

Table of Contents

Lab Overview - HOL-2182-01-HBD - VMware Cloud Provider Platform - DR and Migration using VMware Cloud Director Availability	2
Lab Guidance	3
Module 1 - VMware Cloud Director Availability Overview and Architecture.....	9
Introduction.....	10
Conclusion.....	36
Module 2 - On-Prem DR and Migration to Cloud with VMware Cloud Director Availability	37
Introduction.....	38
Site Pairing from On-Premises to Cloud using VMware vCloud Director Availability.....	39
Failover Workflows from On-Premise to Cloud Using vCloud Availability	65
Conclusion.....	107
Module 3 - Administrator-driven Cloud-to-Cloud DR with VMware Cloud Director Availability	108
Introduction.....	109
Site Pairing and Failover Workflows from Cloud to Cloud using vCloud Availability.....	110
Conclusion.....	151
Module 4 - Tenant-driven Cloud-to-Cloud DR with VMware Cloud Director Availability ..	152
Introduction.....	153
Tenant Self Service Site Pairing and Failover Workflows from Cloud to Cloud using vCloud Availability.....	154
Conclusion.....	205

Lab Overview - HOL-2182-01-HBD - VMware Cloud Provider Platform - DR and Migration using VMware Cloud Director Availability

Lab Guidance

Note: It will take more than 90 minutes to complete this lab. You should expect to only finish 2-3 of the modules during your time. The modules are independent of each other so you can start at the beginning of any module and proceed from there. You can use the Table of Contents to access any module of your choosing.

The Table of Contents can be accessed in the upper right-hand corner of the Lab Manual.

This lab will help you learn how to use VMware Cloud Director Availability for Disaster Recovery to fail over or fail back a datacenter or use it to migrate a data center in vSphere and vCloud Director environments.

Lab Module List:

- **[Module 1 - VMware Cloud Director Availability Overview and Architecture](#)** (15 minutes) (Basic) This module will show an overview of the architecture and deployment of VMware Cloud Director Availability 4.0
- **[Module 2 - On-Prem DR and Migration to Cloud with VMware Cloud Director Availability](#)** (45 Minutes) (Basic) This module will walk through the steps to pair On-Premises site with Cloud and how to use VMware Cloud Director Availability for disaster recovery and migration from on-prem to cloud.
- **[Module 3 - Administrator-driven Cloud-to-Cloud DR with VMware Cloud Director Availability](#)** (30 minutes) (Basic) This module will show how administrators can use Cloud Director Availability for cloud-to-cloud DR.
- **[Module 4 - Tenant-driven Cloud-to-Cloud DR with VMware Cloud Director Availability](#)** (30 minutes) (Basic) This module will demonstrate how to pair Cloud-to-Cloud sites and tenant-driven Cloud-to-Cloud DR with VMware Cloud Director Availability.

Lab Captains:

- **Module 1 - Eric Stine, Parul Garg**
- **Module 2 - Eric Stine, Parul Garg**
- **Module 3 - Eric Stine, Parul Garg**
- **Module 4 - Eric Stine, Parul Garg**

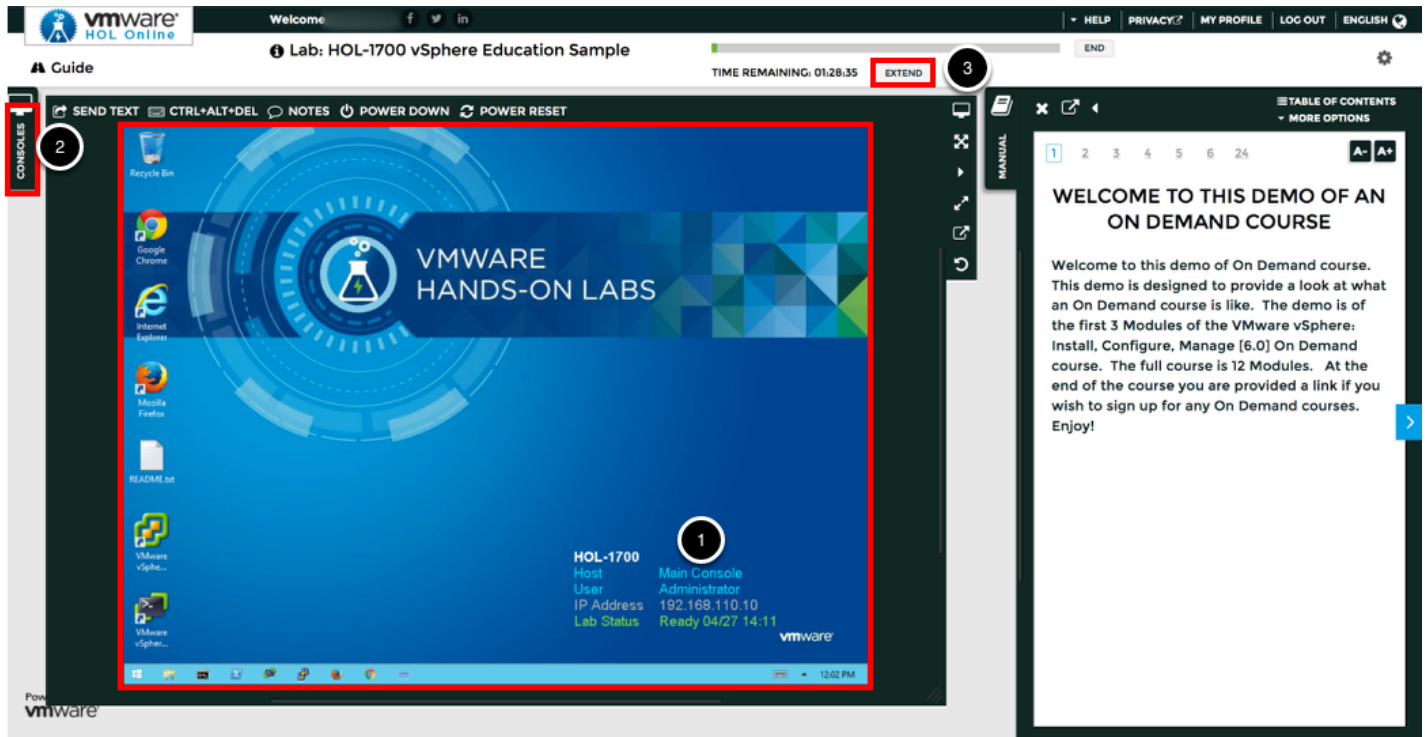
This lab manual can be downloaded from the Hands-on Labs Document site found here:

<http://docs.hol.vmware.com>

This lab may be available in other languages. To set your language preference and have a localized manual deployed with your lab, you may utilize this document to help guide you through the process:

<http://docs.hol.vmware.com/announcements/nee-default-language.pdf>

Location of the Main Console



1. The area in the RED box contains the Main Console. The Lab Manual is on the tab to the Right of the Main Console.
2. A particular lab may have additional consoles found on separate tabs in the upper left. You will be directed to open another specific console if needed.
3. Your lab starts with 90 minutes on the timer. The lab can not be saved. All your work must be done during the lab session. But you can click the **EXTEND** to increase your time. If you are at a VMware event, you can extend your lab time twice, for up to 30 minutes. Each click gives you an additional 15 minutes. Outside of VMware events, you can extend your lab time up to 9 hours and 30 minutes. Each click gives you an additional hour.

Alternate Methods of Keyboard Data Entry

During this module, you will input text into the Main Console. Besides directly typing it in, there are two very helpful methods of entering data which make it easier to enter complex data.

Click and Drag Lab Manual Content Into Console Active Window

You can also click and drag text and Command Line Interface (CLI) commands directly from the Lab Manual into the active window in the Main Console.

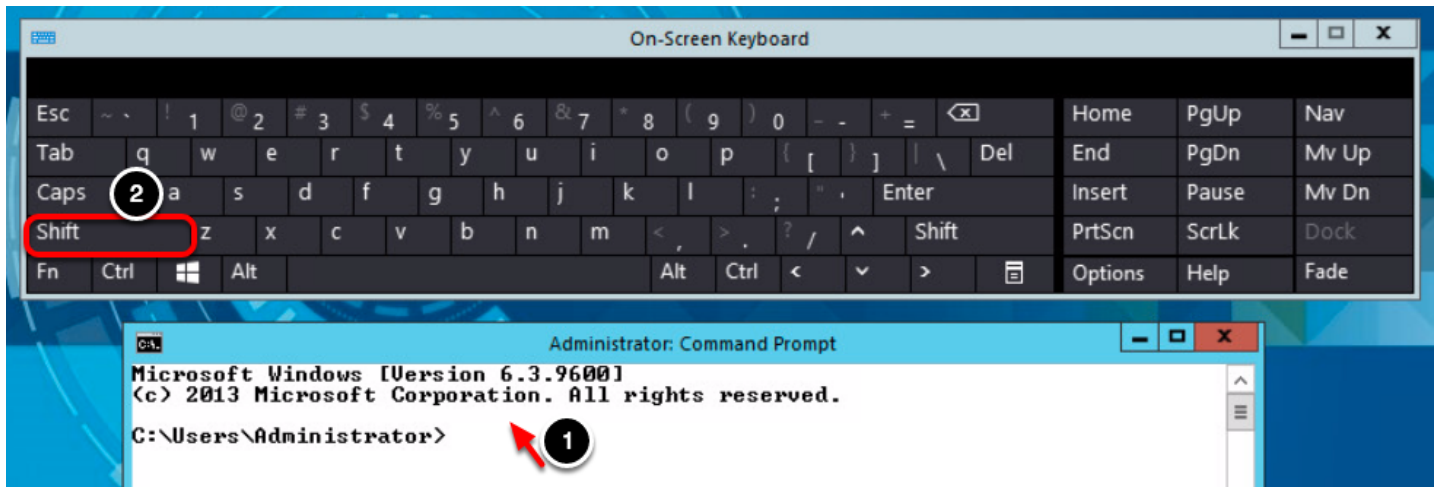
Accessing the Online International Keyboard



You can also use the Online International Keyboard found in the Main Console.

1. Click on the Keyboard Icon found on the Windows Quick Launch Task Bar.

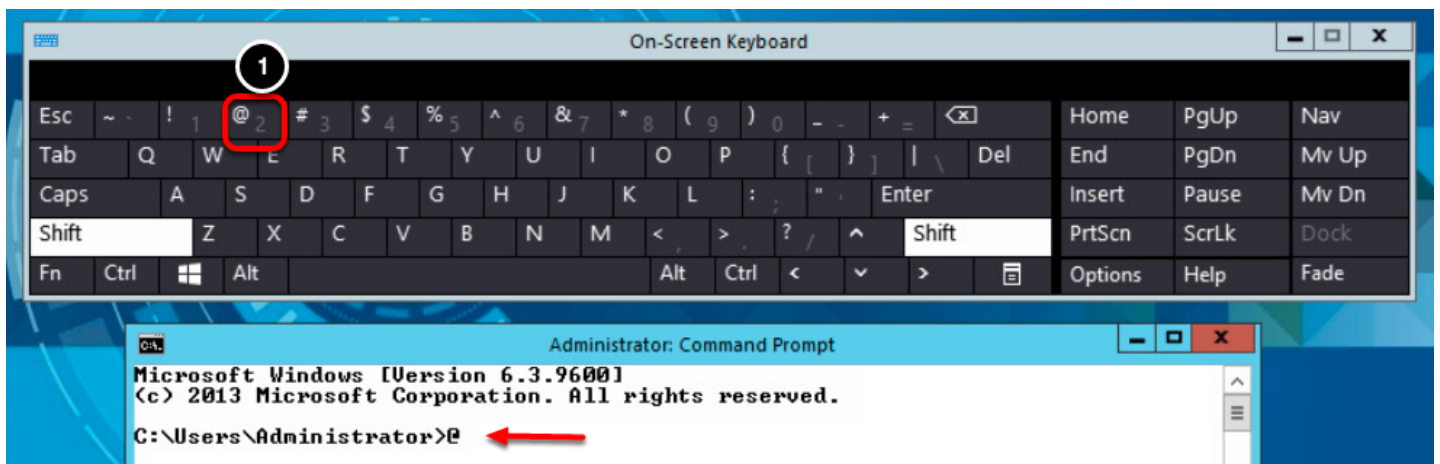
Click once in active console window



In this example, you will use the Online Keyboard to enter the "@" sign used in email addresses. The "@" sign is Shift-2 on US keyboard layouts.

1. Click once in the active console window.
2. Click on the **Shift** key.

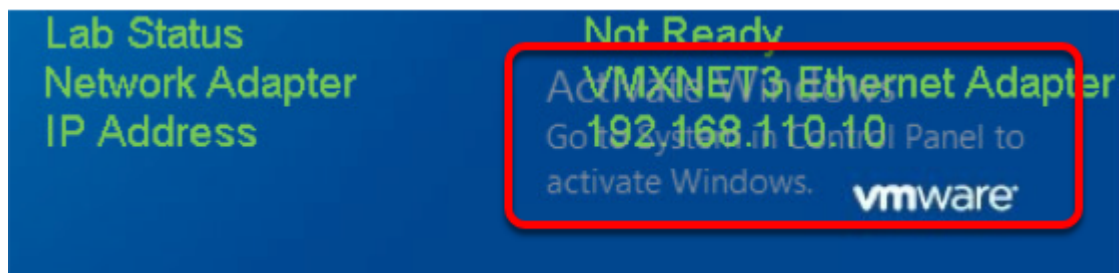
Click on the @ key



1. Click on the "@ key".

Notice the @ sign entered in the active console window.

Activation Prompt or Watermark



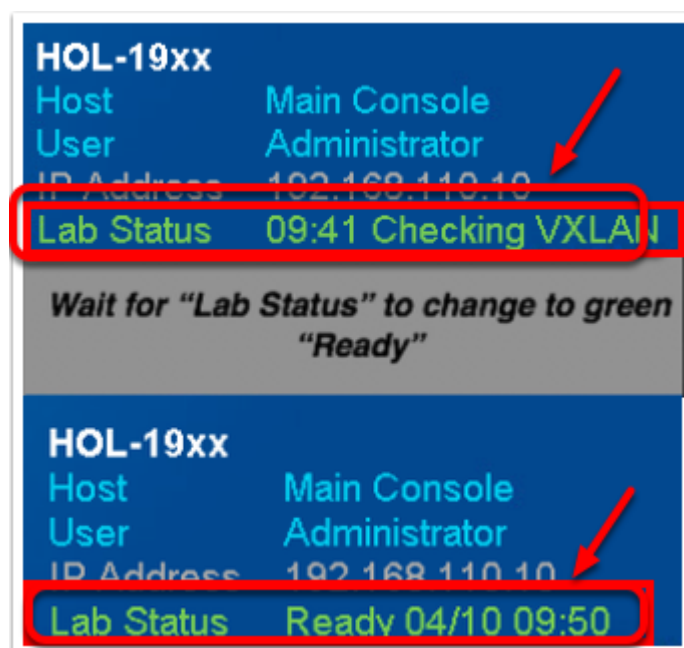
When you first start your lab, you may notice a watermark on the desktop indicating that Windows is not activated.

One of the major benefits of virtualization is that virtual machines can be moved and run on any platform. The Hands-on Labs utilizes this benefit and we are able to run the labs out of multiple datacenters. However, these datacenters may not have identical processors, which triggers a Microsoft activation check through the Internet.

Rest assured, VMware and the Hands-on Labs are in full compliance with Microsoft licensing requirements. The lab that you are using is a self-contained pod and does not have full access to the Internet, which is required for Windows to verify the activation. Without full access to the Internet, this automated process fails and you see this watermark.

This cosmetic issue has no effect on your lab.

Look at the lower right portion of the screen



Please check to see that your lab is finished all the startup routines and is ready for you to start. If you see anything other than "Ready", please wait a few minutes. If after 5 minutes your lab has not changed to "Ready", please ask for assistance.

Module 1 - VMware Cloud Director Availability Overview and Architecture

Introduction

In this module, we will learn:

- Introduction of Whats New with VMware Cloud Director Availability 4.0 highlighting key features and Business value.
- Introduction of What's New with VMware Cloud Director Availability 3.5

Note - This module is purely an overview of the solution and updates made in recent releases. The hands-on configuration portion of the lab starts in Module 2.

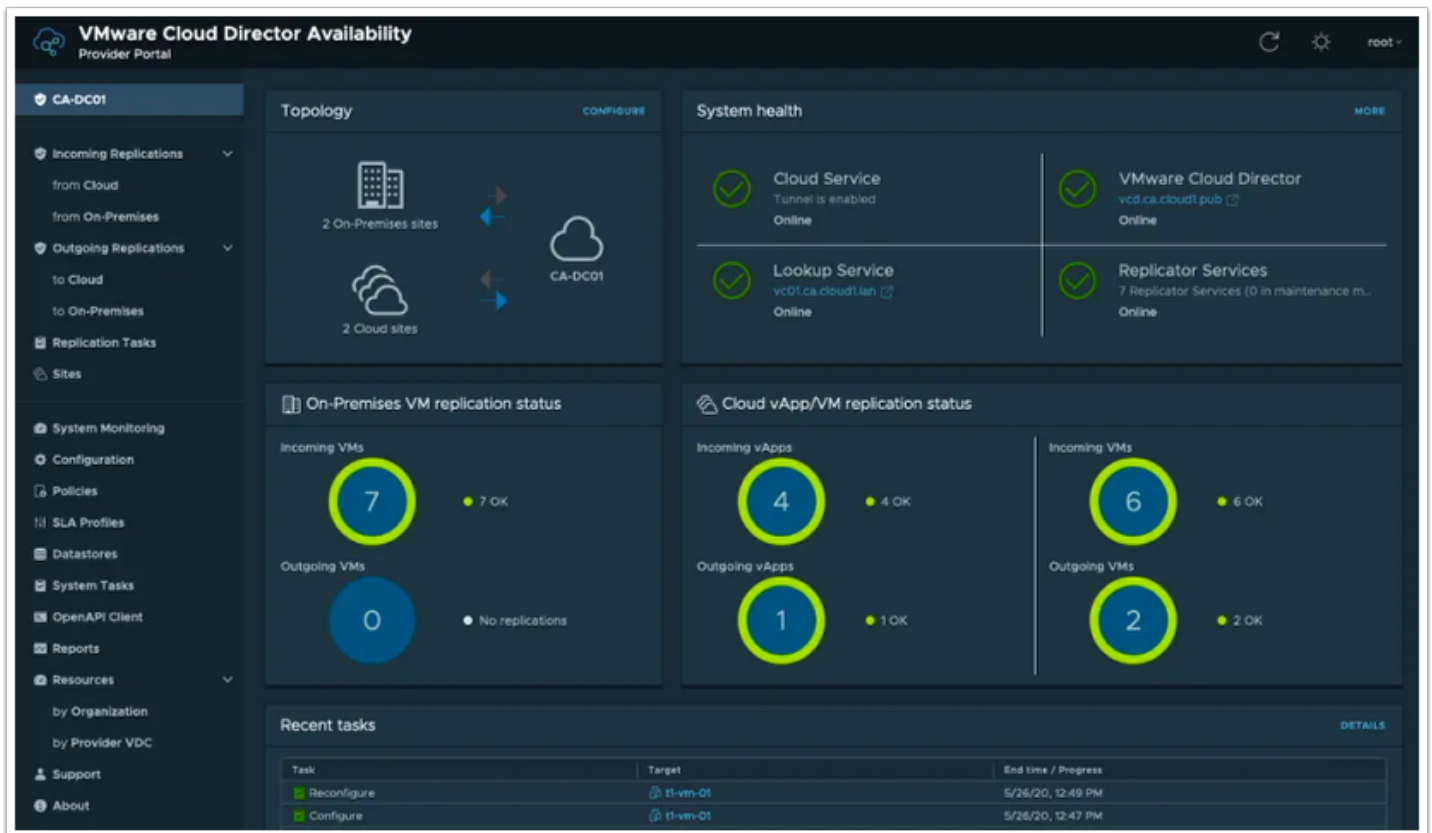
Thank You!

Special thanks go to Daniel Paluszek and his series of blog posts on VMware Cloud Director Availability 4.0 . This lab is based on his blog posts:

<https://www.paluszek.com/wp/2020/06/02/vmware-cloud-director-availability-4-0-whats-new-and-sla-profile-review/>

<https://www.paluszek.com/wp/2019/11/14/whats-new-with-vmware-vcloud-availability-3-5/>

Review Core Capabilities of VMware Cloud Director Availability

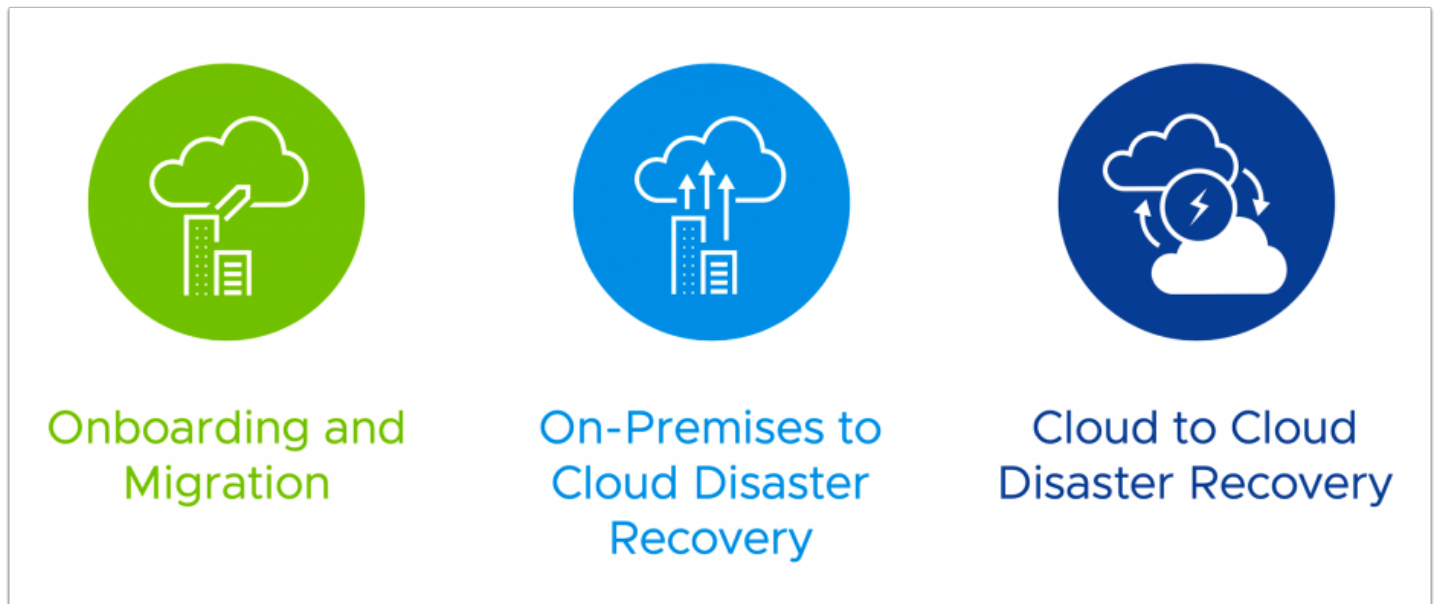


Lets briefly look at core capabilities of VMware Cloud Director Availability

- Intuitive, Disaster Recovery as a service protection and wizard driven workflows to protect virtual machines (VM) or vApps, Replication and Recovery of VMs and vApps between VMware Cloud Director sites or on-premise to VMware Cloud Director and visa versa.
- Single on-premise appliance installation for ease of deployment and simplicity for customers replicating to provider clouds. Supports a migration path and DR functionality from vSphere 6.5+ U3
- The capability of each deployment to serve as both source and recovery instances (sites). There are no dedicated source and destination sites with symmetrical replication flow that can be started and managed from either the source or the recovery site means the UI can be accessed from anywhere with correct context.
- Maximum replicated VMs and retained replications (stored instances) as well as minimum 5min RPO Policy controls for providers to apply to one to-many VDC or replications via SLA policies. This helps to control storage costs and provide tiered services to customers.
- Secure tunneling through TCP proxy between sites with builtin encryption and optional compression availability

- **Multi-tenant support** native within the VMware Cloud Director hierarchy and now in-context DRaaS providing customers a very simple view and action capability directly in VMware Cloud Director

Overview of VMware Cloud Director Availability 4.0



Formerly known as vCloud Availability (vCAv), VMware Cloud Director Availability 4.0 (**VCDA**) provides a simple, cost-effective and secured onboarding, migration and disaster recovery as a service solution to or between multi-tenant VMware clouds.

Part of the VMware Cloud Provider Platform, VMware Cloud Director Availability has been designed from the ground-up to dramatically simplify cloud onboarding, enable cost-effective availability and recovery, and better secure operations to cloud providers and their end customers.

From a functionality perspective, VCDA is the convergence of multiple products and covers the following use cases:

- **Disaster Recovery** With ongoing risk of human error, natural disasters, and cyber-attacks, disaster recovery is an even more critical part of a cloud providers portfolio than ever. Intuitive, Disaster Recovery as a service protection and wizard driven workflows to protect virtual machines (VM) or vApps, Replication and Recovery of VMs and vApps between VMware Cloud Director sites or on-premise to VMware Cloud Director and visa versa.
- **Cloud to Cloud Migrations** Cloud providers must help customers migrate from clouds where their workloads are already running.
- **Cloud Onboarding** With so many workloads moving off-premises, cloud providers need to help customers onboard efficiently.

What's New in VMware Cloud Director Availability 4.0?

Version 4.0 of VMware Cloud Director Availability
Key Themes

Service Operation

Monitoring, Reporting, Control

Service Consumption

Service Tiering, Optional Upsell Functions

Platform Integration

In-context DR In VCD, NSX-T support

VMware Cloud Director Availability 4.0 enhancements and new capabilities focus on three main themes: **Service Operation**, **Service Consumption**, and **Platform Integration**. We will drill into these themes as we review what is new with 4.0 below.

For our cloud providers that are already running vCAv, an in-place upgrade from vCloud Availability 3.0.5 and 3.5.1 is possible. Cloud Director doesn't bring any significant architectural changes: the real surprise concerns the new features and how they can maximize your capability and value as a cloud provider.

Service Operation - Resource UI Visualization

VMware Cloud Director Availability
Provider Portal

CA-DC01

Incoming Replications

- from Cloud
- from On-Premises

Outgoing Replications

- to Cloud
- to On-Premises

Resources by Organization

The table below indicates the amount of resources that will be provisioned on failover. In case of insufficient resources failover may fail or workloads may not power on.

Destination Org / VDC	Virtual CPUs required	Memory required	Disk capacity required
tenant1	8 CPU(s)	4.75 GB	58.00 GB
tenant1-ovdc2	4 CPU(s)	2.75 GB	18.00 GB
tenant1-ovdc1	4 CPU(s)	2.00 GB	40.00 GB
tenant2	5 CPU(s)	2.50 GB	50.00 GB
tenant2-ovdc1	5 CPU(s)	2.50 GB	50.00 GB

Provider View per Organization (Tenant)

Resources by PVDC

The table below indicates the amount of resources that will be provisioned on failover. In case of insufficient resources failover may fail or workloads may not power on.

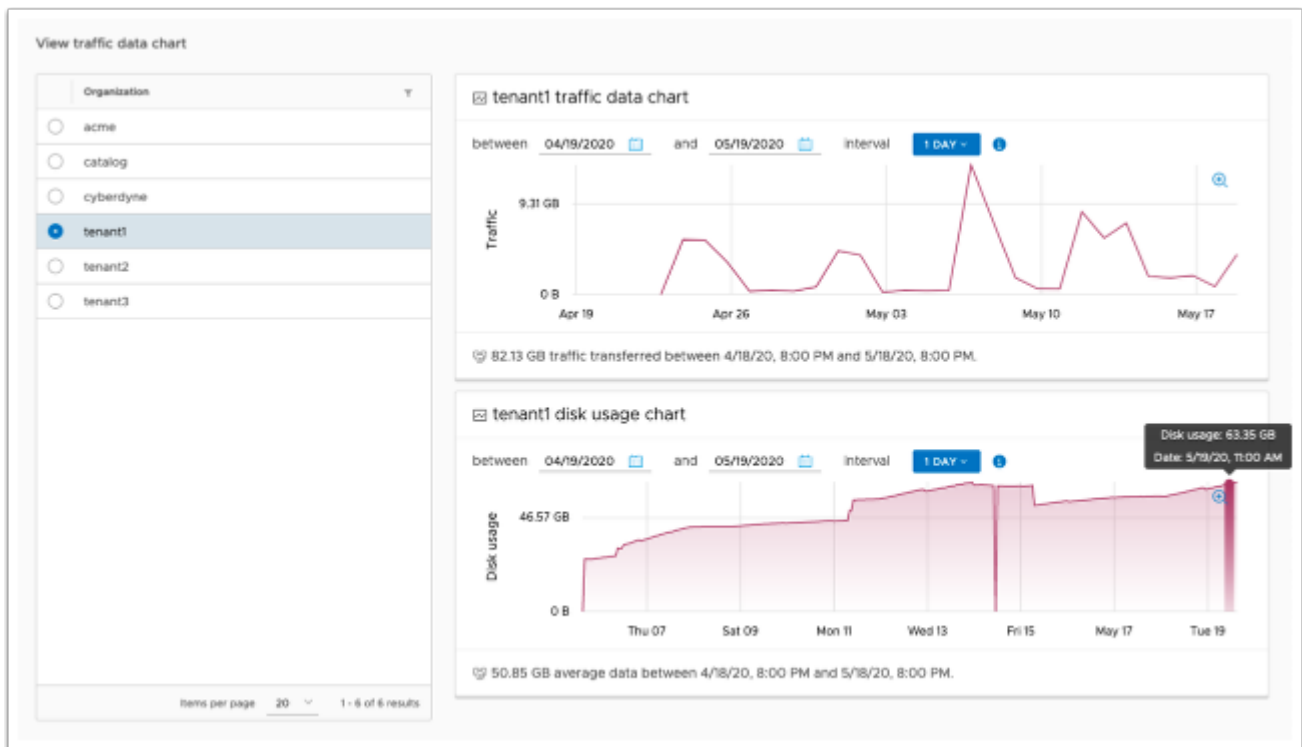
Destination VDC	Virtual CPUs required	Memory required	Disk capacity required
vc01-pvdc01	9 CPU(s)	4.50 GB	90.00 GB
vc02-pvdc01	4 CPU(s)	2.75 GB	18.00 GB

Provider View per pVDC

13 CPU(s) 7.25 GB 108.00 GB

With VCD 4.0, providers and tenants can comprehensively monitor resource utilization. The provider can see an organization or provider VDC (pVDC) view what would be required to ensure proper failover for any protected workloads. From a tenant perspective, they can see what resources are required for each respective orgVDC along with specific utilization on a per-VM perspective:

Service Operation - Resource Manageability

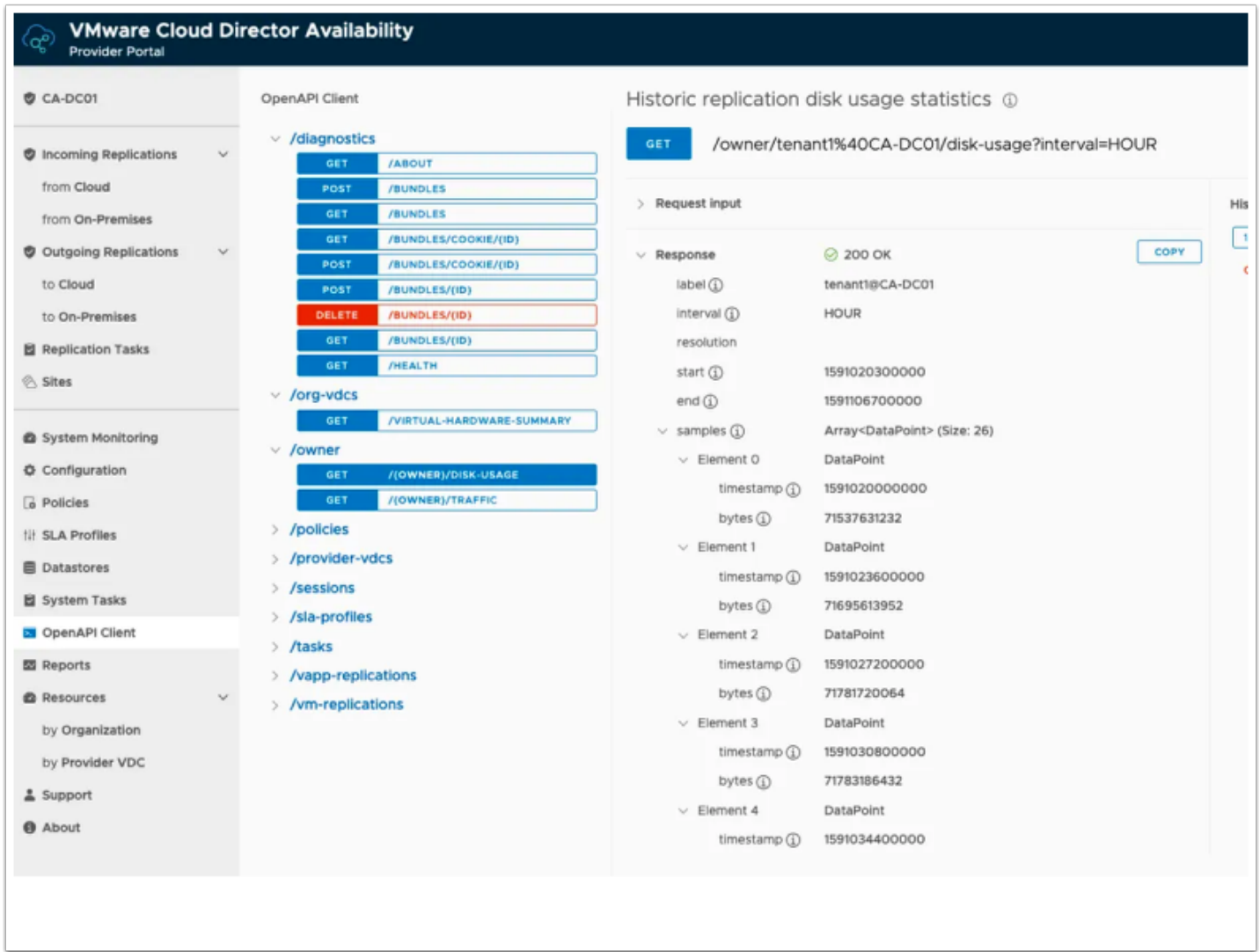


First, **storage consumption reporting** is made available in the user interface as well as via **API**. While tenants and providers have full visibility of the disk space used by each virtual machine replication, providers can also aggregate storage reporting from an organizations perspective.

Just like storage utilization, VCD 4.0 provides visibility to **network utilization** (via the UI and API) on a per-protected workload. Besides network metering, improvements to network throttling have been made in this release: **bandwidth throttling** was previously available for system throttling, but with 4.0, we have introduced the ability to throttle on a per-policy basis (at the organization level). This change allows granular control on what the provider can control on a per-tenant perspective. Bandwidth throttling allows you to enforce:

- limits for replication data traffic from the on-premises to cloud sites, which is appropriate for expensive bandwidth areas.
- a global limit for the total incoming replication traffic from all cloud sites.

Public API enhancements



While the UI has greatly improved to visualize this data, a provider requires automation to retrieve these statistics and export them for metering and monitoring requirements.

VMware Cloud Director Availability now provides public APIs that help to onboard tenants, see the storage usage, the network settings, and the compute resource usage of the replications on a per-org/tenant basis.

It allows a provider to gain visibility into the entire platform and organizations: this is a great addition for cloud providers to be able to further automate delivery of the service to customers and configuration of the service, speeding up the time to consumption, whilst minimizing configuration errors and providing consistency.

The API is in the form of swagger definition (as all API are for Cloud Director Availability), making it very friendly for cloud providers to use their coding preferences.

One can view the entire API structure on code.vmware.com

Service Operation -Logging

The screenshot shows a configuration window titled "Cloud event notifications" with a close button (X) in the top right corner. The window contains the following settings:

Setting	Value	Unit
Config poll interval	1	days
Connectivity poll interval	30	sec
Replications poll interval	5	min
Certificate expiry threshold	30	days
RPO violation threshold	30	min
RPO violation threshold	50	count
Event reposting time	86400	sec

Below the table, there are two toggle switches and a text field:

- ☒ Syslog events
- Syslog server address and port: `syslog.infra.lan:514`
- ☒ VMware Cloud Director events

At the bottom right, there are two buttons: "CANCEL" and "APPLY".

With VMware Cloud Director Availability 4.0, we have the ability to export out VCDA logs to a syslog collector (such as vRealize Log Insight). However, we also show tasks and events within the native VCD interface. This is a great addition, especially when we pair with the new UI functionality.

From the Provider UI screen, the administrator can establish event notifications along with the syslog configuration.

Service Consumption -SLA Profiles

The screenshot displays the VMware Cloud Director Availability 4.0 interface for managing SLA Profiles. At the top, there are tabs for 'PROFILES' and 'ORGANIZATIONS'. Below the tabs is a table of SLA profiles with columns: Name, RPO, Retention, Quiescing, Compression, Initial Synchronizing, and Usage. The table lists four profiles: Silver, Bronze, Gold, and Platinum. A 'Settings' dialog box is open, showing the 'Bronze' profile selected. The dialog includes a 'Show details' link and options to 'Exclude disks' and 'Configure Seed VMs'.

Name	RPO	Retention	Quiescing	Compression	Initial Synchronizing	Usage
Silver	2h	7 instances over 1 week	No	Enabled	No delay	2 Orgs, 3 Replications
Bronze	4h	Keep latest instance only	No	Enabled	No delay	3 Orgs, 4 Replications
Gold	30m	14 instances over 2 weeks	No	Enabled	No delay	1 Orgs, 2 Replications
Platinum	5m	24 instances over 1 day	Yes	Enabled	No delay	1 Orgs, 1 Replications

Settings

SLA profile

☒ Bronze (4h RPO, Keep latest instance only) [Show details](#)

☐ Gold (30m RPO, 14 instances over 2 weeks)

☐ Platinum (5m RPO, 24 instances over 1 day)

☐ Silver (2h RPO, 7 instances over 1 week)

Exclude disks

☐ Save disk space on the target site by excluding disks that are not necessary.

Configure Seed VMs

☐ Use an older copy of the protected VMs on the target site to reduce the data traffic.

VMware Cloud Director Availability 4.0 introduces **SLA Profiles**, making protection configuration intuitive for customers. Previously, many decisions needed to be made by tenants, involving implied knowledge on how disaster recovery is working. Now, customers can select an SLA Profile that the cloud provider has created for them, which can be as simple as Gold, Silver and Bronze nomenclature essentially hiding complex wizard-driven choices from the customers.

For more advanced customers, these profiles can be overridden and modified at the point of usage, but this is optional for each customer.

In short, the premise of a SLA Profile is to provide a grouping of target settings when protecting a workload. This minimizes the amount of time spent configuring for protection. Think of this as a logical grouping construct.

The end value for a tenant is this is a single selection to protect a workload. One does not need to think about what settings to configure. Just select the SLA profile, and done.

Service Consumption -SLA Profiles Properties

Edit SLA profile

SLA profile name * Gold

Target recovery point objective (RPO)

5 min 30 min 2 hours 8 hours 24 hours

30m

Retention policy for point in time instances

☒ Preserve 14 instances spread evenly over the last 2 weeks

Enable quiesce

☐ Enabling quiescing will ensure application level consistency before creating an instance.

Compress replication traffic

☒ Enabling compression will reduce network traffic at the expense of CPU.

Delay start synchronization i

☐ Set time that is convenient for the first synchronization.

CANCEL **APPLY**

A provider can either leverage the default SLA profiles (Gold, Silver, and Bronze) available upon VMware Cloud Director Availability 4.0 deployment/upgrade, or create additional ones and assign them as required to one or multiple organizations. The following properties define an SLA profile:

- Target Recovery Point Objective (RPO)
- Retention policy for point in time instances
- Quiescing
- Compression
- Timeslot to delay the initial synchronization

Service Consumption -SLA Profiles and Policy

Edit Policy
Gold Tier

Policy name: *
Gold Tier

☒ Allow custom SLA settings

☒ Allow outgoing replications

☒ Allow incoming replications

Maximum number of vm replications: *
☒ Unlimited
☐ 10

Max point-in-time instances per replication: ⓘ *
24

Max stored instances per replication: ⓘ *
20

☐ Enable bandwidth throttling

Max throughput per On-Premises Replicator Appliance: *
512
(1 - 10000 mbit/s)

Minimum allowed RPO:

5 min
30 min
2 hours
8 hours
24 hours

5m

CANCEL
APPLY

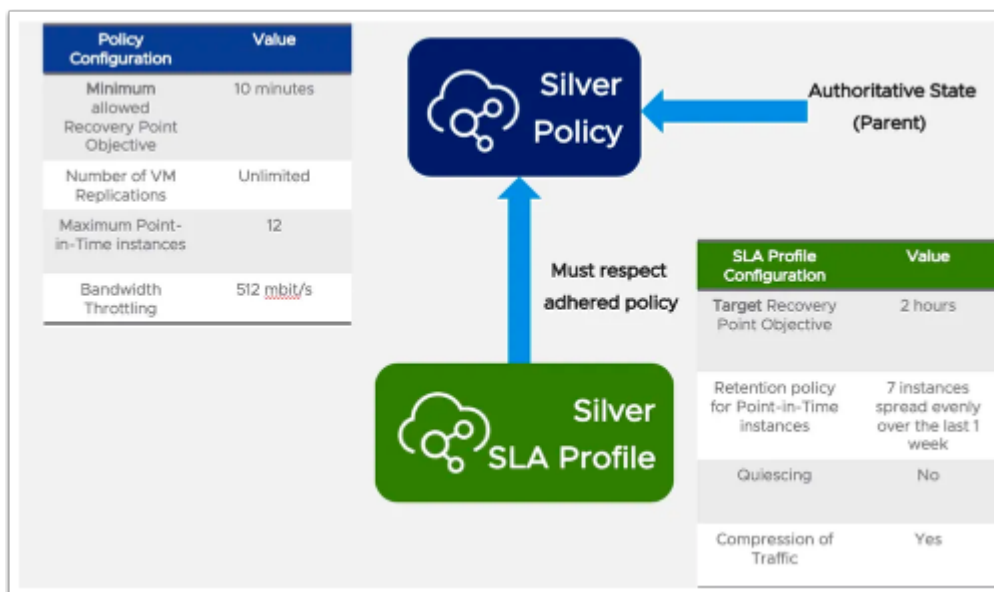
Policies didn't disappear with this release; they are still mandatory for any organization using VMware Cloud Director Availability. To further explain SLA profiles in relations to policies:

- Think of the policy as the parent state of any protection and are the authoritative state for organizations.
- Then, the SLA profile is the child object that must respect the exposed policy to the organization.
- Both operate independently; however, they can work in unison to accomplish the stated protection goal.

SLA profiles are a key construct from Cloud Director Availability: this new capability is designed to provide better control to the provider, to configure replications faster avoiding complex decisions, and to establish service profiles based on application or organization requirements. As a tenant, protecting a workload has never been so easy!

1. Select the workload(s) to protect.
2. Select the destination organization Virtual Data Center (oVDC) and the Storage Policy.
3. Select the SLA profile from a drop-down list.
4. Confirm and done!

Service Consumption -SLA Profiles and Policy explained with example



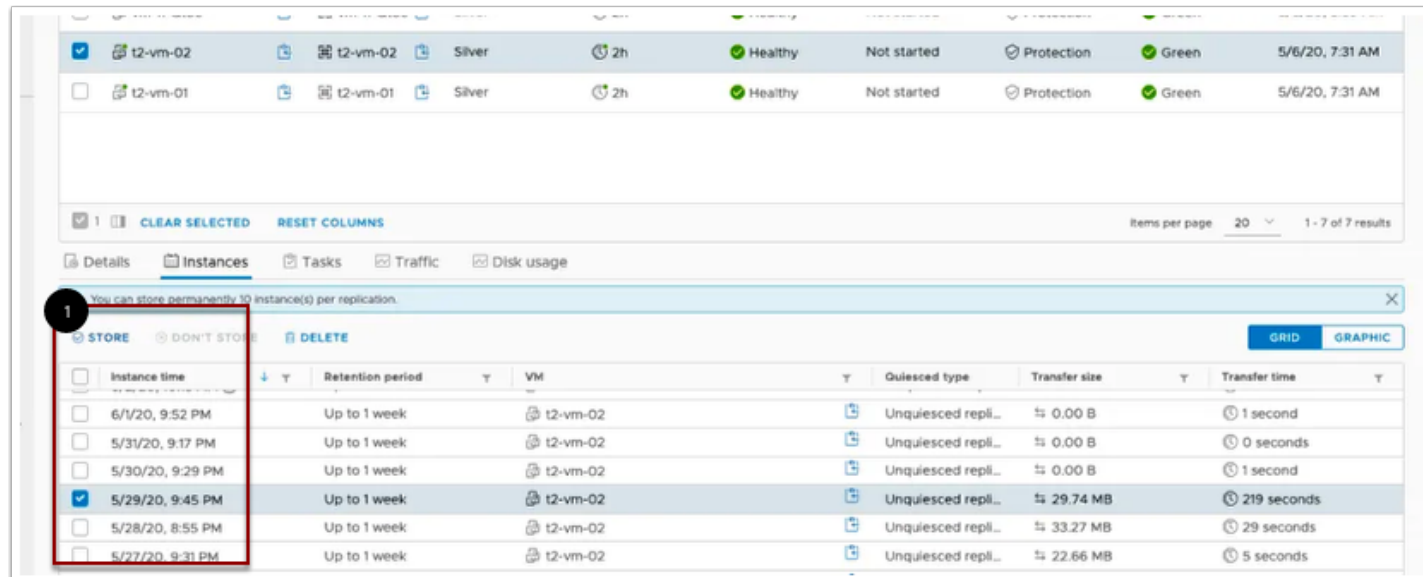
This example showcases how a Silver SLA Profile can be paired with a Silver Policy for an organization

CONSIDERATIONS

- SLA profiles are optional. One can continue with Policies, but we highly recommend these to simplify operations.
- SLA profiles only pertain to protections. They are not utilized for migrations at this time.

- A provider can revise a SLA profile if there is not any active protections consuming this profile. Please be aware of this consideration.

Service Consumption -Stored Instances



The screenshot shows the 'Instances' tab in the VMware Cloud Director interface. A red box highlights the 'STORE' button and a table of stored instances. A callout bubble with the number '1' points to the 'STORE' button.

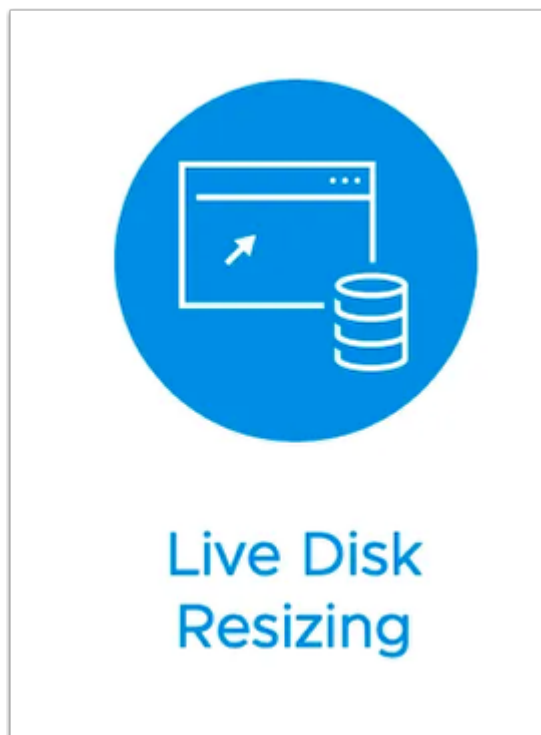
Instance time	Retention period	VM	Quiesced type	Transfer size	Transfer time
☐ 6/1/20, 9:52 PM	Up to 1 week	t2-vm-02	Unquiesced repli...	0.00 B	1 second
☐ 5/31/20, 9:17 PM	Up to 1 week	t2-vm-02	Unquiesced repli...	0.00 B	0 seconds
☐ 5/30/20, 9:29 PM	Up to 1 week	t2-vm-02	Unquiesced repli...	0.00 B	1 second
☒ 5/29/20, 9:45 PM	Up to 1 week	t2-vm-02	Unquiesced repli...	29.74 MB	219 seconds
☐ 5/28/20, 8:55 PM	Up to 1 week	t2-vm-02	Unquiesced repli...	33.27 MB	29 seconds
☐ 5/27/20, 9:31 PM	Up to 1 week	t2-vm-02	Unquiesced repli...	22.66 MB	5 seconds

This is a great new feature. With VMware Cloud Director Availability 4.0, one has the ability to preserve a point in time instance of a protected workload. This would supersede the stated policy, but is still controlled by the provider. This is done within the Policy framework as the selection of the maximum number of stored instances per replication.

1. Upon selection of the Store button, user will receive a confirmation to confirm this selection to make the specific instance Permanent.

