Prepared for

ABI

ABI Cloud Management Project Infrastructure Build Guide

Document Control

Document Information

|  |  |
| --- | --- |
| ***File Name*** | ABI Cloud Management Project Infrastructure Build Guide - FINAL.docx |
| ***Author(s)*** |  |
| ***Status*** | Final |
| ***Publication Date*** | Dec 1, 2017 |

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Changes |
| 0.1 | Aug 12, 2017 | Vincent Johnson-Thacker | Initial draft |
| FINAL | Dec 1, 2017 | Rahul Argade | Final QA an |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[1 Introduction 5](#_Toc500949298)

[1.1 Landing Zones 5](#_Toc500949299)

[2 Azure Subscriptions 6](#_Toc500949300)

[2.1 RBAC Requirements 6](#_Toc500949301)

[2.2 Local Currency Support 7](#_Toc500949302)

[3 Land Zone Components 8](#_Toc500949303)

[3.1 Base Network 8](#_Toc500949304)

[3.2 UDR & NSG 8](#_Toc500949305)

[3.3 Express Route 9](#_Toc500949306)

[3.4 Key Vaults 10](#_Toc500949307)

[3.5 Security Center 11](#_Toc500949308)

[3.6 Palo Alto 12](#_Toc500949309)

[3.7 Azure Backup 13](#_Toc500949310)

[3.8 Operations Management Suite (OMS) 17](#_Toc500949311)

[3.8.1 Azure Automation Account 17](#_Toc500949312)

[3.8.2 OMS Workspace – Log Analytics 17](#_Toc500949313)

[3.8.3 Dashboards & Queries 18](#_Toc500949314)

[3.8.4 Log searches in Log Analytics 20](#_Toc500949315)

[3.8.5 Agents 23](#_Toc500949316)

[3.9 Logic Apps 23](#_Toc500949317)

[4 SharePoint Self-Service Portal 25](#_Toc500949318)

[4.1 Service Catalog List 25](#_Toc500949319)

[4.1.1 Columns and Content Types 25](#_Toc500949320)

[4.1.2 List Settings 30](#_Toc500949321)

[4.2 Approval Workflow 30](#_Toc500949322)

[4.2.1 Overview 31](#_Toc500949323)

[4.2.2 Set Item Details 32](#_Toc500949324)

[4.2.3 Approval – Set Up 34](#_Toc500949325)

[4.2.4 Approval – Details 37](#_Toc500949326)

[4.2.5 Post Approval Actions 44](#_Toc500949327)

[4.3 SharePoint Framework Add-In 45](#_Toc500949328)

[4.3.1 SharePoint Framework Overview 45](#_Toc500949329)

[4.3.2 Service Catalog Add-In 46](#_Toc500949330)

[4.4 Source Control 62](#_Toc500949331)

[4.4.1 Workflow 62](#_Toc500949332)

[4.4.2 SharePoint Framework Add-in 62](#_Toc500949333)

[4.5 Application Support Scenarios 63](#_Toc500949334)

[4.6 Adding a new Landing Zone 63](#_Toc500949335)

[4.7 Adding a new Service Catalog Item 63](#_Toc500949336)

[5 Visual Studio Online (VSO) 65](#_Toc500949337)

[5.1 Code Repository 65](#_Toc500949338)

[5.2 Build Definitions 66](#_Toc500949339)

[5.3 Release Definitions 66](#_Toc500949340)

[5.4 Linking VSO to Azure 68](#_Toc500949341)

[6 Appendix 71](#_Toc500949342)

[6.1 JSON VNET Parameters file 71](#_Toc500949343)

[6.2 Backup Vault ARM Template 74](#_Toc500949344)

[6.3 Logic App Code 74](#_Toc500949345)

[6.3.1 TriggerRelease 74](#_Toc500949346)

[6.3.2 DeploymentStatusUpdate 78](#_Toc500949347)

[6.3.3 UpdateAzureDataSP 84](#_Toc500949348)

# Introduction

The goal of this document is to describe how to:

* Setup the Azure Subscriptions for a Landing Zone (LZ)
* Build the infrastructure components of an Azure Subscription for a LZ
* Integrate the Self-Service Portal with a Landing Zone

The description of the components and their architectural goals are discussed as part of the infrastructure architecture document. The ARM templates and PowerShell scripts used to build out a Landing Zone will be attached as part of the appendix.

## Landing Zones

The landing zones and their Azure region location are as follows:

* Global
  + Location: West Europe
  + Abbreviation: GB
* North America
  + Location: Central US
  + Abbreviation: NAZ
* Mexico
  + Location: South Central US
  + Abbreviation: MX
* Europe
  + Location: West Europe
  + Abbreviation: EU
* China
  + Location: China East
  + Abbreviation: CN
* Korea
  + Location: Korea Central
  + Abbreviation: KR
* Australia
  + Location: South East Australia\*
  + Abbreviation: AU
* Brazil
  + Location: South Brazil
  + Abbreviation: BR

# Azure Subscriptions

For Greenfield Landing Zones, LZs without existing or limited Azure workloads, the recommended path is to create 2 new Azure subscriptions. Each Landing Zone by default has 2 subscriptions: one for production workloads; a second for non-production workloads. For Brownfield LZs, existing Azure subscriptions can be re-purposed and become the ABI LZ.

The names for the Azure subscriptions are as follows:

* ABI BR NON-PROD
* ABI BR PROD
* ABI EU NON-PROD
* ABI EU PROD
* ABI KR NON-PROD
* ABI KR PROD
* ABI NAZ NON-PROD
* ABI NAZ PROD
* ABI GLOBAL NON-PROD
* ABI GLOBAL PROD
  + Rename from existing Azure sub: ABI-DC-WE
* ABI MX NON-PROD
  + Rename from existing Azure sub: Microsoft Azure Non Production
* ABI MX PROD
  + Rename from existing Azure sub: Microsoft Azure Production
* ABI CN NON-PROD
* ABI CN PROD
* ABI AU NON-PROD
* ABI AU PROD

The Azure Subscriptions that are part of an ABI LZ must use the Global ABI directory (anheuserbuschinbev.onmicrosoft.com). This enables Single Sign On and ABI directory support. Subscriptions can be provisioned from the site <https://account.azure.com/Subscriptions>. The user creating the new Landing Zone subscriptions must have, at a minimum, Account Administrator privileges.

