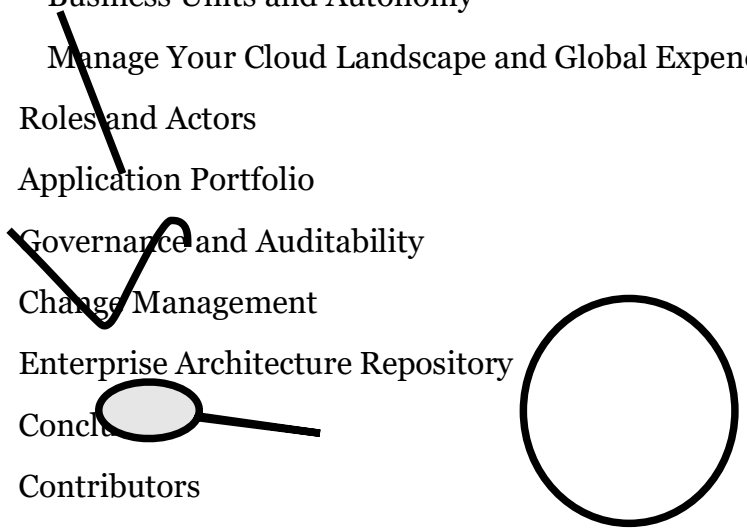
Establishing Enterprise Architecture on AWS

March 2018

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents



Abstract

This whitepaper outlines AWS practices and services that support enterprise architecture (EA) activities. It is written for IT leaders and enterprise architects in large organizations.

Enterprise architecture guides organizations in the delivery of the target production landscape to realize their business vision in the cloud. There are many established enterprise architecture frameworks and methodologies. In this whitepaper, we will focus on the AWS services and practices that you can use to deliver common enterprise architecture artifacts and tools and provide business benefit to your organization.

This whitepaper uses terms and definitions that are familiar to The Open Group Architecture Framework (TOGAF) practitioners, but it is not restricted to TOGAF or any other EA framework.[1]

Introduction

A key challenge facing many organizations is demonstrating the business value of their IT assets. Enterprise architecture aims to define the target IT landscape that realizes the business vision and drives value.

The key goals of enterprise architecture are to:

- Analyze and evolve the organization's business vision and strategy
- Describe the business vision and strategy in a common manner (for example, business capabilities, functions, and processes)
- Provide tools, frameworks, and specifications to support governance in all the architectural practices
- Enable traceability across the IT landscape
- Define the programs and architectures needed to realize the target IT state

A key value proposition of a mature enterprise architecture practice is being able to do better "What if?" analysis or impact analysis. Being able to identify what applications realize what business capabilities lets you make informed decisions on delivering your organization's business vision.

For example:

- "What is the impact on our IT landscape if we decide to outsource a certain business service?"
- "What business capabilities and processes are impacted if we retire a certain IT system?"
- "What is the cost of realizing this aspect of our business vision?"

This whitepaper will help you create end-to-end traceability of IT assets, which is one of the main goals of enterprise architecture teams.

Traceability, audit, and capture of "current state" is a perpetual challenge in a world of vendor-specific hardware and legacy systems. Often it is simply not possible for enterprises to catalog all of their assets. In this scenario, they cannot determine the business value of their IT landscape. Moving to the cloud

gives enterprises an opportunity to achieve traceability of their assets in the cloud.

Enterprise Architecture Tenets

Enterprise architecture tenets are general rules and guidelines that inform and support the way in which an organization sets about fulfilling its mission. They are intended to be enduring and seldom amended.

You should use tenets to guide your architecture design and cloud adoption. Tenets can be used through the entire lifecycle of an application in your IT landscape—from conception to delivery—and to support ongoing maintenance and continuous releases. Tenets are used in application design and should guide application governance and architectural reviews.

We highly recommend creating cloud-based tenets to guide you in creating applications and workloads that will help you realize and govern your enterprise's target landscape and business vision.