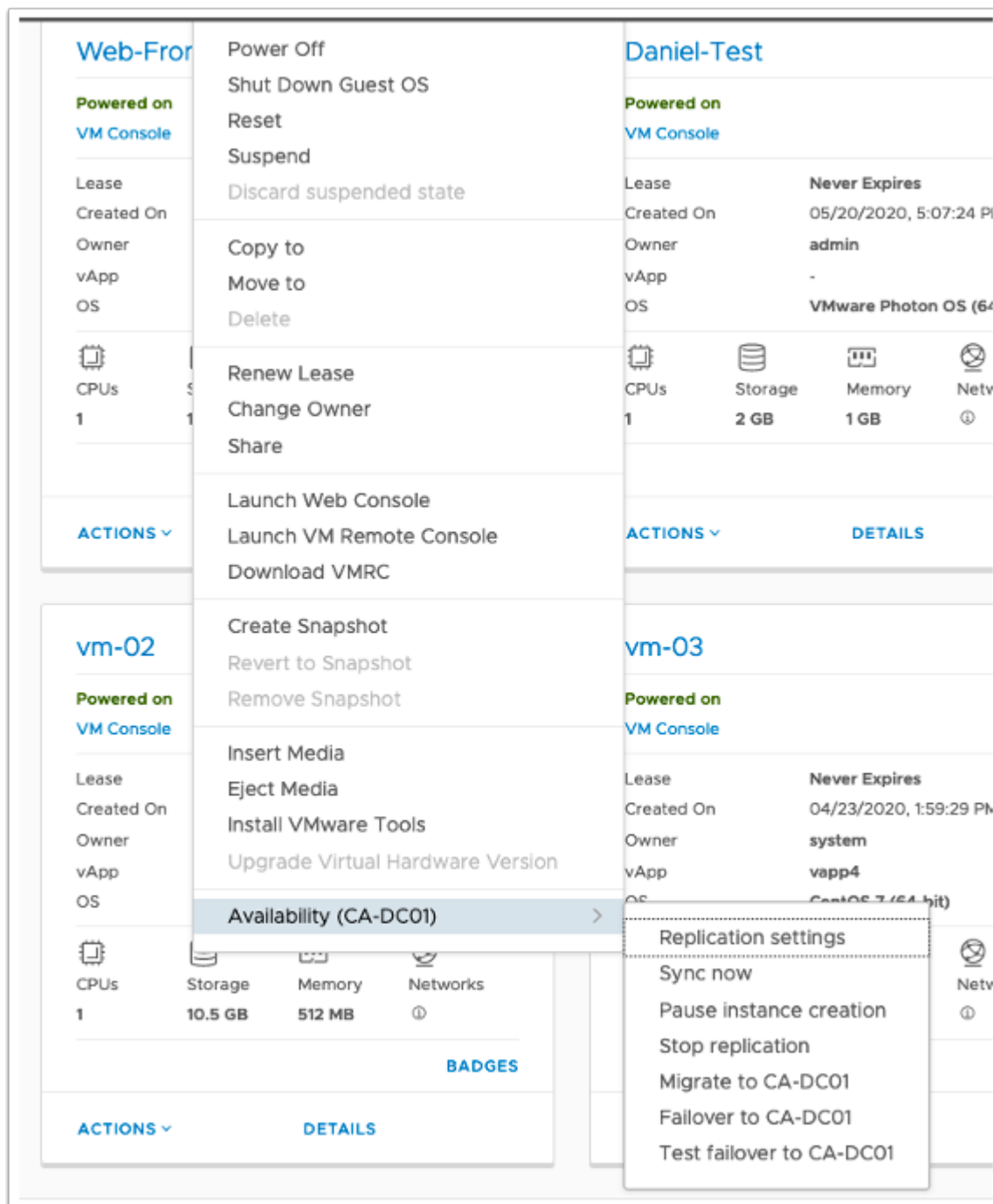
This can be removed or deleted at any time. Do note, storage of any instances impacts any associated disk utilization over a period of time.

Service Consumption -Live Disk Resizing



In the source site with vCenter Server 7.0 and ESXi 7.0, when resizing the disk of the source virtual machine, VMware Cloud Director Availability now automatically resizes the protected virtual machine disk in the destination site, running any supported vSphere version. The existing replication instances are retained. Failover and Test Failover are supported from any instance, before and after the disk resizing. Until the replication instances before the resizing expire, the replica files continue to take the additional storage space. To save the storage space, you can remove the old replication instances or change the retention policy.

Platform Integration - User Experience

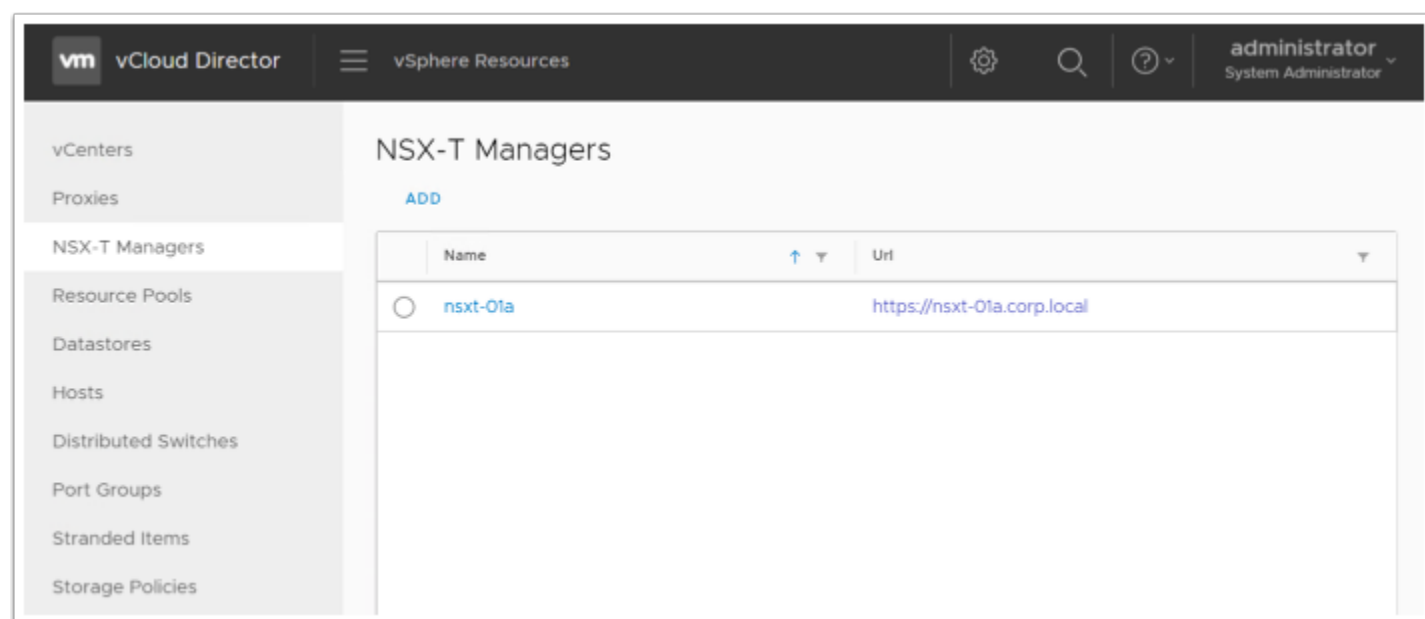


In terms of platform integration, there has been a lot of work to make Cloud Director Availability simpler and easier to consume. This includes improvements such as:

- Icons now represent the main operations.
- Improved workflows and reduced steps in wizards.
- Each workload now has a sub-context menu that shows the details, instances, tasks, traffic, and disk utilization

- Multi-selection is allowed and provides context menus based on the actual selection
- **In-context protection and status from VMware Cloud Director UI** Easier to ascertain protection status and run protective actions right from the vAPP and/or VM in VMware Cloud Director interface, rather than the VMware Cloud Director Availability plugin. Protected vApps and virtual machines now have a protection indicator badge in the interface of VMware Cloud Director. The protection badge is visible to providers in VMware Cloud Director with VMware Cloud Director Availability 4.0 in the source and in the destination cloud site.

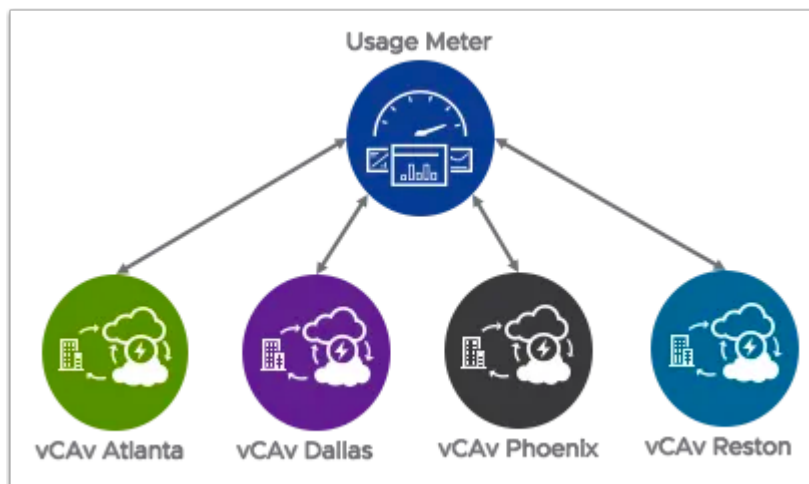
Support and Interoperability with NSX-T



Interoperability with NSX-T: Support for NSX-T is key for cloud providers who are evolving their VMware Cloud Director platform in line with VMware's networking strategy. In on-premises sites and in cloud sites, you can now replicate workloads that use NSX-T networks. You can also use environments with mixed NSX-V and NSX-T networks, and you can replicate workloads from NSX-V to NSX-T, and from NSX-T to NSX-V. VMware Cloud Director Availability does not apply or translate the networking features that VMware Cloud Director and NSX-T do not support. VMware Cloud Director Availability replicates the source site NSX-V to NSX-T NAT-routed vApp networks and bridged vApp networks, and does not replicate the DHCP service.

Note: please refer to the VMware Product Interoperability Matrices (https://www.vmware.com/resources/compatibility/sim/interop_matrix.php) to confirm which versions of VCD, VCD, and NSX-T are supported together.

Usage Meter Integration

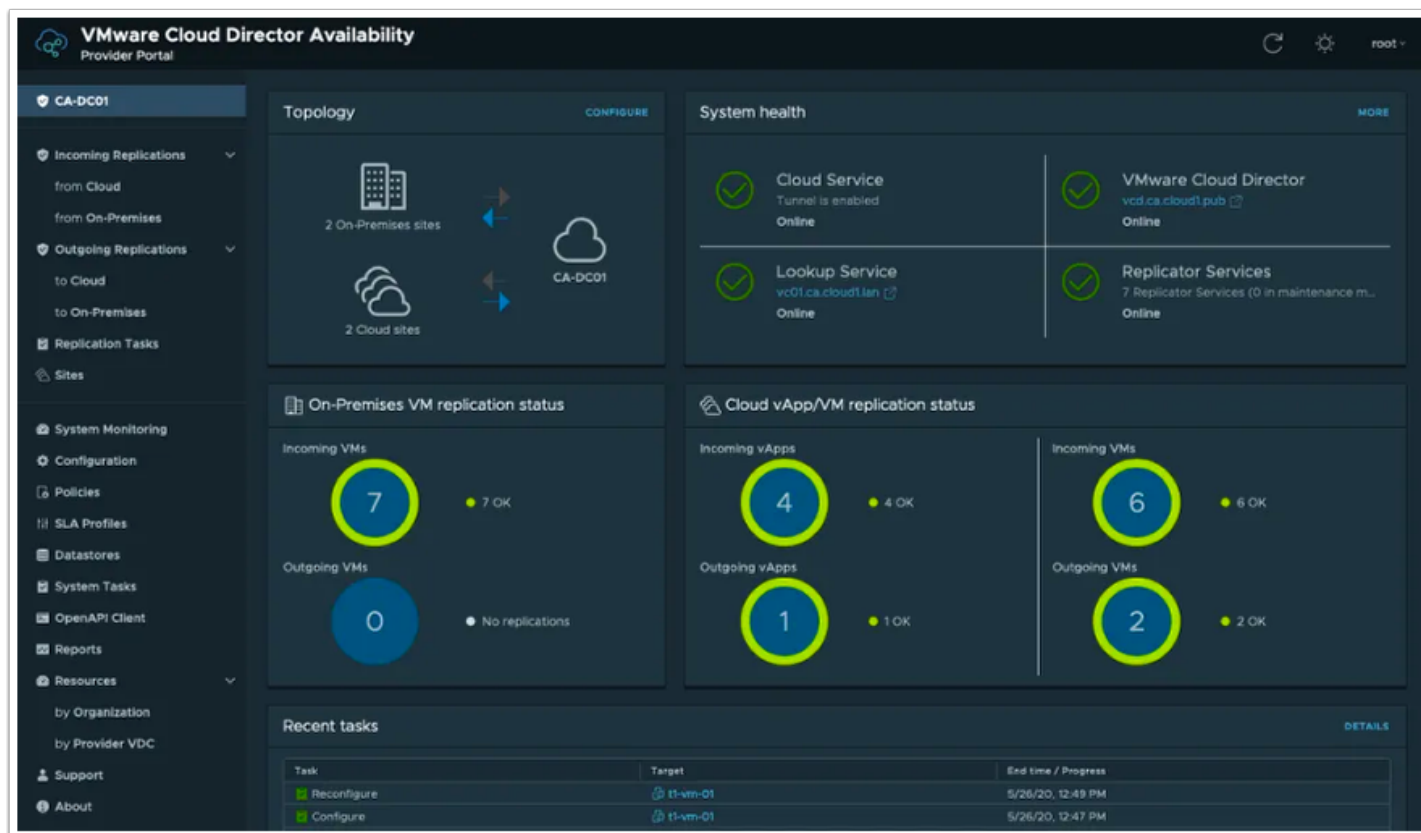


VMware vCloud Usage Meter integration: There is an indication in the management interface that vCloud Usage Meter meters the Cloud Service instance. Any protected workload during the calendar month will count towards the Monthly Usage Units. It will be depicted in the Monthly Usage Report. When vCloud Usage Meter has not requested metering information for more than three days, you now see a warning message in the management interface. VMware Cloud Director Availability has supported automatic metering from Usage Meter since 3.6.1. Hot Patch 3.

In addition, another great capability added to VMware Cloud Director Availability 4.0 is -

Multi-NIC traffic conditioning enables configuring multiple nics leading to advanced network setups with higher security requirements and optimization of the replication data traffic. Providers can configure on-premise tunnel environments to send replication traffic from on-premise to cloud via nic1 (connected to public network) and go out from a tunnel to a cloud replicator via nic2 (connected to private network). Replicator traffic can be similarly conditioned to tunnel to replicator over nic1 (internal provider network) and replicator to esxi over nic2 (high-throughput replication data network).

VMware Cloud Director Availability 4.0 Configuration Limits



For the tested uptime, concurrency, and scale limits of VMware Cloud Director Availability 4.0 -

1. Scale Limits

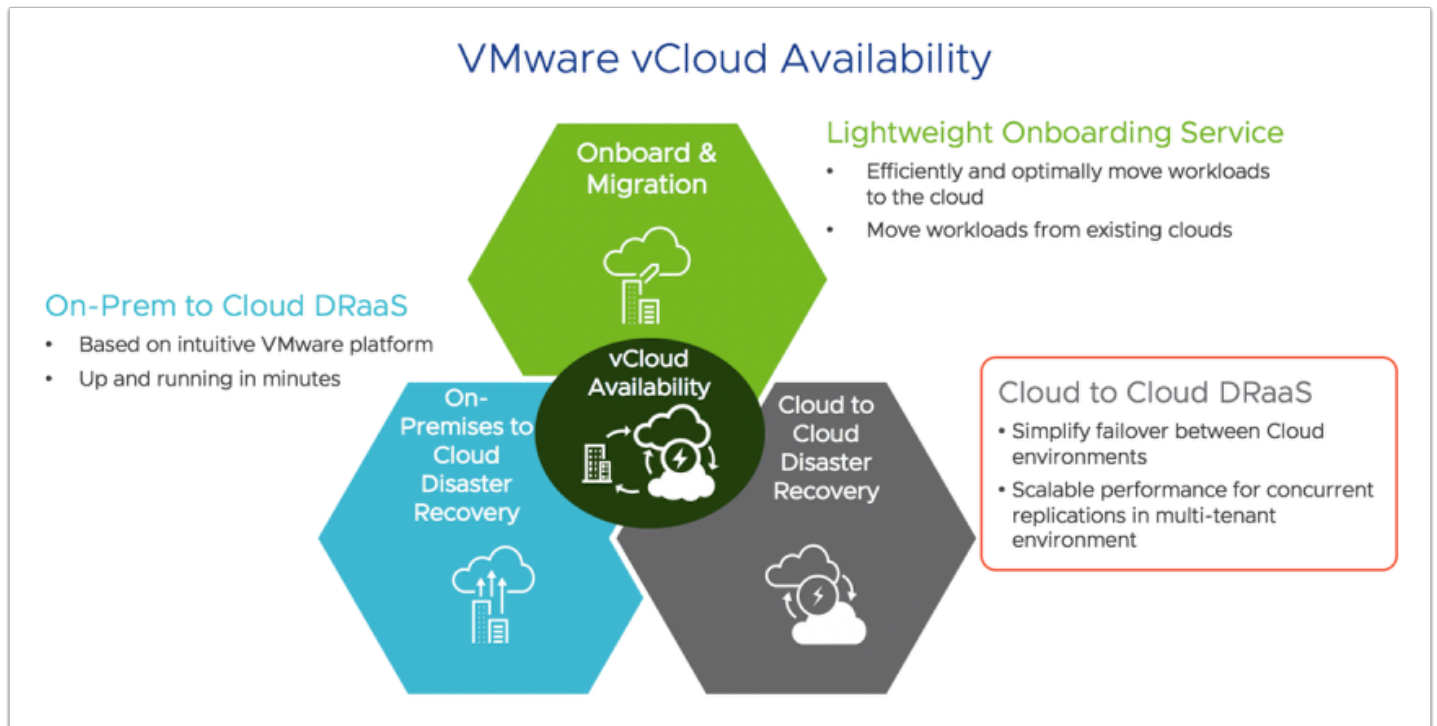
- Tenants with active protection paired to a cloud site - 500**
- Active protections across tenants to a cloud site - 15000**
- Protected virtual machine size - 15 TB** The maximum protected VM size depends on the size of a single data store available in the cloud.
- Cloud Replicator Appliance instances per cloud site - 30**
- Active protections per Cloud Replicator Appliance instance - 2000**

2. Concurrency Limits

- Concurrent Protect & Test Failover & Failover & Reverse protect operations from on-premises to a cloud site - 200**
- Concurrent Protect & Test Failover & Failover operations from a cloud site to a cloud site - 200**
- Concurrent Reverse protect operations from a cloud site to a cloud site - 200**

Note: please refer to <https://configmax.vmware.com> for the latest configuration limits.

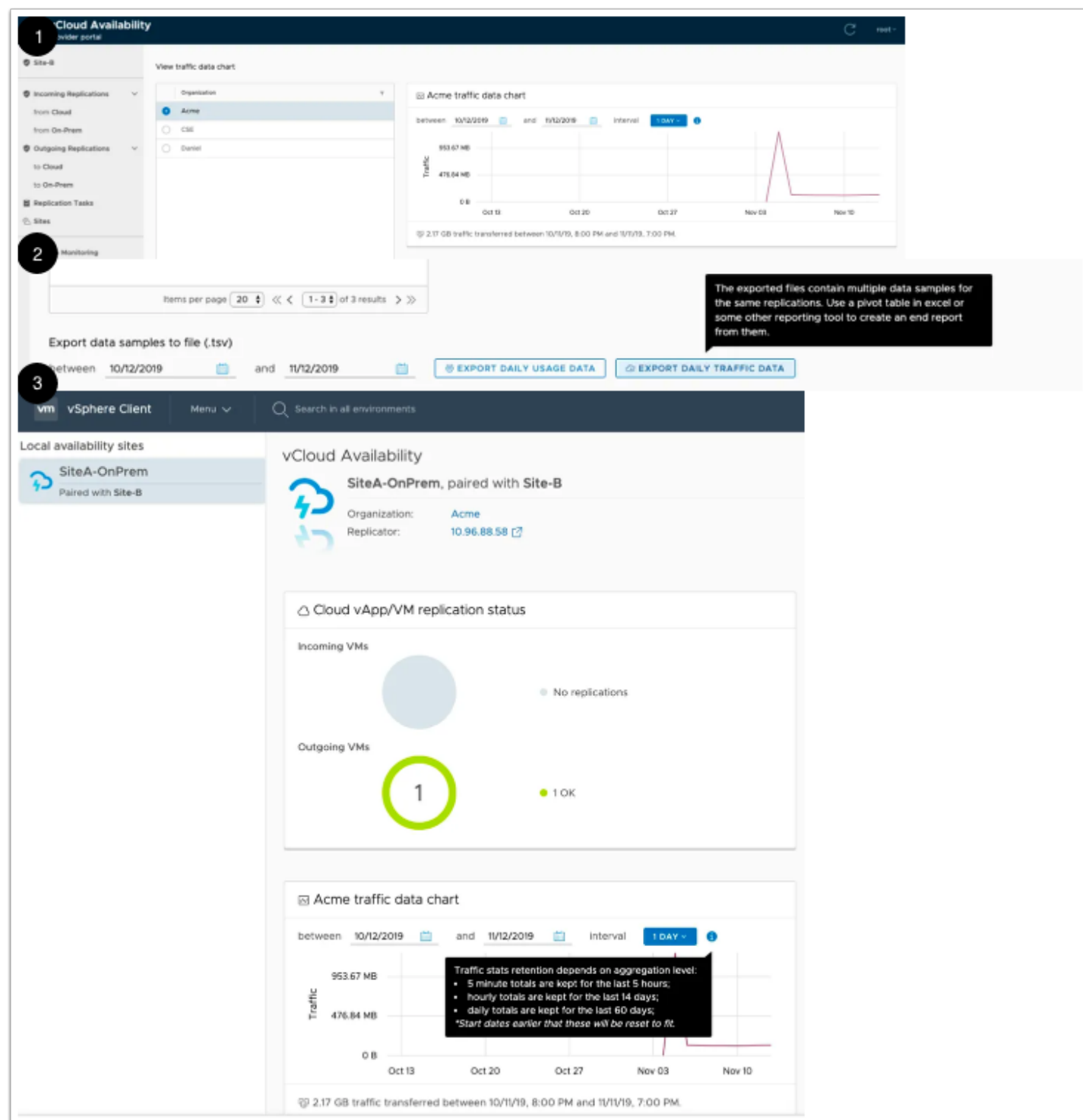
What's New in VMware vCloud Availability 3.5



Lets review new technical additions that are now part of the VMware vCloud Availability 3.5. VMware vCloud Availability 3.5, or vCAv, is a comprehensive Disaster Recovery as a Service and Migration platform. Here are the few features that were added in VMware vCloud Availability 3.5

1. Bandwidth UI Visibility
2. Automatic vCAv Metering by Usage Meter -We already reviewed this enhancement early in the module.
3. Regional Data Center Support and Flexible Network Connectivity
4. Enhanced Grouping and Protection Workflows
5. Operational Enhancements

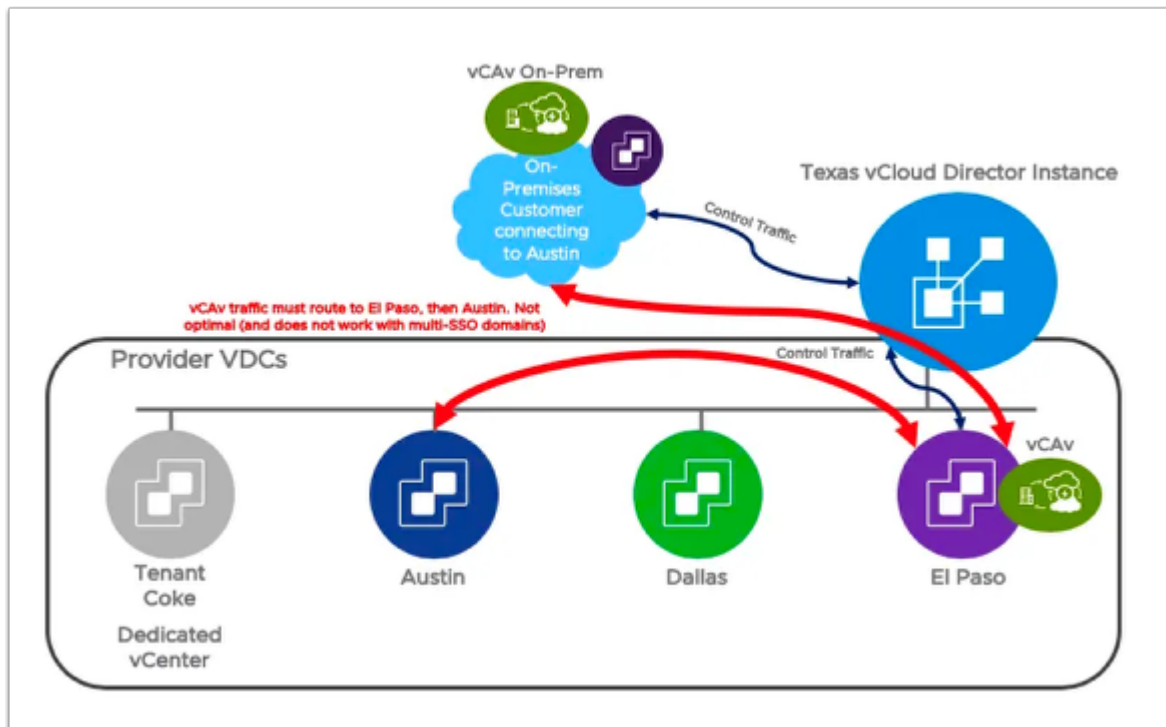
What's New in VMware vCloud Availability 3.5 - Bandwidth UI Visibility



1. Within the Provider User Interface (UI), we can see traffic utilization on a per organization basis, but also on a per-VM/vApp basis.
2. Moreover, these traffic statistics can be exported out to a tab-delimited file (TSV) for ease of consumption.

3. Within the on-premises vSphere plugin, we can see similar data available on a per-org or workload basis.

What's New in VMware vCloud Availability 3.5 - Regional Data Center Support and Flexible Network Connectivity



Regional Data Center Support

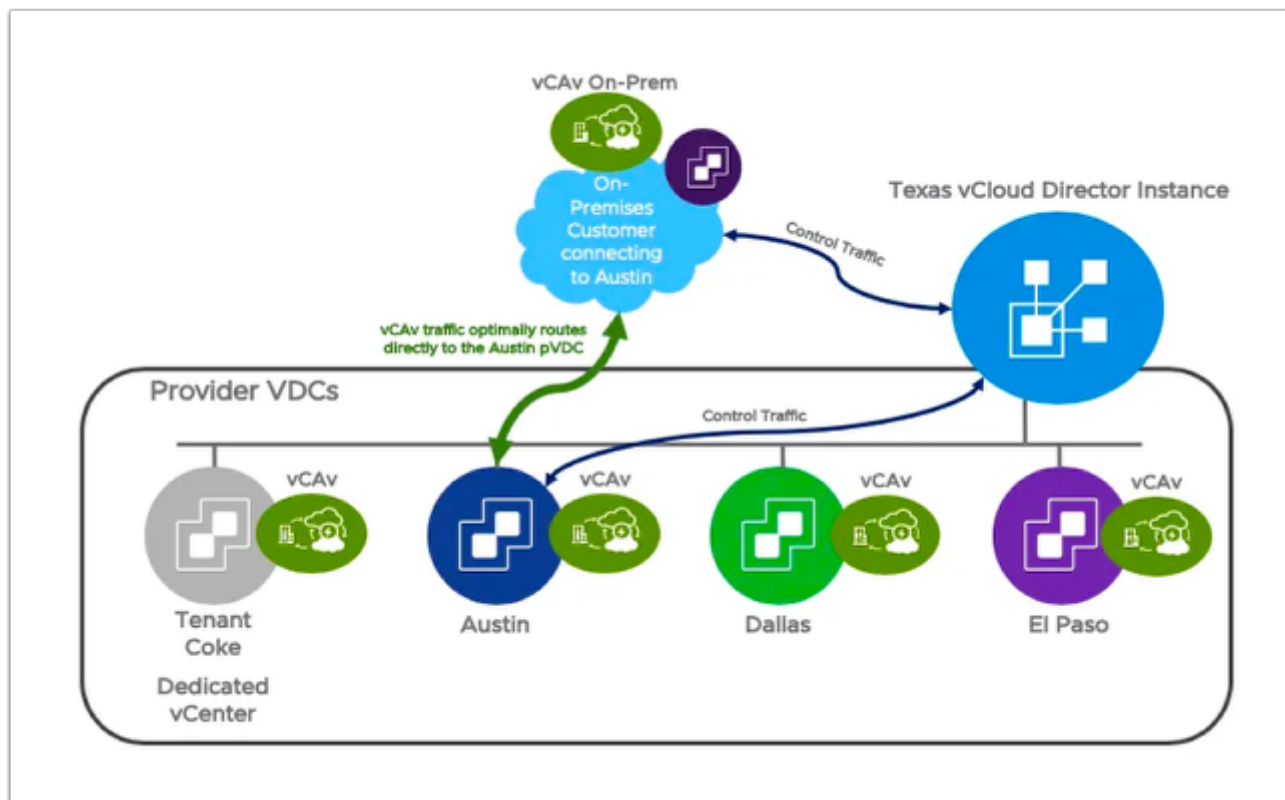
One of the main requests was the ability to optimally route vCAv traffic. This is extremely important for multiple regional data centers inside of a single VCD instance. Lets start off with a diagram that lays out this scenario.

BEFORE

Previously, we could only deploy a single vCAv instance per VCD platform. In the diagram below, we have multiple Texas-based data centers where workloads and organizations reside.

If we had an on-premises customer that wanted to protect workloads to Austin, this would have to traverse to El Paso first (since the vCAv stack resides there), then route to Austin. Not an efficient use of resources. Moreover, this did not work when crossing multiple SSO domains.

What's New in VMware vCloud Availability 3.5 - Regional Data Center Support and Flexible Network Connectivity (contd..)

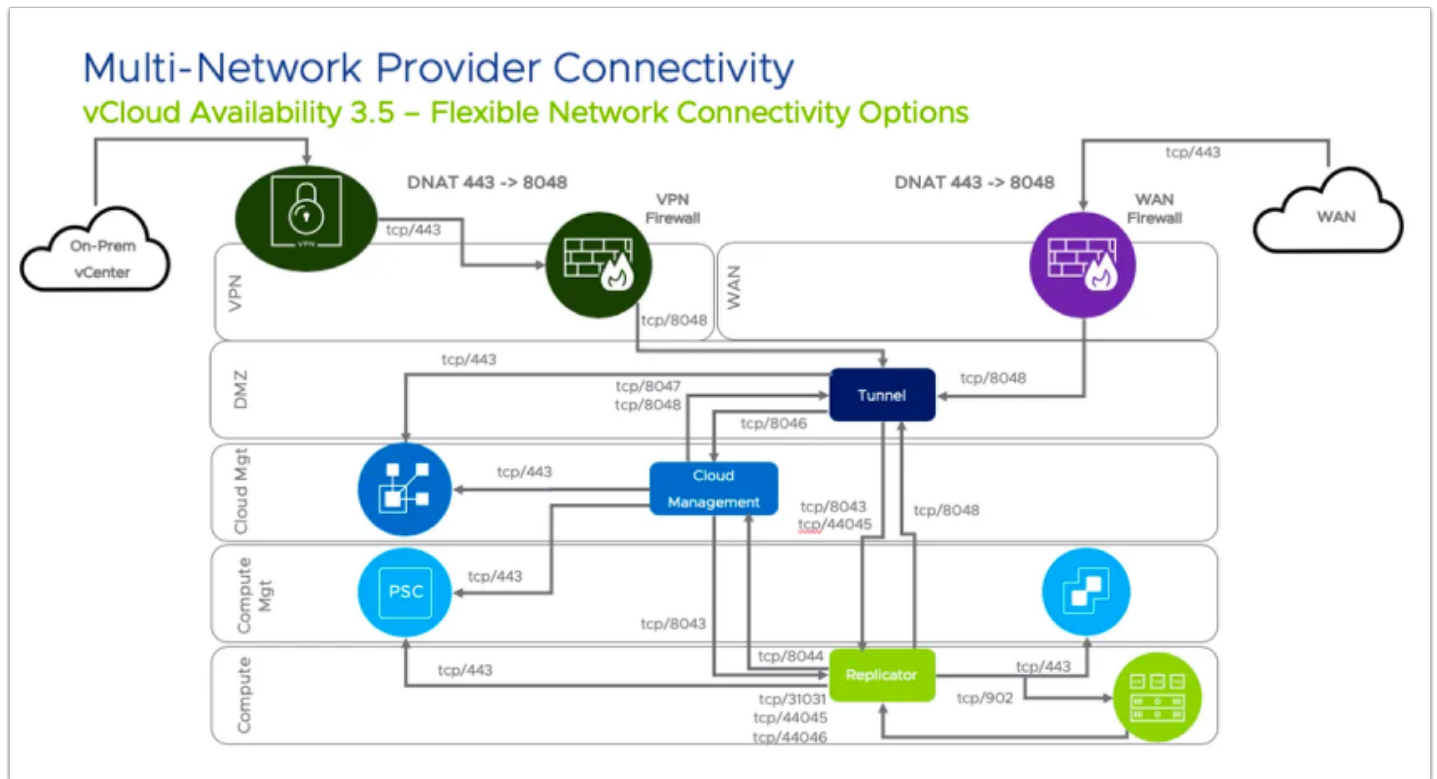


WITH VCAV 3.5

With 3.5, the logic and foundation has been changed to allow for multiple vCAv deployments per VCD instance. Moreover, we can optimally route traffic directly to Austin once control traffic traverses the VCD instance. Therefore, we now have a design like in the image.

Moreover, this allows for support multiple SSO domains.

What's New in VMware vCloud Availability 3.5 - Flexible Network Connectivity



Lets review this new enhancement for flexible northbound connections for Cloud Providers. It is very evident that Cloud Provider want to control replication (protection) traffic and consume across multiple northbound links Wide Area Networks (WAN), Virtual Private Network (VPN), Direct Connection, and so forth.

With vCAv 3.5, the platform introduces flexibility to allow for multiple endpoint inbound connections. Lets review the image.

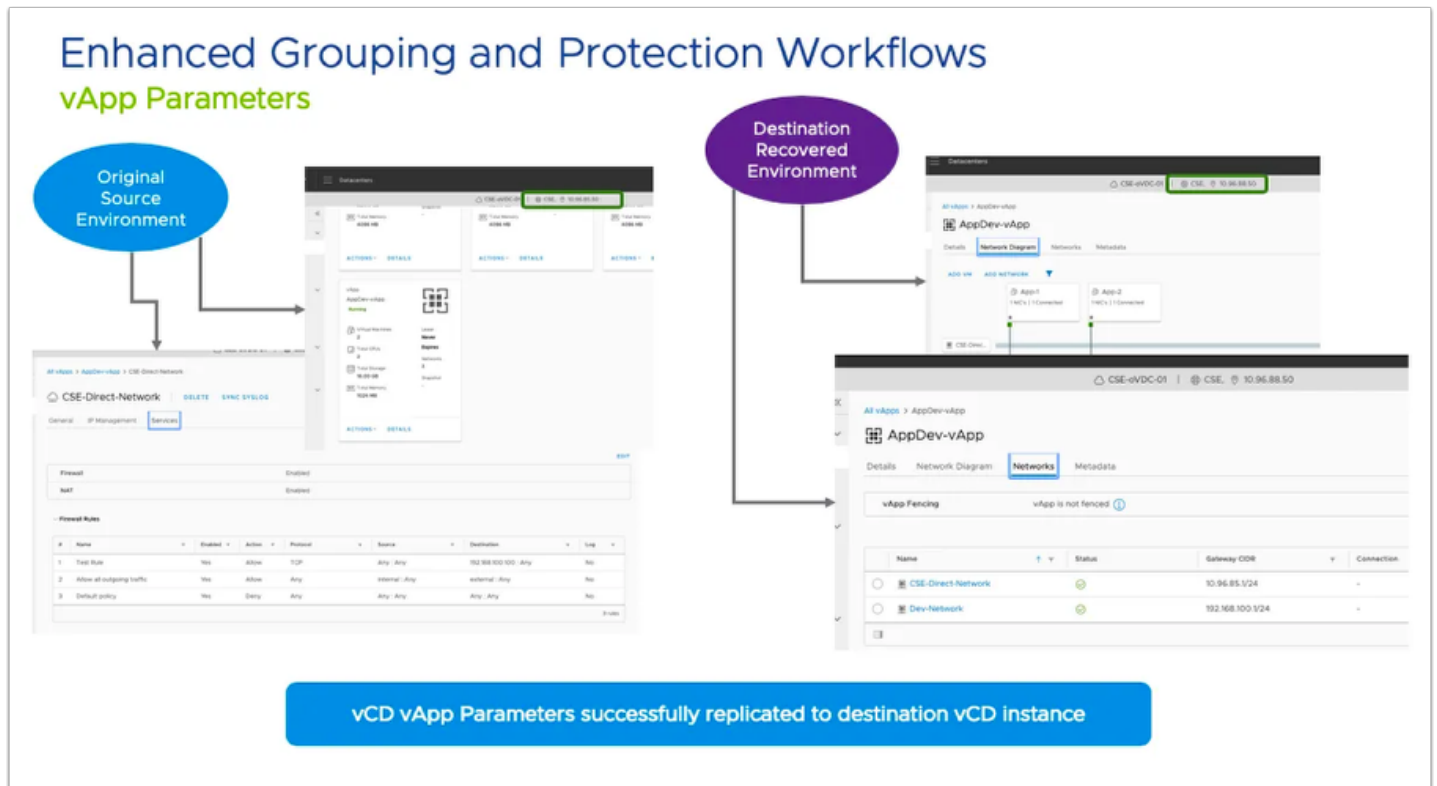
From the image, we can see we have our traditional WAN connectivity that terminates to the Tunnel via a DNAT rule for inbound connections. Nothing different there.

However, we now can to route other types of northbound traffic. In the example above, we have a dedicated VPN connection. The traffic routes to the vCAv Tunnel which then terminates on the Cloud Replication Manager (CRM) instance.

Previously, this was not allowed. All traffic had to route through the external endpoint URL, which typically sat on the WAN.

The result is further flexibility for Cloud Providers that allows for optimal routing of vCAv traffic.

What's New in VMware vCloud Availability 3.5 - Enhanced Grouping and Protection Workflows



For on-premises to cloud replications, you can create a collection of virtual machines in a single container, managed and replicated as a single unit. You can specify the virtual machines boot order, boot delays, and protect or migrate them as a single vApp replication in the destination cloud site. During the protection workflow, one can select Advanced Settings and select specific VMDKs they want to protect or exclude

In the destination cloud site, the grouped multiple virtual machines are represented as a vApp replication. In this vApp, the virtual machines relations are:

- The boot order works from top to bottom.
- By default, there is no set boot delay. The start wait is measured as the time that passed after the boot of the previous virtual machine.

Partial Failover

You can perform replication operations on the vApp or on a single virtual machine from the vApp.

Failing over one of the virtual machines from a vApp replication, in the destination site results in two vApp replications with the same name. One replication contains the failed over virtual machine and the other replication contains the remaining virtual machines that are not failed over.

What's New in VMware vCloud Availability 3.5 - vApp Network Properties

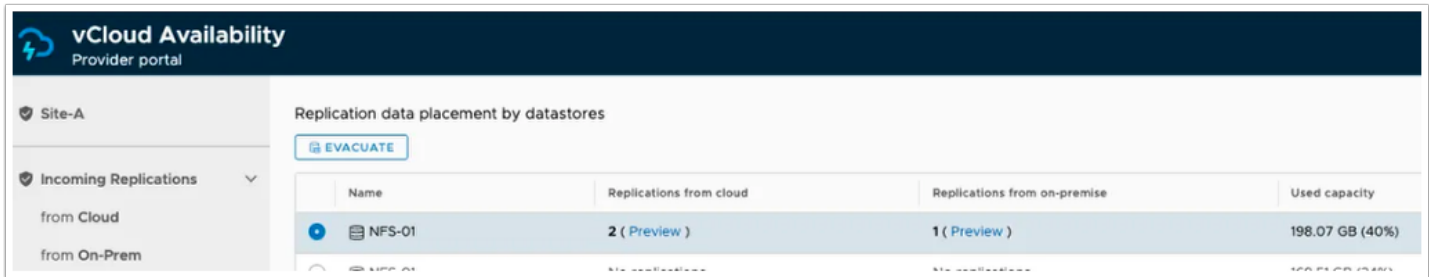
With vCAv 3.5, we are now able to replicate some vApp network characteristics within the vApp. The following list is what is available for protection:

- Network Type (Isolated/Routed/Direct)
- Gateway/DNS
- Connection Type
- Edge Firewall and NAT
- DHCP
- Static Pools
- Guest OS Customization
- OVF properties

For on-premises to cloud, or cloud to cloud replications, you can set the target network settings of a vApp or virtual machine. vCloud Availability applies these network settings in the target cloud site, after a migration, failover, or a test failover.

- For the cloud to cloud replications, vCloud Availability replicates all the types of source vApp networks in the target cloud site: Isolated, bridged (direct) and fenced (NAT-routed) networks. vCloud Availability replicates the source networks settings like: IP pools, NAT routes, firewall rules, and DNS settings, in the target site.
- For the on-premises to cloud replications, vCloud Availability creates a new bridged vApp network in the target cloud site and you can configure the vApp network settings.

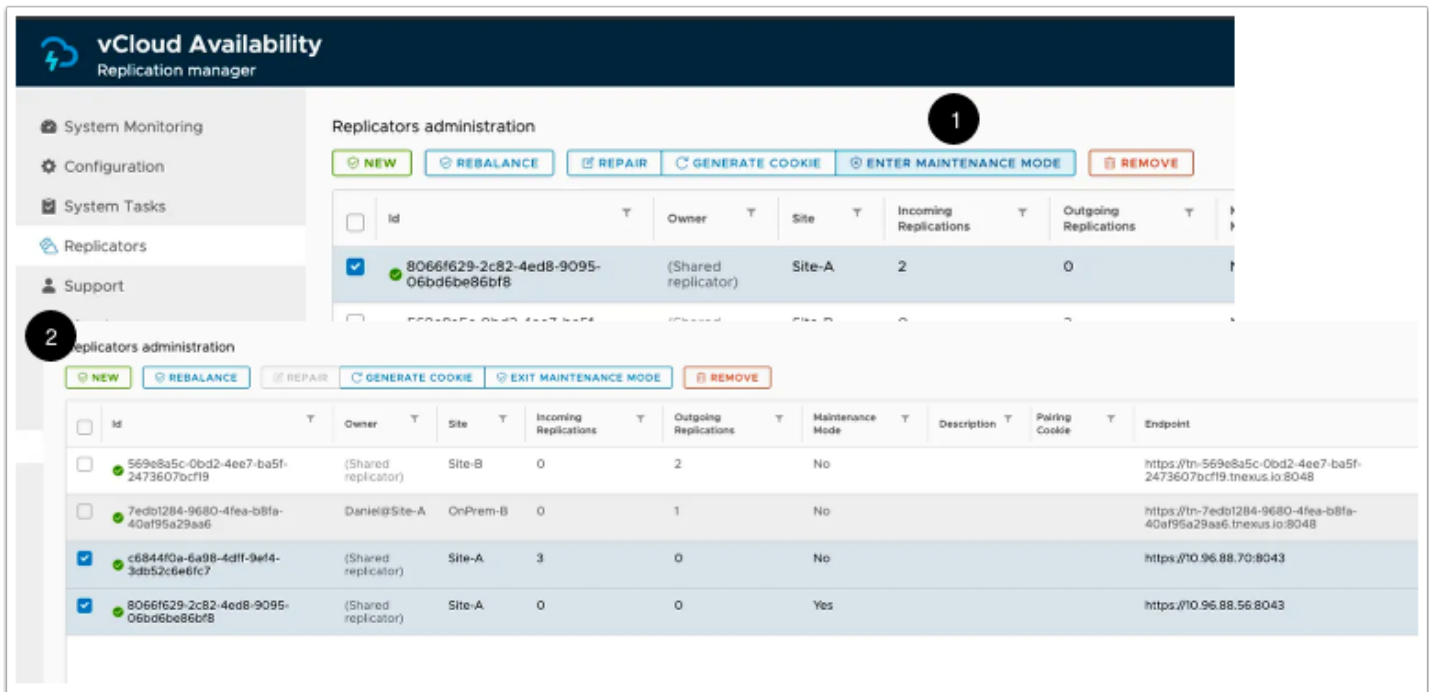
What's New in VMware vCloud Availability 3.5 - DATASTORE EVACUATION



We can now migrate protected instances to another storage policy (datastore) for operational maintenance activities. This allows our tenants to continue to meet their specified recovery point objectives (RPOs) while not disrupting any existing protected workload.

For a provider to execute a datastore evacuation, select Datastores on the left panel. From there, its easy as hitting the Execute button and selecting your destination Storage Policy.

VWhat's New in VMware vCloud Availability 3.5 - REPLICATOR MAINTENANCE MODE

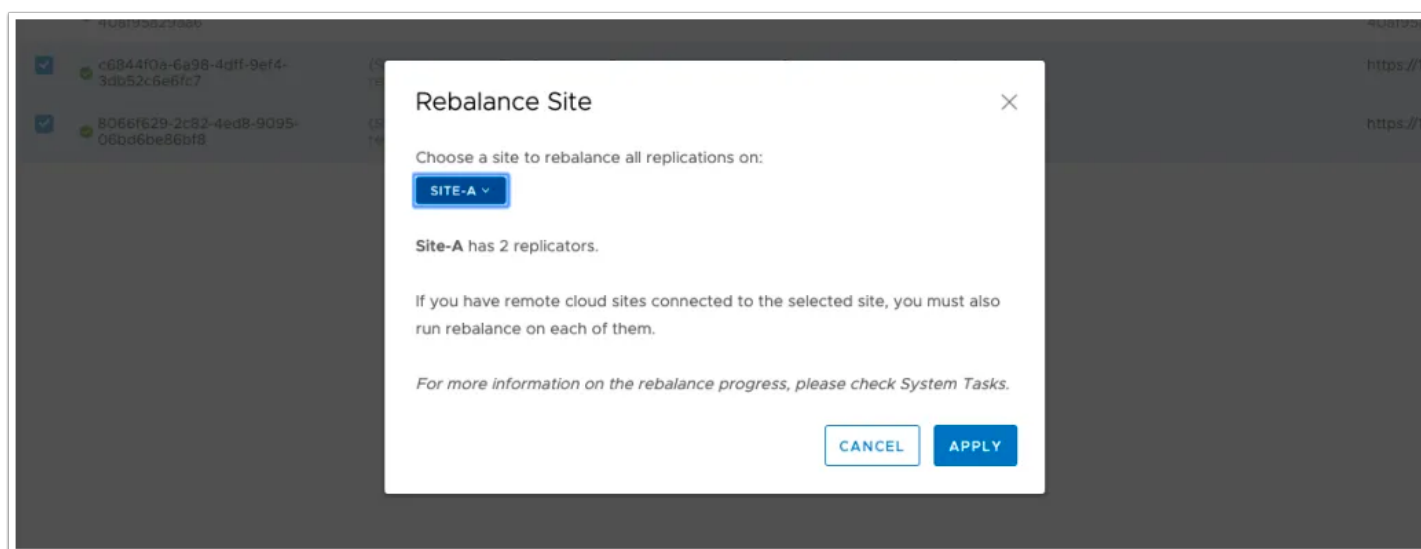


vCAv can put a replicator in maintenance mode during any operational activities. Again, this minimizes any potential tenant/organization disruption. The Cloud Provider executes on these operations within the Replication Manager UI from the CRM instance.

1. To execute on a replicator maintenance mode operation, select the specified replicator and click Enter Maintenance Mode from the UI.
2. Upon completion, we can see my replicator in maintenance mode while all traffic is now residing on my remaining replicator instance for this specific site.

Once your maintenance operation has been completed, we can then exit Maintenance Mode.

VWhat's New in VMware vCloud Availability 3.5 - REBALANCING OF REPLICATIONS



To distribute the incoming replications evenly over all vCloud Availability Replication instances in the site, you can rebalance the replications.

vCloud Availability assigns all new replications to the vCloud Availability Replicator with the fewest number of replications in the site. After adding an extra vCloud Availability Replicator instance, vCloud Availability assigns all new replications to the new vCloud Availability Replicator instance. Replications that existed before adding the new vCloud Availability Replicator instance remain assigned to the previous vCloud Availability Replicator instances. The result is an unequal balance of the number of replications per vCloud Availability Replicator instance. You can see how many replications are assigned to each vCloud Availability Replicator instance and rebalance the replications. This operation migrates the replications from vCloud Availability Replicator instances with more replications to vCloud Availability Replicator instances with fewer replications.

This brings us to the end of reviewing new enhancements in VMware Cloud Director Availability 4.0 and 3.5.

Congratulations on completing Module 1!!

Conclusion

In this module, we learned about the overview and new features of VMware vCloud Director Availability 4.0 and VMware vCloud Director Availability 3.5

You've finished Module 1

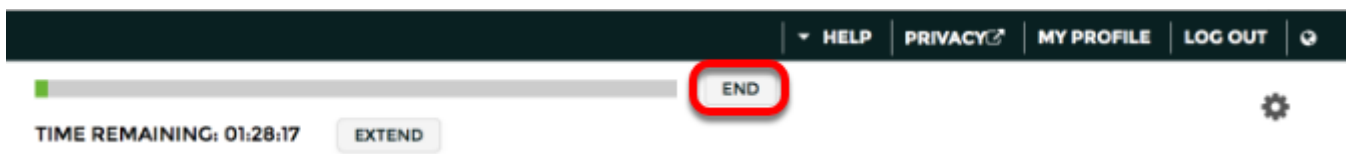


Congratulations on completing Module 1.

