WHITEPAPER

ADVANCED CLOUD MANAGEMENT

Going Beyond the Built-In AWS and Azure Tools

Cloud Checkr

EXECUTIVE SUMMARY

Around the world, public cloud adoption is on the rise. In fact, according to the market research firm Gartner, "the cloud services market is growing faster than virtually every other IT market today." While much of that growth comes at the expense of traditional, non-cloud offerings, there is little doubt that it will continue to grow well into the future, driven by digital business initiatives, ongoing consolidation within the datacenter, and increasing migration of applications to the cloud. In this arena, the top two cloud providers are Amazon and Microsoft, with their AWS and Azure platform offerings. Together, these two providers control more than 50% of the total cloud market share.

In this paper, we will take a closer look at the various tools built into the Amazon AWS and Microsoft Azure platforms, examining both their advantages and shortcomings. Gaps where third-party tools may be needed will also be identified.

EYE ON CLOUD SOLUTIONS

Migrating applications to the cloud is a substantial undertaking and it requires a well-thought-out plan. Key to successfully accomplishing this goal is ensuring you have a clear understanding of the cloud platform options and their built-in tools. With this information, you can begin to fully understand what you will and won't be able to do with the platform, and what shortcomings you might need to address with a third-party solution. In general, these are the four key areas where cloud platforms offer native tools:

- Security
- Automation
- Cost management
- Resource utilization, inventory, and monitoring

Security

With public cloud adoption becoming a natural strategy for enterprises around the globe, IT decision makers are facing a number of concerns. Chief among those concerns is the security of the cloud and its ability to quickly adapt to the ever-evolving threat landscape. To better understand how cloud providers help mitigate this concern, it's important to take a closer look at the native security tools and processes built into the AWS and Azure cloud platforms. These tools and processes fall into one of three categories:

Protect and Mitigate

AWS

On the AWS platform, Distributed Denial of Service (DDoS) protection is possible using AWS Shield, a managed DDoS protection service for applications running on AWS. The built-in tool has two tiers: standard and advanced.

The standard version of AWS Shield is free of charge and uses a combination of traffic and anomaly signatures to protect applications from common Layer 3 and Layer 4 attacks.

Additionally, AWS Windows Application Firewall (WAF) can be purchased to write custom rules that provide application layer (Layer 7) attack mitigations like SQL injection or cross-site scripting. The advanced version of AWS Shield is a premium service that includes WAF and provides additional features like Layer 7 attack mitigations using the AWS DDoS Response Team (DRT), attack historical reports, DDoS mitigation capacity for large attacks, and dedicated protection against AWS resources like the CloudFront, ELB, and Route 53.

One of the key advantages of the AWS Shield service is the ability to use built-in rules, or rules built by the DRT team, to block large Layer 7 attacks. Without these rules, blocking such attacks would entail having to use expensive security appliances, a dedicated security team, honeypots, and management of application security, around the clock, for critical applications.

What about protecting the single-most precious commodity in the public cloud — tenant data? How is that accomplished in AWS? For this task, Server Side Encryption (SSE) is used in conjunction with AWS Key Management Service (KMS) to provide an encryption service that uses a customer's master keys (CMKs) to encrypt Amazon S3 objects.

AZURE

In the Azure platform, DDoS protection is offered as a turnkey DDoS protection service that automatically mitigates Layer 3 to Layer 7 DDoS attacks. Azure DDoS protection offers two service tiers: basic and standard.

The basic tier is a free service designed to mitigate against common network-level attacks on Azure provided public Internet Protocol (IP) addresses. It uses Azure's global network to distribute and mitigate attack traffic across regions. The standard tier provides additional protection policies that are tuned through dedicated traffic monitoring and machine learning algorithms.The main type of attacks that the standard tier mitigates are volumetric attacks (e.g., UDP floods and spoofed-packet floods), protocol attacks like SYN flood attacks, and application layer attacks like SQL injection and cross-site scripting (in conjunction with the Web Application Firewall). Azure Storage Service Encryption (SSE) provides encryption at rest for Azure Storage like Azure Blob Storage and File Storage.

Assess and Evaluate

AWS

For assessing and evaluating security issues, the AWS platform offers Amazon Inspector. This security vulnerability assessment service assesses resources for vulnerability or deviations from best practices, and summarizes the results, according to level of security, in a detailed report. The service features a knowledge base of hundreds of rules mapped to common security standards, as well as vulnerability definitions that are constantly updated by AWS security researchers. While the tool does not replace the traditional pen testing and risk assessment, it does help users determine inherent security loopholes and vulnerabilities without having to enlist a security consultant.

AZURE

To protect workloads running in the Azure platform, on-premises or in other clouds, the Azure Security Center can be used. This unified security management and advanced threat protection system delivers visibility and control over these workloads. It also provides active defenses that help reduce exposure to threats and intelligent detection to keep pace with rapidly evolving cyberattacks.