Examples of tenets might be:

"Maximize Cost Benefit for the Enterprise"

A cost-centric tenet encourages architects, application teams, IT stakeholders, and business owners to always consider the cost effectiveness of their workloads. It encourages your enterprise to focus on projects that differentiate the business (value), not the infrastructure. Your enterprise should examine capital expenditure and operational expenditure for each workload. It will result in customer-centric solutions that are most cost effective. These savings benefit both your organization and your customers.

"Business Continuity"

A business continuity tenet informs and drives the non-functional requirements for all current and future workloads in your enterprise. The geographic footprint and wide range of AWS services supports the realization of this tenet. The AWS Cloud infrastructure is built around AWS Regions and Availability Zones. Each AWS Region is a separate geographic area. Each Region has multiple, physically separated, and isolated locations know as Availability Zones. Availability Zones

are connected with low latency, high throughput, and highly redundant networking.

This tenet guides the architecture and application teams to leverage the reliability and availability of the AWS Cloud.

"Agility and Flexibility"

This tenet enforces the need for all applications to be "future proof."

In a cloud computing environment, new IT resources are only ever a click away, which means you reduce the time it takes to make those resources available to your developers from weeks to just minutes. This results in a dramatic increase in agility for your organization, since the cost and time it takes to experiment and develop is significantly lower.

Being flexible and agile also mean that your enterprise responds rapidly to business requirements as customer behaviors evolve. The AWS Cloud enables teams to implement continuous integration and delivery practices across all development stages. DevOps, DevSecOps, and methodologies such as Scrum become easier to set up. Teams can quickly compare and evaluate architectures and practices (e.g., microservices and serverless) to determine what solution best fits enterprise needs.

"Cloud First Strategy"

Such a tenet is key to an organization that wishes to migrate to the cloud. It prescribes that new applications should be in the cloud. This governance prohibits the deployment of new applications on non-approved infrastructure. Architectural and review boards can closely examine why a workload should be granted an exception and not deployed in the cloud.

"All Users, Services, and Applications Belong in an Organizational Unit"

An enterprise may use this tenet to ensure that its target landscape reflects the enterprise's organizational structure. It mandates that all cloud activities belong in an AWS organizational unit, which lets your enterprise govern the business

vision globally but gives autonomy when necessary to various local business units.

"Security First"

This tenet describes the security values of the organization. For example, "Data is secured in transit and rest," or "All infrastructure should be described as code," or "All workloads are approved by the security organization," etc.

Using this tenet, your architecture team can determine what level of trust they have in the cloud. Enterprises vary from zero trust to total trust. In a zero trust scenario, the enterprise would control all encryption keys, for example. They would decide to use customer-managed keys with AWS Key Management Service.[2] They would manage key rotation themselves and store the keys in their own hardware security module (HSM). In a total trust scenario, the enterprise would choose to allow AWS to manage the encryption keys and key rotation. They would also choose to use AWS CloudHSM.[3] AWS can support your enterprise in both zero trust and total trust scenarios.

The security tenet guides you in deciding where your enterprise is at on that scale.

Tenets should be used to guide architectural design and decisions that drive the target landscape in the cloud. They provide a firm foundation for making architecture and planning decisions, for framing policies, procedures, and standards, and for supporting resolution of contradictory situations. Tenets should also be heavily leveraged during the architectural review phases of applications and workloads before they go live, to ensure the correct target landscape is being realized.

Enterprise Architecture Domains

Enterprise architecture guides your organization's business, information, process, and technology decisions to enable it to execute its business strategy and meet customer needs.

There are typically four architecture domains:

- **Business architecture** domain – describes how the enterprise is organizationally structured and what functional capabilities are necessary to deliver the business vision. Business architecture addresses the questions WHAT and WHO:

  WHAT is the organization's business vision, strategy, and objectives that guide creation of business services or capabilities?

  WHO is executing defined business services or capabilities?

- **Application architecture** domain – describes the individual applications, their interactions, and their relationships to the core business processes of the organization. Application architecture addresses the question HOW:

  HOW are previously defined business services or capabilities implemented?