Detailed steps on how to create a new subscription can be found here: <https://azure.microsoft.com/en-us/resources/videos/sign-up-for-microsoft-azure/>

The deviation from the Microsoft video is that the subscription will be generated from regional Enterprise Agreement so that billing will be generated in local currency.

## RBAC Requirements

To build out the Landing Zone, the operator/worker process must have Owner or Co-Administrator permissions to the subscriptions. The actions that require the high authorization level are:

* Link VSTS to the Azure subscription
  + For more information click [here](#_Visual_Studio_Online).
* Create automation accounts
* Grant permissions team
* Create custom Resource Policy Template for VSTS Service Principal account. Example instructions can be found [here:](https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-create-service-principal-portal)

## Local Currency Support

For local currency support, you must create the Azure subscriptions under the correct Enterprise Agreement (EA) specific to the region. There are multiple Enterprise enrollments within ABI. Selecting the correct enrollment ensures local billing in local currency to support the landing zone.

# Land Zone Components

## Base Network

The base Azure network is composed of 2 VNETs, 1 public and 1 private. They are created in the LZ using an ARM template. All the zone-specific values are entered as configuration inside of a parameters JSON file. An example of the JSON parameters is found in the Appendix [here](#_JSON_VNET_Parameters). A landing zone consists of a production and non-production replica of these VNETs in adjacent address space. This spreadsheet is maintained separate from this document.

The private VNET RFC 1918 address space must be approved and provided from the ABI global networking team. This is to make sure that the IP address space is unique across all the ABI network.

|  |  |
| --- | --- |
| Private VNET | Description |
| Gateway Subnet | Required for the Express Route Gateway. Cannot have NSG or UDR defined on Subnet. No VMs can be inside this subnet. |
| Web App Subnet | Consumes half of the allocated IP address spaces. Any Web or App VM should be located inside of this subnet. |
| DB Subnet | Used for any database workloads as well as any Hadoop private IP address space. |
| Infra Subnet | Used for Domain controllers and any other shared infrastructure resource. |
| DMZ Subnet | Used for the Palo Alto appliance to handle outbound routes from the Private VNET to the internet or Azure PaaS services. |

|  |  |
| --- | --- |
| Public VNET | Description |
| Web App Subnet | Consumes half of the allocated IP address spaces. Any Web or App VM should be located inside of this subnet. |
| DB Subnet | Used for any database workloads as well as any Hadoop private IP address space. |
| Infra Subnet | Used for any shared infrastructure resources. |

The excel sheet below contains the CIDR allocation for each region.



## UDR & NSG

**The final UDR and NSG’s are being finalized by zone pending Express Route BGP universal advertisement of the network address space, and deployment of Palo Alto’s to the public VNET in the landing zones.**

User defined routing is defined differently for the private vs public VNETs. The table below shows the association between UDR and Subnet:

|  |  |  |
| --- | --- | --- |
| Subnet | UDR | NSG |
| Private WebApp | WebApp-route |  |
| Private DB | DB |  |
| Private Infra |  |  |
| Private DMZ |  |  |
| Private Gateway Subnet | N/A | N/A |
| Public WebApp |  |  |
| Public DB |  |  |
| Public Infra |  |  |

The routes for the private VNETs use the route 0.0.0.0/0 and point to the Palo Alto Load Balancer. If the zone advertises a default route, then all traffic use that route and point back on-prem.

## Express Route

For a Landing Zone, only 1 Express Route circuit is required per Geo-Political region. Details on the regions within Azure can be found [here](https://docs.microsoft.com/en-us/azure/expressroute/expressroute-locations#partners). The Express Route Circuit Azure Resource is associated with 1 Subscription in the region and provides connectivity to both subscriptions.



//Express Route details can be found in the subscription. No Express Route should be modified unless Accenture is involved. Express Routes, Virtual Network Gateways and peering information is not end-user configurable. Modifications to these settings risk orphaning the landing zone.

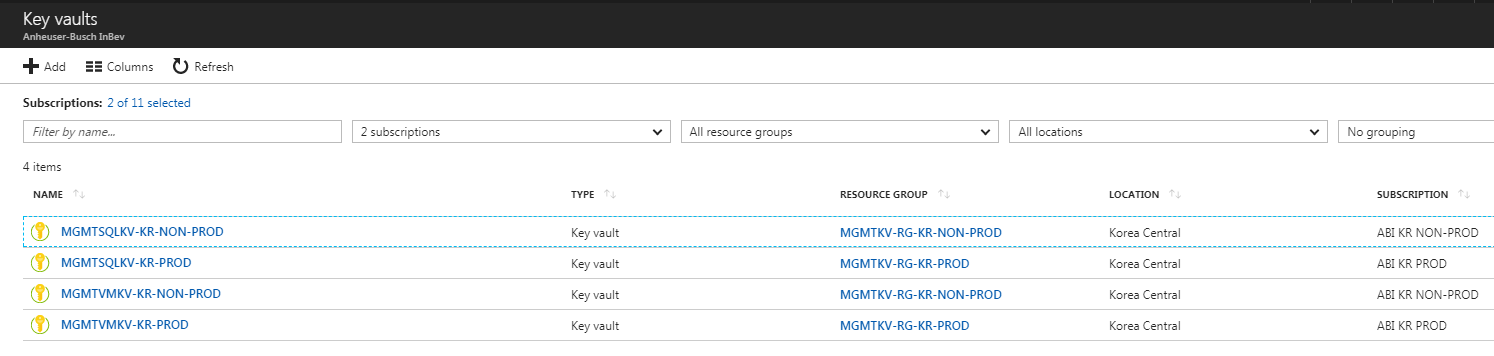
To build this environment you must first ensure that the VNET has a subnet called “Gateway Subnet”. If the name is not exactly “Gateway Subnet” it will not work and you will not be able to associate with Virtual Network Gateway with the VNET.

