**Automated Installation of Tanium, Qualys and Splunk Agents using AWS SSM**

|  |  |
| --- | --- |
| Document Owner | |
| Author | Position / Responsibility |
| Shambo Basu | App/Cloud Support Specialist |
|  |  |

|  |  |  |
| --- | --- | --- |
| Document Reviewer | | |
| Name | Title / Role | Signature |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

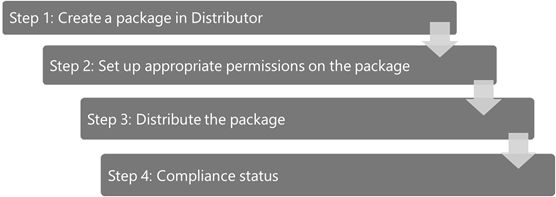
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | Document Version Revisions | | |
| Date | Version | | Editor | Signature |
| 12/2/2021 | 1.0 | | Shambo Basu |  |
|  |  | |  |  |
|  |  | |  |  |

|  |  |  |
| --- | --- | --- |
| Document Approver | | |
| Name | Title / Role | Signature |
|  |  |  |
|  |  |  |
|  |  |  |

**Introduction**

AWS Systems Manager Distributor automates the process of packaging and publishing software to managed Windows and Linux instances across AWS.

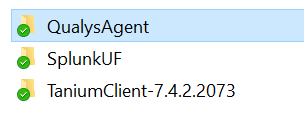
The typical process for distributing the software packages to EC2 using Systems Manager Distributor involves the following steps.



**Step 1: Create a package in Distributor**

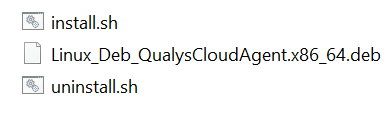
These are the steps for creating a package in Distributor and should be followed for all agent packages individually:

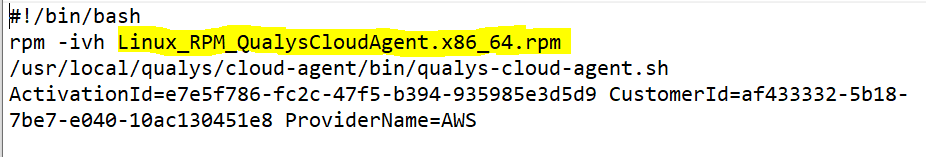
1. Prepare the compressed zip folders of the Datadog agent
2. Upload the zip files to an Amazon S3 bucket
3. Prepare the manifest file
4. Create the package in the AWS Systems Manager Distributor console
5. You can find the Distributor packages attached here. Extract the attached zip and you will find folders which has been packaged and is ready to be uploaded to the S3 bucket.



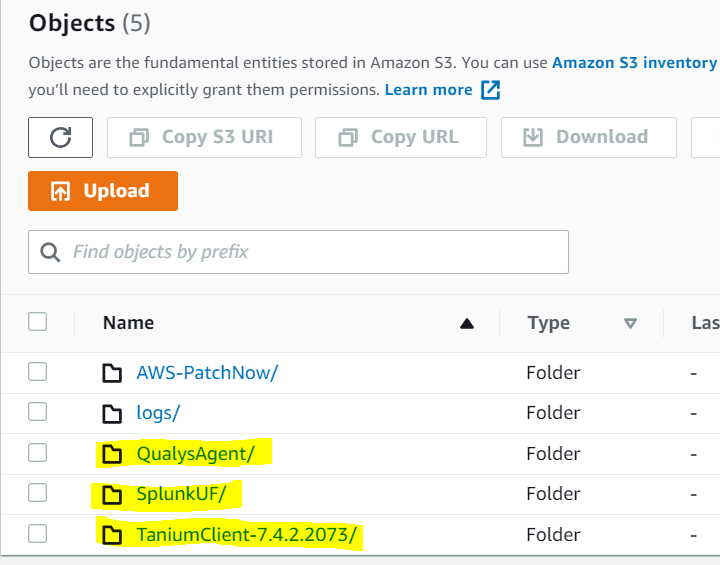
**Modifying zips with updated agents or scripts**

The distributor package contains scripts for installation of agents. You need to change the file name of the agent installer in the install.sh for Linux packages and install.ps1 for Windows packages.





