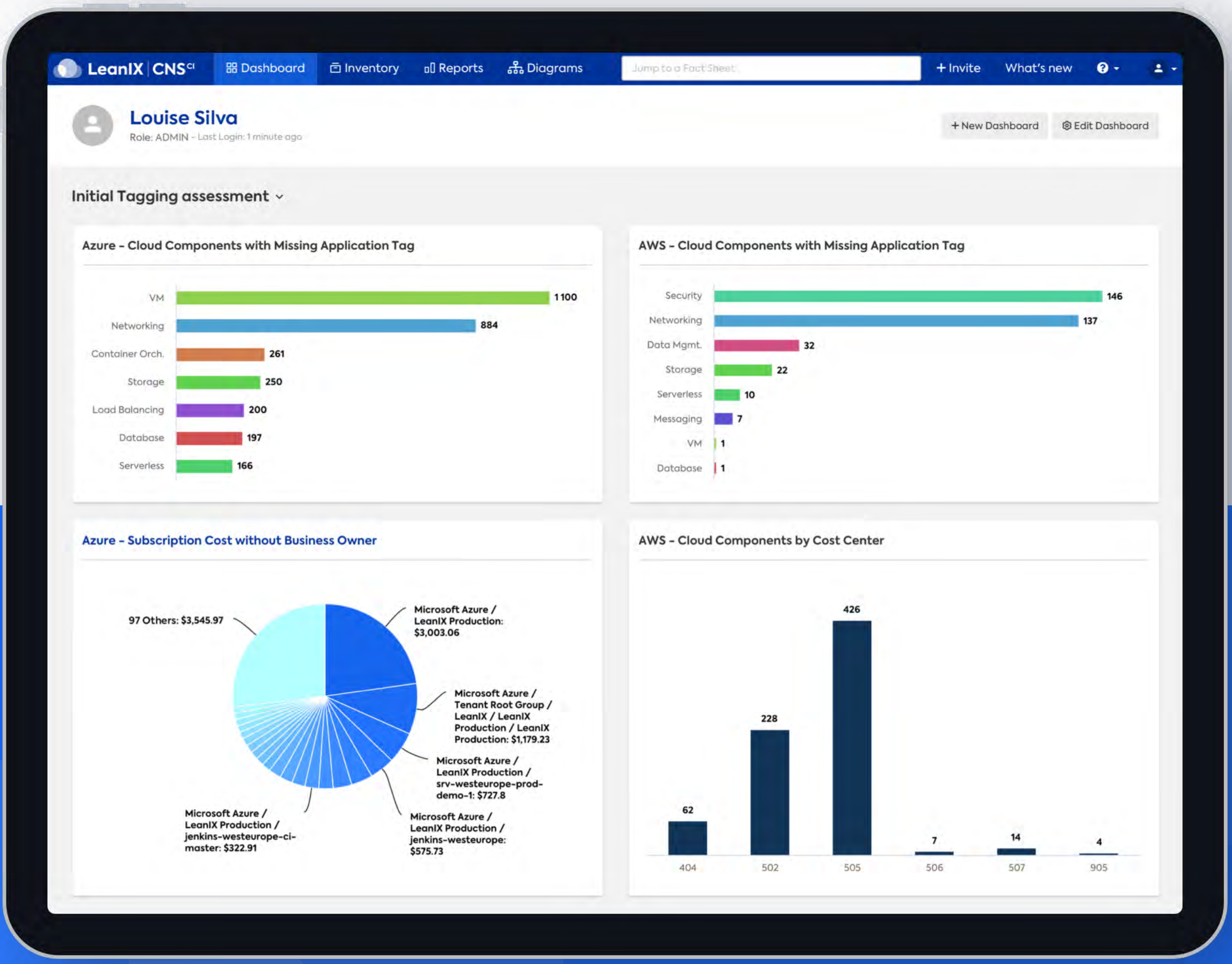
WHITE PAPER

A Guide to Managing Cloud Tagging Policies

Best Practices From LeanIX and CLOUDETEER



LeanIX | CNS
Dashboard
Inventory
Reports
Diagrams
Jump to a Fact Sheet
+ Invite
What's new
Louise Silva
Role: ADMIN - Last Login: 1 minute ago
+ New Dashboard
Edit Dashboard
Initial Tagging assessment
Azure - Cloud Components with Missing Application Tag
VM 1 100
Networking 884
Container Orch. 261
Storage 250
Load Balancing 200
Database 197
Serverless 166
AWS - Cloud Components with Missing Application Tag
Security 146
Networking 137
Data Mgmt. 32
Storage 22
Serverless 10
Messaging 7
VM 1
Database 1
Azure - Subscription Cost without Business Owner
97 Others: $3,545.97
Microsoft Azure / LeanIX Production: $3,003.06
Microsoft Azure / Tenant Root Group / LeanIX / LeanIX Production / LeanIX Production: $1,179.23
Microsoft Azure / LeanIX Production / srv-westeurope-prod-demo-1: $727.8
Microsoft Azure / LeanIX Production / jenkins-westeurope: $575.73
Microsoft Azure / LeanIX Production / jenkins-westeurope-ci-master: $322.91
AWS - Cloud Components by Cost Center
404 62
502 228
505 426
506 7
507 14
905 4

WHITE PAPER

A Guide to Managing Cloud Tagging Policies

Best Practices From LeanIX and CLOUDETEER

CONTENT

LeanIX

Introduction

Cloud adoption is now a familiar topic for corporate leaders. Most CIOs nowadays promote a cloud-preferred, if not cloud-first strategy, and there is hardly any company without some workloads already within Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP).

