use.\n\n**Key Benefits of Using AWS:**\n\n* **Cost Savings:** AWS eliminates the need for upfront capital expenses and allows you to pay only for the resources you use.\n* **Scalability and Elasticity:** AWS provides the ability to scale your applications and infrastructure up or down as needed, without any downtime.\n* **Reliability and Availability:** AWS has a global network of data centers and multiple availability zones to ensure high availability and reliability for your applications.\n* **Security:** AWS offers a wide range of security features and compliance certifications to protect your data and applications.\n* **Innovation:** AWS is constantly innovating and releasing new services and features, allowing you to stay at the forefront of technology.\n* **Flexibility:** AWS supports a wide range of operating systems, programming languages, and application frameworks, giving you the flexibility to build and deploy applications using the tools you prefer.\n\n**Common Use Cases for AWS:**\n\n* Web and mobile app hosting\n* Data storage and backup\n* Enterprise applications\n* Machine learning and AI\n* IoT device management\n* Big data analytics\n* Cloud-based gaming\n\n**Conclusion:**\n\nAWS is a comprehensive cloud computing platform that provides a wide range of services and benefits to businesses and individuals. By understanding the key concepts and terminology related to AWS, you can leverage its capabilities to innovate, scale, and secure your applications and infrastructure."
  }
  role: "model",
  parts {
    text: "aes devoper guide,As per the above document"
  }
  role: "user",
  parts {
    text: "**Key Concepts and Terminology Related to AES Developer Guide:**\n\n* **AES (Advanced Encryption Standard):** A symmetric block cipher that is widely used for encrypting and decrypting data.\n* **Block Cipher:** A type of encryption algorithm that operates on fixed-size blocks of data.\n* **Key:** A secret value used to encrypt and decrypt data.\n* **Initialization Vector (IV):** A random value used to initialize the encryption process and prevent identical plaintext from producing identical ciphertext.\n* **Ciphertext:** The encrypted form of plaintext.\n* **Plaintext:** The original, unencrypted data.\n* **Encryption:** The process of converting plaintext into ciphertext.\n* **Decryption:** The process of converting ciphertext back into plaintext.\n* **Key Schedule:** A set of round keys derived from the original key, used in the encryption and decryption process.\n* **Round:** A single iteration of the encryption or decryption algorithm.\n* **S-Box:** A substitution box used in the encryption and decryption process to provide non-linearity.\n\n**Key Steps in AES Encryption and Decryption:**\n\n**Encryption:**\n\n1. Convert the plaintext into a block of 128 bits.\n2. Apply the initial round key to the block.\n3. Perform a series of rounds (typically 10, 12, or 14), each consisting of:\n    * SubBytes: Substitute each byte in the block using an S-Box.\n    * ShiftRows: Shift the rows of the block cyclically.\n    * MixColumns: Perform a linear transformation on the columns of the block.\n    * AddRoundKey: Apply the round key to the block.\n4. Apply the final round key to the block.\n\n**Decryption:**\n\n1. Convert the ciphertext into a block of 128 bits.\n2. Apply the final round key to the block (in reverse order).\n3. Perform a series of inverse rounds, each consisting of:\n    * AddRoundKey: Apply the round key to the block (in reverse order).\n    * MixColumns: Perform an inverse linear transformation on the columns of the block.\n    * ShiftRows: Shift the rows of the block cyclically in reverse order.\n    * SubBytes: Substitute each byte in the block using an inverse S-Box.\n4. Apply the initial round key to the block (in reverse order).\n\n**Conclusion:**\n\nThe AES Developer Guide provides detailed information on the AES encryption and decryption algorithms, including the mathematical operations involved and implementation considerations. By understanding the key concepts and steps involved in AES, developers can effectively use it to protect sensitive data in their applications and systems."
  }
  role: "model",
  parts {
    text: "topics"
  }
  role: "user",
  parts {
    text: "**Key Topics Covered in the AES Developer Guide:**\n\n* Overview of AES (Advanced Encryption Standard)\n* AES Encryption Algorithm\n* AES Decryption Algorithm\n* Key Expansion and Round Keys\n* Implementation Considerations\n* Security Analysis and Attacks\n\n**Additional Topics:**\n\n* **Modes of Operation:** AES can be used in different modes of operation, such as ECB, CBC, and CTR, to provide additional security and flexibility.\n* **Padding Schemes:** Padding schemes are used to ensure that the plaintext is a multiple of the block size before encryption.\n* **Key Management:** Proper key management practices are essential to ensure the security of AES encryption.\n* **Performance Optimization:** Techniques for optimizing the performance of AES encryption and decryption algorithms.\n* **Hardware Implementations:** Hardware implementations of AES can provide significant performance improvements for high-throughput applications.\n\n**Summary of Key Topics:**\n\n**1. Overview of AES:**\n   - History, design principles, and applications of AES\n\n**2. AES Encryption Algorithm:**\n   - Step-by-step description of the encryption process, including SubBytes, ShiftRows, MixColumns, and AddRoundKey\n\n**3. AES Decryption Algorithm:**\n   - Step-by-step description of the decryption process, including inverse operations of SubBytes, ShiftRows, MixColumns, and AddRoundKey\n\n**4. Key Expansion and Round Keys:**\n   - Derivation of round keys from the original key using the key expansion algorithm\n\n**5. Implementation Considerations:**\n   - Data representation, endianness, and memory alignment for efficient AES implementation\n\n**6. Security Analysis and Attacks:**\n   - Known attacks against AES and countermeasures to mitigate them\n\n**Additional Considerations:**\n\n* Understanding modes of operation, padding schemes, and key management is important for secure and efficient use of AES.\n* Performance optimization techniques can improve the throughput of AES implementations.\n* Hardware implementations can provide significant performance advantages for high-volume encryption tasks.\n\nBy understanding these key topics, developers can effectively implement AES encryption and decryption in their applications and systems to protect sensitive data."