1. Create a S3 bucket named **cf-security-software-repo-<SITE ID>** and upload all the folders from the extracted zip. Do replace SITE ID with actual Site ID.



1. **Manifest.json is already prepared for you and is included within the zip which will work out of the box.** In case you make any changes to the zip packages for each agent, you need to update the manifest file with correct zip package name and need to update the checksum value.

*As an additional security measure to protect the integrity of the files, the checksum value of the zip file is verified during the package installation process. The checksum value is captured in the package manifest file during the package creation. After you create the zip file with the agent packages, you can calculate the SHA256 checksum of the file zip. On a Windows system, you can use the following PowerShell command.*

*Get-FileHash -Algorithm SHA256 datadog-windows\_6.zip*

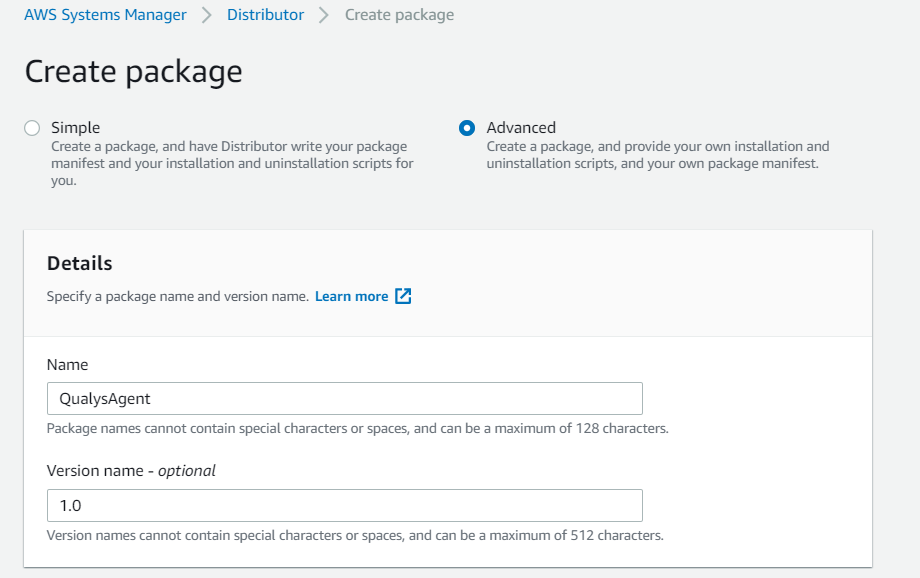
**Above step is required only if you modify any of the provided zips, else this step can be ignored.**

Manifest should look like below screenshot:

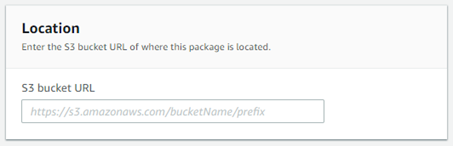


1. **Create the package in AWS Systems Manager console**

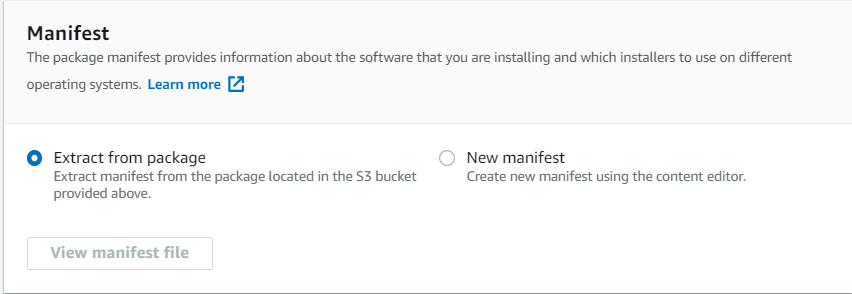
Navigate to the Distributor page in AWS Systems Manager console and create the package. Select Advanced. Provide the name of the package and a version associated with the package.



