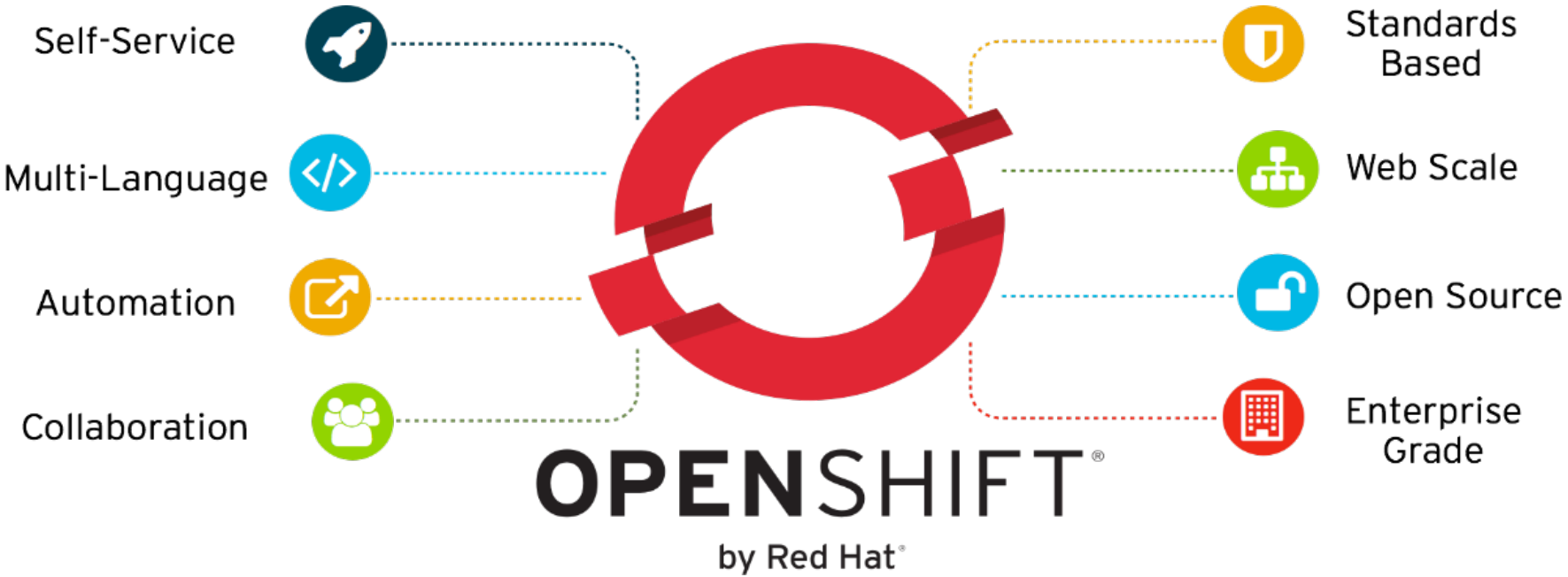
Changing the Open Hybrid Cloud Game

Deploying OpenShift to Azure

Harold Wong
Cloud Architect
Commercial Software Engineering
harold.wong@microsoft.com

redhat.

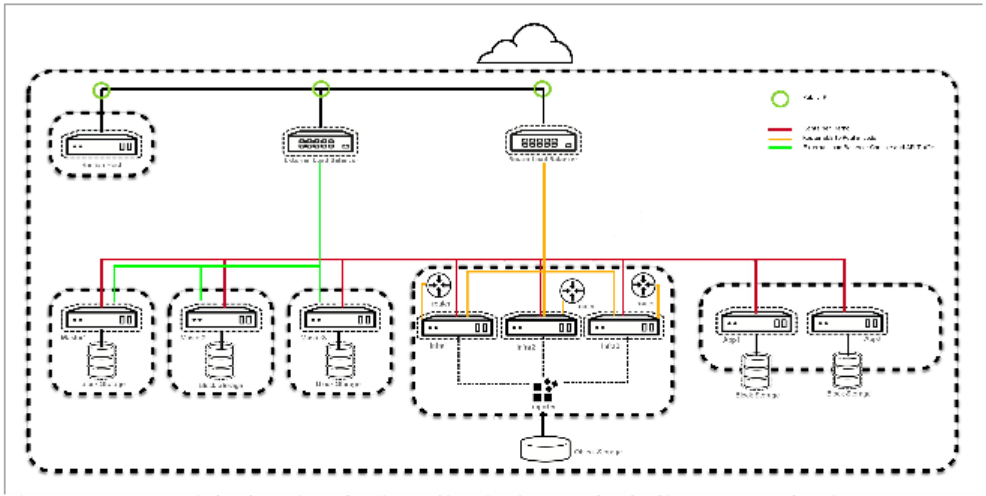
Red Hat OpenShift Container Platform



DEPLOYING RED HAT OPENSHIFT CONTAINER PLATFORM 3 ON MICROSOFT AZURE

REFERENCE ARCHITECTURES
2017

Glenn West
Ryan Cook

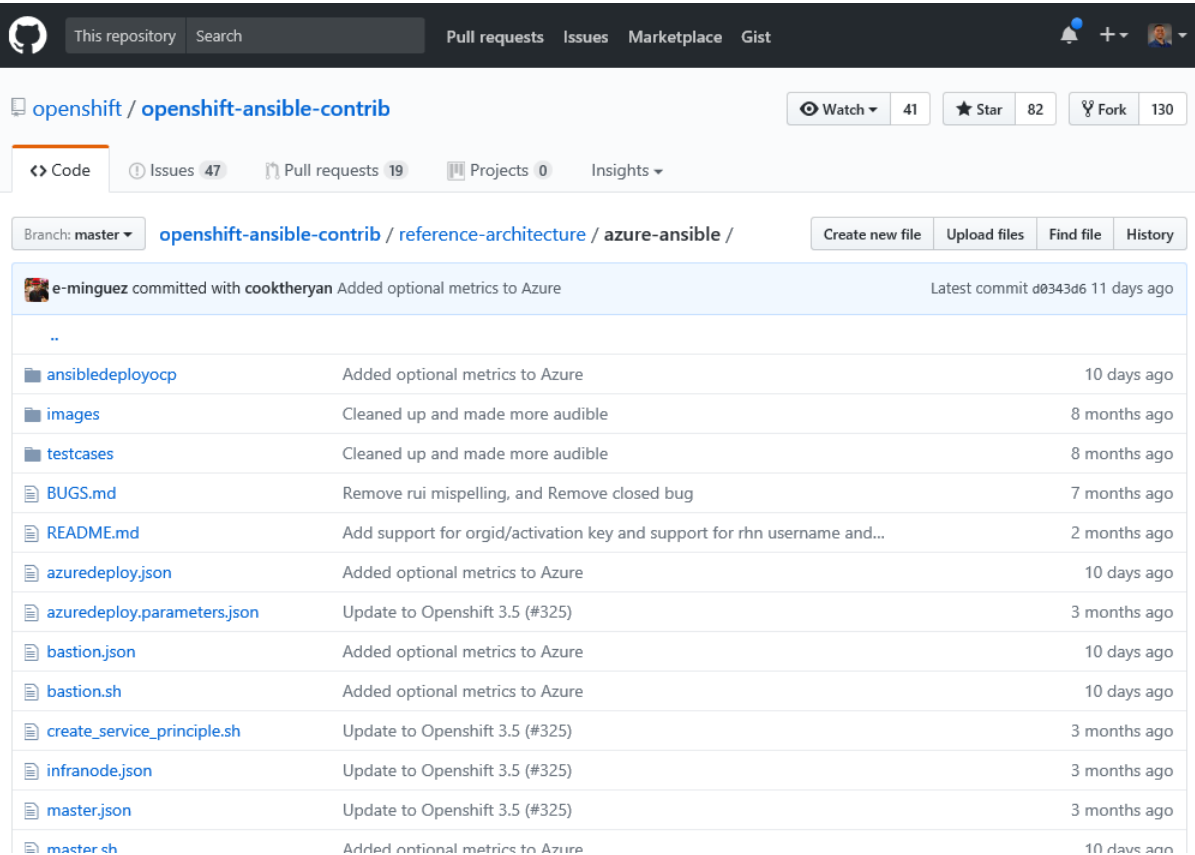


This reference architecture breaks down the deployment into three separate phases.

- Phase 1: Provision the Virtual Machines on **Microsoft Azure**
- Phase 2: Install **OpenShift Container Platform** on **Microsoft Azure**
- Phase 3: Post deployment activities

For Phase 1, the provisioning of the environment is done using a series of `Azure Resource Manager` templates (`ARM`) provided in the openshift-ansible-contrib `git` repository. Once the infrastructure is deployed by `ARM` , as the last action, the `ARM` templates will start the next phase by running a bash script that starts phase 2.

Phase 2 is the provisioning of **OpenShift Container Platform** using the ansible playbooks


This repository
Search
Pull requests
Issues
Marketplace
Gist
openshift / openshift-ansible-contrib
Watch 41
Star 82
Fork 130
Code
Issues 47
Pull requests 19
Projects 0
Insights
Branch: master
openshift-ansible-contrib / reference-architecture / azure-ansible /
Create new file
Upload files
Find file
History
e-minguez committed with cooktheryan Added optional metrics to Azure
Latest commit d0343d6 11 days ago
..
ansibledeployocp Added optional metrics to Azure 10 days ago
images Cleaned up and made more audible 8 months ago
testcases Cleaned up and made more audible 8 months ago
BUGS.md Remove rui mispelling, and Remove closed bug 7 months ago
README.md Add support for orgid/activation key and support for rhn username and... 2 months ago
azuredeploy.json Added optional metrics to Azure 10 days ago
azuredeploy.parameters.json Update to Openshift 3.5 (#325) 3 months ago
bastion.json Added optional metrics to Azure 10 days ago
bastion.sh Added optional metrics to Azure 10 days ago
create_service_principle.sh Update to Openshift 3.5 (#325) 3 months ago
infranode.json Update to Openshift 3.5 (#325) 3 months ago
master.json Update to Openshift 3.5 (#325) 3 months ago
master.sh Added optional metrics to Azure 10 days ago

README.md

Red Hat OpenShift Container Platform on Azure

When creating the Red Hat OpenShift Container Platform on Azure, you will need a SSH RSA key for access.

SSH Key Generation

1. Windows
2. Linux
3. Mac

Create the Installation

Create the Installation on the Azure Portal

Development Branch

Parameters

Parameters

For macOS:

1. SSHKeyData - Public Key - Copy/Paste from .ssh/id_rsa.pub - pbcopy < ~/.ssh/id_rsa.pub
2. PoolId - From RHEL - subscription-manager list --available
3. SSHPrivate Data - Base64 Encoded id_rsa - cat ~/.ssh/id_rsa | base64 | pbcopy

For RHEL/Fedora/CentOS:

1. SSHKeyData - Public Key - Copy/Paste from .ssh/id_rsa.pub - xclip -selection clipboard < ~/.ssh/id_rsa.pub
2. PoolId - From RHEL - subscription-manager list --available
3. SSHPrivate Data - Base64 Encoded id_rsa - cat ~/.ssh/id_rsa | base64 | xclip -selection clipboard

Input Parameters

Name	Type	Description
adminUsername	String	Username for SSH Login and OpenShift Webconsole
adminPassword	SecureString	Password for the OpenShift Webconsole
sshKeyData	String	Public SSH Key for the Virtual Machines
masterDnsName	String	DNS Prefix for the OpenShift Master / Webconsole
numberOfNodes	Integer	Number of OpenShift Nodes to create
masterVMSize	String	The size of the Master Virtual Machine

Output Parameters

Name	Type	Description
OpenShift Webconsole	String	URL of the OpenShift Webconsole
OpenShift Master ssh	String	SSH String to Login at the Master
OpenShift Router Public IP	String	Router Public IP. Needed if you want to create your own Wildcard DNS

This template deploys Red Hat OpenShift on Azure.

Attribution:

Thanks to: Daniel Falkner - Microsoft Germany - For original templates.

Harold Wong Harold.Wong@microsoft.com for his great support.