- **Data architecture** domain – describes the structure of an organization's logical and physical data assets and data management resources. Knowledge about your customers from data analytics lets you improve and continuously evolve business processes.

- **Technology architecture** domain – describes the software and hardware needed to implement the business, data, and application services.

Each of these domains have well-known artifacts, diagrams, and practices.

Enterprise architects focus on each domain and how they relate to one another to deliver an organization's strategy. In addition, enterprise architecture tries to answer WHERE and WHY as well:

- WHERE are assets located?
- WHY is something being changed?

Figure 1 shows how these domains fit together:

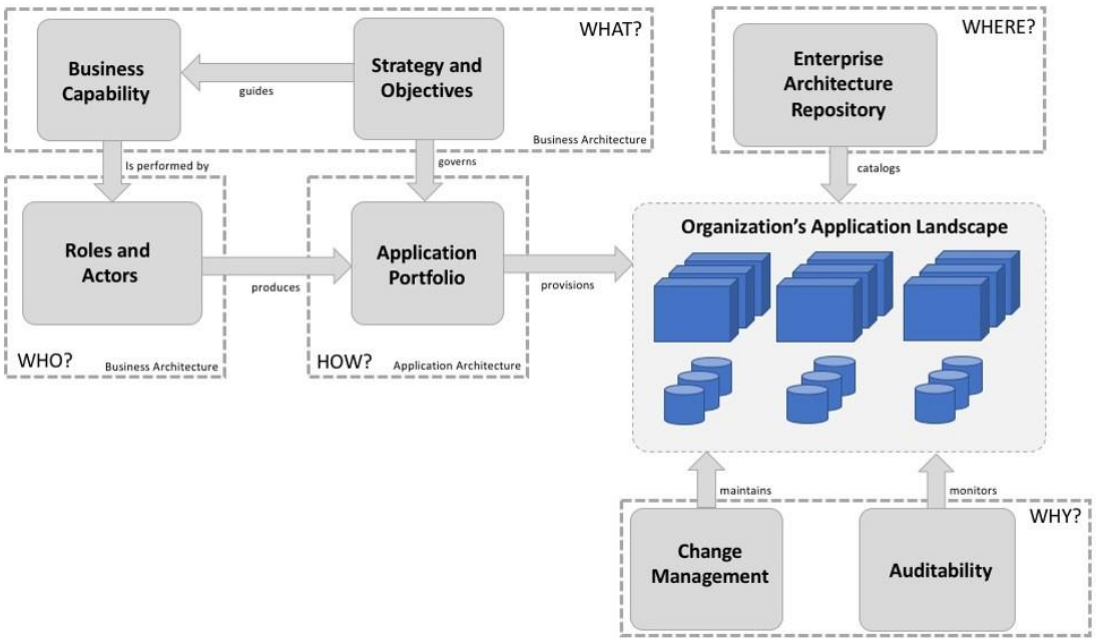


Figure 1: The four domains of an enterprise architecture

AWS Services that Support Enterprise Architecture Activities

Several AWS services can support your enterprise architecture activities:

- AWS Organizations
- AWS Identity & Access Management (IAM)
- AWS Service Catalog
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- AWS Tagging and Resource Grouping

Figure 2 shows how these services support your enterprise architecture:

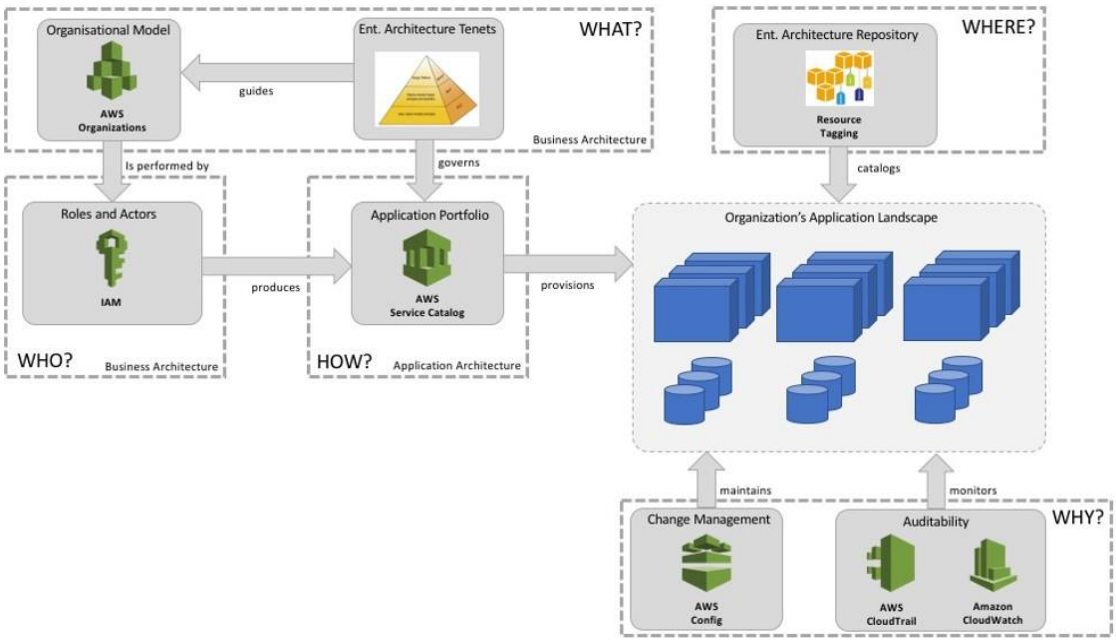


Figure 2: AWS services that support an enterprise architecture

The following sections discuss each of the enterprise architecture activities and AWS services shown in Figure 2.

Organizational Model

AWS Organizations[4] lets you arrange your AWS accounts[5] into groups called organizational units (OUs)[6] that reflect your business organizational model. Within and across those OUs you can define centrally managed policies and apply them in a uniform manner. You can also define how accounts are created and removed from the organization. With AWS Organizations, you can:

- Replicate your organizational structure in your cloud environment
- Give your business units autonomy while maintaining a global governance
- Manage your cloud landscape (the creation and deletion of accounts) and global expenditure

Replicate Your Organizational Structure in Your Cloud Environment

In AWS Organizations, the root is the parent container for all the accounts for your organization. OUs are nested under the root. You can define OUs to reflect your existing or target organizational model. OUs can contain accounts or other OUs, and you can create tiers of OUs.

Figure 3 shows an example of an organization that consists of 14 AWS accounts (Ax) that are organized into 9 OUs under the root.

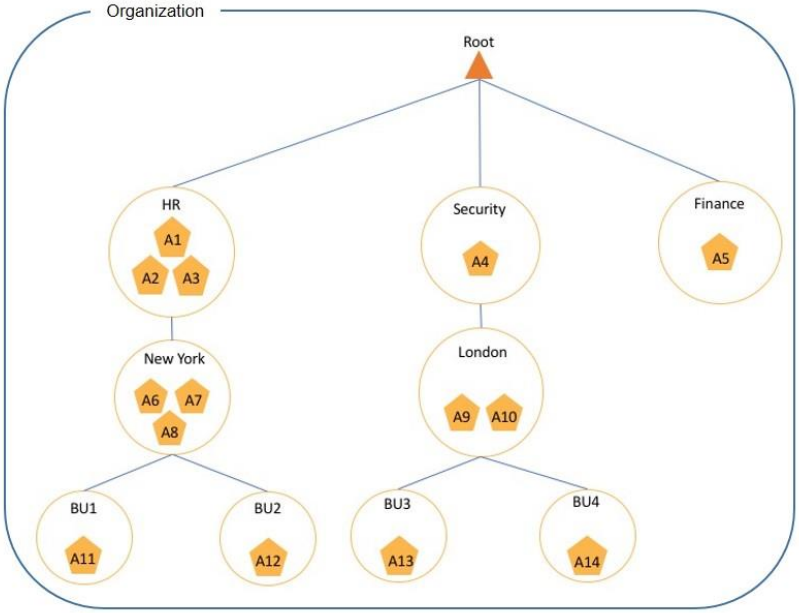


Figure 3: Organizations reflect an enterprise's organizational model

In this example, the OUs represent the enterprise's global Human Resources (HR), Security, and Finance departments, New York and London locations, and four business units (BUx).This maintains an AWS Cloud account structure that reflects the enterprise's organizational model.

