**Updating Custom Software Deployed**

**It is categorized in 5 steps:**

**1)Device Update Agent Provisioning**

1.1)Prerequisites

If you're setting up the IoT device/IoT Edge device for package based updates, add packages.microsoft.com to your machine’s repositories by following these steps:

a)Log onto the machine or IoT device on which you intend to install the Device Update agent.

b)Open a Terminal window.

c)Install the repository configuration that matches your device’s operating system.

curl https://packages.microsoft.com/config/ubuntu/18.04/multiarch/prod.list > ./microsoft-prod.list

d)Copy the generated list to the sources.list.d directory.

sudo cp ./microsoft-prod.list /etc/apt/sources.list.d/

e)Install the Microsoft GPG public key.

curl https://packages.microsoft.com/keys/microsoft.asc | gpg --dearmor > microsoft.gpg

sudo cp ./microsoft.gpg /etc/apt/trusted.gpg.d/

1.2)How to provision the Device Update agent as a Module Identity:

a)On IoT Edge enabled devices:

-Install and provision the Azure IoT Edge runtime.

-Install the Device Update image update agent.

-Install the Device Update package update agent.

sudo apt-get update

sudo apt-get install deviceupdate-agent deliveryoptimization-plugin-apt

-You are now ready to start the Device Update agent on your IoT Edge device.

1.3)How to start the Device Update Agent:

-Log into the machine or device that has the Device Update agent installed.

-Open a Terminal window, and enter the command below.

sudo systemctl restart adu-agent

-You can check the status of the agent using the command below.

sudo systemctl status adu-agent

-You should see status OK.

-On the IoT Hub portal, go to IoT device or IoT Edge devices to find the device that you configured with Device Update agent. There you will see the Device Update agent running as a module.

**2)Create an Update Device Account**

2.1)Go to Azure Portal.

-Marketplace.

-Click Create a Resource and search for "Device Update for IoT Hub"

-Click Create -> Device Update for IoT Hub

-Specify the Azure Subscription to be associated with your Device Update Account and Resource Group

-Specify a Name and Location for your Device Update Account

-Click "Next: Review + create>"

-You will see the deployment status change to "complete" in a few minutes. Click "Go to resource"

2.2)Create a device update instance

An instance of Device Update is associated with a single IoT hub. Select the IoT hub that will be used with Device Update. We will create a new Shared Access policy during this step to ensure Device Update uses only the required permissions to work with IoT Hub (registry write and service connect). This policy ensures that access is only limited to Device Update.

To create a Device Update instance after an account has been created.

-Once you are in your newly created account resource, go to the Instance Management "Instances" blade

-Click "Create and specify an instance name and select your IoT Hub

-Click "Create". You will see the instance in a "Creating" state.

-Allow 5-10 mins for the instance deployment to complete. Refresh the status till you see the "Provisioning State" turn to "Succeeded".

2.3)Configure IoT Hub

In order for Device Update to receive change notifications from IoT Hub, Device Update integrates with the "Built-In" Event Hub. Clicking the "Configure IoT Hub" button configures the required message routes and access policy required to communicate with IoT devices.

To configure IoT Hub

-Once the Instance "Provisioning State" turns to "Succeeded", select the instance in the Instance Management blade. Click "Configure IoT Hub"

-Select "I agree to make these changes"

-Click "Update"

2.4)Configure access control roles

In order for other users to have access to Device Update, users must be granted access to this resource.

-Go to Access control (IAM) within the Device Update account

-Click "Add role assignments"

-Under "Select a Role", select a Device Update role from the given options

Device Update Administrator

Device Update Reader

Device Update Content Administrator

Device Update Content Reader

Device Update Deployments Administrator

Device Update Deployments Reader

-Assign access to a user or Azure AD group

-Click Save

-You are now ready to use the Device Update experience from within your IoT Hub

**3)Add an update to Device Update for IoT Hub**

3.1)Prerequisites

-Access to an IoT Hub with Device Update for IoT Hub enabled.

-An IoT device (or simulator) provisioned for Device Update within IoT Hub.

-PowerShell 5 or later (includes Linux, macOS and Windows installs)

-Supported browsers:

Microsoft Edge

Google Chrome

3.2)Create a Device Update import manifest

-Ensure that your update file(s) are located in a directory accessible from PowerShell.

-Create a text file named AduUpdate.psm1 in the directory where your update image file or APT Manifest file is located. Then open the AduUpdate.psm1 PowerShell cmdlet, copy the contents to your text file, and then save the text file.

-In PowerShell, navigate to the directory where you created your PowerShell cmdlet from step 2. Use the Copy option below and then paste into PowerShell to run the commands:

Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope Process

Import-Module .\AduUpdate.psm1

-Run the following commands by replacing the sample parameter values to generate an import manifest, a JSON file that describes the update:

$compat = New-AduUpdateCompatibility -DeviceManufacturer 'deviceManufacturer' -DeviceModel 'deviceModel'

$importManifest = New-AduImportManifest -Provider 'updateProvider' -Name 'updateName' -Version 'updateVersion' `

-UpdateType 'updateType' -InstalledCriteria 'installedCriteria' `

-Compatibility $compat -Files 'updateFilePath(s)'

$importManifest | Out-File '.\importManifest.json' -Encoding UTF8

-Review the generated import manifest

3.3)Import an update

-Log in to the Azure portal and navigate to your IoT Hub with Device Update.

