Examples of Landing Zone implementations

22 July 2022 - 6 min. read

AWS Organizations | *governance and compliance* | *Landing Zone*

Our previous articles discussed what a Landing Zone is and why it is important for any company to implement. Then, we detailed which fundamental pillars to build it.

In the following paragraphs, we'll propose two different examples of Landing Zone implementations based on two radically different company types:

- **Small IT**: companies with few workloads and small IT teams
- **Large IT**: companies with thousands of workloads and multiple distributed and specialized IT teams

For each of these, we will apply the pillars described in a general way in **part two** of our series.

These implementations are not ready-to-use frameworks, but they are a perfect way to highlight how radically different organizations with different business needs are all sharing the same criticality: AWS environments governance.

Small IT

Organization

Simplification must be the key. In these cases, a light organization can be envisaged with a main Organizational Unit (OU) in which there are one or two Foundational accounts. An account dedicated to billing and access management, in charge of

managing our organization. Another account could be used to manage the networking and security part.

An excellent initial structure, therefore, could be based on two OUs, one for internal services and one for services aimed at the public in which to create accounts dedicated to production and accounts dedicated to non-productive environments.

Identity and Access management

To start with ease in managing access, you can think of directly leveraging the AWS IAM service. IAM users could be listed in a centralized account and IAM roles could be created in the accounts containing the workloads (production and development environments). If you want to think about an initial integration with your IdP, you can proceed by federating it directly with AWS IAM.

If you are interested in this topic, we already covered it in **this article**, describing how it is possible, for example, to federate GSuite with AWS IAM.

Networking

In these cases, connections from the office and our users to the Cloud infrastructures must be provided. We recommend that you take advantage of the **Transit Gateway** service to centralize management and connections. This object also allows us to save money without sacrificing high availability by implementing a configuration that includes **centralized NAT Gateways**.

Security

As for traceability, it is imperative to centralize all Audit Logs from the various AWS accounts.

As far as infrastructure security is concerned, we must try to reduce the attack surface as much as possible, keeping all data private and avoiding exposing publicly weak and vulnerable exchange protocols.

Proper backup management of data and configurations is essential to protect the company from attacks directed against our services.

Governance and compliance

In order to distribute centrally and in a standard way the basic configurations of the various accounts, **the Infrastructure-as-Code** (**IaC**) principle - e.g., through the **CloudFormation Stack Sets** service - is a fundamental aspect. This service allows us to centrally control the basic configuration stacks of the various corporate organization accounts.

Costs Control

Implementing budget **alarms** defined for each workload or account is important to keep costs under control.

Then costs can be optimized with **Saving Plans** which offer a discount for a commitment of at least an annual and at most three-year.

Disaster recovery

In the case of companies with few workloads, it is better to start by trying to reduce the impact of Disaster Recovery on costs. **Backup & Restore** is the perfect strategy to achieve this. The data must be identified and replicated continuously, and the infrastructure must be coded in such a way to automate the recovery procedures.

Large IT

Organization

Companies with digital departments that have many teams require a complex and highly stratified organization. However, it is necessary to limit the number of accounts to avoid the structure's explosion.

As for the Foundational accounts, you can still think of a single main OU with several accounts divided between security, logging, access management, billing management, and networking.

Things get more complicated when it comes to the classification of workloads. Since the number of accounts tends to grow in case of many development environments, a trade-off must be found between workloads that are meant to be separated and workloads that can be grouped.

To provide **DevOps** with the opportunity to experiment in sandbox environments, it is possible to build an ***Account Vending Machine*** *that allows the automatic* provisioning

and de-provisioning of accounts.

Identity and Access management

A centralized dashboard to manage the permissions to the various OUs or the different accounts is another certain need. A Landing Page to facilitate daily access for those who use the console is a must. If you're also considering integrating your IdP, then the perfect service is **AWS Single Sign-on**. With AWS SSO it is possible to manage identities and access authorizations to your multi-account structure centrally.

Networking

It is difficult for companies with a complex network topography to find an exhaustive summary of it. Indeed Transit Gateway is necessary. Connecting two transit gateways set in different regions and accounts is also possible.

The **AWS VPN Client** is, in turn, integrated with AWS SSO avoiding the need to manage additional login credentials

In case of continuous and massive data transfer between offices, datacenters, and virtual environments, it is essential to provide physical connections in order to reduce latency. This is achieved through the creation of a mesh network of private physical connections via **Direct Connect**, backed up by backup **SiteToSite VPNs**.

In a complex company, it is convenient to define the network access requirements by identifying paths that potentially do not meet them. You can achieve this using **the Network Access Analyzer** service.

Security

AWS Security Hub allows you to have a centralized dashboard on which to collect and cross-reference all our metrics based on security rules.

Thanks to **AWS Organization**'s involvement, you can use **Firewall Manager**, a single service to create firewall rules and security policies and apply them consistently and hierarchically to the entire infrastructure from a central administrator account.

Governance and compliance

In the case of very large companies, it is helpful to provide a self-service portal from which to implement configurations validated by the company. **Service Catalog**, together with **CloudFormation**, helps you achieve consistent governance and meet compliance requirements.

Procedures must be supported by the collection of metrics; with the **Audit Manager**, it is easier to evaluate the efficiency of policies, procedures and controls.

Costs control

The cost allocation can be achieved through the **Billing Conductor** service. It allows you to create ad hoc invoices in case of complex needs in separating the costs (customers or business).

A cost control strategy is necessary, and it must go through a process of optimization of the computational part (**AWS Compute Optimizer**) and follow the automatic recommendations for the **Reservation** plans and the **Saving Plans**.

Disaster recovery

Critical workloads with strict business continuity constraints require implementing an **active-active multi-site strategy**. This strategy consists of two workloads located in different accounts and regions ready to receive all production traffic without creating data split-brain scenarios.

To conclude

The Cloud is a revolutionary tool, but only when properly used; therefore, it is essential to have an informed, structured approach to the new model before you even think about services and features. First, companies evaluating a paradigm shift should provide IT teams with adequate training to build a Cloud Center of Excellence (CCoE) within the company. This group will be designated for making strategic decisions based on new responsibilities and available data and will successfully lead the transformation process.

In this blog series, we focused on the concept of Landing Zone, the primary aspects that a CCoE should be able to understand and apply. The collaboration between the CCoE and an expert partner allows companies to design their own Cloud environments in the best possible way and to customize it according to each company-specific need.

Always with evolution in mind: just like any IT project, the Landing Zone is not a static object. Instead, it is something dynamic that must be adapted continuously to the never-ending change both in the company and the AWS world.

Nicola Ferrari

Cloud Infrastructure Line Manager @ beSharp and AWS authorized instructor champion.I live my life one level at a time getting superpowers by collecting caffeine hidden here and there in my daily map. I'm a hardened internet surfer (yes, I surfed the whole internet... twice!) and tech-addicted with a passion for computers and networking. Building great IT things all nice and tidy contribute to achieving my main goal: the pursuit of perfection!

Simone Merlini

CEO and co-founder of beSharp, Cloud Ninja and early adopter of any type of * aaS solution. I divide myself between the PC keyboard and the one with black and white keys; I specialize in deploying gargantuan dinners and testing vintage bottles.
