VERITAS The truth in information.

Technical Brief – Information Map

Veritas Information Map Support for Amazon S3

Veritas Information Map Support for Amazon S3

Feature Description

Veritas Information Map initially only supported metadata collection from Veritas NetBackup catalogs. With the May 2017 update, Veritas Information Map now can collect metadata from Amazon S3.

Integrating Information Map with Amazon S3 is a relatively simple, straight forward process. Customers will not need to configure an on-premise agent as everything is performed in the cloud. The customer will only need to grant the Veritas Information Map Amazon S3 permissions to view metadata stored within their Amazon S3 environment.

Business Value

Customers are looking for ways to migrate their unstructured content from on-premise configurations to cloud solutions in order to cut costs associated with storage management. One popular cloud storage solution is Amazon S3.

Recent studies have shown that 73% of Amazon S3 customers have over 500TB of unstructured information stored in the cloud. As more and more information is added, it is more difficult to determine what information is valuable and worth keeping in the cloud. There could be information stored in Amazon S3 that does not adhere to an organization's storage policies or there could be personally identifiable information than an organization may need to delete to comply with regulations such as GDPR.

There are not many tools available to today that allow Amazon S3 customers to visualize the content that they have stored. Information Map now provides this capability.

Underlying Principles

The method for Information Map collecting metadata on information stored in Amazon S3 is a relatively straight forward process. Customers will not need to configure an on-premise agent as all metadata collection is performed and managed in the cloud.

When customers log into their Information Map environment and navigate to the **Administration → Agents** section, they will notice that there is an agent called "Veritas Cloud Agent" as shown in Figure 1. This agent is responsible for all metadata collection from Amazon S3. Customers will need to create security policies and roles using the Amazon Web Services console in order to grant Information Map the necessary permissions to collect metadata.

