IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **3V0-31.22**

Title : Advanced Deploy VMware vRealize Automation 8.x (v2)

Version : DEMO

1.TASK 1 CMA DEPLOY
As the Cloud Administrator. you have been tasked to
1. Create a new Cloud Zone
2 Create a new Project
3. Update the default pricing card.
Information requited to create the Cloud Zone and the Project;
. Account / Region: AWS - US West / us-west-2
• Name: Mercury AWS Cloud Zone
• Placement Policy: Default
• Include only Availability Zones us-west-2a and us-west-2c
• Capability Tags o Key: region
o Value: us-west
• Project Name: Mercury
• Project Administrators: Project Mercury Admins group
• Project Members: Project Mercury Users group
• Cloud Zones: vRA-Managed vSphere Datacenter.
Mercury AWS Cloud Zone Information required to update the Pricing Card:
• Assign only for project "Mercury"
• Pricing is Rale based, as follows:
o vCPU cost is S10 per vCPU. charge monthly and only charge when powered on o Memory cost is S5 per GB. charge monthly and only charge when powered on o Storage cost is S1 per GB. charge monthly and always

Answer:

Task 1: Create a New Cloud Zone
Log in to the vRealize Automation console as a Cloud Administrator.
Navigate to Infrastructure > Configure > Cloud Zones.
Click New Cloud Zone.
Enter the following details:
Account / Region: Select AWS - US West / us-west-2.
Name: Enter “Mercury AWS Cloud Zone”.
Placement Policy: Choose Default.
Availability Zones: Include only us-west-2a and us-west-2c.
Capability Tags: Add a tag with Key as “region” and Value as “us-west”.
Save the cloud zone.
Task 2: Create a New Project
In the vRealize Automation console, go to Administration > Projects.
Click New Project.
Provide the Project Name: “Mercury”.
Under Project Administrators, add the “Project Mercury Admins” group.
Under Project Members, add the “Project Mercury Users” group.
In the Cloud Zones section, select the previously created “Mercury AWS Cloud Zone” and any other required zones.
Save the project.
Task 3: Update the Default Pricing Card

Navigate to Infrastructure > Pricing Cards.
Select the default pricing card and click Edit.
Assign the pricing card to the “Mercury” project by selecting it from the list.
Set the pricing details as follows:
vCPU Cost: Enter $10 and set the charge to monthly and only when powered on.
Memory Cost: Enter $5 per GB, charge monthly and only when powered on.
Storage Cost: Enter $1 per GB, charge monthly and always.
Save the changes to the pricing card.

2.TASK 2
As a Cloud Administrator you have two tasks to complete:
1. Onboard new interns into vRealize Automation and assign the correct access. The Interns are split into two Active Directory groups, interns-group-a and interns-group-b. The interns-group-a group requires access to Cloud Assembly and the interns-group-b group requires access to Service Broker. The interns should be allocated the most restrictive access available.
2 Assist in resolving issues reported by the following users who do not have the correct access permissions in vRealize Automation. Each user should have the minimum permissions required to fulfill their role:
• A User with logon id appdevuset2@corp.local is only responsible for creating new and deploying from cloud templates in Cloud Assembly.
The following additional information is provided to help complete both tasks:
• IDM URL: https://identity-manager.corp.tocal/SAAS/admin or use bookmark
• IDM System Domain Username: admin
• IDM Admin Password: VMware1!
• AD Organization Unit ON: OU=Interns.DC=corp.DC=local
• vRealize Automation URL: vr-automalion.corp.local
• Cloud Administrator Username: vca pad mm @corp. local
• Cloud Administrator Password: VMware1!
Answer:
To complete the tasks as a Cloud Administrator, follow these steps:
Task 1: Onboard New Interns into vRealize Automation
Log in to the Identity Manager (IDM) using the provided URL and credentials.
Navigate to Identity & Access Management.
Under Enterprise Groups, find and select interns-group-a and interns-group-b.
Assign interns-group-a with the role of Cloud Assembly User, which is the most restrictive access for Cloud Assembly.
Assign interns-group-b with the role of Service Broker User, which is the most restrictive access for Service Broker.
Ensure that the AD Organization Unit is correctly set to OU=Interns,DC=corp,DC=local for proper group synchronization.
Task 2: Resolve Access Permissions Issues
Log in to the vRealize Automation URL using the Cloud Administrator credentials.
Go to Identity & Access Management.
Locate the user with the logon id appdevuser2@corp.local.

Assign this user the role of Cloud Assembly User to allow creating and deploying from cloud templates in Cloud Assembly.
Verify that the user has the minimum permissions required and does not have any additional roles that exceed their responsibility.
By following these steps, you should be able to onboard the interns with the correct access and resolve the access permissions issues for the specified user. Always ensure to adhere to the principle of least privilege, granting users the minimum level of access necessary to perform their roles.