Audit and Compliance

AWS

For auditing purposes, the AWS platform offers AWS CloudTrail. As its name suggests, AWS CloudTrail is used to trail or keep track of the AWS API calls made, including those made from the AWS Management Console, AWS SDKs, command-line tools, and higher-level AWS Services. The details include information like the IP address from where calls were requested and the timestamp of each call.

A tool that helps assess compliance of the AWS resources is AWS Config. This service continuously monitors AWS resource configurations and evaluates any deviations from the desired configuration. By keeping track of all the changes in configuration and relationships of the AWS resources, the service helps simplify compliance, security analysis, and operational troubleshooting. AWS Artifact is an audit and compliance portal that provides AWS security and compliance reports like PCI and SOC reports.

AZURE

In the Azure platform, Azure Security Center provides compliance reports that keep track of the security posture of the various resources. Azure Trust Center is a portal that provides information about Azure's security, privacy, and compliance policies and features.

While these built-in tools can be highly beneficial, there is a key shortcoming: Due to the dynamic nature of the cloud, the changes recorded by AWS Config and AWS CloudTrail cannot be easily deciphered and applied by administrators. As a result, tools are needed to disseminate this data in an intelligent and readable format. That's exactly where a tool like CloudCheckr comes in. The AWS Config and CloudTrail tools feed into CloudCheckr to quickly search and analyze this data.

Below are some of the features not addressed by the built-in tools in the Amazon and Microsoft cloud platforms. These features are available in CloudCheckr.

- Automatic dissemination of AWS Config and AWS CloudTrail data.
- Vendor recommendation checklists.
- Perimeter assessments.

See CloudCheckr in Action

Visit CloudCheckr.com/Demo now for a custom demo with our cloud experts.

Automation

AWS

One of the major catalysts for rapid adoption of the public cloud is the wide availability of a slew of built-in automation tools that help speed deployment of resources and automate repetitive tasks ranging from scheduled maintenance to common DevOps processes. One of the most widely used automation tools in the AWS Infrastructure as a Service (IaaS) stable is the EC2 Systems Manager. The tool is a management service that helps automate the collection of system inventory, apply operating system patches, automate the creation of Amazon Machine Images (AMIs), and configure operating systems and applications at scale. The managed instances can span across both AWS resources and on-premises deployments. Some common examples include automating the installation and pre-configuration of applications and agents in AMIs, deployment of operating system updates in Windows Server Environments (both EC2 and on-premises), and running the EC2Rescue Tool on unreachable instances.

Another great hybrid automation tool is AWS OpsWorks, which is based on the popular Chef tool that treats server configuration as code. OpsWorks helps deploy, manage, and configure EC2 instances and on-premises server deployments.

AWS CloudFormation is a tool that can be used to automate deployment of customized AWS resources. It provides built-in templates and also gives users the option of creating custom templates (using CloudFormation Designer) to help define and deploy AWS resources, along with any associated dependencies or runtime parameters needed to run an application.

For developers or DevOps administrators looking to consistently deploy applications to development, test, and production environments, the AWS platform offers AWS CodeDeploy. Some of its key advantages are its ability to allow centralized management and deployment, its compatibility with any application due to it being platform and language agnostic, and its ability to integrate with popular Continuous Deployment (CD) tools like Jenkins.

AZURE

On the Azure platform, Azure Automation provides a Software as a Service (SaaS) solution that allows users to automate the most manual, error-prone, repetitive tasks commonly performed in a cloud and enterprise environment. The two methods employed are Runbooks for processes and Desired State Configuration (DSC) for configuration management. Since Azure Automation Runbooks are based on Windows Powershell or Windows Powershell Workflows, they can interact with any application with an API or use powershell cmdlets to complete a task. These

runbooks run in the Azure Cloud and can access Azure cloud resources or on-premises resources with the help of the Hybrid Runbook Worker. Users can either create their own runbooks or modify one from the Runbook Gallery. There are six types of runbooks: Graphical, Graphical Powershell Workflow, Powershell, Powershell Workflow, Python, and Bash. More details on each type of runbook is available here.

DSC is a management platform in Powershell that enables deployment and management infrastructure with configuration as code. DSC helps users define and configure instances of resources. It polls system resources to ensure they adhere to the state of the configuration. When needed, it rectifies the state of the resources to match the desired state. Azure Automation DSC adds a management layer to Powershell DSC and offers advantages such as a built-in pull server and the ability to manage all DSC configurations, resources, and target nodes from a single Azure portal. It can also feed data into Azure Operations Management Suite (OMS) to gain insights. One noteworthy Azure Automation tool is Auto Shutdown. The tool helps users shut down ARM Virtual Machines (VMs) based on schedule or conditions that are not being used to save costs -- a prime example being Dev/Test Labs.

Although AWS and Azure provide a rich set of tools for automation, they lack some important features. Fortunately, the following gaps can be plugged with CloudCheckr.

- Resizing of EC2 Reserved Instances (RI) and Azure Reserved Instances (RI).
- Reallocation of the reserved instances to different accounts and resources.
- Cost optimization through automatic resizing of Redshift and RDS Clusters.
- Scaling DynamoDB up or down to match capacity.
- Integration of best practice checks from industry leaders into a single platform.

