|  |
| --- |
| New York Life |
| Cloud Services |
| NYL Cloud Tagging and Naming Standard |

|  |
| --- |
| Samuel Brinley Corporate vice President, Operations  1/26/2017 |

Table of Contents

[Document Revision History 3](#_Toc495499423)

[Executive Summary 3](#_Toc495499424)

[General Best Practices 3](#_Toc495499425)

[Tags 4](#_Toc495499426)

[Name 4](#_Toc495499427)

[Required 4](#_Toc495499428)

[Optional 5](#_Toc495499429)

[Service tags 5](#_Toc495499430)

[Monitoring 6](#_Toc495499431)

[Preventive actions 7](#_Toc495499432)

[Corrective actions 7](#_Toc495499433)

[Appendix 8](#_Toc495499434)

[Reference 8](#_Toc495499435)

# Document Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Document History | | | | |
| Version | **Date** | **Author** | **Changes Made** | **Approved by** |
| 1.0 | 1/26/2017 | Samuel Brinley | created |  |
| 1.1 | 7/27/2017 | Sal Cardello | Updated with latest tags |  |
| 1.2 | 10/11/2017 | Matt Dolian | Updated with Name and Naming convention, other fixes |  |

# Executive Summary

New York Life (NYL) uses Cloud resources to provide an environment where provisioning compute and storage resources in an easier and faster way than using standard on premise resources.

To ensure the proper identification and tracking of the most critical resources deployed, each resource must have a set of key/value pairs known as ‘Tags’. NYL has defined a set of tags that are required as well as optional. NYL has also defined acceptable values for these tags.

The compliance with the Tagging standard described in this document will be enforced by monitoring the appropriate assignation of Tags and values to each resource deployed in the Cloud. Upon detection of resources not correctly tagged, NYL will take corrective action to prevent the use of unidentified resources running on the Cloud. The corrective actions may include:

* Stop of compute instance resources
* Decommission of compute instance resources
* Decommission of storage resources

All the corrective action will be preceded by appropriate notification to the resource Owner and/or to the Group Platforms Owners before being executed.

# General Best Practices

When creating a tagging strategy for Cloud resources, make sure that it accurately represents organizationally relevant dimensions and adheres to the following tagging best practices:

* With the exception of the ‘Name’ tag, always use a standardized, case-sensitive format for tags, and implement it consistently across all resource types. **New York Life standard will be all lowercase.**
* Consider tag dimensions that support the ability to manage resource access control, cost tracking, automation, and organization.
* Err on the side of using too many tags rather than too few tags.
* Remember that it is easy to modify tags to accommodate changing business requirements, however consider ramifications of future changes, especially in relation to tag-based access control, automation, or upstream billing reports.

An effective tagging strategy uses standardized tags and implements them consistently across cloud resources. Customers use both reactive and proactive approaches for governing the use of tags in their cloud environments. Reactive governance leverages tools such as Tag Editor, detailed billing reports, Config Rules, or custom scripts to identify improperly tagged resources. Proactive governance leverages tools such as Cloud Formation and Service Catalog to ensure standardized tags are consistently applied at resource creation. More rigorous forms of proactive governance include automation to regularly scan an environment’s tags and quarantine or delete improperly tagged resources.

Tagging allows you to track resources in several dimensions:

* Ownership
* Cost management
* Business service/application relationships
* Audit and compliance
* Monitor account/subscription proliferation
* Data sensitivity

# Tags

Infrastructure issues such as compliance violations, security risks, or performance related problems, require a cloud manager to quickly understand who the owner is and the urgency of a given asset it so that responsible parties can be contacted in a timely manner. It is also important to clearly designate who is paying for a given asset. Below is a list of required and optional tags. This standard is subject to change at any time.

## Name

All resources must have the tag ‘Name’ (capitalized). The Name tag will be comprised of a series of other tags listed in the charts below. When appropriate, the resource name must match the tag Name. For some resources on AWS, the tag Name and the resource name must both be specified.

**Resource and Tag Name:** {lob}-{csg\_env}-{app\_env}-{application}-{service}

For acceptable lob, csg\_env, app\_env and application values, please refer to the [Required tags chart](#_Required) below. For acceptable service values, please refer to the [Service Tags chart](#_Service_tags) below.

In some cases, AWS may not support long resource names. In this case, the tag Name should still follow the naming convention but the resource name should just contain just the application and service name.

**Short Resource Name:** {application}-{service}

## Required

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***provider*** | ***lob*** | ***division*** | ***csg\_env*** | ***app\_env*** | ***Project*** | ***Platform*** | ***application*** | ***Function*** | ***mode*** |
| aws | Direct | AARP | nonprod | dev | CDN | aem | broadmarket | publisher | active |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *aws* | *cloudsec* | *free form name* | *prod* | *dev* | *Freeform* | *aem* | *free form name* | *publisher* | *active* |
| *goog* | *corptech* |  | *nonprod* | *mdl* |  |  |  | *author* | *primary* |
| *msft* | *direct* |  | *sandbox* | *stg* |  |  |  | *app* | *backup* |
| *nyl* | *eis* |  |  | *www* |  |  |  | *automation* | *slave* |
|  | *ecs* |  |  |  |  |  |  | *compute* |  |
|  | *insure* |  |  |  |  |  |  | *database* |  |
|  | *invest* |  |  |  |  |  |  | *directory* |  |
|  |  |  |  |  |  |  |  | *itsm* |  |
|  |  |  |  |  |  |  |  | *monitor* |  |
|  |  |  |  |  |  |  |  | *proxy* |  |
|  |  |  |  |  |  |  |  | *router* |  |
|  |  |  |  |  |  |  |  | *search* |  |
|  |  |  |  |  |  |  |  | *security* |  |
|  |  |  |  |  |  |  |  | *storage* |  |
|  |  |  |  |  |  |  |  | *queue* |  |
|  |  |  |  |  |  |  |  | *web* |  |