Proceed to any module below which interests you most.

- [Module 2 - On-Prem DR and Migration to Cloud with VMware Cloud Director Availability](#) (45 Minutes) (Basic) This module will walk through the steps to pair On-Premises site with Cloud and how to use VMware Cloud Director Availability for disaster recovery and migration from on-prem to cloud.
- [Module 3 - Administrator-driven Cloud-to-Cloud DR with VMware Cloud Director Availability](#) (30 minutes) (Basic) This module will show how administrators can use Cloud Director Availability for cloud-to-cloud DR.
- [Module 4- Tenant-driven Cloud-to-Cloud DR with VMware Cloud Director Availability](#) (30 minutes) (Basic) This module will show Tenant Self-Service Cloud-to-Cloud DR using VMware Cloud Director Availability.

How to End Lab



To end your lab click on the **END** button.

Module 2 - On-Prem DR and Migration to Cloud with VMware Cloud Director Availability

Introduction

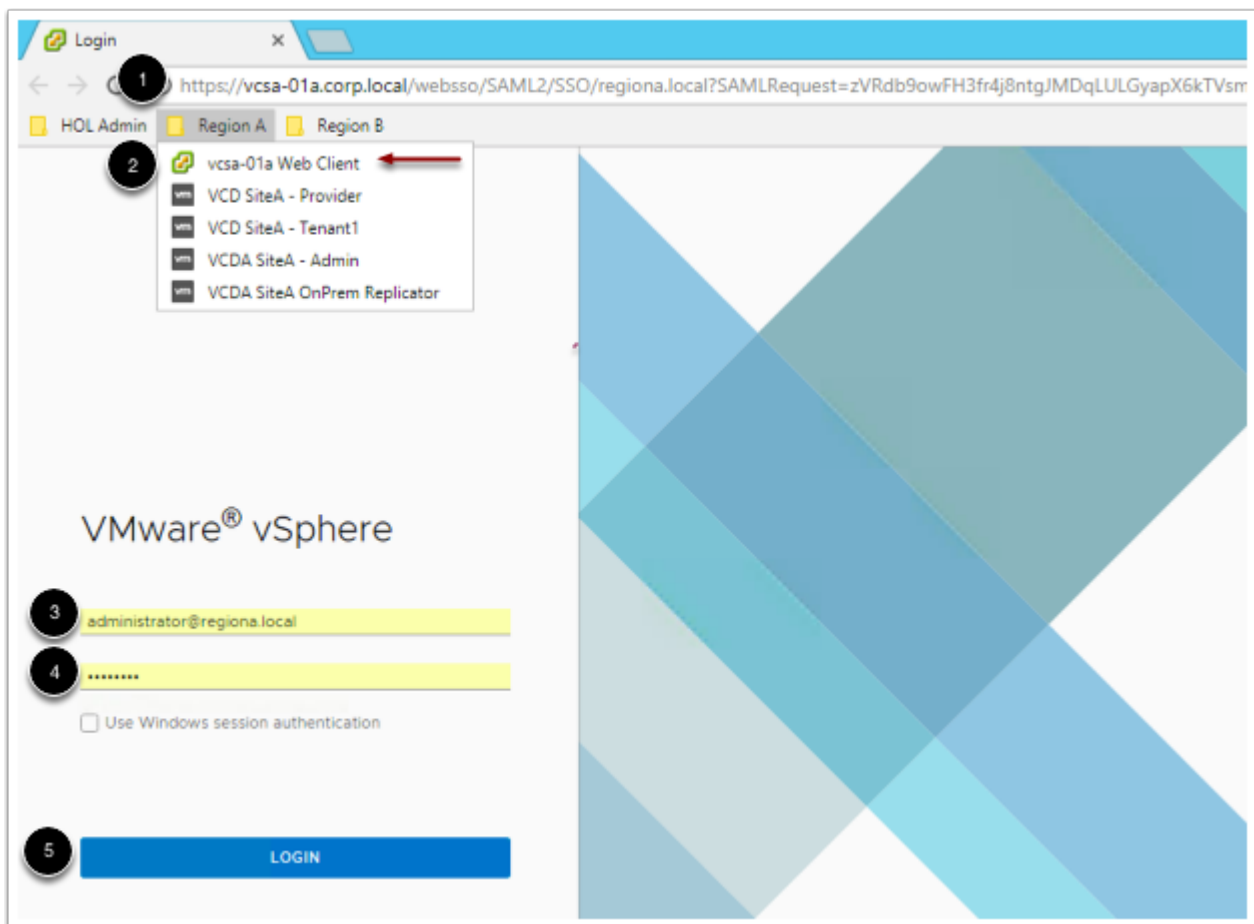
In this module, you will learn -

- Step-by-Step instructions to pair On-Premises site with Cloud
- Configure replication from On-Premises to Cloud
- Test Failover/ Test Cleanup the VM in Cloud
- Run Failover to Cloud
- Reverse replication of the VM from Cloud to On-Premises
- Migrate the VM back from Cloud to On-Premises
- Reprotect the VM from On-Premises to Cloud

Site Pairing from On-Premises to Cloud using VMware vCloud Director Availability

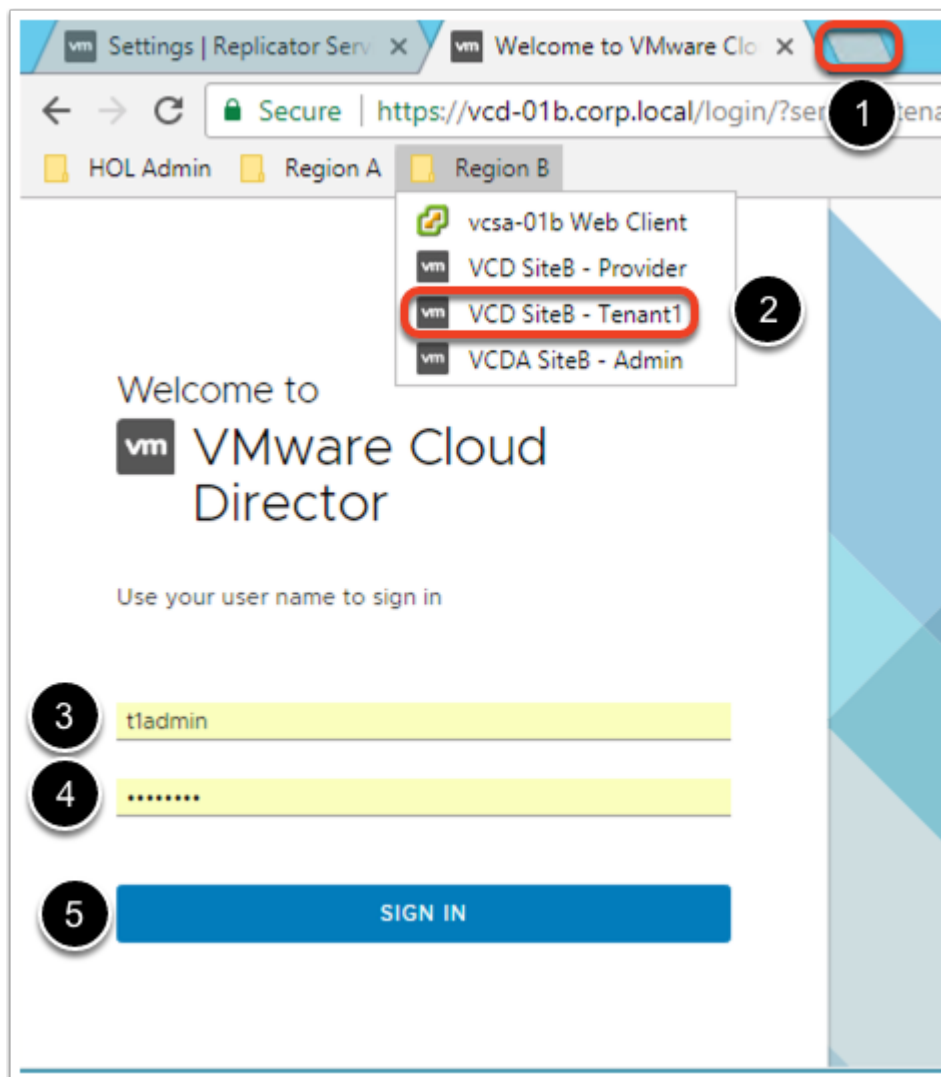
In this exercise, we will be pairing our On-Premises vSphere Instance with the Cloud Instance.

Login to RegionA vCenter (On-Premise)



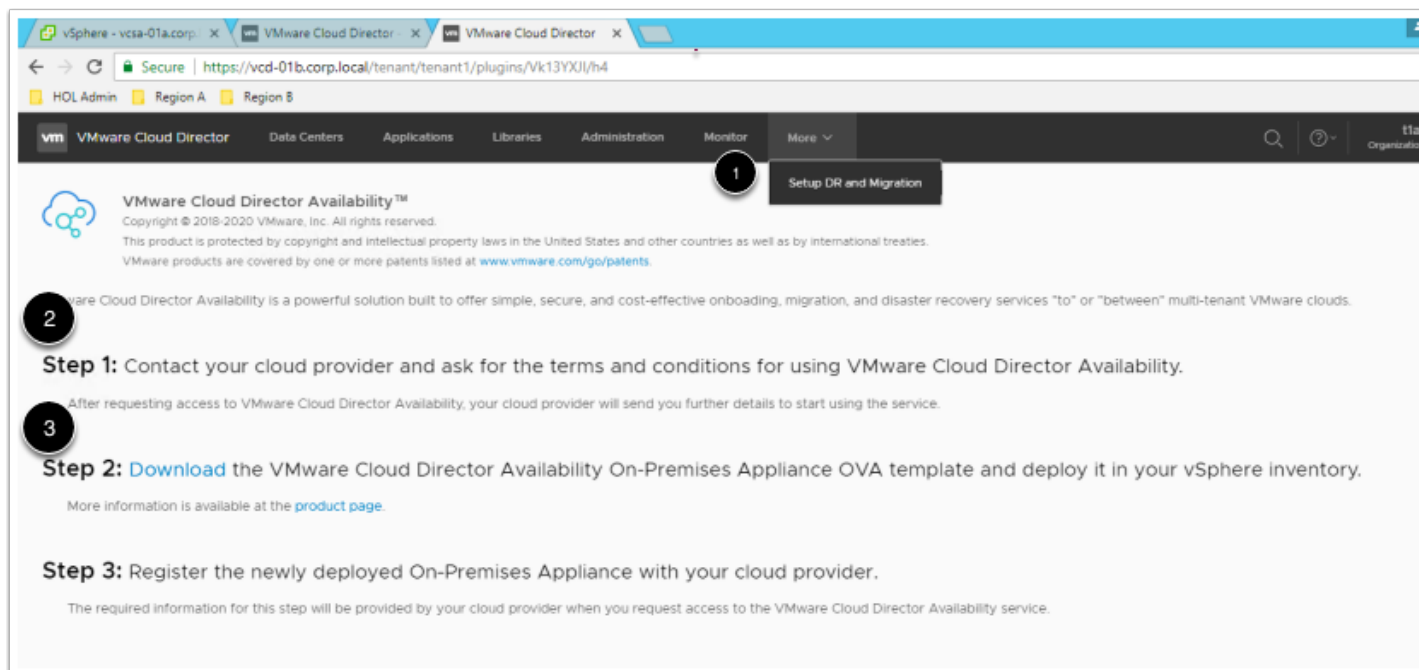
1. Start the Chrome Browser from the desktop. Click on **RegionA** in the bookmarks bar.
2. Click on vcsa-01a Web Client. Verify the address as : **https://vcsa-01a.corp.local/**
3. Enter Username: **administrator@regiona.local**
4. Enter Password: **VMware1!**
5. Click on **LOGIN**

Login to RegionB Tenant



1. Open a new browser tab
2. In the bookmarks bar, click on **Region B** and select **VCD SiteB - Tenant1**
3. Username: **t1admin**
4. Enter Password: **VMware1!**
5. Click on **Sign In**

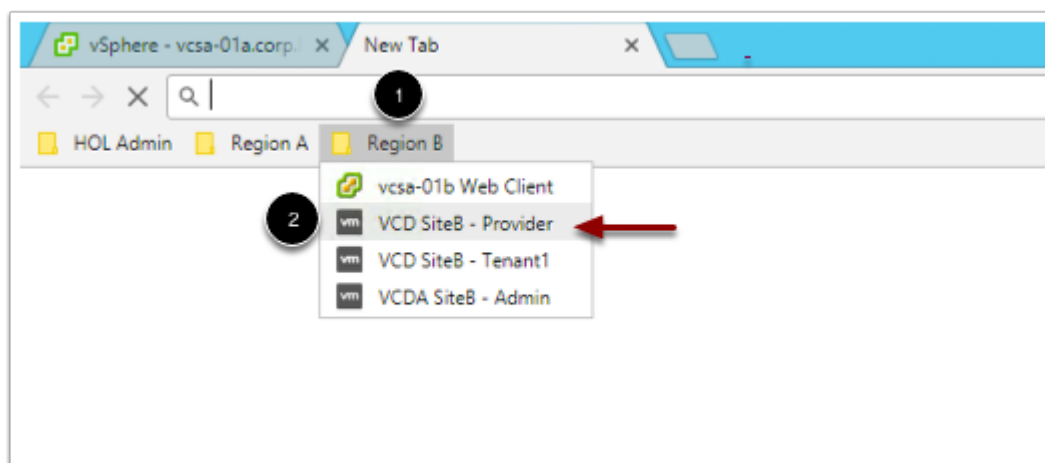
VMware Cloud Director Availability at Tenant SiteB



1. Click on **More - Setup DR and Migration**

This page outlines the steps to be completed in order to use VMware Cloud Director Availability service. We need the Cloud Administrator to configure VMware Cloud Availability so we can use it as a tenant.

Open SiteB Provider Interface



Now we will play the part of the Cloud Administrator and configure VMware Cloud Availability so Tenant1 can use it.

1. On the chrome browser, click on **RegionB** in the bookmarks bar.
2. Select **VCD SiteB - Provider**

Login to SiteB Cloud

vSphere - vcsa-01a.corp x Welcome to VMware Cloud Director x

Secure | <https://vcd-01b.corp.local/login/?service=provider&redirectTo=%2Fprovider%2F>

HOL Admin Region A Region B

Welcome to
vm VMware Cloud Director

Use your user name to sign in

1 administrator

2

3 SIGN IN

1. Username: **administrator**
2. Enter Password: **VMware1!**
3. Click on **SIGN IN**

Open Tenant1-OVDC-B

The screenshot shows the VMware Cloud Director interface. The top navigation bar includes 'vm', 'VMware Cloud Director', 'Resources', 'Libraries', 'Administration', 'Monitor', and 'More'. Below this, there are tabs for 'Cloud Resources' and 'vSphere Resources'. The left-hand navigation bar lists 'Organizations', 'Organization VDCs' (highlighted with a red circle and a '1' in a black circle), 'Organization VDC Templates', 'Provider VDCs', 'Cloud Cells', 'Edge Gateways', 'External Networks', and 'Network Pools'. The main window is titled 'Organization VDCs' and features a 'NEW' button. Below the button is a table with columns: Name, Status, State, and Actions. The table contains two rows: 'Tenant1-OVDC-A' and 'Tenant1-OVDC-B' (highlighted with a red circle and a '2' in a black circle). Both rows show a status of 'Enabled' and a state of 'A' or 'F'.

Name	Status	State	Actions
Tenant1-OVDC-A	Enabled	A	
Tenant1-OVDC-B	Enabled	F	

First, we need to expand the resources in Tenant1-OVDC-B.

1. Click **Organization VDCs** in the left-hand navigation bar
2. Click the **Tenant1-OVDC-B** name in the main window

Edit Allocation

The screenshot shows the VMware Cloud Director interface. The top navigation bar includes 'vm VMware Cloud Director', 'Resources', 'Libraries', 'Administration', 'Monitor', and 'More'. Below this, the 'Cloud Resources' tab is selected, showing a sidebar with 'Organizations', 'Organization VDCs', 'Organization VDC Templates', 'Provider VDCs', 'Cloud Cells', 'Edge Gateways', 'External Networks', 'Network Pools', and 'VM Sizing Policies'. The main content area shows the path 'All Organization VDCs > Tenant1-OVDC-B'. The 'Tenant1-OVDC-B' header includes a cloud icon, the name, and buttons for 'OPEN IN TENANT PORTAL', 'DISABLE', and 'DELETE'. A left-hand menu lists 'General', 'Allocation' (highlighted with a red box and a circled '1'), 'Storage', 'Network Pool', 'Metadata', 'Resource Pools', 'VM Placement Policies', and 'VM Sizing Policies'. The right-hand pane shows the 'Allocation Model' section with a red box around the 'EDIT' button and a circled '2'. Below the 'EDIT' button, the 'Allocation Model' section is expanded, showing 'Allocation Model', 'Elasticity', and 'Include VM Memory Overhead'. The 'CPU' section is also expanded, showing 'CPU allocation used', 'CPU allocation', and 'CPU limit'.

1. Click on **Allocation**
2. Click **Edit**

Edit Allocation (cont'd.)

Edit Allocation

Allocation Model: Flex

Elasticity: ☐

Include VM Memory Overhead: ☒

CPU allocation: 1 3 GHz ⓘ

CPU limit: ☐ 3 GHz ⓘ
☒ Unlimited

CPU resources guaranteed: 0 % ⓘ

vCPU speed: 1 GHz ⓘ

Memory allocation: 1024 MB ⓘ

Memory resources guaranteed: 20 % ⓘ

Total Provider VDC Consumption

CPU

Available	0.95 GHz
Allocated	210.08% (2 GHz / 0.95 GHz)
Reserved	0% (0 GHz / 0.95 GHz)
Used	0% (0 GHz / 0.95 GHz)

Memory

Available	2.87 GB
Allocated	32.58% (1 GB / 3.07 GB)
Reserved	6.55% (0.2 GB / 3.07 GB)
Used	6.52% (0.2 GB / 3.07 GB)

DISCARD

2 **SAVE**

1. Change CPU Allocation to 3 GHz
2. Click **Save**

Go to Availability (SiteB)

vSphere - vc5a-01a.corp
VMware Cloud Director - X

Secure | https://vcd-01b.corp.local/provider/cloud/organizations

HOL Admin Region A Region B

vm VMware Cloud Director
Resources
Libraries
Administration
Monitor
More

Cloud Resources vSphere Resources

Organizations
Organization VDCs
Organization VDC Templates
Provider VDCs
Cloud Cells

Organizations

NEW MIGRATE TENANT STORAGE

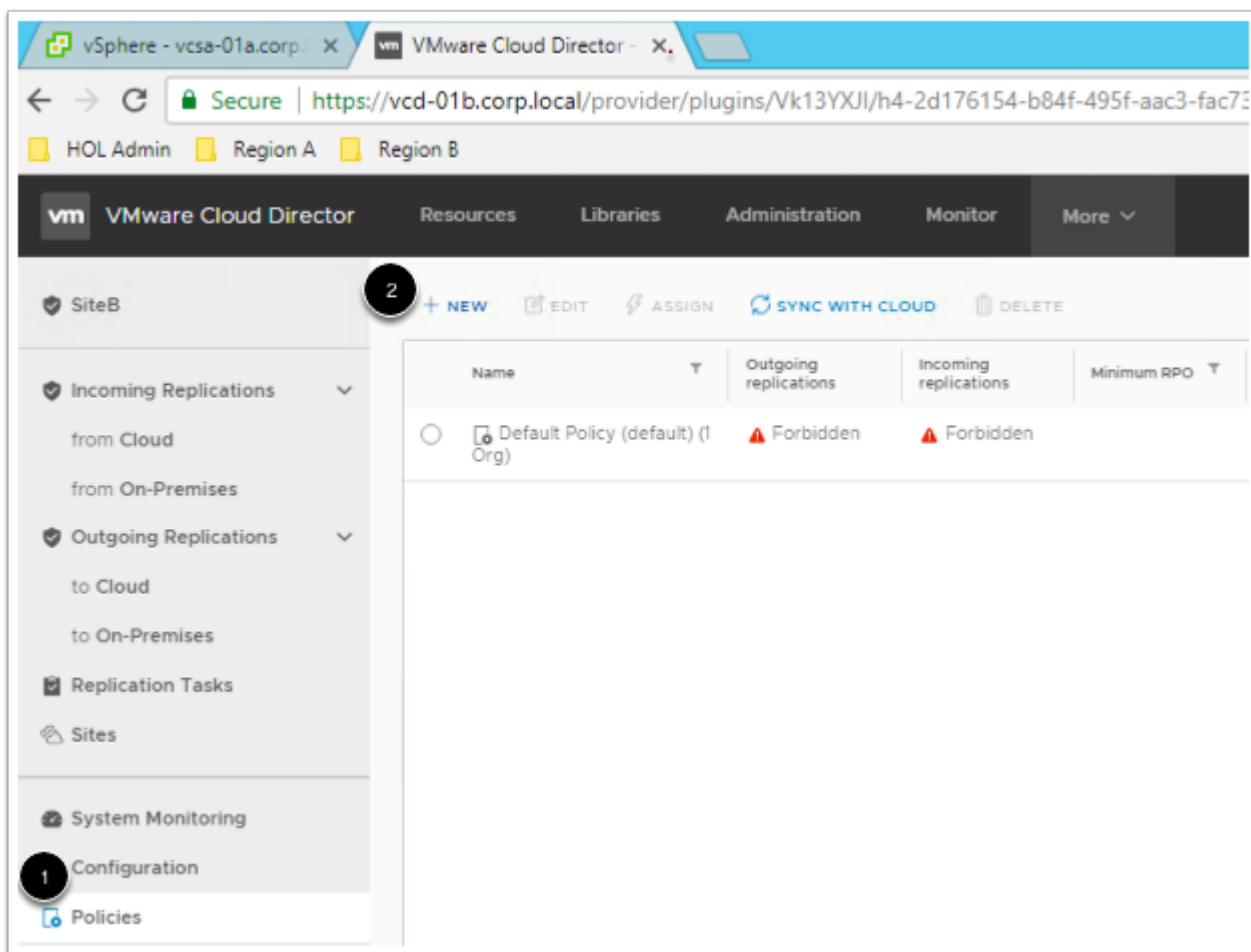
Name	State	Organization VDCs	Can Publish	Catalogs
☐ Tenant1	Enabled	1	No	1
☐ Tenant1	Enabled	1	No	1

1

Availability (SiteB)
Customize Portal

1. Click on **More - Availability (SiteB)**

Adding New Replication Policy



Replication policies are sets of rules that define and control the replication attributes on a VMware Cloud Director organization level. To control the replication settings allowed for replications on a VMware Cloud Director organization level, the service providers can create replication policies.

When configuring a protection or a migration, the New Replication wizard validates the replication attributes of the policy that is assigned to the organization. Lets add a new policy that will be validated while configuring replication.

1. Click on **Policies**
2. Click on **NEW**

Create New Replication Policy

New Policy

Policy name: * T1-Policy

☒ Allow custom SLA settings

☒ Allow outgoing replications

☒ Allow incoming replications

Maximum number of vm replications: * ☐ Unlimited ☒ 10

Max point-in-time instances per replication: ⓘ * 24

Max stored instances per replication: ⓘ * 24

☐ Enable bandwidth throttling

Max throughput per On-Premises Replicator Appliance: * 512
(1 - 10000 mbit/s)

Minimum allowed RPO:

5 min | 30 min | 2 hours | 8 hours | 24 hours

5m

Just brief overview for each parameter in this wizard-

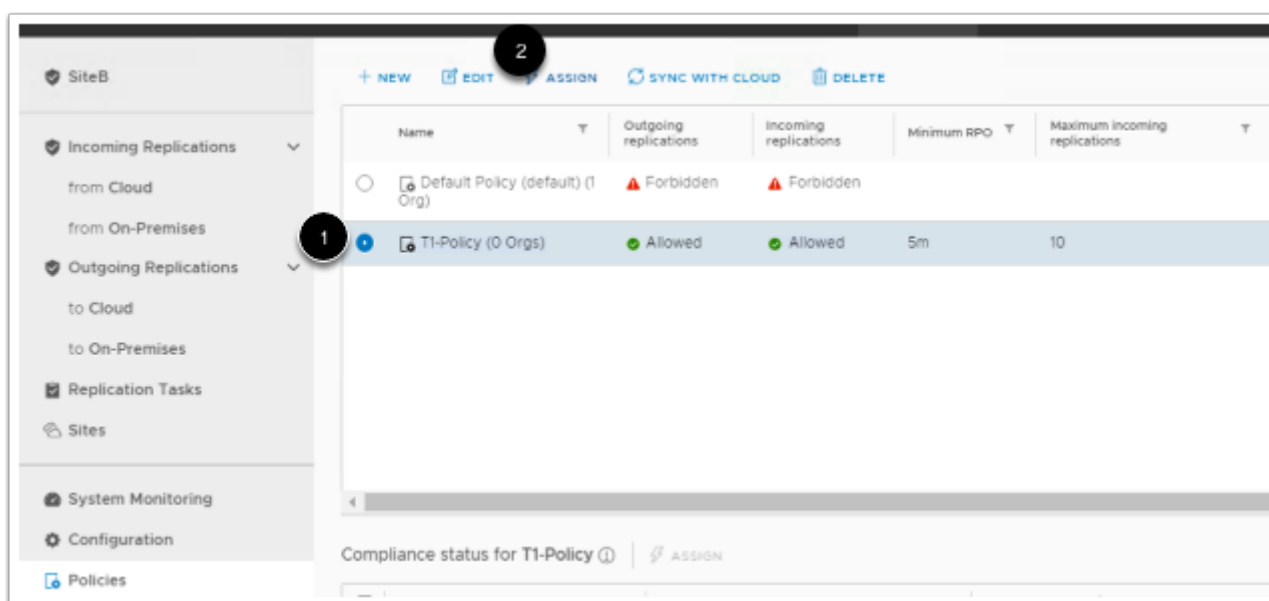
- Enter a unique, case-sensitive name for the replication policy.
- Select whether to allow custom SLA settings per replication or only to allow SLA profiles to set the SLA settings.
- Select whether to allow incoming and outgoing replications.
- If incoming replications are enabled, enter the maximum number of virtual machines replications.
- If incoming replications are enabled, enter the maximum number of point-in-time instances per replication.
- If incoming replications are enabled, enter the maximum number of stored instances per replication.

-Select whether to allow bandwidth throttling and if enabled enter the maximum throughput per VMware Cloud Director Availability On-Premises Appliance.

-If incoming replications are enabled, set the minimum allowed RPO by using the Recovery Point Objective (RPO) slider or by clicking the time ranges.

1. Policy Name: **T1-Policy**.
2. Leave everything as Default
3. Click on **CREATE**

Assign the Policy to Tenant



To control the replication settings of VMware Cloud Director organizations, the service providers assign replication policies to the organizations.

1. Select the Policy **T1-Policy**
2. Click on **ASSIGN**

Assign Policy to Tenant (contd..)

Assign Policy | T1-Policy

1. Check all organizations to be included to the policy.

Organization	Policy
☒ Tenant1	Default Policy

☒ 1 CLEAR SELECTED

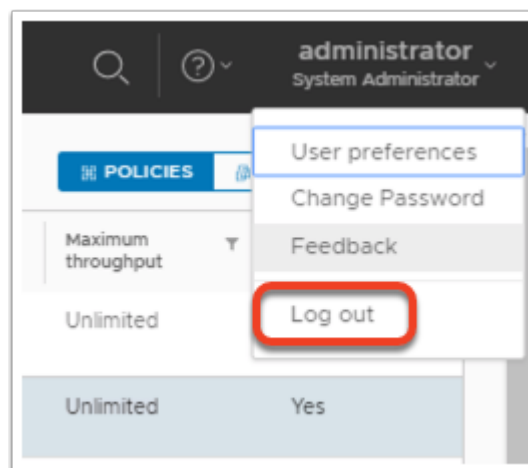
Items per page: 20 1 - 1 of 1 results

CANCEL ASSIGN

1. Enable checkbox for **Tenant1**
2. Click on **ASSIGN**

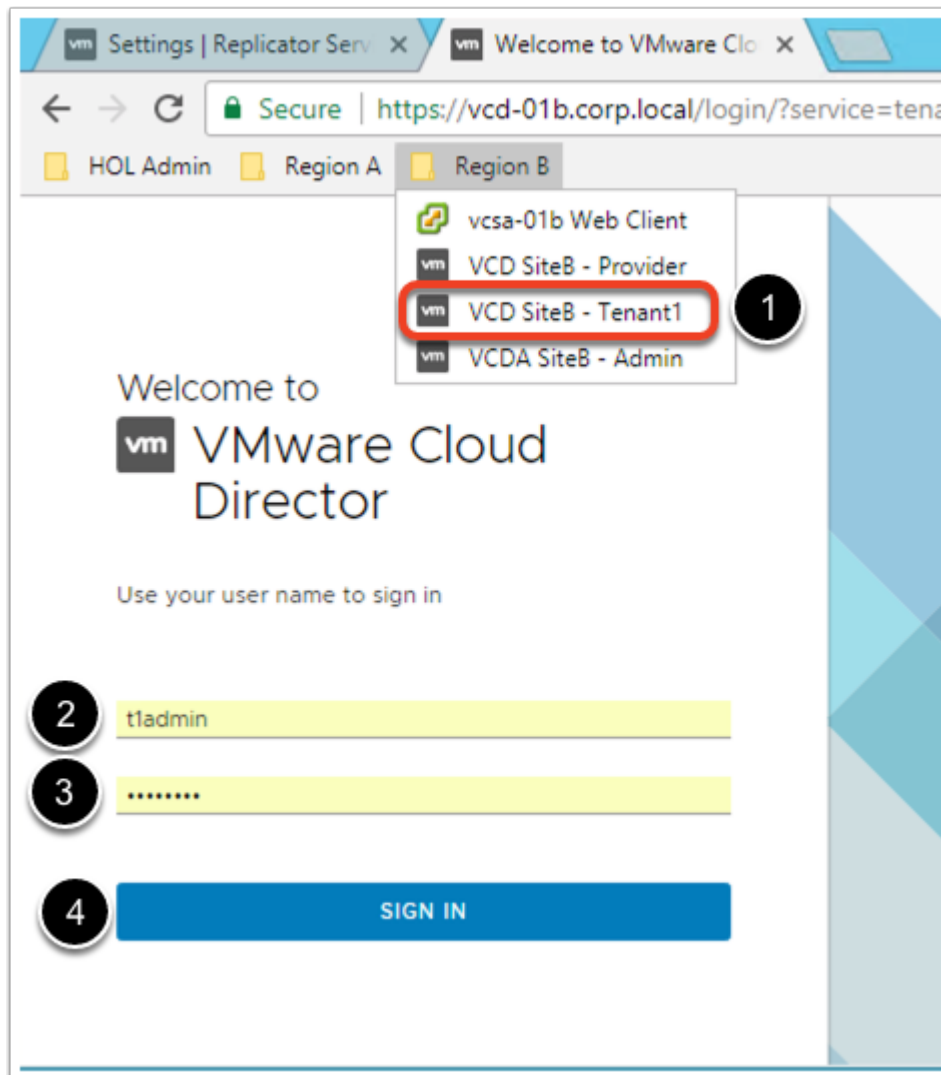
Let's log in as Tenant1 and see what it looks like now that we have assigned a policy.

Log out of Provider



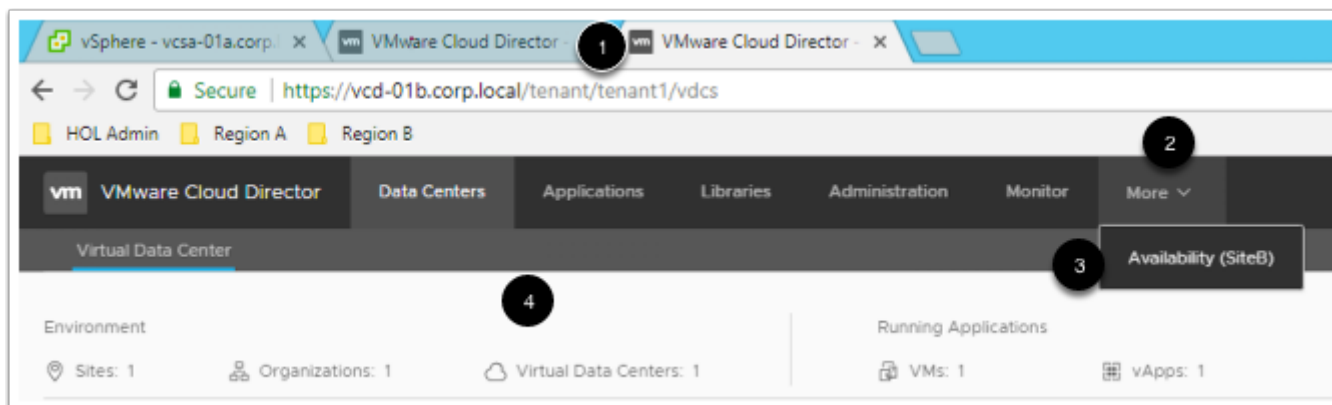
In the upper right-hand corner, click on **administrator** and select **Log out**.

Login to RegionB Tenant



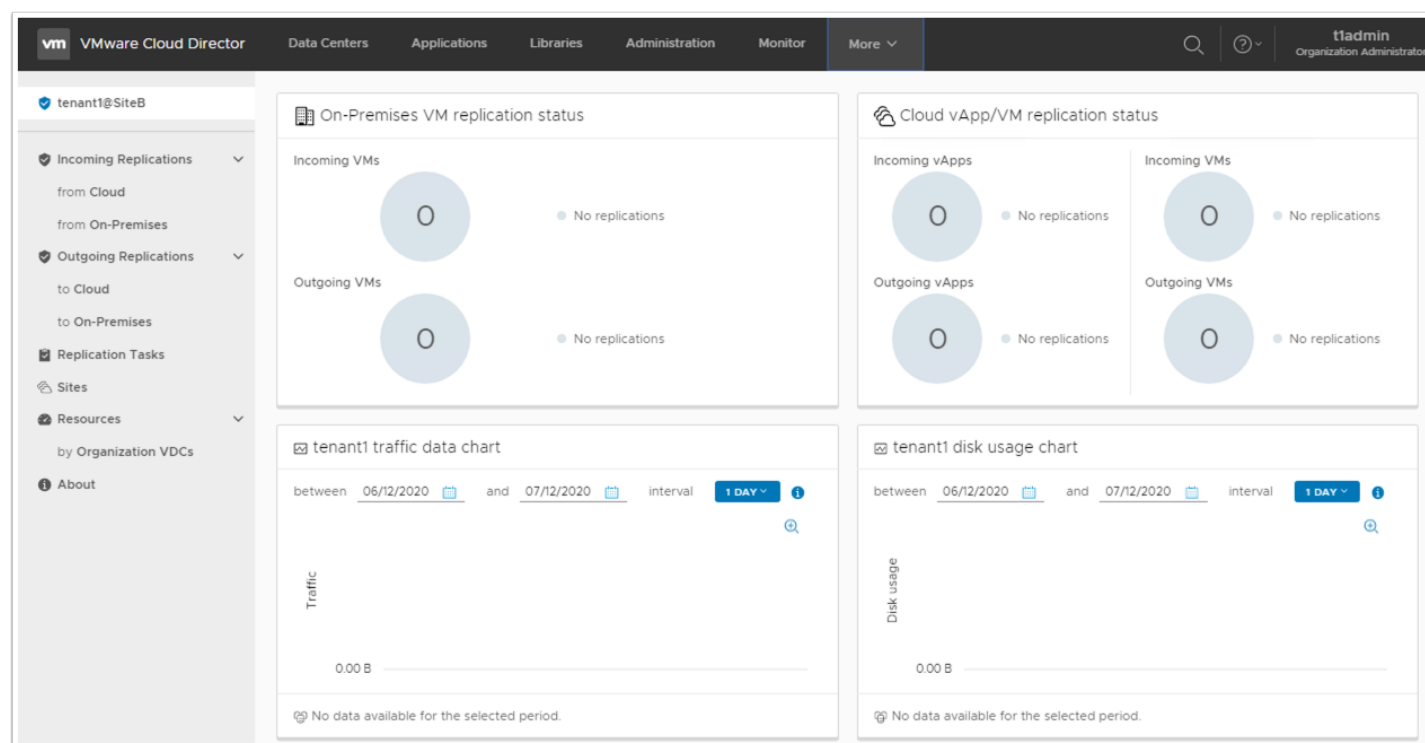
1. In the bookmarks bar, click on **Region B** and select **VCD SiteB - Tenant1**
2. Username: **t1admin**
3. Enter Password: **VMware1!**
4. Click on **Sign In**

Go to Availability



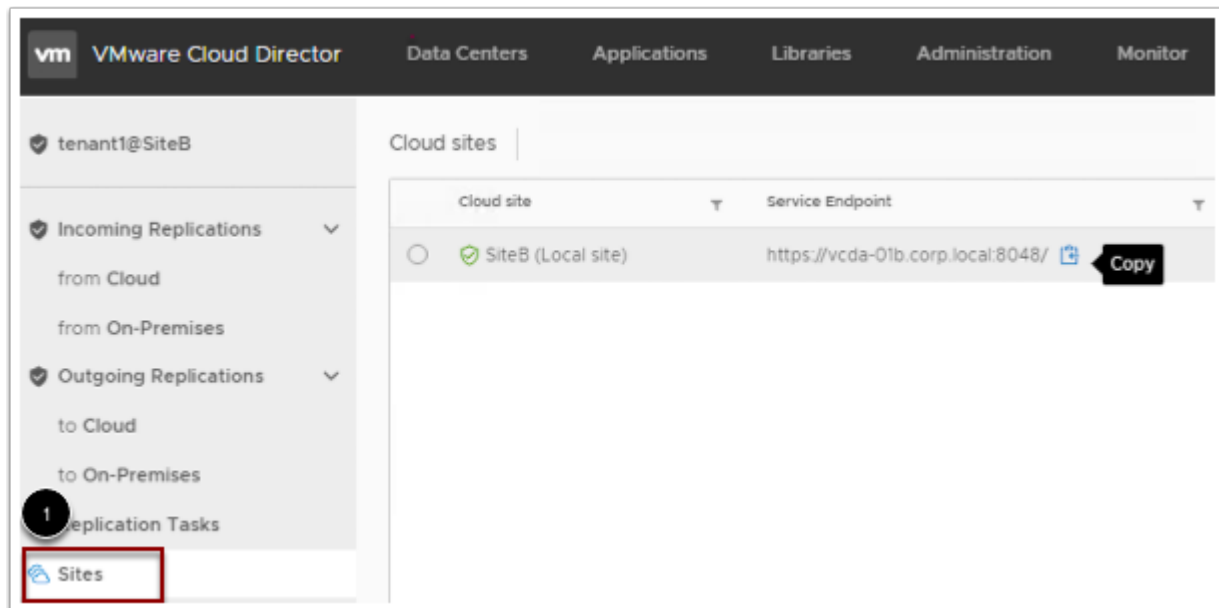
1. Expand **More**
2. Notice it no longer shows **Setup DR and Migration**. Click on **Availability (SiteB)**

Availability



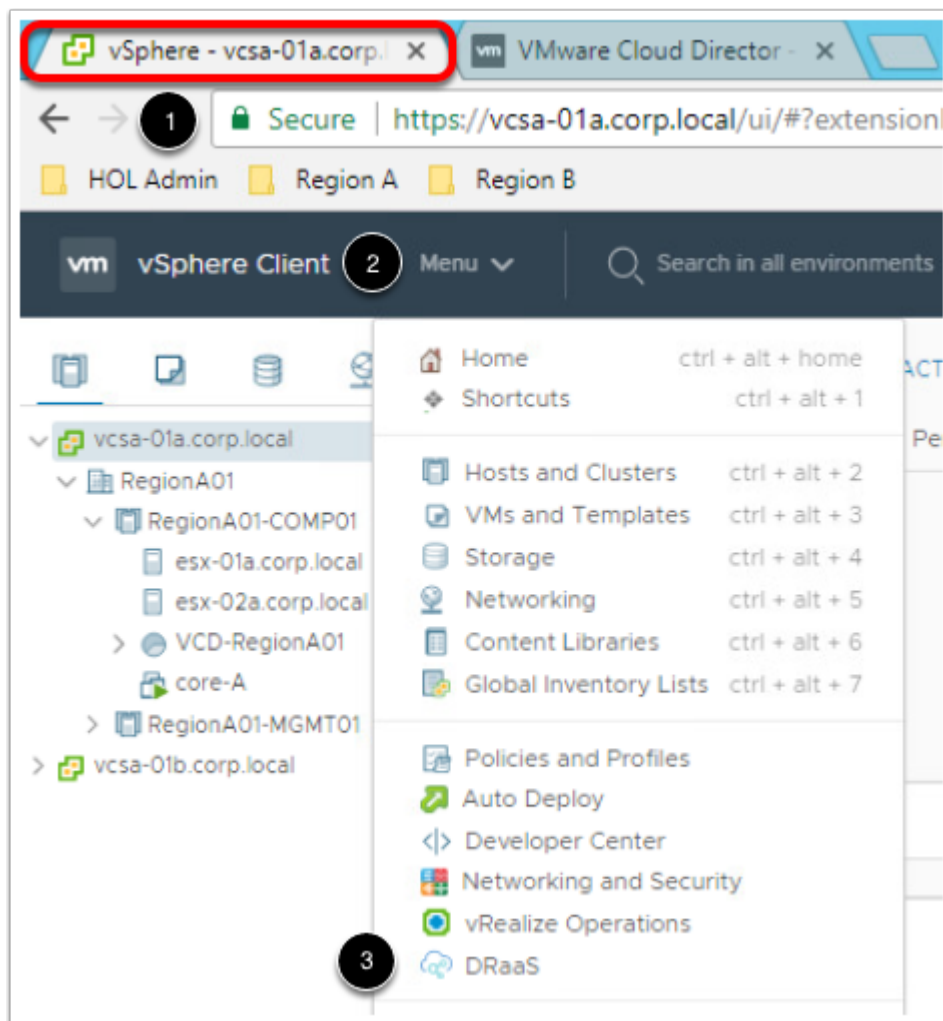
Notice that we no longer have the "Setup DR and Migration" window and now we have VMware Cloud Availability in our Cloud Director UI.

Retrieve Service Endpoint Address



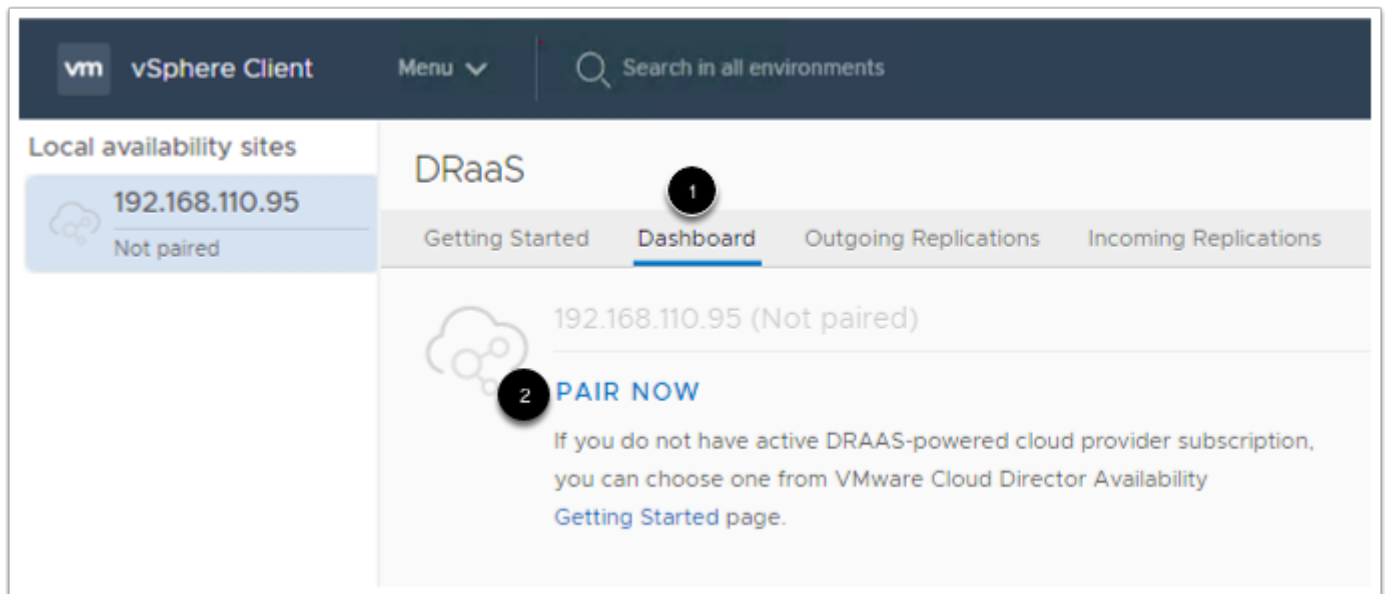
1. Click on **Sites**
2. Copy the **Service Endpoint URL** using the icon **Copy**

Switch to On-Prem Site



1. Switch to tab **On-Premises site**
2. Expand **Menu**
3. Click on **DRaaS**

Configure pairing from On-Premises to Cloud



1. Click on **Dashboard**
2. Click on **PAIR NOW**

Enter Site Details for pairing

The screenshot shows the 'New Pairing' wizard with '1 Site Details' selected in the left sidebar. The main form area is titled 'Site Details' and contains a description: 'Enter a name that will identify your vSphere site to the cloud provider.' There are two input fields: 'Site name' (with a red asterisk) containing 'vSphere-OnPrem' and a 'Description' text area with the placeholder 'Enter some meaningful information about the site.' Callout '1' points to the 'Site name' field. At the bottom right, there are 'CANCEL' and 'NEXT' buttons, with callout '2' pointing to the 'NEXT' button.

1. Enter Site name **vSphere-On-Prem**
2. Click **NEXT**

Enter Lookup Service Details

The screenshot shows a 'New Pairing' wizard with four steps: 1 Site Details, 2 Lookup Service (selected), 3 Cloud Service Details, and 4 Ready To Complete. The 'Lookup Service Details' step is active, showing a form to enter connection details. The form has three fields: 'Lookup Service Address' (pre-populated with 'https://vcsa-01a.corp.local:443/lookupservice/sdk'), 'SSO Admin Username' (pre-populated with 'administrator@regiona.local'), and 'Password' (masked with '*****'). A 'CANCEL' button and 'BACK' and 'NEXT' buttons are at the bottom right. Numbered callouts 1, 2, 3, and 4 point to the respective fields and the 'NEXT' button.

New Pairing

1 Site Details

2 Lookup Service

3 Cloud Service Details

4 Ready To Complete

Lookup Service Details

Enter the connection details for the Lookup service.

1 Lookup Service Address *

2 SSO Admin Username *

3 Password *

4

CANCEL BACK NEXT

1. Lookup Service Address: Confirm it is pre-populated
2. Enter SSO Admin Username: **administrator@regiona.local**
3. Enter Password: **VMware1!**
4. Click **Next**

Enter the Cloud Service Details

New Pairing

- 1 Site Details
- 2 Lookup Service
- 3 Cloud Service Details**
- 4 Ready To Complete

Cloud Service Details

Enter VMware Cloud Director Availability Cloud Site details.

- 1 Service Endpoint address *
- 2 Organization Admin *
- 3 Organization Password *
- 4 ☒ Allow Access from Cloud

Privileged VMware Cloud Director users are allowed to remotely browse the VMs on this site and configure them for replication.

