
NUTANIX
YOUR ENTERPRISE CLOUD
Smart Tag Management
for Cloud Governance

NUTANIX™
YOUR ENTERPRISE CLOUD

Industry leading analysts predict that by 2020, 80% of organizations will overshoot their cloud IaaS budgets due to a lack of cost optimization approaches. This is only one of the many governance challenges that customers may face as they embark on their cloud journey.

Governance comes from defining and enforcing policies and role management. This is where the tagging cloud resources can help, enabling automated tracking and control of policies that let cloud users meet their governance objectives.

WHAT ARE TAGS?

A tag is a label that you assign to a cloud resource. By applying tags, we add metadata to logically organize resource groups using a taxonomy. Each tag consists of a key and an optional value, both of which the user defines. In AWS and Azure, we call them 'tags,' and in GCP, they are called 'labels.' While the tagging concept is mostly the same, each cloud has its own specific rules as explained in the table below:

	AWS	Azure	Google (GCP)
Tags per resource	50	15	64
Length of key	127	512	63
Length of value	256	256	63
Case sensitive	Yes (keys and values)	No	Lowercase only

TAGGING BEST PRACTICES

To drive policy-based governance and realize optimal tag management, cloud users should follow a consistent taxonomy to ensure policy compliance and tracking can be managed programmatically. This section shares some of the best practices in tag management to meet these objectives.

Name Tags

Name tags are displayed by default on cloud consoles, and users typically use them as a point of reference to refer to a specific cloud instance or instantiation. In many cases, this key can also be used as the host name registered in DNS, Active Directory, LDAP, and Asset Management systems. Hence, it's important to adopt a standard when setting the value of the name tag so you have consistency in your cloud deployment and a single point of reference for identifying the tagged resource. We recommend that you set the name tag's value in the following compounded format:

"CloudName-ResourceType-Zone-Environment-Tier-Resource-Role-UnitNumber"

Here are a few examples:

Resource Description	Name Tag
An Azure VM resource in US East Zone, Production environment, Web server, Linux OS	Azure-VM-UE1-P-WEB-LIN-001
An AWS RDS resource in US West, Test environment database server of Oracle	RDS-UW1-T-DBA-ORA-002
An AWS Elasticache resource in Asia Pacific, Development environment, cache tier of Memcache	ECH-AN1-D-CAC-MEM-003

With this consistent taxonomy, users can easily identify the cloud, location, service used, environment, and application component or tier.

TOP TAGGING CATEGORIES AND TAXONOMY RECOMMENDATIONS

Given the limited key value pairs available for tagging, it's important to have a structured approach for tag management. This section provides guidance on key tagging categories and some of the taxonomy best practices for key value pairs.

Business Categories

The key business categories recommended for tagging are:

- Business Unit
- Cost Center
- Project
- End Customer
- Owner Contact

Some examples for business categories include:

Scenario	Key	Value
Business: Unit Name	BusinessUnit	Marketing-Dept
Business: Contact	OwnerContact	Bob|1-555-555-1212|bob@example.com
Business: Unit Billing Code	CostCenterID	USMKTG12345

TECHNICAL CATEGORIES

The key application attributes that are recommended to be tagged are:

- Application Name/ID
- Application Component
- Environment
- Version
- Tech Stack

Below are some examples for technical categories:

Scenario	Key	Value
Technical: Application Name/ID	AppID	USCRMAPP001
Technical: Application Environment	AppEnv	• Production|Business Critical|Level 1 • Dev|Alpha|Level 2 • Test|Beta1|Level
Technical: Application Tier	AppTier	• WebServer • AppServer • Cache • Search • Database

RESOURCE FUNCTION CATEGORIES

These keys allow functions to be performed on the resource-based policy defined by tags:

- Backup
- Start-Stop
- Monitoring
- Support Contact

Some examples for resource function categories are:

Scenario	Key	Value
Function: Backup	Backup	Daily
Function: Start Stop As Per Business Hours	BusinessHours	UTC8-10 (Start at UTC 0800 Hours and Stop after 10 Hours)

COMPLIANCE CATEGORIES

Tags can be used for tracking resource groups that need to be mapped to specific compliance requirements, including:

- Regulatory Compliance
- Data Encryption
- Data Confidentiality

Here are a few compliance category examples:

Scenario	Key	Value
Compliance: Data	Confidentiality	DataConf Tier1
Compliance: Regulatory	ComplianceCheck	PCI / HIPAA

How Tags Help in Governance

RESOURCE GROUPING

Tags across Business and Technical categories help create dynamic resource groups that can drive governance based on business policies.