That being said, the complexity from one's cloud footprint increases as new stakeholders become involved. In order to leverage the benefits offered by the cloud, such as increased agility and productivity as well as reduced operational costs and infrastructure sprawl, enterprises need to scale cloud usage appropriately. Many companies do so by establishing a centrally organized, cross-functional team referred to as the Cloud Center of Excellence (CCoE) and assign it with the tasks of coordinating cloud migration, reporting on migration progress, and implementing effective guidelines to streamline business requirements with IT objectives. The CCoE usually consists of members from Enterprise Architecture, Governance, Finance, and Change Management functions as well as IT Security, IT Operations, and IT Infrastructure departments.

The diverse set of skills and experience within such a team represents a variety of views and interests. As such, it is recommended to set up a central inventory that automatically discovers cloud resources provisioned from across different hyperscalers in use. Core information like used services, accounts, regions, and costs can be shared consistently via this approach. However, since there is not yet a native way to see cloud resources according to business context and ownership, tagging and policies around tagging have emerged as a way for stakeholders to understand why certain resources are in use. Further, in order to reconcile all stakeholder interests, companies strive to bring a consistent interpretation of tags to central reports and views.

Organizing workloads in the cloud can nonetheless become challenging if tagging strategies are not implemented consistently, thereby making the benefits of categorizing cloud resources by owner, environment, or other criteria hard to realize. The business context of resources is especially hard to grasp when tagging is not set up effectively. Also, since tags are not retroactive, reports that rely on certain tags can only go back as far as the data that was first tagged. Tagging as early as possible is thereby advantageous, and there are ways and best practices to effectively implement tagging policies throughout your organization and track the progress of adherence.

This white paper will cover:

- **The benefits of having a cloud tagging strategy**
- **Best practices on which tags to start with**
- **How to implement tagging policies ranging from both technical (e.g., Infrastructure as Code) and organizational (e.g., policies to shut down untagged resources) solutions**
- **A five-step walkthrough on how LeanIX Cloud Intelligence supports effective tagging implementation to better utilize and manage cloud resources**

Understand Cloud Environments Through Tagging

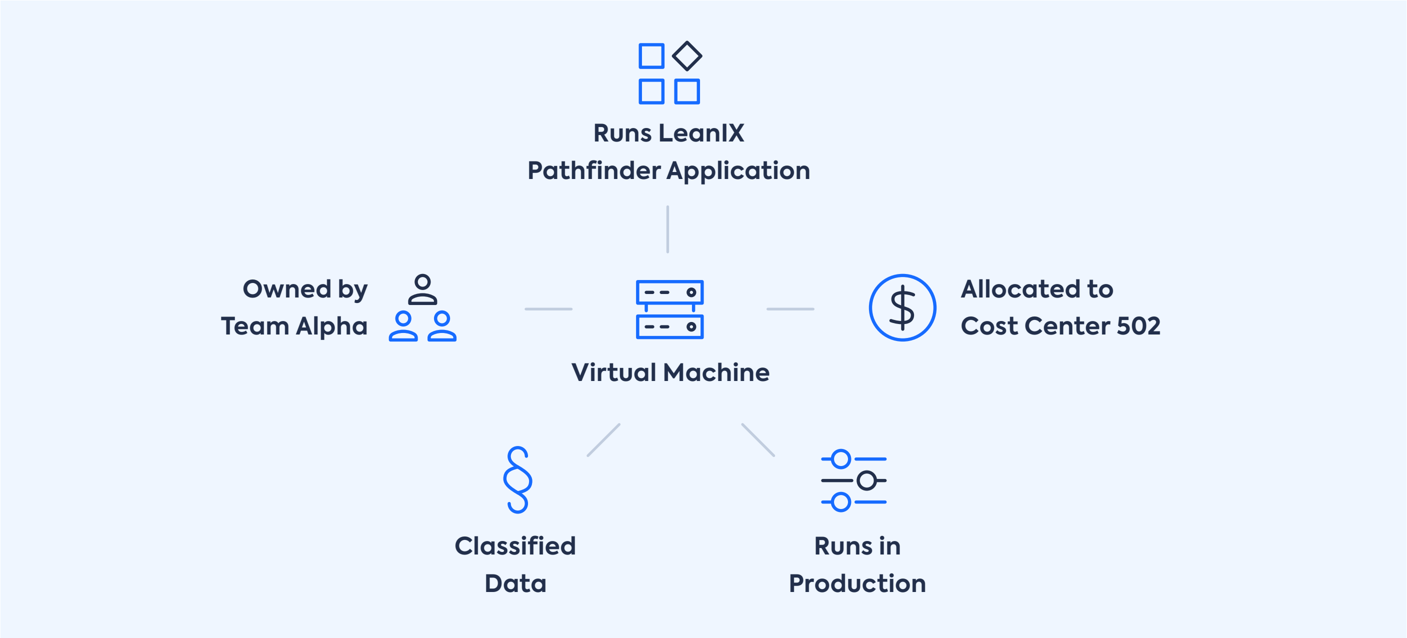
The accelerated adoption of public cloud services requires enterprises of all sizes to define their cloud governance requirements. Though venturing to the cloud, spinning up virtual machines (VM), provisioning storage, and running applications or other workloads takes only a matter of minutes, companies face the issue of not being able to understand which resources are used for which objective and how each ties back to the business.

While promises like economies of scale, faster time-to-market, and a greater focus on business value are alluring, companies frequently realize how easy it is to lose track of their workloads. A well-defined and properly managed cloud tagging policy forms the backbone of any cloud governance setup. Without one, companies are effectively blind and cannot answer essential questions like:

- Who is the owner of a virtual machine? Who can be reached if something goes wrong?
- What is the purpose of a VM? Is it hosting, for example, a business-critical customer relationship management (CRM) system or a website?
- Who pays for the usage of this VM and specifically, which cost center?
- In which environment does any given VM run (i.e., productive, development, or testing)?
- Are business-critical applications and servers backed up properly across all hyperscalers?
- Is a given VM processing customer data?

