ActioNews

FALL 2021
THE NEWSLETTER OF ACTIONET

Turning VISION into ACTION®

CHAIRMAN'S NOTE

Dear Friends,

ActioNet leverages Microservices to simplify application architecture into more granular Functional Services. This provides more resiliency by performing code updates at the function level with the benefit of agility, flexibility and scalability to facilitate Digital Transformation.

Recent Cyber Attacks have targeted a water treatment plant and oil production, impacting both public health and gasoline prices. Security Information and Event Management (SIEM) capability in Security Operations Centers (SOCs) enables proactive monitoring and alerts across the Enterprise with the ability to ingest large amounts of data. A strong offense is the best defense.

Please take care of yourselves and each other!

Ashley W. Chen
Chairman & CEO

IN THIS ISSUE

Microservices: Upending the Application Development Landscape

By Venkata Kollati, Solutions Architect & Reuben Maher, SVP & Chief Innovation Officer

As emerging technologies continue to evolve, so too does the IT industry as it figures out new, innovative ways to develop and deliver applications. We've come a long ways from back on June 21, 1948, when computer scientist Tom Kilburn ran the first piece of monolithic software as it performed mathematical calculations via machine code on the Manchester Small-Scale Experimental Machine – aka "Baby". Fast forward just over 73 years and we've moved into ubiquitous cloud-native environments leveraging DevSecOps and AIOps as more standard development and operational best practices. One of the most significant progressions in this continuously evolving development journey is the pivot towards microservices. But before we dive deeper, it helps to set the stage and ensure we have a baseline understanding of microservices.

What are Microservices? Microservices are software-developed small services that perform a specific business function or task over web interfaces. Microservices are built on cloud-native architectures that are autonomous, independently deployable services, and communicate with one another over a combination of defined APIs (Application Programming Interfaces).

"Evolving development journey is the pivot towards microservices"

Evolution of Microservices: The term "micro web services" was used in a conference on cloud computing in 2005 by Dr. Peter Rogers. "Microservices" were discussed in a software architects' workshop held near Venice in 2011. In March 2012, James Lewis presented a case study on various microservices concepts at 33rd Degree in Krakow.

Today, microservices are gaining momentum due to the fact that conservative monolithic architectures are no longer able to support the growing technology and performance needs of many organizations. With the

continued on page 2

ActioNews, the newsletter of ActioNet, Inc. is published to provide examples and applications of cutting edge IT topics and practices.

ActioNews is published quarterly (March, June, September, and December) as a service to its staff, customers, and potential customers.

ActioNews Staff

Lead Designer

Karen Tepera

Contributing Authors

Venkata Kollati
Reuben Maher
Jeff Masiello
Kate Russell

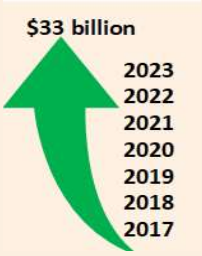
"Microservices provide the ability to quickly update the code of a single function in the application."

Microservices

continued from page 1

increased focus on containerization and cloud computing solutions, microservices are being developed and deployed easily on different platforms using various programming languages.

In fact, a February 2021 report from Market Research Future indicated that industry use of microservices architectures is expected to rise at a Compound Annual Growth Rate (CAGR) of 17% through 2023, reaching $33 billion.

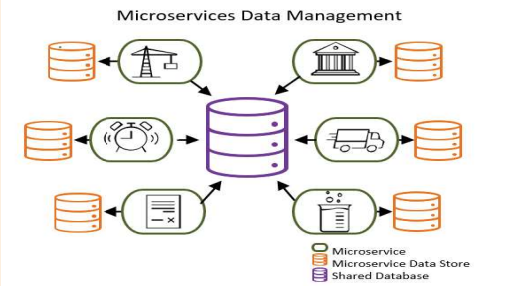


Additionally, a 2021 IBM survey reinforces the fact that microservices are here to stay. Within the next two years, 56% of current non-users are likely to adopt microservices, 78% of users will increase their investment in microservices, and 59% of all applications will be created with microservices.

