AZURE CLOUD WORKLOAD PROTECTION

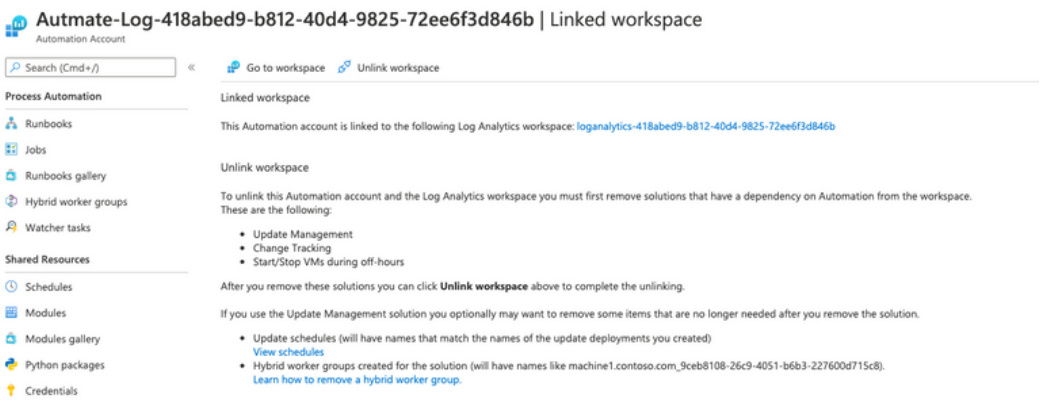
threatworx

Agent-less discovery for no-scan always on detection powered by ThreatWorx

1 CONFIGURING YOUR AZURE ENVIRONMENT

LogAnalytics workspace and Automation account is required to gather inventory for your Azure cloud, ensure both exist as part of your subscription using Azure Portal.

Link the automation account with the LogAnalytics workspace.



2 ENABLE INVENTORY COLLECTION FOR THE AUTOMATION ACCOUNT.

In automation account , select “Configuration Management => Inventory” to enable inventory collection.

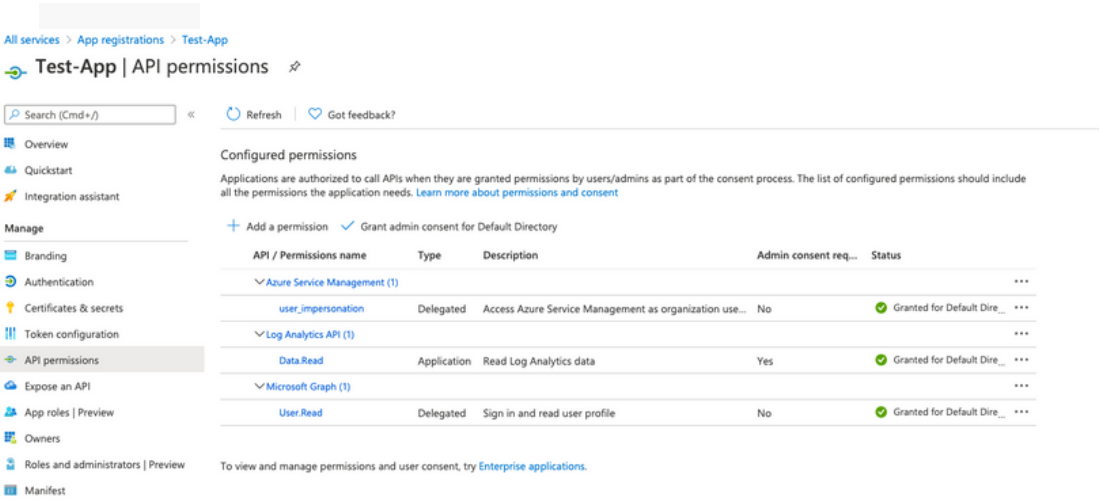
Follow the instructions mentioned here for details, https://docs.microsoft.com/en-us/azure/automation/automation-tutorial-installed-software