Enter the S3 bucket url where you uploaded the package earlier.



Choose Extract from package in the Manifest section and paste the contents of the manifest file that you prepared earlier.

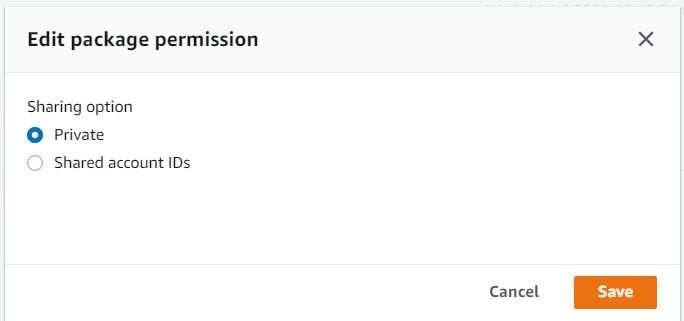


Choose Create package button to create the Datadog package after completing all the above mentioned steps. Upon successful creation of the package, the package gets listed on the Distributor main page.

**Step 2: Set up appropriate permissions on the package**

By default, all packages are set to Private, meaning only those with access to the package creator’s AWS account can view package information, update or delete the package and distribute it.

In our case the packages should be Private.

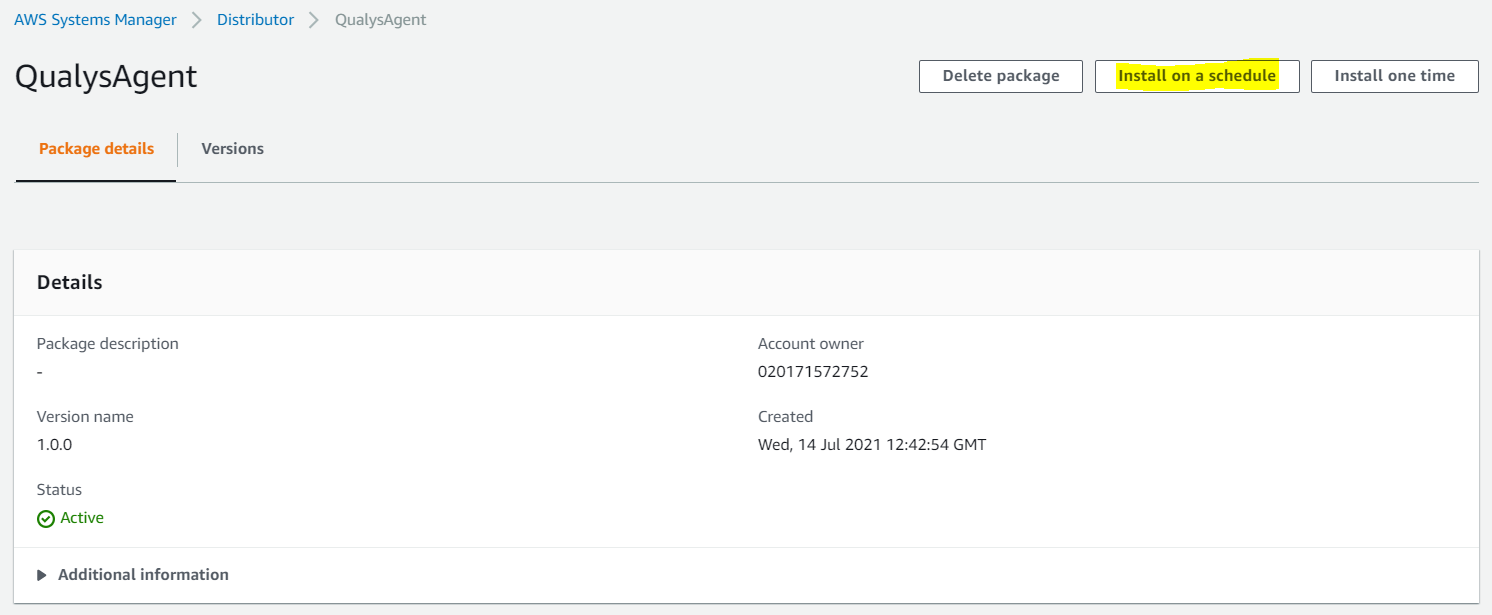