How Microservices Work: In a monolithic architecture, users interact with the presentation layer, which then talks to the business logic and database layers, and information travels back up the stack to the end user. A monolithic architecture adds risk for application availability because it creates many single points of failures.

Microservices, however, break down the monolithic application into more granular functional services, thus providing the ability to quickly update the code of a single function in the application. The failure points are independent of each other in the application and thus helps mitigate broader application failure.

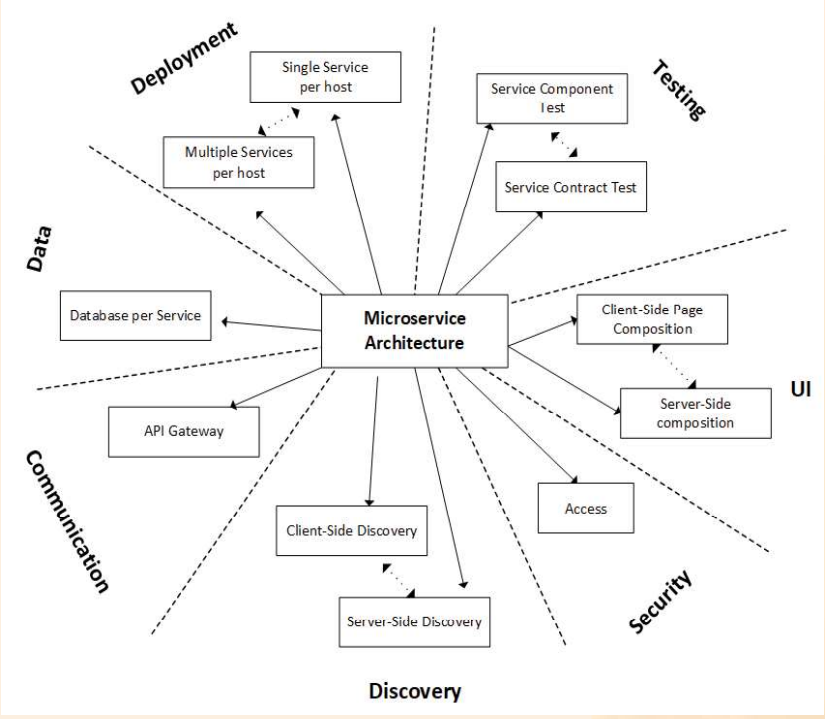
How Microservices Manage Data: Microservices are typically developed to perform a single purpose, and are thus simple and autonomous. The shared database is a coupling point for the microservice, causing them to be interdependent as opposed to independent. Microservices leverage database services through defined APIs and manage their own data in private data stores.



Benefits of Microservices: Leveraged by industry leading corporations such as Netflix, Amazon, Uber, Twitter, PayPal, Spotify, and LinkedIn – among many others – microservices are rapidly gaining traction as a best practice for the host of benefits they provide, a few which include the following.

Agility: Microservices can be adapted rapidly and are easily reusable.

Flexible Scaling: Microservices are individually scaled to meet demand for the



Microservices

continued from page 2

application and are also extremely cost-effective.

Individual Deployment: As independent components, microservices can be quickly fixed with little downtime, thus frequent updates can be done with minimal risk.
Technological Choice: Microservices leverage the most current technologies, thus teams can choose the right tool to develop microservices and standardize the technology where it makes sense.
Small Services: Microservices are easier to understand and the underlying code can easily be rewritten.

The benefits are compelling and the increased use of microservices across the enterprise is a development game changer. ActioNet is helping our clients in their digital transformation journeys to increasingly leverage microservices as they pivot to the cloud in alignment with their infrastructure modernization mandates. By providing a rapid means to deploy smaller business functions in a more flexible and real-time manner with a lower risk profile across a distributed cloud-based infrastructure, microservices will continue to be a valuable design decision organizations must consider incorporating when building modern applications.