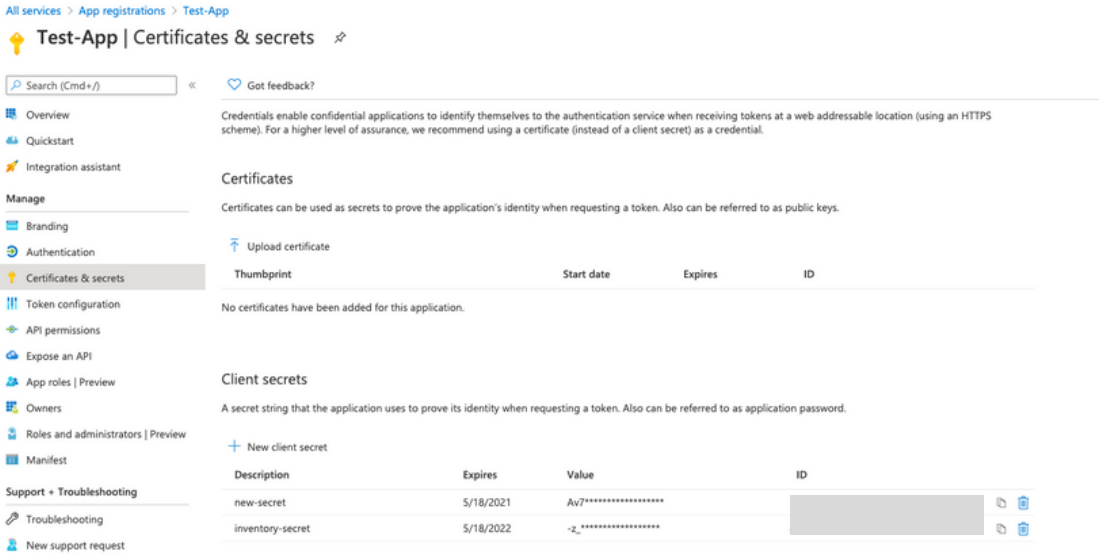
3

CREATE AN AZURE ACTIVE DIRECTORY APP

This app will be used by ThreatWorx to pull inventory information so you can choose to name it as your “ThreatWorx” app.
- Associate the permissions, “Read Logs Analytics Data” and “user_impersonation” to this app.
- Generate a client secret that the app uses to prove its identity

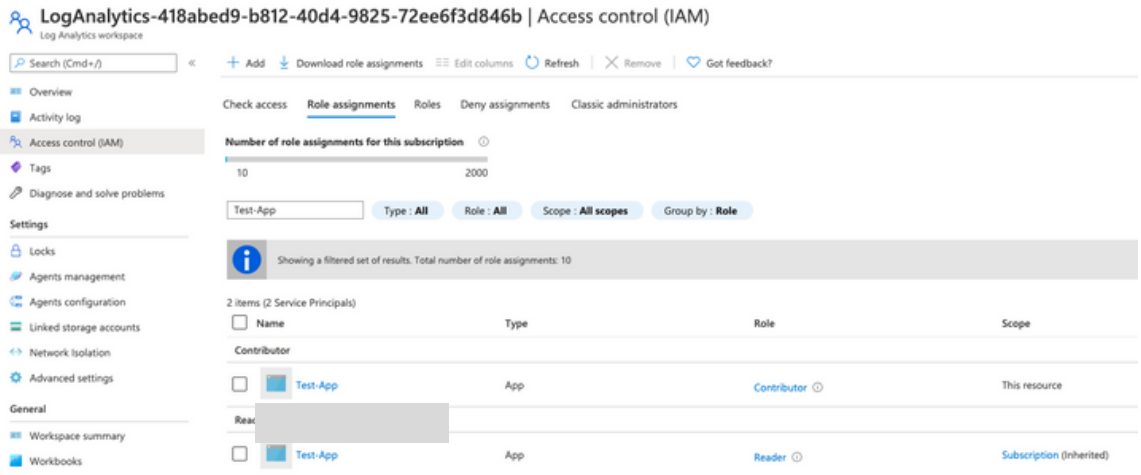
Note, that ThreatWorx as a service does not not need access to this app and the credentials of this app remain local to your environment.





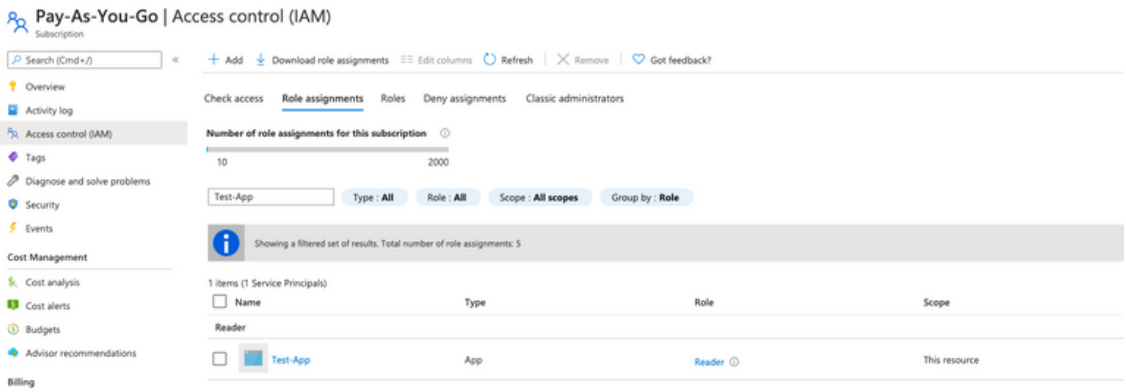
4 GRANT ACTIVE DIRECTORY APPLICATION ACCESS TO LOG ANALYTICS WORKSPACE

Select “Access Control (IAM)” after selecting the LogAnalytics workspace. Add the app created in step(3) and give it a “Reader” or “Contributor” role.