In addition to improving documentation of cloud environments, a tagging strategy translated into effective and properly implemented tagging policies provides numerous other benefits. Consider, for example, the ability to better understand cost management plus application tiering, automated backup generation, or reporting capabilities that can be leveraged based on certain tags (see Figure 1). This reduces the likelihood of errors and allows a CCoE to focus on creating business value instead of tasks such as ensuring virtual servers are backed up regularly.

Figure 1
Virtual Machine Tagging Example



Source: LeanIX GmbH

How to Organize Tagging Policies

Tag naming conventions

Major hyperscalers like AWS, Azure, and GCP support two major concepts to ensure comprehensive tagging policies are in place: explicit and implicit tagging.

Explicit tagging: Assign metadata and key-value pairs to cloud resources that allow adding specific business dimensions and context to cloud assets.

Implicit tagging: Impose naming conventions regarding the cloud account. For example, (1) all resources in account “abc-prod” support the application abc in production; (2) all resources in account “abc-dev” support the application abc in development.

At LeanIX, we often see companies combining both concepts. However, implementing proper tagging policies initially comes with the challenge of manual overhead. This can be reduced by automation and by including the tagging policy in Infrastructure as Code (IaC) templates. Still, even automation is prone to human error and tied to the conventions of the hyperscaler (e.g., how many characters are permitted to be in use). The setup of the account structure has other implications as well, as policies, access, and management overhead are connected to it.

Tag recommendations

When deciding what tags to implement across every hyperscaler, it’s best to start with a simple shortlist so as to ensure that your organization gets into the habit of continuously tagging resources. Of course, the more mature a cloud footprint becomes the more tags one will want to install to organize it to their needs. IT Service provider CLOUDETEER has codified their long experience in helping with cloud adoption into a list of 28 tags, grouped according to Operation Management, Security, Compliance & Governance, and Workload (Service) Specific. Such a list will certainly require some company-specific adaptation but building on top of best practices can save valuable time.

Table 1

CLOUDETEER’s 28 Tags for Organizing the Cloud (Recommended Tags for PROD/Q-Environment)

Scope	Key	Value (Examples)	Description
Operations Management			
	sla	24x7	How this service is covered by operation, like 24x7 or 10x5
	availability	ha	Define how this service is built — set up as standard availability or high-availability mode
	criticality	business-critical-24	Even availability is providing already the foundation for this, it is recommended to use a dedicated tag for later Group critical business workloads
	backup	daily-full	Backup policy reference, based on BCM specifications
	region	germany	Cloud region - can be later used for resource grouping (like GPDR/ non-GPDR).
	maintainer	internal-cloudops	Define operation responsibility, e.g., internal or external

continues on next page

Scope	Key	Value (Examples)	Description
Operations Management			
	deployment	pipeline-gitlab-tf	Define deployment type, e.g., such as DevOps pipieline or manual
	optimized	reserved	Define if any reserved capacity are in use, or regular charges, like AWS Saving Plans or Azure reserved instances
	runbook	06:00;19:00	Define times when a resource can be automatically shutdown or spun up or whether it runs 24/7
	last-update	20200916	Timestamp of last resource deployment update
Security, Compliance & Governance			
	data-classification	strictly-internal	Use well-known data classification or company existing rules
	compliance	iso27001	Define in-scope and if so to which compliance standard
	audit	enforced	Define security audit enforcement
	secops	user@cloudeteer.de	Define the key contact for cloud security operations
	vul-mgmt	monthly	Define if this resource is in-scope of vulnerability management (like vulnerability scanning in this case monthly)
	exposure	public	Define exposure of a resource, e.g., public or internal
Workload (Service) Specific			
	costcenter	intito0021	Define the relevant costcenter, like SAP department ID
	department	ito	Define relevant department this resource belongs to
	owner	team-xyz@cloudeteer.de	Define the owner of the resource
	service	app-project-xyx	Define the business service or function a resource belongs to
	tier	backend-database	Define the layer this resource belongs to. Grouping is quite important for several different cases, like applying consistent firewall rules
	billing	internal-costcenter	Define the billing policy of a resource
	budget	60000	Define monthly budget of a resource
	inventoryid	azr-vm-ito-08281	Define the CMDB configuration item ID of a resource, if applicable
	project	intralogistics-40	Define project if relevant
	environment	prod	Define stage like Dev, Prod, QA, Test
	type	PaaS	Define resource type, like IaaS, PaaS, SaaS or FaaS
	license	hybrid	Define the used licensing model of a resource, e.g., monthly charged marketplace item, hybrid licensing or none

Source: CLOUDTEER

If one wants to get started with tagging to ensure that tags are uniform, accurate, and up to date at all times, LeanIX recommends five tags to every resource to guarantee, right from the start, that an organization has concise information on the purpose and ownership of the resource.

1.

First, creating an **application** tag. The idea is that the organization installs a unique ID to identify the end product (in most cases an application) which is used for a particular purpose or process. This unique identifier does not vary across teams and remains consistent with the end product. It is best to use the concept of implicit tagging here. Choosing naming conventions such as app-123 instead of a name-based reference helps to avoid ambiguity. Ideally, one will apply naming already used in other tools or CMDBs that maintain an inventory of applications. As an example, LeanIX offers an enterprise architecture tool that holds a repository of a company's applications.

2.