CANCEL BACK **NEXT**

Here we will update the Cloud Service details. Enter the following information:

1. Service Endpoint address: Paste the url we copied from the Cloud Site. Confirm the address is <https://vcda-01b.corp.local:8048/>
2. Organization Admin: **t1admin@tenant1**
3. Organization Password: **VMware1!**
4. Allow Access from Cloud: **Turn it On.** For the enterprise administrators, this option under Cloud Details, gives the users an option to set up new replications from vCD. If this is disabled, vCD users cannot remotely browse vCenter. The only way to establish new replications is leveraging through vCenter. If this option is enabled, new replications can be established from either side.
5. Click **NEXT**

Accept the server certificate



1. Click on **ACCEPT**

Ready To Complete the pairing between the 2 sites

New Pairing

- 1 Site Details
- 2 Lookup Service
- 3 Cloud Service Details
- 4 Ready To Complete**

Ready To Complete

Site Name	vSphere-OnPrem
Site Description	
Lookup Service Address	https://vcasa-01a.corp.local:443/lookupservice/sdk
SSO Admin Username	administrator@regiona.local
Service Endpoint address	https://vcda-01b.corp.local:8048/
Organization Admin	t1admin@tenant1
Allow Access from Cloud	Yes

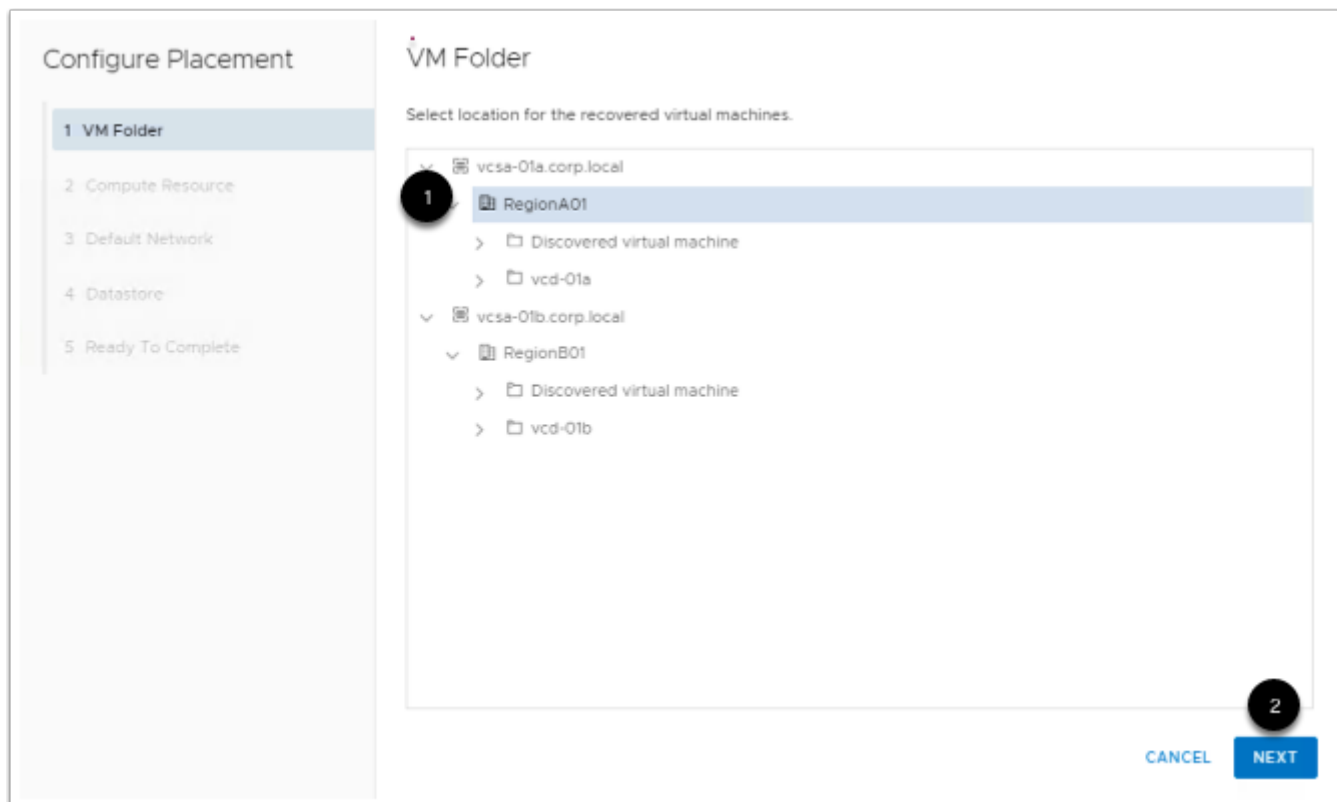
 After you finish the pair/repair setup, you will be able to configure **datacenter to cloud** replications. To enable **cloud to datacenter** replications, you must specify local placement settings.

1  Edit / configure local placement now

CANCEL BACK **2 FINISH**

1. Review the details, enable **Edit / configure local placement now**. To enable Cloud to on-premises replications, local placement settings need to be configured to indicate where to put your recovered VMs.
2. Click on **FINISH**

Configure Placement Settings for Recovered VMs



Because the "Edit / configure local placement now" option was enabled in the last step, the Configure Placement wizard should now be visible. (If you didn't enable this setting in the previous step, you can access this wizard in the DRaaS Configuration section. Look for "Placement to newly recovered VMs on this site".)

1. Select **RegionA01**
2. Click on **Next**

Configure Compute Resource

The screenshot shows the 'Configure Placement' wizard with the 'Compute Resource' step selected. The left sidebar lists the steps: 1 VM Folder, 2 Compute Resource, 3 Default Network, 4 Datastore, and 5 Ready To Complete. The main area is titled 'Compute Resource' and contains the instruction 'Select the destination compute resource for the recovered virtual machines.' Below this is a tree view showing the hierarchy: RegionA01 (expanded) -> RegionA01-COMP01 (selected) -> VCD-RegionA01. Other options under RegionA01 include RegionA01-MGMT01 (expanded) with sub-items esx-03a.corp.local, esx-04a.corp.local, and esx-05a.corp.local, and a Resources folder. At the bottom right, there are three buttons: CANCEL, BACK, and NEXT. A black circle with the number 1 points to the 'RegionA01-COMP01' selection, and a black circle with the number 2 points to the 'NEXT' button.

Configure Placement

- 1 VM Folder
- 2 Compute Resource
- 3 Default Network
- 4 Datastore
- 5 Ready To Complete

Compute Resource

Select the destination compute resource for the recovered virtual machines.

- RegionA01
 - RegionA01-COMP01
 - VCD-RegionA01
- RegionA01-MGMT01
 - esx-03a.corp.local
 - esx-04a.corp.local
 - esx-05a.corp.local
- Resources

CANCEL BACK NEXT

1. Select **RegionA01-COMP01**
2. Click **Next**

Configure Default Network

Configure Placement

- 1 VM Folder
- 2 Compute Resource
- 3 Default Network**
- 4 Datastore
- 5 Ready To Complete

Default Network

Select the network to connect VM network interfaces after failover.

Resources

- ESXi-RegionA01-vDS-COMP
- Storage-RegionA01-vDS-COMP
- Uplink-RegionA01-vDS-COMP
- VM-RegionA01-vDS-COMP**
- vMotion-RegionA01-vDS-COMP
- vxw-dvs-45-virtualwire-3-sid-5000-dvs.VCDVSDLR_to_EDGE_tenant1-esg-01a-be52c88e-
- vxw-dvs-45-virtualwire-4-sid-5001-dvs.VCDVSTenant1-OVDC-A-OrgNet-Rtd-4fa7fe8c-2c
- vxw-vmknipg-dvs-45-0-365370a1-79f9-4ee0-8aae-f8c2ca00a3ef

CANCEL BACK **NEXT**

1. Select Network **VM-RegionA01-vDS-COMP**
2. Click **Next**

Configure Datastore

The screenshot shows a 'Configure Placement' wizard with five steps: 1 VM Folder, 2 Compute Resource, 3 Default Network, 4 Datastore, and 5 Ready To Complete. Step 4, 'Datastore', is currently selected. The main area is titled 'Datastore' and contains the instruction 'Select the datastore in which to store the replicated VMs and disk files'. Below this is a list of resources with 'RegionA01-ISCSI01-COMP01' selected. A circular callout with the number '1' points to the resource list. At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'. A circular callout with the number '2' points to the 'NEXT' button.

Configure Placement

- 1 VM Folder
- 2 Compute Resource
- 3 Default Network
- 4 Datastore
- 5 Ready To Complete

Datastore

Select the datastore in which to store the replicated VMs and disk files

Resources

- RegionA01-ISCSI01-COMP01

CANCEL BACK NEXT

1. Select Datastore as **RegionA01-ISCSI01-COMP01**
2. Click **Next**

Ready to Complete the Configuration of VM Placement

Configure Placement

- 1 VM Folder
- 2 Compute Resource
- 3 Default Network
- 4 Datastore
- 5 Ready To Complete

Ready To Complete

Verify the selected configuration is correct.

VC

VM Folder

Compute Resource

Default Network

Datastore

vcsa-01a.corp.local

RegionA01

RegionA01-COMP01

VM-RegionA01-vDS-COMP

RegionA01-ISCSI01-COMP01

1

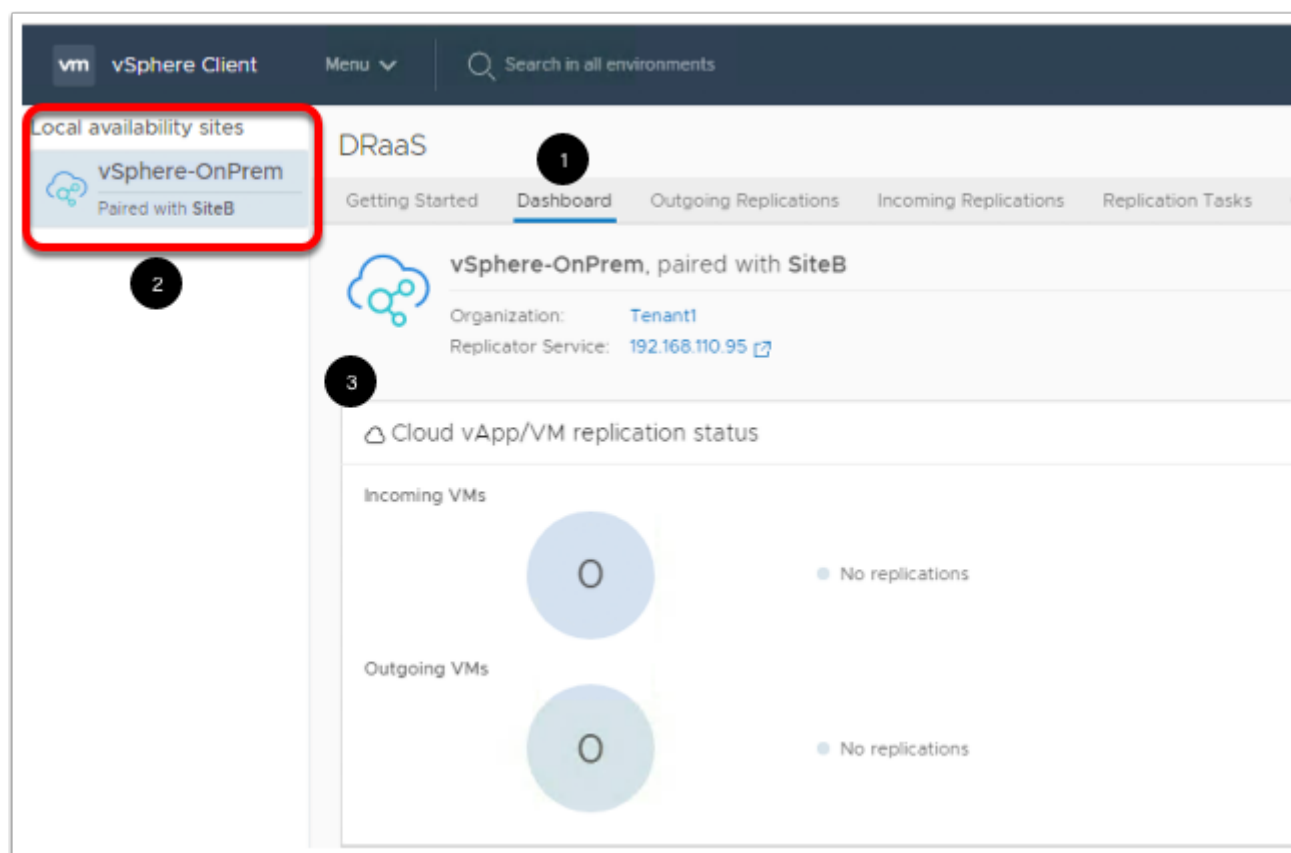
CANCEL

BACK

FINISH

1. Review the details and Click on **FINISH**

Confirm the pairing is Completed successfully



Let's take a look at the Dashboard at On-Premises site.

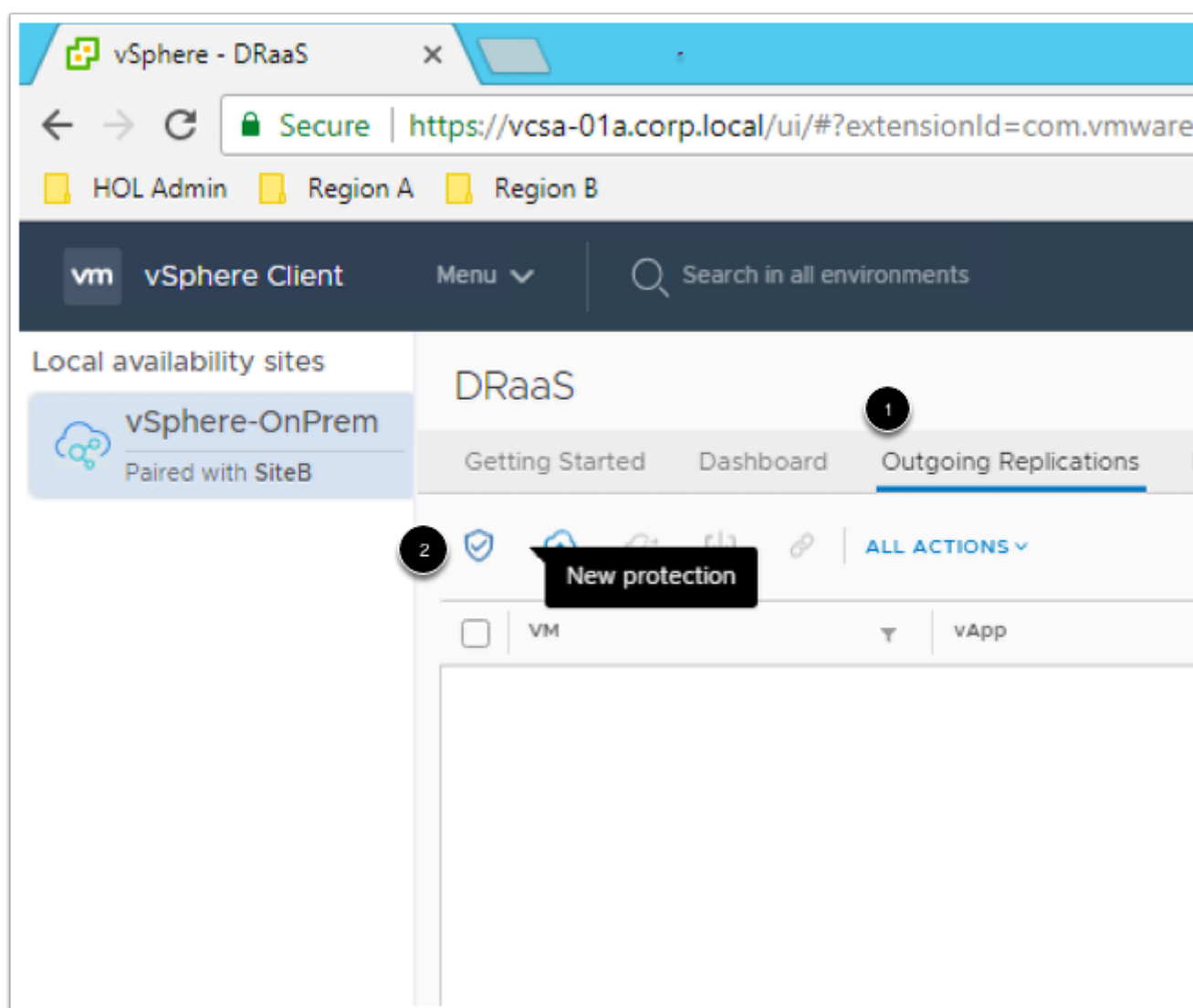
1. Click on **Dashboard**
2. **Local Availability Sites** - Confirm the On-Premises site is paired with Cloud SiteB
3. **Cloud vApp/VM replication status** - We just paired On-Premises with Cloud. There are no Incoming or Outgoing Replications to Cloud.

Failover Workflows from On-Premise to Cloud Using vCloud Availability

In this exercise, we will be learn

- How to protect VMs from On-Prem to Cloud.
- How to Test recover, Test Cleanup, Recover and Reverse Replicate the VMs from on-premises to cloud and back.

Configure Replication from On-Prem to Cloud



You should still be logged in to vSphere Region A and in the DRaaS section. If not, open a browser window, log in to vSphere as administrator@regiona.local, and go to the DRaaS section under the Menu.

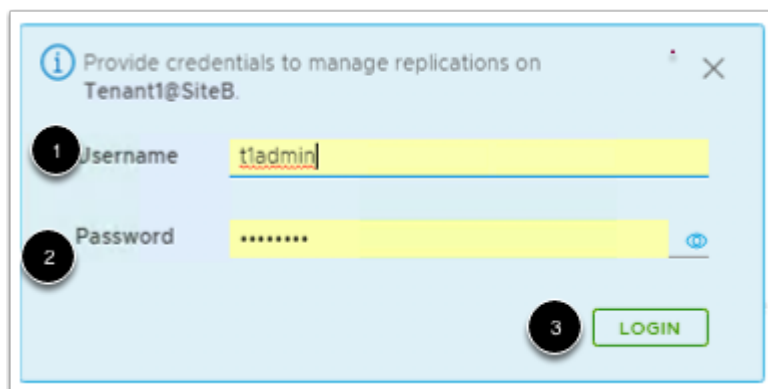
Now we will configure an Outgoing Replication. There are two replication options:

- **Protection** - Protecting a virtual machine from on-prem to a VCD target; keeps the workload running in the source site.
- **Migration** - Migrating a virtual machine from on-prem to a VCD target; powers off the source and runs the workload in the destination site.

In this lab exercise, we will configure Protection of VM from On-Premises to Cloud.

1. Click on **Outgoing Replications**
2. Click on the icon **New protection**

Enter Credentials to manage replications to Cloud



1. Username: **tladmin**
2. Enter Password: **VMware1!**
3. Click on **LOGIN**

Select vCenter VM for Replication

New Outgoing Replication

1 vCenter VMs

2 Destination VDC and Storage policy

3 Settings

4 Ready To Complete

vCenter VMs

Source Site VSPHERE-ONPREM

Select VMs to replicate from: VCSA-01A.CORP.LOCAL

☐ Group VMs to a single vApp

☐	VM	CPU	Memory	Disk capacity
☐	Controller-1A-NSX-controller-1	4	4.00 GB	28.00 GB
☒	core-A	1	256.00 MB	100.00 MB
☐	photon-base-IRvg	1	256.00 MB	512.00 MB
☐	tenant1-photon-01a-MSat	1	256.00 MB	512.00 MB
☐	vcda-01a	4	6.00 GB	10.00 GB
☐	vcda-02a	2	4.00 GB	10.00 GB
☐	vse-tenant1-esg-01a (f7b86112-334c-4758-bcf3-0aa727f2411c)-0	1	512.00 MB	1.07 GB

☒ 1 CLEAR SELECTED

Items per page 20 1 - 7 of 7 results

CANCEL NEXT

- 1. Select VM **core-A**
- 2. Click on **Next**

Select Destination VDC and Storage Policy for Replication

New Outgoing Replication

1 vCenter VMs

2 Destination VDC and Storage policy

3 Settings

4 Ready To Complete

Destination VDC and Storage policy

Select a virtual data center from SiteB to be used as replication target:

REFRESH

Name	Used CPU	Used memory	Used storage	VMs	Quota	Ongoing replications
Tenant1...	0 M	256.00 MB	1.25 GB	1	Currently unavailable	0

Items per page 20 1 - 1 of 1 results

Storage policy

Select the new storage policy placement for the recovered VMs

Name	Used	Limit
Any	1.25 GB	10.00 GB

Items per page 20 1 - 1 of 1 results

CANCEL

BACK

NEXT

1. Select vDC **Tenant1**
2. Select Storage policy **Any**
3. Click on **Next**

HOL-2182-01-HBD

Page 68

Configure Settings

Brief overview of the parameters on this page -

SLA Profile - The premise of a SLA Profile is to provide a grouping of target settings when protecting a workload. This minimizes the amount of time spent configuring for protection. Think of this as a logical grouping construct which is a single selection to protect a workload. One does not need to think about what settings to configure. A SLA Profile consists of the following:

1. Target Recovery Point Objective (target being the key word here)
2. Retention Policy for Point in Time Instances
3. Ability to Quiesce or Compress Replication Traffic
4. Time select of the synchronization.

Just select SLA profile, and done. You can either use default or custom created SLA profile. SLA profiles are optional and only pertain to protections. They are not utilized for migrations at this time.

Target recovery point objective (RPO) - The RPO is the longest tolerable timeframe of data loss. For example, with one hour RPO the recovered virtual machine can have no more than one hour of data lost. Shorter RPO intervals, ensure less data loss during recovery, at the expense of consuming more network bandwidth to keep the replica up to date.

Retention Policy - Maximum number of retained snapshots per single virtual machine replication within an organization.

Delay start synchronization

- To schedule the start of the replication, select this option and enter the local date and time to start the replication.
- To start the replication when the wizard finishes, leave this option deselected.

Exclude disks -To exclude some hard disks of the virtual machines from replicating to the destination site, select this option.

Configure Seed VMs - For each new replication that you configure, an initial full synchronization operation is performed. During this operation, vCloud Availability copies the whole data from the source vApp or VM to a datastore in the target site. Due to the size of the vApp or VM or to the network bandwidth, an initial full synchronization might take a long time.

To reduce the initial synchronization time, you copy the source vApp or VM to the target site by using removable media, failover of a previous replication, or other means of data transfer. Then, in the target site, configure a replication that uses the vApp or VM copy as a replication seed.

When a replication uses a seed vApp or VM, vCloud Availability does not copy the whole source vApp or VM data to the target site. Instead, vCloud Availability copies only the different data blocks between the source vApp or VM and the seed and reuses the seed data in the target site as a basis for replication.

We do not have Seed VM available at the target site for this exercise

1. Leave everything as Default and Click **Next**

Complete Replication to Cloud

New Outgoing Replication

- 1 vCenter VMs
- 2 Destination VDC and Storage policy
- 3 Settings
- 4 Ready To Complete

Ready To Complete

Verify the selected settings before proceeding:

VMs	core-A
Source Site	vSphere-OnPrem
Destination Site	SiteB
Destination VDC	Tenant1-OVDC-B
Storage policy	Any
Target RPO	24h
Quiescing	Disabled
Retention	Keep latest instance only
Sync time	No delay

CANCEL

BACK

1

FINISH

1. Verify the Replication Settings are correct and click **Finish**

Confirm the Replication is started

vSphere - DRaaS

Secure

https://vcsa-01a.corp.local/ui/#?extensionId=com.vmware.h4.portalView

HOL Admin

Region A

Region B

vm vSphere Client

Menu

Search in all environments

Administrator@REGIONALLOCAL

Local availability sites

vSphere-OnPrem

Paired with SiteB

DRaaS

Getting Started Dashboard Outgoing Replications Incoming Replications Replication Tasks Configuration System Monitoring System Tasks Support About

ALL ACTIONS

STATUS TOPOLOGY INSTANCES RESOURCES

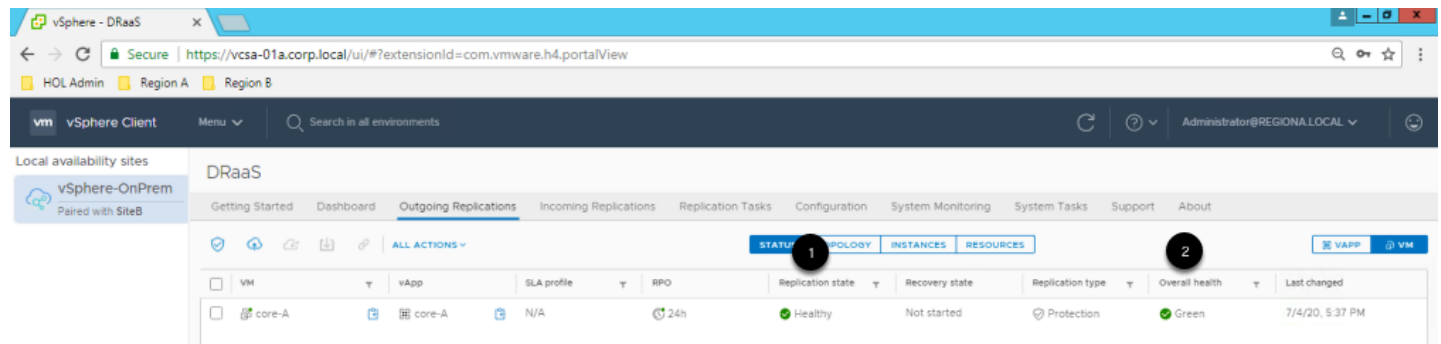
VAPP VM

VM	vApp	SLA profile	RPO	Replication state	Recovery state	Replication type	Overall health	Last changed
core-A	core-A	N/A		Unknown	Unknown	Protection	Red	Configure 2%

1. Confirm that the replication is started. You can monitor the % progress here.

Note: the time it takes to replicate a VM depends on the size of the VM. In this case, the VM is relatively small, so it should only take a minute or two.

Replication is Completed

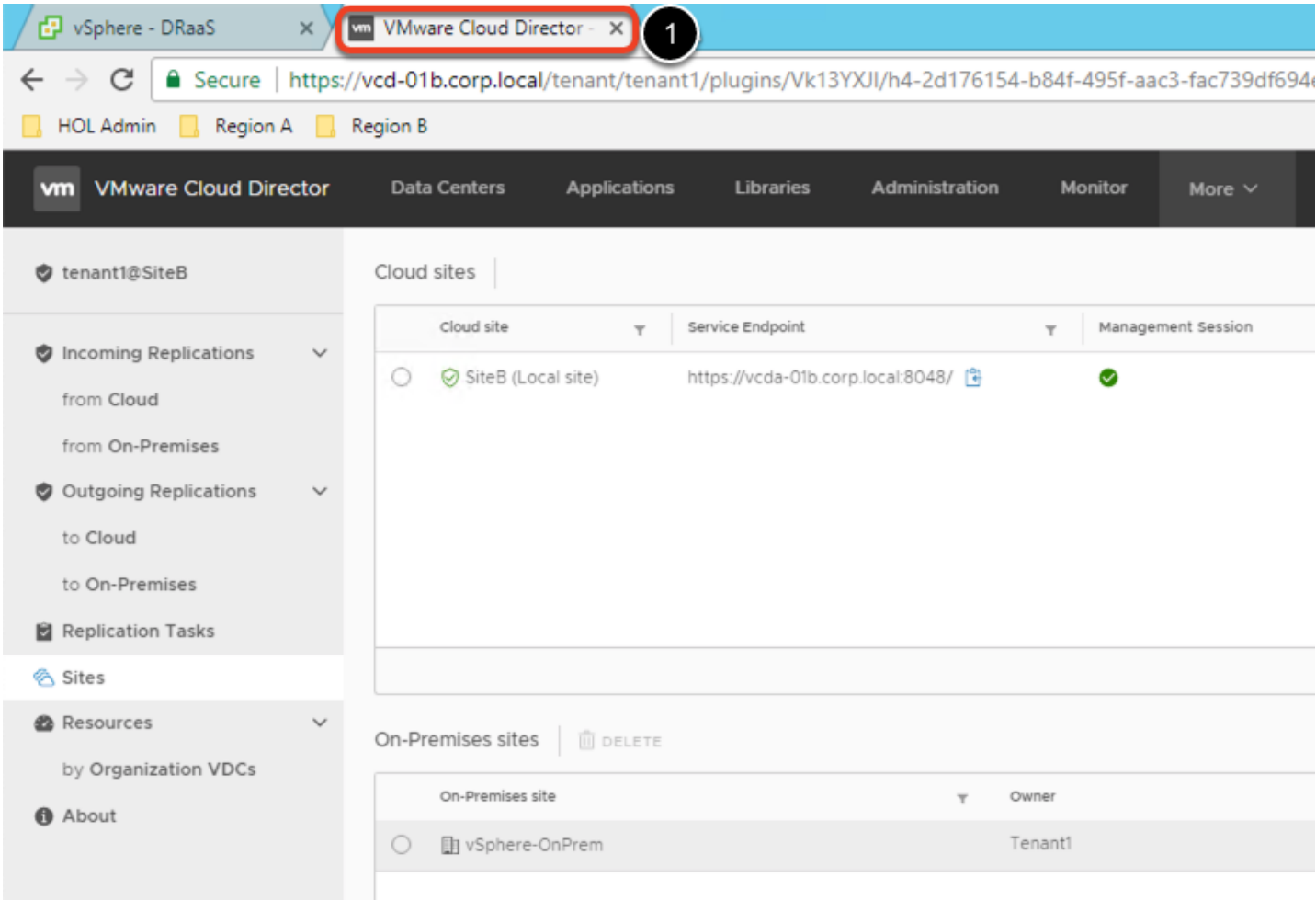


Confirm the replication status of VM core-A

1. Replication State is **Healthy**
2. Overall health is **Green**

Note: In case you see Unexpected vCloud Director error during replication, please retry. Due to the nested environment in Hands On Lab, sometimes the error is seen, in real world it should work seamlessly.

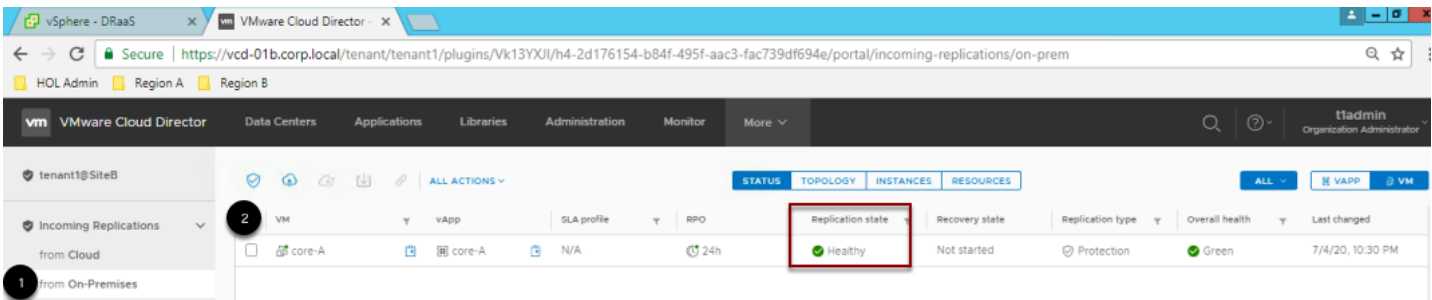
Confirm the Replication Status from Cloud Provider Site



You should still have a second tab open logged in to the Cloud SiteB as t1admin. If not, open a new tab, go to VCD-SiteB - Tenant1 from the Region B folder in the bookmarks bar, log in as t1admin, and click on the More menu and select Availability (SiteB).

1. Click on the second browser tab to go back to the Tenant1 OVDC in VCD SiteB.

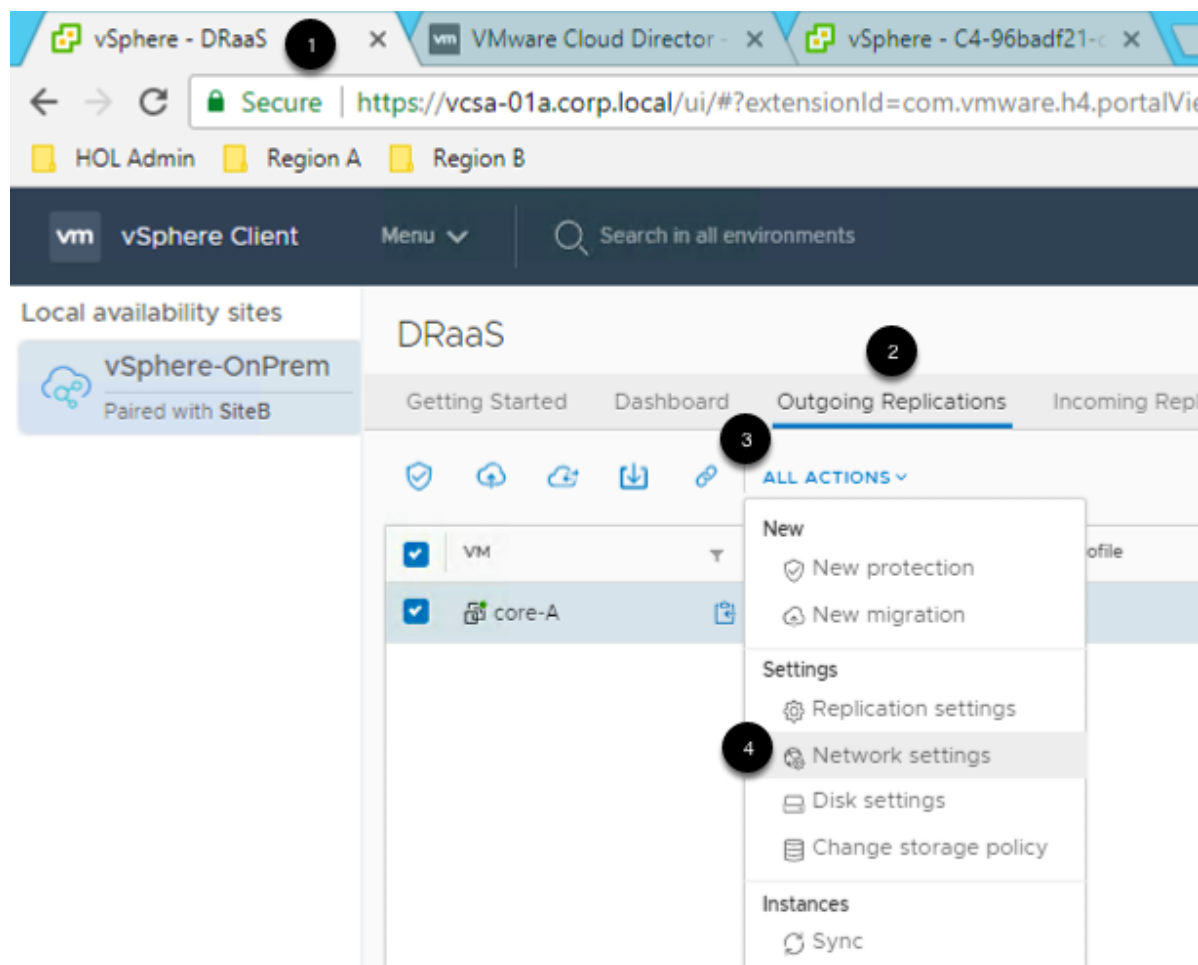
Confirm the Replication Status at Cloud Site



1. Click on **Incoming Replication - from On-Premises**

2. Confirm the VM core-A replication state is **Healthy**

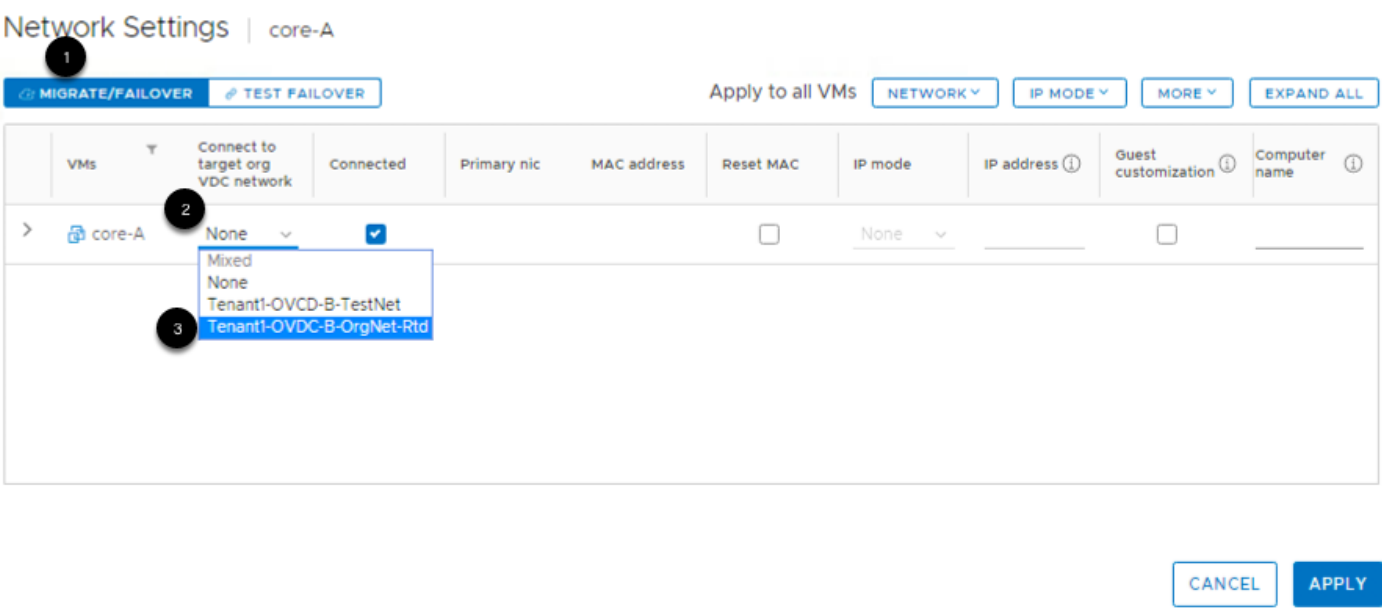
Configure Network for Recovery Workflows



Before we can run Recovery of the replicated VM, we need to configure a Test/Failover Network. This step can be either done from On-Premises or the Cloud. This Network would be connected to the Recovered VM.

1. Switch to **On-Premises tab**
2. From the **Outgoing Replications**, check the checkbox for **core-A**
3. Expand **ALL ACTIONS**
4. Click on **Network Settings**

Configure Network for Recovery Workflows

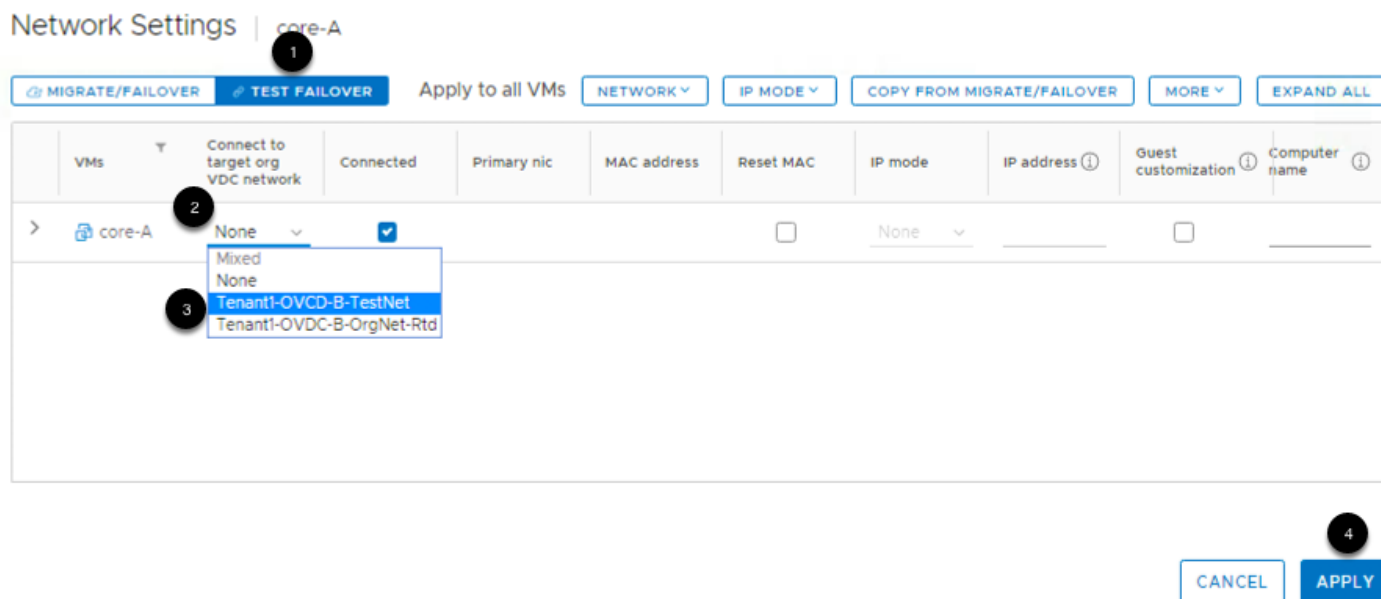


Before we can run Recovery of the replicated VM, we need to configure a Test/Failover Network. This step can be either done from On-Premises or the Cloud. This Network would be connected to the Recovered VM.

For HOL lab exercise, Migrate and Test Failover networks are pre-configured. In production environment, please create migrate/test failover networks before configuring it here.

1. Select **MIGRATE/FAILOVER**
2. Expand **None**
3. Select **Tenant1-OVDC-B-OrgNet-Rtd**

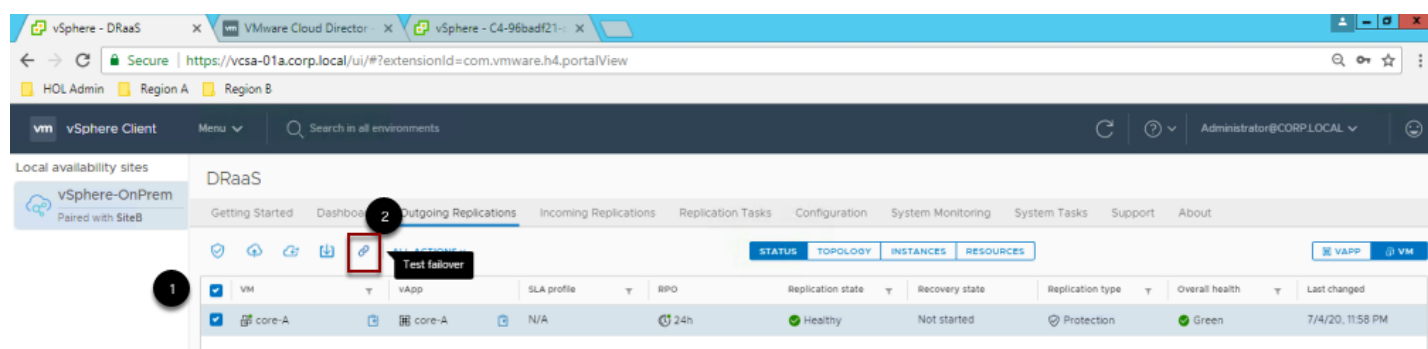
Configure Network for Recovery Workflows (contd..)



1. Select **TEST FAILOVER**
2. Expand **None**
3. Select **Tenant1-OVDC-B-TestNet**
4. Click **APPLY**

We have successfully configured network for both Migrate/Failover and Test Failover workflows.

Configure Test Failover



By performing a test failover you can validate that the data from the source site replicates correctly in the destination site. Test Failover can be configured from either the On-Premises or Cloud site. For HOL exercise, we will configure Test Failover from On-Premises.

1. Check the checkbox for VM **core-A**
2. Click on the icon **Test Failover**

Configure Recovery Settings for Test Failover

Test Failover

1 Recovery Settings
2 Recovery Instance
3 Ready To Complete

Recovery Settings

Select configuration for the recovered VMs

1 ☒ Power on recovered VMs

Network Settings

2 ☒ Apply preconfigured network settings on failover
☐ Connect all VMs to network ▼

3

CANCEL NEXT

For the recovered VMs, here are Recovery Settings:

- **Power on recovered vApps** - Select to power on the virtual machines in the destination site after the task completes.
- **Network settings**
 - Select Apply preconfigured network settings on failover, to assign the network configured during the virtual machine replication.
 - Select Connect all VMs to network and from the drop-down menu select a network to connect the replicated virtual machines to.

1. Check the checkbox **Power on recovered VMs**
2. Network Settings: Select **Apply preconfigured network settings on failover** . We preconfigured network settings in the previous steps.
3. Click **NEXT**

Configure Recovery Instance for Test Recovery Workflow

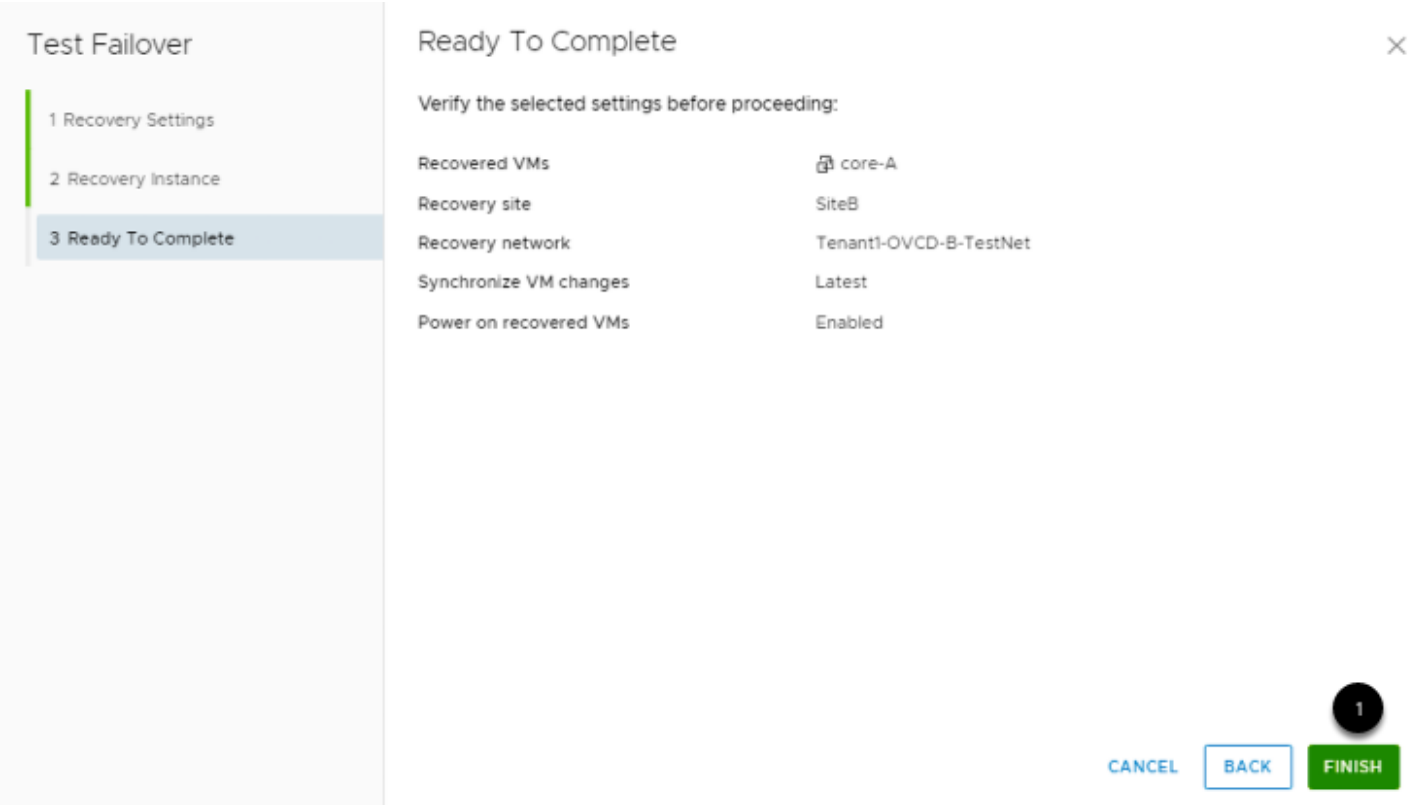
Select recovery point in time -

- **Synchronize all VMs to their current state** - Creates an instance of the powered on vApp with its latest changes and uses that instance for the Test Failover operation.

- **Manually select existing instance** - Select an instance without synchronizing the data for the recovered workload.

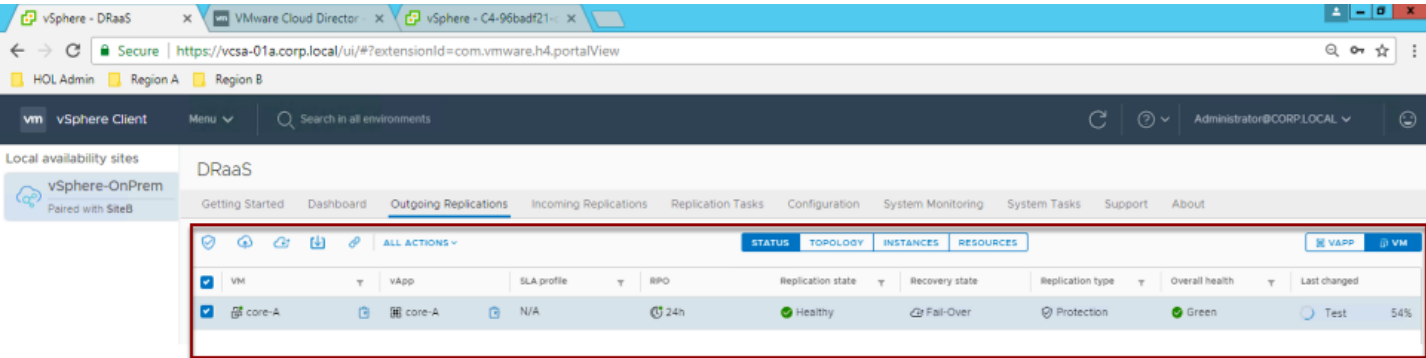
1. For the Recovery point in time select **Synchronize all VMs to their current state**
2. Click on **Next**

Ready To Complete the Test Failover



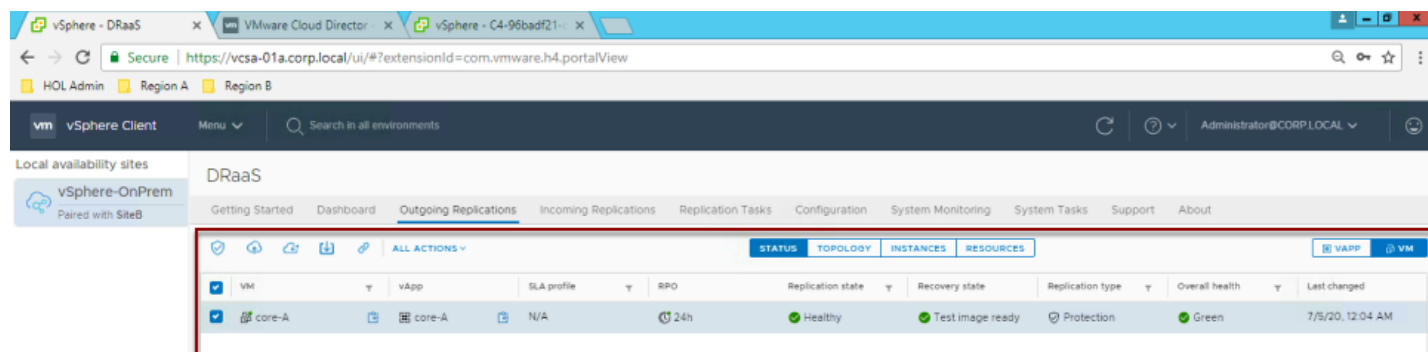
- 1. On the Ready To Complete page, review the test details and click **FINISH** to initiate the Test Failover

Test Failover is in progress



Verify the Test Failover is started and Recovery state is updated to **Fail-Over**. You can monitor the % progress for test failover.