3.TASK 3
As the Cloud Administrator, you have been tasked to do the following;
1. Create a new operating system image.
2. Create a new machine size.
3. Add two new Cloud templates:
a Import the first Cloud template from the provided file.
b. Create the second Cloud template based on the imported Cloud Template with the following requirements:
i. Allow the user to pick from a list of operating system images.
ii. Allow the user to pick from a list of machine sizes.
iii. Deployment must use the selected input values.
iv. Ensure you are able to review/compare any previous changes that have been made since the Cloud template was cloned in Cloud Assembly. NOTE: Do not deploy the Cloud template Information required to complete the tasks:
• vRealize Automation FODN: vr-automation.corp.local
• Cloud Admin Username: vcapadmin@corp.local
• Cloud Admin Password: VMwarel!
• vRA Project Name: Jupiter
• Flavor Mapping Name: extra large - Flavor Mapping Config:
o Account: vSphere Private Cloud ° Region: Local Datacenter o CPUs: 4 CPU o RAM: 16GB
• Image Mapping Name Windows Server 2019
• Image Mapping Configuration:
o Account: vSphere Private Cloud o Region: Local Datacenter o Image: windows2019
• Imported Cloud template Name: Jupiter Ubuntu Server
• Imported Cloud template File: C: VExam Files\Question 3\jupiter.yaml
• New Cloud template Name: Jupiter Cloned Server
• New Cloud template Size Input:
o Name: size
o Title: Select a Size
o Valid Options: small, medium, extra large
• New Cloud template Image Input: o Name: image
o Title: Select an OS Image
o Valid Options: Windows Server 2019. Ubuntu18

Answer:

To accomplish Task 3 as a Cloud Administrator, you would perform the following steps:
Create a new operating system image:

Log in to the vRealize Automation console using the Cloud Admin credentials.
Navigate to Design > Image Mappings and click New Image Mapping.
Enter the details for the new operating system image, including the name and the Account/Region.
Select the appropriate content library or image to use for the new image mapping12.
Create a new machine size (Flavor Mapping):
Go to Design > Flavor Mappings and click New Flavor Mapping.
Provide the configuration details for the new machine size, such as the number of CPUs and RAM size.
Assign the new flavor mapping to the vSphere Private Cloud account and the Local Datacenter region.
Add two new Cloud templates:
a. Import the first Cloud template:
Navigate to Design > Cloud Templates.
Click Import and select the provided file jupiter.yaml to import the Jupiter Ubuntu Server template.
b. Create the second Cloud template based on the imported Cloud Template:
After importing, clone the Jupiter Ubuntu Server template and rename it to Jupiter Cloned Server. Modify the cloned template to include input options for the operating system image and machine size.
Use the YAML code editor to add an inputs section where users can select the machine size and operating system image at deployment time34.
Ensure that the deployment uses the selected input values by referencing the input parameters in the resources section of the cloud template.
To review and compare any previous changes, utilize the version control features in Cloud Assembly to track changes made to the cloud template

4.TASK 4
As the Cloud Administrator, you have received the following request to make the changes in vRealize Automation to support new service capabilities.
1. Create a Storage Tier to support encryption.
2. Create a Network Profile for Phobos Project.
• Choose the NSX-T network from the available list.
3. The existing Phobos Zone should offer the following capabilities
• Initial workload placement should use VMware vRealize Operations and all workloads should be placed into a specific virtual machine folder by default.
The following information has been provided to assist you in these tasks:
The following information has been provided to assist you in these tasks:
• vRealize Automation URL: vr-automation.corp.local
• Cloud Admin Username: vcapadmin@corp.local
• Cloud Admin Password: VMware1!
Storage Profile Settings:
• Name: Encrypted Storage Tier
• Disk Type: Standard disk
• Region: vSphere Private Cloud / Local Dat
. Datastore/Cluster: RegionAOUSCSIOI-CC3'
• Provisioning Type: Thin
• Supports Encryption: Yes
• Capability Tag:

o Key: storage
o Value: encrypted
Network Profile Settings:
• Name: Phobos Networks
• Region: vSphere Private Cloud / Local Datacenter
• Network Segment: nsx-phobos-external
• Network IPv4 CIDR: 172.16.15.0/24
• Network Default Gateway: 172.16.15.1
• Domain: cofp.local
• IP Range Name: Phobos-range
• IP Range: 172.16.15.5-172.16.15.250
• Network Profile Capability Tag:
o Key: net
o Value: phobos
Cloud Zone Settings:
• Name: Phobos
• Folder: Workloads

Answer:

To support the new service capabilities in vRealize Automation, you will need to perform the following tasks:
Task 1: Create a Storage Tier to Support Encryption
Log in to the vRealize Automation console using the provided Cloud Admin credentials.
Navigate to Infrastructure > Configure > Storage Profiles.
Click New Storage Profile.
Enter the Name as “Encrypted Storage Tier”.
Set the Disk Type to “Standard disk”.
Choose the Region as “vSphere Private Cloud / Local Datacenter”.
Select the Datastore/Cluster as “RegionA01USCSIOI-CC3”.
For Provisioning Type, select “Thin”.
Ensure Supports Encryption is set to “Yes”.
Add a Capability Tag with Key as “storage” and Value as “encrypted”.
Save the storage profile.
Task 2: Create a Network Profile for Phobos Project
In the vRealize Automation console, go to Infrastructure > Configure > Network Profiles.
Click New Network Profile.
Provide the Name as “Phobos Networks”.
Set the Region to “vSphere Private Cloud / Local Datacenter”.
Under Network Segment, choose “nsx-phobos-external”.
Enter the Network IPv4 CIDR as “172.16.15.0/24”.
Set the Network Default Gateway to “172.16.15.1”.
Specify the Domain as “corp.local”.
Go to the IP Ranges tab and add a new range named “Phobos-range” with the range “172.16.15.5-172.16.15.250”.
Add a Network Profile Capability Tag with Key as “net” and Value as “phobos”.
Save the network profile.

Task 3: Configure Workload Placement for Phobos Zone
Ensure that VMware vRealize Operations is integrated with vRealize Automation for advanced workload placement1.
In the vRealize Automation console, navigate to Infrastructure > Cloud Zones.
Locate and edit the existing cloud zone named “Phobos”.
In the Placement Policy section, set it to use VMware vRealize Operations.
Specify the default virtual machine folder for workload placement as “Workloads”.
Save the changes to the cloud zone.
By completing these steps, you will have created a storage tier that supports encryption, a network profile for the Phobos Project, and configured the Phobos Zone to offer advanced capabilities using VMware vRealize Operations. Always ensure to follow your organization’s best practices and security policies when making changes to the infrastructure.

5.TASK 5
As the Cloud Administrator, you have been tasked lo complete the following tasks tor the Pluto Project.
1. Configure the following on the network nsx-pluto-existing in the network profile called Pluto Networks
a. IPv4 CIDR: 172.16.17.0/24
b. IPv4 Gateway: 172.16.17.1
c Default Domain: corp.local
d. Assign a Capability Tag:
• key: net
• value: existing
2. Define a new IP Range on the nsx-pluto-existing network that has the following configuration: a. Network IP Range Name: pluto-existing-range b IP Range: 172.16.17.5-172.16.17.250
3. Assign a new capability tag to the sgPlutoDatabase Security Group:
a. key: sg
b. value: plutodatabase
4. Update the Pluto Networks Network Profile:
a. Ensure it only has the following networks assigned:
i. nsx-pluto-extemal
ii. nsx-pluto-existing
iii. nsx-pluto-outbound b Configure nsx-pluto-outbound as the external network for the network policy c. Assign a new capability tag to the Pluto Networks network profile:
i. key: net
ii. value: pluto
Answer: See the
Explanation for
complete Solution.
Explanation:
To complete the tasks for the Pluto Project as a Cloud Administrator, you would follow these steps:
Task 1: Configure Network nsx-pluto-existing in Pluto Networks Profile
Access the vRealize Automation console.
Navigate to Infrastructure > Configure > Network Profiles.
Select the “Pluto Networks” profile.

Configure the network nsx-pluto-existing with the following settings:
IPv4 CIDR: 172.16.17.0/24
IPv4 Gateway: 172.16.17.1
Default Domain: corp.local
Assign a Capability Tag with key: net and value: existing.
Task 2: Define a New IP Range
Within the “Pluto Networks” profile, select the nsx-pluto-existing network.
Add a new IP Range with the following configuration:
Network IP Range Name: pluto-existing-range
IP Range: 172.16.17.5-172.16.17.250
Task 3: Assign Capability Tag to sgPlutoDatabase Security Group
Locate the sgPlutoDatabase Security Group within the vRealize Automation console. Assign a new capability tag to the security group with key: sg and value: plutodatabase. Task 4: Update the Pluto Networks Network Profile
Ensure the Pluto Networks profile includes only the following networks:
nsx-pluto-external
nsx-pluto-existing
nsx-pluto-outbound
Configure nsx-pluto-outbound as the external network for the network policy.
Assign a new capability tag to the Pluto Networks network profile with key: net and value: pluto.
Please ensure to follow the specific steps and configurations as per your organization’s standards and the vRealize Automation documentation for detailed instructions on each task