Ivan McKinley

For full commit history: Please see - https://github.com/glennswest/azure-openshift/

e-minguez Added optional metrics to Azure — d0343d6 10 days ago

5 contributors

Executable File | 1351 lines (1350 sloc) | 41.3 KB | Raw | Blame | History

```
{
  "$schema" : "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion" : "1.0.0.0",
  "parameters" : {
    "adminUsername" : {
      "type" : "string",
      "minLength" : 1,
      "metadata" : {
        "description" : "User name for the Virtual Machine and OpenShift Webconsole."
      }
    },
    "adminPassword" : {
      "type" : "securestring",
      "metadata" : {
        "description" : "User password for the OpenShift Webconsole"
      }
    },
```

```
{
  "$schema" : "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion" : "1.0.0.0",
  "parameters" : {
    "adminUsername" : {
      "type" : "string",
      "minLength" : 1,
      "metadata" : {
        "description" : "User name for the Virtual Machine and OpenShift Webconsole."
      }
    },
    "adminPassword" : {
      "type" : "securestring",
      "metadata" : {
        "description" : "User password for the OpenShift Webconsole"
      }
    },
    "sshKeyData" : {
      "type" : "securestring",
      "metadata" : {
        "description" : "SSH RSA public key file as a string."
      }
    },
    "WildcardZone" : {
      "type" : "string",
      "minLength" : 1,
      "metadata" : {
        "description" : "Globally unique wildcard DNS domain for app access."
      }
    },
    "numberOfNodes" : {
      "type" : "int",
      "defaultValue" : 3,
      "minValue" : 3,
      "maxValue" : 30,
      "metadata" : {
        "description" : "Number of OpenShift Nodes to deploy (max 30)"
      }
    },
    "image" : {
      "type" : "string",
      "allowedValues" : [
        "rhel"
      ],
      "defaultValue" : "rhel",
```

Branch: master ▾ openshift-ansible-contrib / reference-architecture / azure-ansible / azuredeploy.json

Find file | Copy path

e-minguez Added optional metrics to Azure — d0343d6 10 days ago

5 contributors

Executable File | 1351 lines (1350 sloc) | 41.3 KB

Raw | Blame | History

```
{
  "$schema" : "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion" : "1.0.0.0",
  "parameters" : {
    "adminUsername" : {
      "type" : "string",
      "minLength" : 1,
      "metadata" : {
        "description" : "User name for the Virtual Machine and OpenShift Webconsole."
      }
    },
    "adminPassword" : {
      "type" : "securestring",
      "metadata" : {
        "description" : "User password for the OpenShift Webconsole"
      }
    },
```

haroldwongms / openshift-ansible-contrib
forked from openshift/openshift-ansible-contrib

Watch 0 | Star 0 | Fork 130

Code | Pull requests 0 | Projects 0 | Settings | Insights

Additional roles and playbooks for OpenShift installation and management https://www.openshift.com

Edit

Add topics

828 commits | 8 branches | 1 release | 46 contributors

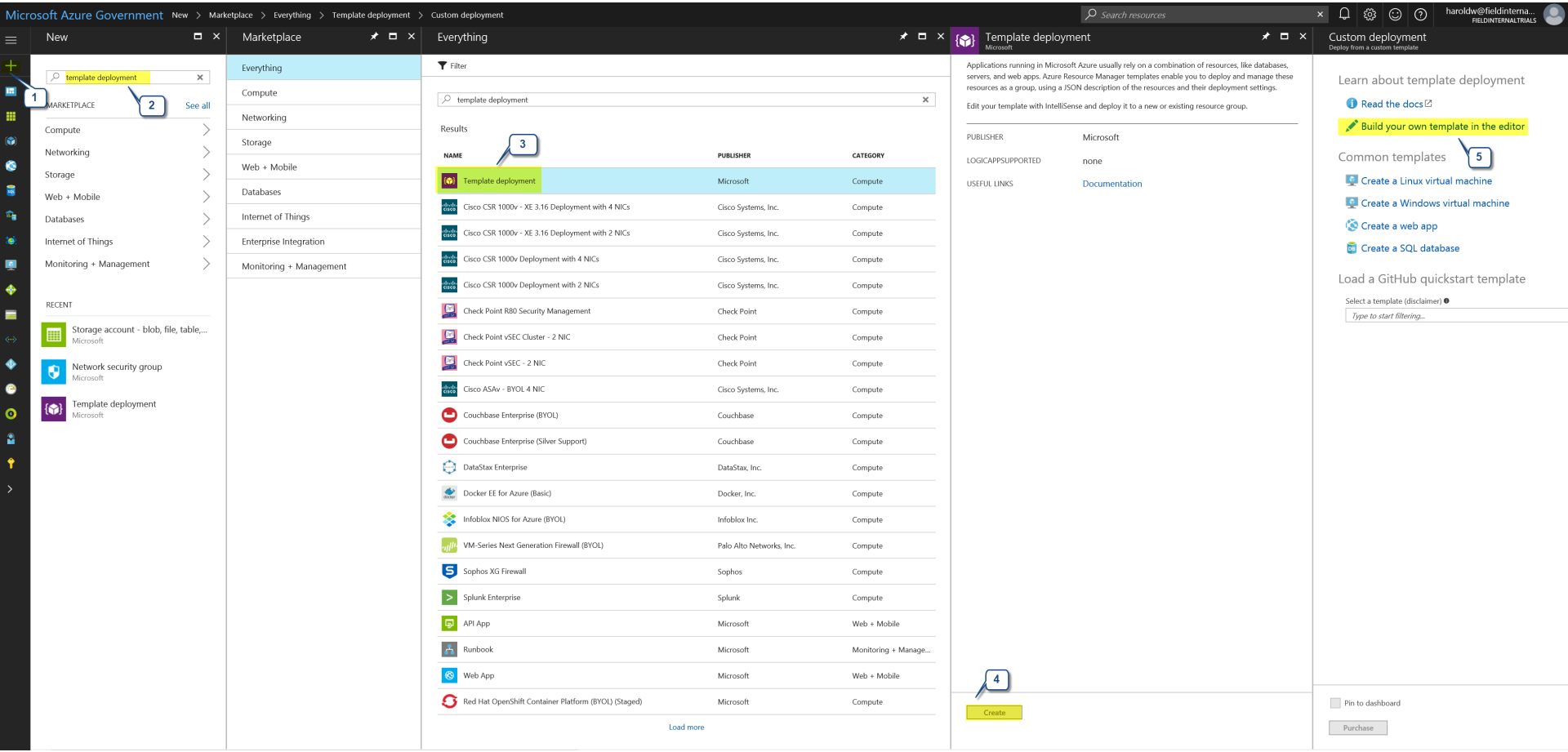
Branch: master | New pull request | Create new file | Upload files | Find file | Clone or download

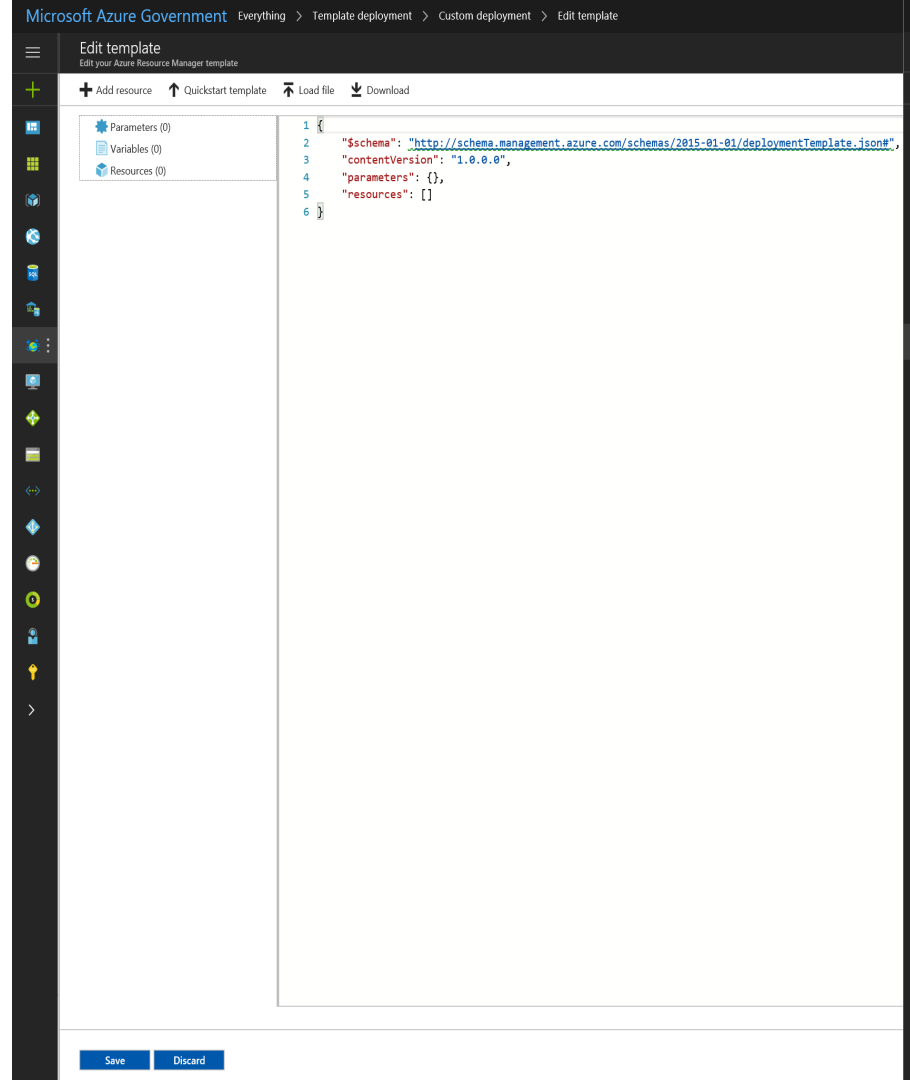
This branch is even with openshift:master. Pull request | Compare

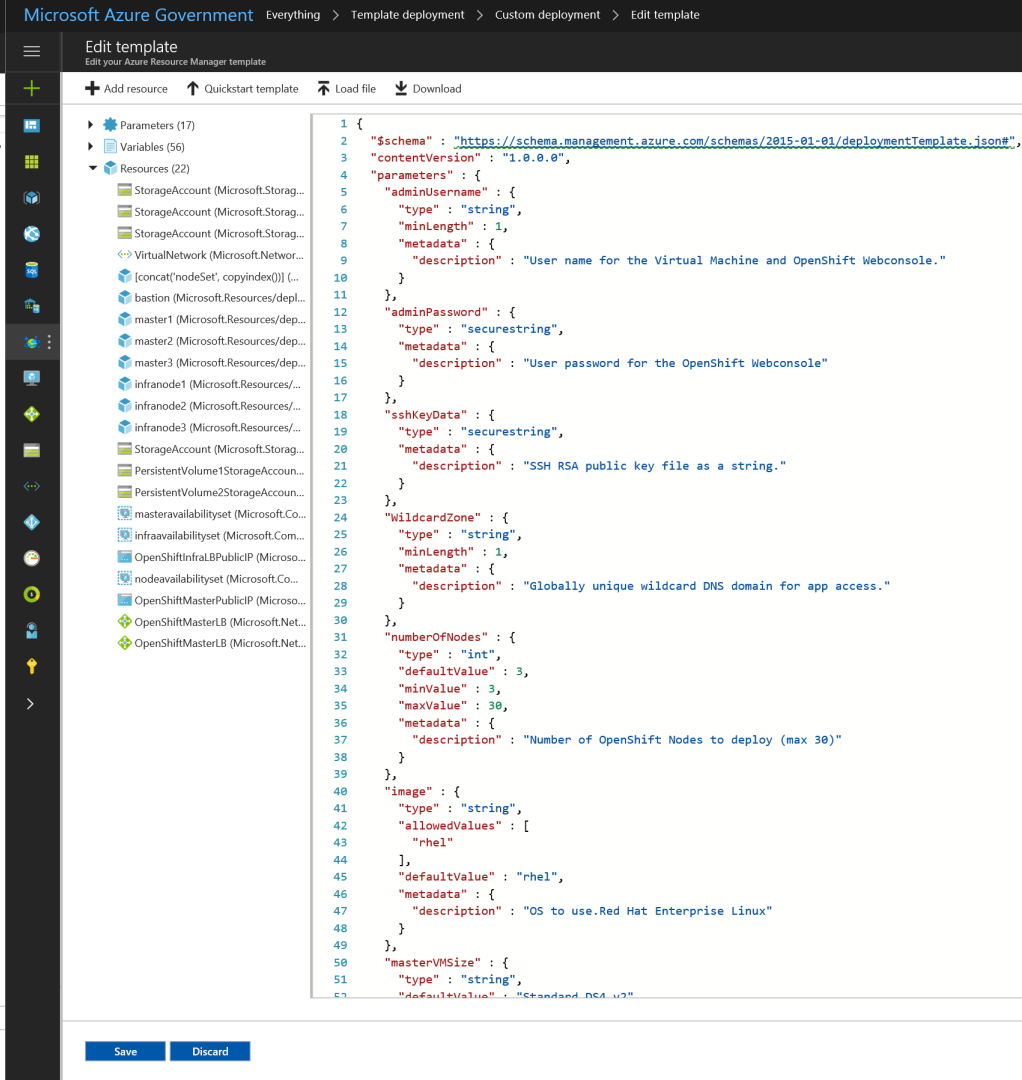
Tlacenka committed with tomassedovic Playbook prerequisites.yml checks that prerequisites are met before p... ... Latest commit a8639ab 16 hours ago