Veritas Information Map Support for Amazon S3

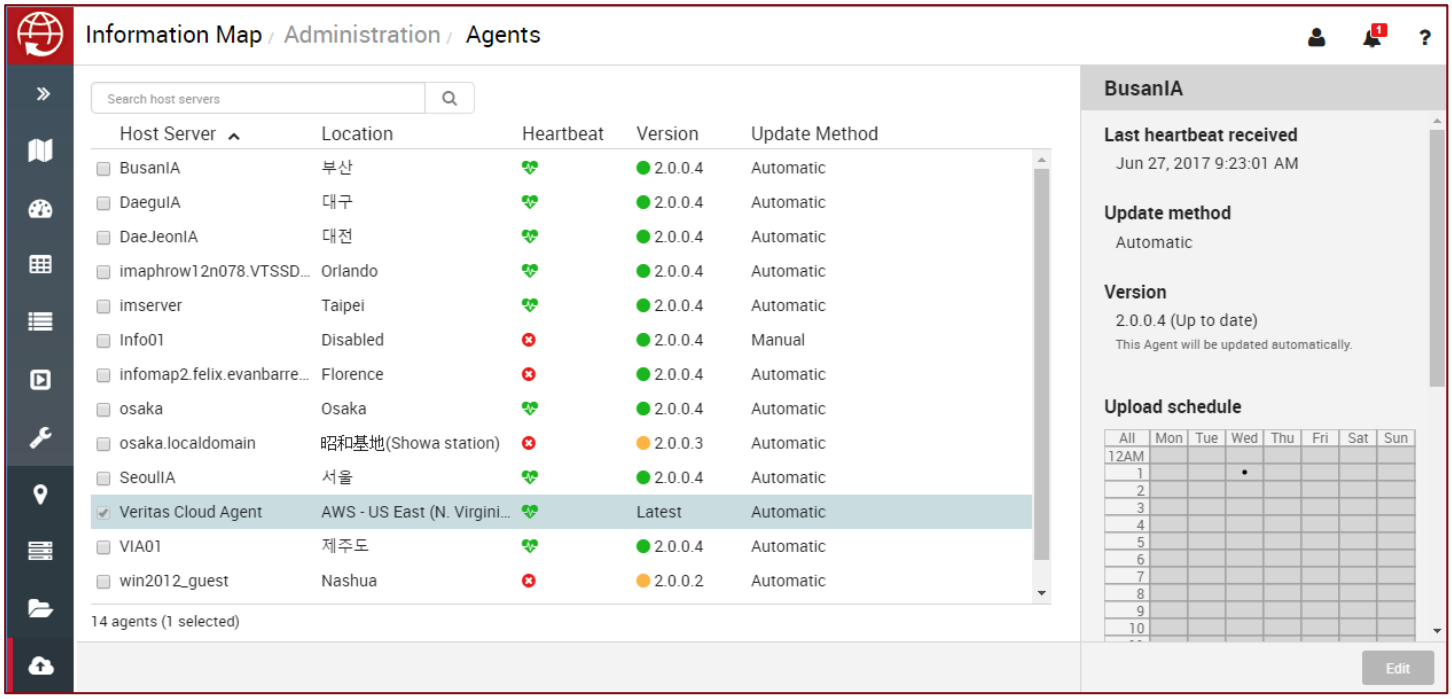

Figure 1 – The Veritas Cloud Agent

Once permissions have been granted in Amazon Web Services, the customer will need to create a new Information Map Task. Once the task has been created, Information Map will begin to collect metadata from Amazon S3. The information shown in Information Map will be updated within 24 hours.

Information Map Users can quickly filter information stored in Amazon S3 by using one of the following methods:

- Filter by location – AWS locations will show up as unique locations such as “AWS – US East”
- Filter by Data Stores – A new filter option for Information Map that allows users to filter data by selecting “Amazon S3”
- Data Stores List View – By using List View in the Information Map bar, users can click on Data Stores. This will separate out data that is stored on on-premise storage or Amazon S3

Similar to NetBackup content, Amazon S3 content can be exported using any of the options available in Information Map such as exporting to CSV and Screen and List Capture.

Guided Tour

Creating an AWS Policy

The first step in granting Information Map the necessary permissions to view metadata in Amazon S3 is to create a Policy. Once logged into the AWS console, navigate to **IAM → Policies**. Click on **Create Policy**.

Next, the administrator would select “Create Your Own Policy” as shown in Figure 2.

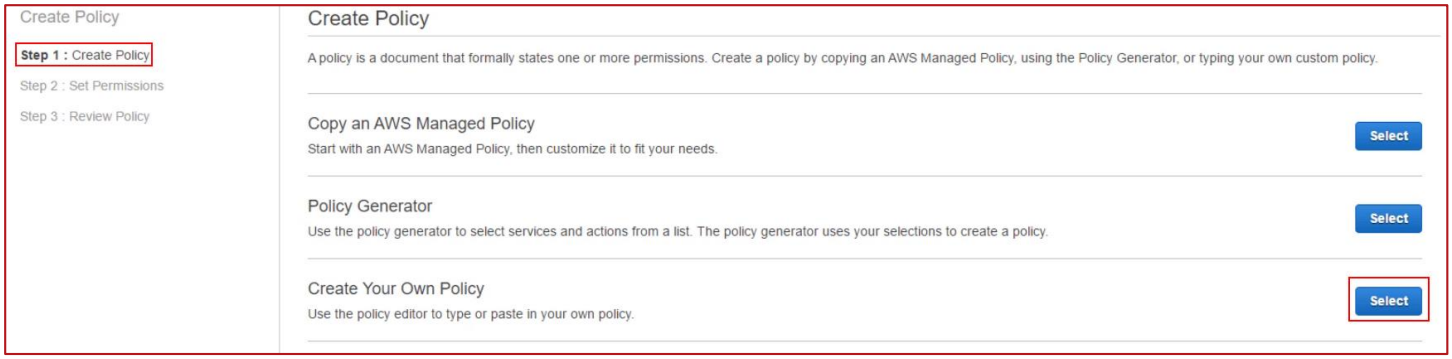

Figure 2 – Creating an AWS Policy

Provide a policy name such as "Veritas-S3-Connector". Provide a description. The policy document defines the permissions for bucket access. The following Policy Document example allows Information Map to have the necessary permissions across all defined buckets in Amazon S3:

```
{

      "Version": "2012-10-17",
      "Statement": [
      {
            "Effect": "Allow",
            "Action": [
                  "s3:ListAllMyBuckets",
                  "s3:GetBucketLocation",
                  "s3:ListBucket"
            ],
            "Resource": [
                  "arn:aws:s3:::*"
            ]
      }
      ]
}
```

Figure 3 shows an example of how to configure the policy.