Business Units and Autonomy

Giving your business units autonomy while maintaining a global governance practice, and giving departments and teams autonomy to explore new technologies and techniques while still maintaining an overview of the

organization are a couple of the challenges with enterprise architecture governance. You can address these challenges with Service Control Policies (SCPs).

SCPs are policies that specify the services and actions that users and roles can use in the accounts that the SCP affects. You can apply SCPs at any layer in the organization. Using the same organization example, Figure 4 shows policies applied to the root and to HR, Security, London, and BU1 OUs:

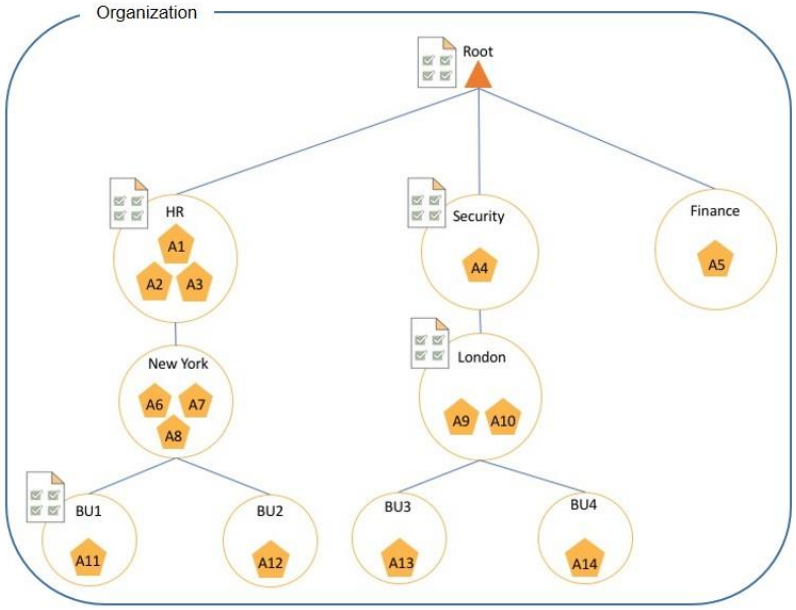


Figure 4: Service control policies applied to organizations in the enterprise organizational model

If you apply a policy to the root, it applies to all OUs and accounts in the organization. For example, the SCP applied at the root level of a healthcare enterprise might deny the use of any non-HIPAA-compliant AWS service[7] or, in a financial organization, it could deny access to services that are not compliant to PCI-DSS financial standards. No OU can use a non-compliant service that is defined in an SCP applied at the root level. Once a service becomes compliant in an AWS Region, you can add it to the policy.

Likewise, you can attach SCPs throughout the organizational hierarchy as appropriate to the business function. For example, as shown in Figure 4, you can attach policies based on different functions (HR and Security), local markets (London), and local business units (BU1).

When you attach a policy to one of the nodes in the hierarchy, it affects all the OUs and accounts beneath it. The SCPs associated with the HR, Security, and London OUs are enforced in all child OUs. An SCP associated with a child AWS account or OU cannot change this behavior—it can only work within the bounds of that policy.

Applying SCPs to your OUs gives your business units autonomy while maintaining a global governance.

You can also add new and existing AWS accounts to an OU and remove accounts from an OU. You can also specify the OU that new accounts can be created in. These accounts will inherit the previously defined policies and behaviors of that OU.

Manage Your Cloud Landscape and Global Expenditure

Enterprise architects are also concerned about the total cost of ownership of the organization's IT landscape. AWS Organizations supports you in this activity.