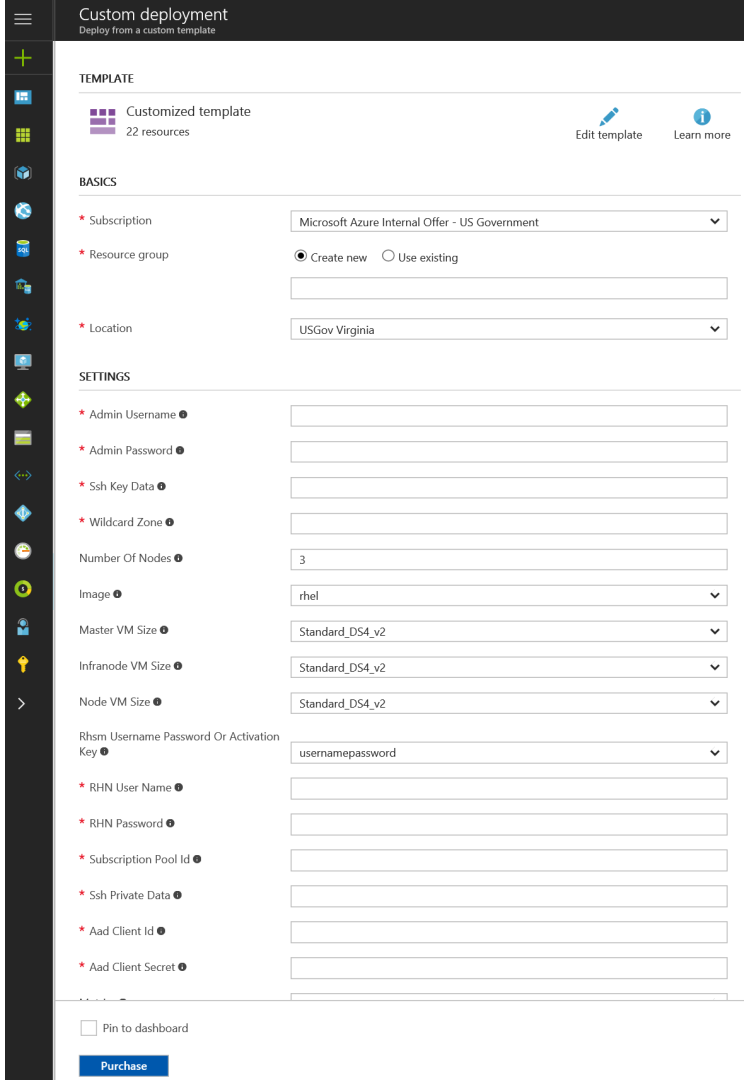
.github	Add ISSUE/PR github templates	15 days ago
inventory/aws	cleanup	a year ago
misc/gce-federation	adding more details to the README for better explanation (#458)	26 days ago
playbooks	Playbook prerequisites.yml checks that prerequisites are met before p...	16 hours ago
reference-architecture	mend	4 days ago
roles	Merge pull request #525 from bogdando/manage_packages	11 days ago
vagrant	Merge pull request #245 from chekolyn/vagrant-fix02	5 months ago
.gitignore	Replace rhsm_* with rhel_subscribe (#332)	2 months ago
.travis.yml	add travis/tox testing	6 months ago
.yamllint	add travis/tox testing	6 months ago
LICENSE.md	Initial Commit	a year ago
README.md	Update README for how to run tests	6 months ago
requirements.txt	add travis/tox testing	6 months ago
setup.cfg	Playbooks for creating a minimal gce federated cluster (#433)	28 days ago
setup.py	update setup.py to fix yamllint error	6 months ago
test-requirements.txt	add travis/tox testing	6 months ago

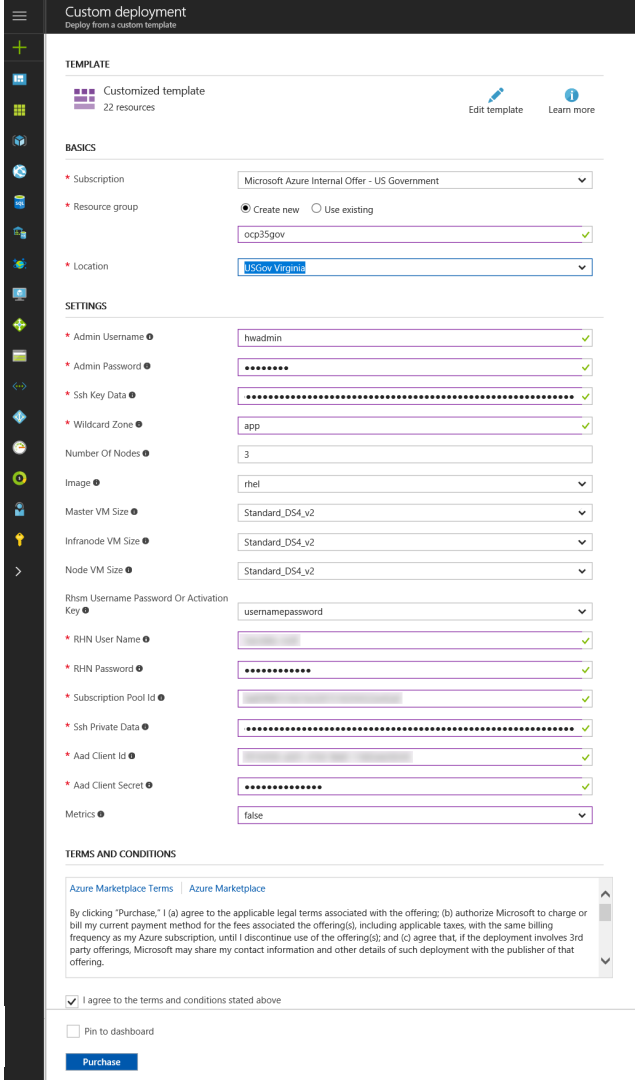
```
      "metadata" :{
        "description" : "Enable OCP metrics"
      }
    }
  },
  "variables" : {
    "gituser" : "haroldwongms",
    "branch" : "hw-azure",
    "baseTemplateUrl" : "[concat('https://raw.githubusercontent.com/',variables('gituser'),'/openshift-ansible-contrib/',variables('branch'
    "baseVMachineTemplateUriInfranode" : "[concat(variables('baseTemplateUrl'), 'infranode.json')]",
    "baseVMachineTemplateUriNode" : "[concat(variables('baseTemplateUrl'), 'node.json')]",
    "baseVMachineTemplateUriMaster" : "[concat(variables('baseTemplateUrl'), 'master.json')]",
    "location" : "[resourceGroup().location]",
    "virtualNetworkName" : "openshiftVnet",
    "addressPrefix" : "10.0.0.0/16",
    "infranodesubnetName" : "infranodeSubnet",
    "infranodesubnetPrefix" : "10.0.2.0/24",
    "nodesubnetName" : "nodeSubnet",
    "nodesubnetPrefix" : "10.0.1.0/24",
    "mastersubnetName" : "masterSubnet",
    "mastersubnetPrefix" : "10.0.0.0/24",
    "infranodeStorageName" : "[concat('sainf', resourceGroup().name)]",
    "nodeStorageName" : "[concat('sanod', resourceGroup().name)]",
    "masterStorageName" : "[concat('samas', resourceGroup().name)]",
    "vhdStorageType" : "Premium_LRS",
    "vnetId" : "[resourceId('Microsoft.Network/virtualNetworks', variables('virtualNetworkName'))]",
    "infranodeSubnetRef" : "[concat(variables('vnetId'), '/subnets/', variables('infranodesubnetName'))]",
    "nodeSubnetRef" : "[concat(variables('vnetId'), '/subnets/', variables('nodesubnetName'))]",
    "masterSubnetRef" : "[concat(variables('vnetId'), '/subnets/', variables('mastersubnetName'))]",
    "rhel" : {
```


Microsoft Azure Government
New > Marketplace > Everything > Template deployment > Custom deployment
Search resources
haroldw@fieldinterna...
FIELDINTERNALTRIALS
New
template deployment
1
2
MARKETPLACE
See all
Compute
Networking
Storage
Web + Mobile
Databases
Internet of Things
Monitoring + Management
RECENT
Storage account - blob, file, table,...
Microsoft
Network security group
Microsoft
Template deployment
Microsoft
Marketplace
Everything
Compute
Networking
Storage
Web + Mobile
Databases
Internet of Things
Enterprise Integration
Monitoring + Management
Everything
Filter
template deployment
Results
3
NAME
PUBLISHER
CATEGORY
Template deployment
Microsoft
Compute
Cisco CSR 1000v - XE 3.16 Deployment with 4 NICs
Cisco Systems, Inc.
Compute
Cisco CSR 1000v - XE 3.16 Deployment with 2 NICs
Cisco Systems, Inc.
Compute
Cisco CSR 1000v Deployment with 4 NICs
Cisco Systems, Inc.
Compute
Cisco CSR 1000v Deployment with 2 NICs
Cisco Systems, Inc.
Compute
Check Point R80 Security Management
Check Point
Compute
Check Point vSEC Cluster - 2 NIC
Check Point
Compute
Check Point vSEC - 2 NIC
Check Point
Compute
Cisco ASAv - BYOL 4 NIC
Cisco Systems, Inc.
Compute
Couchbase Enterprise (BYOL)
Couchbase
Compute
Couchbase Enterprise (Silver Support)
Couchbase
Compute
DataStax Enterprise
DataStax, Inc.
Compute
Docker EE for Azure (Basic)
Docker, Inc.
Compute
Infoblox NIOS for Azure (BYOL)
Infoblox Inc.
Compute
VM-Series Next Generation Firewall (BYOL)
Palo Alto Networks, Inc.
Compute
Sophos XG Firewall
Sophos
Compute
Splunk Enterprise
Splunk
Compute
API App
Microsoft
Web + Mobile
Runbook
Microsoft
Monitoring + Manage...
Web App
Microsoft
Web + Mobile
Red Hat OpenShift Container Platform (BYOL) (Staged)
Microsoft
Compute
Load more
Template deployment
Microsoft
Applications running in Microsoft Azure usually rely on a combination of resources, like databases, servers, and web apps. Azure Resource Manager templates enable you to deploy and manage these resources as a group, using a JSON description of the resources and their deployment settings.
Edit your template with IntelliSense and deploy it to a new or existing resource group.
PUBLISHER
Microsoft
LOGICAPPSUPPORTED
none
USEFUL LINKS
Documentation
4
Create
Custom deployment
Deploy from a custom template
Learn about template deployment
Read the docs
Build your own template in the editor
Common templates
5
Create a Linux virtual machine
Create a Windows virtual machine
Create a web app
Create a SQL database
Load a GitHub quickstart template
Select a template (disclaimer)
Type to start filtering...
Pin to dashboard
Purchase


Microsoft Azure Government
Everything
Template deployment
Custom deployment
Edit template
Edit template
Edit your Azure Resource Manager template
Add resource
Quickstart template
Load file
Download
Parameters (0)
Variables (0)
Resources (0)
{
"$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
"contentVersion": "1.0.0.0",
"parameters": {},
"resources": []
}
Save
Discard