Test Failover is Completed and Successful



Confirm the Recovery State is **Test Image Ready** and Overall Health is **Green**.

Please be patient, it may take few minutes for the Test Failover to be Complete.

Note: In case you see Unexpected vCloud Director error during test failover, please retry. Due to the nested environment in Hands On Lab, sometimes the error is seen, in real world it should work seamlessly.

View Failover VM at Cloud Site

The screenshot shows the VMware Cloud Director web interface. The browser tabs at the top include 'vSphere - DRaaS', 'VMware Cloud Director', and 'vSphere - C4-96badf21-c'. The address bar shows a secure connection to 'https://vcd-01b.corp.local/tenant/tenant1/vdcs'. The navigation bar includes 'HOL Admin', 'Region A', 'Region B', and a main menu with 'VMware Cloud Director', 'Data Centers', 'Applications', 'Libraries', 'Administration', 'Monitor', and 'More'. The 'Data Centers' tab is selected, and the 'Virtual Data Center' sub-tab is active. Below the navigation bar, the 'Environment' section displays 'Sites: 1', 'Organizations: 1', and 'Virtual Data Centers: 1'. The 'Running Applications' section shows 'VMs: 2' and 'vApps: 1'. The main content area displays details for 'Tenant1-OVDC-B', including 'Tenant1' and IP address '192.168.210.40'. A table shows resource usage for CPU, Memory, and Storage. The CPU usage is 0 MHz (1 GHz allocated), Memory usage is 256 MB (1 GB allocated), and Storage usage is 2 GB (10 GB allocated). The 'Applications' section shows '2 vApps' and '2 of 2 Running VMs'.

Resource	Usage	Allocated
CPU	0 MHz	1 GHz
Memory	256 MB	1 GB
Storage	2 GB	10 GB

1. Switch to tab **VMware Cloud Director Availability as a tenant**
2. Click on **Data Centers**
3. Click on Virtual Datacenters **Tenant1-OVDC-B**

Verify Test Recovery on Cloud Site

The screenshot shows the VMware Cloud Director web interface. The left sidebar contains navigation menus for Compute, Networking, Storage, and Settings. The main content area displays a list of Virtual Machines under the heading 'Virtual Machines'. Two VMs are listed: 'core-A' and 'tenant1-photon-01b'. A red box highlights the 'core-A' VM details, and a callout box shows its network details.

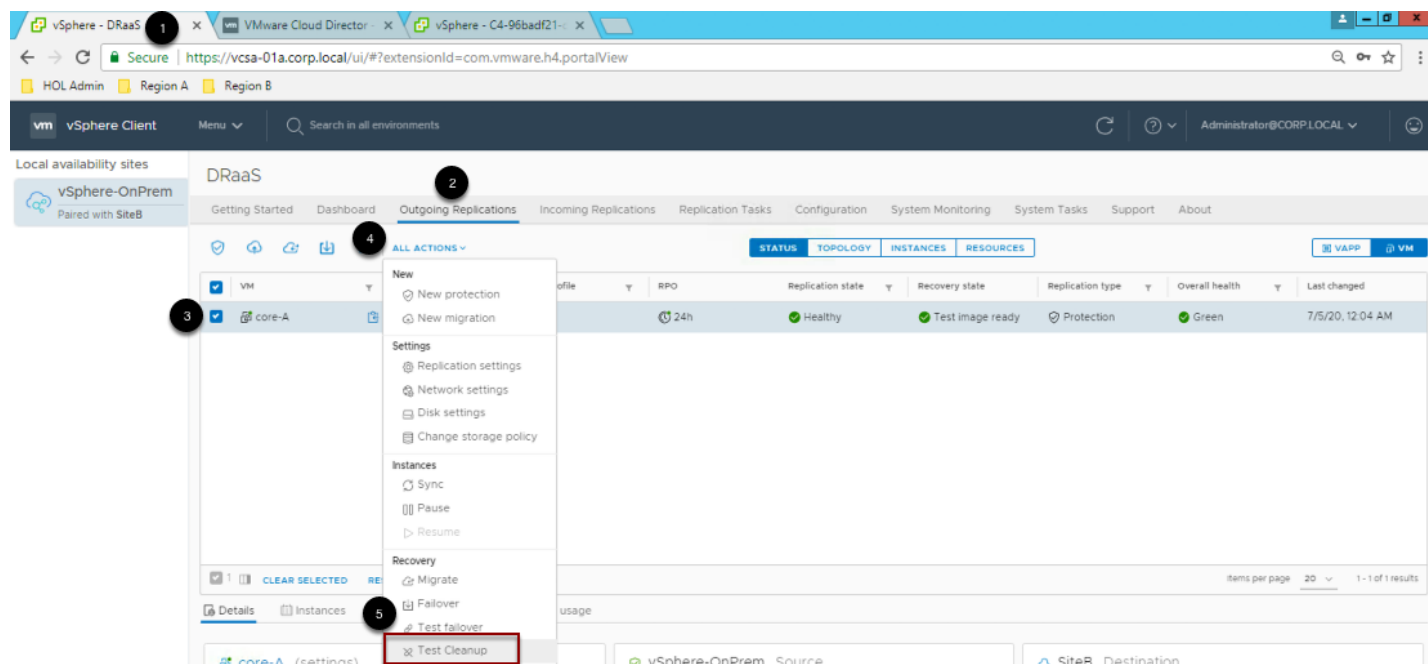
VM Name	Status	Lease	Created On	Owner	vApp	OS	CPU	Storage	Memory	Network
core-A	Powered on	Never Expires	07/04/2020, 10:43:22 PM	ttadmin	core-A	Other 3.x Linux (32-bit)	1	356 MB	256 MB	Tenant1-OVCD-B-TestNet
tenant1-photon-01b	Powered on	Never Expires	06/25/2020, 9:38:08 AM	system						

Network Details for core-A:

- Network: Tenant1-OVCD-B-TestNet
- NIC 0: Connected
- IP Address: 192.168.120.51
- Copy to Clipboard

1. Confirm that **core-A VM** shows up here.
2. Verify the network is **Tenant1-OVDC-B-TestNet**

Configure Test Cleanup



To delete the test failover results, we will configure Test Cleanup. The cleanup deletes all recovered vApps and virtual machines.

1. Switch to On-Premises tab
2. Click on **Outgoing Replications**
3. Check the checkbox for VM **core-A**
4. Expand **ALL ACTIONS**
5. Click on **Test Cleanup**

Confirm Test Cleanup

Test Cleanup | core-A

You are about to **clean-up** the test failover results for the selected replications.

This will cause all recovered VMs and vApps to be **deleted**.



1. Click on **CLEANUP**.

Test Cleanup is Started

The screenshot shows the vSphere Client interface for DRaaS. The 'Outgoing Replications' tab is active. A table lists replication details for 'core-A'. The 'Recovery state' column shows 'Test image ready'. A 'Clean up' button with a '10%' progress indicator is visible in the bottom right corner, highlighted by a red box and a circled '1'.

VM	vApp	SLA profile	RPO	Replication state	Recovery state	Replication type	Overall health	Last changed
core-A	core-A	N/A	24h	Healthy	Test image ready	Protection	Green	Clean up 10%

1. Confirm Test Cleanup is started.

Test Cleanup is Successful

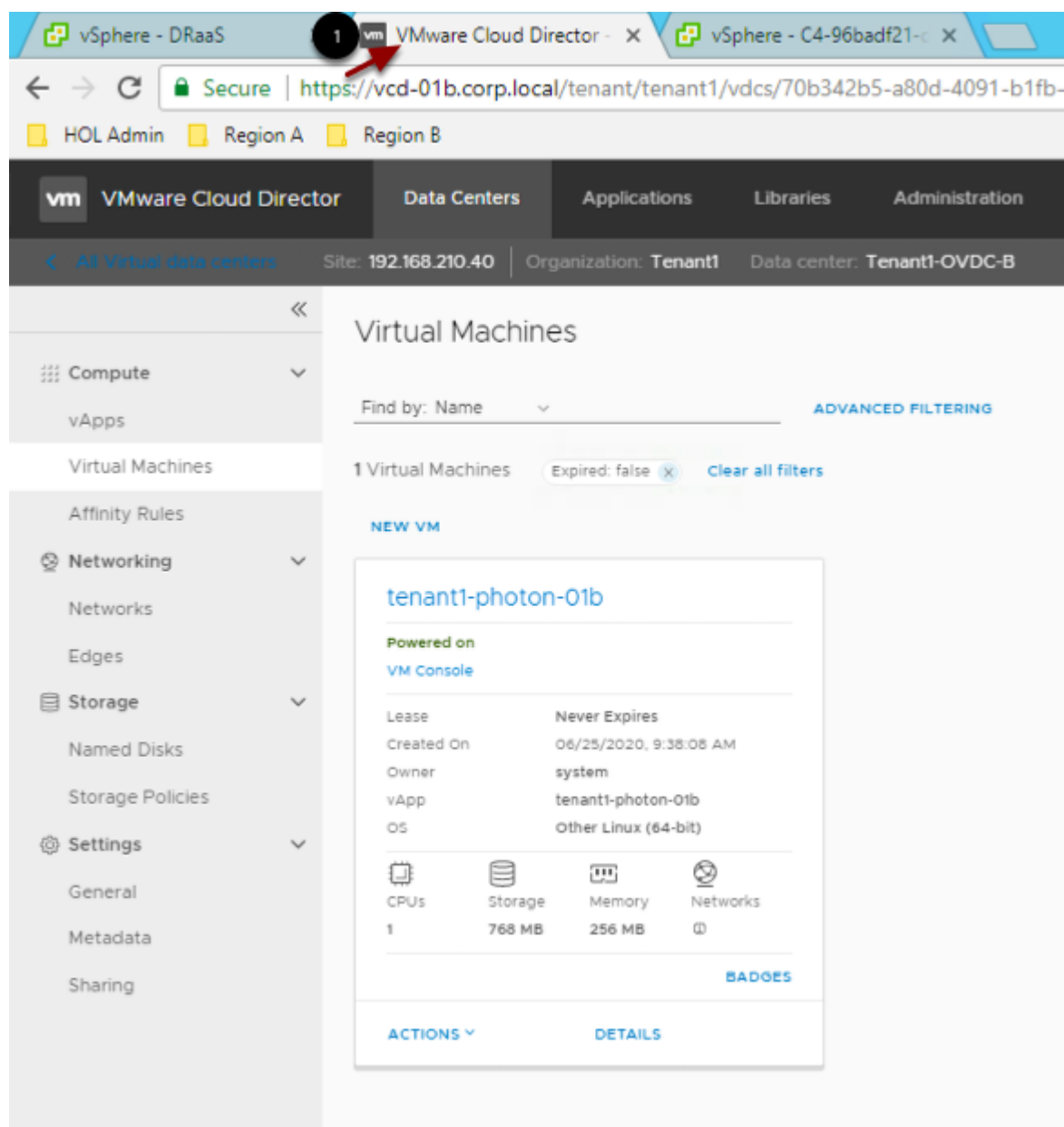
The screenshot shows the vSphere Client interface for DRaaS. The 'Outgoing Replications' tab is active. The 'Recovery state' column now shows 'Not started' and the 'Overall health' column shows 'Green'. A circled '2' points to the 'Recovery state' column.

VM	vApp	SLA profile	RPO	Replication state	Recovery state	Replication type	Overall health	Last changed
core-A	core-A	N/A	24h	Healthy	Not started	Protection	Green	7/5/20, 1:09 AM

Test Cleanup is completed successfully. Please Confirm

1. Recovery State is **Not Started**
2. Overall health is **Green**

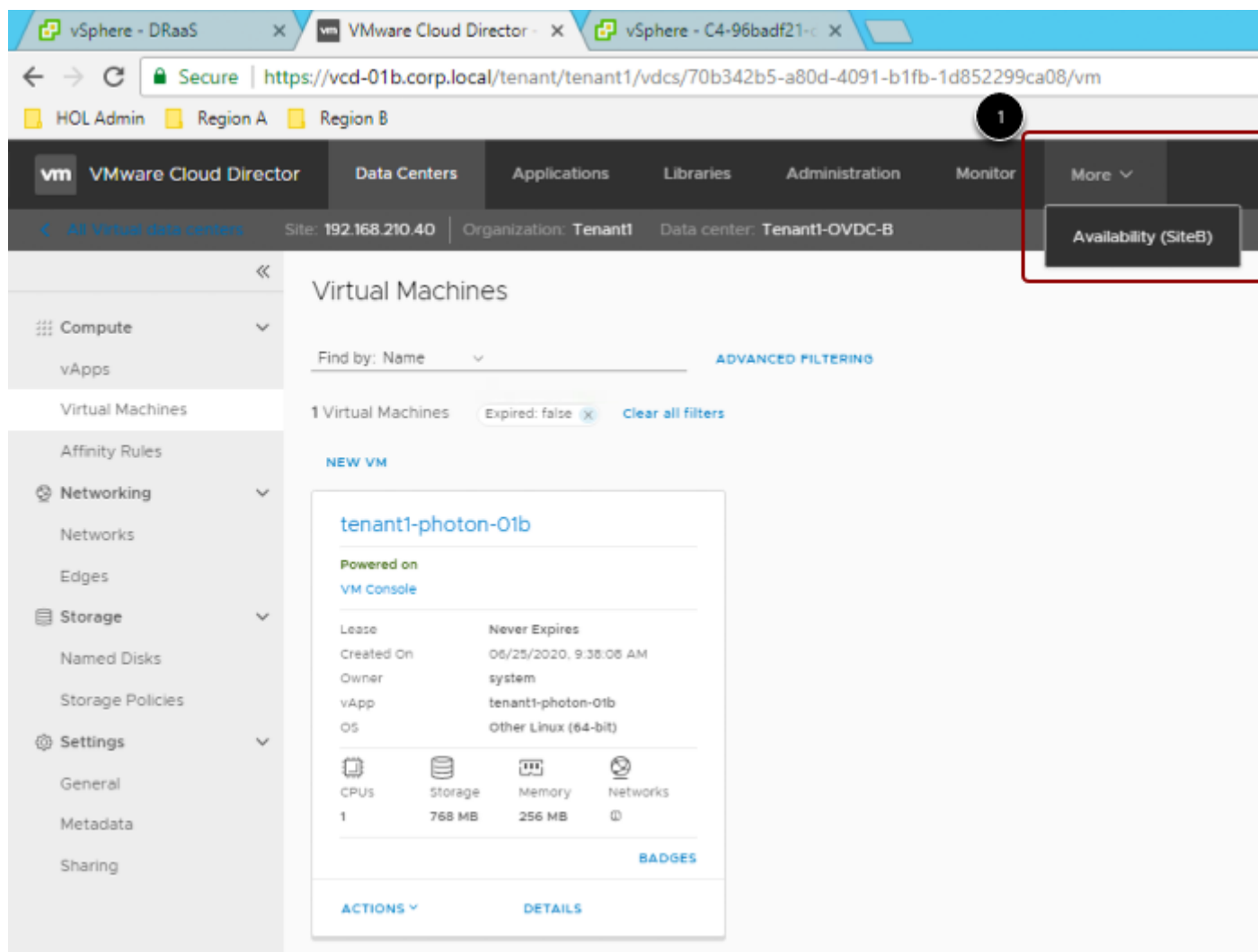
Confirm VM is removed from Cloud Site



1. Switch to tab **VMware Cloud Director Availability as a tenant**

Notice core-A VM is removed from here after Test Cleanup is successful.

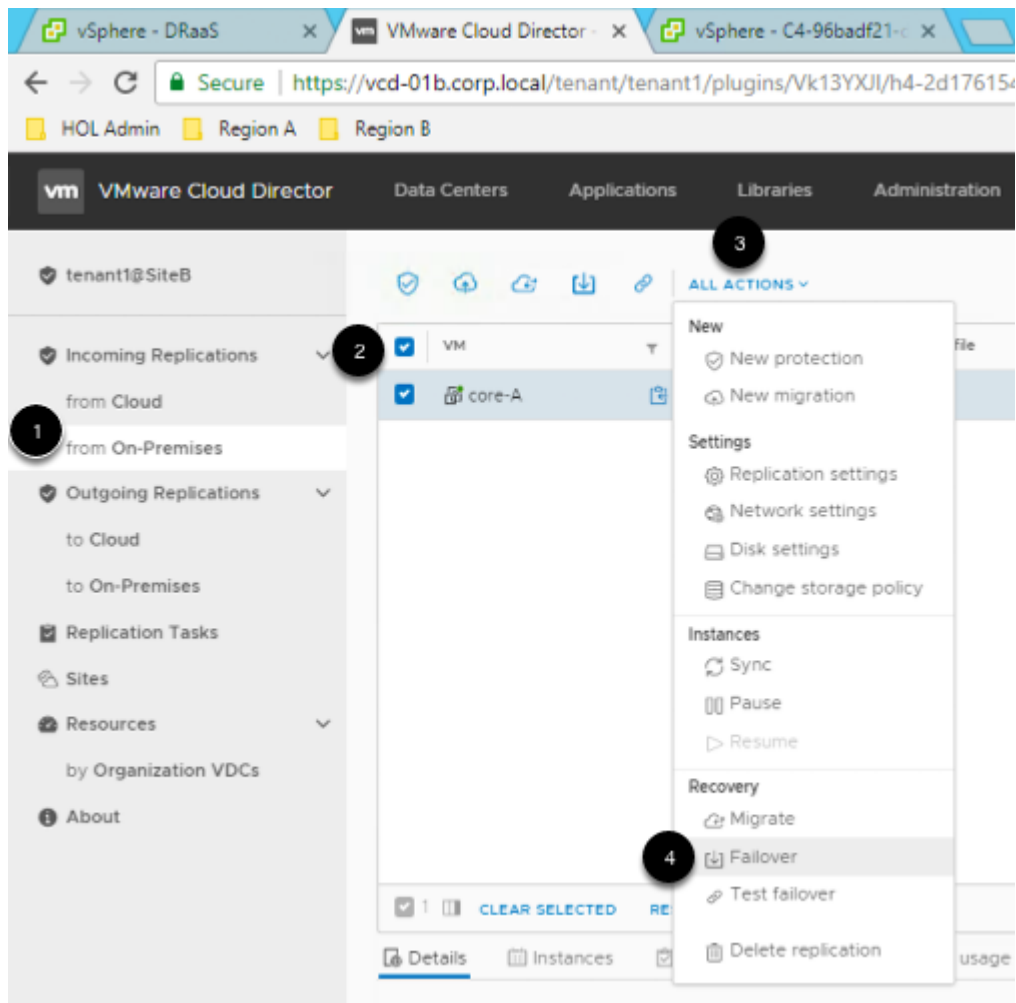
Perform a Failover Task from On-Prem to Cloud



If the protected source site is unavailable, in the destination site user can perform a workload disaster recovery operation. Lets DR failover a VM in Cloud.

1. Expand More and Click on **Availability (SiteB)**

Perform a Failover Task from On-Prem to Cloud



1. Click on **Incoming Replication from On-Premises**
2. Check the checkbox for VM **core-A**
3. Expand **ALL ACTIONS**
4. Click on **Failover**

Configure Recovery Settings for Failover

Failover

- 1 Recovery Settings
- 2 Recovery Instance
- 3 Ready To Complete

Recovery Settings

Select configuration for the recovered VMs

☐ Consolidate VM disks

*Turning on this option will consolidate all instances into the recovered disk.
This can improve the runtime performance of the recovered VM, but may greatly increase RTO.*

☒ Power on recovered VMs

Network Settings

☒ Apply preconfigured network settings on failover

☐ Connect all VMs to network

CANCEL **1** **NEXT**

Consolidate VM disks - Enable for a better performance of the recovered virtual machines at the expense of the failover task taking longer to complete.

Power on recovered vApps - Select to power on the virtual machines on the destination site after the task completes.

Network settings

- Select **Apply preconfigured network settings on failover**, to assign the network configured during the virtual machine replication
- Select **Connect all VMs to network** and from the drop-down menu select a network to connect the replicated virtual machines to.

1. Leave the defaults and Click on **NEXT**

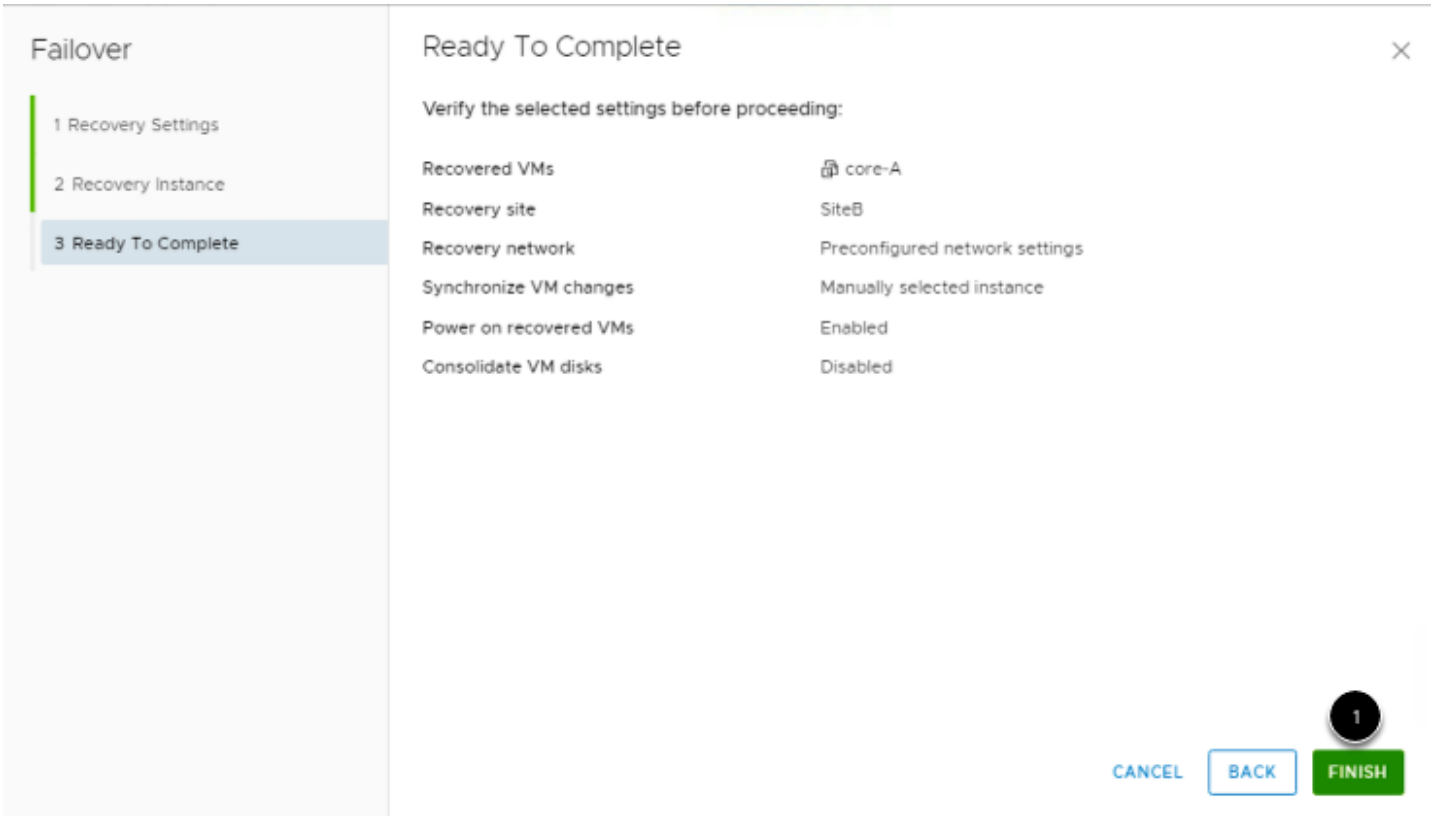
Configure Recovery Instance for Failover

The screenshot shows a web interface for configuring a recovery instance for failover. On the left, a sidebar titled 'Failover' contains three steps: '1 Recovery Settings', '2 Recovery Instance' (which is highlighted), and '3 Ready To Complete'. The main area is titled 'Recovery Instance' and has a close button (X) in the top right corner. Below the title, it says 'Select recovery point in time.' There is a small icon of a server labeled 'core-A'. To the right of this is a large light blue rectangular area representing a timeline, with a single blue dot in the center. At the bottom left of this area, the text '7/6/20, 12:05 AM' is visible. At the bottom right of the main area, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'. The 'NEXT' button is highlighted in blue and has a small black circle with the number '1' above it.

On the Recovery Instance page, you can choose the recovery point in time instance for failover.

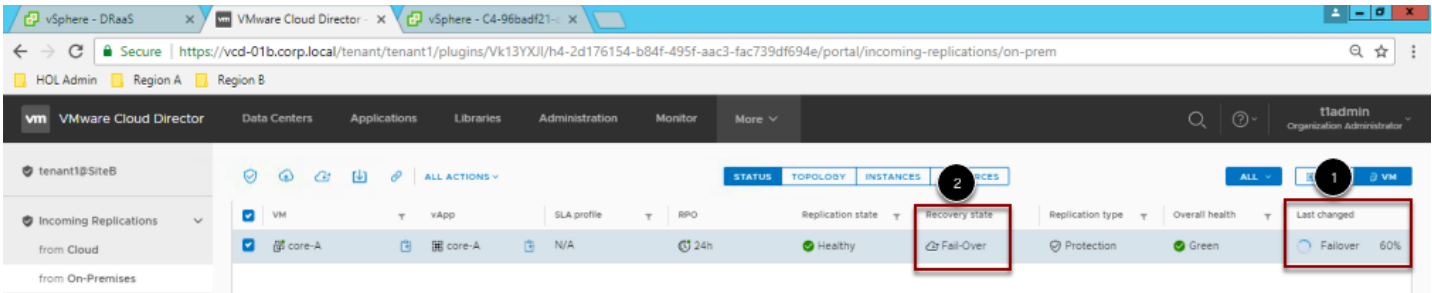
1. We'll continue with default latest instance and Click on **NEXT**

Ready to Complete the Failover



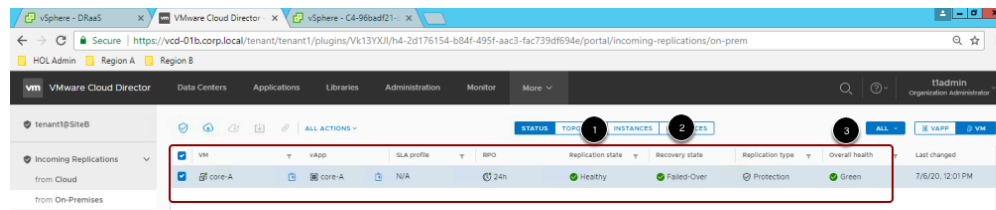
1. Review the Failover details and Click on **FINISH**

Failover in Progress



1. In the Detailed Status, you will notice **Failover in Progress with % progress**.
2. While Failover progresses, you will notice the Recovery State is updated to **Fail-Over**

Failover completed successfully

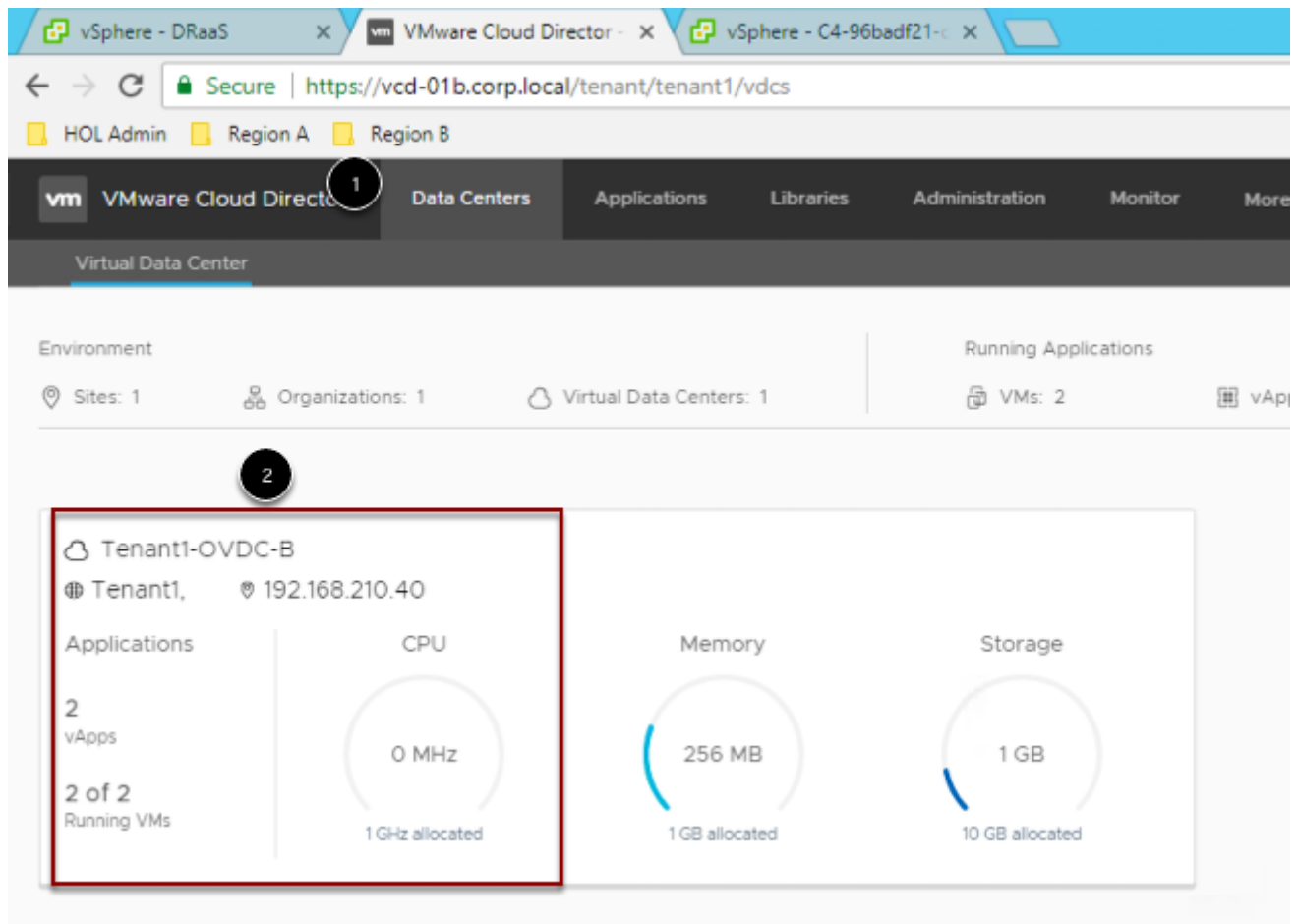


This process will take a couple of minutes. Please be patient. After the failover task finishes, the failed over workload is running in the destination site and the workload is no longer protected upon the task completion

1. Replication State is **Healthy**
2. Recovery State shows **Failed-Over**.
3. Overall health is **Green**

Note: In case you see Unexpected vCloud Director error during failover, please retry. Due to the nested environment in Hands On Lab, sometimes the error is seen, in real world it should work seamlessly.

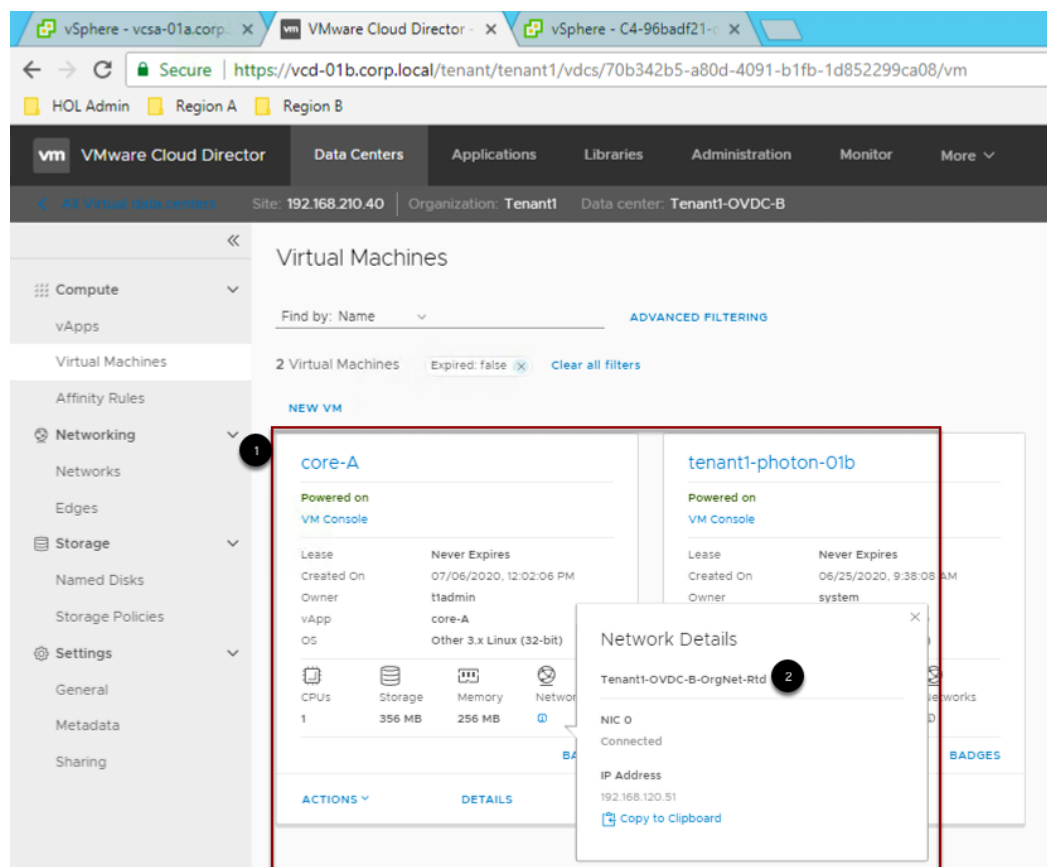
Verify VM is Failed-Over to Cloud



After DR failover, we will confirm that the VM is Failed-Over and powered-on in Cloud site

1. Click on **Data Centers**
2. Click on virtual datacenter **Tenant1-OVDC-B**

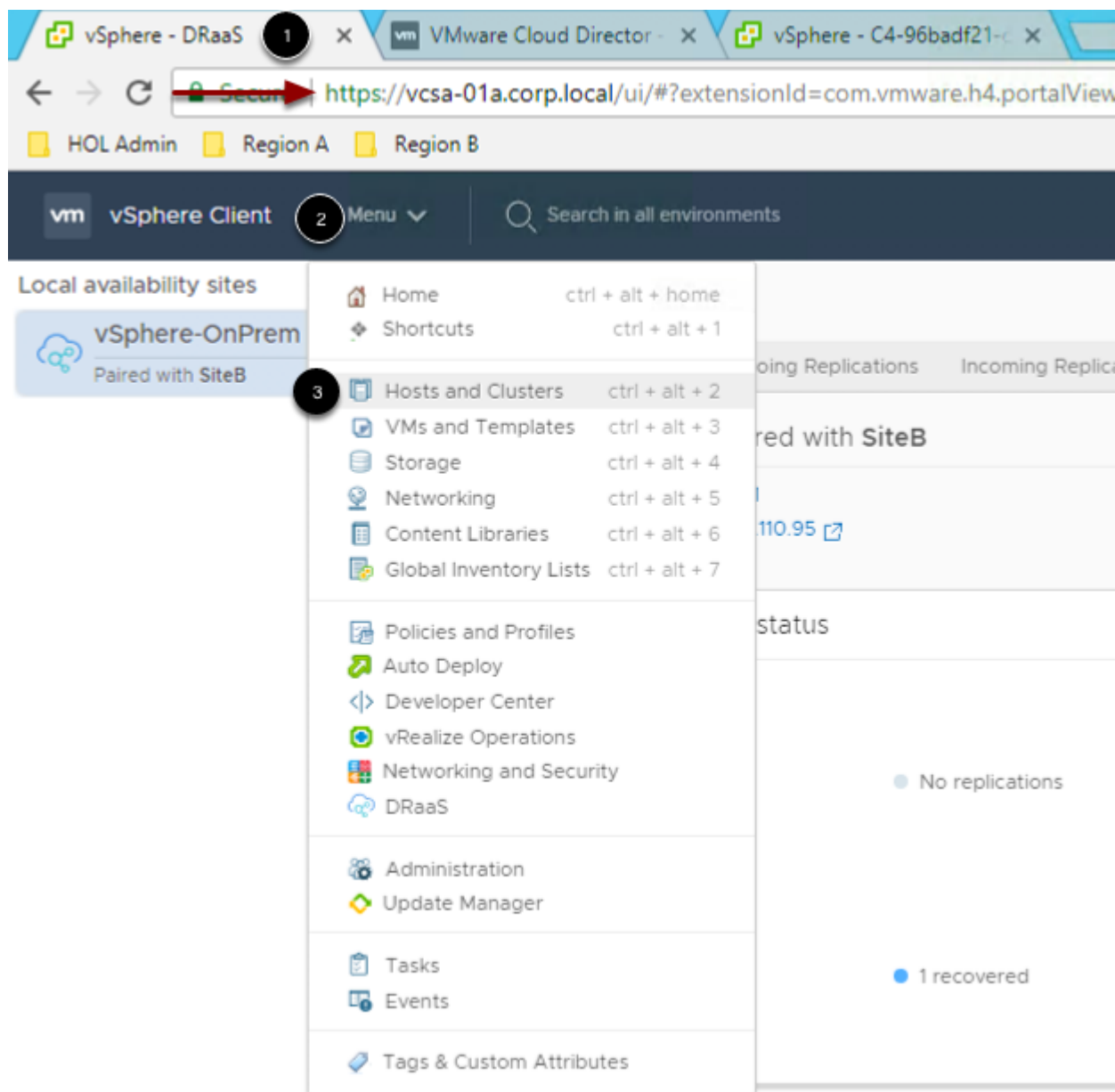
Confirm VM is Failed-Over and Running in Cloud



1. Confirm that **core-A VM** shows up here.
2. Verify the network is **Tenant1-OVDC-B-OrgNet-Rtd** (since this was the one preconfigured for Failover workflows in the previous exercise).

The Failed-Over VM is running on the destination site now. The VM is no longer protected.

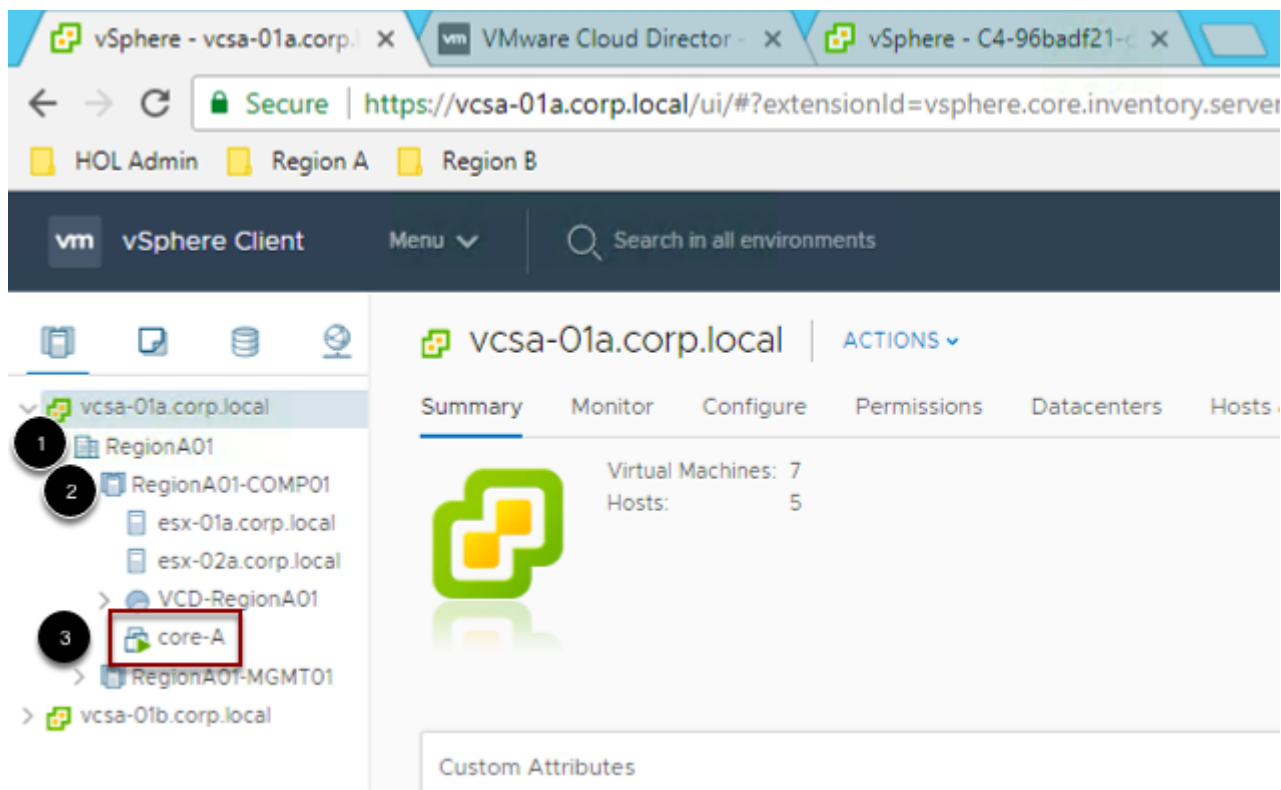
Go to Hosts and Clusters view on On-Premises Site A



Since we performed DR failover in Cloud assuming protected source site is unavailable, VM remains powered on in Site A. Lets confirm that.

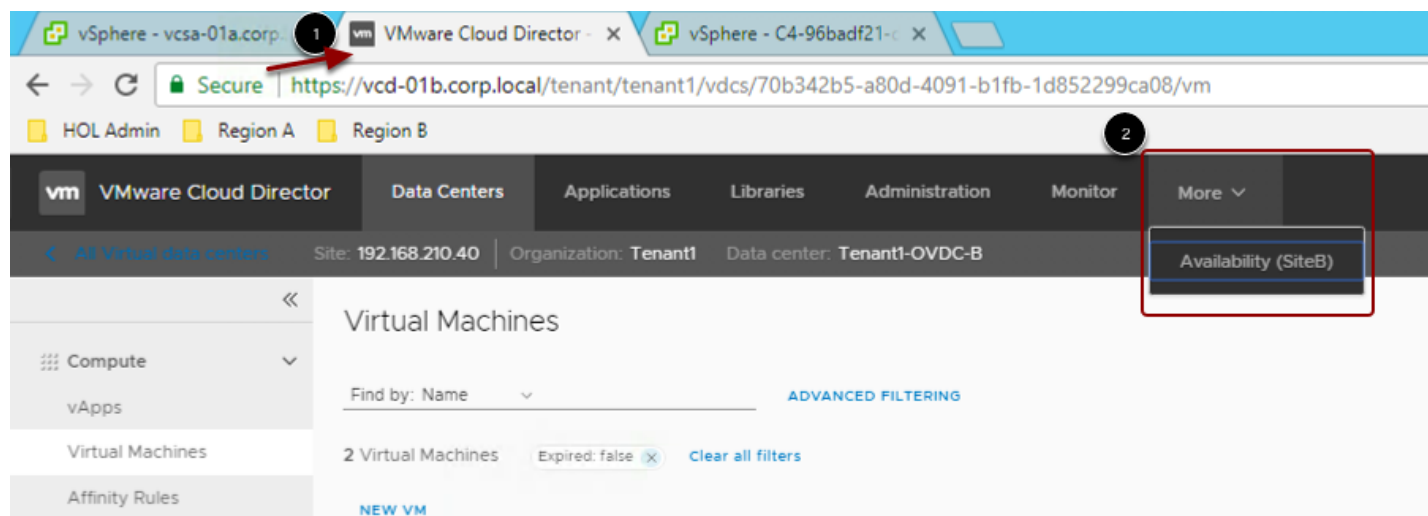
1. Switch to tab for **vSphere On-Premises site**
2. Expand **Menu**
3. Click on **Hosts and Clusters**

Go to Hosts and Clusters view on On-Premises Site A (contd..)



1. Expand **RegionA01**
2. Expand **RegionA01-COMP01**
3. Confirm core-A is still powered on at On-Premises SiteA

Configure Reverse Replication from Cloud to On-Prem

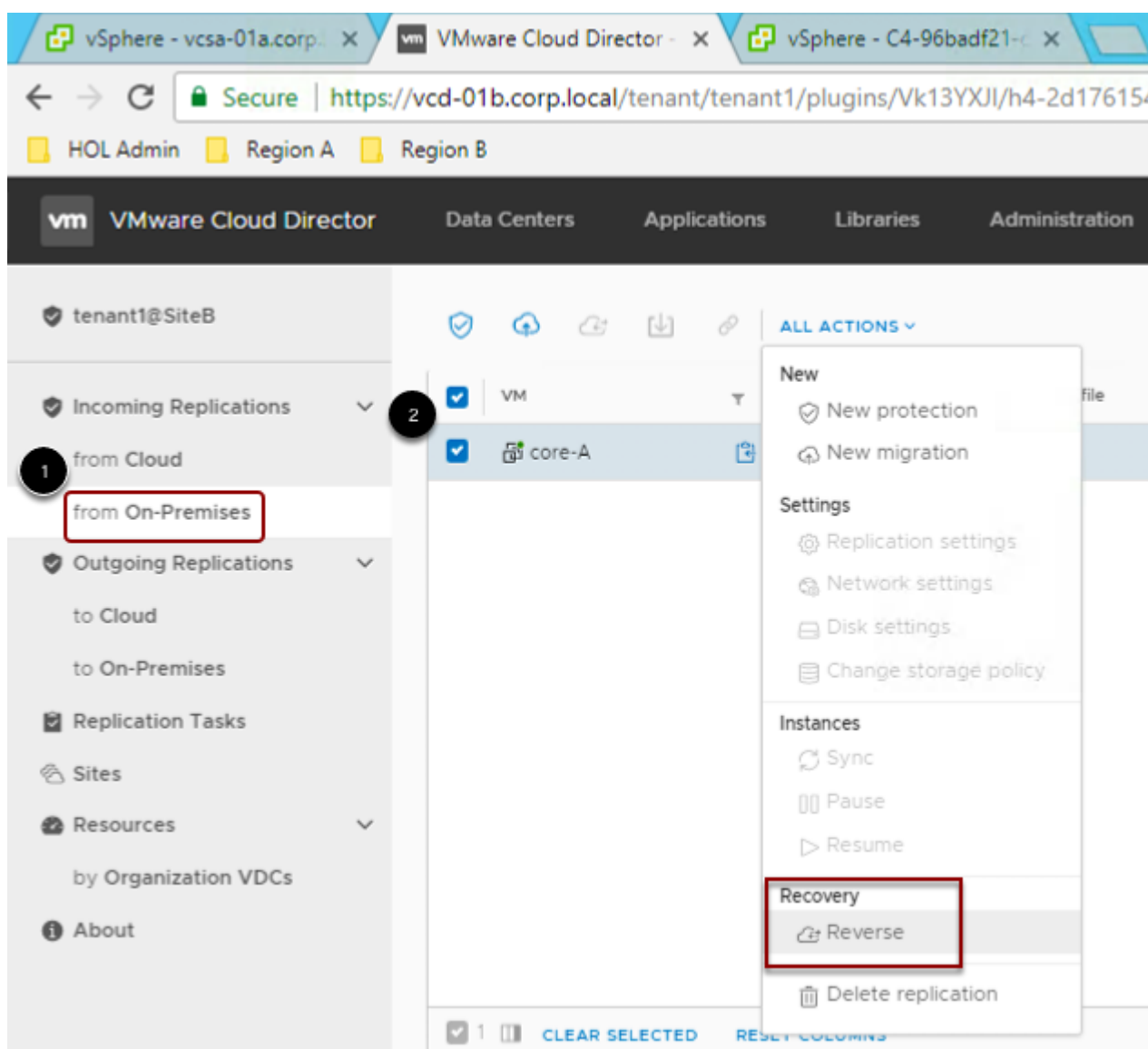


After a failover from the source site to the destination site, the migrated workload runs on the destination site. A subsequent reverse task replicates the recovered workload data back to the source protected vApp or virtual machine.

We will reverse replicate the VM core-A from Cloud to On-Premise in this exercise.