5 ENSURE THAT THE APPLICATION IS ALSO ADDED AS PART OF THE SUBSCRIPTION

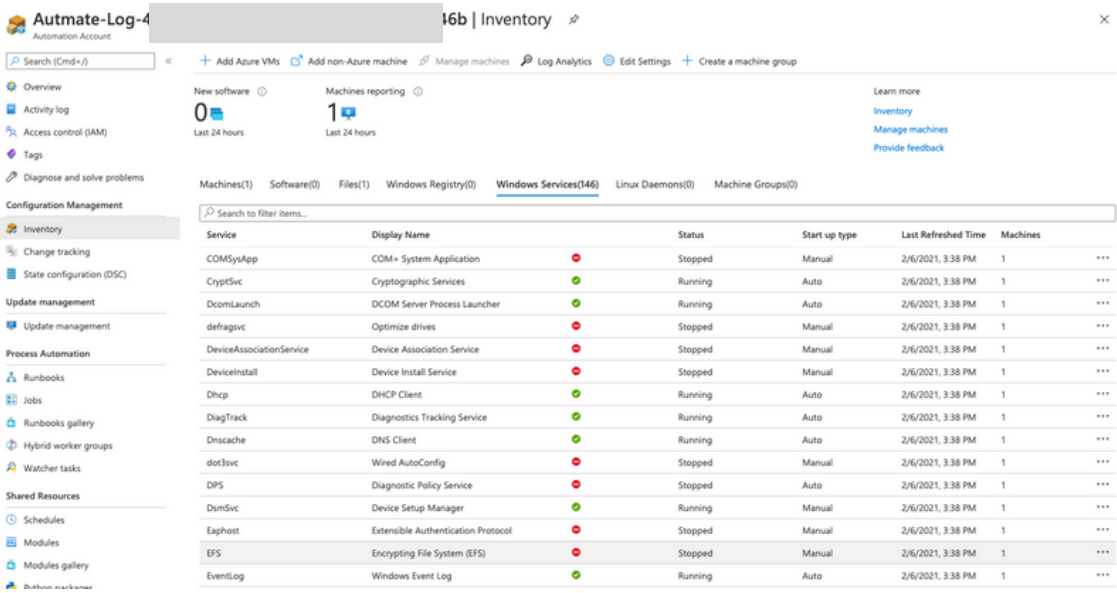
Select the Subscription, and Access Control (IAM). Add your application with a “Reader” role



6 INVENTORY IN LOG ANLYTICS WORKSPACE

You should now see inventory in the log analytics workspace. Ensure that you are able see the inventory before moving on to the next steps.

Tip: If you don't see inventory flowing in the log analytics workspace, follow the trouble shooting steps provided in the Azure documentation.



7

Using the twigs CLI you can now pull the inventory into your ThreatWorx instance (threatworx.io for public SaaS or yourcompany.threatworx.io for dedicated).

```
twigs -v azure –azure_tenant_id “   [TENANT_ID]" --
azure_application_id “[APPLICATION_ID]" –
azure_application_key “[APPLICATION_KEY]" --
azure_subscription  “[SUBSCRIPTION_ID]" --
azure_resource_group  “[RESOURCE_GROUP_NAME]" --
azure_workspace  “[LOG_ANALYTICS_WORKSPACE_ID]"
```

Checkout twigs guide & help videos for additional options including CIS benchmark checks for your Azure cloud, https://twigs.threatworx.io/guide

8 THREATWORX CONSOLE

Analytics, security vulnerabilities, mis-configurations, static and dynamic analysis for base images, running apps and containers can now be managed from the I3 console.

