Introduction to Tagging, Tag Keys and Tag Values

> ⓘ **Description**
>
> This article provides an overview of the Tagging feature including a description of what Tagging is, what Tag Keys and Tag Values represent, which roles support tagging actions, and which assets users can Tag.
>
> - Introduction to Tagging
> - Understanding Tag Keys and Tag Values
> - Tagging of Billable Cloud Assets
> - Tagging and Detailed Usage Reporting
> - Tag Details
> - Tagging Strategies and API Possibilities

Content / Solution:

Introduction to Tagging

Tagging is a CloudControl function that allows you to associate additional metadata with billable Cloud assets for grouping and reporting purposes. Tagging metadata is supported for the following billable Cloud assets:

- Network Domains
- VLANs
- Cloud Servers
- Client Images
- Sub-Administrators
- Public IP Blocks

Although Tagging metadata may be used for different scenarios, one of the main benefits of the CloudControl implementation is to correlate usage patterns with the tagging metadata. Tag metadata can be included on the Detailed Usage Report described in How to Create a Detailed Usage Report to allow you to correlate usage with specific tagging metadata. For example, if you have three departments using Cloud infrastructure in your organization, you can use the tagging feature to associate each billable asset with a given department and then use the Detailed Usage Report to identify how much of your overall usage is associated with each department's assets.

Understanding Tag Keys and Tag Values

Each tag consists of a tag "key" and a "value" associated with that key. For example, if you wanted to use the tagging feature to track billable assets by department, the "key" would be "Department" and the "value" would be the specific department. So you would tag a Cloud Server owned by Marketing with (Key=Department, Value=Marketing) and tag one owned by Finance with (Key=Department, Value=Finance). You would then correlate information about which department owns which assets by filtering your assets based on the tag metadata of the "Department" key.

Tagging is the application of a Tag Key and Tag Value to an asset. Many tagging implementations are **arbitrary** approaches that allow users to apply any Tag Key and Tag Value as metadata to an asset. The problem with such approaches is that if users use different key conventions (or if they misspell an entry), it breaks the ability to properly correlate assets as intended. Using the above example of tagging by department, if a user tags a server with (Key=Dept, Value=Finance), then filtering by Key=Department would not identify this tag. Similarly, if a user misspells their entry and tags a server with (Key=Departm*net,* Value=Finance), the same problem occurs.

To reduce the incidence of such issues, CloudControl's tagging implementation uses a **structured** approach to the key values. For each organization, either the Primary Administrator or a user with the "Tag" role must define the universe of **Tag Keys** that may be applied to billable Cloud assets. Users with these roles can choose to add, edit, or delete the universe of Tag Keys at any time.The system will allow users to tag assets only with the Tag Keys that have been defined for their organization.

Each Tag Key consists of the following:

- **Id:** This property is assigned by the system when a Tag Key is created and remains constant throughout the life of a Tag Key. API implementations should use the Id where possible.
- **Tag Key Name** (required): This property represents the Tag Key that can be used when tagging a Cloud Asset.
  - The system allows you to change the name of a Tag Key after it is created. If the Tag Key name is changed, the system updates all asset tagging using that key to conform to the new name. For example, suppose you create a Tag Key with the name of "Dept." and then begin tagging assets with (Key=Dept). You can later choose to change the Tag Key name from "Dept." to "Department". When you do so, the system will update all tagging (both current and historical) to reflect the new "Department" name.
  - This feature is why we recommend that API implementations use the **Id** field.
- **Tag Key Description** (optional): This property represents metadata used to track information regarding the Tag Key.
- **Tag Key Value Required** (True/False): Identifies whether or not the system requires a value to be assigned when an asset is tagged. Using our Department example:
  - If the Tag Key Value Required = False, the system will allow an asset to be tagged with (Tag Key="Department", and no value). In our proposed scenario where you are looking to track which department owns which asset, you would probably want to avoid this scenario.
  - If the Tag Key Value Required = True, the system requires a value be provided when the Tag Key is used. This would make the most sense for our scenario.

- Note that this value can be edited after a Tag Key is created. The value only defines whether the value is currently required. For example, suppose the value is set to False and users can tag assets with just the Tag Key. If it is later changed to True, all new tagging will require a value, but the existing tags without a value will not be allowed to remain without one.
- **Tag Key Report Display** (True/False): This property identifies whether this Tag Key should currently be displayed in the Detailed Usage Report.
  - Note that there is a **current limit of 5 Tag Keys** that can be displayed in the Detailed Usage Report at any given time. However, users with the ability to manage Tag Keys can change which Tag Keys appear on the Detailed Usage Report at any given time.