**Step 3: Distribute the package**

The following preparation steps are required before you can distribute the package to the target instances.

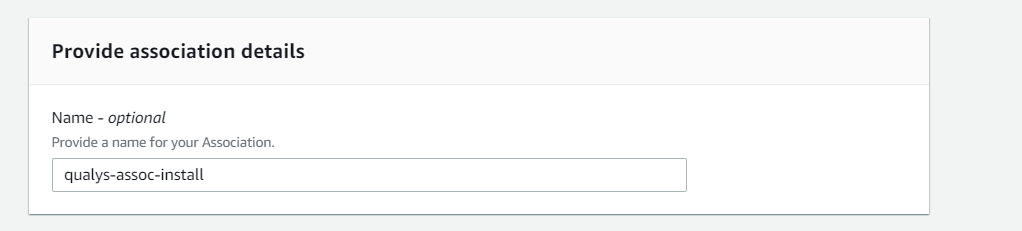
* Ensure that the version of the Systems Manager agent running on the instances is 2.3.274.0 or later. To ensure the latest version of the Systems Manager agent is installed, run the AWS-UpdateSSMAgent document on all the targeted instances.

After your readiness is complete, you are ready to distribute the Datadog package. In the Systems Manager console, navigate to the QualysAgent package in the Distributor and select Install on schedule.

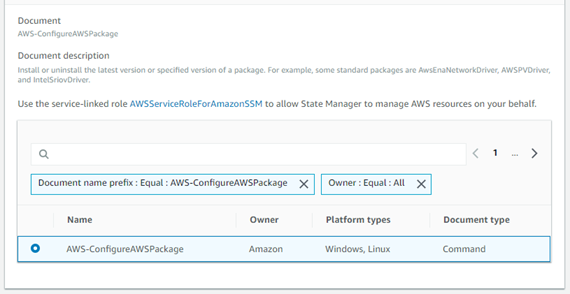


Install on schedule

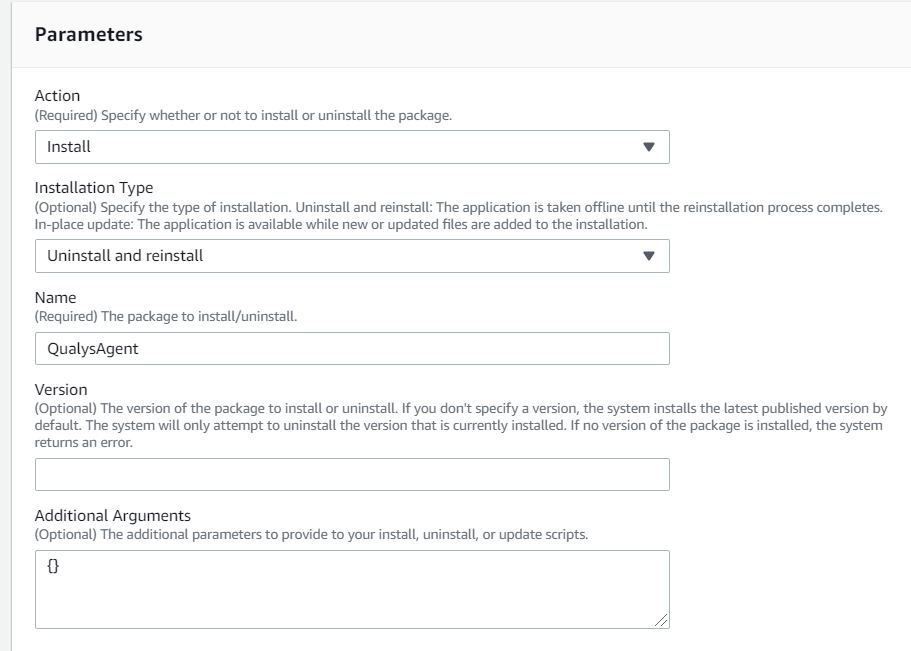
When you choose Install on schedule, the State Manager Create Association page opens. Provide an appropriate name for the association.