  }
  role: "model",
  parts {
    text: "aws developer guide,As per the above document"
  }
  role: "user",
  parts {
    text: "**Key Concepts and Terminology Related to AWS Developer Guide:**\n\n* **AWS (Amazon Web Services):** A comprehensive cloud computing platform that provides a wide range of services to businesses and individuals.\n* **Developer Guide:** A technical documentation that provides detailed instructions and best practices for developing applications on a specific platform or using a specific technology.\n* **SDK (Software Development Kit):** A set of tools and libraries that allows developers to interact with AWS services programmatically.\n* **API (Application Programming Interface):** A set of protocols and routines that define how applications interact with each other or with external services.\n* **Credentials:** Unique identifiers and secret keys used to authenticate and authorize access to AWS services.\n* **Regions and Availability Zones:** AWS has a global network of data centers located in multiple regions and availability zones to ensure high availability and reliability.\n* **Services:** AWS offers a wide range of services, including compute, storage, networking, security, databases, analytics, machine learning, IoT, and AI.\n\n**Key Steps for Developing on AWS:**\n\n1. **Create an AWS account:** Sign up for an AWS account and set up your credentials.\n2. **Choose a region:** Select the AWS region where you
```

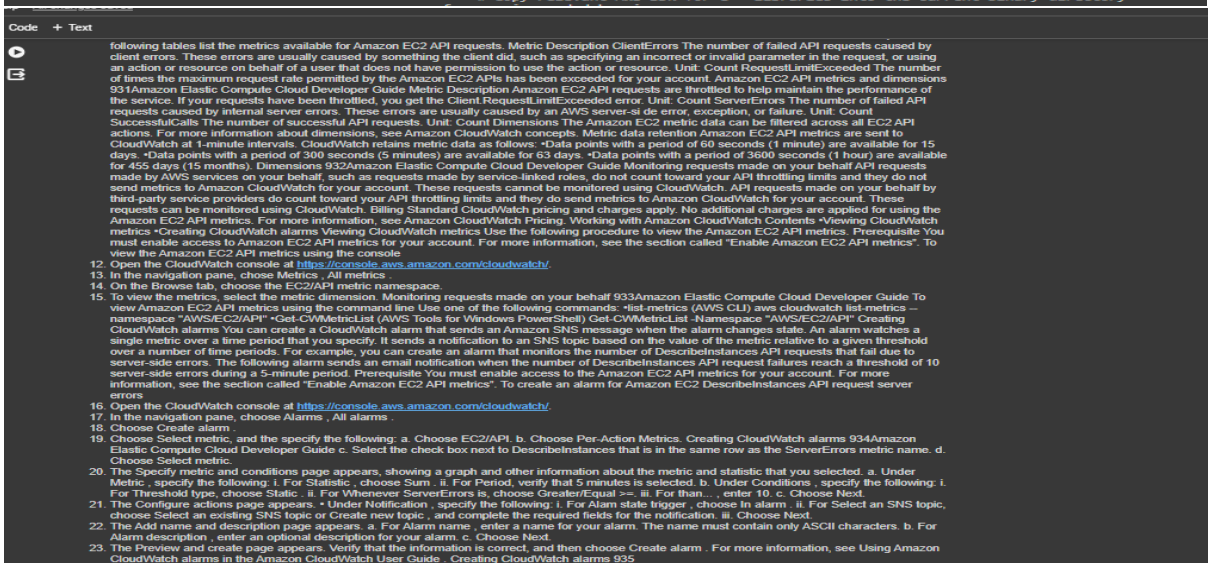




Developer Guide Amazon Elastic Compute Cloud Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.Amazon Elastic Compute Cloud Developer Guide Amazon Elastic Compute Cloud: Developer Guide Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved. Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.Amazon Elastic Compute Cloud Developer Guide Table of Contents







Code + Text

following tables list the metrics available for Amazon EC2 API requests. Metric Description ClientErrors The number of failed API requests caused by client errors. These errors are usually caused by something the client did, such as specifying an incorrect or invalid parameter in the request, or using an action or resource on behalf of a user that does not have permission to use the action or resource. Unit: Count RequestLimitExceeded The number of times the maximum request rate permitted by the Amazon EC2 APIs has been exceeded for your account. Amazon EC2 API metrics and dimensions 931Amazon Elastic Compute Cloud Developer Guide Metric Description Amazon EC2 API requests are throttled to help maintain the performance of the service. If your requests have been throttled, you get the Client.RequestLimitExceeded error. Unit: Count ServerErrors The number of failed API requests caused by internal server errors. These errors are usually caused by an AWS server-si de error, exception, or failure. Unit: Count SuccessfulCalls The number of successful API requests. Unit: Count Dimensions The Amazon EC2 metric data can be filtered across all EC2 API actions. For more information about dimensions, see Amazon CloudWatch concepts. Metric data retention Amazon EC2 API metrics are sent to CloudWatch at 1-minute intervals. CloudWatch retains metric data as follows: •Data points with a period of 60 seconds (1 minute) are available for 15 days. •Data points with a period of 300 seconds (5 minutes) are available for 63 days. •Data points with a period of 3600 seconds (1 hour) are available for 455 days (15 months). Dimensions 932Amazon Elastic Compute Cloud Developer Guide Monitoring requests made on your behalf API requests made by AWS services on your behalf, such as requests made by service-linked roles, do not count toward your API throttling limits and they do not send metrics to Amazon CloudWatch for your account. These requests cannot be monitored using CloudWatch. API requests made on your behalf by