AWS Organizations lets you set up a single payment method for all the AWS accounts in your organization through consolidated billing. With consolidated billing, you can see a combined view of charges incurred by all your accounts, as well as take advantage of pricing benefits from aggregated usage, such as volume discounts for Amazon Elastic Compute Cloud (Amazon EC2)[8] and Amazon Simple Storage Service (Amazon S3).[9]

Roles and Actors

In the business architecture domain, there are actors and roles. An actor can be a person, organization, or system that has a role that initiates or interacts with activities. Actors belong to an enterprise and, in combination with the role, perform the business function.

Understanding the actors in your organization enables you to create a definitive listing of all participants that interact with IT, including users and owners of IT systems. Understanding actor-to-role relationships is necessary to enable organizational change management and organizational transformation.

The actors and roles of your enterprise can be modelled on two levels. Typically, an organization has a corporate directory (e.g. Active Directory) that reflects its actors and roles. On a different level, you can enforce these components with AWS Identity and Access Management (IAM).[10]

IAM achieves the actor-role relationship while complementing AWS Organizations. In IAM, an actor is known as a user. An AWS account within an OU defines the users for that account and the corresponding roles that users can adopt. With IAM, you can securely control access to AWS services and resources for your users. You can also create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources.

SCPs put bounds around the permissions that IAM policies can grant to entities in an account, such as IAM users and roles. The AWS account inherits the SCPs defined in, or inherited by, the OU. Then, within the AWS account, you can write even more granular policies to define how and what the user or role can access. You can apply these policies at the user- or group-level.

In this manner, you can create very granular permissions for the actors and roles of your organization. Key business relationships between OUs, actors (users), and roles can be reflected in IAM.

Application Portfolio

Application portfolio management is an important part of the application architecture domain in an enterprise architecture. It covers managing an organization's collection of software applications and software-based services that are used to attain its business goals or objectives. An agreed application portfolio allows a standard set of applications to be used in an organization.

You can use AWS Service Catalog to manage your enterprise's application portfolio in the cloud.[11] and centrally manage commonly deployed applications. It helps you achieve consistent governance and meet your compliance requirements.

AWS Service Catalog ensures compliance with corporate standards by providing a single location where organizations can centrally manage catalogs of their applications. With AWS Service Catalog, you can control which applications and

versions are available, the configuration of the available services, and permission access by an individual, group, department, or cost center.

AWS Service Catalog lets you:

- **Define your own application catalog** - End users of your organization can quickly discover and deploy applications using a self-service portal.
- **Centrally manage lifecycle of applications** - You can add new application versions as necessary, as well as control the use of applications by specifying constraints such as the AWS Region in which a product can be launched.
- **Grant access at a granular level** – You can grant a user access to a portfolio to let that user browse and launch the products.
- **Constrain how your AWS resources are deployed**- You can restrict the ways that specific AWS resources can be deployed for a product. You can use constraints to apply limits to products for governance or cost control. For example, you can let your marketing users create campaign websites but restrict their access to provision the underlying databases.

Governance and Auditability

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account.[12] With CloudTrail you can log every API call made. This enables compliance with governance bodies, internal and external to your organization. CloudTrail gives your organization transparency across its entire AWS landscape. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.

Amazon CloudWatch is a monitoring service for AWS Cloud resources and the applications you run on AWS.[13] You can use CloudWatch to collect and track metrics, collect, and monitor log files, set alarms, and automatically react to changes in your AWS resources. CloudWatch monitors and logs the behavior of

your application landscape. CloudWatch can also trigger events based on the behavior of your application.

While CloudTrail tracks usage of AWS, CloudWatch monitors your application landscape. In combination, these two services help with architecture governance and audit functions.

Change Management

Enterprise architects manage transition architectures. Transition architectures are the incremental releases in production that bring the current state to the target state architecture. The goal of transition architectures is to ensure that the evolving architecture continues to deliver the target business strategy. Therefore, you need to manage changes to the architecture in a cohesive way.

