

#ANSIBLEFEST2019

Take Control of Containers in the Public Cloud

Stuart Kirk, Cloud Native / Open Source Black Belt
Zim Kalinowski, Senior Software Engineer



ANSIBLE

STUART KIRK

Cloud Native Technical Specialist
Open Source Black Belt
Microsoft Corporation

- Home: Ann Arbor, Michigan
- Entirety of Career in Open Source: Dell, Cisco, Red Hat
- Joined Microsoft & Started with Ansible in 2016
- First RHCA hired by Microsoft
- Core focus is OpenShift on Azure & OSS
- Favorite thing to do with Ansible: Extending on-premise Ansible deployments seamlessly into Microsoft Azure
- Twitter: @StuartAtMSFT
- LinkedIn: <https://www.linkedin.com/in/stuartkirk>



ZIM KALINOWSKI

Software Engineer
Microsoft Corporation

- Home: Shanghai, China
 - Working on Open Source, previously involved mostly in Embedded Systems
 - Started with Ansible in 2017
 - Favorite thing to do with Ansible: new modules
 - Big fan of American BBQ & Craft Beer
-
- Twitter: @ZimOnAzure
 - LinkedIn: <https://www.linkedin.com/in/smarterphone/>



Housekeeping/ Prep Work!

Agenda & Playbooks

AGENDA

- Building containers with Docker
- Uploading containers to Azure Container Registry (ACR) and Docker Hub
- Running containers using Azure Container Instance (ACI)
- Using the managed Azure Kubernetes Service (AKS)
- Build Azure Red Hat OpenShift (ARO) cluster in 10 minutes
- Deploy Container to ARO using Ansible
- Other OpenShift on Azure Options

PLAYBOOKS

- 00-prerequisites.yml
- 01-build-and-push-to-dockerhub.yml
- 02-build-acr-image.yml
- 03-create-container-instance.yml
- **04-aks-create.yml (Housekeeping)**
- **05-cosmosdb-deploy.yml (Housekeeping)**
- 06-aks-deploy.yml
- 07-create-aro.yml
- 08-aro-deploy.yml

Create Azure Resource Group
Build ARO Container & Push to Dockerhub
Build ACR, Container & Connect to GitHub
Create Azure Container Instance
Create Azure Kubernetes Service cluster
Create Azure CosmosDB for MongoDB
Deploy Voting App definition to AKS
Create Azure Red Hat OpenShift cluster
Deploy container to ARO



HELP

**Let's Start the
Demonstrations!**

Container Ecosystems & Azure Red Hat OpenShift

CONTAINER ECOSYSTEMS IN AZURE



App Service

Deploy web apps or APIs using containers in a PaaS environment



Service Fabric

Modernize .NET applications to microservices using Windows Server containers



Kubernetes Service

Scale and orchestrate Linux containers using Kubernetes



Container Instance

Elastically burst from your Azure Kubernetes Service (AKS) cluster



Azure Red Hat OpenShift

Deploy a fully-managed OpenShift cluster with ARO or choose to run OpenShift on IaaS



Azure Container Registry



Docker Hub

RUNNING YOUR OWN OPENSHIFT IN AZURE (IaaS)