third-party service providers do count toward your API throttling limits and they do send metrics to Amazon CloudWatch for your account. These requests can be monitored using CloudWatch. Billing Standard CloudWatch pricing and charges apply. No additional charges are applied for using the Amazon EC2 API metrics. For more information, see Amazon CloudWatch Pricing. Working with Amazon CloudWatch Contents •Viewing CloudWatch metrics •Creating CloudWatch alarms Viewing CloudWatch metrics Use the following procedure to view the Amazon EC2 API metrics. Prerequisite You must enable access to Amazon EC2 API metrics for your account. For more information, see the section called "Enable Amazon EC2 API metrics". To view the Amazon EC2 API metrics using the console

12. Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
13. In the navigation pane, chose Metrics , All metrics .
14. On the Browse tab, choose the EC2/API metric namespace.
15. To view the metrics, select the metric dimension. Monitoring requests made on your behalf 933Amazon Elastic Compute Cloud Developer Guide To view Amazon EC2 API metrics using the command line Use one of the following commands: •list-metrics (AWS CLI) aws cloudwatch list-metrics --namespace "AWS/EC2/API" •Get-CWMetricList (AWS Tools for Windows PowerShell) Get-CWMetricList -Namespace "AWS/EC2/API" Creating CloudWatch alarms You can create a CloudWatch alarm that sends an Amazon SNS message when the alarm changes state. An alarm watches a single metric over a time period that you specify. It sends a notification to an SNS topic based on the value of the metric relative to a given threshold over a number of time periods. For example, you can create an alarm that monitors the number of DescribeInstances API requests that fail due to server-side errors. The following alarm sends an email notification when the number of DescribeInstances API request failures reach a threshold of 10 server-side errors during a 5-minute period. Prerequisite You must enable access to the Amazon EC2 API metrics for your account. For more information, see the section called "Enable Amazon EC2 API metrics". To create an alarm for Amazon EC2 DescribeInstances API request server errors
16. Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
17. In the navigation pane, choose Alarms , All alarms .
18. Choose Create alarm .
19. Choose Select metric, and the specify the following: a. Choose EC2/API. b. Choose Per-Action Metrics. Creating CloudWatch alarms 934Amazon Elastic Compute Cloud Developer Guide c. Select the check box next to DescribeInstances that is in the same row as the ServerErrors metric name. d. Choose Select metric.
20. The Specify metric and conditions page appears, showing a graph and other information about the metric and statistic that you selected. a. Under Metric , specify the following: i. For Statistic , choose Sum . ii. For Period, verify that 5 minutes is selected. b. Under Conditions , specify the following: i. For Threshold type, choose Static . ii. For Whenever ServerErrors is, choose Greater/Equal >= . iii. For than... , enter 10. c. Choose Next.
21. The Configure actions page appears. • Under Notification , specify the following: i. For Alarm state trigger , choose In alarm . ii. For Select an SNS topic, choose Select an existing SNS topic or Create new topic , and complete the required fields for the notification. iii. Choose Next.
22. The Add name and description page appears. a. For Alarm name , enter a name for your alarm. The name must contain only ASCII characters. b. For Alarm description , enter an optional description for your alarm. c. Choose Next.
23. The Preview and create page appears. Verify that the information is correct, and then choose Create alarm . For more information, see Using Amazon CloudWatch alarms in the Amazon CloudWatch User Guide . Creating CloudWatch alarms 935

SIMPLE CHATBOT USING GEMINI -Sample outputs