AWS Config is a service that lets you assess, audit, and evaluate the configurations of your AWS resources.[14] AWS Config continuously monitors and records your AWS resource configurations and lets you automate the evaluation of recorded configurations against desired configurations. With AWS Config, you can review changes in configurations and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

Enterprise Architecture Repository

An enterprise architecture repository is a collection of artifacts that describes an organization's current and target IT landscape. The goal of the enterprise architecture repository is to reflect the organization's inventory of technology, data, applications, and business artifacts and to show the relationships between these components.

Traditionally, in a non-cloud environment, organizations were restricted to choose expensive, off-the-shelf products to meet their enterprise architecture repository needs. You can avoid these expenses with AWS services.

AWS Tagging and Resource Groups let you organize your AWS landscape by applying tags at different levels of granularity.[15] Tags allow you to label, collect, and organize resources and components within services.

The Tag Editor lets you manage tags across services and AWS Regions.[16] Using this approach, you can globally manage all the application, business, data, and technology components of your target landscape.

A Resource Group is a collection of resources that share one or more tags.[17] It can be used to create an enterprise architecture "view" of your IT landscape, consolidating AWS resources into a per-project (that is, the on-going programs that realize your target landscape), per-entity (that is, capabilities, roles, processes), and per-domain (that is, Business, Application, Data, Technology) view.

You can use AWS Config, Tagging, and Resource Groups to see exactly what cloud assets your company is using at any moment. These services make it easier to detect when a rogue server or shadow application appear in your target production landscape.

You may wish to continue using a traditional repository tool, perhaps due to existing licensing commitments or legacy processes. In this scenario, the enterprise repository can run natively on an EC2 instance and be maintained as before.[18]

Conclusion

The role of an enterprise architect is to enable the organization to be innovative and respond rapidly to changing customer behavior. The enterprise architect holds the long-term business vision of the organization and is responsible for the journey it has to take to reach this target landscape. They support an organization to achieve their objectives by successfully evolving across all domains; Business, Application, Technology and Data.

This is no different when moving to the cloud. The Enterprise Architect role is key in successful cloud adoption. Enterprise architects can use AWS services as architectural building blocks to guide the technology decisions of the organization to realize the enterprise's business vision.

It has been challenging for enterprise architects to measure their goals and demonstrate their value with on-premises architectures. With AWS Cloud adoption, enterprise architects can use AWS services to create traceability and relationships across the enterprise architecture domains, allowing the architect

to correctly track how their organization is changing and improving. AWS lets the enterprise architect address end-to-end traceability, operational modeling, and governance. It is easier to gather data on transition architectures in the cloud as the organization moves to its target state.

The wide breadth of AWS services and agility means it is also easier for architects and application teams to respond rapidly when architectural deviations are identified and changes need to take place.

Using AWS services, you can more easily execute and realize the value of enterprise architecture practices.

Contributors

The following individuals and organizations contributed to this document:

- Margo Cronin, Solutions Architect, AWS
- Nemanja Kostic, Solutions Architect, AWS

Notes

[1] http://www.opengroup.org/subjectareas/enterprise/togaf

[2] https://aws.amazon.com/kms/

[3] https://aws.amazon.com/cloudhsm/

[4] https://aws.amazon.com/organizations/

[5] https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html#account

[6] https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html#organizationalunit

[7] https://aws.amazon.com/compliance/hipaa-compliance/

[8] https://aws.amazon.com/ec2/

[9] https://aws.amazon.com/s3/

[10] https://aws.amazon.com/iam/

[11] http://docs.aws.amazon.com/servicecatalog/latest/adminguide/introduction.html

[12] https://aws.amazon.com/cloudtrail/

[13] https://aws.amazon.com/cloudwatch/

[14] http://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html

[15] http://docs.aws.amazon.com/awsconsolehelpdocs/latest/gsg/what-are-resource-groups.html

[16] http://docs.aws.amazon.com/awsconsolehelpdocs/latest/gsg/tag-editor.html

[17] http://docs.aws.amazon.com/awsconsolehelpdocs/latest/gsg/what-are-resource-groups.html

[18] https://aws.amazon.com/ec2/