Shodhshauryam, International Scientific Refereed Research Journal
Available online at : www.shisrrj.com
OPEN ACCESS
© 2024 SHISRRJ | Volume 7 | Issue 2
ISSN : 2581-6306
doi : https://doi.org/10.32628/SHISRRJ

Application Gateway Implementation with Azure

Minchala Sai Krishna[1], K. Padmanaban[2]

[1]Post Graduate, Department of MCA, Annamacharya Institute of Technology & Sciences, Tirupati, Andhra Pradesh, India

[2]Assistant Professor, Department of MCA, Annamacharya Institute of Technology & Sciences, Tirupati, Andhra Pradesh, India

Article Info

Article History
Received : 25 March 2024
Published : 05 April 2024

Publication Issue :
March-April-2024
Volume 7, Issue 2

Page Number : 364-369

ABSTRACT

You can control the amount of traffic going to your online applications with Azure Application Gateway, a load balancer for web traffic (OSI layer 7). Conventional load balancers route traffic based on source IP address and port to a destination IP address and port at the transport layer Application Gateways provide the ability to route requests based on additional information contained in the HTTP request, such as the host headers or URI path. For instance, traffic can be routed according to the incoming URL. You can thus direct traffic to a particular group of servers (referred to as a pool) that are set up for images if the incoming URL has the prefix /images. If the URL contains /video, that traffic is diverted to an additional optimized pool. You can set up host name or domain name routing for many web applications on the same application gateway using Application Gateway. It lets you join up to 100+ websites to a single application gateway, enabling you to create deployments with a more efficient topology. It is possible to route each website to a different backend pool. For instance, the IP address of the application gateway is pointed to by the three domains contoso.com, fabrikam.com, and adatum.com. Three multi-site listeners would be created, and each listener would be set up for the appropriate port and protocol.

Keywords: Azure Application Gateway, Load balancer, OSI layer 7, Web traffic management, URL-based routing, Backend pool, Session affinity, TLS termination, Web application firewall (WAF), Encryption, Azure services, On-premises data center, Traffic mediation.

I. INTRODUCTION

Azure Application Gateway is an Azure service that processes traffic to web apps that are hosted on a pool of web servers. The processing performed by Azure Application Gateway includes load balancing HTTP traffic and inspecting traffic

using web application firewall. It also includes encrypting traffic between users and an application gateway, and encrypting traffic between application servers and an application gateway Adatum is a new and expanding online commerce store that sells industrial drones. You're responsible for networking at the company Adatum has several web applications that are hosted on computers in its on-premises data centre. At the moment, a special but aging hardware device is deployed on the Adatum perimeter network that manages traffic to the web applications hosted on these computers. You want to retire this device and have traffic mediated by an Azure service.

To meet your goals, you need to ensure that the Azure service replicates the functionality that the special hardware currently provides. Important functionality that must be present in the replacement service.

II. LITERATURE REVIEW

Examining the Literature on application gateway implementation with azure

Azure focuses on examining existing research, publications, and documentation related to the utilization of Azure Application Gateway for managing web traffic and load balancing in cloud environments. Various sources such as academic papers, technical articles, and vendor documentation are reviewed to understand the features, capabilities, and best practices associated with Azure Application Gateway deployment.The literature that is currently available emphasizes the importance of Azure Application Gateway as an OSI layer 7 web traffic load balancer that allows for effective routing decisions based on HTTP request attributes.Studies emphasize its ability to route traffic based on URI paths, host headers, and other HTTP attributes, offering granular control over traffic management. Furthermore, the literature highlights how Azure Application Gateway can improve security by mitigating risks like SQL injection and cross-site scripting attacks through features like TLS termination, session affinity, and integration with web application firewalls (WAFs).

An over view of the Azure cloud service PAAS service and Storage account

One instance of a platform as a service (PaaS) is Azure Cloud Services. This technology is intended to support apps that are scalable, dependable, and low-cost to run, much like Azure App Service. Azure Cloud Services are hosted on virtual machines (VMs), just as App Service. On the other hand, the VMs are more in your hands. On virtual machines (VMs) that make use of Azure Cloud Services, you can remotely access and install your own applications. Creating virtual machines is not necessary while using Azure Cloud Services. Rather, you supply Azure with a configuration file that specifies how many of each you want, for example, "three web role instances" and "two worker role instances."

Platform-as-a-service (PaaS) is a distributed computing concept in which consumers use the Internet to rent hardware and software from an external provider. These are usually necessary to improve the application. The PaaS provider uses its own framework for programming and equipment. As such, it frees designers from having to install hardware and software in order to run or create another application. Press gadget is used in a simple and practical way. Generally speaking, customers pay for each usage premise. By using local alternatives, an association can take over for

PAS that takes prospective cost investment funds into consideration.