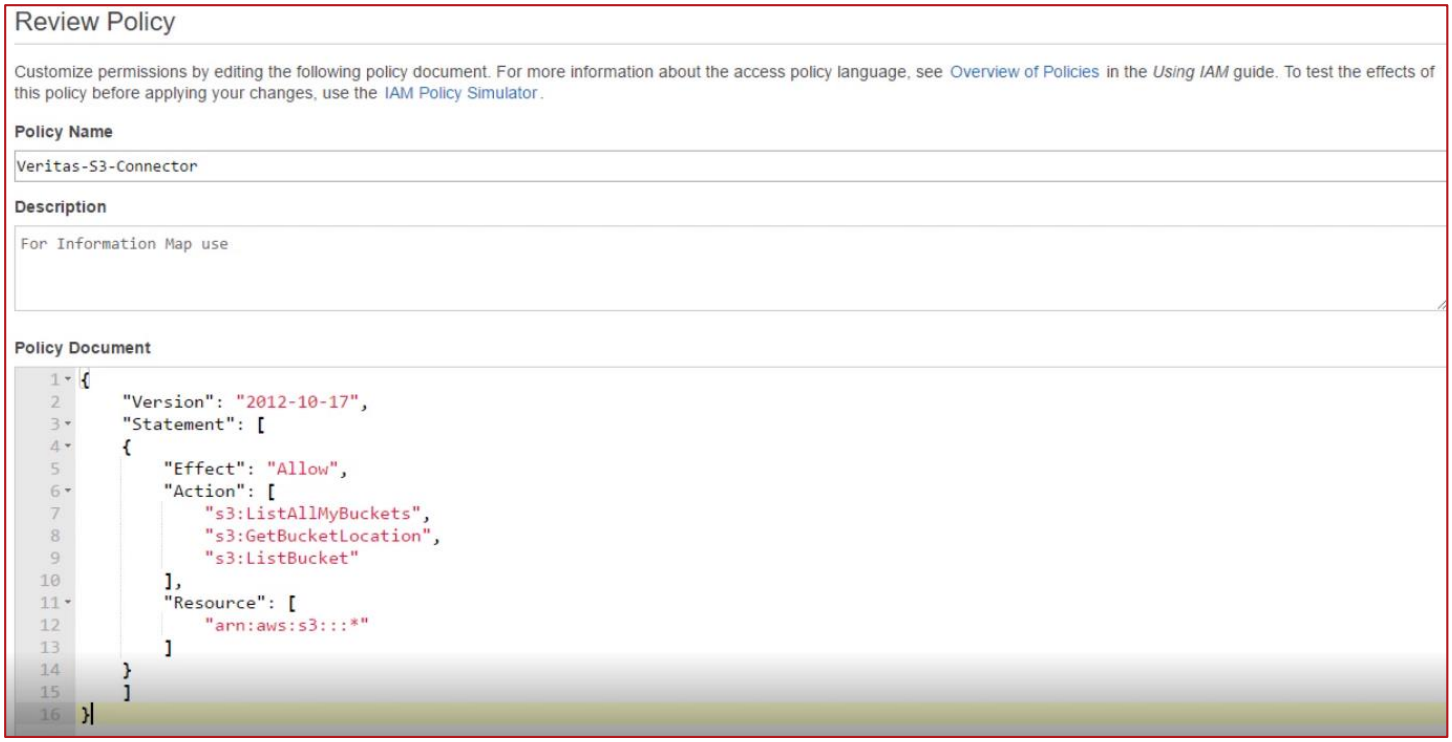

Figure 3 – Configuring the AWS Policy document

Click on **Create Policy** to finish this process.

Creating an AWS Role

Once the policy has been created, a role can now be created. In the AWS console, click on **Roles**. Click on Cr**eate new role**. The role type should be **Role for cross-account access** and **Provide access between your AWS account and a 3rd party AWS account**. The details for the trust should be the following:

- Account ID – **071997631119** ← This is the AWS account number for Veritas Information Map
- External ID – This ID should match the name of the previously configured AWS Policy (such as **Veritas-S3-Connector**)
- Require MFA – Unchecked

After configuring the trust portion, attach the previously configured policy ("Veritas-S3-Connector").

Lastly, provide a role name and description:

- Role name – Must be set to ***VeritasInformationMapS3Connector***
- Role description – optional

Finish by **clicking** on Create role.

Once the role has been created, bring up its properties by clicking on it. Record the Role ARN as this will be needed to create a task in Information Map. Figure 4 shows where to find the Role ARN.

