Landing Zone on AWS: design strategies and best practices

6 July 2022 - 9 min. read

governance and compliance | Landing Zone

In the previous article, we explained what a Landing Zone is and focused on some basic notions on how to approach this topic.

In this article, we will analyze and detail the aspects on which a Landing Zone should be built and which AWS services to leverage.

Let's dive deep into the core aspects of a well-designed Landing Zone.

Organization

The first argument that must be considered concerns the accounts structure - aka the Organization - which, as specified by Conway's Law (link to article 1), must reflect the company's organizational structure. This means that different teams have both their own responsibilities and different resource needs.

This is where the **AWS Organizations** service comes into play. It allows us to organize accounts by scope, create Organizational Units (OUs), simplify the allocation of costs, and automate the creation of new Accounts. An account is the only way to separate costs at the billing level. Multiple accounts help separate generated billing volumes between business units, functional teams, or individual users.

The multi-account strategy leads to the highest level of resource and security isolation. As appropriate, the isolation must also take place at the data level.

Isolating data stores into accounts limits the number of people who can access and manage that data store by helping to comply with the General Data Protection Regulation (GDPR).

The first step on the path that leads us to a correct configuration is to create two macro groups of accounts: the **Foundational** ones and those dedicated to **Products and Workloads**.

The **Foundational** accounts are dedicated to the structure teams and designed to meet the company's needs.

For **Product and Workloads**, it is convenient to create OUs grouping products into accounts according to development environments (from Dev to Production), as well as OUs dedicated to hosting environments or accounts dedicated to structure's workload groups. Different business units or products may have different purposes and processes.

Not to be underestimated is the presence of default service quotas in AWS accounts. Separating workloads into different accounts prevents them from consuming limits and helps streamline business processes.

Foundational Accounts

Identity and Access Management

The principle of **least privileges** is the mantra of those who manage access and permissions to infrastructures or parts of them. Respecting this principle means reducing the blast radius in the case of malicious subtraction of access rights to the Cloud environment.

This principle must not lead to overhead in management, thus implying the need for centralized management of credentials.

In the AWS scenario, it is possible to create resources both through the web console and through the use of Authenticated REST APIs. Therefore, the possibility of automating our actions through these APIs emphasizes even more how current the management of access credentials is.

Also, Practices such as **Multi-Factor Authentication**, **automatic rotation of credentials**, **a strong password policy**, and restricted authorization must certainly be implemented.

With regards to **authentication** and **authorization**, AWS offers several possibilities: from the use of **AWS IAM** to the possibility of integrating the corporate **Identity Provider (IdP)** with **AWS SSO**. These services allow both centralized access management and the compliance with all the security practices described above.

For console access, it is possible to create a landing page that allows to select our credentials and, perhaps, have a client that helps us manage our everyday programmatic accesses.

In addition to the centralized authorization and authentication management services, some tools can come to the rescue to help users to be efficient and effective in these daily steps. For example, **Leapp** is the tool we use every day to fulfill this need: it is an open-source tool used to manage the access credentials to Cloud environments in a secure and automated way.

Networking

The reachability of the Cloud environment is fundamental. From the connections of business users or collaborators to the connections of our external users, such as integrators or public users.

First of all, it is necessary to structure the subnetting of private networking by defining the **CIDRs** to be assigned to the various virtual networks present in the different accounts defined in the Organizations section. In this phase, it is important to **avoid overlapping** to avoid running into complicated scenarios in terms of implementation and management. Centralizing your endpoints and controlling their routes is important to ease connections' management and creation.

Virtual Networks are defined through the service **AWS VPC**, and they should be configured taking into account some critical aspects like the Provider's physic infrastructure and the infrastructures' availability requirements. Internet connectivity is delivered by the managed **Internet Gateway** and **AWS Managed NAT Gateways implementation.**

AWS Transit Gateway is another essential service in the AWS ecosystem for connecting different environments. It enables centralized management and set up of connections - both physically via **Direct Connect** and virtually - leveraging on AWS SiteToSite Managed VPN. **AWS SiteToSite Managed VPN** allows connections to company on-prem environments and data centers, and to partners, customers or system integrators. AWS Transit Gateway also allows inter-VPC connections.

It is common for companies to have users accessing remotely to virtual networks on a daily basis from all around the world. In this case, implementing a **VPN Dial Up** by taking advantage of **AWS Client VPN** and its integration with Transit Gateway should be taken into account.

DNS and domains management is another aspect that a properly designed Landing Zone can manage to govern. **AWS Route 53** and its peculiarities such as DNS Resolver can be used to manage both private, and public domains and determine which records are resolved from specific networks.

Security

Today, security practices affect IT as a whole. For these reasons, it should be integrated into every aspect and methodology, as already happened with **DevSecOps** (security applied to DevOps practices).

