StackZone

SaaS
Blueprint

StackZone Ltd., 2023

Hello!
In this document, you will learn how to improve your AWS cloud infrastructure by aligning to the **SAAS industry Blueprint with StackZone's Cloud Management Platform.** This blueprint was designed based on the industry best practices as well as our customer's feedback. **Because we built this CMP with our customer feedback: our mission is to make it easy for businesses to run their workloads and at the end of the day, they can focus on selling their product.**

By implementing the following Blueprint, you will take to the next level your AWS Workload, putting special focus on **Security, Performance, Availability and Cost Optimization.**

StackZone's SaaS Setup includes the necessary components enabled to prevent, detect and in some cases remediate high-risk items defined by the AWS Startup Security Baseline (AWS SSB) and build compliance according to AWS Prescriptive Guidance.

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 take the following actions and deploy the following **Baseline Services:**

> Remove all Default VPCs in all Regions

StackZone SAAS blueprint removes all Default VPCs in all regions because the default VPC lacks the proper security and auditing controls. The default VPC does not make the best use of critical VPC functionality. VPC flow logs, the default VPC does not enable flow logs. This feature allows users to track network flows in the VPC for auditing and troubleshooting purposes. StackZone customers can deploy compliant VPCs by simply launching them on StackZone networking portfolio on AWS service catalog.

Enable AWS Budgets for $1,000USD Monthly in all Accounts

AWS Budgets allow AWS customers to set custom budgets and monitor their cost and usage over a set period of time. Once you have chosen your desired thresholds, StackZone is then able to set up SNS Notifications and Email Notifications, so that you are informed when actual or forecasted cost and usage exceed your set amount.

Enable AWS Managed KMS Keys for EBS Volumes

This action will allow StackZone to encrypt EBS Volumes using AWS Managed KMS Keys.

Enable CloudTrail S3 Events

CloudTrail can be used to track data events to get information about a bucket and object-level requests in Amazon S3. Usually, this is enabled manually, but StackZone does it on every account and region through automation.

CloudWatch Logs

CloudWatch Logs enables you to centralize the logs from all of your systems, applications, and AWS services that you use, in a single, highly scalable service. It can be used to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Route 53, and other sources.

SNS Topics

An Amazon SNS topic is a logical access point that acts as a communication channel. A topic lets you group multiple endpoints (such as AWS Lambda, Amazon SQS, HTTP/S, or an email address).

CloudTrail Multi-Region

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

AWS Config and Global and Local Aggregators

We deploy 52 AWS Config Rules and 6 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.

4 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 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 number of backups stored, based on the retention period. This is to ensure that you don't grow exponentially with the number of backups stored.

AWS Service Catalog Network and Security Portfolios

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

- SSM Associations using Tags for EC2 Resources (gather-inventory, cloudwatch-agent update, and query-scan-patches)

  Enable a variety of AWS Systems Manager (SSM) Associations. These associations are what AWS SSM uses to manage different aspects of your EC2 Instances. UpdateSSMAgent will try to update the AWS SSM Agent installed on your SSM Managed EC2 Instance. QueryScanPatches will gather information around software patches, and GatherInventory will gather information about your EC2 Instance so you can see it from the SSM Dashboard in the AWS Console.

- 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.

- 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.

- 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.

So far we have covered the most important and general services and tools **StackZone** provides our customers when applying the **SaaS 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-saas-ssb or simply book a call with us and take your AWS workloads to the next level in just 2 hours of human intervention!