Second, we recommend setting up **cost center** tags to create showback overviews and chargeback possibilities. Assigning cloud resources to corresponding cost center tags allows one to better assess from a business perspective which applications and teams create the highest costs and whether this expenditure is proportionate to the business value being generated. We've talked to companies that spend hours of human labor assembling cost reports for CFOs. Removing such labor from these teams helps the overall organization evolve from reactive to forward-thinking approaches wherein preventative actions are taken before costs have the chance to swell. The value for this tag is simply based on how the cost center is identified by the organization.

3.

Third, we recommend a **department** tag. Declaring ownership of resources allows organizations to immediately reach out to the right person(s) for cases perhaps related to security, training, cost-tracking, managing, and compliance. The reason to tag the department in a resource instead of specific developers or product managers is that individuals tend to change more than the department itself. The values that typically come in this tag follow the company's nomenclature for the departments (e.g., Internal IT / Platform Team) or for id-like naming (e.g., gb30c / gb40c).

4.

Fourth, we advise using a simple **environment** tag. Using the values of development, testing, and production, one can immediately understand how specific resources affect cloud environments. This tag is especially helpful when making critical decisions since individuals are able to spend minimal amounts of time analyzing the maximum impact of their decisions. Developers can also benefit from not having to spend additional time determining where workloads can be tested and instead spend more time creating new features for the company. Another benefit of this tag is that new hires will be safeguarded and not make the mistake of deploying test versions of critical applications to a productive and consumer-used deployment.

5.

Finally, when setting up **data classification** as a tag, individuals and their teams receive clear-cut guides as to who can access which services. This also speeds up the delivery times of services by protecting only what's needed plus eliminating the need to figure out how to protect an asset by marking all of them with either strictly internal, internal, classified, or public.

Of course, depending on the needs of the stakeholders and DevOps teams, additional tags will be relevant (see list above). Hence, the recommendation of using five tags is a good starting point but tailoring these to your specific needs is important to make sure stakeholders get the benefits they need.

Tag ownership

The tags presented previously should be owned by a central unit such as the CCoE. This group will hence be given the responsibility of the tag values in use and will ensure alignment with the stakeholders involved with each tag group. The initial implementation of tags can be straightforward when the company sets up the initiative, but ownership must occur at lower levels to maintain and secure accurate pictures of what a company is actually doing. We recommend that the nature of the tags be documented within a shared resource across the company alongside the agreed upon responsibilities of owners. Having this documentation can clear any confusion as to what roles a team plays.

For the application tag, we regularly see its management handled by enterprise architecture (EA) teams. The EA team manages the applications used in the organization and most often already have a repository of applications in place. In case of questions as to how to tag an application, the EA team serves as the best contact. Ideally, the CCoE has an enterprise architect as a member and hence can closely align the definition of the policy for the application tag.

The cost center tag reflects the nomenclature of cost centers set up in the company. The CCoE should work closely with the IT Controlling department to define the specific rules. This tag, as per its name, is all about costs, and the end-user is the person(s) responsible for reporting those costs as operating expenses.

The department tag will likely require the CCoE to work with different departments to collect the applicable team names.

The environment tag is most likely to be driven by the DevOps organization. As DevOps teams continue to manage deployments, it is they who have an overall picture of the condition of the resource. If there's not a DevOps culture within the organization, the CCoE should work with the operation manager to define which names to use for which situation.

Data classification is a tag that we see being managed by a security/compliance team run by the IT security department. Given that this team already manages other company compliance policies, it is a good practice to continue aligning within the realm of the cloud. Questions concerning what any tag entails can be answered directly by this team along with corresponding documentation to help comply with security certifications such as ISO 27001 and SOC 2I.

Tag policy documentation

Finally, tagging policies must be thoroughly documented and should cover policies of the tagging strategy that the company employs. This documentation should mainly list which tags are being used, who is in charge of the tags, and what values each tag contains. Also, it should be documented what the tagging policies are and what they do. The documentation should be centrally accessed and be approved by leaders.

Ideally, one has a central tool in place for providing an overview of tagging policies, its documentation, and the progress of the implementation. This central repository helps teams to ensure the completeness of a company's tagging strategy and governance. LeanIX's Cloud Intelligence module not only provides such potential for documentation but, alongside customizable dashboards, offers the opportunity to create centrally accessible overviews on tagging implementation progress, recent changes, or to notify tag owners to confirm or add tags to their resources. Managing cloud resources in this manner is thereby very effective.

Public Cloud Provider Best Practices

For additional reading, please see the following documentation from Amazon AWS, Microsoft Azure, and Google Cloud Platform:

- AWS Tagging Best Practices
- Microsoft Azure Best Practices
- Google Cloud Platform Best Practices

Set Up and Manage Tagging Policies

Once a company has decided upon a tagging strategy, it must then choose how to best implement it. One option is to set up governance and monitoring controls which work fairly reactively. Or, on the other hand, it can be decided to strictly regulate and control the provisioning of resources based on tags. Figuring out which approach best suits a company's needs is a cultural decision that comes with unique advantages and disadvantages.

For example, in case one chooses to govern tagging by monitoring the usage of tags, clear rules need to be communicated about tags to all employees and then monitor their application. However, though this approach is less intrusive to the daily work of cloud operations teams and can help foster a culture of trust and autonomy, it is also prone to human errors as there are no direct controls to prevent mistakes (e.g., typos). Further, clearly communicating tag policies is only one thing — ensuring that they are applied and understood properly is another.

In contrast to this reactive yet trust-building approach, there is the possibility of implementing tagging by setting up regulations that only allow the provisioning of resources if accurate tags are set. This guarantees that no untagged resource is spun up while simultaneously also increasing data quality. However, it also installs guardrails for developers and might cause them to feel less agile or, even worse, micro-managed.

So, how to best set up and manage effective tagging policies? Well, as is so often the answer, it depends on a company's culture and needs.