Responsibilities

User management

Project and quota management

Application lifecycle

Cluster creation

Cluster management

Monitoring and logging

Network configuration

Software and security updates

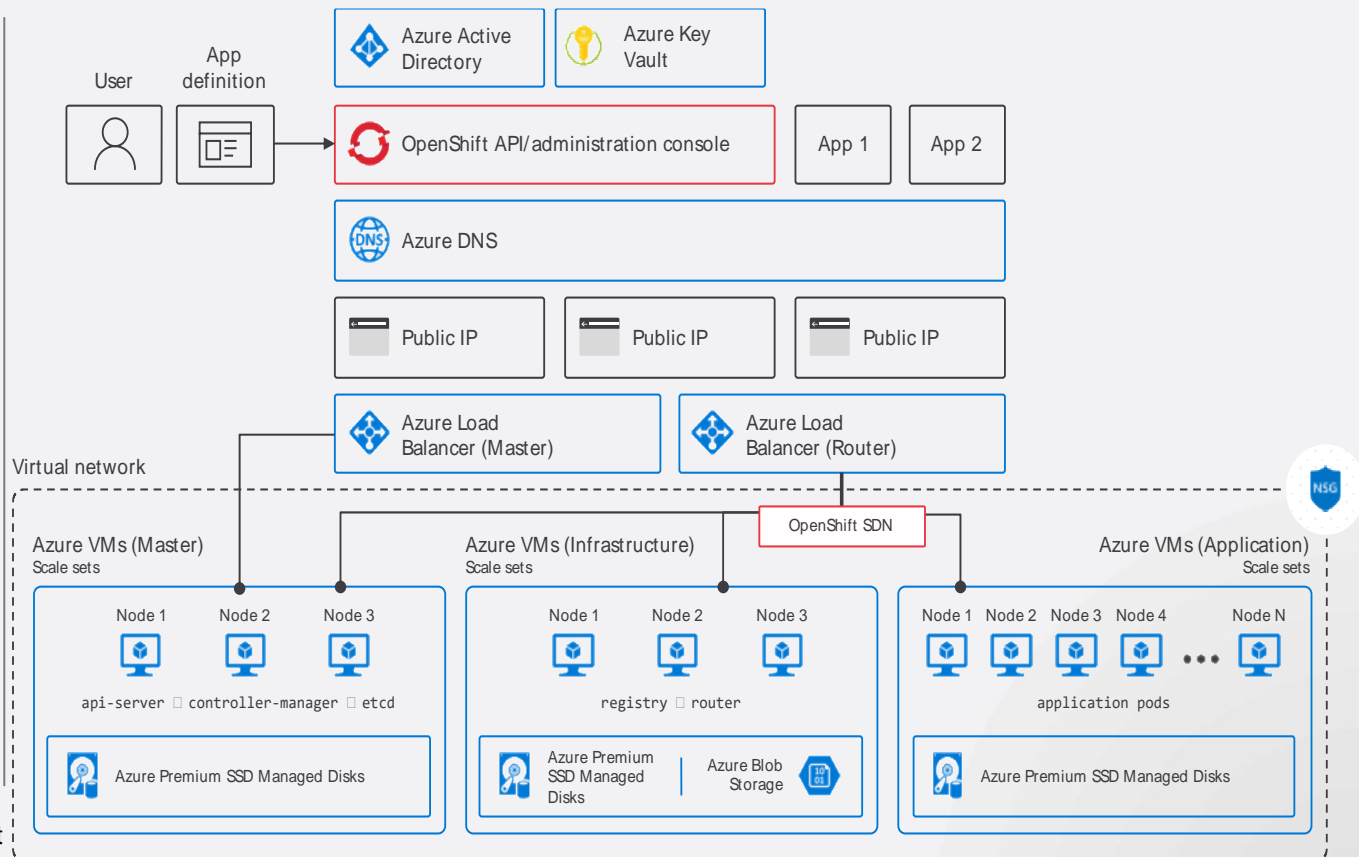
Platform support



Customer



Microsoft and Red Hat



SIMPLIFY CLUSTER OPS WITH AZURE REDHAT OPENSSHIFT

Responsibilities

User management



Project and quota management



Application lifecycle



Cluster creation



Cluster management



Monitoring and logging



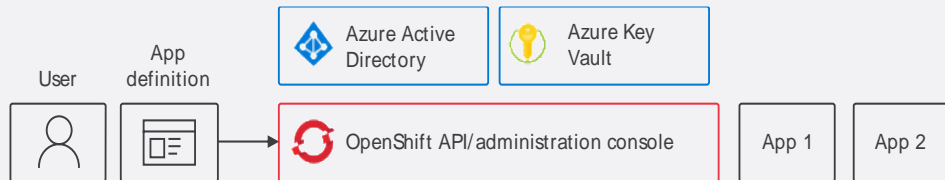
Network configuration



Software and security updates



Platform support



Let **Microsoft** and **Red Hat**...

Manage all your clusters

Monitor and operate your VMs

Secure your nodes

Manage environment patches

Customer



Microsoft and Red Hat

Setting Up OpenShift

AZURE PORTAL

- Create Tenant (if required)
- Create Application
- Create Secret

COMMAND LINE / ANSIBLE

- Create OpenShift Cluster
- Get Cluster URL and Reply URL

AZURE PORTAL

- Update Application Reply URL

OPENSIFT CONTROL PANEL

- Get Token

COMMAND LINE / ANSIBLE

- Create New Project using "oc" to create namespace
- Update Token
- Create Application

CREATE NEW TENANT FOR OPENSIFT

Microsoft Azure (Preview)

Search resources, services, and docs (G+/)

«

Create a resource

Home

Dashboard

All services

FAVORITES

Resource groups

Recovery Services vaults

Azure Database Migrati...