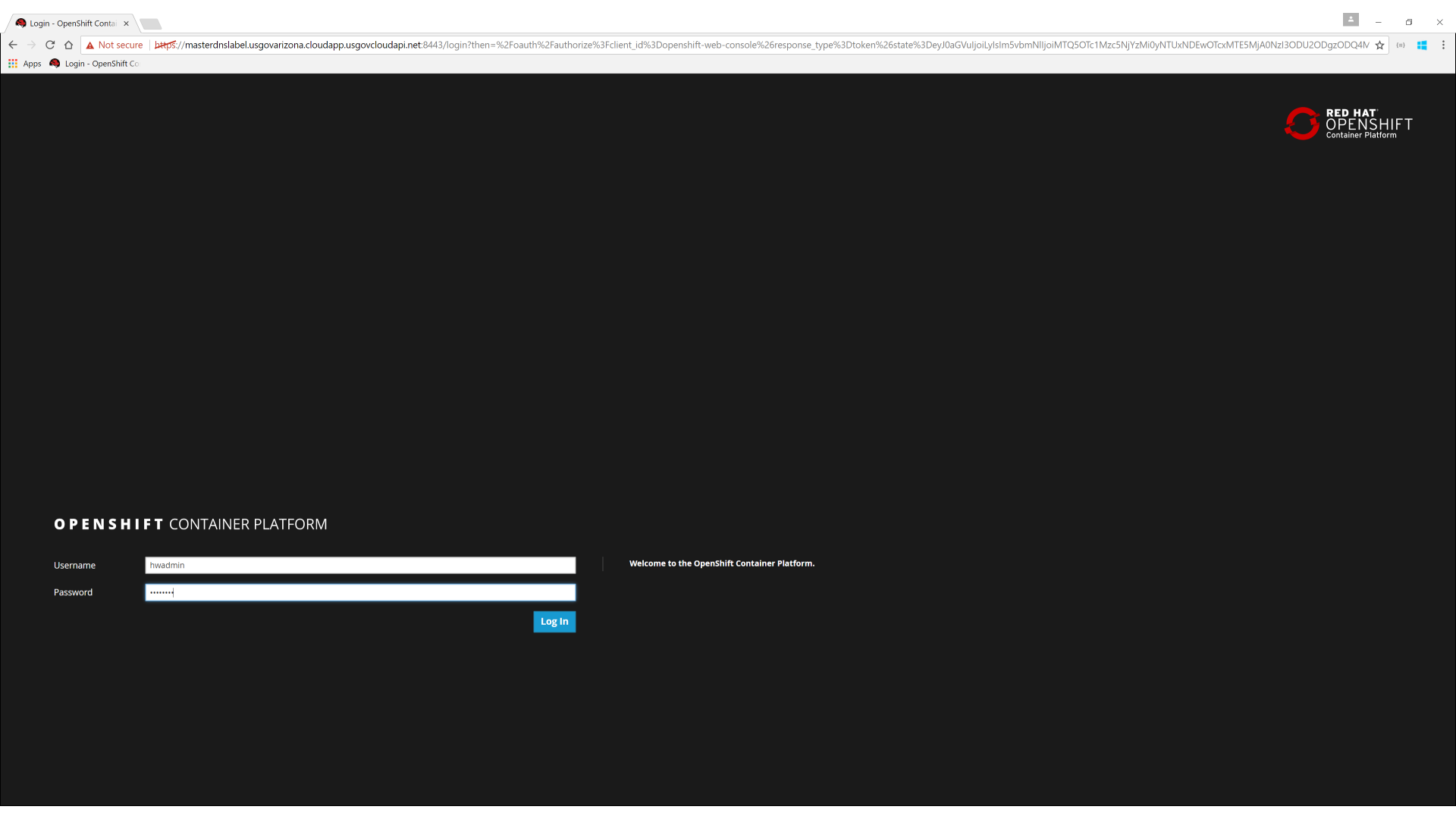

Microsoft Azure Government
Everything
Template deployment
Custom deployment
Edit template
Edit template
Edit your Azure Resource Manager template
Add resource
Quickstart template
Load file
Download
Parameters (17)
Variables (56)
Resources (22)
StorageAccount (Microsoft.Storag...
StorageAccount (Microsoft.Storag...
StorageAccount (Microsoft.Storag...
VirtualNetwork (Microsoft.Networ...
[concat('nodeSet', copyindex())] (...
bastion (Microsoft.Resources/depl...
master1 (Microsoft.Resources/dep...
master2 (Microsoft.Resources/dep...
master3 (Microsoft.Resources/dep...
infranode1 (Microsoft.Resources/...
infranode2 (Microsoft.Resources/...
infranode3 (Microsoft.Resources/...
StorageAccount (Microsoft.Storag...
PersistentVolume1StorageAccoun...
PersistentVolume2StorageAccoun...
masteravailabilityset (Microsoft.Co...
infraavailabilityset (Microsoft.Com...
OpenShiftInfraLBPublicIP (Microso...
nodeavailabilityset (Microsoft.Co...
OpenShiftMasterPublicIP (Microso...
OpenShiftMasterLB (Microsoft.Net...
OpenShiftMasterLB (Microsoft.Net...
{
"$schema" : "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
"contentVersion" : "1.0.0.0",
"parameters" : {
"adminUsername" : {
"type" : "string",
"minLength" : 1,
"metadata" : {
"description" : "User name for the Virtual Machine and OpenShift Webconsole."
}
},
"adminPassword" : {
"type" : "securestring",
"metadata" : {
"description" : "User password for the OpenShift Webconsole"
}
},
"sshKeyData" : {
"type" : "securestring",
"metadata" : {
"description" : "SSH RSA public key file as a string."
}
},
"WildcardZone" : {
"type" : "string",
"minLength" : 1,
"metadata" : {
"description" : "Globally unique wildcard DNS domain for app access."
}
},
"numberOfNodes" : {
"type" : "int",
"defaultValue" : 3,
"minValue" : 3,
"maxValue" : 30,
"metadata" : {
"description" : "Number of OpenShift Nodes to deploy (max 30)"
}
},
"image" : {
"type" : "string",
"allowedValues" : [
"rhel"
],
"defaultValue" : "rhel",
"metadata" : {
"description" : "OS to use.Red Hat Enterprise Linux"
}
},
"masterVMSize" : {
"type" : "string",
Save
Discard

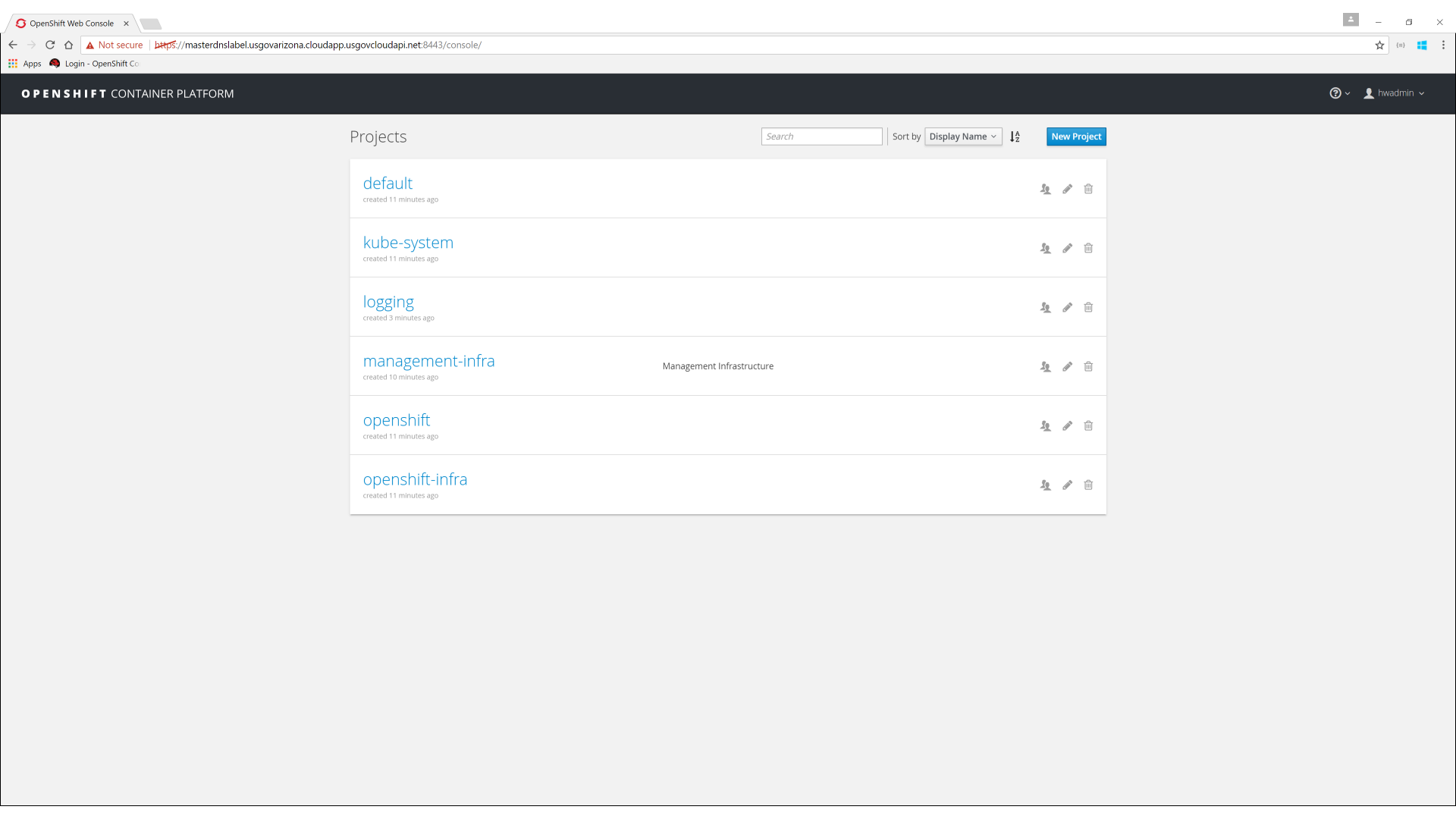

Custom deployment
Deploy from a custom template
TEMPLATE
Customized template
22 resources
Edit template
Learn more
BASICS
* Subscription
Microsoft Azure Internal Offer - US Government
* Resource group
Create new
Use existing
* Location
USGov Virginia
SETTINGS
* Admin Username
* Admin Password
* Ssh Key Data
* Wildcard Zone
Number Of Nodes
3
Image
rhel
Master VM Size
Standard_DS4_v2
Infranode VM Size
Standard_DS4_v2
Node VM Size
Standard_DS4_v2
Rhsm Username Password Or Activation Key
usernamepassword
* RHN User Name
* RHN Password
* Subscription Pool Id
* Ssh Private Data
* Aad Client Id
* Aad Client Secret
Pin to dashboard
Purchase

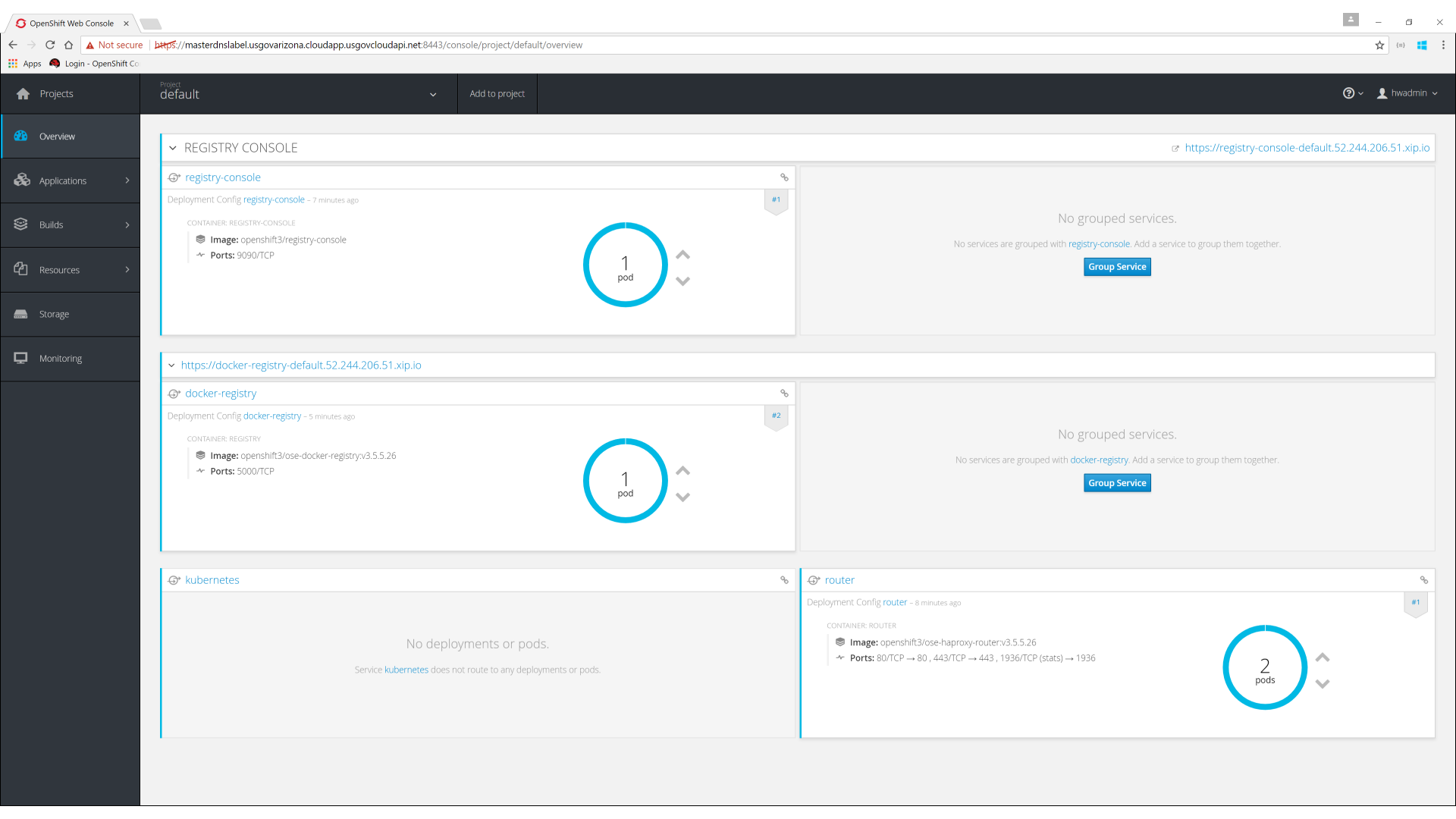

Custom deployment
Deploy from a custom template
TEMPLATE
Customized template
22 resources
Edit template
Learn more
BASICS
* Subscription
Microsoft Azure Internal Offer - US Government
* Resource group
Create new
Use existing
ocp35gov
* Location
USGov Virginia
SETTINGS
* Admin Username
hwadmin
* Admin Password
* Ssh Key Data
* Wildcard Zone
app
Number Of Nodes
3
Image
rhel
Master VM Size
Standard_DS4_v2
Infranode VM Size
Standard_DS4_v2
Node VM Size
Standard_DS4_v2
Rhsm Username Password Or Activation Key
usernamepassword
* RHN User Name
* RHN Password
* Subscription Pool Id
* Ssh Private Data
* Aad Client Id
* Aad Client Secret
Metrics
false
TERMS AND CONDITIONS
Azure Marketplace Terms
Azure Marketplace
By clicking "Purchase," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.
I agree to the terms and conditions stated above
Pin to dashboard
Purchase