Figure 4 – Recording the Role ARN

Creating a Task for Amazon S3 in Information Map

A user must have the "Information Map configuration" right in order to create a task in Information Map. Once logged in, navigate to **Administration → Tasks**.

Click on New to create a new task. Fill the properties for new Task:

- Task Type – **Amazon S3 Collection**
- Display Name – Unique name for the task
- External ID – This ID needs to match the policy ID created in the AWS Console such as "Veritas-S3-Connector" (as shown in Figure 3)
- Role ARN – The ARN is generated when the role is created using the AWS Console

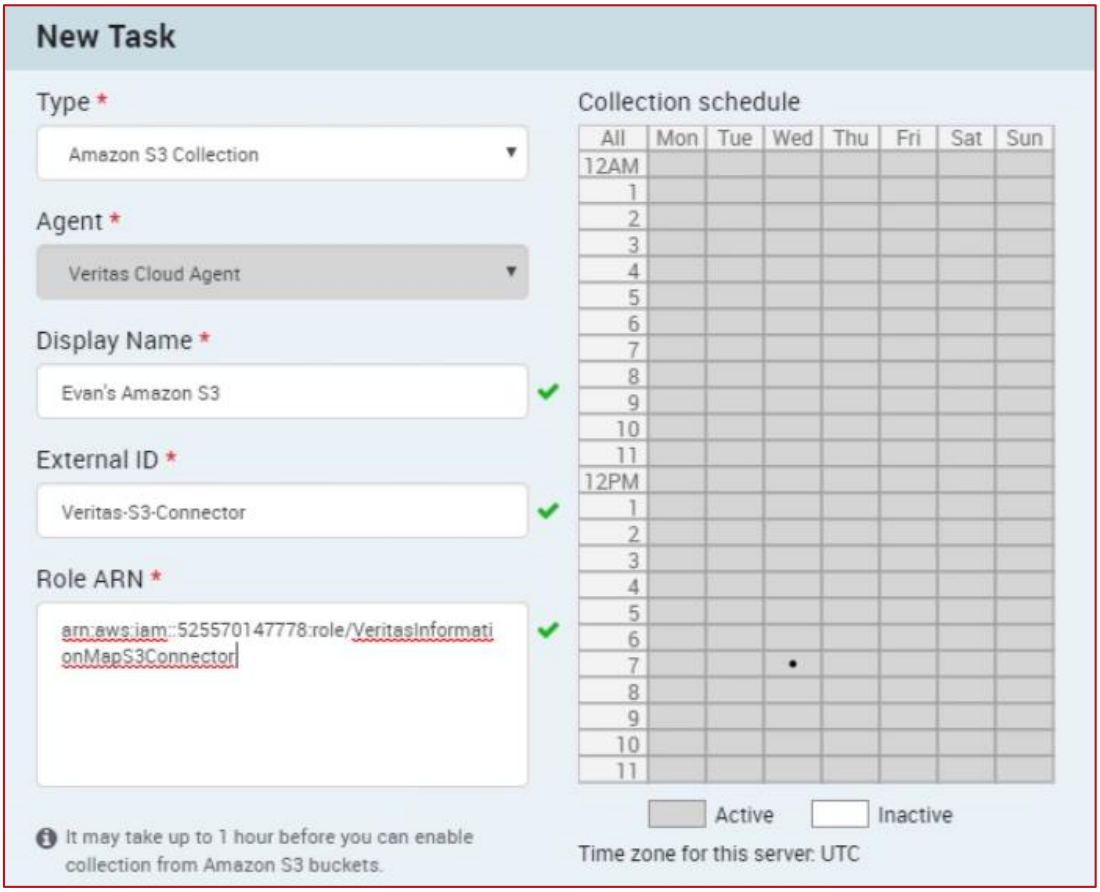

Figure 5 – Creating a task for Amazon S3

Licensing and Support Considerations

Licensing for Information Map and Amazon S3 integration is based upon a frontend terabyte (FETB) model.

Veritas Information Map Support for Amazon S3

About Veritas Technologies LLC. Veritas Technologies LLC enables organizations to harness the power of their information, with solutions designed to serve the world's largest and most complex heterogeneous environments. Veritas works with 86 percent of Fortune 500 companies today, improving data availability and revealing insights to drive competitive advantage.

Visit our website
http://www.veritas.com

Veritas World Headquarters
500 East Middlefield Road
Mountain View, CA 94043
+1 (650) 933 1000
www.veritas.com