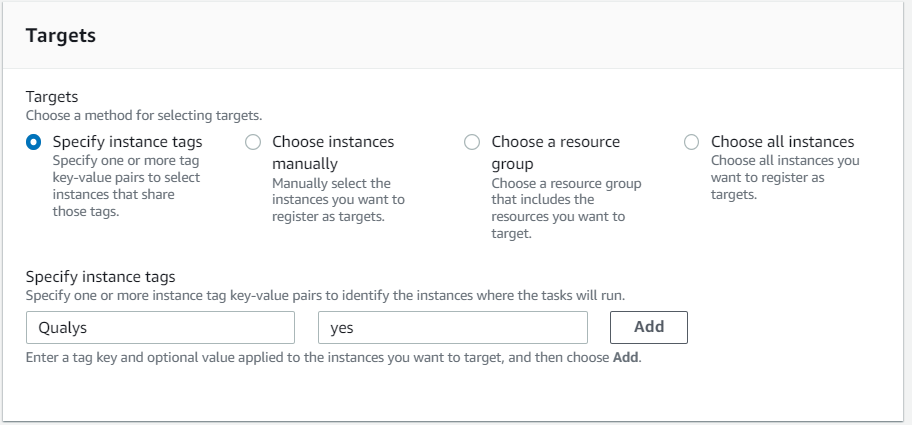
The Document section includes the ‘*AWS-ConfigureAWSPackage*’ document by default.



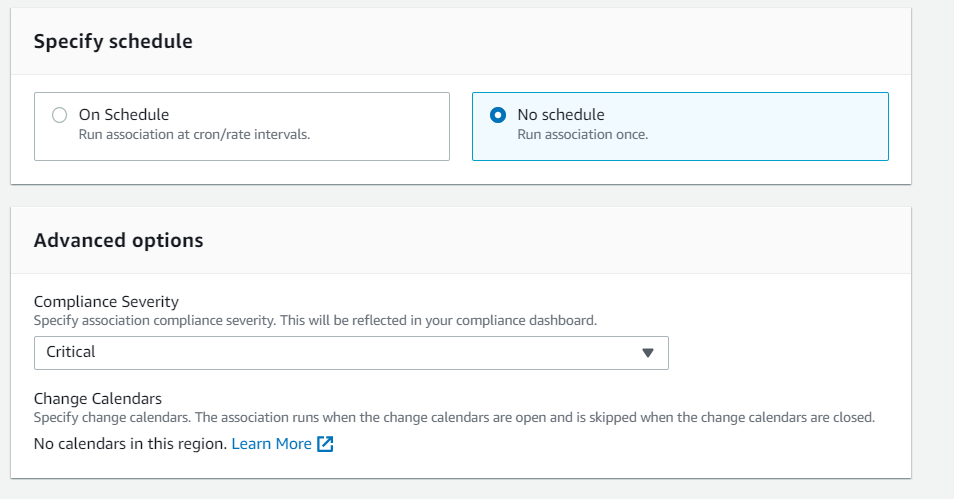
In Parameters, Action is set to the default, Install. Name defaults to the package name. In the Version field, by default, the latest published version of the package is picked up for installation when the version field is left blank. Alternately, you can choose a specific version of the package to be installed.