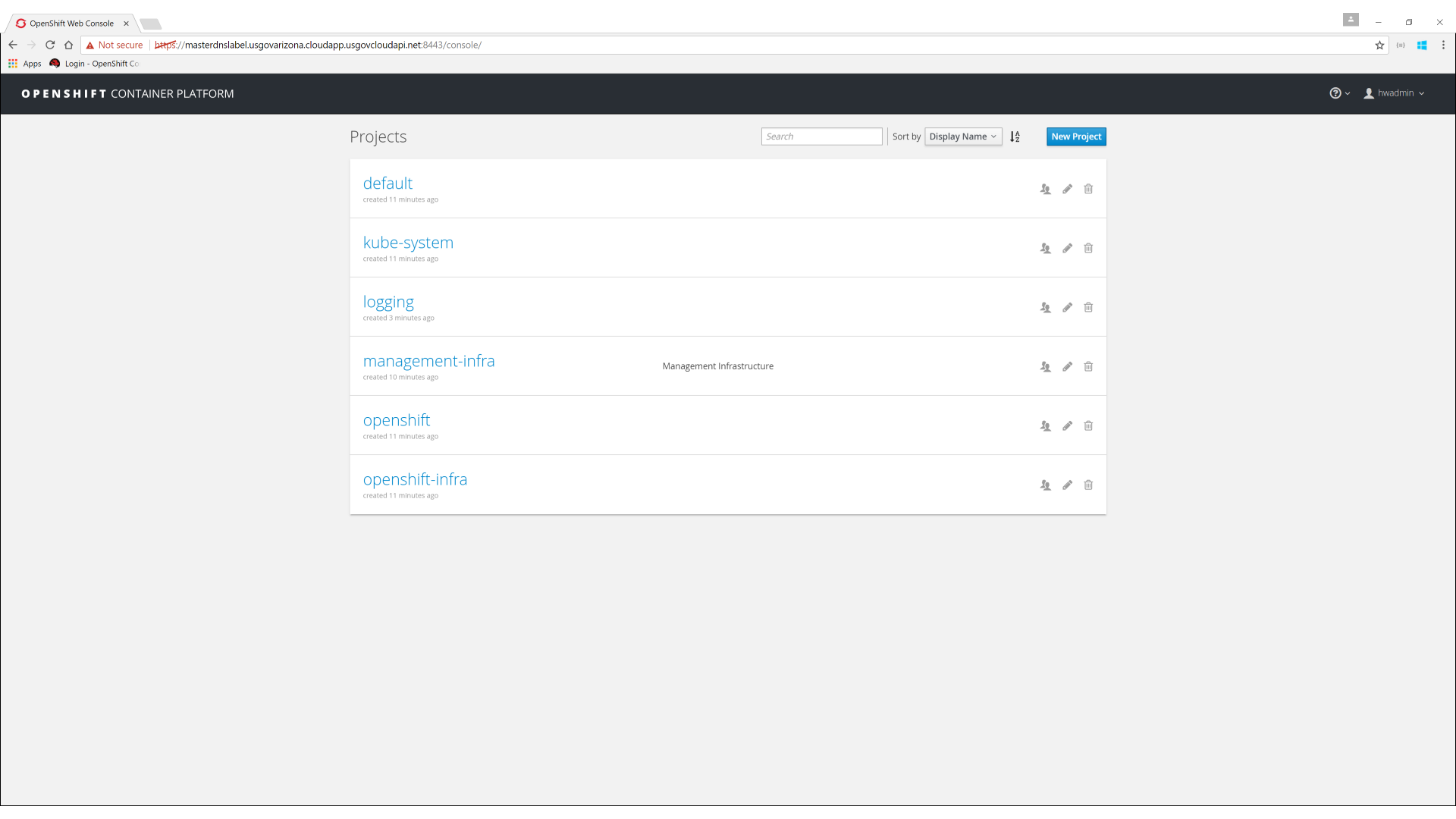
Outputs

OPENSHIFT CONSOLE URL	https://masterdnslabel.usgovarizona.cloudapp.usgovc...
BASTION DNS FQDN	bastiondnsnsmu3kfcdmuda.usgovarizona.cloudapp.us...
OPENSHIFT MASTER SSH	ssh hwadmin@masterdnslabel.usgovarizona.cloudapp...


Login - OpenShift Contai
Not secure
https://masterdnslabel.usgovarizona.cloudapp.usgovcloudapi.net:8443/login?then=%2Foauth%2Fauthorize%3Fclient_id%3Dopenshift-web-console%26response_type%3Dtoken%26state%3DeyJ0aGVuIjoiLyIsIm5vbmNlIjoiMTQ5OTc1Mzc5NjYzMi0yNTUxNDEwOTcxMTE5MjA0NzI3ODU2ODgzODQ4M
Apps
Login - OpenShift Co
RED HAT
OPENSHIFT
Container Platform
OPENSHIFT CONTAINER PLATFORM
Username
hwadmin
Password
Log In
Welcome to the OpenShift Container Platform.


OpenShift Web Console
Not secure
https://masterdnslabel.usgovarizona.cloudapp.usgovcloudapi.net:8443/console/
Apps
Login - OpenShift Co
OPENSHIFT CONTAINER PLATFORM
hwadmin
Projects
Search
Sort by
Display Name
New Project
default
created 11 minutes ago
kube-system
created 11 minutes ago
logging
created 3 minutes ago
management-infra
created 10 minutes ago
Management Infrastructure
openshift
created 11 minutes ago
openshift-infra
created 11 minutes ago


OpenShift Web Console
Not secure
https://masterdnslabel.usgovarizona.cloudapp.usgovcloudapi.net:8443/console/project/default/overview
Apps
Login - OpenShift Co
Projects
Project
default
Add to project
hwadmin
Overview
Applications
Builds
Resources
Storage
Monitoring
REGISTRY CONSOLE
https://registry-console-default.52.244.206.51.xip.io
registry-console
Deployment Config registry-console – 7 minutes ago
#1
CONTAINER: REGISTRY-CONSOLE
Image: openshift3/registry-console
Ports: 9090/TCP
1
pod
No grouped services.
No services are grouped with registry-console. Add a service to group them together.
Group Service
https://docker-registry-default.52.244.206.51.xip.io
docker-registry
Deployment Config docker-registry – 5 minutes ago
#2
CONTAINER: REGISTRY
Image: openshift3/ose-docker-registry:v3.5.5.26
Ports: 5000/TCP
1
pod
No grouped services.
No services are grouped with docker-registry. Add a service to group them together.
Group Service
kubernetes
No deployments or pods.
Service kubernetes does not route to any deployments or pods.
router
Deployment Config router – 8 minutes ago
#1
CONTAINER: ROUTER
Image: openshift3/ose-haproxy-router:v3.5.5.26
Ports: 80/TCP → 80 , 443/TCP → 443 , 1936/TCP (stats) → 1936
2
pods


OpenShift Web Console
Not secure
https://masterdnslabel.usgovarizona.cloudapp.usgovcloudapi.net:8443/console/
Apps
Login - OpenShift Co
OPENSHIFT CONTAINER PLATFORM
hwadmin
Projects
Search
Sort by
Display Name
New Project
default
created 11 minutes ago
kube-system
created 11 minutes ago
logging
created 3 minutes ago
management-infra
created 10 minutes ago
Management Infrastructure
openshift
created 11 minutes ago
openshift-infra
created 11 minutes ago

New Project

* Name

govtest

A unique name for the project.

Display Name

My Project

Description

A short description.

Create Cancel

Browse Catalog | Deploy Image | Import YAML / JSON

Choose from web frameworks, databases, and other components to add content to your project.

Filter by name or description

Languages

- Java
- JavaScript
- .NET
- Perl
- PHP
- Python
- Ruby

Technologies

Business Process Services

Model, automate, and orchestrate business processes across applications, services, and data.

Continuous Integration & Deployment

Automate the build, test, and deployment of your application with each new code revision.

Data Stores

Store and manage collections of data.

Messaging

Facilitate communication between applications and distributed processes with a messaging server.

Single Sign-On

A centralized authentication server for users to log in, log out, register, and manage user accounts for applications and RESTful web services.

Uncategorized

PHP

Filter by name or description

PHP

BUILDS SOURCE CODE

Build and run PHP 7.0 applications on RHEL 7. For more information about using this builder image, including OpenShift considerations, see https://github.com/sclorg/s2i-php-container/blob/master/7.0/R...

Version

7.0 — latest

Select

CakePHP + MySQL (Ephemeral)

An example CakePHP application with a MySQL database. For more information about using this template, including OpenShift considerations, see https://github.com/openshift/cakephp-ex/blob/master/README...

Select

CakePHP + MySQL (Persistent)

An example CakePHP application with a MySQL database. For more information about using this template, including OpenShift considerations, see https://github.com/openshift/cakephp-ex/blob/master/README...

Select

default

* Database User

cakephp

Database Password

(generated if empty)

CakePHP secret token

(generated if empty)

Set this to a long random string.

CakePHP Security Salt

(generated if empty)

Security salt for session hash.

CakePHP Security Cipher Seed

(generated if empty)

Security cipher seed for session hash.

OPcache Revalidation Frequency

2

How often to check script timestamps for updates, in seconds. 0 will result in OPcache checking for updates on every request.

Custom Composer Mirror URL

The custom Composer mirror URL

Labels

About Labels

The following labels are being added automatically. If you want to override them, you can do so below.

template | cakephp-mysql-example

app | cakephp-mysql-example

Each label is applied to each created resource.

Name | *Value* ×

Add Label

Create Cancel

Application created. Continue to overview.

The following service(s) have been created in your project: cakephp-mysql-example, mysql.

For more information about using this template, including OpenShift considerations, see https://github.com/openshift/cake-ex/blob/master/README.md.

Manage your app

The web console is convenient, but if you need deeper control you may want to try our command line tools.

Command line tools

Download and install the `oc` command line tool. After that, you can start by logging in, switching to this particular project, and displaying an overview of it, by doing:

```
oc login https://masterdnslabel.usgovarizona.cloudapp.usgovcloudapi.net:8443
oc project govtest
oc status
```

For more information about the command line tools, check the CLI Reference and Basic CLI Operations.

Making code changes

A GitHub webhook trigger has been created for the **cakephp-mysql-example** build config.

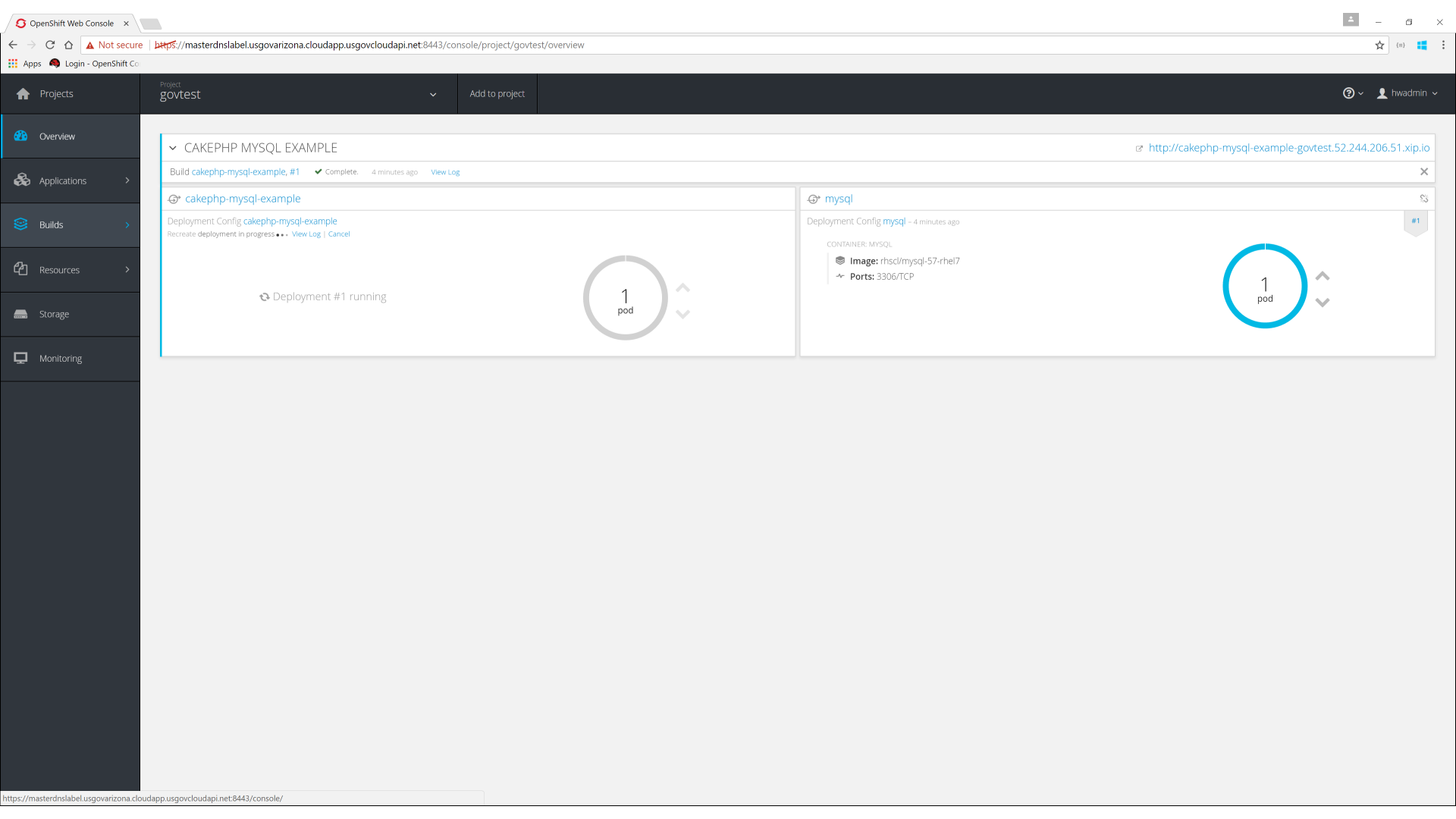
You can now set up the webhook in the GitHub repository settings if you own it, in https://github.com/openshift/cakephp-ex/settings/hooks, using the following payload URL:

https://masterdnslabel.usgovarizona.cloud

Applied Parameter Values

These parameters often include things like passwords. If you will need to reference these values later, copy them to a safe location. Parameters SOURCE_REPOSITORY_REF, CONTEXT_DIR, APPLICATION_DOMAIN, GITHUB_WEBHOOK_SECRET, DATABASE_PASSWORD, CAKEPHP_SECRET_TOKEN, CAKEPHP_SECURITY_SALT, CAKEPHP_SECURITY_CIPHER_SEED, COMPOSER_MIRROR were generated automatically.