Azure storage Account:

All of the data services from Azure storage are gathered together in an Azure Storage Account, which is a resource (Azure blobs, Azure files, Azure Queues, and Azure Tables). This aids in our collective management of them all. All of the services within the storage account are subject to the policies we establish when the account is created or modified thereafter. All installed storage services and the data they contain are deleted when a storage account is deleted.

III. METHODOLOGY

Approach

Azure Application Gateway involves several key steps. Firstly, a thorough analysis of the existing infrastructure and traffic patterns is conducted to identify the specific requirements and challenges. Then, a detailed design is developed, outlining the configuration of the Application Gateway, including routing rules, backend pools, and security policies. Next, the implementation phase involves deploying the Application Gateway within the Azure environment according to the design specifications, ensuring proper integration with existing resources. Throughout the process, thorough testing is conducted to validate the functionality and performance of the Application Gateway, including load balancing, routing, and security features. Finally, ongoing monitoring and optimization are essential to ensure the continued effectiveness and scalability of the Application Gateway solution.

Implementation

Deploying an Azure virtual network's web traffic load balancer is a prerequisite for implementing Azure Application Gateway.

This gateway operates at OSI layer 7, allowing for URL-based routing and session affinity. It supports features like TLS termination, web application firewall (WAF) integration, and security filtering to protect against malicious attacks. By configuring backend pools and routing rules, organizations can efficiently manage traffic to their web applications hosted on Azure. Additionally, Azure Application Gateway provides scalability, high availability, and seamless integration with other Azure services, making it a versatile solution for optimizing web traffic management in the cloud.

Characteristics

Implementing Azure Application Gateway offers several key characteristics that enhance the management and optimization of web traffic. Firstly, it operates at OSI layer 7, allowing for the making of complex routing decisions using HTTP properties like host headers and URI paths. This makes URL-based routing easier. Directing traffic to specific backend pools tailored for different purposes, such as serving images or videos. Additionally, Application Gateway supports TLS termination, reducing CPU overhead for encryption and decryption operations. Moreover, its integration with Web Application Firewall (WAF) provides robust security features, guarding against common threats like SQL injection and cross-site scripting attacks. With scalability, high availability, and seamless integration with other Azure services, Application Gateway offers a comprehensive solution for efficiently managing and securing web applications in the cloud.

Data preprocessing

Data preprocessing may involve TLS termination to optimize encryption and decryption operations, ensuring efficient utilization of CPU resources on the backend servers. By effectively preprocessing the data, Azure Application Gateway enhances the reliability, security, and performance of web applications hosted on the Azure platform.

Preprocessing Data

Preprocessing data for Azure Application Gateway implementation involves gathering and organizing relevant information about web applications, backend servers, routing requirements, and security policies, it involves assessing the scalability and high availability requirements, as well as considering any compliance or regulatory considerations. For the Application Gateway to be configured and deployed in the Azure environment without a hitch, the data must be processed and organized after it has been gathered.

IV.EXPERIMENTAL SETUP

Azure Application Gateway, several Azure services will be utilized. Firstly, Azure Cloud Service will provide the platform for deploying and managing the application gateway. This service offers scalability, reliability, and cost-effectiveness, making it an ideal choice for hosting cloud-based solutions.

To provide scalable and safe storage options, the Storage Account will serve as a container for data services including files, queues, tables, and blobs.

Meanwhile, the App Service will host the web applications that will be load-balanced by the Application Gateway. App Service offers features like automatic scaling, continuous deployment, and integration with various programming languages and frameworks.

By integrating these services, the experimental setup will enable the deployment of the Application Gateway, allowing for efficient traffic management, URL-based routing, TLS termination, and security filtering. This setup will provide a comprehensive environment for testing and evaluating the functionality, performance, and scalability of the Azure Application Gateway in real-world scenarios.