## Optional

Optional tags are listed below in yellow with an example value in blue.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***businessemail*** | ***clarity*** | ***costcenter*** | ***datatype*** | ***gig-backup*** | ***noscan*** | ***expired*** | ***appid*** |
| [Project\_owner@nyl.com](mailto:Project_owner@nyl.com) | xyz 1234 | 000011111 | private | 7d4w6m | noscan | 12/19/1976 | 54321 |

## Service

Below is a list of services and associated abbreviations to be used as values. This tag is optional but the abbreviations in this chart are used in the required Name tag and resource name on AWS.

|  |  |  |  |
| --- | --- | --- | --- |
| *service* | | | |
|  |  |  |  |
| cloudformation | **cloudtrail** | **cloudwatch** | **directory services** |
| stack | trail | alarm | directory |
|  |  | event | dc : directory connector |
|  |  |  |  |
|  |  |  |  |
| ec2 | **elasticache** | **iam** | **rds** |
| i: instance | cache : cache cluster | role | rds-pg : parameter group |
| vol : volume | cache-pg : param grp | group | rds-og : option group |
| snap : snapshot | cache-rg : replication grp | policy | rds-[type] : RDS instance |
| ami : amazon img |  |  | rds-subnet : subnet grp |
| elb : elastic load bal |  |  | es : event subscription |
| asg : auto scaling grp |  |  | dbc : cluster |
|  |  |  | dpg : cluster param grp |
|  |  |  |  |
|  |  |  |  |
| route53 | **s3** | **sns** | **sqs** |
| hc : health check | bucket | topic | queue |
| rs : record set | bp : bucket policy | tp : topic policy | qp : queue policy |
| rsg : record set group |  | queue |  |
| zone : hosted zone |  | sub : subscription |  |
|  |  | pa : platform app |  |
|  |  |  |  |
|  |  |  |  |
| vpc | |  |  |
| igw : internet gateway | rtb : route table |  |  |
| cgw : customer gateway | sg : security group |  |  |
| dopt: DHCP option set | vpce : VPC endpoint |  |  |
| nat : nat gateway | vpn : VPN connection |  |  |
| acl : network ACL | vgw : VPN gateway |  |  |
| eni : network interface |  |  |  |
|  |  |  |  |

# Monitoring

As part of your IT administration responsibilities, you are considered to be an ‘owner’ of resources created on the Amazon Cloud then you must inventory and assign a proper Classification to all resources created in the Cloud providers.

How you classify and Tag resources on the Cloud will depend on business objectives, Project objective or Platform group objectives, and the potential impact should the data be lost or compromised in case of inappropriate Tagging policy. Your resource classification and identification actions will drive into one of the following three NYL classifications.

NYL reserves the right to monitor, scan Cloud computing and storage resources creation, identification and usage and the right to stop, decommission and delete resources not in compliance with this standard. NYL will respect the privacy rights of all users and will comply with all applicable laws and government regulations when monitoring, scanning, usage of NYL Cloud computing resources.

NYL reserves the right to scan cloud computing and storage resources for appropriate identification and tracking, including but not limited to EC2 computing resources, RDS database resources, EBS and S3 storage resources. If such monitoring reveals evidence of not adequate resources identification (by using Tagging mechanism described in this policy), appropriate corrective actions will be taken, which may include:

Preventive actions:

* Preventive notification to the owner of the resource about the lack of appropriate identification

Corrective actions:

* Stop the computing resources, to prevent unnecessary costs related to the resource usage.
* Decommission computing or storage resources to prevent unnecessary costs related to the resource usage.

NYL reserves the right to immediately take corrective actions, after the preventive actions were taken and no corrective actions were taken over the resources being observed by the monitoring tools. Any device that is removed from the network cannot be reconnected until compliance is automatically detected.

## Preventive actions

Upon detecting Cloud resources not properly tagged, the automated monitoring tools will notify the owners of the resources to request the corrective actions on the resource to ensure compliance with the tagging policies described in this document. The notification will be sent by email to the Owner of the resource, to the Group mailing address of the Project owner and to the mailing group of Platform group owner. Email notification about inappropriate tagging policies to resources will be send by the end of working days. Email with notification will include details about the resource not in compliance including one or more of the following attributes:

* EC2 instance ID
* EC2 instance name
* EBS Volume ID
* EBS volume name
* S3 bucket name
* RDS Database instance ID
* RDS Database instance name

## Corrective actions

All cloud resources being marked as “Notified for correction” will continue be scanned and monitors to verify if appropriate corrective actions were taken to ensure the compliance with the tagging policy described in this document every 24 hours since the email notification to the owners. The automated monitoring tools, upon detecting that notified resources still continue having inappropriate tagging or values assigned will take corrective actions, which may include:

* Stop compute instance resources (including EC2 instances)
* Decommission compute instance resources (including EC2 instances and RDS Database instances)
* Decommission storage resources (including EC2 instances, EBS volumes, S3 buckets)

# Appendix

## Reference

Below is a link to the tagging spreadsheet where all the tags are listed.

<https://newyorklife.sharepoint.com/sites/CloudServices/Cloud%20Mgmt/Shared/Operations>