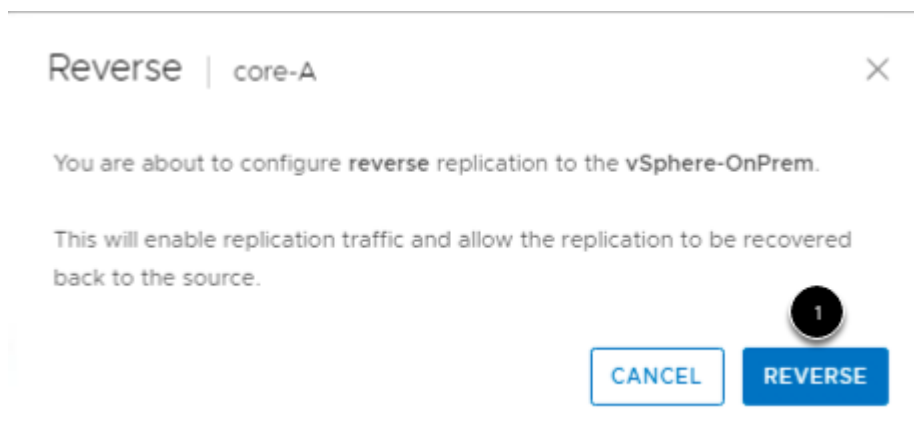
1. Switch to tab **Cloud Site**
2. Expand More and click on **Availability**

Configure Reverse Replication from Cloud to On-Prem (contd..)



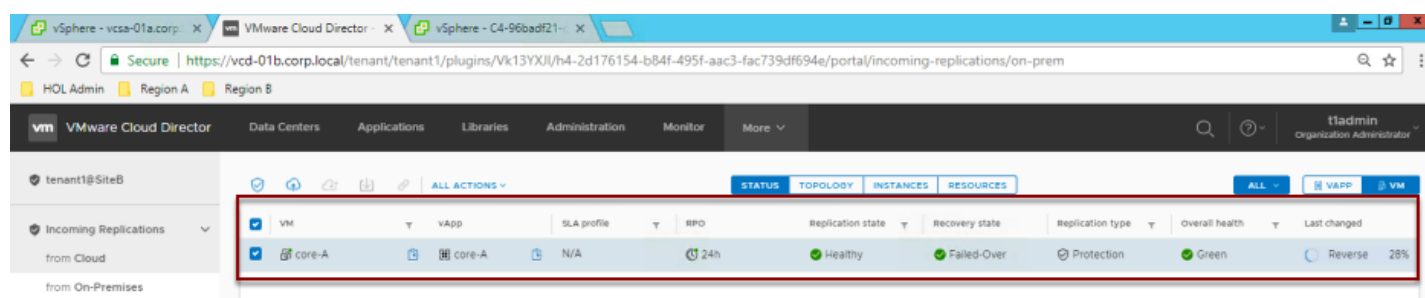
1. Click on **Incoming Replications from On-Premises**
2. Check the checkbox for VM **core-A**
3. Expand **ALL ACTIONS** and click on **Reverse**

Confirm Reverse Replication from Cloud to On-Prem



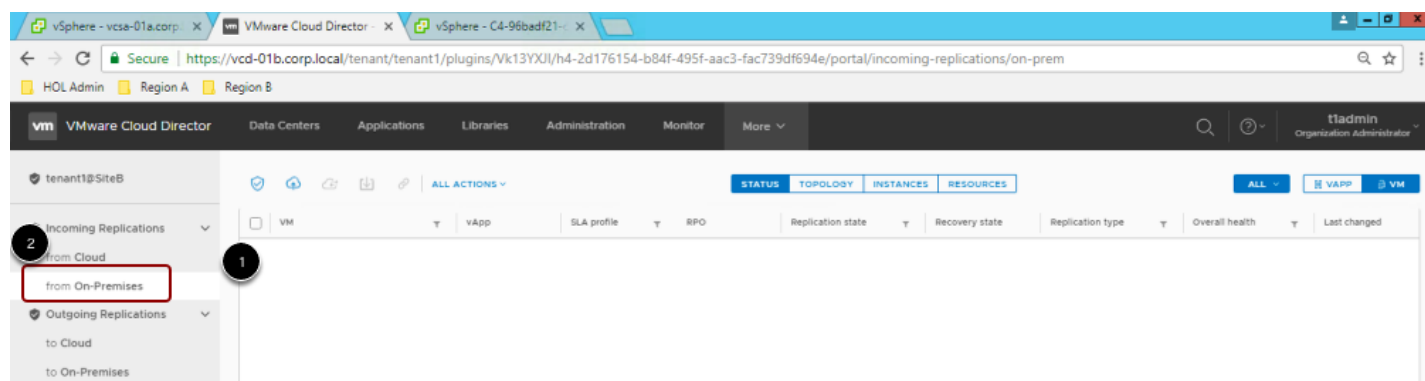
1. Click on **REVERSE**

Reverse Replication is in Progress



Reverse Replication is in progress. You can monitor the progress of the Reverse task in Last changed section.

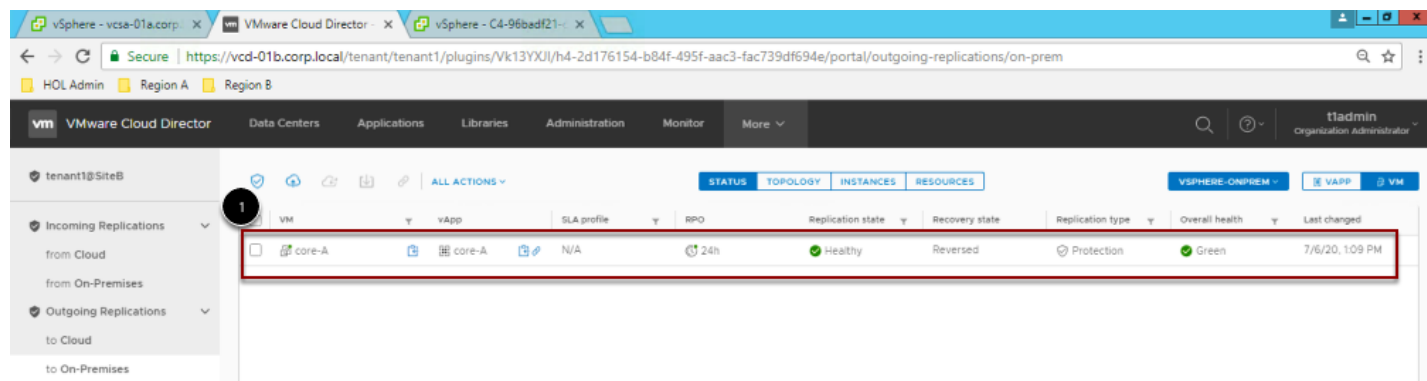
Reverse Replication is Completed



1. As soon as Reverse replication is successfully completed, Incoming Replications from On-Prem is empty now

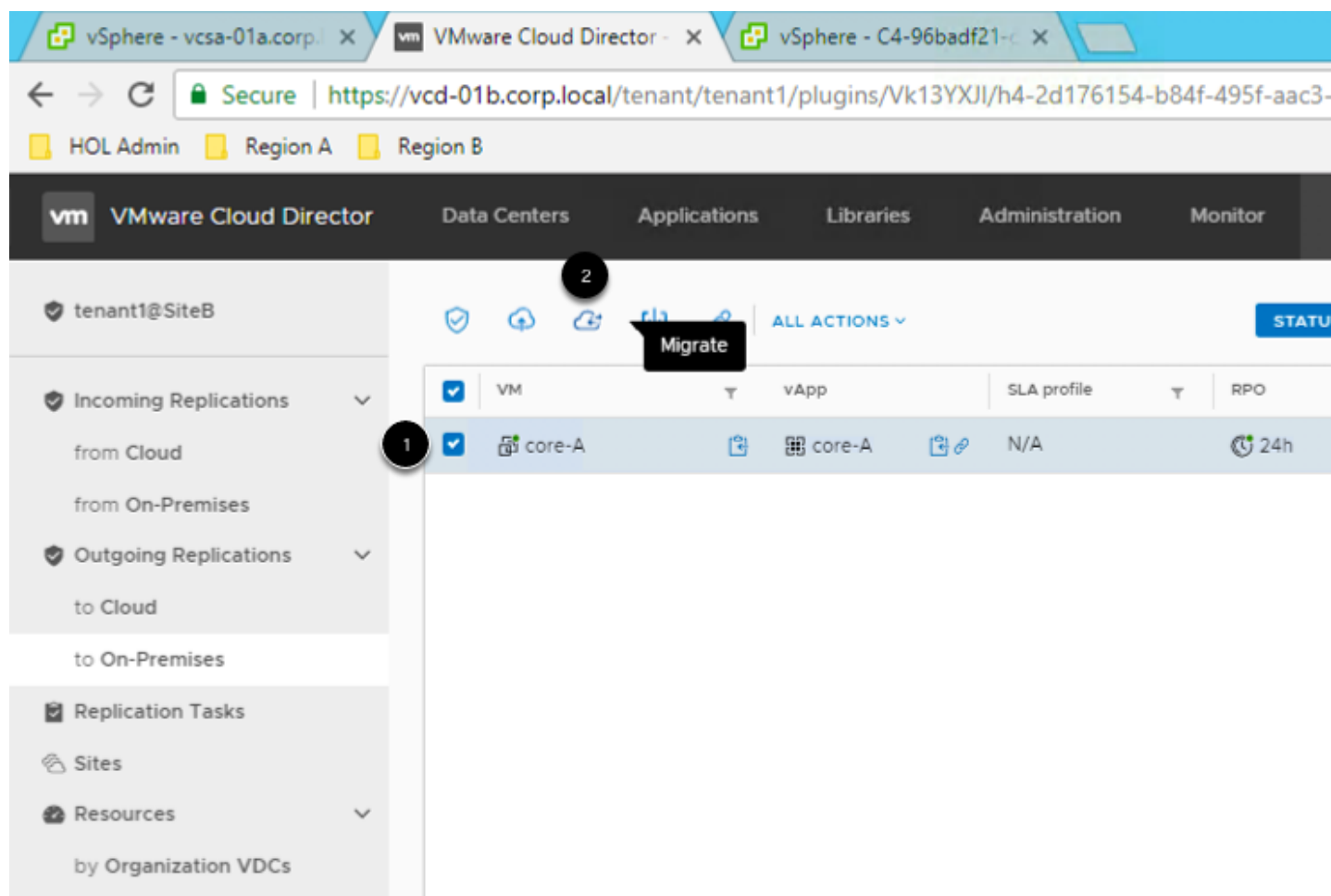
- Since the replication is now configured from Cloud to On-Prem, we will view **Outgoing Replications to On-Prem**

View Outgoing Replications from Cloud to On-Prem



- Here you will notice VM core-A is replicated back to On-Prem and Recovery State is **Reversed**

Migrate VM back to On-Prem



Since the VM is successfully replicated back from Cloud to On-Prem, we will learn to Migrate the VM from Cloud back to On-Prem. Migrating a vApp or a virtual machine to a remote organization runs the workload in the destination site.

The difference between Migrate and Failover workflow is that Migration assumes everything is up and running well at both sites so it powers off the VM/vApp at source site whereas Failover workflow assumes source site is not reachable and leaves the VM/vApp at source running in the same state.

1. Check the checkbox for **VM core-A**
2. Click on Migrate

Configure Migrate Settings

Migrate

1 Migrate Settings

2 Ready To Complete

Migrate Settings

Select configuration for the recovered VMs

Instance options: Do nothing (selected), Do nothing, Expose PITs, Consolidate

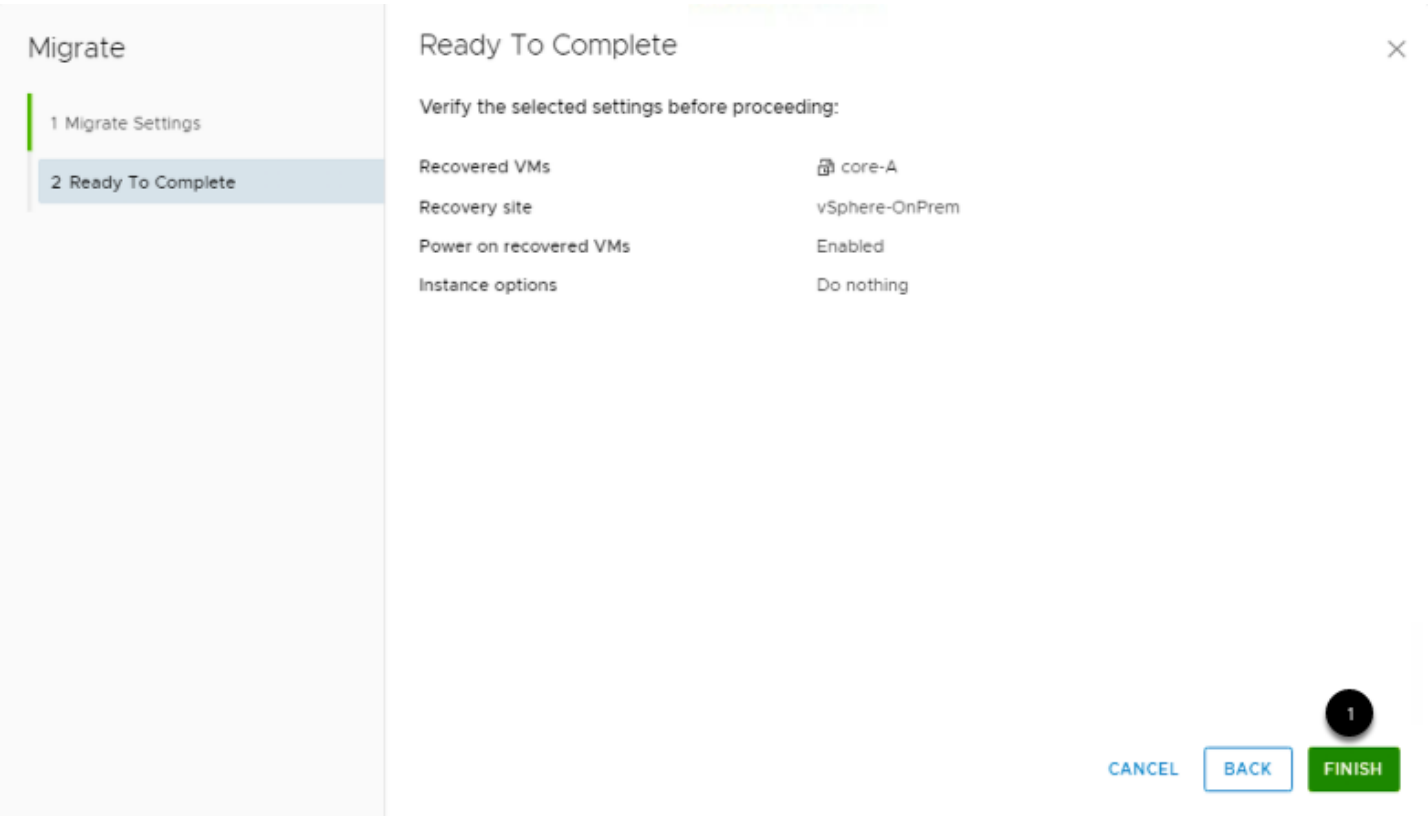
☒ Power on recovered VMs

⚠ All source VMs will be powered-off after successful recovery.

CANCEL NEXT

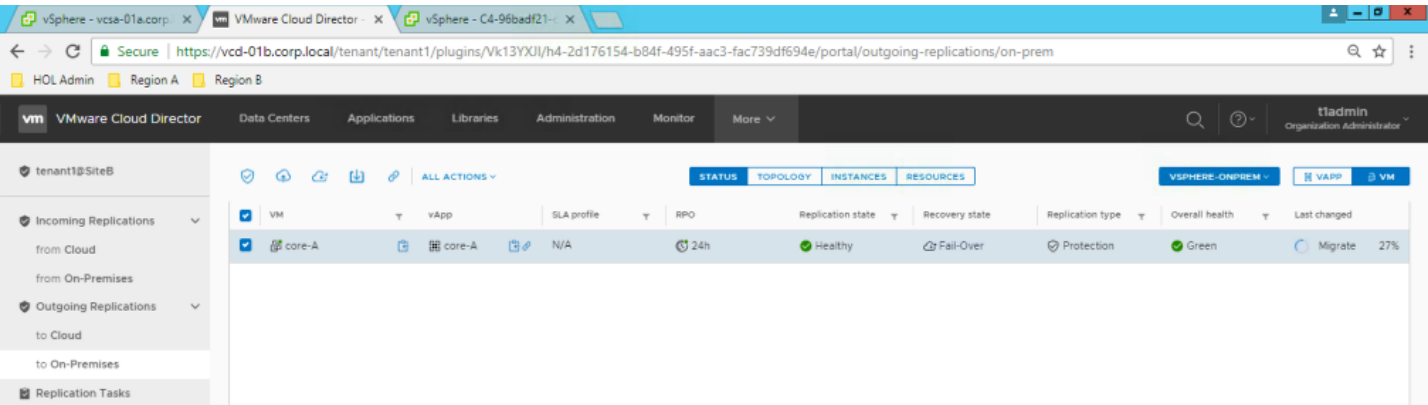
1. Leave the Defaults and Click on **NEXT**

Complete Migration to SiteA



1. Review the Migation Settings and click on **FINISH**

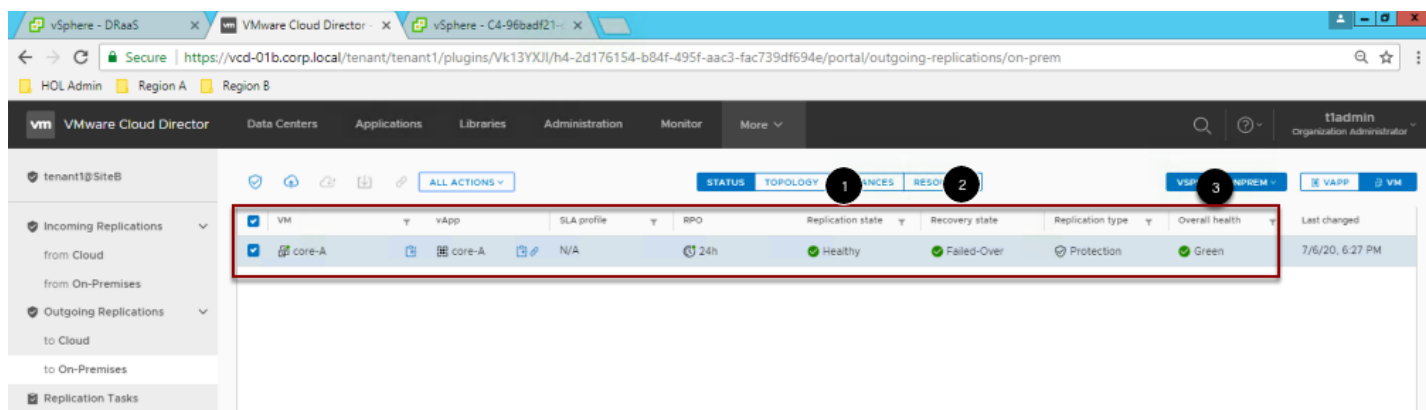
Migrate to SiteA in Progress



Migration is **in progress**.

Note: This process will take a few minutes. In case you see an error during, please retry. Due to the nested environment in Hands On Lab, sometimes the error is seen, in real world it should work seamlessly.

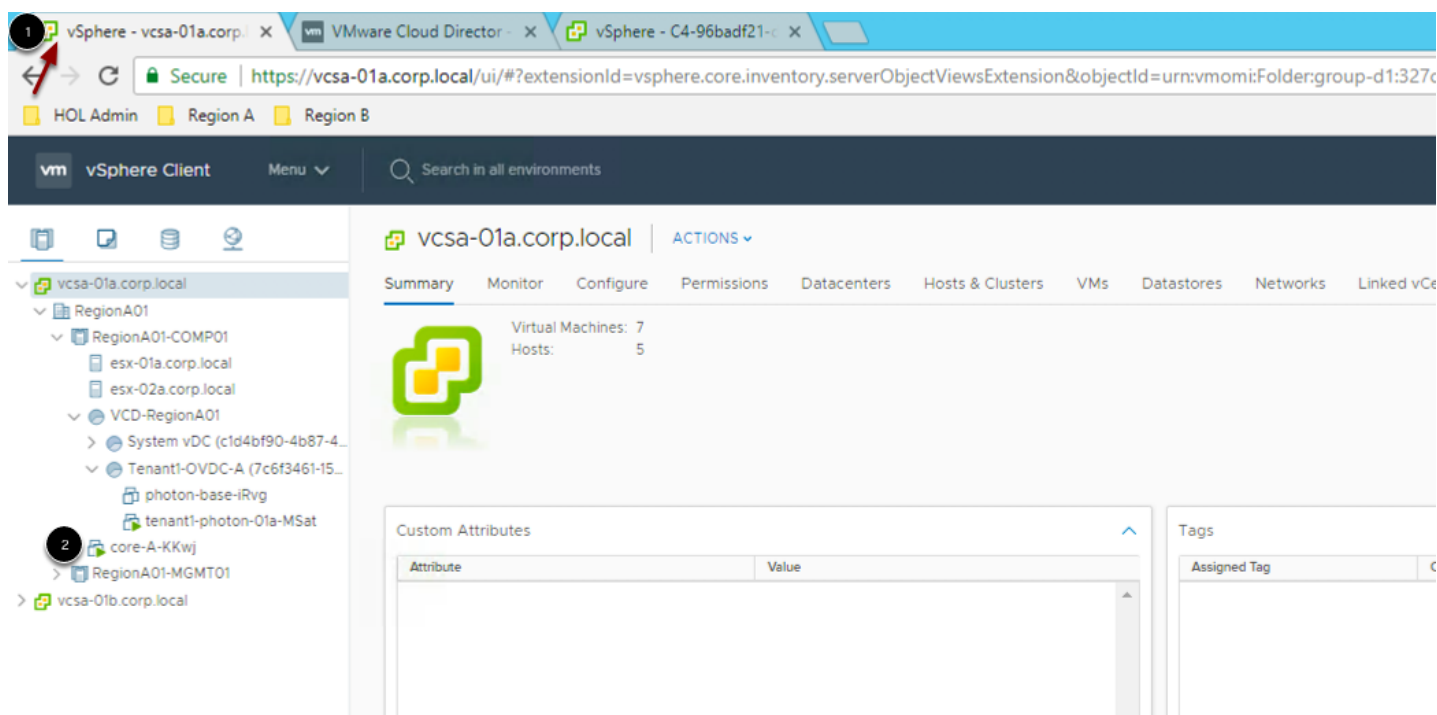
Migration to SiteA is Completed Successfully



Confirm the:

1. Replication state is **Healthy**
2. Recovery state is **Failed-Over**
3. Overall health is **Green**

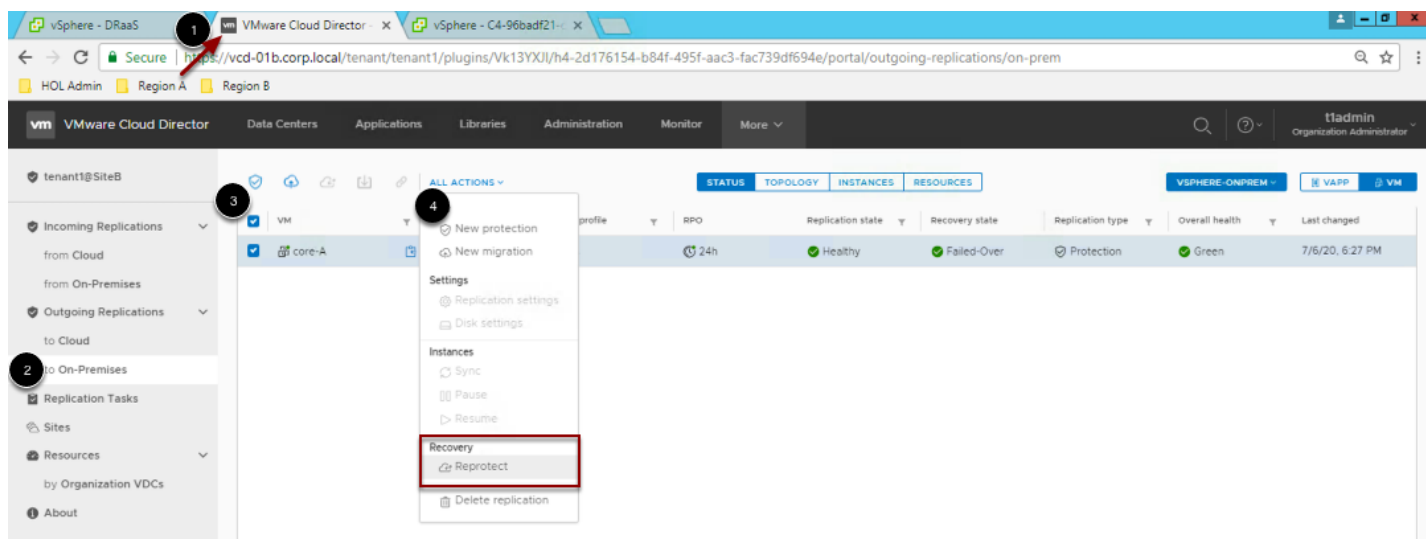
Confirm VM is Migrated back to SiteA



Since Migration from Cloud to On-Premises site is successful, workload now is powered on and runs in the destination site (On-Premises here)

1. Switch back to tab **vCenter SiteA**
2. **VM core-A** now shows up in the inventory.

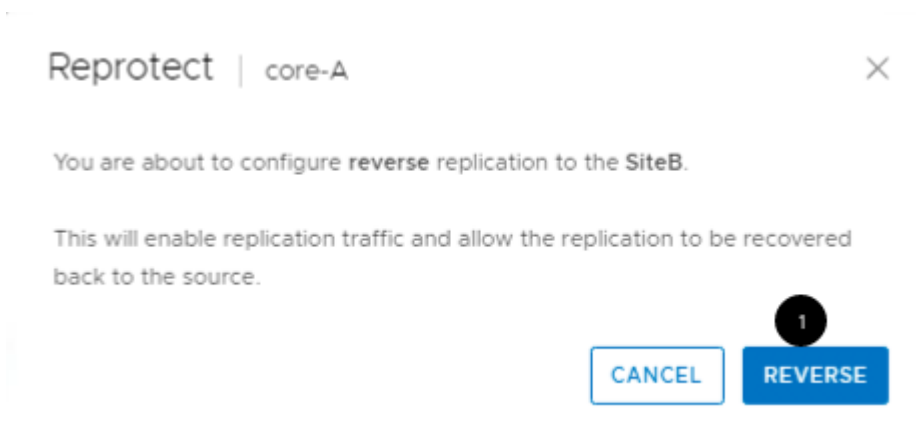
Reprotect VM back from On-Prem to Cloud



After migrating over the workload to On-Premises, we can reverse the replication and reprotect it back to Cloud site. This is done by selecting the Reprotect button. Once Reprotect is successful, this will show as outgoing replication from On-Premises to Cloud

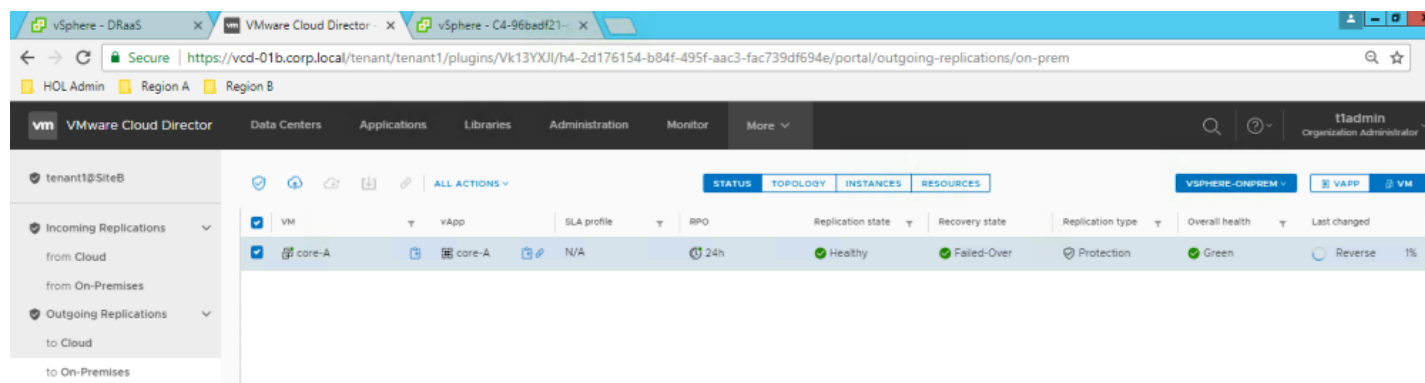
1. Switch to tab **vCD SiteB**
2. Expand Outgoing Replication to **On-Premises**
3. Check the checkbox for **VM core-A**
4. Expand **ALL ACTIONS** and Click on **Reprotect**

Configure Reprotect Settings



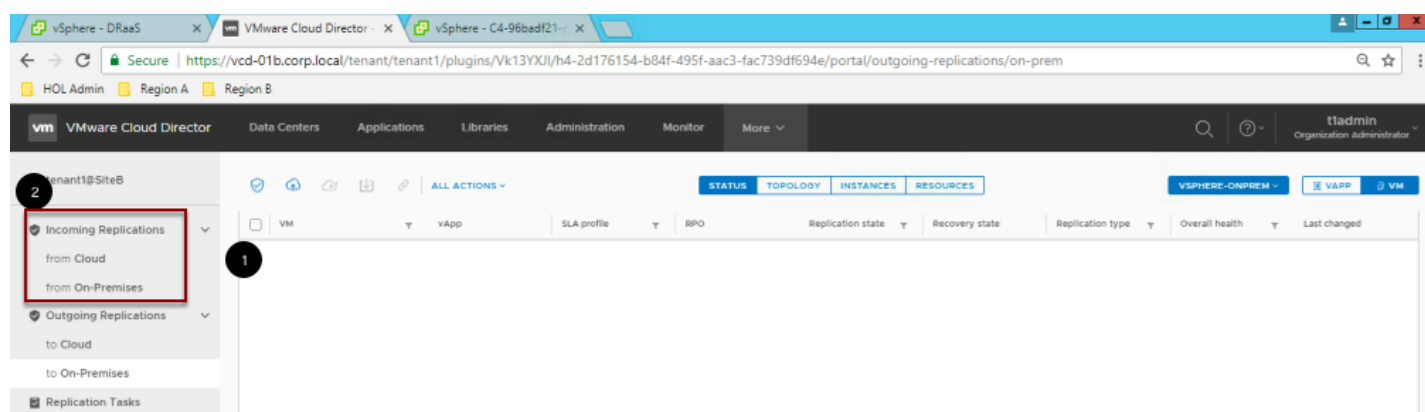
1. Click on **REVERSE**

Reprotect from On-Premises to Cloud Is In Progress



Reprotect is **in progress**.

Reprotect from On-Premises to Cloud Completed Successfully



1. As soon as Reproprotect is successfully completed, Outgoing Replications to On-Prem is empty now
2. Since the replication is now configured from On-Premises to Cloud, we will view **Incoming Replications from On-Prem**

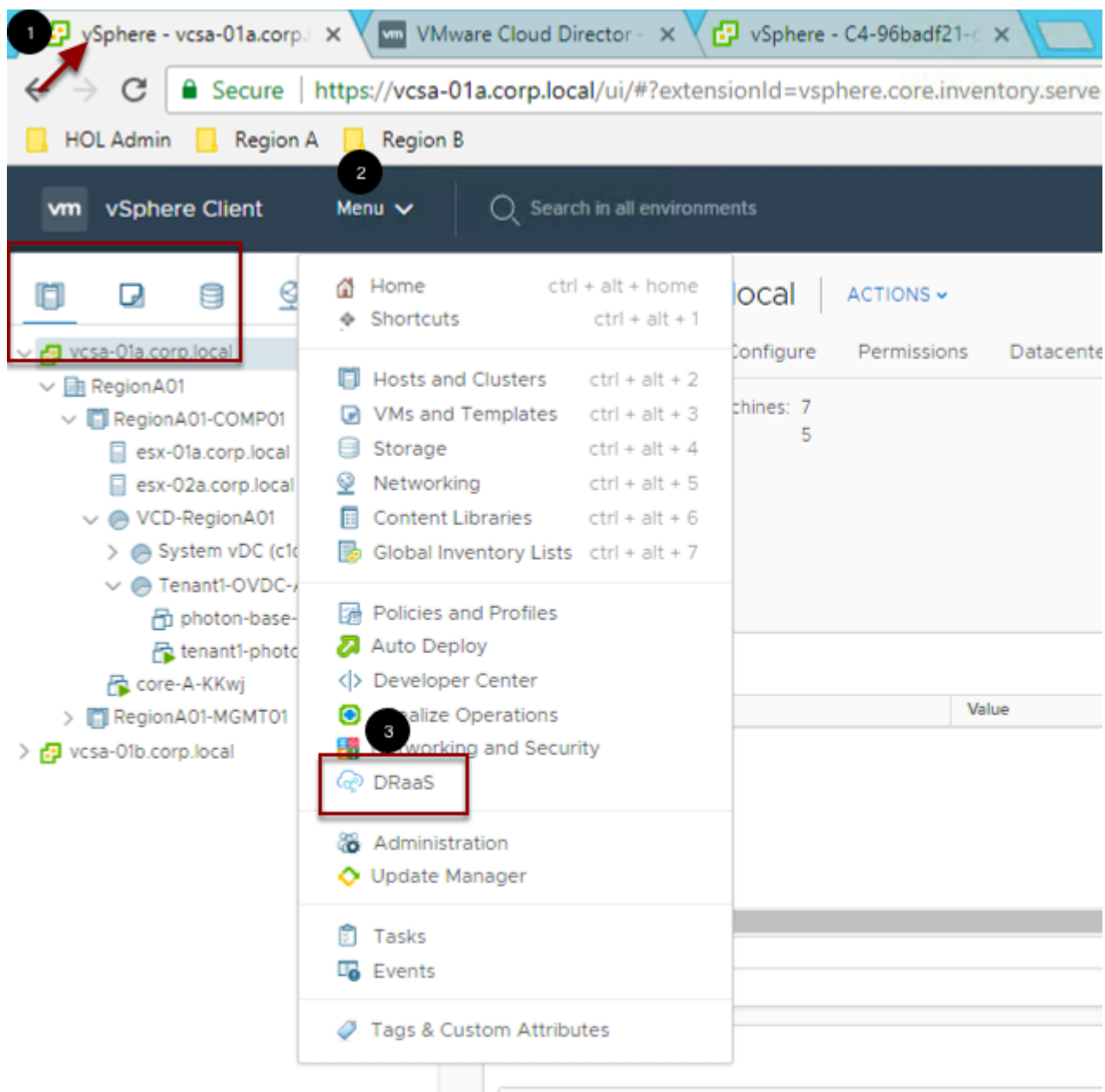
View Incoming Replications from On-Prem

The screenshot shows the VMware Cloud Director web interface. The browser address bar displays the URL: <https://vcd-01b.corp.local/tenant/tenant1/plugins/Vk13YXJl/h4-2d176154-b84f-495f-aac3-fac739df694e/portal/incoming-replications/on-prem>. The left sidebar menu is open, and a red box highlights the 'Incoming Replications' section, which includes 'from Cloud' and 'from On-Premises' options. The main content area shows a table of incoming replications. The table has columns for VM, VApp, SLA profile, RPO, Replication state, Recovery state, Replication type, Overall health, and Last changed. One replication is listed: VM 'core-A-KKwj', VApp 'core-A', SLA profile 'N/A', RPO '24h', Replication state 'Healthy', Recovery state 'Not started', Replication type 'Protection', Overall health 'Green', and Last changed '7/6/20, 6:29 PM'.

VM	VApp	SLA profile	RPO	Replication state	Recovery state	Replication type	Overall health	Last changed
core-A-KKwj	core-A	N/A	24h	Healthy	Not started	Protection	Green	7/6/20, 6:29 PM

1. Select Incoming Replications from **On-Premises**
2. Here you will notice VM core-A is replicated back from On-Premises to Cloud and Replication type is **Protection**

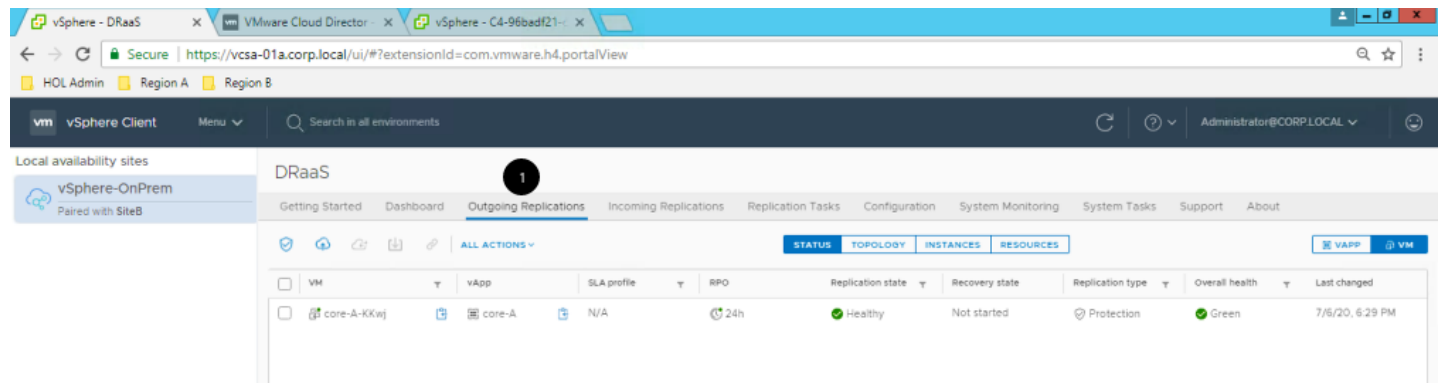
Verify replication status from On-Premises site



Lets look at On-Premises site and confirm the VM is reprotected from On-Premises back to Cloud site.

1. Switch to tab vSphere On-Premises site
2. Expand **Menu**
3. Click on **DRaaS**

Verify replication status from On-Premises site



1. Click in Outgoing Replications
2. Confirm VM core-A-xxxx is replicated back from On-Premises to Cloud and Replication type is **Protection**

Congratulations!! You have successfully replicated a VM from On-Premises to Cloud, run the recovery in Cloud, and now replicated and migrated the VM from Cloud back to On-Premises and reprotected the VM from On-Premises back to Cloud.

Please close all tabs on the browser.

Conclusion

In this module, we went over Site pairing from On-Premises to Cloud, Failover Recovery workflows from On-Premises to Cloud using VMware Cloud Director Availability

You've finished Module 2

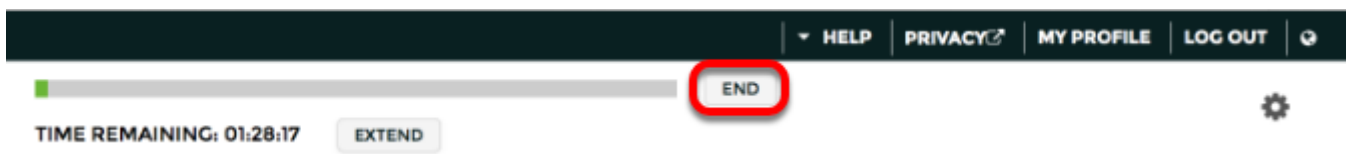


Congratulations on completing Module 2.

Here are the other modules in this lab that may interest you:

- [Module 1 - VMware Cloud Director Availability Overview and Architecture](#) (15 minutes) (Basic) This module will show an overview of the architecture and deployment of VMware Cloud Director Availability 4.0
- [Module 3 - Administrator-driven Cloud-to-Cloud DR with VMware Cloud Director Availability](#) (30 minutes) (Basic) This module will show how administrators can use Cloud Director Availability for cloud-to-cloud DR workflows.
- [Module 4- Tenant-driven Cloud-to-Cloud DR with VMware Cloud Director Availability](#) (30 minutes) (Basic) This module will show Tenant Self-Service Cloud-to-Cloud DR using VMware Cloud Director Availability.

How to End Lab



To end your lab click on the **END** button.

Module 3 - Administrator-driven Cloud-to-Cloud DR with VMware Cloud Director Availability

Introduction

In this article, you will learn how to -

- Pair Cloud to Cloud sites
- Administrator driven Replication and Recovery workflow between Cloud Provider Sites

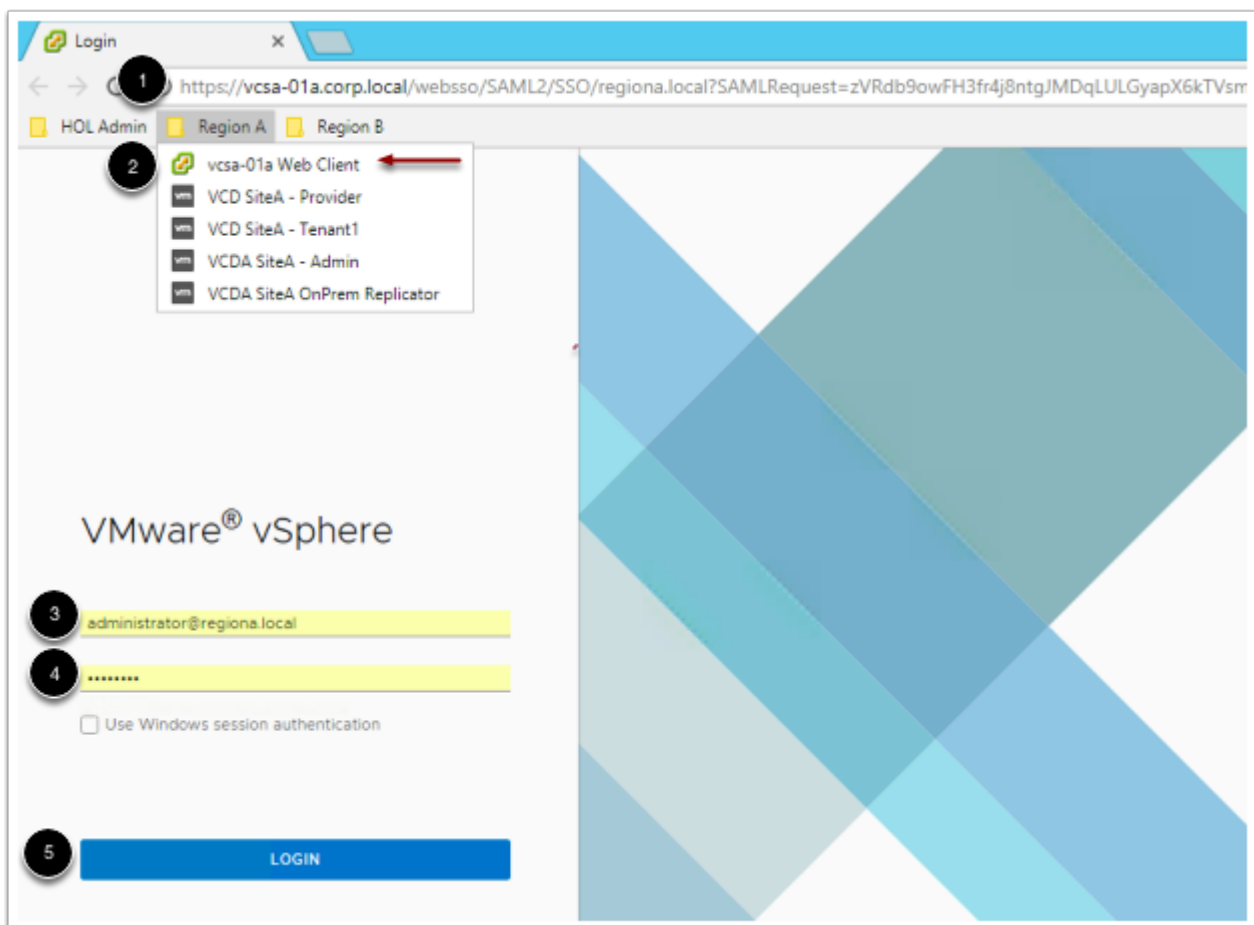
Site Pairing and Failover Workflows from Cloud to Cloud using vCloud Availability

In this exercise, we will learn to -

- Configure Site Pairing from Cloud to Cloud and
- Configure Failover Workflows from Cloud to Cloud using VMware Cloud Director Availability

Note that in the lab environment, we have already deployed and configured the VMware Cloud Availability appliances for each site, but we have not configured any site pairing yet.

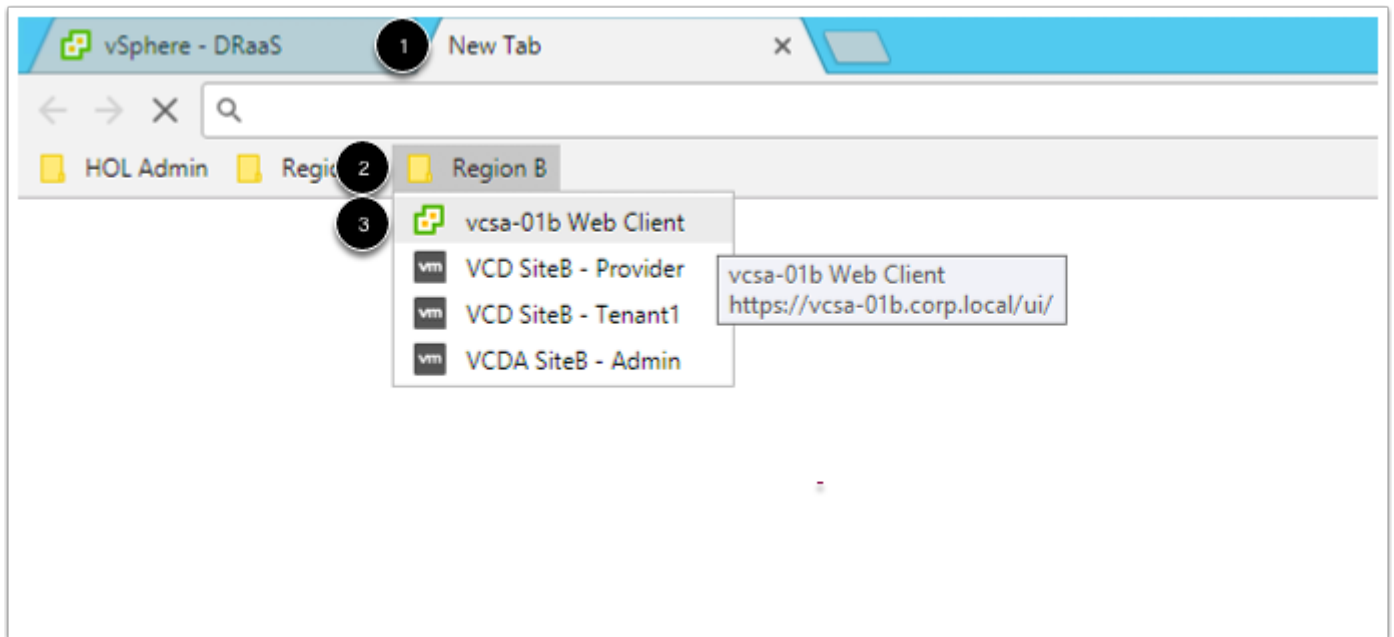
Login to RegionA vCenter (On-Premise)



1. Start the Chrome Browser from the desktop. Click on **RegionA** in the bookmarks bar.

2. Click on vcsa-01a Web Client. Verify the address as :
<https://vcsa-01a.corp.local/>
3. Enter Username: **administrator@regiona.local**
4. Enter Password: **VMware1!**
5. Click on **LOGIN**

Open RegionB vCenter



1. Open a new tab on the browser.
2. Click on **RegionB**
3. Click on vcsa-01b Web Client. Verify the address as :
<https://vcsa-01b.corp.local/>

Login to RegionB vCenter

The screenshot shows a web browser window with two tabs: 'vSphere - DRaaS' and 'Login'. The address bar displays the URL: <https://vcsa-01b.corp.local/webssso/SAML2/SSO/regiona.local?SAMLRequest=zVTljpswFN33K5D3YCCZPKyQU>. Below the address bar, there are three tabs: 'HOL Admin', 'Region A', and 'Region B'. The main content area displays the 'VMware® vSphere' logo. Below the logo, there are two input fields for login credentials. The first field is labeled '1' and contains the text 'administrator@corp.local'. The second field is labeled '2' and contains a series of dots representing a password. Below these fields is a checkbox labeled 'Use Windows session authentication'. At the bottom, there is a blue button labeled '3' and 'LOGIN'. The right side of the page features a decorative graphic with overlapping blue and teal triangles.