Tag governance

To implement effective tag governance, one should assess how capable an organization is to communicate clear guidelines to every developer that uses a cloud resource. If it is thought that this can be achieved, then it's necessary to find ways to effectively monitor untagged resources (e.g., by account or by department) and chase down the responsible owner for those. This means a cloud inventory such as that offered with LeanIX Cloud Intelligence, which automatically discovers and lists all cloud resources, their interdependencies, and the assigned owners, can simplify the process.

Once a tagging strategy has been chosen and an overview of your current tagged and untagged resources created, it is important to make properly tagging cloud resources an integral part of a company's development culture. One tactic for doing so is the gamification of policies to make tagging a habit in the daily lives of your employees. For example, consider adopting rules where developers cannot take their agenda items to a meeting to be further discussed unless they are correctly tagged and monitored in the LeanIX Cloud Intelligence inventory. Alternatively, one can incentivize the team by noting that only properly tagged items will be selected for upcoming sprints. Another idea might be to run team tagging contests and compare which team ranks highest in their tagging completion and award them.

Regardless of which approach suits a company best, when it comes to implementing tagging, it depends on the interests of tag owners themselves. Whoever is obsessed with data quality may not wish to rely on monitoring. In cases like these, we recommend implementing both partial and full tag controls. One can leverage the identity and access management concepts of the hyperscalers (e.g., the Identity Access Management policies in AWS/Azure) and enforce tagging upon resource creation by only allowing the provisioning of new resources if certain tags are set. One can also think about switching off non-productive, improperly tagged resources every night. This can be achieved by using automation runbooks or by notifying and following up with the resource owner until the required tags are set.

As a rule of thumb, when it comes to cloud operations, automating as much as possible is key. Hence, we recommend using automation to provision resources. Wherever possible and feasible, implement tagging requirements into the automation in use. For example, if IaC is already in use, embed tagging to templates for development and make it part of a pull request review to ensure that all tags are set. This mechanism comes very handily as you set the tagging for your service once and it will appear automatically on all resources that you provision thereafter using this particular template.

Popular services for productive IaC are CloudFormation or Terraform but one can also consider using a tool for non-productive environments. For example, Env0 manages resources for developers to ensure that no test or development environment is unnecessarily kept running. It also allows for tags to be centrally managed.

Further, one can think about implementing a central self-service portal containing all relevant details for resource provisioning. The hyperscalers provide these natively (e.g., AWS Service Catalog, GCP Private Catalog) and they also support central tag management.

We believe that effective tag management can be best achieved using a hybrid approach. Where automation is heavily used, governance and monitoring activities can easily be relied upon as the automation ensures that what is defined in the code is applied to all provisioned resources. Resources that are mainly managed manually, however, should be controlled using strict identity and access management policies.

Regardless of the implementation approach, a central tool should be in place that provides transparency into tagging status quo and also provides the ability to identify and notify tag owners. LeanIX Cloud Intelligence, for example, helps to effectively implement and execute tagging strategies throughout an organization. The following section will reveal how this can actually be achieved.

5 Steps to Implement Effective Tagging With LeanIX Cloud Intelligence

LeanIX Cloud Intelligence helps organizations define and monitor tagging policies in two ways. First, it provides a repository to match cloud information against business context, ownership, and various other sets of information. Doing so reduces the number of tags that need to be maintained at the hyperscaler and thereby contribute to more stable and reliable information. Secondly, it helps to make the technical concept of cloud tags visible and tangible in ways that business users can easily understand.

Here's a five-step approach to consolidating, improving, and leveraging your tagging with LeanIX Cloud Intelligence.

STEP 1
Get an initial overview of tag implementation

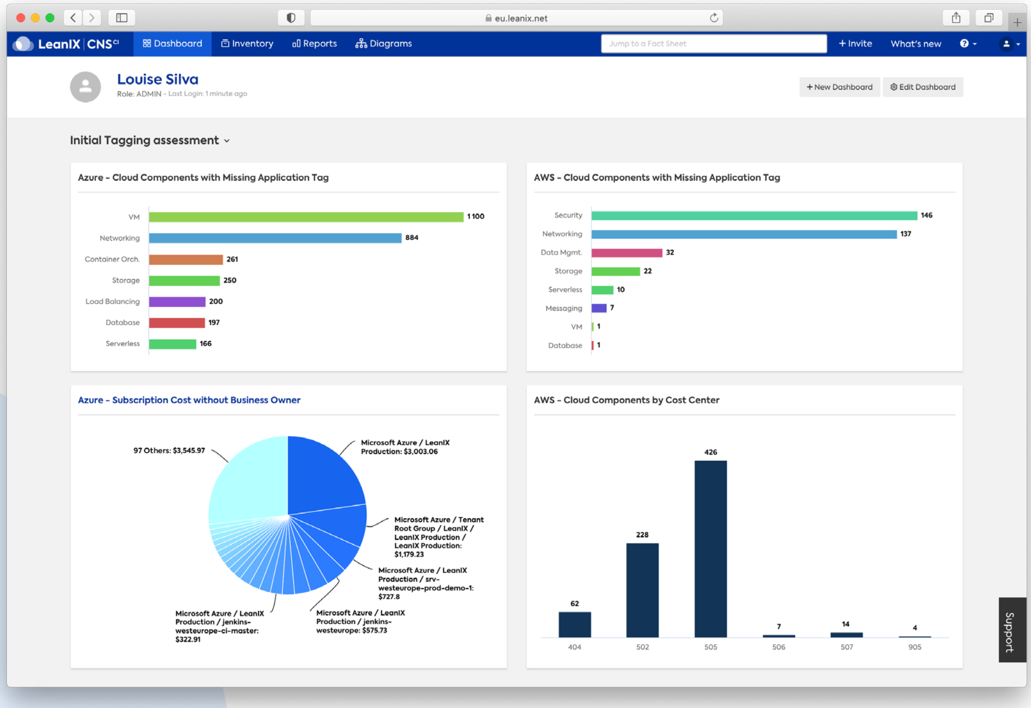
With LeanIX Cloud Intelligence, users immediately get an automatically discovered overview of their cloud inventory to assess the current status quo of tagging implementation efforts. Once Product IT leadership understands the importance of tagging, LeanIX Cloud Intelligence can support the team responsible for cloud governance to document and make tagging policies centrally accessible throughout an organization. Users are also provided with customizable dashboards to monitor and track central KPIs — those either global or dedicated to specific business areas (e.g., the tagging completion rate over time).