Show parameter values


OpenShift Web Console
Not secure
https://masterdnslabel.usgovarizona.cloudapp.usgovcloudapi.net:8443/console/project/govtest/overview
Apps
Login - OpenShift Co
Projects
Project
govtest
Add to project
hwadmin
Overview
Applications
Builds
Resources
Storage
Monitoring
CAKEPHP MYSQL EXAMPLE
http://cakephp-mysql-example-govtest.52.244.206.51.xip.io
Build cakephp-mysql-example, #1
Complete.
4 minutes ago
View Log
cakephp-mysql-example
Deployment Config cakephp-mysql-example
Recreate deployment in progress
View Log | Cancel
Deployment #1 running
1
pod
mysql
Deployment Config mysql - 4 minutes ago
#1
CONTAINER: MYSQL
Image: rhscl/mysql-57-rhel7
Ports: 3306/TCP
1
pod
https://masterdnslabel.usgovarizona.cloudapp.usgovcloudapi.net:8443/console/

OpenShift Web Console

Not secure | https://masterdnslabel.usgovarizona.cloudapp.usgovcloudapi.net:8443/console/project/govtest/overview

Apps | Login - OpenShift Co

Projects

Overview

Applications

Builds

Resources

Storage

Monitoring

Project
govtest

Add to project

hwadmin

CAKEPHP MYSQL EXAMPLE

http://cakephp-mysql-example-govtest.52.244.206.51.xip.io

Build cakephp-mysql-example, #1 ✔ Complete. 5 minutes ago View Log

cakephp-mysql-example

Deployment Config cakephp-mysql-example – 2 minutes ago #1

CONTAINER: CAKEPHP-MYSQL-EXAMPLE

Image: govtest/cakephp-mysql-example

Ports: 8080/TCP

1 pod

mysql

Deployment Config mysql – 5 minutes ago #1

CONTAINER: MYSQL

Image: rhscl/mysql-57-rhel7

Ports: 3306/TCP

1 pod

11:37 PM
7/10/2017

Welcome to your CakePHP application on OpenShift

How to use this example application

For instructions on how to use this application with OpenShift, start by reading the Developer Guide.

Deploying code changes

The source code for this application is available to be forked from the OpenShift GitHub repository. You can configure a webhook in your repository to make OpenShift automatically start a build whenever you push your code:

1. From the Web Console homepage, navigate to your project
2. Click on Browse > Builds
3. Click the link with your BuildConfig name
4. Click the Configuration tab
5. Click the "Copy to clipboard" icon to the right of the "GitHub webhook URL" field
6. Navigate to your repository on GitHub and click on repository settings > webhooks > Add webhook
7. Paste your webhook URL provided by OpenShift
8. Leave the defaults for the remaining fields — that's it!

After you save your webhook, if you refresh your settings page you can see the status of the ping that Github sent to OpenShift to verify it can reach the server.

Note: adding a webhook requires your OpenShift server to be reachable from GitHub.

Working in your local Git repository

If you forked the application from the OpenShift GitHub example, you'll need to manually clone the repository to your local system. Copy the application's source code Git URL and then run:

```
$ git clone <git_url> <directory_to_create>

# Within your project directory
# Commit your changes and push to OpenShift

$ git commit -a -m 'Some commit message'
$ git push
```

After pushing changes, you'll need to manually trigger a build if you did not setup a webhook as described above.

Expanding on sample app

In order to access the original CakePHP application, you have to remove the app/View/Layouts/default.ctp file which serves as the welcome page and rename the default.ctp.default to default.ctp.

Managing your application

Documentation on how to manage your application from the Web Console or Command Line is available at the Developer Guide.

Web Console

You can use the Web Console to view the state of your application components and launch new builds.

Command Line

With the OpenShift command line interface (CLI), you can create applications and manage projects from a terminal.

Development Resources

- OpenShift Documentation
- Openshift Origin GitHub
- Source To Image GitHub
- Getting Started with PHP on OpenShift
- Stack Overflow questions for OpenShift
- Git documentation

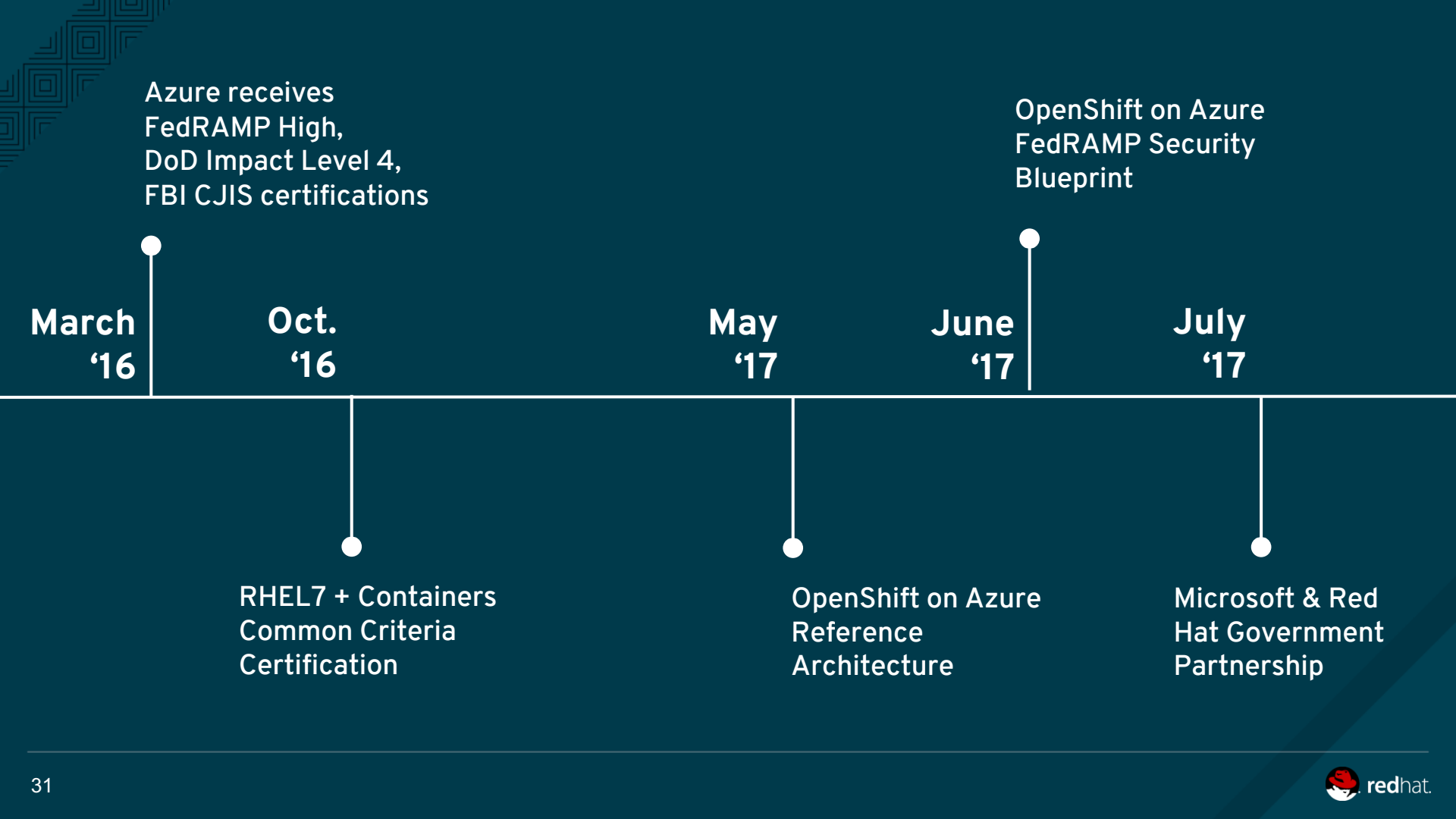
Request information

Page view count: 9

Accrediting OpenShift On Azure

Shawn Wells
Office of the Chief Technologist
U.S. Public Sector
shawn@redhat.com || 443-534-0130

redhat.


Azure receives FedRAMP High, DoD Impact Level 4, FBI CJIS certifications
OpenShift on Azure FedRAMP Security Blueprint
March '16
Oct. '16
May '17
June '17
July '17
RHEL7 + Containers Common Criteria Certification
OpenShift on Azure Reference Architecture
Microsoft & Red Hat Government Partnership

Azure for Government Certifications

DoD Impact Level 4

ITAR Readiness

FedRAMP High

- Allows all DoD and mission partners to leverage Azure for “Controlled Unclassified Information”
- aka “FOUO”

Azure for Government Certifications

DoD Impact Level 4

ITAR Readiness

FedRAMP High

- Store and process regulated data.
- Azure facilities and personnel US-based.

Azure for Government Certifications

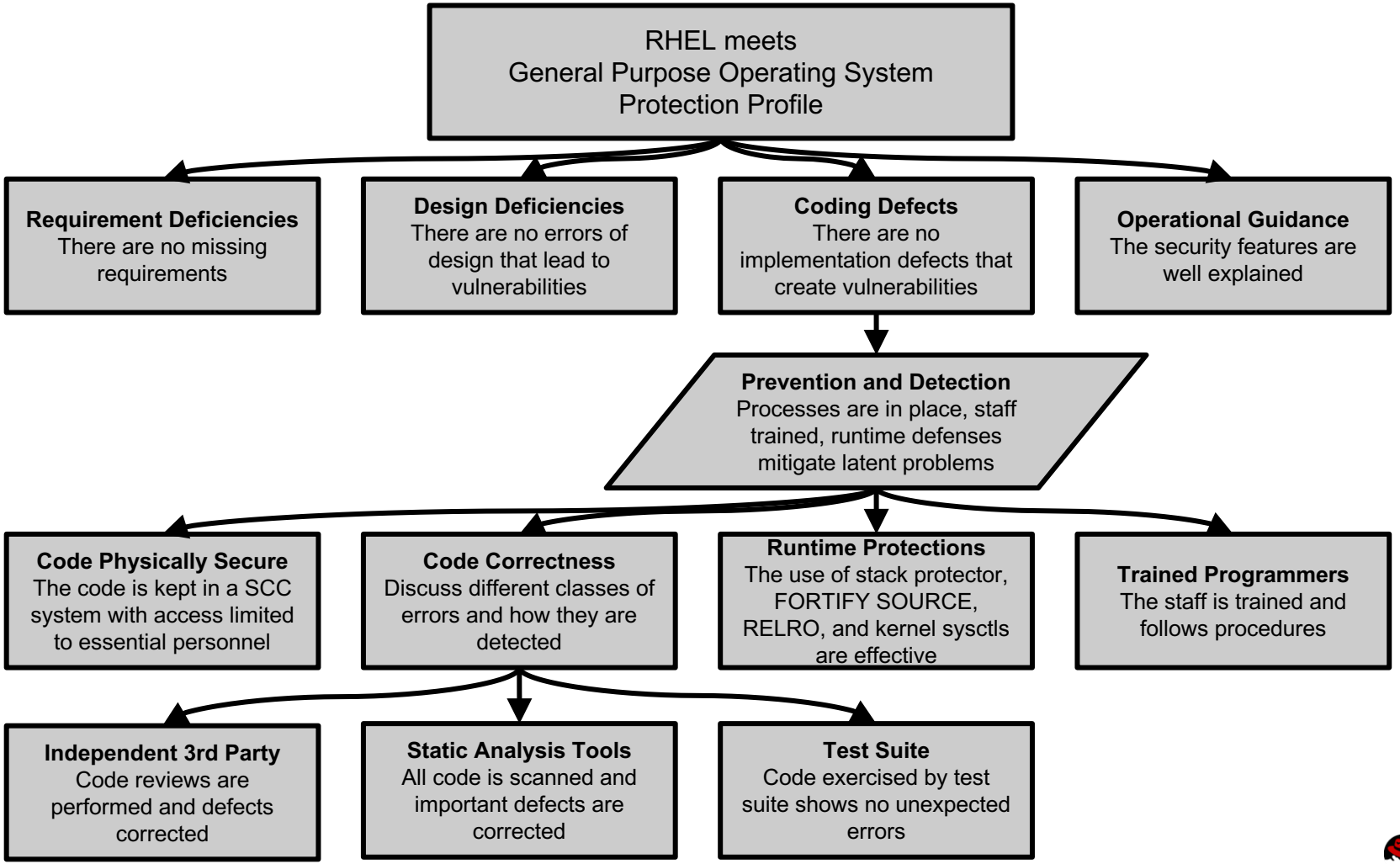
DoD Impact Level 4
ITAR Readiness
FedRAMP High