For more details on defining and managing Tag Keys, refer to the following articles:

- How to View and Manage Tag Keys for your Organization
- How to Delete a Tag Key for your Organization

Tagging of Billable Cloud Assets

Once Tag Keys have been defined, any user with the role that allows them to manage a given type of asset is allowed to tag such assets using any of the defined Tag Keys. For example, a user with the Network role is allowed to tag Network Domains while a user with the Server role is allowed to tag Servers. In addition, both the Primary Administrator and users with the Tag role are allowed to tag any type of asset. Each asset that is supported for tagging in the UI has a "Tags" item in the management menu that allows you to apply tags to the asset. You can apply up to 10 tags to an asset at any given time.

If you apply a Tag Value to an asset that is already tagged with a Tag Value, the new Tag Value will overwrite the current Tag Value. For example, if a Network Domain is currently tagged with (Key=Department, Value=Finance) and you apply (Key=Department, Value=Marketing) to it, the "Marketing" value will overwrite the "Finance" value and the asset will be considered tagged only with "Marketing". In this sense, the **Apply Tagging** function is both an "add" and an "edit" function.

Tags are tracked historically as of the time of tagging, so the system will remember which tags were applied to an asset at a given point in time.

The current UI functionality supports tagging of Network Domains, VLANs, Cloud Servers, Client Images, and Sub-Administrators in MCP 2.0 environments. Public IP Blocks can currently only be tagged using the **Apply Tags** API function. For more details, see the API 2.x documentation.

Note: You may see tags with a "~" in front of it. These are reserved for use by Operations personnel.

For additional details and step-by-step instructions on the tagging process, see How to View and Apply Tags to your Cloud Assets.

Tagging and Detailed Usage Reporting

If a Tag Key is designated to appear on the Detailed Usage Report, a new column with the title "user: <Tag Key Name>" is added to the usage report. For each row associated with an asset and tagged with such a Tag Key, the value of the Tag Key will be displayed in that column. For example, if the "Department", "Purpose", and "Organization" Tag Keys were flagged to appear on the Detailed Usage Report, it might look like this:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
							Tag Key Columns										High Performan
1	Name	UUID	Type	Location	Private IP Address	Status	user: Department	user: Purpose	user: Organiza	Start Time	End Time	Duration (Hours)	CPU Type	CPU Count	RAM (GB)	Storage (GB)	ce Storage (GB)
2	Server A	62893f28	Server	NA1	10.162.12.1	Running	Accounting			3/19/16 0:00	3/19/16 11:17	11.29	Standard	1	2	10	0
3	Server A	62893f28	Server	NA1	10.162.12.1	Running	Accounting			3/19/16 11:17	3/20/16 0:00	12.71	High Performanc	1	2	10	0
4	Server B	9945041	Server	NA1	10.162.12.1	Running	Accounting			3/19/16 3:42	3/19/16 11:18	7.61	Standard	1	2	10	0
5	Server B	9945041	Server	NA1	10.162.12.1	Stopped	Accounting			3/19/16 11:18	3/20/16 0:00	12.69	Standard	1	2	10	0
6	Customer Image A	9945041	Image	NA1		Running				3/19/16 3:30	3/19/16 9:00	5.5		0	0	10	0
7	Customer Image A	9945041	Image	NA1		Running	Accounting			3/19/16 9:00	3/19/16 9:01	0.02		0	0	10	0
8	Customer Image A	9945041	Image	NA1		Running	Accounting	Backup		3/19/16 9:01	3/19/16 9:01	0.01		0	0	10	0
9	Customer Image A	9945041	Image	NA1		Running	Accounting	Backup		3/19/16 9:01	3/20/16 0:00	14.97		0	0	10	0
10	Customer Image B	f95902e4	Image	NA1		Running	IT	Wasting Space		3/19/16 0:00	3/20/16 0:00	24		0	0	10	0
11	Customer Image B	f95902e4	Image	NA1		Running	IT	Wasting Space	~unspecified~	3/19/16 9:02	3/20/16 0:00	14.96		0	0	10	0
12	Frank Fiore	3b08a4b6	Sub-Administrator			Running	IT			3/19/16 0:00	3/20/16 0:00	24		0	0	0	0
13	Joe Guy	2184156	Sub-Administrator			Running	Accounting			3/19/16 0:00	3/20/16 0:00	24		0	0	0	0
14	MCP 1 Network	151532e	Network	NA1		Running	Accounting			3/19/16 1:39	3/20/16 0:00	22.34		0	0	0	0
15	Essentials	1047e63(	Network Domain	NA9		Running	IT	<- Tag Key Value as of the time of the row->		3/19/16 1:49	3/20/16 0:00	22.18		0	0	0	0
16	Advanced Network Domain	1bd5f922	Network Domain	NA9		Running				3/19/16 4:19	3/20/16 0:00	19.68		0	0	0	0
17	Rick's VLAN	3707680	VLAN	NA9		Running				3/19/16 4:22	3/20/16 0:00	19.63		0	0	0	0
18	testbed	88f9dc7f	Cloud Files			Running		Files		3/19/16 0:00	3/20/16 0:00	24		0	0	0	0
19	NetworkDomain: Essentials IP Block: 165.180.12.100(2)	cbdc5753	IpBlock	NA9		Reserved				3/19/16 11:47	3/20/16 0:00	12.21		0	0	0	0
20	TOTAL for 19/03/16									3/19/16 0:00	3/20/16 0:00	24		0	0	40	0

As you can see, each Tag Key is represented by a column that is populated with the Tag Value (or "~unspecified~" if the Tag Key was applied without a value) only if the asset was tagged during the period of time represented by the row. The key thing to remember is that tagging is tracked historically, so Tags are displayed on the Detailed Usage Report only on rows that represent time periods when the asset was tagged.