Azure Cosmos DB

Azure Active Directory

Virtual machines

Virtual networks

Storage accounts

Disks

Container instances

Dashboard > Create directory

Create directory

* Organization name ⓘ

Some New Non-Production Tenant ✓

* Initial domain name ⓘ

ansiblejunkie

.onmicrosoft.com

Country or region ⓘ

United States ▼

Directory creation will take about one minute.

Create

CREATE APPLICATION

[Home](#) > [Zim's Tenant - App registrations](#) > Register an application

Register an application

*** Name**

The user-facing display name for this application (this can be changed later).

✓

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Zim's Tenant only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

CREATE SECRET

Home > Zim's Tenant - App registrations > zimsapp - Certificates & secrets

zimsapp - Certificates & secrets

Search (Ctrl+J)

Overview

Quickstart

Manage

Branding

Authentication

Certificates & secrets

API permissions

Expose an API

Owners

Roles and administrators (Previous)

Manifest

Support + Troubleshooting

Troubleshooting

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

No certificates have been added for this application.

THUMBPRINT

START DATE

EXPIRES

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

New client secret

DESCRIPTION

EXPIRES

VALUE

Password uploaded on Fri Sep 13 2019




12/31/2299


1Yt*****




Setting RBAC Permissions for OpenShift


[Home](#) > [Microsoft - Overview](#) > principal-for-ansible-rbac-tests - API permissions


 principal-for-ansible-rbac-tests - API permissions  


 Overview


 Quickstart


Manage


 Branding


 Authentication


 Certificates & secrets

 API permissions


 Expose an API


 Owners


 Roles and administrators (Previ...

 Manifest

Support + Troubleshooting


 Troubleshooting

 Refresh


 Permissions have changed, please wait 10 seconds before granting admin consent. Users and/or admins will have to consent even if they have already done so previously.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

 Add a permission

Grant admin consent for Microsoft

| API / PERMISSIONS NAME | TYPE | DESCRIPTION | ADMIN CONSENT RE... | STATUS |
|------------------------------------|-------------|-------------------------------|---------------------|---|
| ▼ AuthorizationAPI (1) ... | | | | |
| user_impersonation | Delegated | Access AuthorizationAPI | - | ... |
| ▼ Azure Active Directory Grapl ... | | | | |
| Directory.Read.All | Application | Read directory data | Yes |  Not granted for Microsoft ... |
| User.Read | Delegated | Sign in and read user profile | - | ... |

OTHER OPENSIFT ON AZURE OPTIONS

OpenShift 3.x (IaaS)

- Build with Azure ARM templates –OR–
- Build with Ansible
- <https://github.com/Microsoft/openshift-container-platform>
- `az group deployment create -g ocp3-iaas --template-file openshift-iaas-deploy.json --parameters openshift-iaas-deploy.parameters.json`

OpenShift 4.x (IaaS)

- Build with Azure CLI
- Use custom installer provided by Red Hat
- <https://bit.ly/2mEqLz6>
- <https://github.com/openshift/installer/blob/master/docs/user/azure/README.md>
- <https://cloud.redhat.com/openshift/install/azure/installer-provisioned>

Replicating the environment in your Azure subscription

PREPARING THE ANSIBLE VM

Create Azure Resource Group

- `az group create -l eastus -n ansibleatl`

Create Virtual Machine

- `az vm create -g ansibleatl -n ansibleatl --public-ip-address-dns-name ansibleatl --image OpenLogic:CentOS-LVM:7-LVM:7.6.20190130 --authentication-type password --accelerated-networking true --size Standard_D2_v2 --admin-username ansibleatl`

Open Network Security Group to allow port 2112 (alternate SSH port)

- `az network nsg rule create -g ansibleatl --nsg-name ansibleatlNSG --name allow-ssh2112 --description "Allow SSH Port 2112" --access Allow --protocol Tcp --direction Inbound --priority 110 --source-address-prefix "*" --source-port-range "*" --destination-address-prefix "*" --destination-port-range "2112"`