Dashboards like in Figure 3 help users to initially assess your tagging status quo and practice. Dashboards help identify items such as which cloud resources are currently untagged, how costs incur that are not identifiable with business context, or which team or cost center is responsible for a cloud bill.

Figure 2

LeanIX Dashboard in Cloud Intelligence

Shows the status quo of tag implementation


eu.leanix.net
LeanIX | CNS
Dashboard
Inventory
Reports
Diagrams
Jump to a Fact Sheet
+ Invite
What's new
Louise Silva
Role: ADMIN - Last Login: 1 minute ago
+ New Dashboard
Edit Dashboard
Initial Tagging assessment
Azure - Cloud Components with Missing Application Tag
VM
1 100
Networking
884
Container Orch.
261
Storage
250
Load Balancing
200
Database
197
Serverless
166
AWS - Cloud Components with Missing Application Tag
Security
146
Networking
137
Data Mgmt.
32
Storage
22
Serverless
10
Messaging
7
VM
1
Database
1
Azure - Subscription Cost without Business Owner
97 Others: $3,545.97
Microsoft Azure / LeanIX Production: $3,003.06
Microsoft Azure / Tenant Root Group / LeanIX / LeanIX Production / LeanIX Production: $1,179.23
Microsoft Azure / LeanIX Production / srv-westeurope-prod-demo-1: $727.8
Microsoft Azure / LeanIX Production / jenkins-westeurope: $575.73
Microsoft Azure / LeanIX Production / jenkins-westeurope-ci-master: $322.91
AWS - Cloud Components by Cost Center
62
228
426
7
14
4
404
502
505
506
507
905
Support

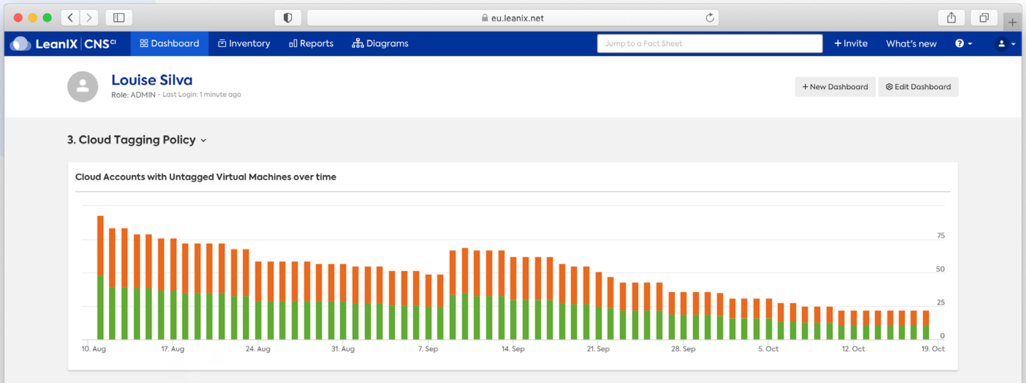
Source: LeanIX GmbH

After initially understanding your tagging status quo you can begin to measure the progress of your tagging practice and closely watch how it evolves over time. The following are exemplary KPIs that companies use for such purposes:

- How is the completion of mandatory tags evolving over time? Do certain business areas perform better than others?
- Are the most expensive cloud resources tagged and allocated to responsible owners?
- For legal restrictions (e.g. GDPR), do I have close to 100% coverage for mandatory tags (i.e., can I prove to external auditors that I understand all S3 Buckets with critical customer data and assure that they are hosted only in allowed regions)?
- How is the maturity of my cloud adoption progressing? Is my adoption of IaC (e.g., Terraform, AWS CloudFormation) proceeding as planned, or am I still relying on manual tagging in critical areas? Can I identify options to improve my centrally maintained hyperscaler tagging policies?