For the LZ build, the Virtual Network Gateway is created manually using the Azure portal. Additionally, the Express Route authorization and connections are also made and connected using the Azure portal.

## Key Vaults

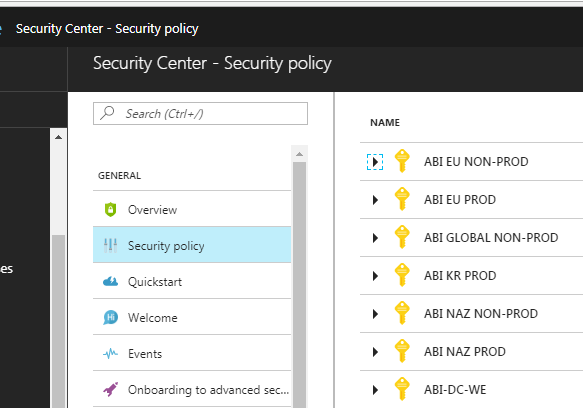
There are 2 Key Vaults required per subscription, making it a total of 4 Key Vaults per Landing Zone. In a single subscription, there is a VM KeyVault and a SQL Server KeyVault. These vaults contain sensitive information, login credentials, for their respective types. For instance, when creating a VM, the administrator credentials are retrieved from Key Vault programmatically, and then set in the VM.

The KeyVault creation is done via ARM Template script located in Visual Studio Online source control and the secrets are set manually by an ABI operations administrator to prevent these values from being distributed.



## Security Center

Azure Security Center is a feature that we enable manually per subscription. This process is done in the portal through the UI.