Date	Title	Rating	Resource	Type	Status
Aug 26, 2020	1.3 Ensure that there are no guest users	Critical	Pay-As-You-Go	Misconfiguration	OPEN
Aug 26, 2020	1.23 Ensure that no custom subscription owner roles are created	Critical	Pay-As-You-Go	Misconfiguration	OPEN
Aug 26, 2020	2.2 Ensure that 'Automatic provisioning of monitoring agent' is set to 'On'	Critical	Pay-As-You-Go	Misconfiguration	OPEN
Aug 26, 2020	2.7 Ensure that 'Network security groups' is set to 'On'	Critical	Pay-As-You-Go	Misconfiguration	OPEN
Aug 26, 2020	2.8 Ensure that 'Web application firewall' is set to 'On'	Critical	Pay-As-You-Go	Misconfiguration	OPEN
Aug 26, 2020	2.11 Ensure that 'Storage Encryption' is set to 'On'	Critical	Pay-As-You-Go	Misconfiguration	OPEN
Aug 26, 2020	2.14 Ensure that 'SQL auditing & Threat detection' is set to 'On'	Critical	Pay-As-You-Go	Misconfiguration	OPEN
Aug 26, 2020	2.15 Ensure that 'SQL Encryption' is set to 'On'	Critical	Pay-As-You-Go	Misconfiguration	OPEN
Aug 26, 2020	2.17 Ensure that security contact 'Phone number' is set	Critical	Pay-As-You-Go	Misconfiguration	OPEN
Aug 26, 2020	2.18 Ensure that 'Send me emails about alerts' is set to 'On'	Critical	Pay-As-You-Go	Misconfiguration	OPEN
Aug 26, 2020	2.19 Ensure that 'Send email also to subscription owners' is set to 'On'	Critical	Pay-As-You-Go	Misconfiguration	OPEN
Aug 26, 2020	5.1 Ensure that a Log Profile exists	Critical	Pay-As-You-Go	Misconfiguration	OPEN
Aug 26, 2020	5.2 Ensure that Activity Log Retention is set 365 days or greater	Critical	Pay-As-You-Go	Misconfiguration	OPEN
Aug 26, 2020	5.3 Ensure that Activity Log Alert exists for Create Policy Assignment	Critical	Pay-As-You-Go	Misconfiguration	OPEN
Aug 26, 2020	5.4 Ensure that Activity Log Alert exists for Create or Update Network Security Group	Critical	Pay-As-You-Go	Misconfiguration	OPEN
Aug 26, 2020	5.5 Ensure that Activity Log Alert exists for Delete Network Security Group	Critical	Pay-As-You-Go	Misconfiguration	OPEN
Aug 26, 2020	5.6 Ensure that Activity Log Alert exists for Create or Update Network Security Group Rule	Critical	Pay-As-You-Go	Misconfiguration	OPEN

	Risk Score	Recorded On	CVE / Advisory	Affected Product	Rating	Priority	Status
	80	Nov 28, 2020	CVE-2018-8453	Windows Server 2019 Datacenter	Critical	Now	OPEN
	80	Nov 28, 2020	CVE-2019-0859	Windows Server 2019 Datacenter	Critical	Now	OPEN
	80	Nov 28, 2020	CVE-2019-0803	Windows Server 2019 Datacenter	Critical	Now	OPEN
	80	Nov 28, 2020	CVE-2019-0703	Windows Server 2019 Datacenter	Medium	Now	OPEN
	80	Nov 28, 2020	CVE-2020-0601	Windows Server 2019 Datacenter	Severe	Now	OPEN
	80	Nov 28, 2020	CVE-2020-0787	Windows Server 2019 Datacenter	Critical	Now	OPEN
	80	Nov 28, 2020	CVE-2020-1054	Windows Server 2019 Datacenter	Critical	Now	OPEN
	80	Nov 28, 2020	CVE-2020-0986	Windows Server 2019 Datacenter	Critical	Now	OPEN
	80	Nov 28, 2020	CVE-2020-1350	Windows Server 2019 Datacenter	Urgent	Now	OPEN
	80	Nov 28, 2020	CVE-2020-1472	Windows Server 2019 Datacenter	Urgent	Now	OPEN
	75	Nov 28, 2020	CVE-2018-8637	Windows Server 2019 Datacenter	Medium	Now	OPEN
	75	Nov 28, 2020	CVE-2018-8638	Windows Server 2019 Datacenter	Medium	Now	OPEN
	75	Nov 28, 2020	CVE-2018-8641	Windows Server 2019 Datacenter	Critical	Now	OPEN
	75	Nov 28, 2020	CVE-2018-8477	Windows Server 2019 Datacenter	Medium	Now	OPEN
	75	Nov 28, 2020	CVE-2018-8514	Windows Server 2019 Datacenter	Medium	Now	OPEN
	75	Nov 28, 2020	CVE-2018-8596	Windows Server 2019 Datacenter	Severe	Now	OPEN
	75	Nov 28, 2020	CVE-2018-8595	Windows Server 2019 Datacenter	Severe	Now	OPEN
	75	Nov 28, 2020	CVE-2019-1040	Windows Server 2019 Datacenter	Severe	Now	OPEN