Figure 3

Tagging Progress for Untagged Virtual Machines Over Time



Source: LeanIX GmbH

STEP 2

Discover untagged resources

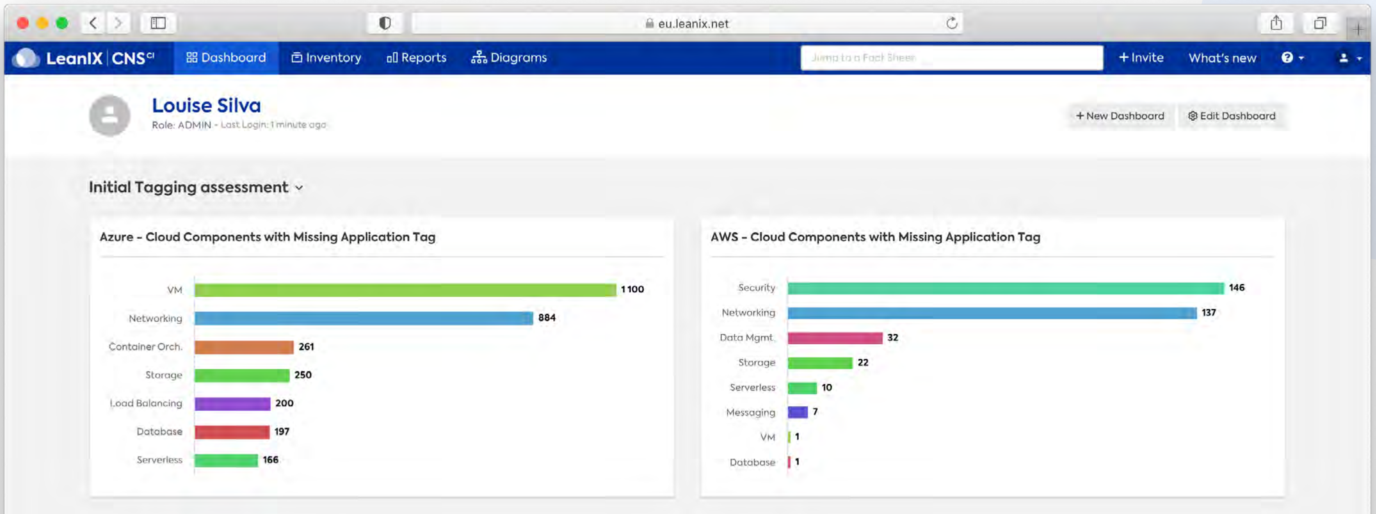
Capturing initial insights on the current status of the tagging practice helps IT management to better understand which incurring cost supports which organizational programs or products. Ideally, one receives this overview automatically and applies filters to generate the detailed views needed.

Since discovering untagged resources is an exercise that should be executed many times, LeanIX Cloud Intelligence provides powerful notification capabilities (e.g., generating Slack messages or notifying accounts owner whenever VMs reach a certain cost or miss a critical tag).

Figure 4

LeanIX Cloud Intelligence Identifies Untagged Cloud Resources

Source: LeanIX GmbH



STEP 3

Simplify tagging setups

As discussed, a best practice tagging framework like the one provided by IT service provider CLOUDETEER covers aspects around Operation Management, Security, or Compliance & Governance but nonetheless requires high rigor and alignment to keep data up to date. Though IaC and automation obviously help, topics like responsibilities become hard to maintain consistently over time. If this information becomes stale, such information tends to become mistrusted or even misleading. As core cloud governance processes rely on information quality, it's clear that every tag omitted increases stability and decreases tedious efforts. LeanIX Cloud Intelligence helps companies simplify maintenance (thus leading to higher efficiency and less errors) as follows:

- Subscriptions are a powerful part of the LeanIX platform. Not only can users express responsibilities on different levels (e.g., Accountable or Responsible, or with dedicated role types like Business Owner, Technical Owner, or Security Responsible), they can even utilize these subscriptions to get personal dashboards and reports or get notified via Mail, Slack, or Microsoft Teams whenever an important change occurs. LeanIX Administrators can reach out to Subscribers via Surveys (e.g., for structured input from all Business Owners in the support area). Finally, LeanIX supports standards like System for Cross-domain Identity Management (SCIM) to keep information automatically synced with the central identity management system.

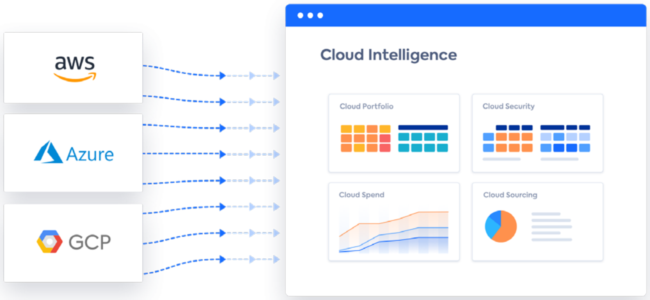
- Application context is important for companies, but the application stack inevitably evolves and changes fast. Application portfolio repositories like the LeanIX Enterprise Architecture Suite (EAS) help companies establish clear definitions around applications amongst business and IT stakeholders by taking into account changing business perspectives and evolving markets. Instead of relying on maintaining application names, department names, and other information as tags in the cloud, LeanIX Cloud Intelligence can map a central application ID into such a repository, thereby always keeping business and cloud information in sync while reducing error-proneness.

- As discussed earlier, a tagging policy consists in 99% of cases of details not only on how to use tags or labels but also of conventions or attributes of cloud accounts themselves. A typical example might be tags on an AWS account level or the convention that every Azure Resource Group with the suffix -dev is used for development purposes and not for production. This knowledge can be established in a small circle of experts (e.g., amongst the CCoE). However, as is especially the case for non-technical users, this information is far from intuitive. Given that core processes like cost showback or chargeback rely on tag accuracy, this imposes a clear risk for every organization that has outgrown the initial cloud adoption phase.

- LeanIX Cloud Intelligence helps make these conventions explicit. Business context with this solution can be extracted based on both account conventions and on tags. Also, LeanIX Cloud Intelligence lets one create powerful filters (e.g., to see only VMs in a productive Azure Subscription), that can be applied to a dashboard or shared in collaboration tools like Confluence and Sharepoint. This way, it helps to increase the transparency towards non-technical users and contributes heavily to the reliability of the information