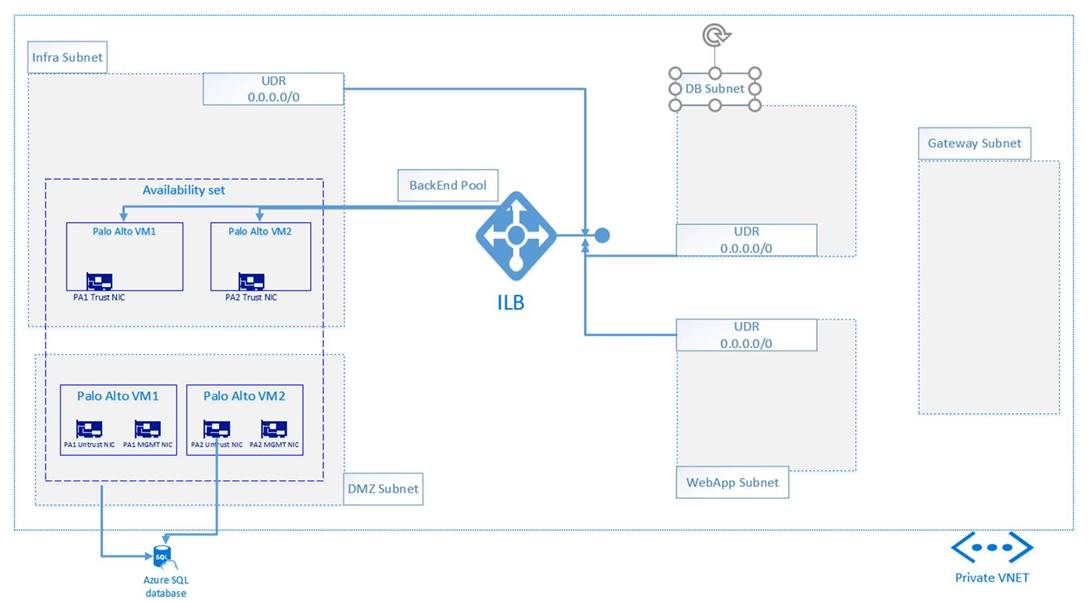


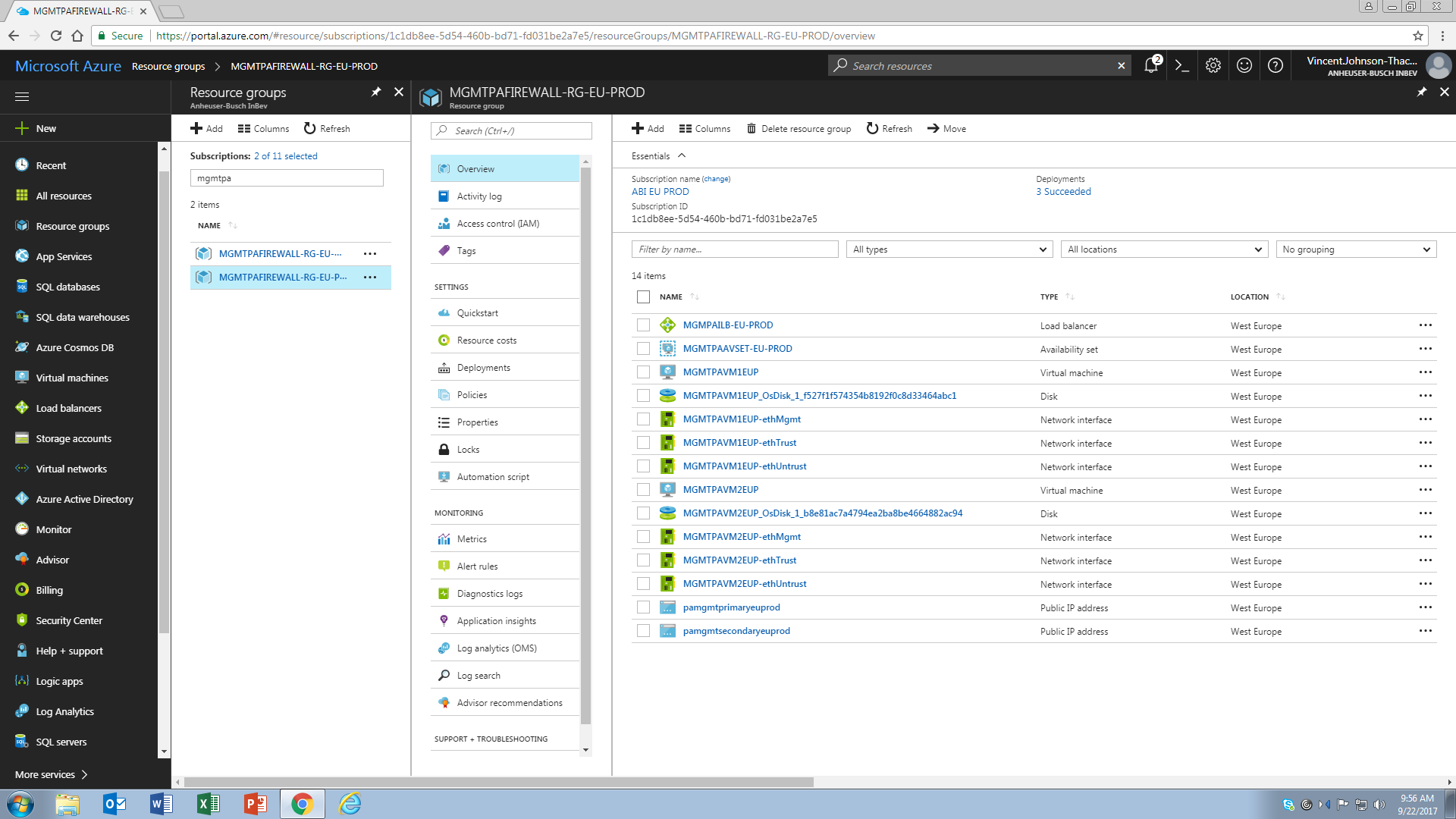
The usage data is assessed for security threats and the information is displayed in the Security Center Dashboard.

## Palo Alto

The Palo Alto Firewalls must be built AFTER the basic VNET infrastructure has been created. Once this is completed we purchase the Palo Altos through the Azure Portal using the Azure Marketplace. They are created using the PAYG 1 license (Pay as you go version 1).

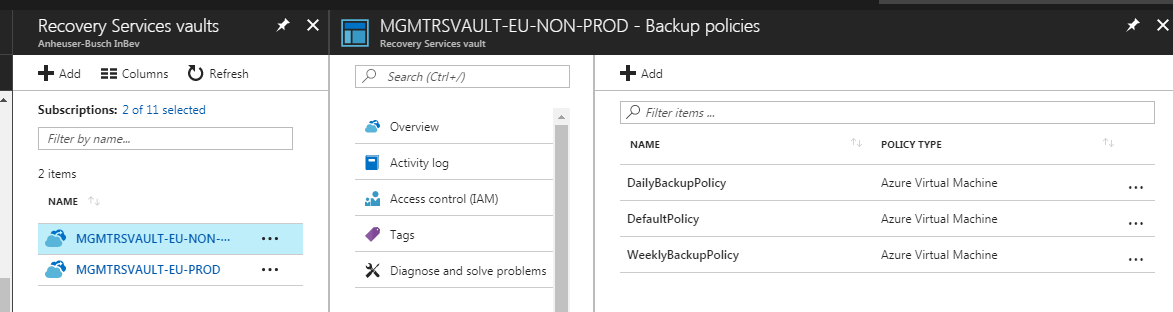
The Palo Altos are built using Linux VMs with Managed Disks in a load balanced HA configuration. There are 3 nics associated with the PAs.





## Azure Backup

The Azure Backup vault is created through an ARM Template script. It is created with 2 default policies, daily and weekly backup schedules. The script is found in the Appendix [here](#_Backup_Vault_ARM). The Landing Zone design requires that these policies are in place because the Self-Service Provisioning Portal uses these policies.



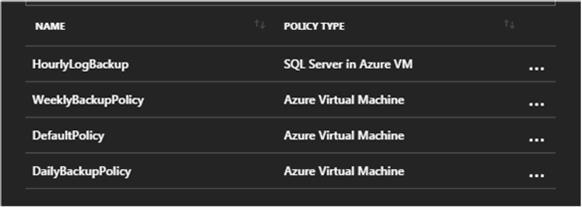
The schedules are created and specified based on ABI’s RPO/RTO objectives based on what has been captured during zone engagement workshops. SQL Logs policies are often added for databases running on IaaS. The nomenclature for the resource, Recovery Vaults, is as follows:

MGMTRSVAULT-<ZONE CODE>-NON-PROD

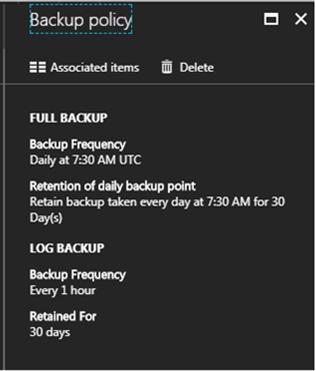
MGMTRSVAULT-<ZONE CODE>-PROD

The following screen shots capture details from the Global Landing Zone. The Landing Zone is as follows:

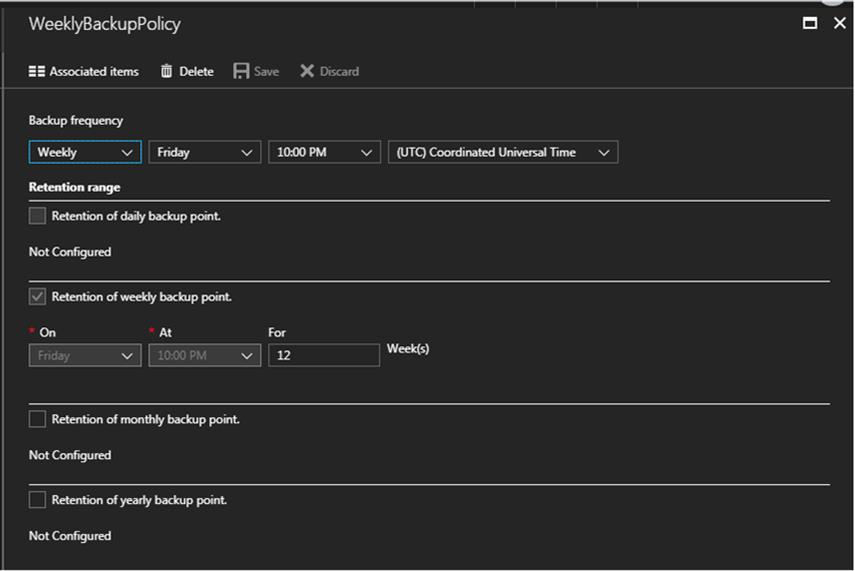
 List of Policies



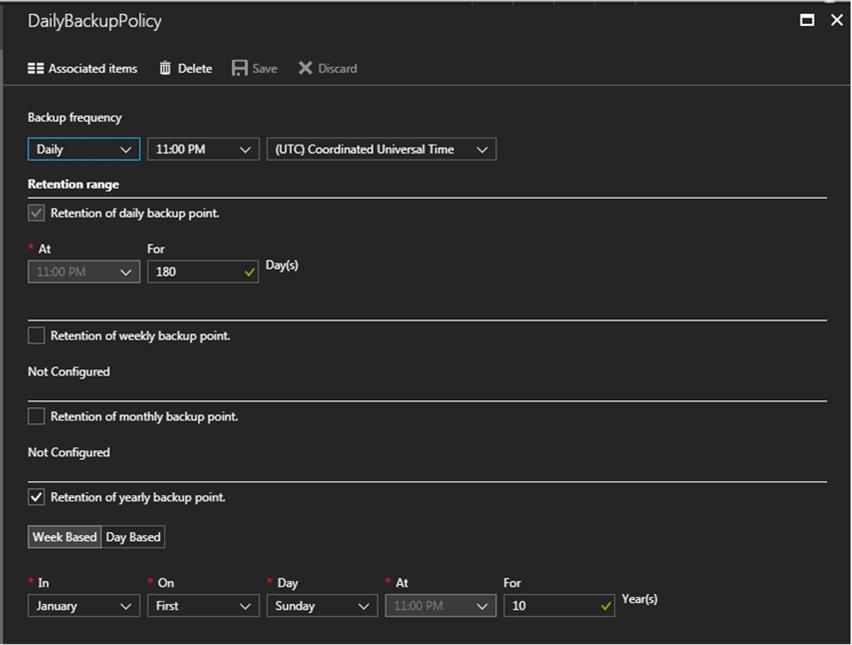
 Back up policy type for the SQL/DB hourly log back ups. (truncation and commit).



Detail on the weekly backup policy that includes, frequency, time, and retention.



Daily Backup policy is listed here – Schedule and Retention



# Visual Studio Online (VSO)

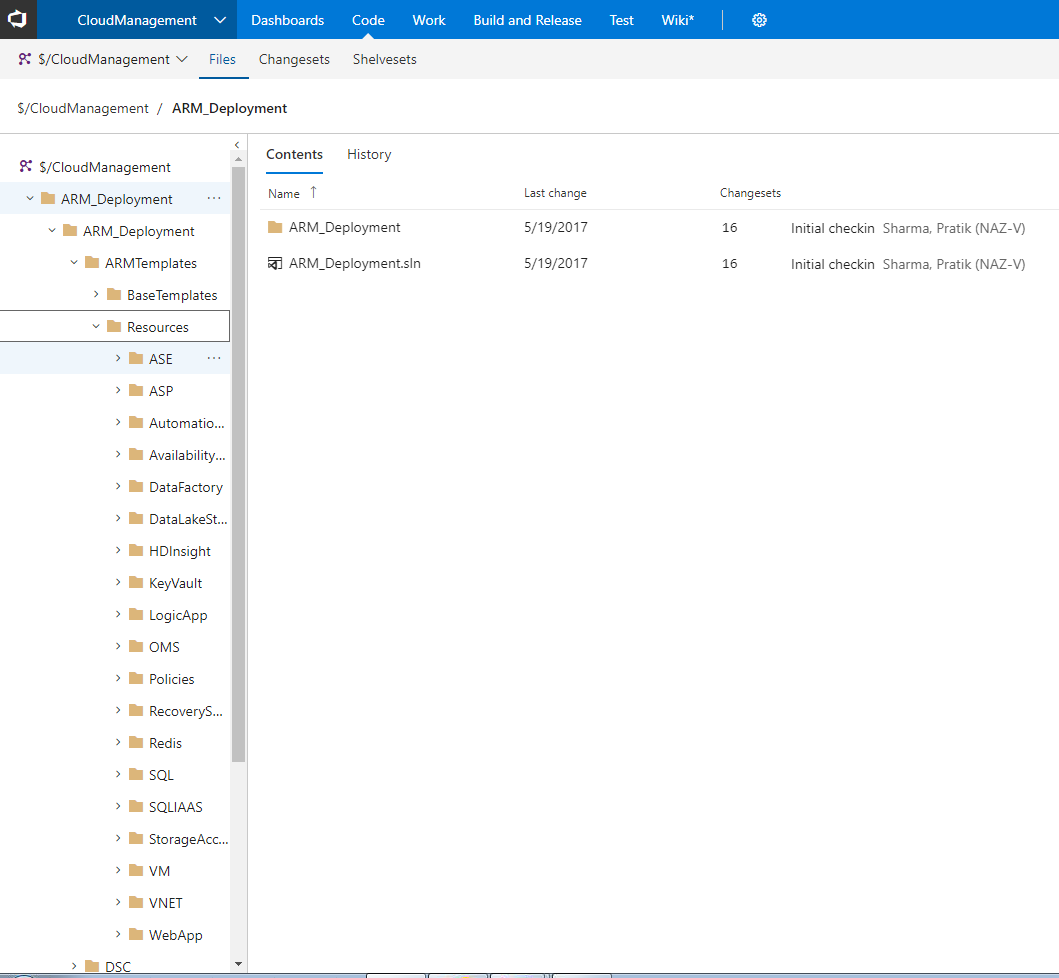
The VSO build instance is comprised on a team project containing source control, Build Definitions, and Release definitions. All of the code, JSON templates for both Build and Release definitions can be found here:

<https://abi-azure-management.visualstudio.com/CloudManagement>

The owner of the VSO instance is currently Anthony Tsai.

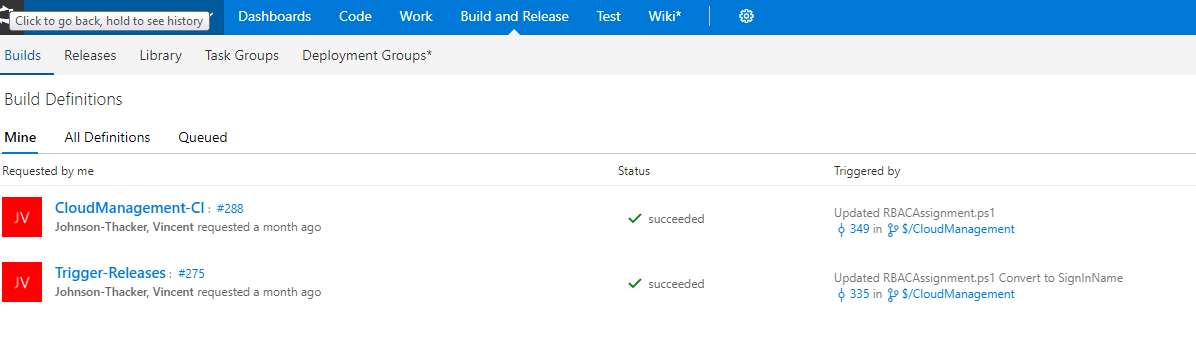
## Code Repository

The code repository has ARM templates that are able to build multiple types of Azure resources.

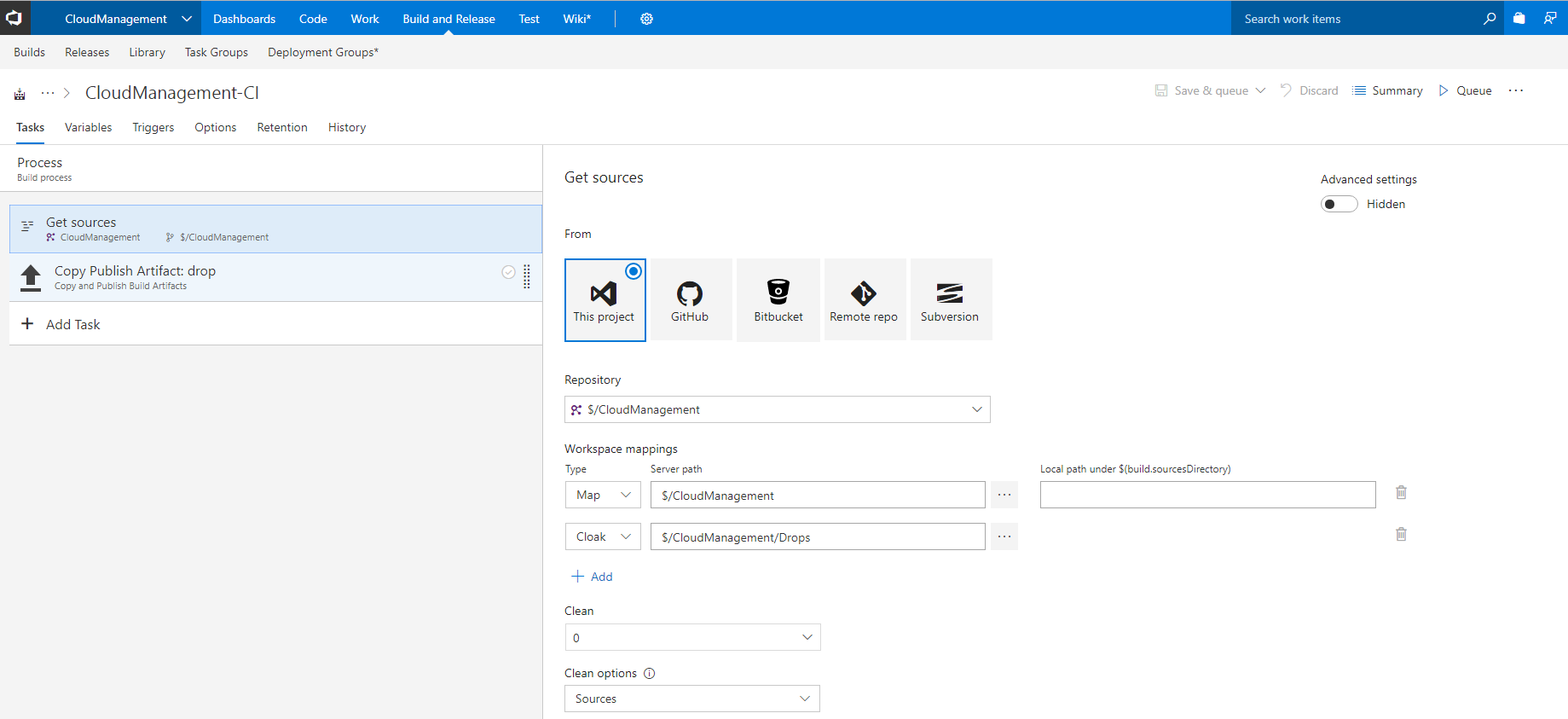


## Build Definitions

The code stored in source control is built using the Build Definition. For the ABI Landing Zone environment we are using 2 different Build definitions. One of them is our standard CI build and the other is the build release trigger.