Traceability, **in-transit** and **at-rest data protection**, and implementation of **isolation** and **identity principles** are particularly critical foundational aspects on which a well-design Landing Zone should rely on. Speaking about isolation and identity, a careful design of the organization and centralized users management make it easy to comply with best practices.

As already explained, the AWS Cloud is based on authenticated APIs (used by the console itself). **AWS CloudTrail** is able to track each API call and consolidate all the logs in a single place.

The inbound traffic can be routed through centralized handling of rules in **AWS WAF**, the web firewall managed by the provider.

Security groups and Network ACL, instead, help to get more granular control over communication protocols and specific connections between networks. These tools

allow to determine which communications between users and company workloads are licit.

Regardless of the just mentioned features, it is a good rule to encrypt all public communications over the internet. Managing SSL certificates connected to our domains from a single point undoubtedly ease their control and distribution.

Governance e Compliance

While **Governance** identifies the roles and responsibilities of those who are in charge of making decisions, the **Compliance** refers to a set of regulatory requirements, legislation, procedures, and codes of conduct applied to a company.

As each organization has its own policies, it must be able to implement controls also in a Cloud environment easily. The introduction of these rules, anyway, should still ensure a certain space for DevOps to act and operate freely according to specific guardrails.

As described in a few paragraphs above, using security best practices is essential to secure every company procedure. Data, for example, should always be encrypted at-rest. It must be ensured an effective way to verify that workloads remain compliant over time. Another important standard to enforce is preventing unintended firewall rules that could expose infrastructures to risks. Exposing known vulnerabilities protocols is one of the most common examples.

We can rely on the AWS Config service to automatically apply all the rules we went through and implement remediations.

Although AWS offers many services designed for different goals, companies usually leverage on a specific subset of them. The same goes for the global regions in which to deploy new workloads. **Service Control Policies** allow organizations to define guardrails and prevent this kind of unwanted actions.

Recommended checks also include a classification of the resources placed in each AWS environment. To achieve this, tagging strategies are the only choice. Tags enable effective costs sharing and provide the possibility to manage permissions on **ABAC** (Attribute-based Access Control) base. In addition, Tag Policies allow resource tagging enforcement and centralized tag management.

Any company should also define the deprovisioning practices for unused resources to reduce complexity and simplify cost attribution, analysis, and understanding.

Costs control

Organizations need an easy and immediate way to access **AWS billing information**, including a **summary of expenses**, a **breakdown of all service costs** incurred by accounts within the organization, along with **discounts** and **credits**.

Both invoices consolidation (consolidated billing) and adequate guardrails provisioning are fundamental for keeping control over costs, governance, and security. AWS enables organizations to balance freedom and control by enabling granular user permission governance.

Making informed decisions requires complete, near real-time visibility of costs and usage information. AWS provides tools for organizing resources as needed and viewing and analyzing cost and usage data in a single pane. As well as centrally controlling costs, real-time cost information can be provided to all the different teams. Detailed, allocable cost data allow teams to gain visibility and information to report spending.

AWS Cost Explorer provides an easy-to-use interface that allows you to view, analyze, and manage AWS costs and usage over time. **AWS Budget** is used to set custom budgets to track costs and usage from the simplest to the most complex use cases.

Disaster Recovery

"Everything fails all the time" - Werner Vogel.

Failures are just around the corner. Designing with failure in mind is the key to building resilient infrastructures. For this reason, **Disaster Recovery** is a strategy that has to be considered from the very beginning of the Landing Zone design process.

The typologies of disasters that can happen in the Cloud, and widely speaking, are divided into three groups:

- Natural disasters, such as earthquakes or floods
- Technical failures, such as power failure or network connectivity

- Human actions, such as inadvertent misconfiguration or unauthorized/outside party access or modification

AWS does not guarantees the resiliency of infrastructures, but it provides all the tools to leverage in order to make them resilient to failures. All that is defined in the **AWS Shared Responsibility Model**.

In this scenario, it is mandatory to define a multi-region and multi-account strategy, isolating the main organization from the disaster recovery one. Access to the two structures must also be separated and assigned to different personnel.

The Disaster Recovery strategies can be categorized into various approaches, ranging from low costs and low complexity, e.g., backup&restore, to more expensive and complex, e.g., active-active strategies.

The definition of two KPIs is crucial in choosing a correct strategy: Recovery Time Objective (**RTO**) and Recovery Point Objective (**RPO**). The first one defines how long business can be interrupted when a disaster happens. The second one identifies how much data loss is acceptable in terms of time in the event of a service interruption. The values assigned to these KPIs determine which strategy should be applied.

To conclude

It has been covered a lot of ground with this overview of the Landing Zone pillars; therefore, depending on the different needs, many customizations can be obtained. Each case must always be addressed starting from a design session aimed to the definition of the requirements that involves both all the company stakeholders and an expert partner.

In the following article, we will take as an example how two different companies with different sizes and needs - one small and one large - could start to think of a well-suited Landing Zone.

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.