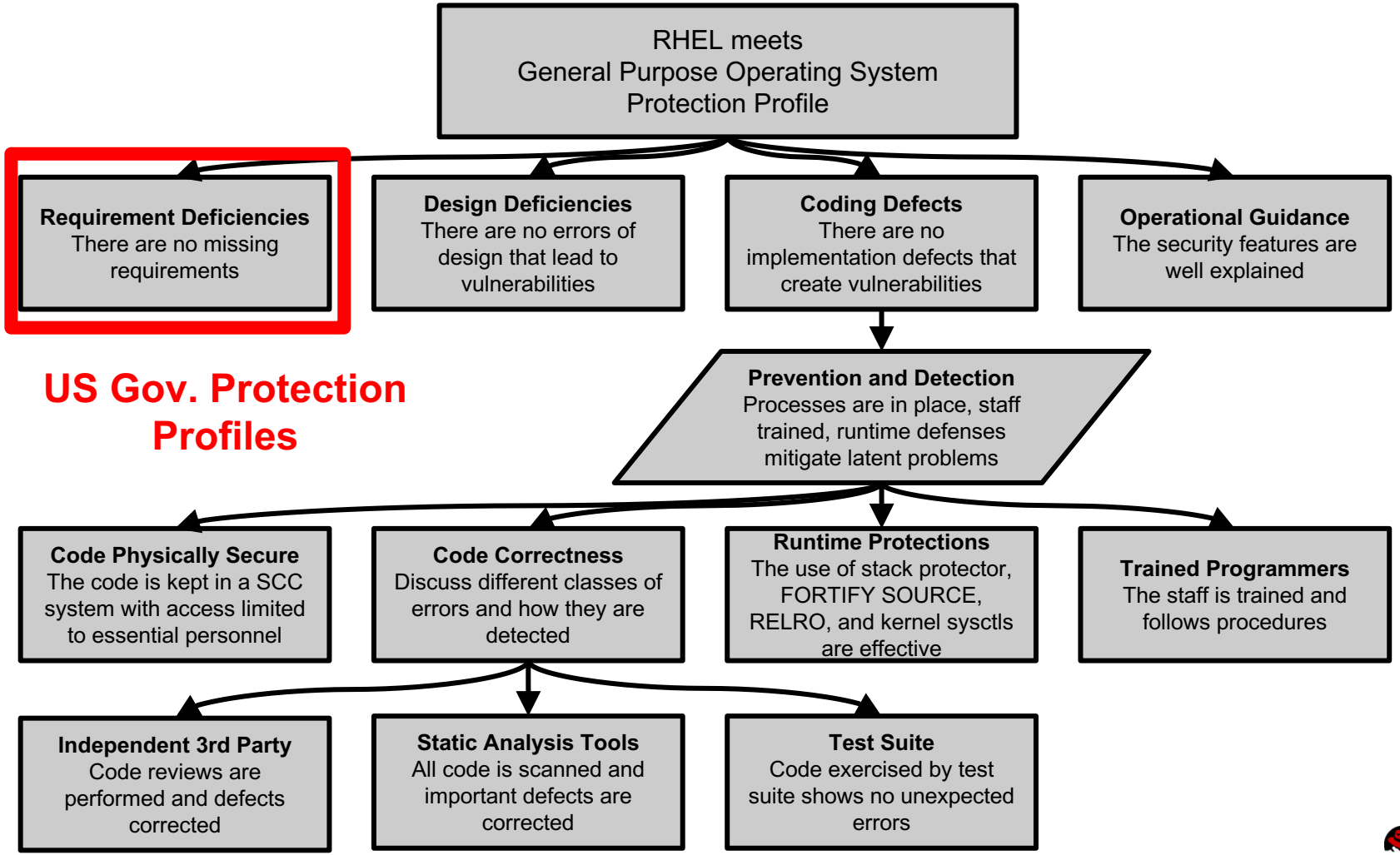
- Focus for today.
- GSA-estimated 50% of $80B Federal IT budget falls under ‘FedRAMP High’

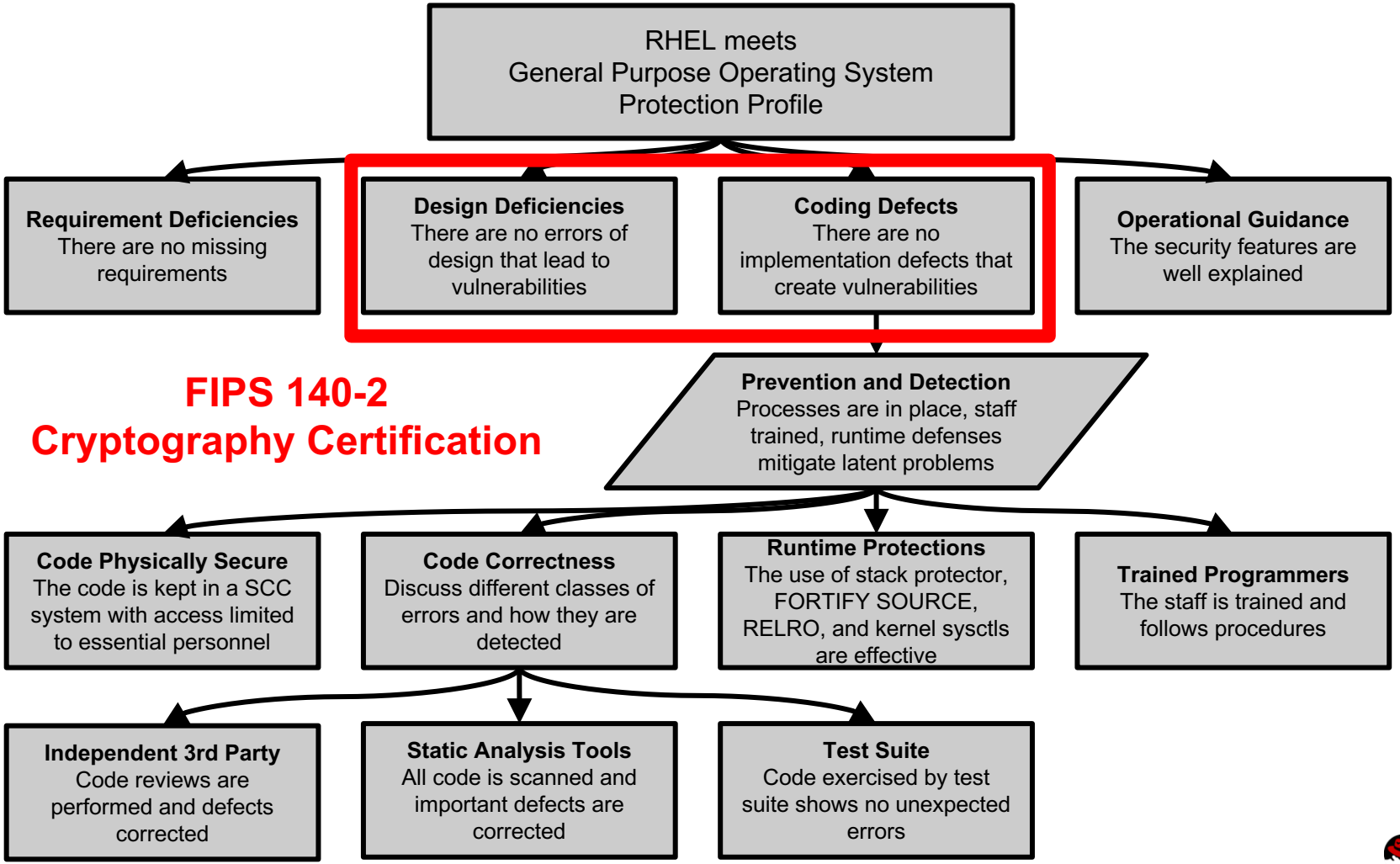
Red Hat Certifications

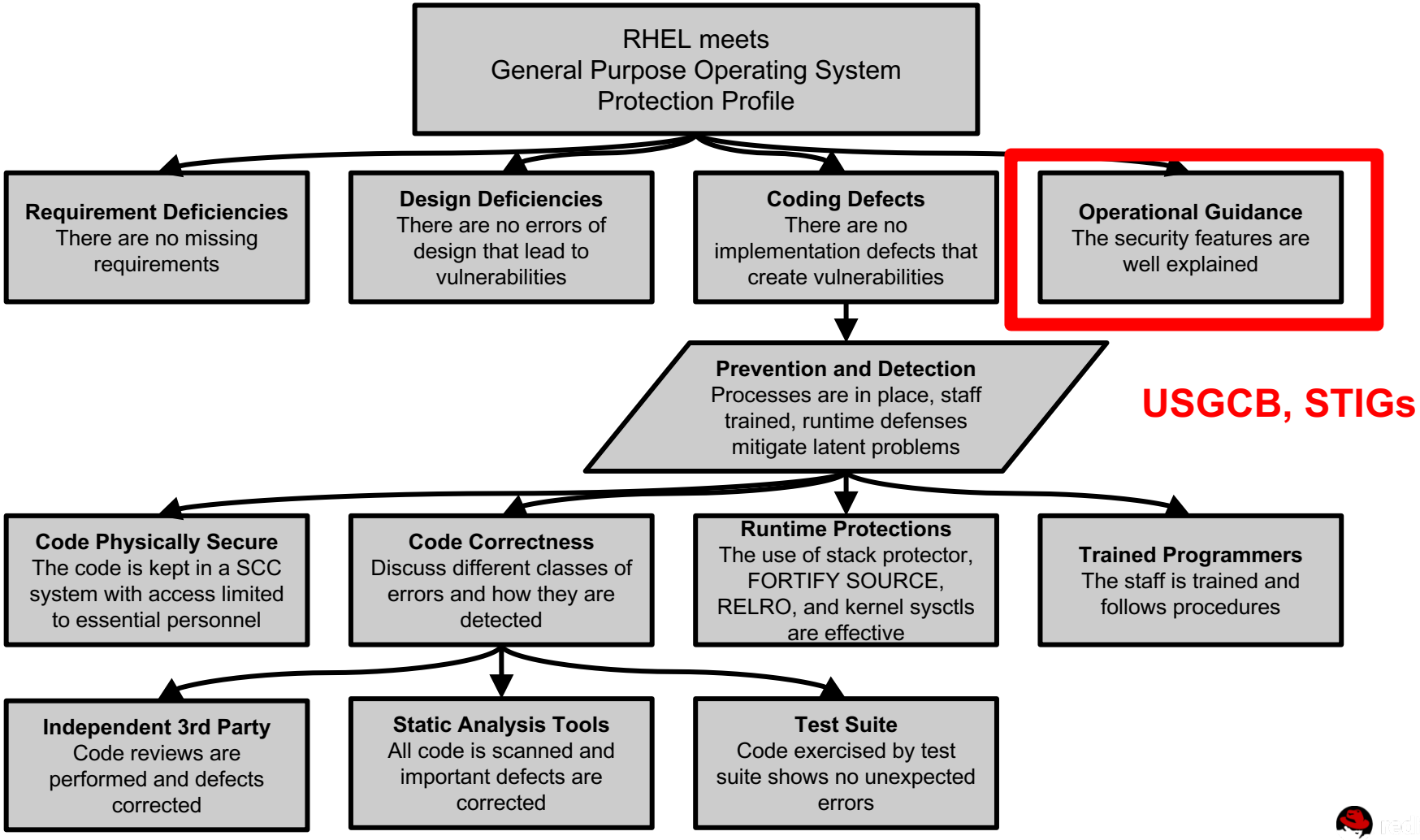
Common Criteria

- RHEL 7.1 certified to EAL4+.
- 3rd party lab verifies security functionality.
- Certified multi-tenancy capabilities.


RHEL meets
General Purpose Operating System
Protection Profile
Requirement Deficiencies
There are no missing requirements
Design Deficiencies
There are no errors of design that lead to vulnerabilities
Coding Defects
There are no implementation defects that create vulnerabilities
Operational Guidance
The security features are well explained
Prevention and Detection
Processes are in place, staff trained, runtime defenses mitigate latent problems
Code Physically Secure
The code is kept in a SCC system with access limited to essential personnel
Code Correctness
Discuss different classes of errors and how they are detected
Runtime Protections
The use of stack protector, FORTIFY SOURCE, RELRO, and kernel sysctls are effective
Trained Programmers
The staff is trained and follows procedures
Independent 3rd Party
Code reviews are performed and defects corrected
Static Analysis Tools
All code is scanned and important defects are corrected
Test Suite
Code exercised by test suite shows no unexpected errors


RHEL meets
General Purpose Operating System
Protection Profile
Requirement Deficiencies
There are no missing requirements
Design Deficiencies
There are no errors of design that lead to vulnerabilities
Coding Defects
There are no implementation defects that create vulnerabilities
Operational Guidance
The security features are well explained
US Gov. Protection Profiles
Prevention and Detection
Processes are in place, staff trained, runtime defenses mitigate latent problems
Code Physically Secure
The code is kept in a SCC system with access limited to essential personnel
Code Correctness
Discuss different classes of errors and how they are detected
Runtime Protections
The use of stack protector, FORTIFY SOURCE, RELRO, and kernel sysctls are effective
Trained Programmers
The staff is trained and follows procedures
Independent 3rd Party
Code reviews are performed and defects corrected
Static Analysis Tools
All code is scanned and important defects are corrected
Test Suite
Code exercised by test suite shows no unexpected errors