Figure 5

Use Tagging as a Basis to Visualize Cloud Environments



Source: LeanIX GmbH

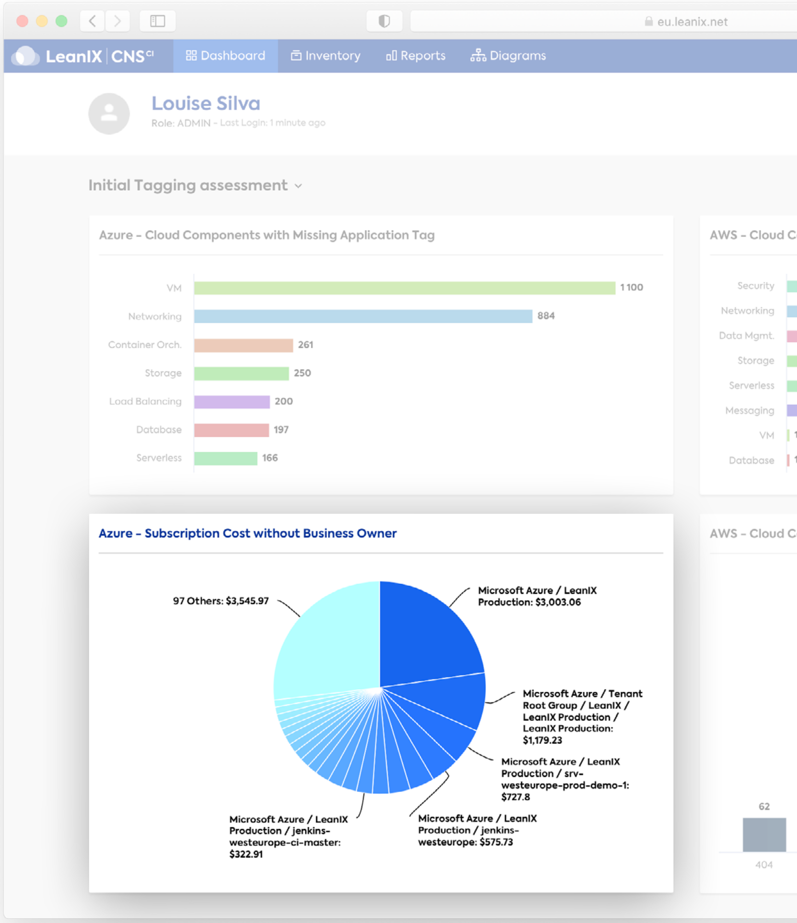
STEP 4

Analyze financial or business impact of tagged resources

It is of paramount importance to have easy insights on whether cloud resources are properly tagged — particularly for the most expensive cloud resources. Reports like those seen in Figure 2 can help to identify which costly resources lack tags so they can be addressed immediately.

Figure 6

Untagged Cost-intensive Resources Identified with LeanIX Cloud Intelligence


eu.leanix.net
LeanIX | CNS CI
Dashboard
Inventory
Reports
Diagrams
VM
Networking
Container Orch.
Storage
Load Balancing
Database
Serverless
1 100
884
261
250
200
197
166
AWS – Cloud C
Security
Networking
Data Mgmt.
Storage
Serverless
Messaging
VM
Database
97 Others: $3,545.97
Microsoft Azure / LeanIX Production: $3,003.06
Microsoft Azure / Tenant Root Group / LeanIX / LeanIX Production / LeanIX Production: $1,179.23
Microsoft Azure / LeanIX Production / srv-westeurope-prod-demo-1: $727.8
Microsoft Azure / LeanIX Production / jenkins-westeurope: $575.73
Microsoft Azure / LeanIX Production / jenkins-westeurope-ci-master: $322.91
AWS – Cloud C
62
404

Louise Silva
Role: ADMIN – Last Login: 1 minute ago

Initial Tagging assessment

Azure – Cloud Components with Missing Application Tag

Azure – Subscription Cost without Business Owner

Source: LeanIX GmbH

Step 5

Inform your business stakeholders

All tags mentioned in this white paper offer clear value for stakeholders throughout the IT value chain. However, to connect with individuals outside IT departments, it's important to limit technical details. Business stakeholders, for example, might be very interested if a certain application leverages AWS, if it hosts data in the U.S., if it carries a technical risk, or how much it costs. A business stakeholder may never fully understand a tagging policy but LeanIX Cloud Intelligence can nevertheless help. Not only does it make the business context explicit, but LeanIX Cloud Intelligence integrates seamlessly with the LeanIX Enterprise Architecture Suite. Here, the findings based in particular on the application tag is aggregated in an actionable way for business stakeholders with technical details just one click away.

Conclusion

Setting up and implementing proper tagging policies brings clarity to cloud environments and will unlock the many benefits offered by the cloud. LeanIX Cloud Intelligence helps to effectively tag these resources and maintain an up-to-date cloud resource inventory. In particular, by creating this single source of truth, any Cloud Center of Excellence can streamline IT objectives with business requirements and greatly assist in the management of cloud operations.

LEANIX.NET

If you'd like to know more about LeanIX Cloud Intelligence and how it supports effective tagging implementation, reach out!

Contact us! ⟶

LeanIX

This document is current at the time of its initial publication. LeanIX GmbH reserves the right to alter it at any time.
THE INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED AS IS, WITH NO WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLICIT.

LeanIX is the single source of truth for Corporate IT and Product IT to create transparency of the present and derive actions, to shape the future in an understandable business context. LeanIX provides its Software-as-a-Service to 300 international customers including well-known brands such as adidas, Atlassian, Dropbox, DHL, Merck, Volkswagen, Vodafone and Zalando. More than 50 certified partners such as Deloitte, Cognizant and PwC rely on the dynamically growing IT company co-founded in 2012 by LeanIX CEO André Christ. With EA Connect Days, LeanIX has been regularly organizing one of the world's most important industry events in the field of Enterprise Architecture since 2014. The company is headquartered in Bonn, Germany with additional offices in Boston, Massachusetts; Munich, Germany; Utrecht, Netherlands; and Hyderabad, India. It has more than 230 employees worldwide.

Copyright© LeanIX GmbH. All rights reserved. LeanIX and the LeanIX logo are trademarks or registered trademarks of LeanIX GmbH in Germany and/or other countries. All other products or services are trademarks of their respective companies.