StackZone

Well Architected

Blueprint

StackZone Ltd., 2023

Hello!
In this document, you will learn how to improve your AWS cloud infrastructure by aligning to the **AWS Well-Architected framework best practices with StackZone's Cloud Management Platform. This results in greater security because the goal of StackZone is to make it easy for businesses to run their workloads and at the end of the day, they can focus on selling their products.**

By implementing the following Blueprint, you will take to the next level your **AWS Workload Security, Resilience, Performance and cost optimization.**

StackZone's Well Architected Setup includes the necessary components enabled to detect and in some cases remediate high-risk items detected by the Well-Architected Framework Review and build compliance according to AWS best practices.

For the core accounts **(Shared Services, Log-Archive, and Management)** we build a default compliant Amazon VPC, an Amazon S3 bucket with a lifecycle policy to store logs for up to 7 years and we delegate some security services administration to the Security account.

We also enable the following services on the **security account:**

A Global Centralized Amazon GuardDuty and Macie aggregation for all your accounts within your StackZone Organization. That gives your SecOps team full visibility of findings. Any new account gets invited to the centralized Amazon GuardDuty Detector and Amazon Macie.

Once StackZone has been deployed, we build a number of **Service Control Policies (SCPs)** for you to apply to the accounts.

Also, we deploy a number of **AWS Lambda** functions and **SNS Topics** that will help with the deployment of the features further on.

These functions will help you simply manage and monitor your Organization, but what about the accounts and environments where you will be running your workload?

Well, on every account and region we deploy the following **Baseline Services:**

- AutoSpotty
  It is a cost-saving feature that automatically migrates Amazon AutoScaling Groups from using Amazon EC2 Instances to Amazon Spot Instances. Within an Amazon AutoScaling Group, AutoSpotty will try to swap out On-Demand Instances with Spot Instances which are considerably cheaper in terms of hourly runtime cost.
- AWS Config and Global and Local Aggregators
  We deploy 68 AWS Config Rules and 13 Remediations. AWS Config rules ensure you actively monitor your Resources configuration which is translated into continuous monitoring of the security and compliance of your resources. The auto remediation rules ensure deviations are automatically solved.

14 CloudWatch Alarms per Region

Remain up to date and get notifications on every change and/or threat on your workload with StackZone CloudWatch alarms.

AWS Service Catalog Network and Security Portfolios

Launch compliant, secure and optimized workloads simply and fast, by doing it through our Service Catalog portfolios.

CloudTrail Multi-Region

It allows you to track every change made to your AWS infrastructure and activity on it.

EBS Optimizer

The StackZone EBS Optimizer will automatically optimize your Amazon EBS Volumes and exchange older generation gp2 volumes with the newer and more cost-efficient gp3 volumes. This will bring a lower cost to your organization too.

S3 Replication

The StackZone Amazon S3 Replication feature enables you to replicate objects from any chosen source S3 Bucket to a designated target S3 Bucket. Simply add a tag to your chosen source S3 Bucket with the name of your target S3 Bucket, and StackZone will copy the contents over! As soon as you have more objects arrive in your source S3 Bucket, it will continue replicating them into your target S3 Bucket. This can also be configured to replicate items cross-account within your AWS Organization.

Instance Scheduler

The StackZone Instance Scheduler is a great money-saving feature that can automatically turn on and off tagged EC2 Instances and RDS Instances, based on a schedule you define. This means, for example, you could automate your Development EC2 Instances to start at 8:30 in the morning, and turn them all off at 17:30 in the evening, on Mondays to Fridays. You can build additional schedules to meet your needs. All you need to do once this is active is tag your resources and StackZone will take care of the rest.

Patch Management

The AWS SSM Patch Management feature leverages Amazon's Systems Manager to build a scalable, reliable patch implementation process. Here you define two different schedules and then tag your EC2 Instances with either the first schedule's tag or the second. When the first schedule's time arrives, SSM will automatically patch all EC2 Instances with the corresponding tag. We will then do the same when the second schedule's time arrives. This means you can auto-patch all UAT and Dev Instances in one day, review the results, and have the Production level instances patched in the same way at a later time in the week. A great way to automate compliance and mitigate software vulnerabilities.

Amazon Inspector (tag-based)

It is an automated Security tool that can detect vulnerabilities and will continue to evaluate your resources on both the hardware and software level. You might have unintended network exposures which could potentially pose as a security risk to you - Amazon Inspector is capable of highlighting these issues and bringing them to your attention. Amazon Inspector works in line with up-to-date common vulnerabilities and exposure (CVE) information to create context-based risk scores which will help you prioritize your workload and tackle vulnerable resources.

- AMI Deprecation Checker

  The StackZone AMI Deprecation Checker is able to scan all AMI's you have in all accounts this feature is deployed within and checks all of the deprecation dates listed on AMI's.

- AWS Backup (tag-based)

  The StackZone AWS Backup feature helps you automate schedule backups of your EC2 Instances, EBS Volumes, and RDS Instances. All you need to do is tag your AWS resource with "daily", "weekly" or "monthly" schedule, and the AWS Backup feature will ensure a backup of your AWS resource is taken depending on your chosen period. AWS Backup will also rotate the amount of backups stored, based on the retention period. This is to ensure that you don't grow exponentially with the amount of backups stored.

- Amazon CloudWatch Auto-Create (tag-based)

  We enable a solution to create cloudwatch alarms for every ec2 instance and lambda function based on a tag. The current set of alarms includes cpu, storage, memory, and execution time and errors for functions.

So far we have covered the most important and general services and tools **StackZone** provides our customers when applying the **Well-Architected Review Blueprint.**

As always this is just the first step because as part of the **StackZone** community you will receive continuous updates that will allow you permanently improve your AWS cloud Workload. We do so based on best practices updates and based on our customer's feedback. **This means you will be able to request the features you need, and our commitment is to evaluate them and add them to our road map.**

Do you want to know in detail all that we deploy by implementing this blueprint to decide to adopt it, or try to do it manually? Access to https://help.stackzone.com/article/stackzone-aws-well-architected or simply book a call with us and take your AWS workloads to the next level in just 2 hours of human intervention!