Cost management

AWS

For cost management purposes, the AWS Cost Explorer lets users perform a granular analysis of the costs associated with AWS resources. The tool features several advantages, including its ability to determine cost drivers, detect anomalies, filter and group costs, and forecast future costs and usage.

Building on this functionality, AWS Budgets helps users maintain their Total Cost of Ownership (TCO) by setting custom budget alerts and sending out notifications when set thresholds are reached. These budgets can be set on a monthly, quarterly, or yearly basis. Notifications are sent out via email or Amazon Simple Notification Service. Budgets can also be set for AWS Reserved Instances (RIs), enabling users to get alerted on RI utilization and the amount consumed by matching instances.

Apart from exploring the billing and setting customized budget alerts, AWS also offers some impressive cost reporting capabilities in AWS Cost and Usage Report and RI Reporting. The Cost and Usage Report provides a holistic and comprehensive view of the costs associated

with AWS resources, which can also be fed into Redshift and Quicksight for intelligent analytics. Although the Cost and Usage Report includes RI data, users have the option of using RI Reports to visualize the RI data at an aggregate level or a particular RI subscription.

AZURE

Thanks to the acquisition of Cloudyn, Azure has a bit more teeth in the game when it comes to cost management. Azure Cost Management is a SaaS platform that helps manage cloud spend across Azure, and other cloud providers. It allows users to track cloud usage and expenditure, and optimize their cloud spending by identifying underutilized resources, which can then be adjusted. Azure Cost Management also detects anomalies through the use of overtime reports and forecasts future spending.

Despite these capabilities, there are a number of missing features in these tools:

- Report sizing with actionable insight
- Resource re-sizing recommendations
- Chargebacks for Managed Service Providers (MSPs)
- Constraint Satisfaction Problems (CSPs) for RIs
- Industry best practices to monitor these idle resources and help lower TCO

Resource utilization, inventory, and monitoring

AWS

One of the most commonly used tools for monitoring AWS resources like EC2 instances, DynamoDB tables, EBS Volumes, and RDS instances is AWS CloudWatch. The tool helps users collect resource metrics like CPU utilization, data transfer, and disk usage activity. It can also collect and monitor log files and set alarms. Moreover, it automatically reacts to changes in AWS resources.

AWS CloudWatch provides two types of status checks for EC2 instances, a system status check and an instance status check. These status checks help in monitoring software, network, or underlying problems of AWS instances, such as a loss of system power, hardware issues on the physical host, a corrupted file system, or a misconfigured startup configuration. Systems Manager Inventory, which is a part of EC2 Systems Manager, can collect metadata like application names, versions, network configuration, and Windows updates, etc.

AZURE

Three of the most commonly used tools to monitor Azure instances are Azure Monitor, Application Insights and Log Analytics. Azure Monitor provides base-level infrastructure metrics and logs for most services in Azure. It is a monitoring data pipeline that feeds the data into Log Analytics to derive actionable insight. It collects information like resource audit logs called Activity Logs, host and guest VM metrics, diagnostics logs (e.g., performance counters, application logs, and memory crash dumps), and Windows event logs.

> Application Insights is an extensible Application Performance Management (APM) service that can be used to monitor live web applications. It monitors things like web app response times, Windows or Linux server resource utilization (e.g., CPU, memory, and network usage), and host diagnostics from Azure. This telemetry can then be used to measure resource usage, modify the development cycle based on usage, and diagnose or debug issues.
>
> The Log Analytics tool is a part of the Azure OMS. It collects data generated by resources in cloud and on-premises environments, from Azure Monitor, and helps quickly retrieve and consolidate that data via a query language. This helps users analyze and act on the collected data, while also allowing them to visualize the data in a dashboard format. In Azure, resource inventory can be done by running an inventory collection and then feeding that data into Log Analytics.

Here again, while these native tools boast some powerful features for the Azure and AWS platforms, they also omit a few key features:

- A unified solution that tracks assets across a multi-cloud environment
- Management of inventory and pinpoint change monitoring
- Identification of underutilized resources
- A checklist for using best practices, including RI mismatches

A FINAL NOTE

It's clear that AWS and Azure each have a number of powerful built-in tools to deal with security, automation, cost management, and the utilization and monitoring of resources. These feature-rich tools and services go a long way toward easing the migration to the public cloud. However, there are gaps in functionality that neither tool is addressing and these gaps are cause for concern.

Perhaps the biggest gap is the lack of a single pane of glass through which the IT, security, and finance teams can all gain access to actionable insights that can be used to govern an enterprise's cloud resources. Third-party tools like CloudCheckr will play a crucial role in filling this gap. By providing security, automation, cost management, reporting, and analytics, enterprises now have an effective way to optimize their AWS and Azure cloud deployments.

Need CloudCheckr for your organization? Learn more at **www.cloudcheckr.com**.

Cloud Checkr

342 N GOODMAN ST,
ROCHESTER, NY 14607

1-833-CLDCHCK

www.cloudcheckr.com