-On the left-hand side of the page, select "Device Updates" under "Automatic Device Management".

-Across the top of the screen. Select the Updates tab.

-Select "+ Import New Update" below the "Ready to Deploy" header.

-Select the folder icon or text box under "Select an Import Manifest File". You will see a file picker dialog. Select the Import Manifest you created previously using the PowerShell cmdlet. Next, select the folder icon or text box under "Select one or more update files". You will see a file picker dialog. Select your update file(s).

-Select the folder icon or text box under "Select a storage container". Then select the appropriate storage account. The storage container is used to stage the update files temporarily.

-If you’ve already created a container, you can reuse it. (Otherwise, select "+ Container" to create a new storage container for updates.). Select the container you wish to use and click "Select".

-Select "Submit" to start the import process.

-The import process begins, and the screen switches to to the "Import History" section. Select "Refresh" to view progress until the import process completes (depending on the size of the update, this may complete in a few minutes but could take longer).

-When the Status column indicates the import has succeeded, select the "Ready to Deploy" header. You should see your imported update in the list now.

**4)Create device groups in Device Update for IoT Hub**

4.1)Prerequisites

-Access to an IoT Hub with Device Update for IoT Hub enabled. It is recommended that you use a S1 (Standard) tier or above for your IoT Hub.

-An IoT device (or simulator) provisioned for Device Update within IoT Hub.

-At least one update has been successfully imported for the provisioned device.

4.2)Add a tag to your devices

-Device Update for IoT Hub allows deploying an update to a group of IoT devices. To create a group, the first step is to add a tag to the target set of devices in IoT Hub. Tags can only be successfully added to your device after it has been connected to Device Update.

-Direct Twin Updates

--Tags can also be added or updated in device twin directly.

--Log into Azure portal and navigate to your IoT Hub.

--From 'IoT Devices' or 'IoT Edge' on the left navigation pane find your IoT device and navigate to the Device Twin.

--In the Device Twin, delete any existing Device Update tag value by setting them to null.

--Add a new Device Update tag value.

-Device Update Tag Format

"tags": {

"ADUGroup": "<CustomTagValue>"

}

4.3)Create a device group by selecting an existing IoT Hub tag

-Go to the Azure portal.

-Select the IoT Hub you previously connected to your Device Update instance.

-Select the Device Updates option under Automatic Device Management from the left-hand navigation bar.

-Select the Groups tab at the top of the page. You will be able to see the number of devices connected to Device Update that are not grouped yet.

-Select the Add button to create a new group.

-Select an IoT Hub tag from the list and then select Create update group.

-Once the group is created, you will see that the update compliance chart and groups list are updated. Update compliance chart shows the count of devices in various states of compliance: On latest update, New updates available, Updates in Progress and Devices not yet Grouped.

-You should see your newly created group and any available updates for the devices in the new group. You can deploy the update to the new group from this view by clicking on the update name.

4.4)View Device details for the group you created

-Navigate to your newly created group and click on the group name.

-A list of devices that are part of the group will be shown along with their device update properties. In this view, you can also see the update compliance information for all devices that are members of the group. Update compliance chart shows the count of devices in various states of compliance: On latest update, New updates available and Updates in Progress.

-You can also click on each individual device within a group to be redirected to the device details page in IoT Hub.

**5)Deploy an Update using Device Update for IoT Hub**

5.1)Prerequisites

-Access to an IoT Hub with Device Update for IoT Hub enabled. It is recommended that you use a S1 (Standard) tier or above for your IoT Hub.

-At least one update has been successfully imported for the provisioned device.

-An IoT device (or simulator) provisioned for Device Update within IoT Hub.

-A tag has been assigned to the IoT device you are trying to update. The device is part of at least one update group.

-Supported browsers:

Microsoft Edge

Google Chrome

5.2)Deploy an update

-Go to Azure portal

-Navigate to the Device Update blade of your IoT Hub.

-Select the Groups tab at the top of the page.

-View the update compliance chart and groups list. You should see a new update available for your device group, with a link to the update under Pending Updates.

-Select the available update.

-Confirm the correct group is selected as the target group. Schedule your deployment, then select Deploy update.

-View the compliance chart. You should see the update is now in progress.

-After your device is successfully updated, you should see your compliance chart and deployment details update to reflect the same.

5.3)Monitor an update deployment

-Select the Deployments tab at the top of the page.

-Select the deployment you created to view the deployment details.

-Select Refresh to view the latest status details. Continue this process until the status changes to Succeeded.

5.4)Retry an update deployment

If your deployment fails for some reason, you can retry the deployment for failed devices.

-Go to the Deployments tab, and select the deployment that has failed.

-Click on the "Failed" Device Status in the detailed Deployment information pane.

- Click on "Retry failed devices" and acknowledge the confirmation notification.