In the Targets section, choose the instances either through a tag or by manually selecting the instances.



In the Specify schedule section, choose the schedule for running the association.

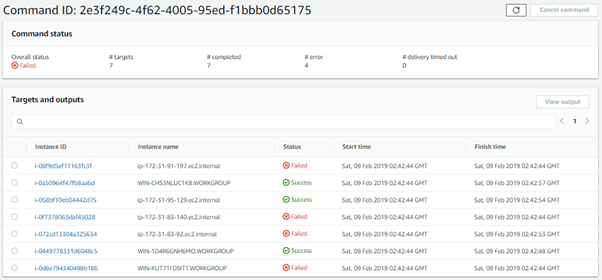


Optionally, in Advanced options, choose the Compliance severity, specify the Concurrency and Error Threshold in the Rate Control pane and Write to S3 in the Output Options window. Choose Create Association to kick-start the package distribution on schedule.

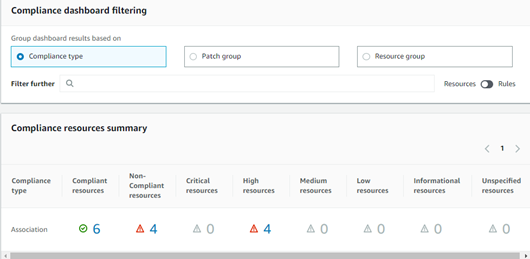
**Follow the above-mentioned steps for installation of all agents, Tanium and Splunk.**

**Step 4: Compliance Status**

You can review the distribution status of the Qualys agent through the Run Command command history if the package is distributed using Install one time. You can review status in the State Manager association status if the package is distributed using the Install on schedule option.



If you used State Manager, you can also see the status of your package distribution through the Compliance console. The following screenshot shows the compliance summary.

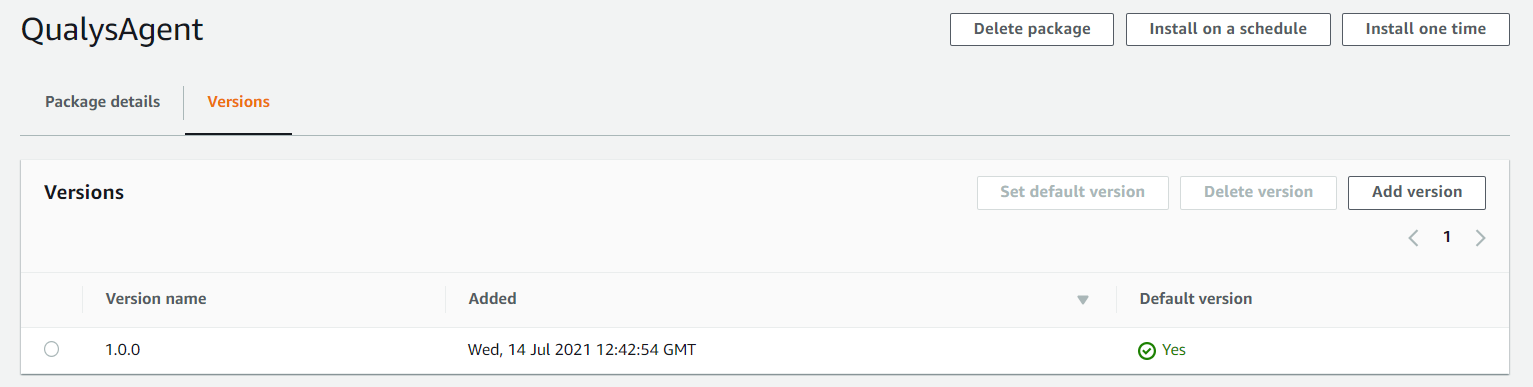


**Managing Package Versions**

Managing changes and updates is part of the lifecycle of any software package. AWS Systems Manager Distributor provides the ability to manage this process.