Not All SIEM Tools Are Created Equal

By Jeff Masiello, Sr. Cloud Architect, & Kate Russell, Program Manager

Recent high-visibility cyber attacks have reinforced the need for stronger cyber defenses across our national infrastructure. In February 2021, a water treatment plant in Florida was hacked and the sodium hydroxide was briefly increased in the water to deadly levels. In May 2021, a ransomware attack was unleashed on the Colonial Pipeline resulting in them shutting down their oil production/distribution for nearly a week and gas prices subsequently spiking along the east coast of the United States.

As part of a holistic cyber strategy, organizations often implement Security and/or Network Operations Centers (SOC/NOC) which are proactively monitoring all facets of the enterprise's virtual and physical infrastructures. A vital bedrock capability in any effective SOC/NOC is implementation of a Security Information and Event Management (SIEM) capability. As a follow up to last month's article, "Network Operations Center/Cell Considerations in Physical or Cloud-Based Environments," it is imperative to drill down further into the topic of SIEM tools, what they are, and how to choose a tool that best suits your client's needs. Below we dive into this in more detail based on our lessons learned at client sites and across industry.

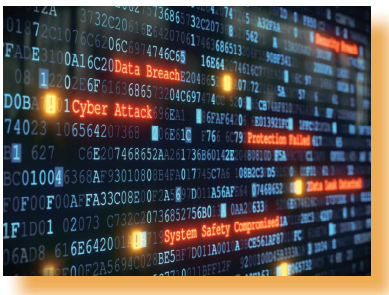
What is a SIEM tool? SIEM tools are widely used through the industry…but what are they and why do we need them?

The purpose of a SIEM tool is to aggregate event logs from multiple sources into a central location and provide searching, correlations, alerting, and response capabilities. Logs are great sources of security events but, unfortunately, logs come in a variety of formats. SIEM tools collect and normalize logs from multiple sources and vendors which makes it easier for the tool to then search and alert on security events. Typically, a SIEM tool is implemented to search for security-related log entries but can be leveraged for any logged event. For example, you have multiple AWS accounts, and your Cybersecurity team wants to know when a user logs in. The SIEM tool ingests the CloudTrail logs from each AWS account and looks for the "Logged In" event in the log entries as they are ingested. Once an event is detected, the SIEM tool can be programmed to take actions. A username could be correlated with a list of recently removed employees to ensure no previous users still have access and an alert sent out, or an alert could be sent to Cyber to take other actions.

What to look for? Requirements vary but some of the most common things to consider are which log sources or vendors the tool supports out of the box. While all SIEM tools require some customization, the broader the support the better. Are you only ingesting logs from on-premises or are you also in the cloud? Most of the major SIEM tools support cloud capability. Some tools have plugins you can download or purchase to prove ingestion capabilities from other log sources.

continued on page 4

"A SIEM tool aggregates event logs from multiple sources for searching, correlations, altering and response."



ActioNews

- Founded in 1998, 500+ ActioNeters
  - Overall Customer Retention Rate > 98%
  - Annualized Professional Staff Retention Rate > 92%
  - Woman Owned Small Business Under NAICS 517311
- CMMI®-DEV Level 4 Externally Assessed
- CMMI®-SVC Level 4 Externally Assessed
- HDI Certified Support Center
- ISO 20000 (ITSM), ISO 27001 (Information Security) and ISO 9001 (Quality) Registered
- GWAC and IDIQ Contract Vehicles:
  - **GSA Alliant 2**
  - **GSA MAS**
  - **GSA IT Schedule 70**
  - **GSA OASIS Pool 1**
  - **CIO-SP3 SB OTSB**
  - **CIO-SP3 WOSB OTSB**
  - **DISA Encore III**
  - **Air Force NETCENTS-2**
  - **ARMY ITES-3S**
  - **HHS SPARC**
  - **NAVY Seaport-NxG**
  - **GSA 8a STARS III (JV)**
- "92 out of 100" Rating from Open Ratings
- "Exceeds Customer Expectations" from D&B
- "5A1" the Highest Financial Rating from D&B
- DCAA-Compliant Accounting and EVM System
- Approved Purchasing and Cost Estimating System
- DoS TS Facility Clearance with Safeguarding Capability

"Having the right defensive measures in place - including a holistic SIEM tool - is a vital component of overall enterprise security readiness and response."