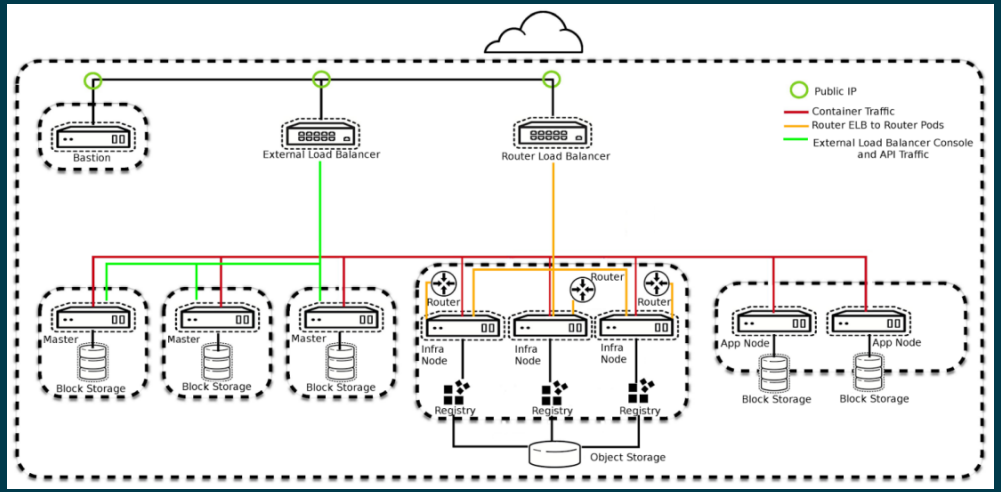

RHEL meets
General Purpose Operating System
Protection Profile
Requirement Deficiencies
There are no missing requirements
Design Deficiencies
There are no errors of design that lead to vulnerabilities
Coding Defects
There are no implementation defects that create vulnerabilities
Operational Guidance
The security features are well explained
FIPS 140-2
Cryptography Certification
Prevention and Detection
Processes are in place, staff trained, runtime defenses mitigate latent problems
Code Physically Secure
The code is kept in a SCC system with access limited to essential personnel
Code Correctness
Discuss different classes of errors and how they are detected
Runtime Protections
The use of stack protector, FORTIFY SOURCE, RELRO, and kernel sysctls are effective
Trained Programmers
The staff is trained and follows procedures
Independent 3rd Party
Code reviews are performed and defects corrected
Static Analysis Tools
All code is scanned and important defects are corrected
Test Suite
Code exercised by test suite shows no unexpected errors


RHEL meets
General Purpose Operating System
Protection Profile
Requirement Deficiencies
There are no missing requirements
Design Deficiencies
There are no errors of design that lead to vulnerabilities
Coding Defects
There are no implementation defects that create vulnerabilities
Operational Guidance
The security features are well explained
Prevention and Detection
Processes are in place, staff trained, runtime defenses mitigate latent problems
USGCB, STIGs
Code Physically Secure
The code is kept in a SCC system with access limited to essential personnel
Code Correctness
Discuss different classes of errors and how they are detected
Runtime Protections
The use of stack protector, FORTIFY SOURCE, RELRO, and kernel sysctls are effective
Trained Programmers
The staff is trained and follows procedures
Independent 3rd Party
Code reviews are performed and defects corrected
Static Analysis Tools
All code is scanned and important defects are corrected
Test Suite
Code exercised by test suite shows no unexpected errors

PUTTING IT TOGETHER:

OpenShift On Azure Reference Architecture + Security Blueprint

OpenShift on Azure Reference Architecture



Provides a comprehensive, step-by-step build of an *enterprise* deployment of OpenShift v3.5 on Azure.

- Public documentation
- Automation scripts on GitHub

FedRAMP Templates | FedRAM

https://www.fedramp.gov/resources/templates-2016/

FedRAMP

HOME ABOUT US PARTICIPATE MARKETPLACE RESOURCES

FedRAMP Templates

Readiness Assessment Phase

Template	Download	Updated
+ FedRAMP High Readiness Assessment Report (RAR) Template		6/6/2017
+ FedRAMP Moderate Readiness Assessment Report (RAR) Template		6/6/2017

Initial Authorization Phase

Template	Download	Updated
Initial Authorization Package Checklist		
+ FedRAMP Initial Authorization Package Checklist		3/9/2017
Document: System Security Plan (SSP)		
+ FedRAMP System Security Plan (SSP) High Baseline Template		6/6/2017
+ FedRAMP System Security Plan (SSP) Moderate Baseline Template		6/6/2017
+ FedRAMP System Security Plan (SSP) Low Baseline Template		6/6/2017

Home Insert Design Layout References Mailings Share

Paste Times New Ro... 12 Paragraph Styles

FedRAMP System Security Plan (SSP) Moderate Baseline Template

FedRAMP

CSP Name

Information System Name

Version #.#

Version Date

Controlled Unclassified Information

Page 1 of 316 Focus 90%

IA-2 User Identification and Authentication (L) (M) (H)

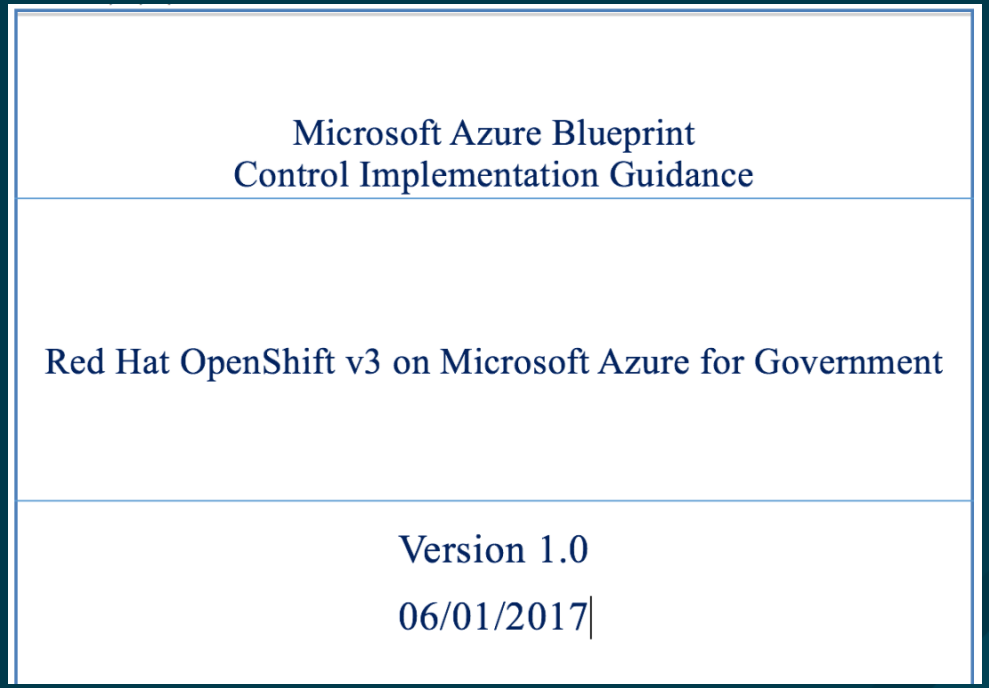
The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

IA-2	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

IA-2 What is the solution and how is it implemented?

OpenShift on Azure Security Blueprint

- ATO paperwork required for all cloud systems
- We went through the ~300pg GSA SSP template and pre-populated answers


Microsoft Azure Blueprint
Control Implementation Guidance

Red Hat OpenShift v3 on Microsoft Azure for Government

Version 1.0

06/01/2017

OpenShift on Azure Security Blueprint

Some controls are implemented in whole or in part by Microsoft Azure

AC-18 What is the solution and how is it implemented?	
Part a	**Microsoft Azure** Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.1.14.
Part b	**Microsoft Azure** Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.1.14.

OpenShift on Azure Security Blueprint

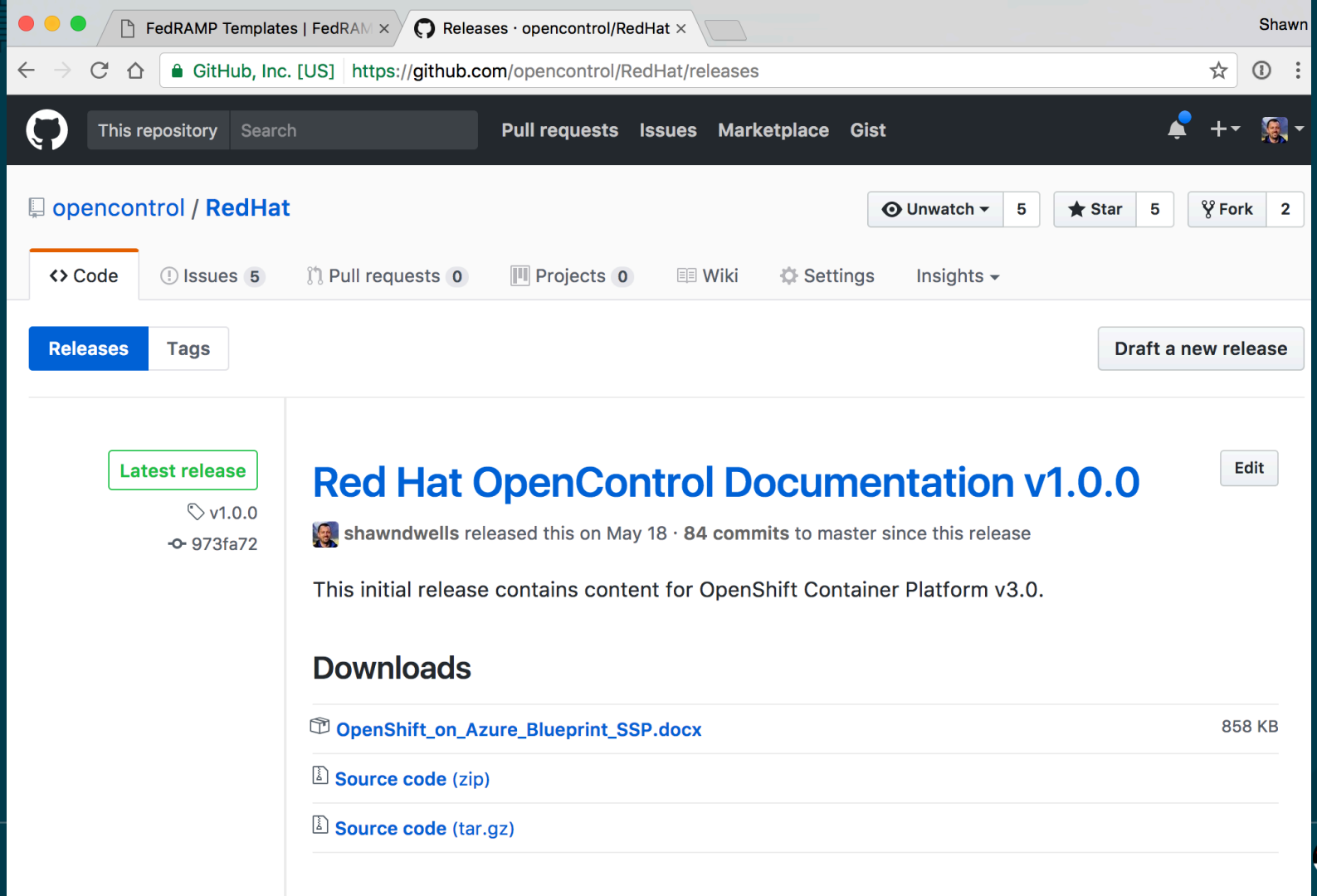
Others are inherently met by use of Red Hat, e.g. FIPS for disk encryption

IA-7 What is the solution and how is it implemented?
Customer Responsibility *<Administrative access to OpenShift nodes is perfomed over SSH. To limit SSH ciphers to those algorithms which are FIPS-approved, update the following line in /etc/ssh/sshd_config:* *Ciphers aes128-ctr,aes192-ctr,aes256-ctr>* *<The OpenShift Console, which is the web interface to the system, converts incoming authentication requests to HTTPS automatically.>*

OpenShift on Azure Security Blueprint

For customer responsibilities, we documented what a successful response would be:

SI-2 (2) What is the solution and how is it implemented?
Customer Responsibility *<The customer will be required to employ automated mechanisms on a monthly basis to determine the state of information system components with regard to flaw remediation on their information systems as required by their organization's security policy. A successful response will address the customer's use of automated tools such as Nessus to preform periodic and on-demand scans through their system to determine the state of system compenents with regard to flaw remediation.>*


FedRAMP Templates | FedRAM
Releases · opencontrol/RedHat
Shawn
GitHub, Inc. [US] https://github.com/opencontrol/RedHat/releases
This repository
Search
Pull requests
Issues
Marketplace
Gist
opencontrol / RedHat
Unwatch 5
Star 5
Fork 2
Code
Issues 5
Pull requests 0
Projects 0
Wiki
Settings
Insights
Releases
Tags
Draft a new release
Latest release
v1.0.0
973fa72
Red Hat OpenControl Documentation v1.0.0
Edit
shawndwells released this on May 18 · 84 commits to master since this release
This initial release contains content for OpenShift Container Platform v3.0.
Downloads
OpenShift_on_Azure_Blueprint_SSP.docx
858 KB
Source code (zip)
Source code (tar.gz)

259 lines (235 sloc) | 10.1 KB

```yaml
---
documentation_complete: false
name: Audit and Accountability
schema_version: 3.0.0
satisfies:

- control_key: AU-4 (1)
  standard_key: NIST-800-53
  covered_by: []
  implementation_status: none
  narrative:
    - text: |
        '//*
        OpenShift Administrators are responsible for configuring the
        offloading of audit records to a central facility. A successful
        control response will outline how audit records are dispatched
        to aggregation points.
        */'

```

Red Hat OpenShift Container Platform on Azure

When creating the Red Hat OpenShift Container Platform on Azure, you will need a SSH RSA key for access.

SSH Key Generation

1. Windows
2. Linux
3. Mac

Create the Installation

Create the Installation on the Azure Portal

click

Development Branch

redhat.

THANK YOU