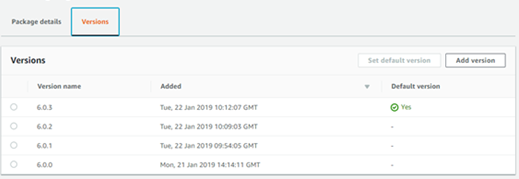
If you want to make any changes to a package, like updating the version of the Qualys, Tanium and Splunk agent, adding support for a new operating system, or modifying the install or uninstall scripts, you can add a new version of the package. Once you’ve done that, both the old and new versions are available to install or uninstall on your instances.

To create a new version of Qualys, Tanium and Splunk Distributor package, navigate to the Agent package in the Distributor, and on the Versions tab, choose Add version.



This opens the package version page with the Version name, S3 Bucket URL, and the Manifest file fields to capture the new package version specifics.

After you provide the details, choose Add version to add a new version to the package. The new version will appear in the Versions tab of the agent package.



Although all versions are available for you to distribute, you can mark one version as the default so that you can easily keep all of your instances up to date. To make a specific version the default, select the version of the package and choose the Set default version option. If you need to do a rollback, you’ll follow the same process of selecting a specific older version and distributing it, which will override the newer version on the managed instances.

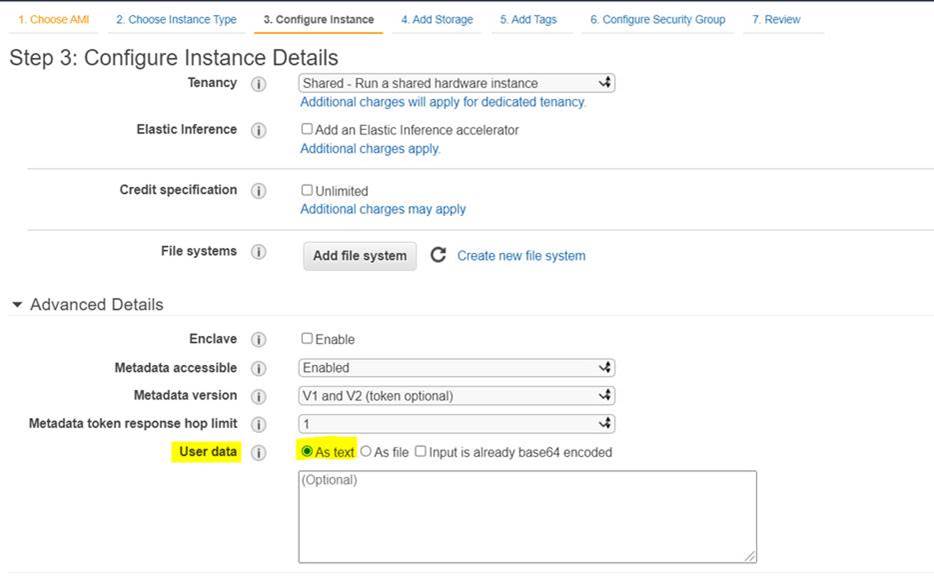
**Tagging instances and installing SSM agent during provisioning**

Manual installation of Tanium, Qualys and Splunk agents will not be required going forward on EC2 instances. You can now simply assign tags to VMs which needs these agents installed and this can be done right after instance provisioning or during launch.



As mentioned in Step 3 there is a pre-requisite to install SSM agent on all the EC2 instances, this can be done while launching of an instance using the user data. To do so, please find the steps below:

1. User data can be found under the Advanced Details section in Step 3 of launching an instance as shown in screenshot below.