COST ALLOCATION AND CHARGEBACK

Cloud providers allow certain tag key value pairs to be mapped to billing files. This lets users map billing reports to business groups, entities, and application workloads. Users can then use that data for internal or external chargeback purposes.

POLICY-BASED AUTOMATED GOVERNANCE

In the era of infrastructure-as-a-code (IaaS), managing cloud resources requires programmatic controls. Tags, which enable certain functions, offer another huge benefit: policy-based automated governance. Here are three use cases to show the power of tag-based governance:

Backup Use Case

Policy De inition:

Back up the resource daily, weekly, or monthly based on the tag key backup, using value to define the backup frequency.

Example:

```
# execute <script> <Daily|Weekly|Monthly>
if [[ "$1" == Daily ]]
then
   ec2-describe-instances --region ap-southeast-1 --filter "tag:Backup=Daily" |
awk '{print "Creating -> " $3; system("ec2-create-image  --region ap-
southeast-1 --name " $3 "-" $5 "-$(date +%Y-%m-%d_%Hh%Mm) --description "
$3 "-" $5 "  --no-reboot " $3)}'

     ec2-describe-images --region ap-southeast-1 | grep  `date +%Y-%m-%d
--date='$RETENTION day ago'` | awk '{print "Deregistering-> " $2; system
("ec2-deregister --region ap-southeast-1 " $2)}'  > $DEREGISTERED_AMI

   awk '{system("ec2-describe-snapshots --region ap-southeast-1 | grep " $2)}'
$DEREGISTERED_AMI > $SNAPSHOT_LIST

   awk '{print "Deleting snapshot-> " $2; system("ec2-delete-snapshot --region
ap-southeast-1 " $2)}'  $SNAPSHOT_LIST
fi
```


Start-Stop Scheduling Service Use Case

Policy De inition:
Based on the start time and stop time defined in the tag, execute a recurring service shutdown and restart schedule.

Example:

```
# execute <script> -tagKey <BusinessHours> -tagValue <UTC10-8>
-operation <start|stop>
param($tagKey, $tagValue, $operation)
'operating on VMs with tagKey : ' + $tagKey + ' and tagValue : ' + $tagValue
$vmList = Get-AzureRmVM

Foreach($vm in $vmList){
   if($vm.Tags.ContainsKey($tagKey) -AND $vm.Tags[$tagKey] -eq $tagValue){
      if($operation -eq 'start'){
         'starting VM : ' + $vm.Name + ' in resource group : ' + $vm.
ResourceGroupName
         Start-AzureRmVM -ResourceGroupName $vm.ResourceGroupName
-Name $vm.Name
      }elseif ($operation -eq 'stop') {
         'stopping VM : ' + $vm.Name + ' in resource group : ' + $vm.
ResourceGroupName
         Stop-AzureRmVM -ResourceGroupName $vm.ResourceGroupName
-Name $vm.Name
      }else {
         'Invalid operation specified. Valid operations are : start, stop'
      }
   }
}
```

Role-Based Access Control Use Case

Policy de inition:
Provide a user with specific resource access based on tag-based user validation.

Example:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
          "Effect": "Allow",
          "Action": [
          "ec2:AttachVolume",
          "ec2:DetachVolume"
     ],
     "Resource": "arn:aws:ec2:AWS-REGION-IDENTIFIER:ACCOUNT-ID-
WITHOUT-HYPHENS:volume/*",
     "Condition": {"StringEquals": {"ec2:ResourceTag/Owner":
"${aws:username}"}}
    }
  ]
}
```


One More Thing

YOU CAN'T TAG EVERYTHING, BUT TAG EVERYTHING YOU CAN!

While tagging is an effective governance strategy, it's important to know which resources can be tagged and which can't. This will help define the proper governance control across all resources.

Specific resources that can be tagged need to have a consistent framework and taxonomy to drive policy-based automated governance. Consider this ebook your user manual to make that objective a reality.

An effective tagging and monitoring strategy is an important first step towards ensuring better cloud governance, cost optimization & compliance. Try Beam today to define, configure & monitor tags for your AWS & Azure cloud environments.

START 14-DAY FREE TRIAL

NUTANIX™
YOUR ENTERPRISE CLOUD

T. 855.NUTANIX (855.688.2649) | F. 408.916.4039
info@nutanix.com | www.nutanix.com | @nutanix