ActioNet

SIEM Tools continued from page 3

Another feature to look for is the various types of detections that come out of the box. Detections are the events the SIEM tool scans for. A tool may be inexpensive up front but by the time you have written all the basic detections, you may have tripled the cost of the product. Given there will always be additional detections any organization will want, the more information you can gather from the start, the better.

Another important consideration is around deployment methodologies. If your organization's infrastructure is cloud-based, you may want containerization capabilities like Kubernetes or Docker. Are you using Infrastructure as code and using Terraform or CloudFormation for deployment? Some tools may require a physical device which could cause issues in cloud or other virtual environments. Another consideration is Software as a Service. This removes the burden of infrastructure maintenance but requires slightly more complex networking.

As this is a security tool, securing the tool itself should be of paramount importance. You should look for a tool which supports two factor authentication at a minimum. Other types of security to consider are CAC authentication, log encryption, and Role Based Access Control (RBAC). RBAC will help a great deal in the delineation of tasks leveraging least access requirements. If the tool requires an agent on all the servers there may be a performance hit on that server. Additionally, the data should be encrypted during transfer to the destination.

What is the cost? While there are free or low cost SIEM tools out there, you also should consider the interface itself. Standing up a SIEM tool, ingesting all the logs, and writing the needed detections takes considerable effort. Having to build out an entire dashboard from scratch means those efforts are not going where they could be more readily used. The visualization component is often thought of as a nice-to-have extra; however, proper User Interface/ User eXperience (UI/UX) is critical for timely response. If your SIEM tool performs the proper detections but an admin cannot see the alert, then the tool is of no value. Further, your clients will typically want a Single Pane of Glass view they can look at.

Speed is another critical consideration when evaluating a SIEM tool. How fast the tool can correlate and scan data will have a direct impact on response times. Speed is often tied into price with higher speed requiring more powerful infrastructure to support it. A corollary to that is expansion capabilities. An application may scale vertically but not horizontally which effects how the network is laid out for a given tool.

Support is an often-overlooked aspect of any tool. A product with no support can leave you at a dead end if something should go wrong. Support should provide an ability to track cases, professional services should they be needed, and enforceable Service Level Agreements (SLAs). A phone contact is also a large plus. If a tool is only ticket-based with email, you are dependent upon the support desk and have no way to escalate a ticket in a critical situation. What support is included in the price may be a game changer. Check to see if the support has more experience in your needed space – federal or commercial. Finally, what is the support cost model? If it is cost per ticket, then having an expert in the tool will be beneficial. Obviously, there is a tradeoff as the cost of the Subject Matter Expert (SME) will need to be considered.

There is another important financial consideration. While pricing is often a prime motivator, the ***Total Cost of Ownership*** (TCO) is usually far more important than the up-front cost. Included in that is the licensing model. Paying per GB ingested can get exorbitantly expensive rapidly, especially when adding the considerations for long-term storage cost and speed of processing. If the environment has fewer logs, this may make sense but as environments grow, the cost will get out of control forcing the decision between cost and which logs to maintain. Other SIEM tool models are licensed by node, which means more infrastructure and maintenance costs.

ActioNet partners with our clients to ensure their missions are both highly secure and resilient. We are committed to working with them to deliver and maintain the strongest security posture throughout the cyber lifecycle. Our experience reinforces our strong belief that having the right defensive measures in place – including a holistic SIEM tool – is a vital component of overall enterprise security readiness and response.