VMware® vSphere

1 administrator@corp.local

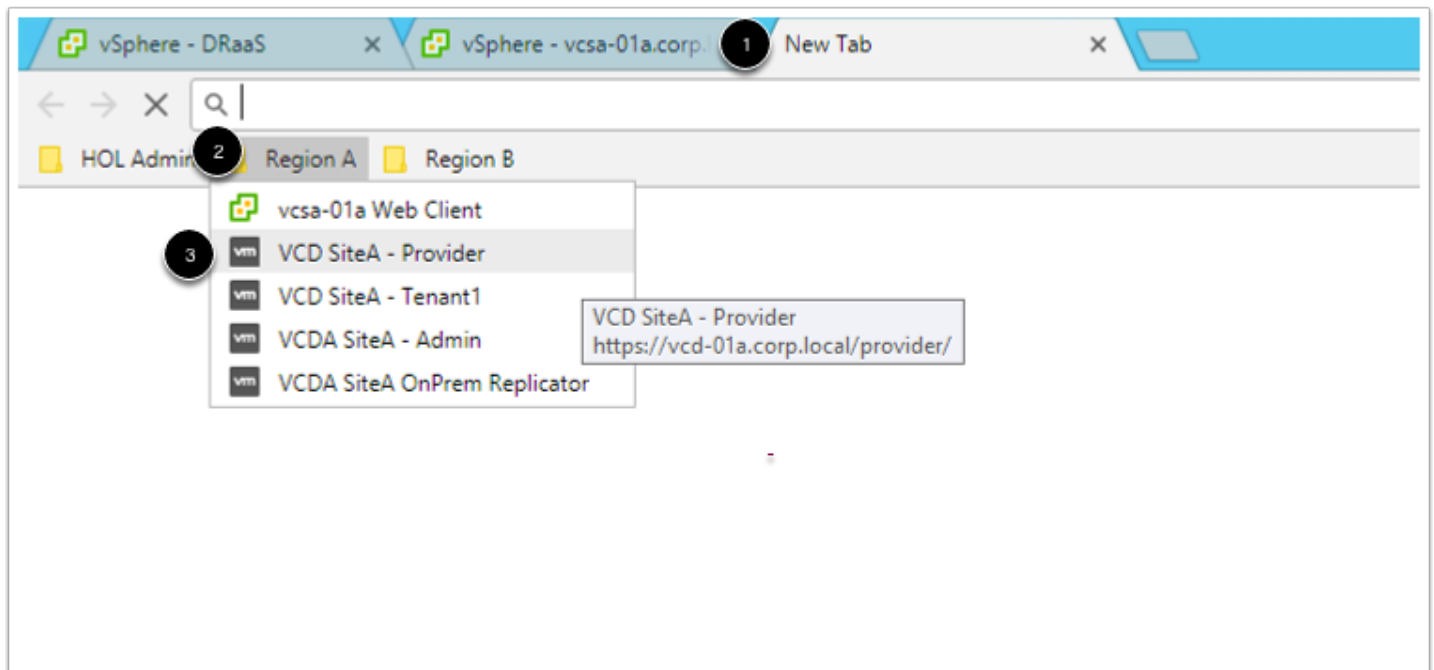
2

☐ Use Windows session authentication

3 LOGIN

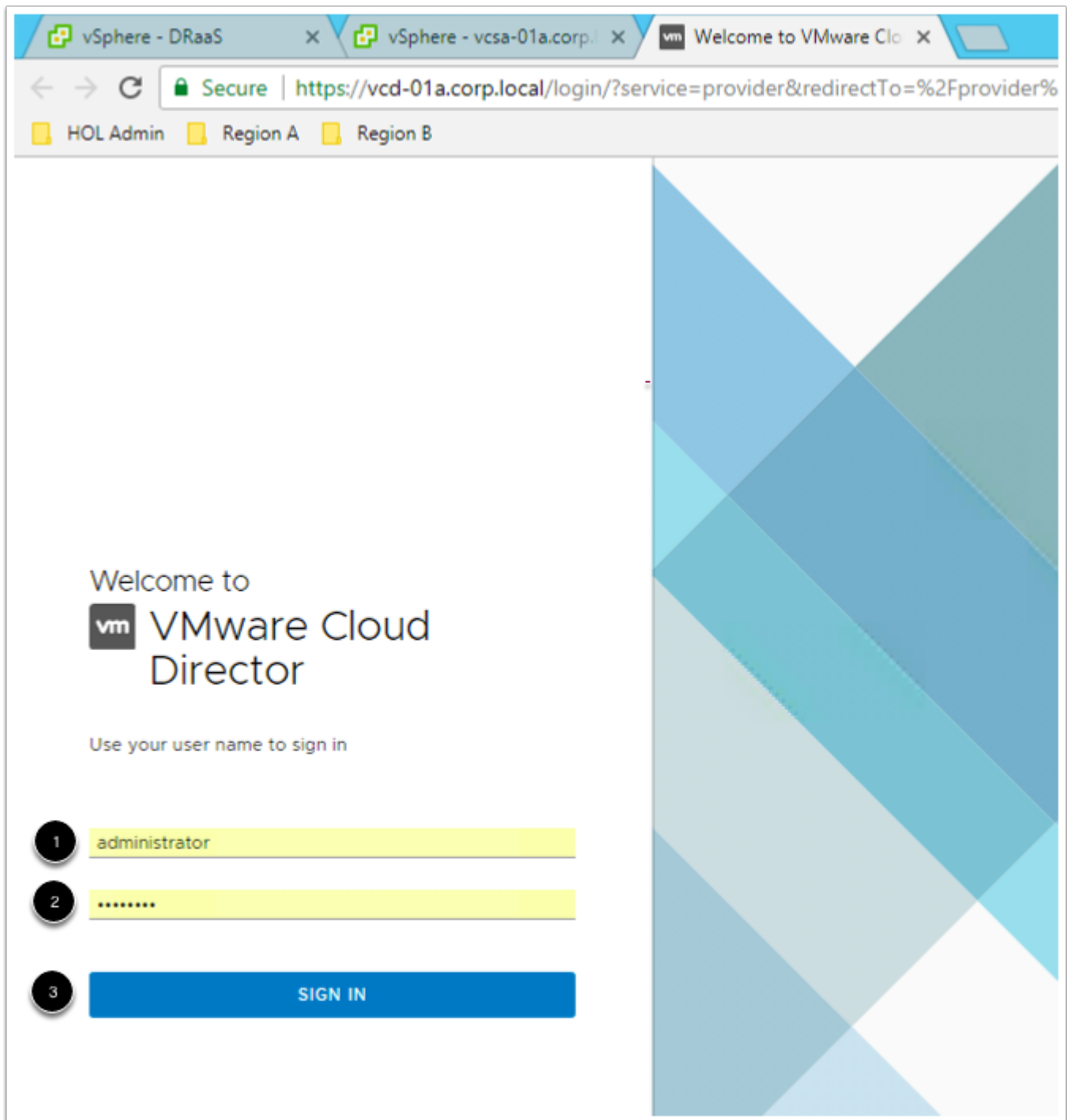
1. Enter Username: **administrator@corp.local**
2. Enter Password: **VMware1!**
3. Click on **LOGIN**

Open SiteA VMware Cloud Director Provider



1. Open a new tab on the browser.
2. Click on **RegionA**
3. Click on VCD SiteA - Provider . Verify the address as :
<https://vcd-01a.corp.local/>

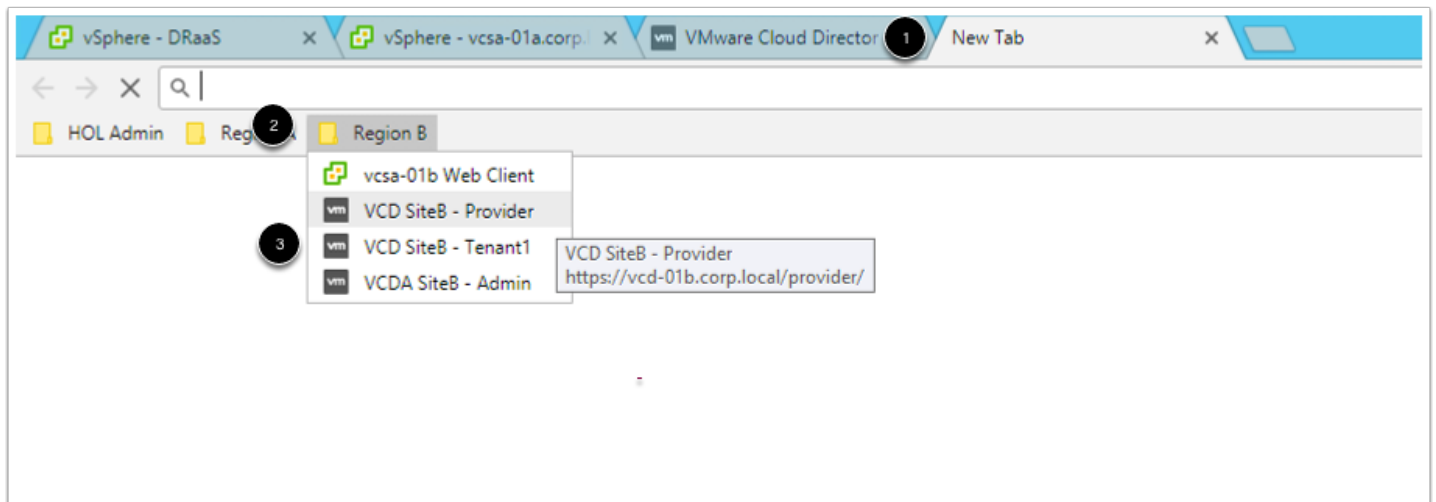
Login to SiteA VMware Cloud Director Provider



The screenshot shows a web browser window with three tabs: 'vSphere - DRaaS', 'vSphere - vcsa-01a.corp.local', and 'Welcome to VMware Cloud Director'. The address bar shows a secure connection to 'https://vcd-01a.corp.local/login/?service=provider&redirectTo=%2Fprovider%'. Below the address bar, there are three tabs: 'HOL Admin', 'Region A', and 'Region B'. The main content area displays the 'Welcome to VMware Cloud Director' message. Below this, it says 'Use your user name to sign in'. There are three numbered steps: 1. Username: 'administrator' (entered in a yellow input field), 2. Password: '*****' (entered in a yellow input field), and 3. Click on 'SIGN IN' (a blue button).

1. Username: **administrator**
2. Password: **VMware1!**
3. Click on **SIGN IN**

Open SiteB VMware Cloud Director Provider



1. Open a new tab on the browser.
2. Click on **RegionB**
3. Click on VCD SiteB - Provider. Verify the address as :
<https://vcd-01b.corp.local/>

Login to SiteB VMware Cloud Director Provider

Browser tabs: vSphere - DRaaS, vSphere - vcsa-01a.corp.local, VMware Cloud Director, Welcome to VMware Cloud Director

Address bar: Secure | <https://vcd-01b.corp.local/login/?service=provider&redirectTo=%2Fprovider%2F>

Navigation: HOL Admin, Region A, Region B

Welcome to
vm VMware Cloud Director

Use your user name to sign in

1 administrator

2

3 SIGN IN

1. Username: **administrator**
2. Password: **VMware1!**
3. Click on **SIGN IN**

Open Tenant1-OVDC-B

The screenshot shows the VMware Cloud Director interface. The top navigation bar includes 'vmware Cloud Director', 'Resources', 'Libraries', 'Administration', 'Monitor', and 'More'. Below this, there are tabs for 'Cloud Resources' and 'vSphere Resources'. The left-hand navigation bar lists 'Organizations', 'Organization VDCs' (highlighted with a red circle and a '1' in a black circle), 'Organization VDC Templates', 'Provider VDCs', 'Cloud Cells', 'Edge Gateways', 'External Networks', and 'Network Pools'. The main window is titled 'Organization VDCs' and shows a table of Organization VDCs. The table has columns for 'Name', 'Status', 'State', and 'A'. The table contains two rows: 'Tenant1-OVDC-A' and 'Tenant1-OVDC-B' (highlighted with a red circle and a '2' in a black circle). Both rows show a status of 'Enabled' and a state of 'A'.

Name	Status	State	A
Tenant1-OVDC-A	Enabled	A	
Tenant1-OVDC-B	Enabled	F	

First, we need to expand the resources in Tenant1-OVDC-B.

1. Click **Organization VDCs** in the left-hand navigation bar
2. Click the **Tenant1-OVDC-B** name in the main window

Note: if you already added resources in the previous module, you can skip ahead to [Open Availability menu at SiteA Provider](#)

Edit Allocation

The screenshot shows the VMware Cloud Director interface. The top navigation bar includes 'vm', 'VMware Cloud Director', 'Resources', 'Libraries', 'Administration', 'Monitor', and 'More'. Below this, the 'Cloud Resources' tab is selected, showing a sidebar with 'Organizations', 'Organization VDCs', 'Organization VDC Templates', 'Provider VDCs', 'Cloud Cells', 'Edge Gateways', 'External Networks', 'Network Pools', and 'VM Sizing Policies'. The main content area shows the path 'All Organization VDCs > Tenant1-OVDC-B'. The 'Tenant1-OVDC-B' header has buttons for 'OPEN IN TENANT PORTAL', 'DISABLE', and 'DELETE'. The 'Allocation' tab is selected in the left sidebar, marked with a red circle and the number '1'. The 'Edit' button is highlighted in the top right of the 'Allocation' section, marked with a red circle and the number '2'. The 'Allocation' section contains a list of settings: 'Allocation Model', 'Elasticity', 'Include VM Memory Overhead', 'CPU', 'CPU allocation used', 'CPU allocation', and 'CPU limit'.

1. Click on **Allocation**
2. Click **Edit**

Edit Allocation (cont'd.)

Edit Allocation

Allocation Model

Flex

Elasticity

☐

Include VM Memory Overhead

☒

CPU allocation

13

GHz ⓘ

CPU limit

☐ 3

GHz ⓘ

☒ Unlimited

CPU resources guaranteed

0

% ⓘ

vCPU speed

1

GHz ⓘ

Memory allocation

1024

MB ⓘ

Memory resources guaranteed

20

% ⓘ

Total Provider VDC Consumption

CPU

Available

0.95 GHz

Allocated

210.08% (2 GHz / 0.95 GHz)

Reserved

0% (0 GHz / 0.95 GHz)

Used

0% (0 GHz / 0.95 GHz)

Memory

Available

2.87 GB

Allocated

32.58% (1 GB / 3.07 GB)

Reserved

6.55% (0.2 GB / 3.07 GB)

Used

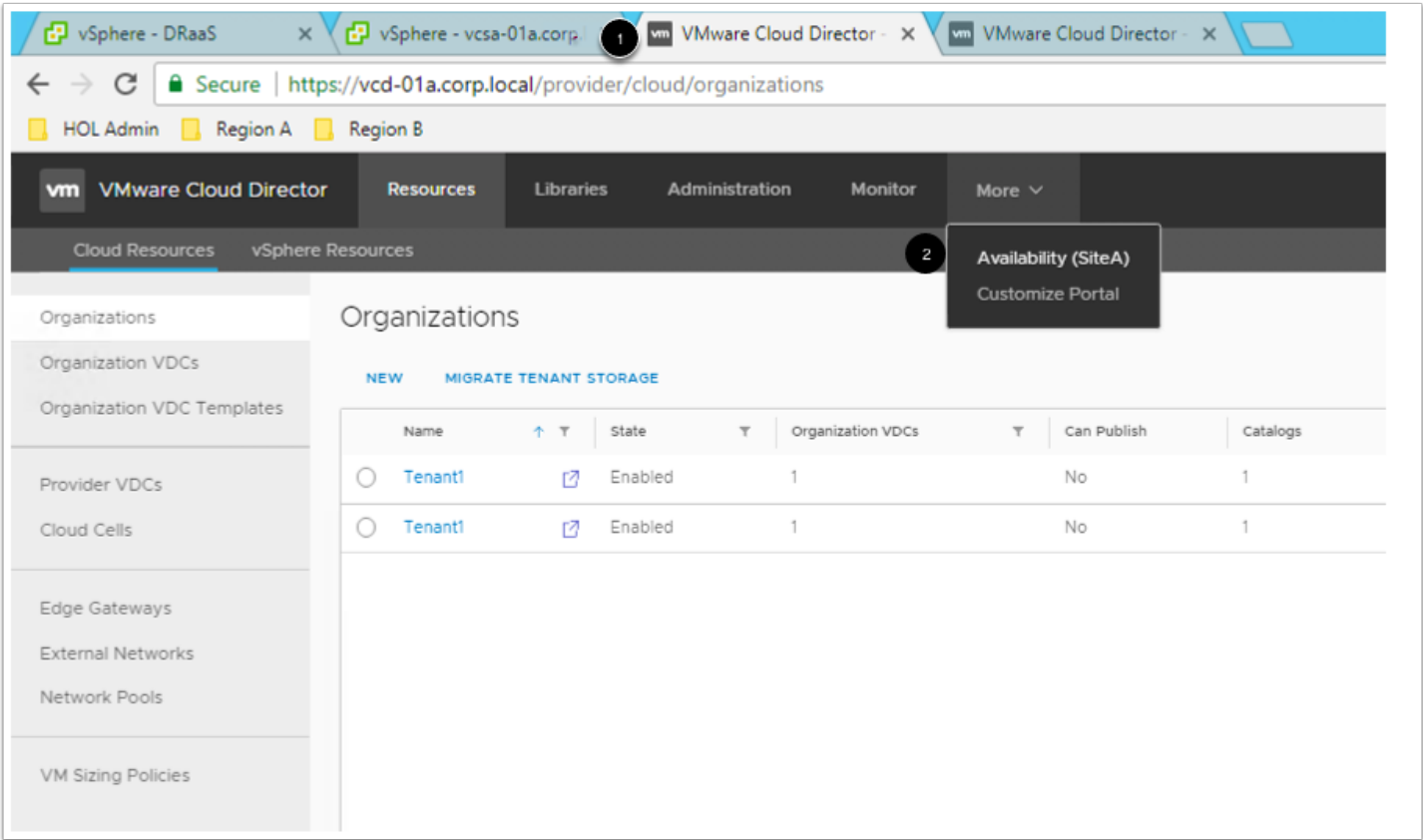
6.52% (0.2 GB / 3.07 GB)

DISCARD

SAVE

1. Change CPU Allocation to 3 GHz
2. Click **Save**

Open Availability menu at SiteA Provider



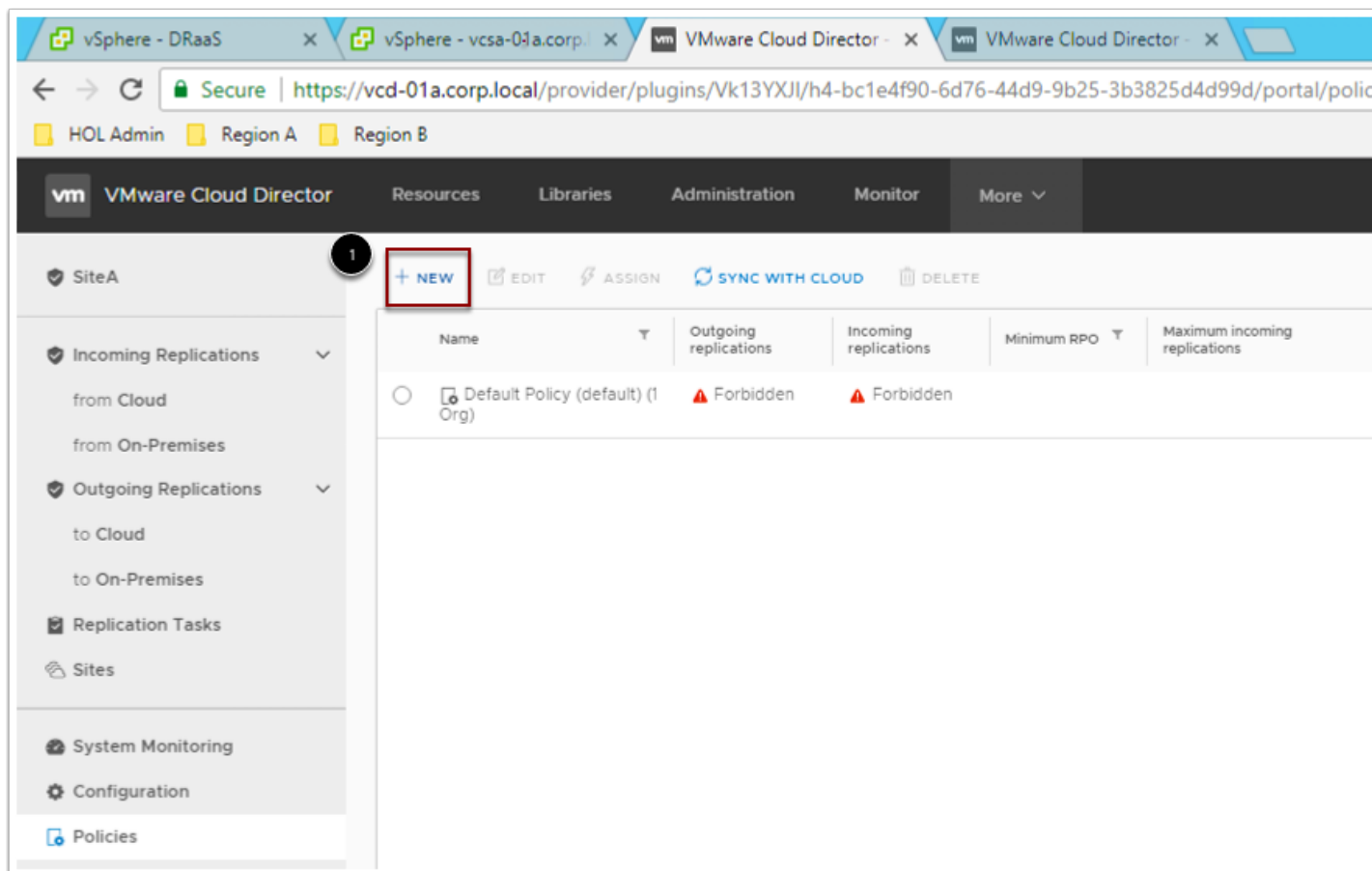
- 1. Switch to tab **Site A Provider**
- 2. Expand More and Click on **Availability (Site A)**

Review Topology and System Health at vCD SiteA

The screenshot displays the VMware Cloud Director web interface for SiteA. The browser address bar shows the URL: <https://vcd-01a.corp.local/provider/plugins/Vk13YXJl/h4-bc1e4f90-6d76-44d9-9b25-3b3825d4d99d/portal/>. The interface includes a top navigation bar with tabs for vSphere - DRaaS, vSphere - vcsa-01a.corp.local, and VMware Cloud Director. The main content area is divided into three sections: 'Topology' (highlighted with a red box and callout 1), 'System health' (callout 2), and 'On-Premises VM replication status' (callout 3). The 'Topology' section shows a diagram with '0 On-Premises sites' and '0 Cloud sites' connected by bidirectional arrows. The 'System health' section shows two green checkmarks indicating 'Cloud Service Tunnel is enabled Online' and 'Lookup Service vcsa-01a.corp.local Online'. The 'On-Premises VM replication status' section shows 'Incoming VMs' with a count of 0 and 'No replications'. The left sidebar contains navigation options: Incoming Replications, Outgoing Replications, Replication Tasks, Sites, System Monitoring, Configuration, Policies (highlighted with callout 3), and SLA Profiles.

1. **Topology:** There are no sites paired and no Replications
2. **System health:** Confirm there are green check marks and everything is healthy and green
3. From the left panel, click **Policies**

Add a new Replication Policy



Replication policies are sets of rules that define and control the replication attributes on a VMware Cloud Director organization level. To control the replication settings allowed for replications on a VMware Cloud Director organization level, the service providers can create replication policies.

When configuring a protection or a migration, the New Replication wizard validates the replication attributes of the policy that is assigned to the organization. Lets add a new policy at SiteA Provider that will be validated while configuring replication.

1. Click on **+ NEW** to add a new Policy

Add a new Policy

New Policy

Policy name: * **1** T1-PolicyA

☒ Allow custom SLA settings

☒ Allow outgoing replications

☒ Allow incoming replications

2 Maximum number of vm replications: * ☐ Unlimited ☒ 10

Max point-in-time instances per replication: ⓘ * 24

Max stored instances per replication: ⓘ * 24

☐ Enable bandwidth throttling

Max throughput per On-Premises Replicator Appliance: * 512
(1 - 10000 mbit/s)

Minimum allowed RPO:

5 min | 30 min | 2 hours | 8 hours | 24 hours

5m

3

Just brief overview for each parameter in this wizard-

- Enter a unique, case-sensitive name for the replication policy.
- Select whether to allow custom SLA settings per replication or only to allow SLA profiles to set the SLA settings.
- Select whether to allow incoming and outgoing replications.
- If incoming replications are enabled, enter the maximum number of virtual machines replications.
- If incoming replications are enabled, enter the maximum number of point-in-time instances per replication.

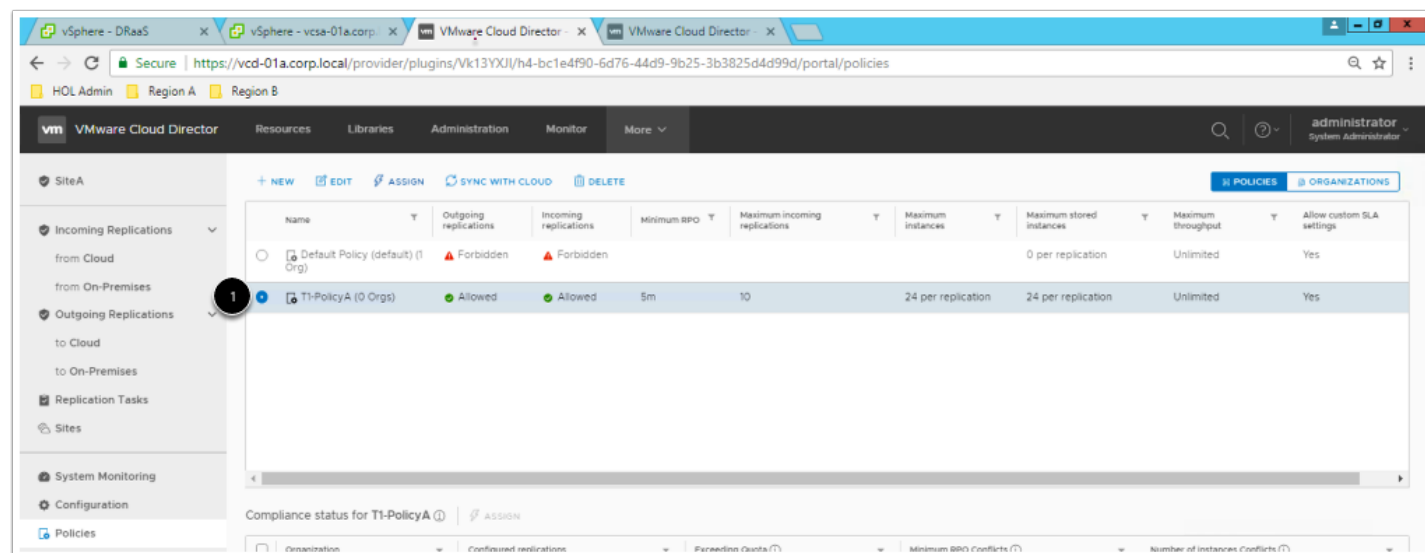
-If incoming replications are enabled, enter the maximum number of stored instances per replication.

-Select whether to allow bandwidth throttling and if enabled enter the maximum throughput per VMware Cloud Director Availability On-Premises Appliance.

-If incoming replications are enabled, set the minimum allowed RPO by using the Recovery Point Objective (RPO) slider or by clicking the time ranges.

1. Enter Policy name: **T1-PolicyA**
2. Leave everything as default
3. Click on **CREATE**

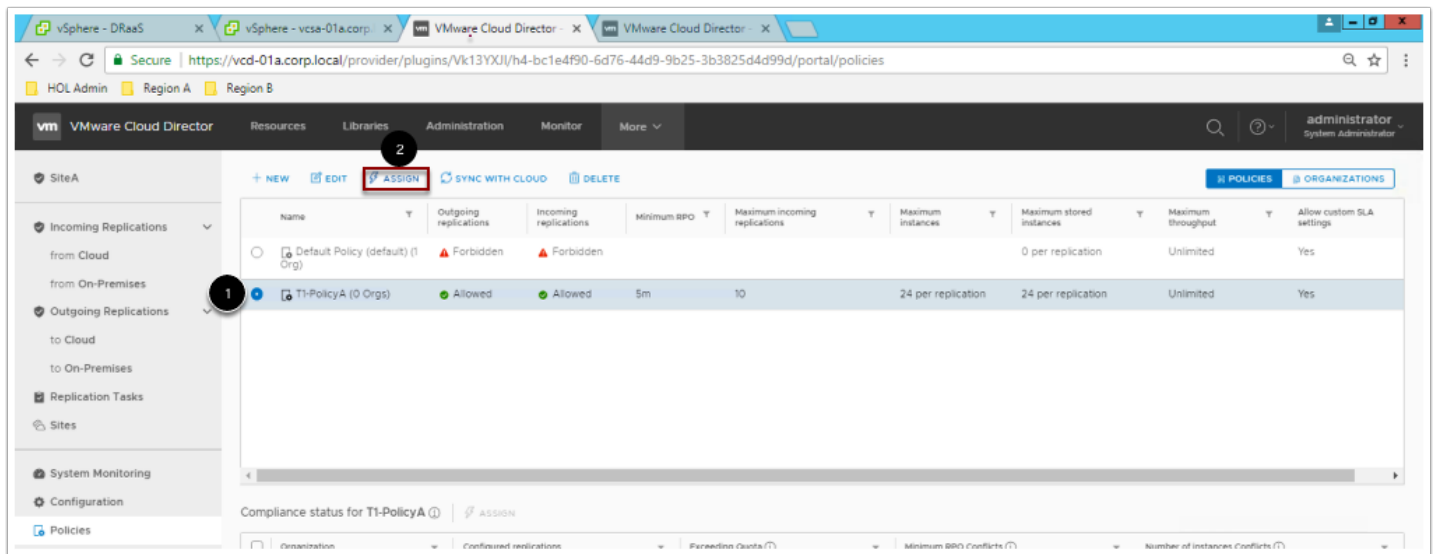
Confirm the Policy is created



Name	Outgoing replications	Incoming replications	Minimum RPO	Maximum incoming replications	Maximum instances	Maximum stored instances	Maximum throughput	Allow custom SLA settings
Default Policy (default) (1 Org)	Forbidden	Forbidden				0 per replication	Unlimited	Yes
T1-PolicyA (0 Orgs)	Allowed	Allowed	5m	10	24 per replication	24 per replication	Unlimited	Yes

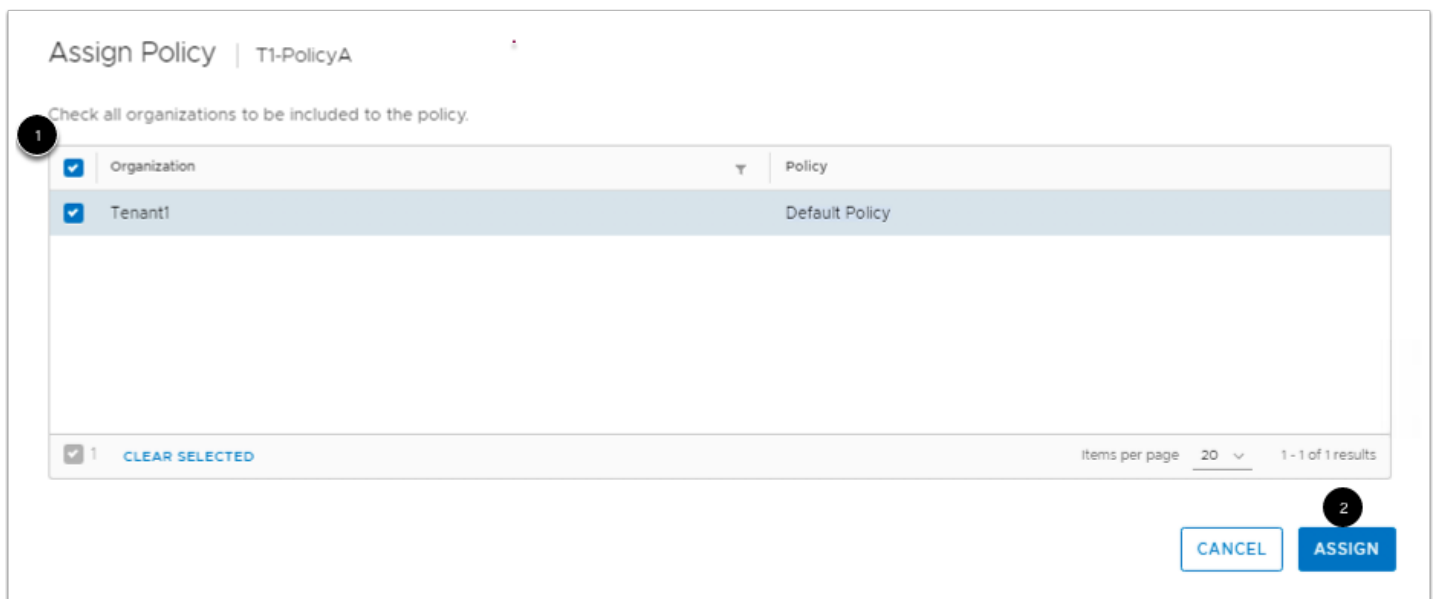
1. Confirm policy **T1-PolicyA** is created successfully

Assign the Policy



1. Click on **T1-PolicyA**
2. Click on **ASSIGN**

Assign the Policy (contd..)



1. Check the checkbox **Tenant1**
2. Click on **ASSIGN**

Confirm the Policy is assigned to Org

The screenshot shows the VMware Cloud Director interface. The left sidebar has a 'Policies' link highlighted. The main area displays a table of policies. The 'T1-PolicyA (1 Org)' policy is selected, and a callout '1' points to the '1 Org' indicator. Below the table, the 'Compliance status for T1-PolicyA' section shows a table with columns for Organization, Configured replications, Exceeding Quota, Minimum RPO Conflicts, and Number of instances Conflicts. The 'Tenant1' row shows 0 for all metrics.

Name	Outgoing replications	Incoming replications	Minimum RPO	Maximum incoming replications	Maximum instances	Maximum stored instances	Maximum throughput	Allow custom SLA settings
Default Policy (default) (0 Orgs)	Forbidden	Forbidden				0 per replication	Unlimited	Yes
T1-PolicyA (1 Org)	Allowed	Allowed	5m	10	24 per replication	24 per replication	Unlimited	Yes

Organization	Configured replications	Exceeding Quota	Minimum RPO Conflicts	Number of instances Conflicts
Tenant1	0	0	0	0

1. Confirm T1-PolicyA is now assigned to 1 Org

Switch to SiteB Cloud Provider tab

The screenshot shows the VMware Cloud Director interface. The left sidebar has a 'Cloud Resources' link highlighted. The main area displays the 'Organizations' page. A callout '1' points to the 'SiteB Provider' tab. A callout '2' points to the 'More' dropdown menu. A callout '3' points to the 'Availability (SiteB)' option in the dropdown menu.

Name	State	Organization VDCs	Can Publish	Catalogs	vApps	Running VMs	Users	Site
Tenant1	Enabled	1	No	1	2	1	1	192.168.210.40
Tenant1	Enabled	1	No	1	1	1	1	192.168.110.40

1. Switch to tab **SiteB Provider**
2. Expand **More**
3. Click on **Availability (SiteB)**

Verify/Create Replication Policy for SiteB

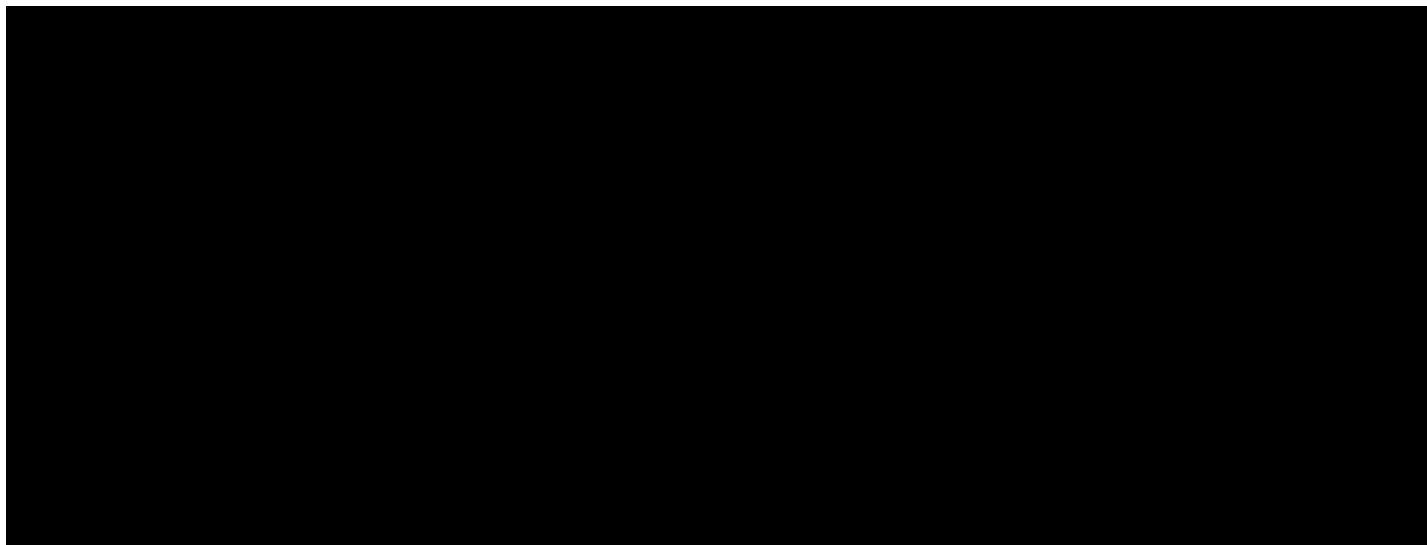
The screenshot shows the VMware Cloud Director interface for SiteB. The left sidebar contains a navigation menu with the following items: SiteB (selected), Incoming Replications (with a dropdown arrow), from Cloud, from On-Premises, Outgoing Replications (with a dropdown arrow), to Cloud, to On-Premises, Replication Tasks, Sites, System Monitoring, Configuration, Policies (highlighted in blue), and SLA Profiles. The main content area has a top bar with buttons: + NEW, EDIT, ASSIGN, SYNC WITH CLOUD, and DELETE. Below this is a table of replication policies.

Name	Outgoing replications	Incoming replications	Minimum RPO
☐ Default Policy (default) (0 Orgs)	Forbidden	Forbidden	
☐ T1-Policy (1 Org)	Allowed	Allowed	5m

If you went through Module 2 before this module, you should already have a replication policy created and assigned. You can go to the next page.

If you do NOT already have a replication policy created and assigned, please use the steps you just completed for SiteA to create and assign a replication policy for SiteB.

Copy Public API Endpoint from SiteA Cloud Provider



Before we pair the 2 sites, we need the Public API Endpoint from SiteA

1. Switch to SiteA Cloud Provider tab
2. From left hand panel, click on **Sites**
3. Copy Public API Endpoint: **https://vcda-01a.corp.local:8048/**

Configure New Pairing between Cloud Provider Sites

Cloud site	Service Endpoint	Management Session	Traffic	Incoming VMs	Outgoing VMs	Api Version	Description
SiteB (Local site)	https://vcda-01b.corp.local:8048/	✓	✓	0	0	4	

1. Switch back to **SiteB Cloud Provider**
2. Click on **Sites**
3. Click on **NEW PAIRING**

Enter New Pairing details

New Pairing

Enter name, description and connection details for the cloud site.

Site name ⓘ * 1 SiteA

Service Endpoint ⓘ * 2 <https://vcda-01a.corp.local:8048/>

Description

3

CANCEL PAIR

1. Enter Site name : **SiteA**
2. **Service Endpoint** - Paste the Public API Endpoint url we copied from Site A cloud provider: <https://vcda-01a.corp.local:8048/>
3. Click on **PAIR**

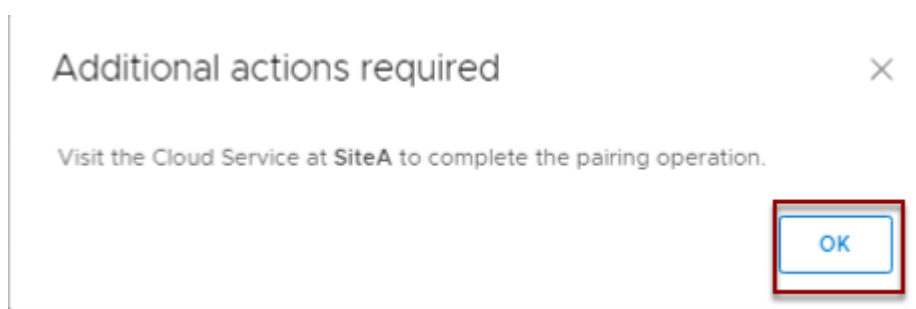
Note: the Site Name is case sensitive and must match the site name at the site being paired.

Accept the Server Certificate



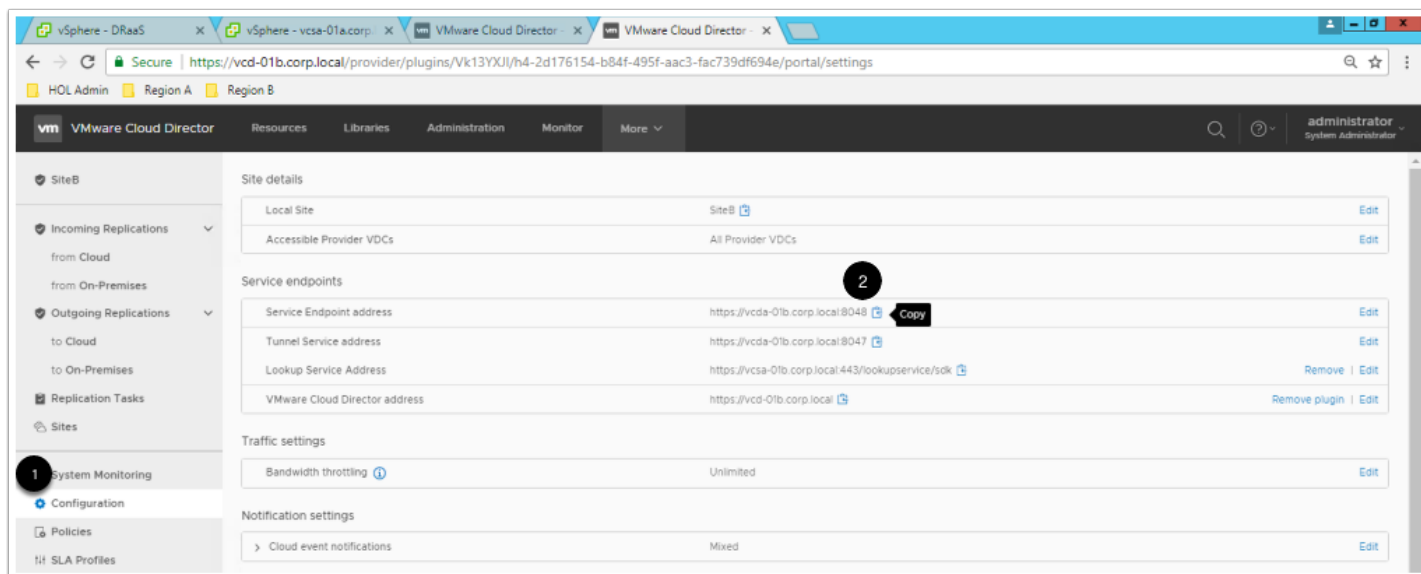
1. Click on **ACCEPT** to accept the SSL certificate from the paired site and you should be able to successfully pair the sites

Additional Action is Required to Complete the Pairing Between 2 Cloud Provider Sites



To complete the pairing between 2 cloud provider sites, additional action is required. Click on OK

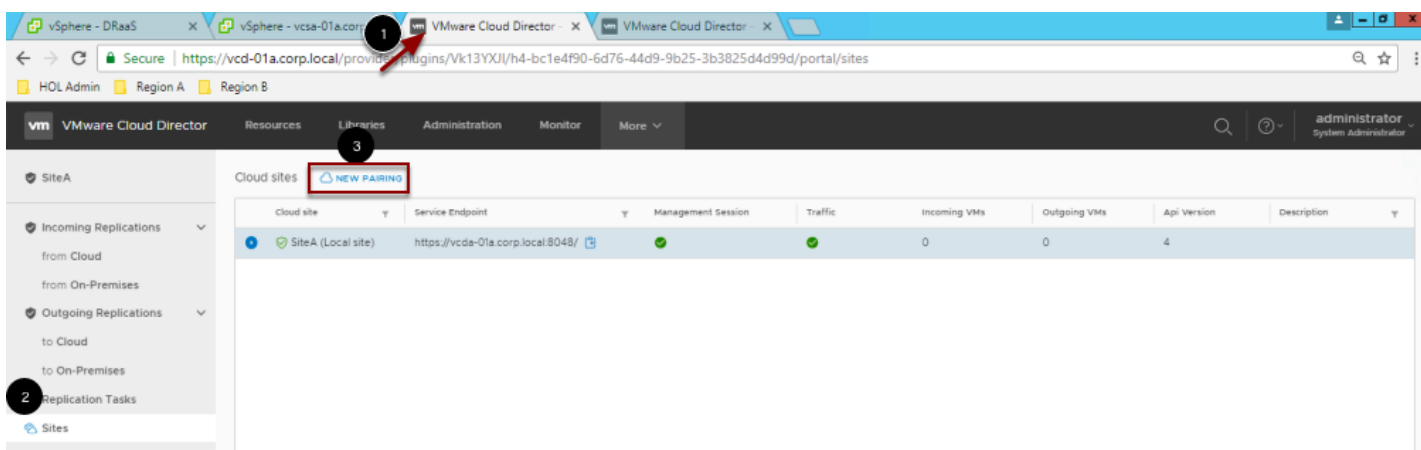
Copy Public API Endpoint from SiteB Cloud Provider



Before we complete pairing the 2 cloud sites, we need the Public API Endpoint from SiteB as well

1. Click on **Configuration** from left-hand navigation bar
2. Copy the Service Endpoint address using the icon
https://vcda-01b.corp.local:8048/

Switch to SiteA Cloud Provider



1. Switch to tab **SiteA Cloud Provider**.
2. Click on **Sites**
3. Click on **NEW PAIRING**

Enter New Pairing details

The screenshot shows a 'New Pairing' form with the following fields and elements:

- Title:** New Pairing
- Instruction:** Enter name, description and connection details for the cloud site.
- Site name:** A text input field containing 'SiteB'. A blue information icon and a red asterisk are to its left. A black circle with the number '1' is above the field.
- Service Endpoint:** A text input field containing 'https://vcda-01b.corp.local:8048'. A blue information icon and a red asterisk are to its left. A black circle with the number '2' is above the field.
- Description:** A large, empty text area.
- Buttons:** 'CANCEL' (blue outline) and 'PAIR' (green solid) buttons are at the bottom right. A black circle with the number '3' is above the 'PAIR' button.

1. Enter Site name : **SiteB**
2. **Service Endpoint** - Paste the Public API Endpoint url we copied from Site B cloud provider: <https://vcda-01b.corp.local:8048/>
3. Click on **PAIR**

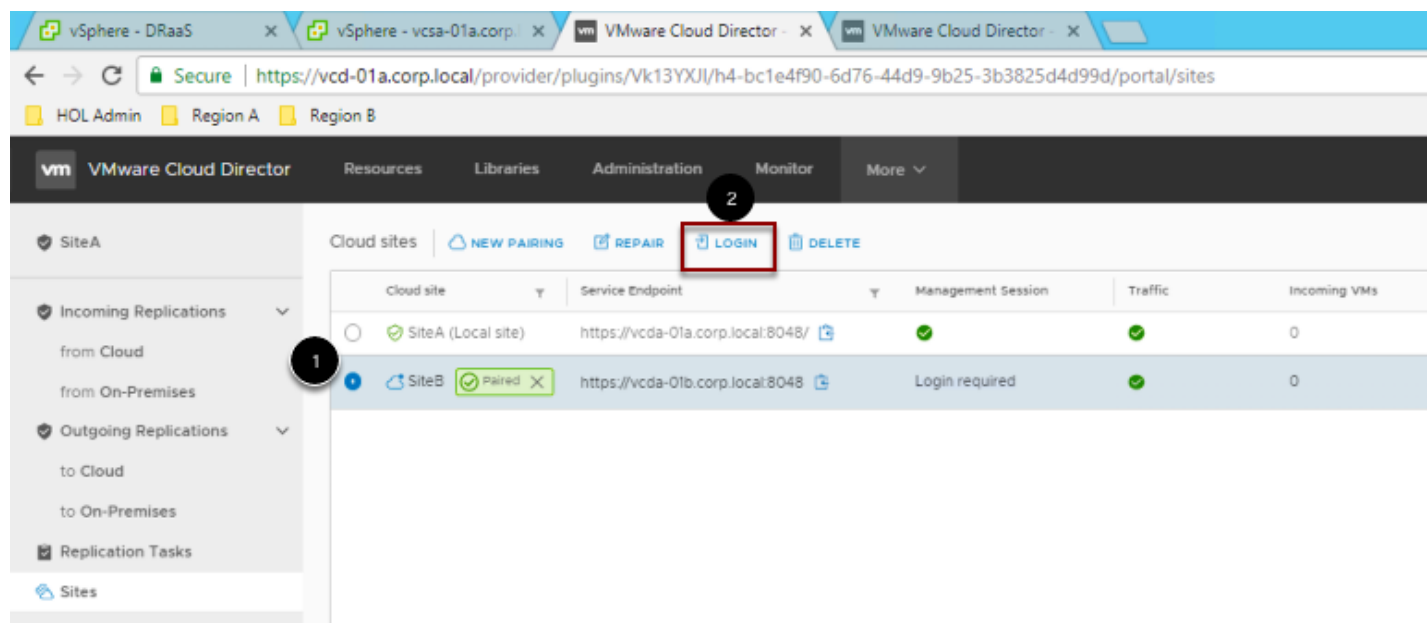
Note: the Site Name is case sensitive and must match the site name at the site being paired.

Accept the Server Certificate



1. Click on **ACCEPT** to accept the SSL certificate from the paired site and you should be able to successfully pair the sites

Login to SiteB to complete the pairing



Once the pairing is completed, a login button appears allowing us to authenticate as our vCloud Director provider admin user (administrator@system) to the 2nd site. After successful authentication the 2 cloud provider sites should be paired and ready to run failover workflows.