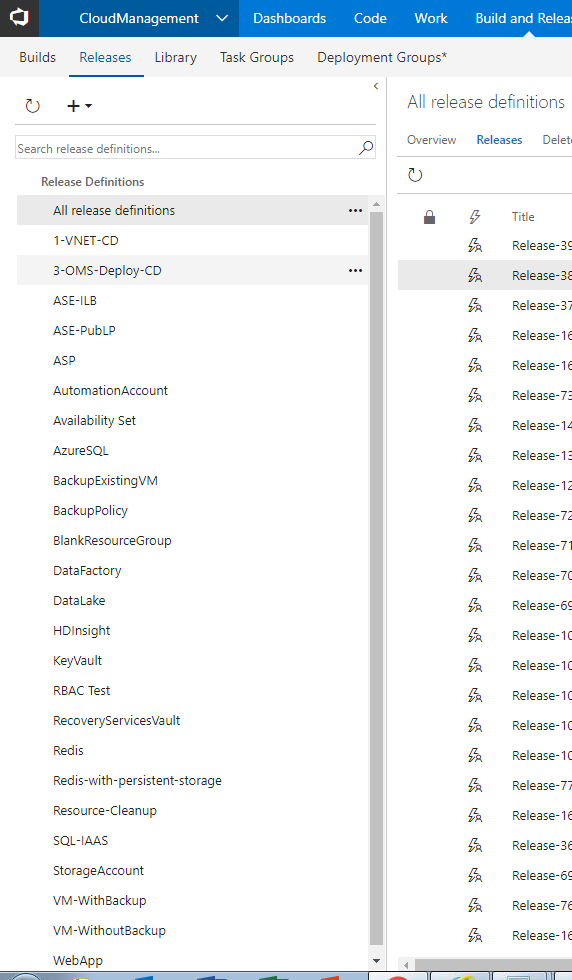
Peeking inside of the build definition, we can see the build steps.



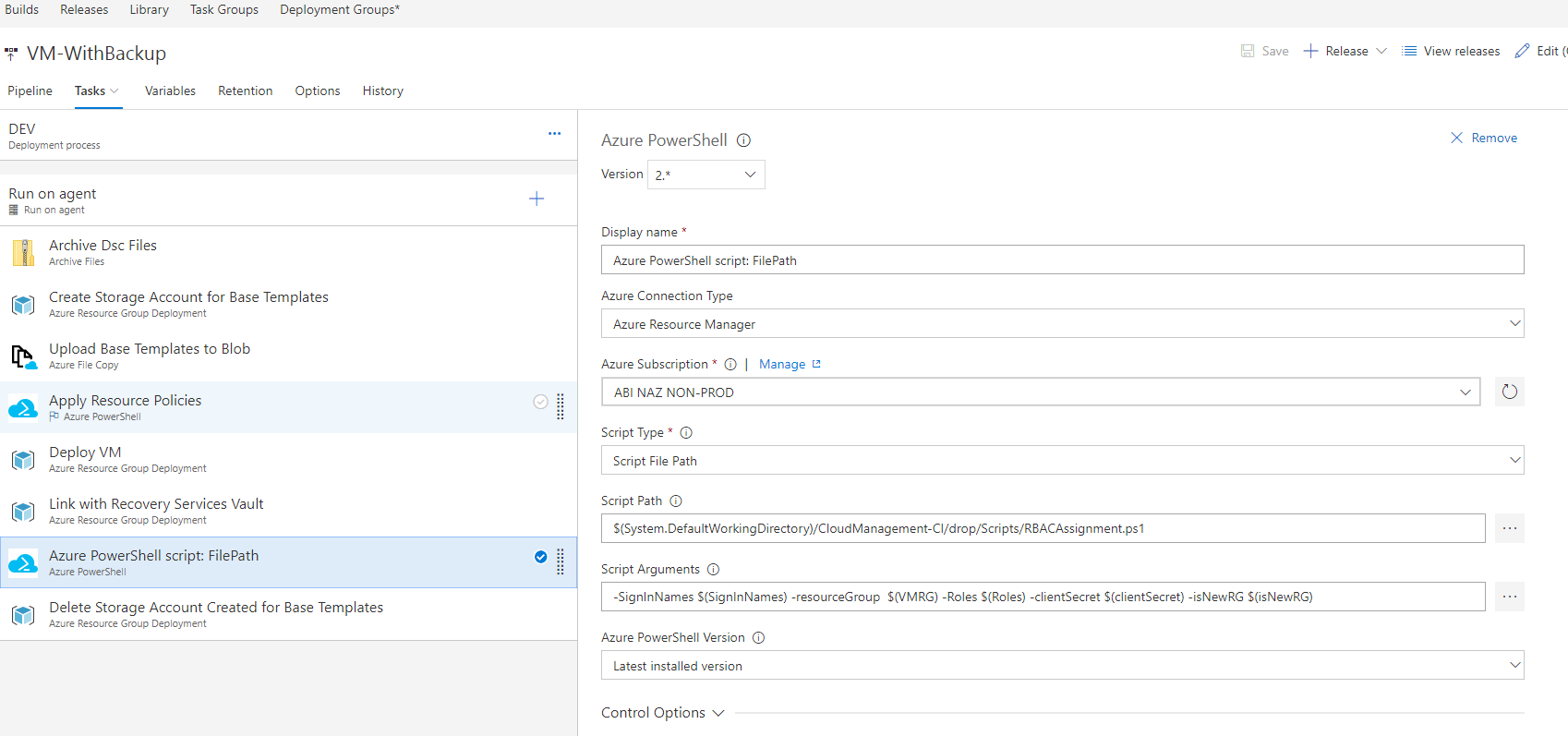
## Release Definitions

Next, from the Build definition, we create individual releases for each type of resource we want to provision. All of the release definitions are located here:

<https://abi-azure-management.visualstudio.com/CloudManagement/_release>

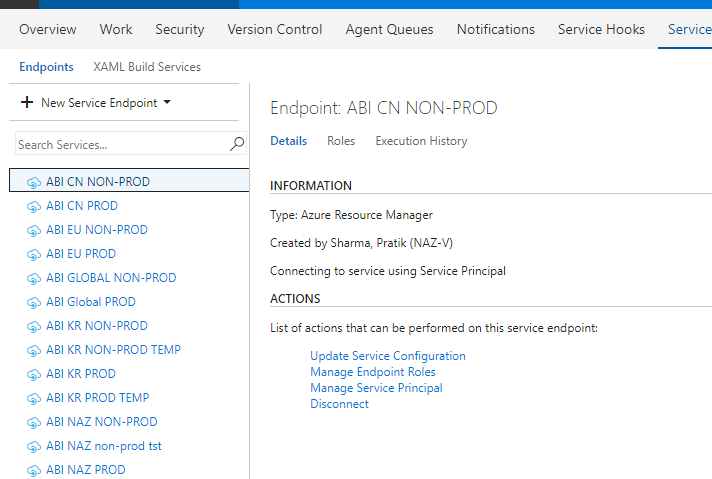


The release definitions are all JSON based in their templates so that they are easily imported/exported. In the UI, after all of the release definitions have been imported, it looks like this:

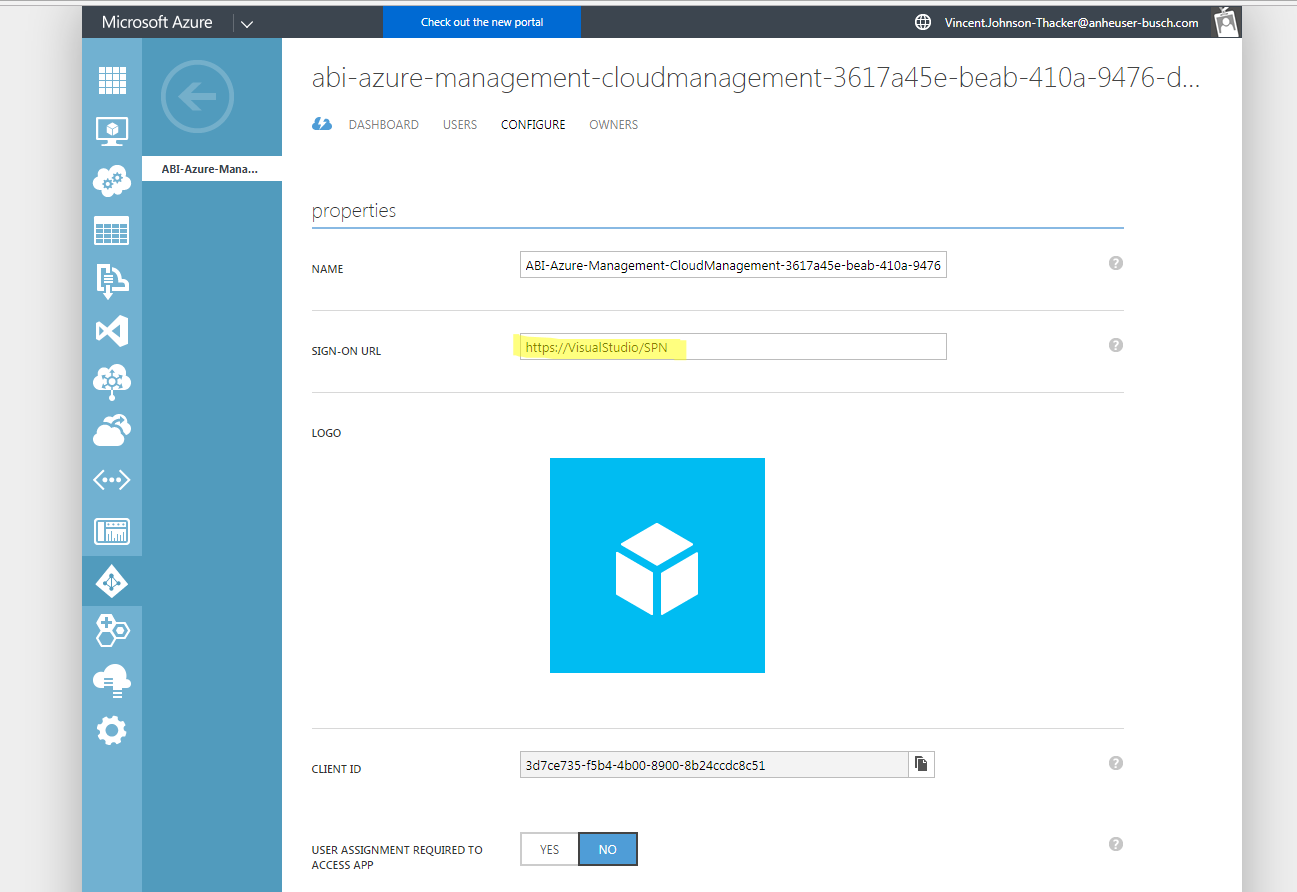


## Linking VSO to Azure

In order to execute the release definitions against the Azure subscription we must link the VSO instance to the environment. This is done using Service Endpoints and SPNs. The initial linking between VSO and Azure requires a user to have Owner permission in the Azure subscription and Administrative permissions in team project.



Inside of Azure, we can see that we create the SPN for the VSO.



In addition to creating the Azure AD application, we must also assign the Read Directory Data permission for the application to the Microsoft Graph application. **Note, when assigning the read Directory Data permissions, you must be sure that a Global Administrator provides consent!**