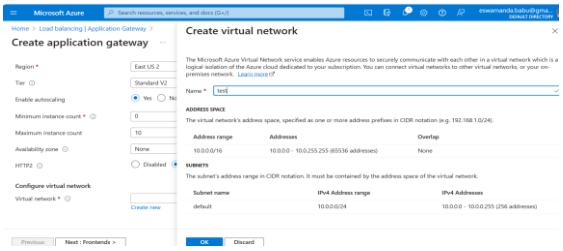


Fig 1 Creating Application Gateway

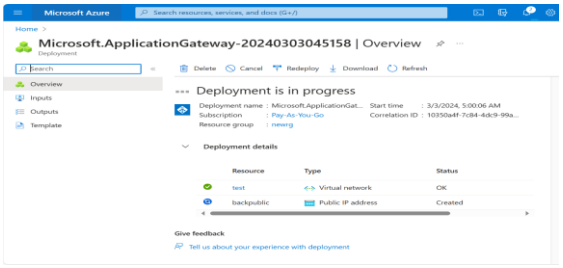
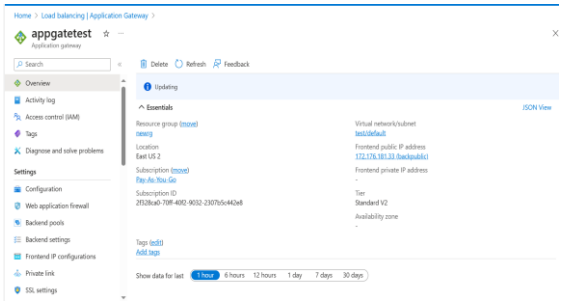


Fig 2 Deployment Progress



VI. DISCUSSIONS

Interpretations of results

By operating at OSI layer 7, the gateway enables URL-based routing, allowing for precise traffic

redirection based on attributes like URI path and host headers. This granularity enhances the efficiency and performance of web applications by directing traffic to specific backend pools optimized for various content types. Additionally, features such as session affinity and TLS termination contribute to improved security and reduced overhead on backend servers.

Application gateway implementation with azure implications

it enhances the efficiency of web application routing by allowing URL-based routing and directing traffic to specific backend pools based on attributes such as URI path or host headers. This leads to improved performance and better resource utilization. The implementation of Azure Application Gateway not only optimizes web traffic management but also reinforces security measures and ensures reliable performance, aligning with organizational objectives for efficient and secure web application delivery.

Benefits and Drawbacks

It enables scalability and high availability, allowing organizations to efficiently manage growing traffic demands. Implementing Azure Application Gateway offers several benefits, including advanced traffic management capabilities such as URL-based routing, session affinity, and TLS termination, which enhance the performance and security of web applications. Application Gateway is limited to handling web traffic which means it may not be suitable for all types of applications or protocols. Additionally, setting up and configuring Application Gateway can be complex, requiring expertise in Azure networking and traffic management. Furthermore, while Application Gateway offers comprehensive security features, organizations need to ensure proper configuration and monitoring to mitigate potential risks effectively. Overall, while Application Gateway provides powerful capabilities for web traffic management, careful consideration of its limitations and complexities is essential for successful implementation.

VII.CONCLUSION

By leveraging its capabilities such as OSI layer 7 routing, URL-based routing, and backend pool configuration, organizations can achieve efficient traffic management and optimization. Additionally, features like session affinity, TLS termination, and integrated web application firewall enhance security and reliability. Azure Application Gateway seamlessly integrates with other Azure services, providing scalability, high availability, and compliance with regulatory requirements. Overall, adopting Azure Application Gateway streamlines traffic management, enhances security, and ensures optimal performance for web applications deployed on Azure.

II. REFERENCES

[1]. A. Chonka, Y. Xiang, W. Zhou, and A. Bonti, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks," Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1097- 1107, 2011.

[2]. B. Halpert, Auditing Cloud Computing. Wiley Online Library, 2011.

[3]. H. AlJahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau, and J. Xu, "Multi-tenancy in cloud computing," in 2014 IEEE 8th International Symposium on Service Oriented System Engineering, 2014: IEEE, pp. 344-351.

[4]. M. A. Zardari, L. T. Jung, and M. N. B. Zakaria, "Hybrid Multi-cloud Data Security (HMCDS) Model and Data Classification," in 2013 International Conference on Advanced Computer Science Applications and Technolo- gies, 2013: IEEE, pp. 166-171.

[5]. N. Sultan and S. van de Bunt-Kokhuis, "Organisational culture and cloud computing: coping with a disruptive innovation," Technology Analysis Strategic Management, vol. 24, no. 2, pp. 167-179, 2012.

[6]. B. Tomas and B. Vuksic, "Peer to peer distributed storage and computing cloud system," in Proceedings of the ITI 2012 34th International Confer- ence on Information Technology Interfaces, 2012: IEEE, pp. 79-84.

[7]. H. Tianfield, "Security issues in cloud computing," in 2012 IEEE Interna- tional Conference on Systems, Man, and Cybernetics (SMC), 2012: IEEE,pp. 1082-1089.