2. Add below command to install SSM agent from user data.

**Amazon Linux 2, RHEL 7, and CentOS 7 (64 bit)**

#!/bin/bash

cd /tmp

sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux\_amd64/amazon-ssm-agent.rpm

sudo systemctl enable amazon-ssm-agent

sudo systemctl start amazon-ssm-agent

**RHEL 8 (64 bit)**

#!/bin/bash

cd /tmp

sudo dnf install python3

sudo dnf install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux\_amd64/amazon-ssm-agent.rpm

sudo systemctl enable amazon-ssm-agent

sudo systemctl start amazon-ssm-agent

**Amazon Linux, CentOS 6 (64 bit)**

#!/bin/bash

cd /tmp

sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux\_amd64/amazon-ssm-agent.rpm

sudo start amazon-ssm-agent

**Ubuntu 20.04 (64 bit)**

#!/bin/bash

mkdir /tmp/ssm

cd /tmp/ssm

wget https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/debian\_amd64/amazon-ssm-agent.deb

sudo dpkg -i amazon-ssm-agent.deb

sudo systemctl enable amazon-ssm-agent

**Windows (64 bit)**

At this point we cannot use user data; this is work in progress. You can manually login and install SSM agent.

Note: Operating Systems listed above are the ones currently supported by the SSM packages for Tanium, Qualys and Splunk. For other OSes please install T/Q/S manually.

Above commands can be used on running VMs also to install SSM.

3. Assign Instance IAM Role to the VM so that SSM agent can trigger installation

To create an IAM role using the IAM console

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose Roles, Create role.
3. On the Select role type page, choose EC2 and the EC2 use case. Choose Next: Permissions.
4. On the Attach permissions policy page, click on Create Policy.
5. On the Create Policy page or tab, change from visual editor to JSON and paste below code. Do replace the SITE ID in the below json policy.

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": [

"cloudwatch:PutMetricData",

"ds:CreateComputer",

"ds:DescribeDirectories",

"ec2:DescribeInstanceStatus",

"logs:\*",

"ssm:\*",

"ec2messages:\*"

],

"Resource": "\*"

},

{

"Effect": "Allow",

"Action": "iam:CreateServiceLinkedRole",

"Resource": "arn:aws:iam::\*:role/aws-service-role/ssm.amazonaws.com/AWSServiceRoleForAmazonSSM\*",

"Condition": {

"StringLike": {

"iam:AWSServiceName": "ssm.amazonaws.com"

}

}

},

{

"Action": [

"s3:PutObject",

"s3:GetObject",

"s3:GetEncryptionConfiguration",

"s3:PutObjectAcl",

"s3:Get\*",

"s3:List\*"

],

"Resource": [

"arn:aws:s3:::cf-security-software-repo-<SITE ID>/\*",

"arn:aws:s3:::cf-security-software-repo-<SITE ID>"

],

"Effect": "Allow"

},

{

"Effect": "Allow",

"Action": [

"iam:DeleteServiceLinkedRole",

"iam:GetServiceLinkedRoleDeletionStatus"

],

"Resource": "arn:aws:iam::\*:role/aws-service-role/ssm.amazonaws.com/AWSServiceRoleForAmazonSSM\*"

},

{

"Effect": "Allow",

"Action": [

"ssmmessages:CreateControlChannel",

"ssmmessages:CreateDataChannel",

"ssmmessages:OpenControlChannel",

"ssmmessages:OpenDataChannel"

],

"Resource": "\*"

}

]

}

Then click Next: Tags and then again click on Next: Review. On the Policy Review page provide name for policy “ssm-distributor-policy” and click on Create Policy.

1. On the Review page, enter a name for the role “cf-ssm-instance-role” and choose Create role.

Once the creation of the IAM "Instance Role" for EC2 instance has been completed you can assign it

to the Instance.

To attach an IAM role to an instance

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, choose Instances.
3. Select the instance, choose Actions, Security, Modify IAM role.
4. Select the IAM role to attach to your instance and choose Save.

**PLEASE NOTE:** An EC2 instance can only have ONE IAM role assigned.

If your Instance already has an attached IAM role, you must modify the existing IAM role adding

necessary access to SSM service. Please follow AWS documentation for details

(<https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-instance-profile.html>)