INSTALLING ANSIBLE & THE AZURE MODULES

- `sudo pip install --upgrade pip`
- `sudo pip install ansible==2.8.5`
- `sudo pip install ansible[azure]`
- `sudo pip install docker`
- `sudo pip install --ignore-installed kubernetes`
- `sudo pip install openshift`

```
[root@ansibleatl ~]# pip install ansible[azure]
DEPRECATION: Python 2.7 will reach the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 won't
Python 2 support in pip, can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support
Requirement already satisfied: ansible[azure] in /usr/lib/python2.7/site-packages (2.8.5)
Requirement already satisfied: jinja2 in /usr/lib64/python2.7/site-packages (from ansible[azure]) (2.10.1)
Requirement already satisfied: PyYAML in /usr/lib64/python2.7/site-packages (from ansible[azure]) (3.10)
Requirement already satisfied: cryptography in /usr/lib64/python2.7/site-packages (from ansible[azure]) (2.7)
Collecting packaging (from ansible[azure])
  Downloading https://files.pythonhosted.org/packages/ec/22/630ac83e8f8a9566c4f88038447ed9e16e6f10582767a01f31c769d9a71e/
Collecting requests[security] (from ansible[azure])
  Downloading https://files.pythonhosted.org/packages/51/bd/23c926cd341ea6b7dd0b2a00aba99ae0f828be89d72b2190f27c11d4b7fb/
    |████████████████████| 61kB 19.8MB/s
Collecting azure-cli-core==2.0.35 (from ansible[azure])
  Downloading https://files.pythonhosted.org/packages/ee/81/561473d6614d15f450eba6b7c8e0e1fbbaf34bf117fe77c1188010870e24/
    |████████████████████| 92kB 26.7MB/s
Collecting azure-cli-nspkg==3.0.2 (from ansible[azure])
  Downloading https://files.pythonhosted.org/packages/7c/94/cf884b92a870422f02c3f1f86573d04d5cc1abdc2ac51b8419c7ee2e2a00/
```

CREATING A SERVICE PRINCIPAL & CONNECTING TO AZURE

- `az account list`
- `az ad sp create-for-rbac --name="stkirk-ansiblefest" --role="Contributor" --scopes="/subscriptions/x"`
- `echo "export AZURE_CLIENT_ID=" >> $HOME/.bashrc`
- `echo "export AZURE_SECRET=" >> $HOME/.bashrc`
- `echo "export AZURE_SUBSCRIPTION_ID=" >> $HOME/.bashrc`
- `echo "export AZURE_TENANT=" >> $HOME/.bashrc`

```
[stkirk@stkirk-fedora ~]$ az ad sp create-for-rbac --name="stkirk-ansiblefest" --role="Contributor" --scopes="/subscriptions/wh7e5gd8-92h4-93f7-q8d4-t56295hf73bb"
AppId                               DisplayName                         Name                                Password                           Tenant
-----
52f8ba96-21rq-7265-z383-e6ee22d6j8ea  stkirk-ansiblefest  http://stkirk-ansiblefest  72962831-2720-4hew-y297-11812e9a8f00  07f720fe-11r4-58er-84be-2d7az071ye00
```

- `source $HOME/.bashrc`

OTHER ANSIBLE MODULES FOR AZURE

- Availability Sets
 - Azure Container Instance (ACI)
 - Azure Container Registry (ACR)
 - Azure Function App
 - Azure Key Vault
 - Azure Kubernetes Service (AKS)
 - Azure Red Hat OpenShift (ARO)
 - Creating System Images
 - Load Balancers
 - Network Security Groups (NSGs)
 - SQL / MySQL / PostgreSQL (PaaS Services)
 - Virtual Machine Extension
 - Virtual Machine Scale Sets (VMSS)
-
- Azure REST API



USEFUL LINKS

Ansiblefest 2019 GitHub:

- <https://www.github.com/stuartatmicrosoft/Ansiblefest2019>

Execution Script:

- <https://github.com/stuartatmicrosoft/Ansiblefest2019/blob/master/execution-script.sh>

Azure Modules:

- <https://github.com/ansible/ansible/tree/devel/lib/ansible/modules/cloud/azure>

Visual Studio Code Extension:

- <https://marketplace.visualstudio.com/items?itemName=vscoss.vscode-ansible>

Azure Preview Modules:

- https://galaxy.ansible.com/Azure/azure_preview_modules/

USEFUL LINKS

Azure Playbook Samples

- <https://github.com/Azure-Samples/ansible-playbooks>

Ansible Labs / Stuart's GitHub

- <https://github.com/Microsoft/AnsibleLabs>
- <https://github.com/stuartatmicrosoft>

IRC

- #ansible-azure (Freenode)
- <https://webchat.freenode.net/?channels=ansible-azure>

Help us by giving us feedback:

<https://aka.ms/ansiblefest2019>



#ANSIBLEFEST2019

THANK YOU



[youtube.com/AnsibleAutomation](https://www.youtube.com/AnsibleAutomation)



facebook.com/ansibleautomation



linkedin.com/company/Red-Hat



twitter.com/ansible

Survey

<https://aka.ms/ansiblefest2019>