IMPORTANT NOTE: When using the usage report to allocate usage by Tag Key, users should be aware that aggregating the usage values provided in the rows in the Detailed Usage Report will not provide an exact match to the usage totals used for billing purposes. This is due to rounding discrepancies between the two data sources. The Detailed Usage Report provides only two digits of accuracy per column, per row. Billed usage uses a higher level of granularity, but is also rounded up to the next highest integer on a per location, per day basis across all assets in a given location.

For more details of the specifics of Tagging in reporting, see How to Create a Detailed Usage Report

Tag Details

A few additional details related to tagging:

- *Tag Key Names and Tag Values are not case-sensitive*
- Maximum number of defined Tag Keys per organization: 1000 at one time
- Maximum number of tags per Cloud Resource: 10 at one time
- Maximum Tag Key name length: 128 Unicode characters in UTF-8

- Maximum Tag Value length: 255 Unicode characters in UTF-8
- The system supports tagging of Cloud Servers, Client Images, Public IP Blocks, and Sub-Administrators in MCP 1.0 locations. However, Cloud Networks (which are billable assets in MCP 1.0) are not supported.
- When managing Tag Keys (Create, Edit, Delete) through the Cloud API, all calls must be made against the Home Geographic Region API endpoint. For more details, see Introduction to Geographic Regions.
    - Related to this, note that such actions are pushed asynchronously from the Home Geographic Region to any other enabled "Shadow" Geographic Region

Tagging Strategies and API Possibilities

- A tagging strategy should be planned in advance with a standard applied to the Tag Key naming. The global sharing of Tags should help in ensuring consistency, but care should be taken to ensure that tags with duplicate purpose do not exist. Tags should be initially categorized between those that are of interest for reporting and those that are not. Although using a greater number of tags can be a good idea, the creation of new tags should be a carefully planned activity. A tagging strategy should be documented, communicated widely and maintained.
- Users can store any and all data (subject to length limitations) about resources in the knowledge that it is always available in one place (unless the tag is deleted) and that there is a historical record of changes. Examples might include a change in, Version, Owner, Purpose, Department or Cost Center. The inclusion of external identifiers such as Asset ID, or Cost Center will enable external systems and reports to be cross-correlated. Some high-level categories to consider might include: Business, Functional, Technical, Automation, Security, Governance, Compliance, Configuration and External Systems.
- CloudControl does not make any presumptions about the usage of tagging, which enables users to come up with innovative and novel uses for tagging to help customize the platform for their own use.
- As an alternative to using multiple Tag Keys with different tag values, namespaces can be included to augment the meaning of tags. Examples might include tags that are created and managed by different departments, the following example shows how tags can be owned and managed by different departments for the same purpose as indicated by their prefix:
    - **Ops:**owner=JHancock
    - **Dev:**owner=SSmith
    - **Sales:**owner=JDoe
    - **Sales:**purpose=demo
    - **Sales:**CostCenter=AB123456
- When working with Tags programmatically through the API:
    - Using Tags as the single point of truth concept can be very powerful since Tags can serve the purpose of coordinating activities between external systems. The risks associated with race conditions should be considered carefully, but tags may be used to acquire and release locks on resources and otherwise build over the top services.
    - A short JSON message could be encoded as a value in place of a simple string, this allows a lot of data to be encoded in a single tag if desired.
        - **Ops:automatedConfig**={"publicIP": "1.2.3.4","externallyManaged": "true","tomcat": "6", "mySQl": "5.5","firewall": {"ports": "80,443,21"}}
- Grouping of resources can be leveraged to help find the correct resource, or resources involved in a common activity, this can help in administration for activities such as maintenance, monitoring deploying and deleting complex multi tier systems and supporting infrastructure.
- In addition to static data, state transitions can be flagged, changes in purpose and capabilities, maintenance activities, bringing resources in or out of service.
- Advanced use cases for tagging can be extended to include manual and eventually automated configuration management. Cloud Control tagging can essentially operate as a configuration repository. Resources can be tagged as being externally managed and automated systems can operate on the data that is encountered, dates and times for starting and stopping or other automated activities

Recently Updated

- Introduction to Tagging, Tag Keys and Tag Values
- New Features by Release
- Introduction to Usage Reporting
- How to Manage a Cloud Server
- Introduction to OS Units