1. Select **SiteB**
2. Click on **LOGIN**

Enter Login Credentials for SiteB

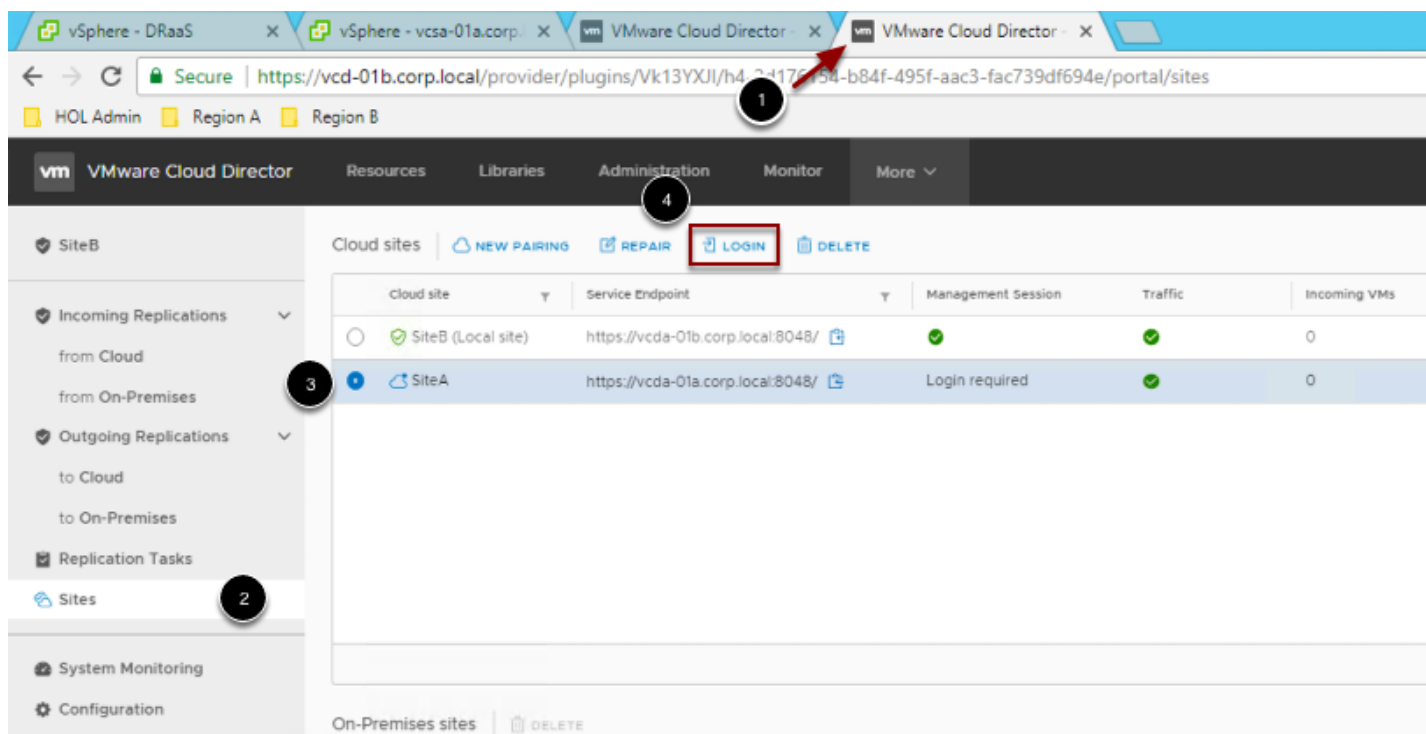
1. Enter Username: **administrator@system**
2. Enter Password: **VMware1!**
3. Click **LOGIN**

Confirm on vCD SiteA that the Pairing is complete

Cloud site	Service Endpoint	Management Session	Traffic	Incoming VMs	Outgoing VMs	Api Version	Description
SiteA (Local site)	https://vcda-01a.corp.local:8048/	✓	✓	0	0	4	
SiteB	https://vcda-01b.corp.local:8048	✓	✓	0	0	4	

Confirm that the pairing to SiteB is **Green** and **Healthy**

Verify the Pairing at vCD SiteB



Before we confirm the pairing between the sites, we need to login to SiteA

1. Switch to tab **SiteB Cloud Provider**
2. Select **Sites** in the left-hand navigation bar
3. Select the Cloud site **SiteA**
4. Click on **LOGIN**

Enter Login Credentials for SiteA

Log In | SiteA
×

Provide credentials to manage replications on SiteA.

1 Username

2 Password

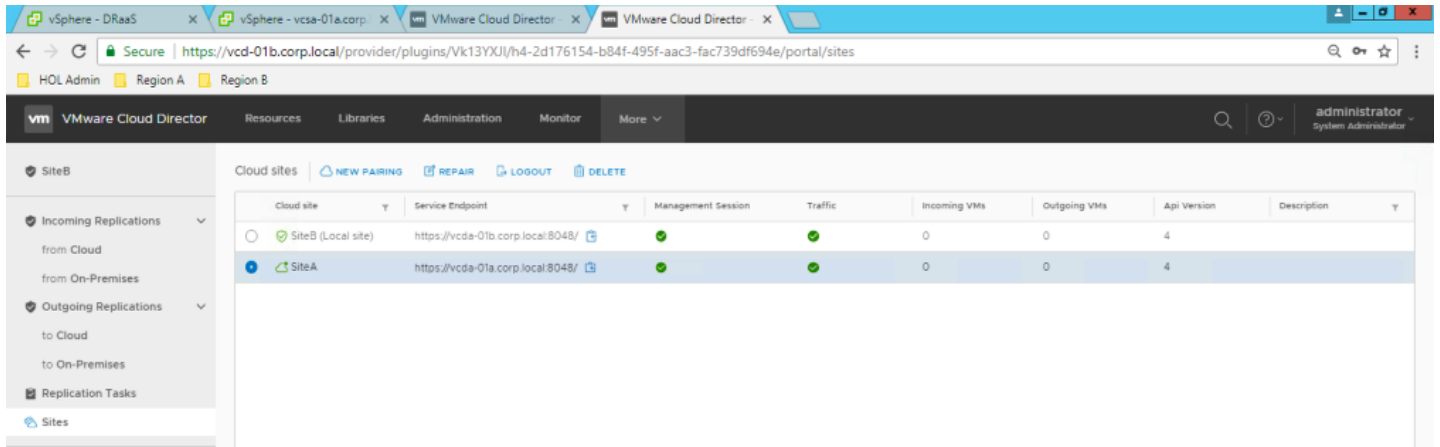
3

CANCEL
LOGIN

1. Enter Username: **administrator@system**
2. Enter Password: **VMware1!**

3. Click on **LOGIN**

Confirm the Pairing from SiteB to SiteA is successful

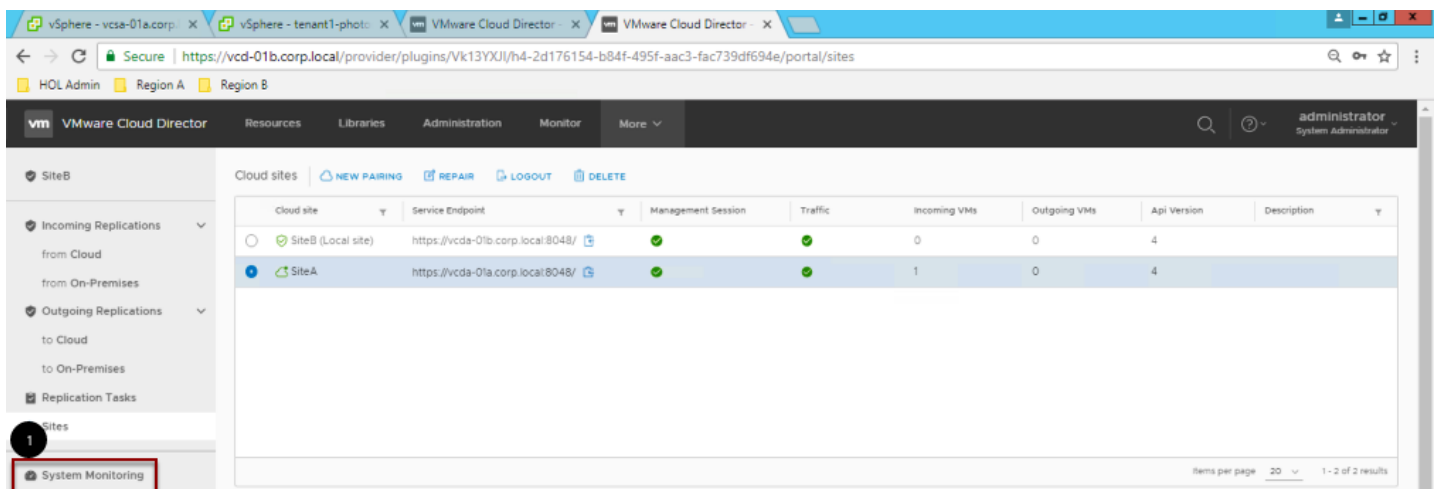


The screenshot shows the VMware Cloud Director interface. The left sidebar has a 'Sites' link. The main area displays a table of Cloud sites. The table has columns: Cloud site, Service Endpoint, Management Session, Traffic, Incoming VMs, Outgoing VMs, Api Version, and Description. Two sites are listed: SiteB (Local site) and SiteA. SiteA is highlighted in blue, indicating it is the selected site. The Management Session and Traffic columns for SiteA show green checkmarks, indicating a successful pairing.

Cloud site	Service Endpoint	Management Session	Traffic	Incoming VMs	Outgoing VMs	Api Version	Description
SiteB (Local site)	https://vcda-01b.corp.local:8048/	✓	✓	0	0	4	
SiteA	https://vcda-01a.corp.local:8048/	✓	✓	0	0	4	

Confirm that the pairing to SiteA is **Green** and **Healthy**

System Monitoring at SiteB Cloud Provider



The screenshot shows the VMware Cloud Director interface. The left sidebar has a 'System Monitoring' link highlighted with a red box. The main area displays a table of Cloud sites. The table has columns: Cloud site, Service Endpoint, Management Session, Traffic, Incoming VMs, Outgoing VMs, Api Version, and Description. Two sites are listed: SiteB (Local site) and SiteA. SiteA is highlighted in blue, indicating it is the selected site. The Management Session and Traffic columns for SiteA show green checkmarks, indicating a successful pairing.

Cloud site	Service Endpoint	Management Session	Traffic	Incoming VMs	Outgoing VMs	Api Version	Description
SiteB (Local site)	https://vcda-01b.corp.local:8048/	✓	✓	0	0	4	
SiteA	https://vcda-01a.corp.local:8048/	✓	✓	1	0	4	

1. Click on **System Monitoring**

View Local and Remote Replicators at Cloud SiteB

The screenshot shows the VMware Cloud Director web interface. The left sidebar contains navigation links for Sites, Incoming Replications, Outgoing Replications, Replication Tasks, System Monitoring, Configuration, Policies, SLA Profiles, Datastores, System Tasks, OpenAPI Client, Reports, Resources, Support, and About. The main content area is titled 'System health' and includes a 'Service status' table and a 'Manager Service status' table. The 'Service status' table lists various services and their status (OK). The 'Manager Service status' table lists the manager service and its status (OK). Below these tables, there are sections for 'Local Replicator Services (1)' and 'Remote Replicator Services (2)'. The 'Remote Replicator Services (2)' section is highlighted with a red box, showing details for a remote replicator service.

Service status	
Traffic	OK
Address	192.168.210.90
Instance ID	20170154-b84f-495f-aac3-fac739df694e
Server time	7/7/20, 11:45 PM GMT-7
Lookup Service connectivity	OK
Database connectivity	OK
VMware Cloud Director connectivity	OK
Tunnel Service connectivity	OK
NTP connectivity	OK

Manager Service status	
Service connectivity	OK
Address	https://192.168.210.90:8044
Instance ID	1ab8f545-c09c-4123-bf1c-a48ecd7dd2
Server time	7/7/20, 11:45 PM GMT-7
Lookup Service connectivity	OK
Replicators lookup service configuration	OK
Database connectivity	OK

1 Local Replicator Services (1)

Local Replicator Services (1)	
Service connectivity (192.168.210.90)	OK

2 Remote Replicator Services (2)

Remote Replicator Services (2)	
Service connectivity (vSphere-OnPrem)	OK
Address	https://192.168.210.90:8044
Instance ID	ea5f8fb-cf4e-41c9-8721-c007243078e8
Maintenance mode	No
Site	vSphere-OnPrem

Scroll down to the bottom of the page to view Local and Remote Replicator details.

1. Here, you should see that both the **Local** (to the site you are logged into) and **Remote** Replicators are shown and connected
2. The odd Address shown for the Remote replicator (boxed in red above) is correct since this is an internal address used to reach the remote replicator appliance via the Tunnel.

System Monitoring at Cloud SiteA

The screenshot shows the VMware Cloud Director web interface. The browser tabs include 'vSphere - vcsa-01a.corp', 'vSphere - tenant1-photo', and two 'VMware Cloud Director' tabs. The address bar shows the URL: <https://vcd-01a.corp.local/provider/plugins/Vk13YXJl/h4-bc1e4f90-6d76-44d9-9b25-3b3825d4d99d/portal/sites>. The navigation bar includes 'HOL Admin', 'Region A', and 'Region B'. The main navigation menu has 'vm VMware Cloud Director', 'Resources', 'Libraries', 'Administration', 'Monitor', and 'More'. The left sidebar shows 'SiteA' selected, with sub-items: 'Incoming Replications' (from Cloud, from On-Premises), 'Outgoing Replications' (to Cloud, to On-Premises), 'Replication Tasks', 'Sites', and 'System Monitoring' (highlighted with a red box and a black circle with the number 2). The main content area shows 'Cloud sites' with a table of two sites: SiteA (Local site) and SiteB. SiteA is highlighted with a blue row. A black circle with the number 1 points to the 'VMware Cloud Director' tab in the browser.

Cloud site	Service Endpoint	Management Session	Traffic	Incoming VMs
SiteA (Local site)	https://vcd-01a.corp.local:8048/	✓	✓	0
SiteB	https://vcd-01b.corp.local:8048	✓	✓	0

Similar to Cloud SiteB, we will now review the local and remote replicators configured at Cloud SiteA

1. Switch back to tab **SiteA Cloud Provider**
2. Click on **System Monitoring**

View Local and Remote Replicators at Cloud SiteA

The screenshot shows the VMware Cloud Director interface for SiteA. The left sidebar contains navigation options: Incoming Replications, Outgoing Replications, Replication Tasks, Sites, System Monitoring, Configuration, Policies, SLA Profiles, Datastores, System Tasks, OpenAPI Client, Reports, Resources, Support, and About. The main content area displays the following tables:

Service status	
Traffic	OK
Address	192.168.110.90
Instance ID	bc1e4f90-6d76-44d9-9b25-3b3825d4d99d
Server time	7/7/20, 11:53 PM GMT-7
Lookup Service connectivity	OK https://vcsa-01a.corp.local
Database connectivity	OK
VMware Cloud Director connectivity	OK
Tunnel Service connectivity	OK https://vcsa-01a.corp.local
NTP connectivity	OK

Manager Service status	
Service connectivity	OK
Address	https://192.168.110.90:8044
Instance ID	8d04ba75-fe16-46bd-ab41-c4863bd8dabc
Server time	7/7/20, 11:53 PM GMT-7
Lookup Service connectivity	OK
Replicators lookup service configuration	OK
Database connectivity	OK

Local Replicator Services (1)

Service connectivity (192.168.110.90)	OK
---------------------------------------	----

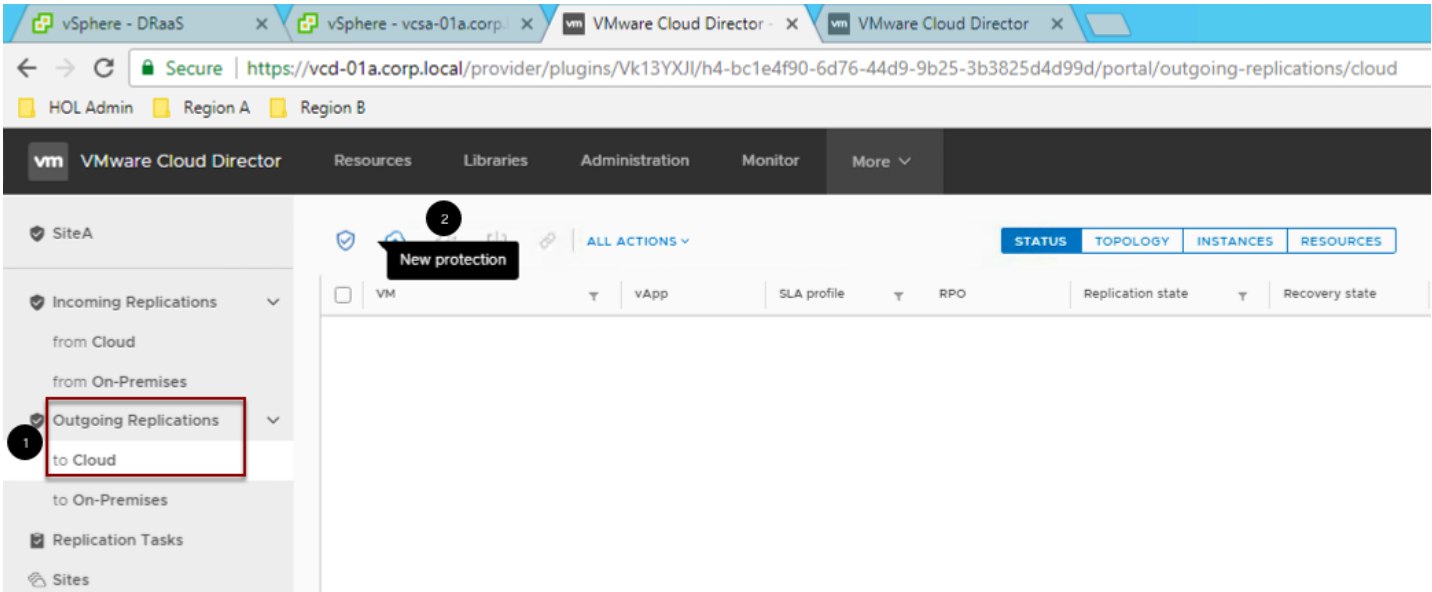
Remote Replicator Services (1)

Service connectivity (SiteB)	OK
Address	https://192.168.110.90:8044
Instance ID	a37c7b26-75e3-40f6-ab6c-39c826e53ba2
Maintenance mode	NO
Site	SiteB

Scroll down to the bottom to the bottom of the page to view Local and Remote Replicator Services details.

1. Here, you should see that both the **Local** (to the site you are logged in to) and **Remote** Replicators are shown and connected
2. The odd Address shown for the Remote replicator (boxed in red above) is correct this is an internal address used to reach the remote replicator appliance via the Tunnel.

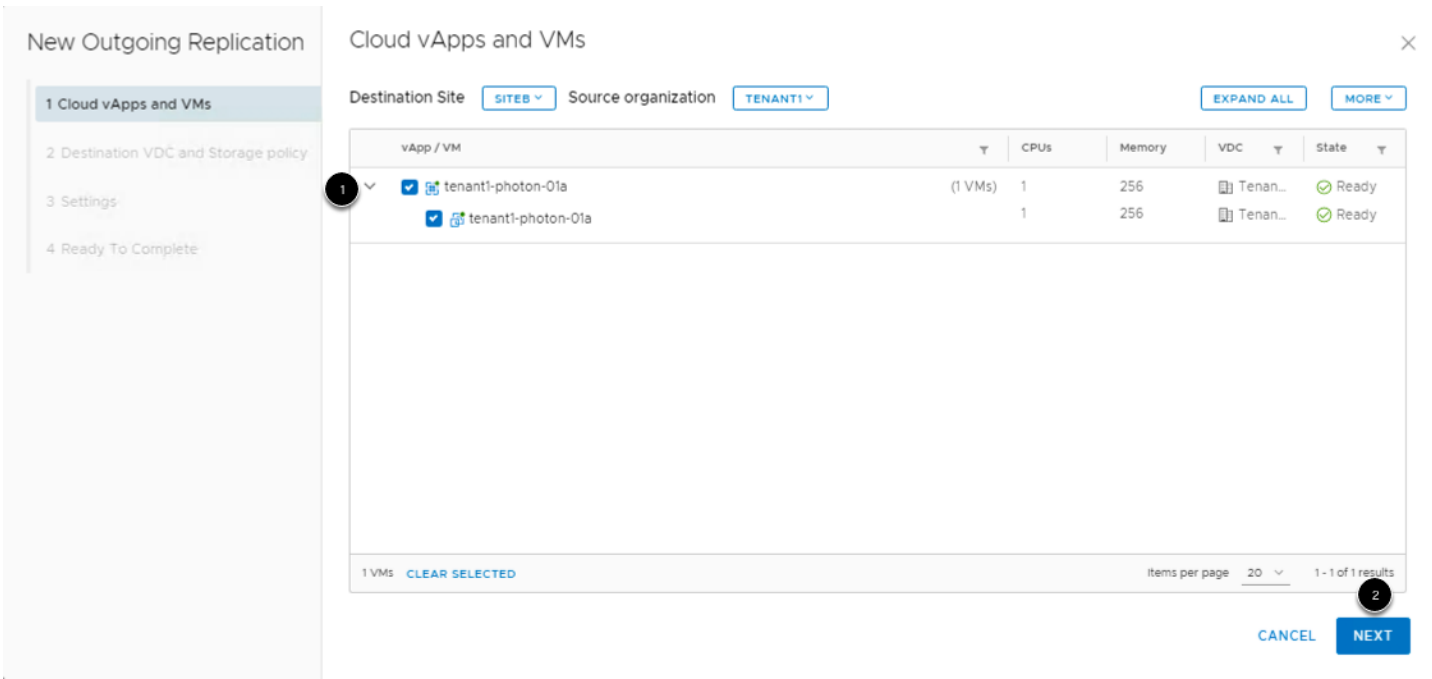
Configure Replication from Cloud to Cloud



We will now configure replication from Cloud Provider SiteA to Cloud Provider SiteB

1. Scroll to the top of the page. From left panel, Click on **Outgoing Replications to Cloud**
2. Click on **icon for New Protection**

New Outgoing Replication - Cloud vApps and VMs



- 1. Check the checkbox for VM **tenant1-photon-01a**
- 2. Click on **NEXT**

New Outgoing Replication - Destination VDC and Storage policy

New Outgoing Replication

1 Cloud vApps and VMs

2 Destination VDC and Storage policy

3 Settings

4 Ready To Complete

Destination VDC and Storage policy

Select a virtual data center from SiteB to be used as replication target:

REFRESH

Name	Used CPU	Used memory	Used storage	VMs	Quota	Ongoing replications
Tenant1-OVD...	0 M	256.00 MB	1.29 GB	1	100	1

items per page 20 1 - 1 of 1 results

Storage policy

Select the new storage policy placement for the recovered VMs

Name	Used	Limit
Any	1.29 GB	10.00 GB

items per page 20 1 - 1 of 1 results

CANCEL

BACK

NEXT

- 1. Review the defaults and Click on **NEXT**

New Outgoing Replication - Configure Settings

New Outgoing Replication

- 1 Cloud vApps and VMs
- 2 Destination VDC and Storage policy
- 3 Settings**
- 4 Ready To Complete

Settings

SLA profile
☐ SLA profiles are not available for 'Tenant!'

Target recovery point objective (RPO)
 5 min | 30 min | 2 hours | 8 hours | 24 hours | 24h

Retention policy for point in time instances
☐ Preserve 4 instances spread evenly over the last 4 days

Enable quiesce
☐ Enabling quiescing will ensure application level consistency before creating an instance.

Compress replication traffic
☒ Enabling compression will reduce network traffic at the expense of CPU.

Delay start synchronization
☐ Set time that is convenient for the first synchronization.

Exclude disks
☐ Save disk space on the target site by excluding disks that are not necessary.

Configure Seed VMs
☐ Use an older copy of the protected VMs on the target site to reduce the data traffic.

CANCEL BACK NEXT

Here's brief overview of the parameters -

SLA Profile - The premise of a SLA Profile is to provide a grouping of target settings when protecting a workload. This minimizes the amount of time spent configuring for protection. Think of this as a logical grouping construct which is a single selection to protect a workload. One does not need to think about what settings to configure. A SLA Profile consists of the following:

1. Target Recovery Point Objective (target being the key word here)
2. Retention Policy for Point in Time Instances
3. Ability to Quiesce or Compress Replication Traffic
4. Time select of the synchronization.

Just select SLA profile, and done. You can either use default or custom created SLA profile. SLA profiles are optional and only pertain to protections. They are not utilized for migrations at this time.

Target recovery point objective (RPO) -The RPO is the longest tolerable timeframe of data loss. For example, with one hour RPO the recovered virtual machine can have no more than one hour of data lost. Shorter RPO intervals, ensure less data loss during recovery, at the expense of consuming more network bandwidth to keep the replica up to date.

Retention Policy- Maximum number of retained snapshots per single virtual machine replication within an organization.

Delay start synchronization

- To schedule the start of the replication, select this option and enter the local date and time to start the replication.
- To start the replication when the wizard finishes, leave this option deselected.

Exclude disks - To exclude some hard disks of the virtual machines from replicating to the destination site, select this option.

Configure Seed VMs -For each new replication that you configure, an initial full synchronization operation is performed. During this operation, vCloud Availability copies the whole data from the source vApp or VM to a datastore in the target site. Due to the size of the vApp or VM or to the network bandwidth, an initial full synchronization might take a long time.

To reduce the initial synchronization time, you copy the source vApp or VM to the target site by using removable media, failover of a previous replication, or other means of data transfer. Then, in the target site, configure a replication that uses the vApp or VM copy as a replication seed.

When a replication uses a seed vApp or VM, vCloud Availability does not copy the whole source vApp or VM data to the target site. Instead, vCloud Availability copies only the different data blocks between the source vApp or VM and the seed and reuses the seed data in the target site as a basis for replication.

We do not have Seed VM available at the target site for this exercise

1. Leave everything as Default and Click **Next**

Ready to Complete the Replication

New Outgoing Replication

- 1 Cloud vApps and VMs
- 2 Destination VDC and Storage policy
- 3 Settings
- 4 Ready To Complete

Ready To Complete

Verify the selected settings before proceeding:

VMs	tenant1-photon-01a
Source site	Tenant1@SiteA
Source VDC	Tenant1-OVDC-A
Destination organization	Tenant1@SiteB
Destination VDC	Tenant1-OVDC-B
Storage policy	Any
Target RPO	24h
Compression	Enabled
Quiescing	Disabled
Retention	Keep latest instance only
Sync time	No delay

CANCEL
BACK
1 FINISH

1. Review the replication details and click on **FINISH**

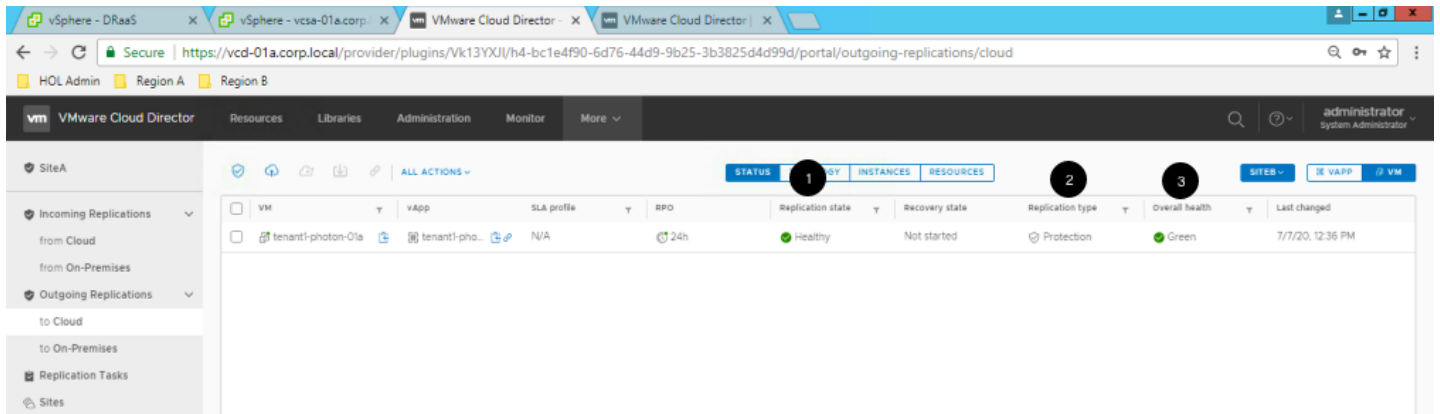
Replication in Progress

The screenshot shows the VMware Cloud Director interface. The left sidebar has a navigation menu with 'Incoming Replications' and 'Outgoing Replications'. The main area shows a table of replication instances. A red box highlights the row for 'tenant1-photon-01a', which shows a replication state of '61% Synchroniz...', a recovery state of 'Not started', and a replication type of 'Protection'. The overall health is 'Green' and it was last changed on '7/7/20, 12:36 PM'.

VM	vApp	SLA profile	RPO	Replication state	Recovery state	Replication type	Overall health	Last changed
tenant1-photon-01a	tenant1-ph...	N/A	24h	61% Synchroniz...	Not started	Protection	Green	7/7/20, 12:36 PM

Review the replication details, it is in progress

Replication is Completed

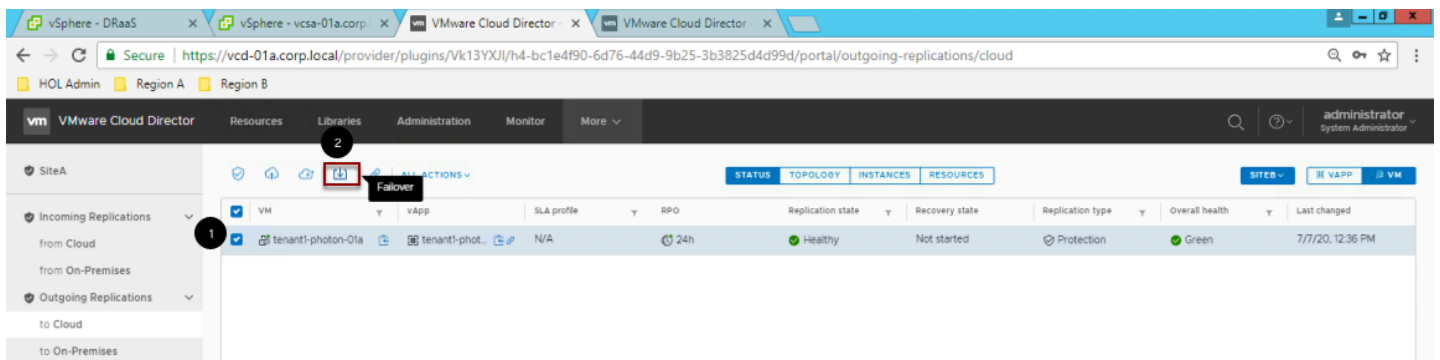


Verify the Replication status, it may take few minutes to complete. Review the details and Confirm:

1. Replication state is **Healthy**
2. Replication type is **Protected**
3. Overall health is **Green**

Note: In case you see Unexpected vCloud Director error during replication, please retry. Due to the nested environment in Hands On Lab, sometimes the error is seen, in real world it should work seamlessly.

Run Failover in Cloud



Now that the VM is successfully replicated in Cloud, we will run Failover workflow such that VM will now run in Cloud SiteB

1. Check the checkbox for **VM tenant1-photon-01a**
2. Click on icon **FAILOVER**

Failover in Cloud - Recovery Settings

Failover

- 1 Recovery Settings
- 2 Recovery Instance
- 3 Ready To Complete

Recovery Settings

Select configuration for the recovered VMs

☐ Consolidate VM disks

Turning on this option will consolidate all instances into the recovered disk. This can improve the runtime performance of the recovered VM, but may greatly increase RTO.

☒ Power on recovered VMs

Network Settings

☒ Apply preconfigured network settings on failover

☐ Connect all VMs to network

Tenant1-OVCD-B-TestNet

Tenant1-OVDC-B-OrigNet-Rtd

CANCEL NEXT

For the cloud to cloud replications, VMware Cloud Director Availability replicates all the types of source vApp networks in the target cloud site: Isolated, bridged (direct) and fenced (NAT-routed) networks. VMware Cloud Director Availability replicates the source networks settings like: IP pools, NAT routes, firewall rules, and DNS settings, in the target site. In this screen, we select the network settings for the recovered VM in the target site.

Brief overview of the parameters on this page

Consolidate VM disks - Enable for a better performance of the recovered virtual machines at the expense of the failover task taking longer to complete.

Power on recovered vApps - Select to power on the virtual machines on the destination site after the task completes.

Network settings

-Apply preconfigured network settings on failover will assign the network that was configured during the virtual machine replication.

-Connect all VMs to network will allow you to select the target network on the fly during the failover

1. Click the radio button for **Connect all VMs to network** and select **Tenant1-OVDC-B-OrgNet-Rtd** from the dropdown menu.
2. Click on **NEXT**

Failover - Recovery Instance

Failover

1 Recovery Settings

2 Recovery Instance

3 Ready To Complete

Recovery Instance

Select recovery point in time.

tenant1-photon-01a

7/7/20, 12:37 PM

CANCEL

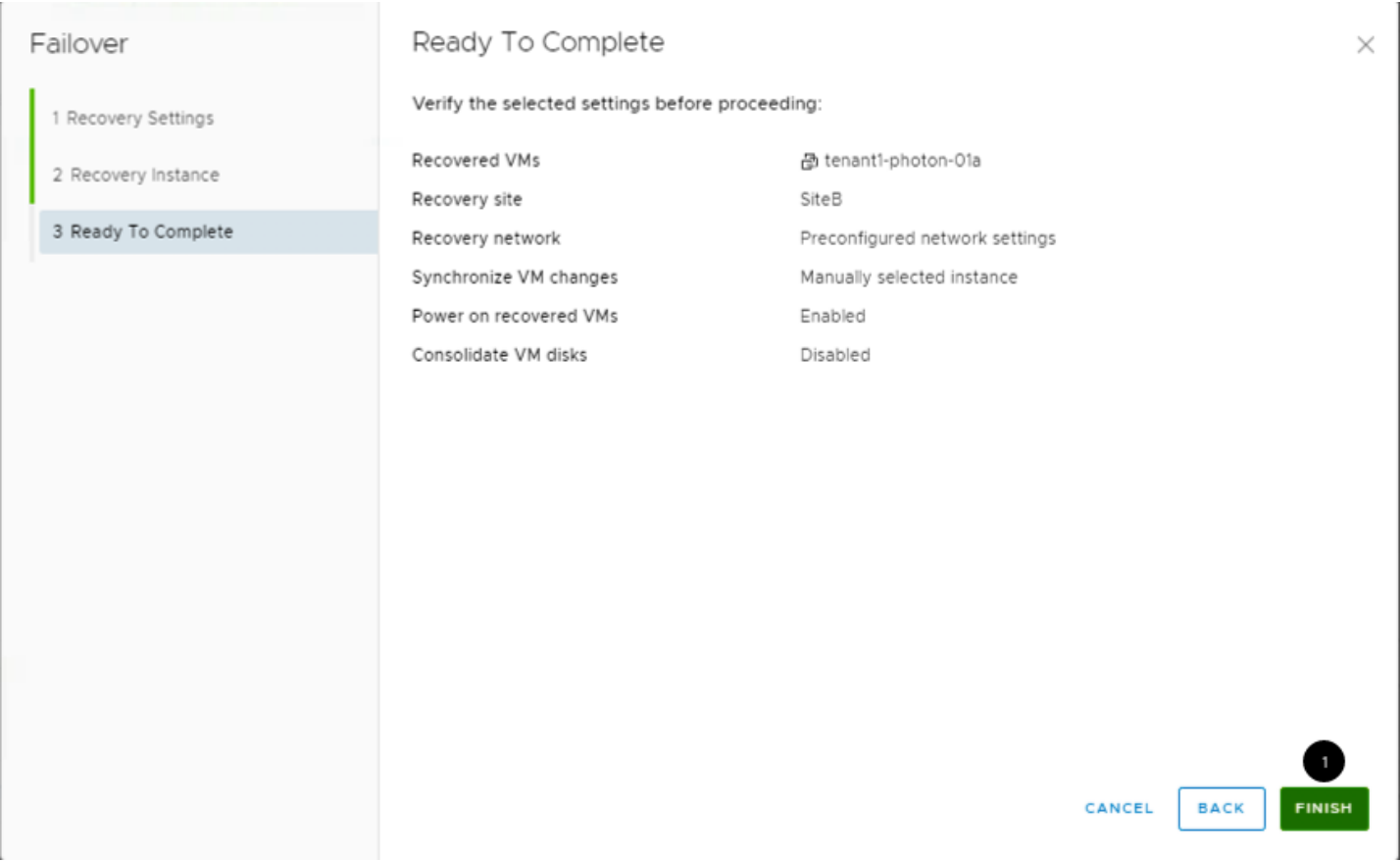
BACK

1

NEXT

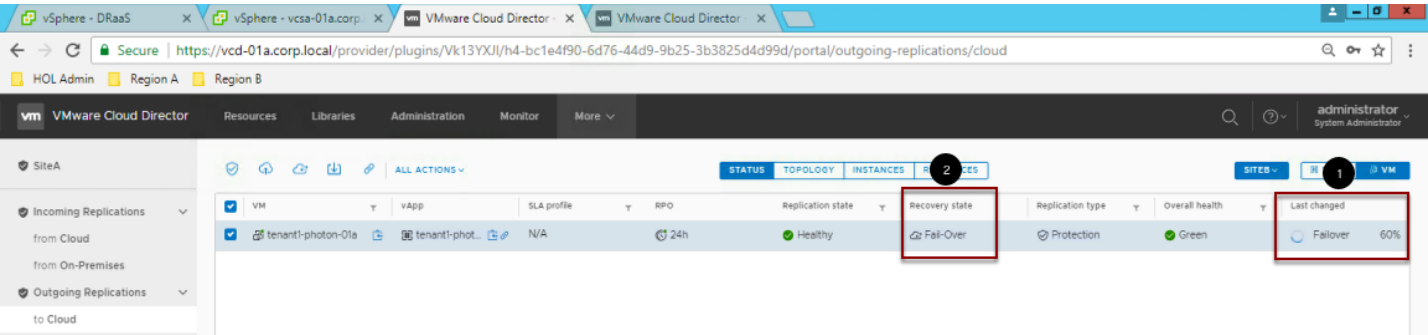
1. Select the latest available Instance and click on **NEXT**

Ready to Complete the Failover Settings



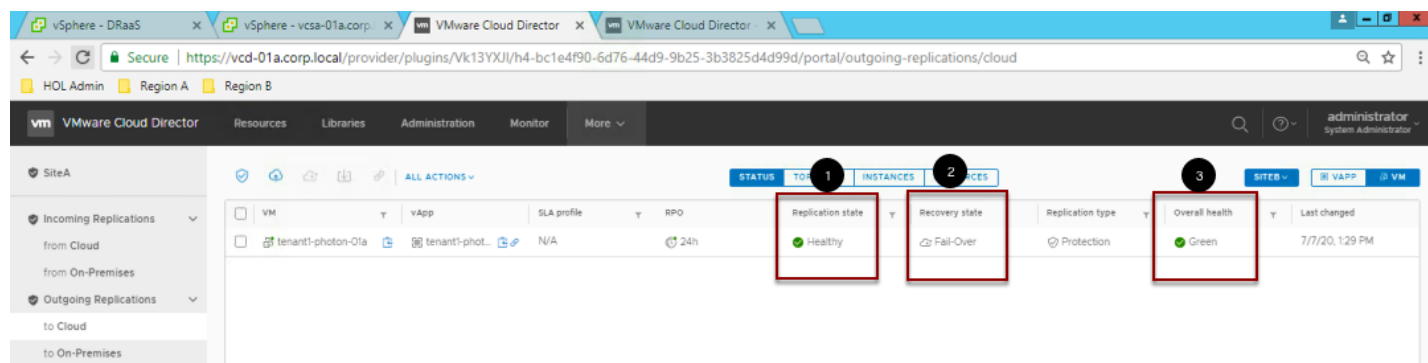
1. Review the Failover Settings and Click on **FINISH**

Failover to Cloud SiteB is in Progress



1. In the Detailed Status, you will notice **Failover in Progress**.
2. Recovery State is updated to **Fail-Over**

Failover completed successfully

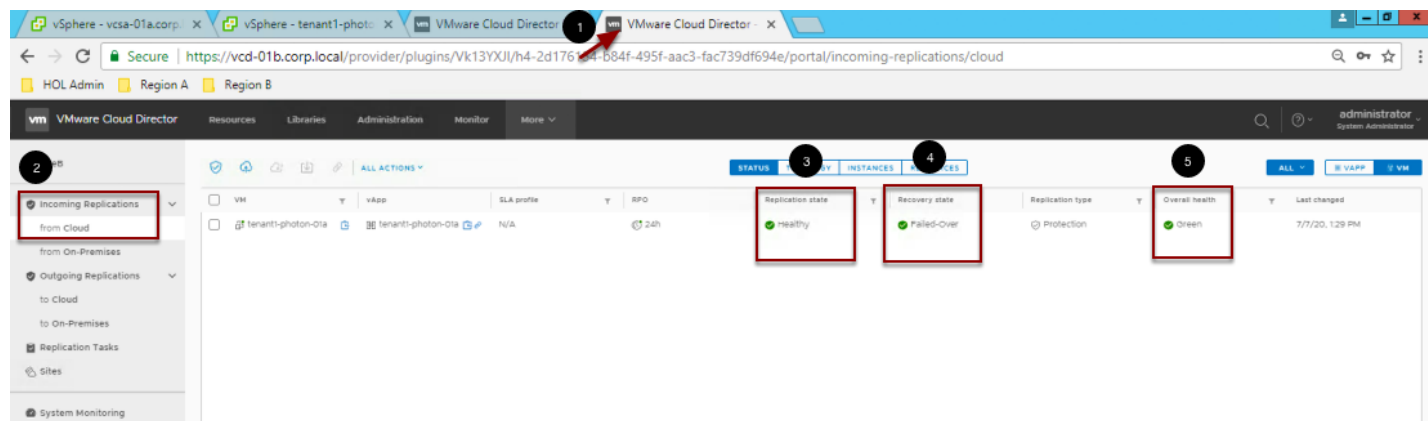


This process will take a couple of minutes. Please be patient.

1. Replication State is **Healthy**
2. Recovery State shows **Failed-Over**.
3. Overall health is **Green**

Note: In case you see Unexpected vCloud Director error during failover, please retry. Due to the nested environment in Hands On Lab, sometimes the error is seen, in real world it should work seamlessly.

Verify Failover is successful at Cloud Provider SiteB



Lets confirm that Failover is completed successfully from Cloud Provider Site B

1. Switch to Site B Cloud Provider
2. Click on **Incoming Replications from Cloud**
3. Replication State is **Healthy**
4. Recovery State shows **Failed-Over**.
5. Overall health is **Green**

Note: In case you see Unexpected vCloud Director error during failover, please retry. Due to the nested environment in Hands On Lab, sometimes the error is seen, in real world it should work seamlessly.

Verify Failed-Over VM is now running in SiteB

The screenshot shows the vSphere Client interface. On the left, the inventory tree is expanded to show the path: **vcsa-01b.corp.local** > **RegionB01** > **RegionB01-COMP01** > **VCD-RegionB01** > **Tenant1-OVDC-B** > **tenant1-photon-01a-hmhB**. The VM **tenant1-photon-01a-hmhB** is highlighted. On the right, the summary page for this VM is displayed, showing it is **Powered On**. The summary includes details such as Guest OS: Other 3.x Linux (64-bit), Compatibility: ESXi 6.5 and later (VM ver), VMware Tools: Running, version:10282 (G), DNS Name: photon-base, IP Addresses: 192.168.145.101, and Host: esx-01b.corp.local. A yellow warning banner indicates that a newer version of VMware Tools is available. Below the summary, the VM Hardware is listed: 1 CPU(s), 0.25 GB memory (0.19 GB active), 512 MB Hard disk 1, and Network adapter 1.

1. Switch back to tab **vCenter SiteB**
2. On the left panel expand **RegionB01**
3. Expand **RegionB01-COMP01**
4. Expand **vCD-RegionB01**
5. Expand **Tenant1-OVDC-B**
6. Verify VM **tenant1-photon-01a-xxxx** is now powered on in SiteB inventory

Congratulations!! You completed the Pairing and Recovery Workflows between the Cloud Provider Sites.

Conclusion

In this module, we covered Site pairing, Replication and Failover workflows from Cloud to Cloud using VMware Cloud Director Availability

You've finished Module 3

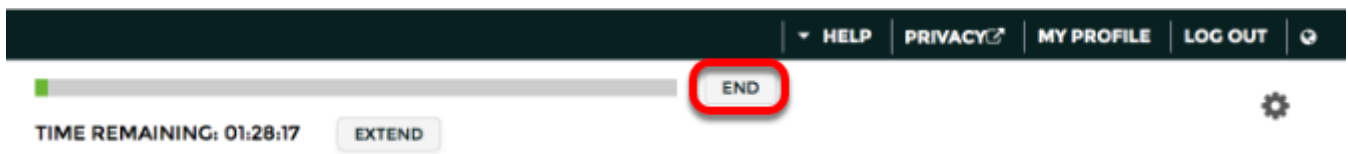


Congratulations on completing Module 3!!

Here are links to other modules in the lab you may be interested in:

- [Module 1 - VMware Cloud Director Availability Overview and Architecture](#) (15 minutes) (Basic) This module will show an overview of the architecture and deployment of VMware Cloud Director Availability 4.0
- [Module 2 - On-Prem DR and Migration to Cloud with VMware Cloud Director Availability](#) (45 Minutes) (Basic) This module will walk through the steps to pair On-Premises site with Cloud and how to use VMware Cloud Director Availability for disaster recovery and migration from on-prem to cloud.
- [Module 4- Tenant-driven Cloud-to-Cloud DR with VMware Cloud Director Availability](#) (30 minutes) (Basic) This module will show Tenant Self-Service Cloud-to-Cloud DR using VMware Cloud Director Availability.

How to End Lab



To end your lab click on the **END** button.

Module 4 - Tenant-driven Cloud-to-Cloud DR with VMware Cloud Director Availability

Introduction

In this article, you will learn how to -

- Pair Cloud to Cloud sites
- Tenant driven Replication and Recovery workflow between Cloud Provider Sites

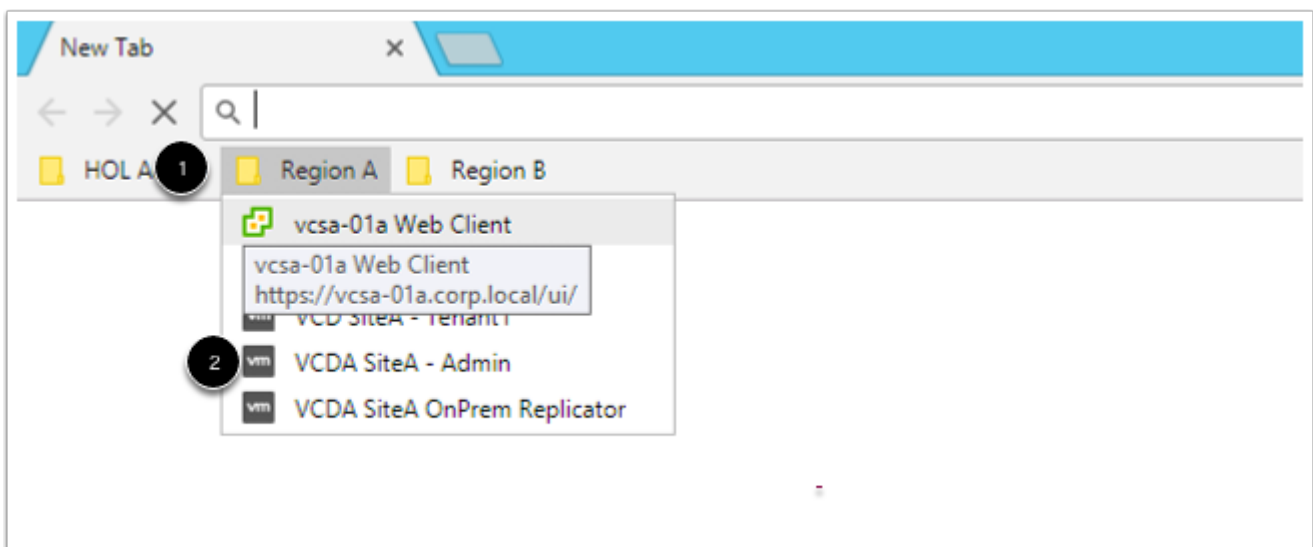
Tenant Self Service Site Pairing and Failover Workflows from Cloud to Cloud using vCloud Availability

In this exercise, we will learn the following workflows -

- Configure Site Pairing from Cloud to Cloud and
- Configure Tenant driven Failover Workflows from Cloud to Cloud using VMware Cloud Director Availability

Note that in the lab environment, we have already deployed and configured the VMware Cloud Availability appliances for each site, but we have not configured any site pairing yet.

Login to RegionA vCenter (On-Premise)



Even though this module is meant to show VMware Cloud Director Availability Tenant Self Service for Cloud-to-Cloud, there are certain things that need to be done by an Administrator, like pairing sites and creating profiles, before the Tenant can use VCDA.

If you went through Module 3 before this module, and completed the site pairing between the two cloud sites, you can skip to the step [Open New Browser to Login as Tenant](#)

Otherwise Please proceed.

1. Start the Chrome Browser from the desktop. Click on **RegionA**.

2. Click on vcsa-01a Web Client . Verify the address as :
https://vcsa-01a.corp.local/

Login to RegionA vCenter (On-Premise)

VMware® vSphere

1 administrator@corp.local

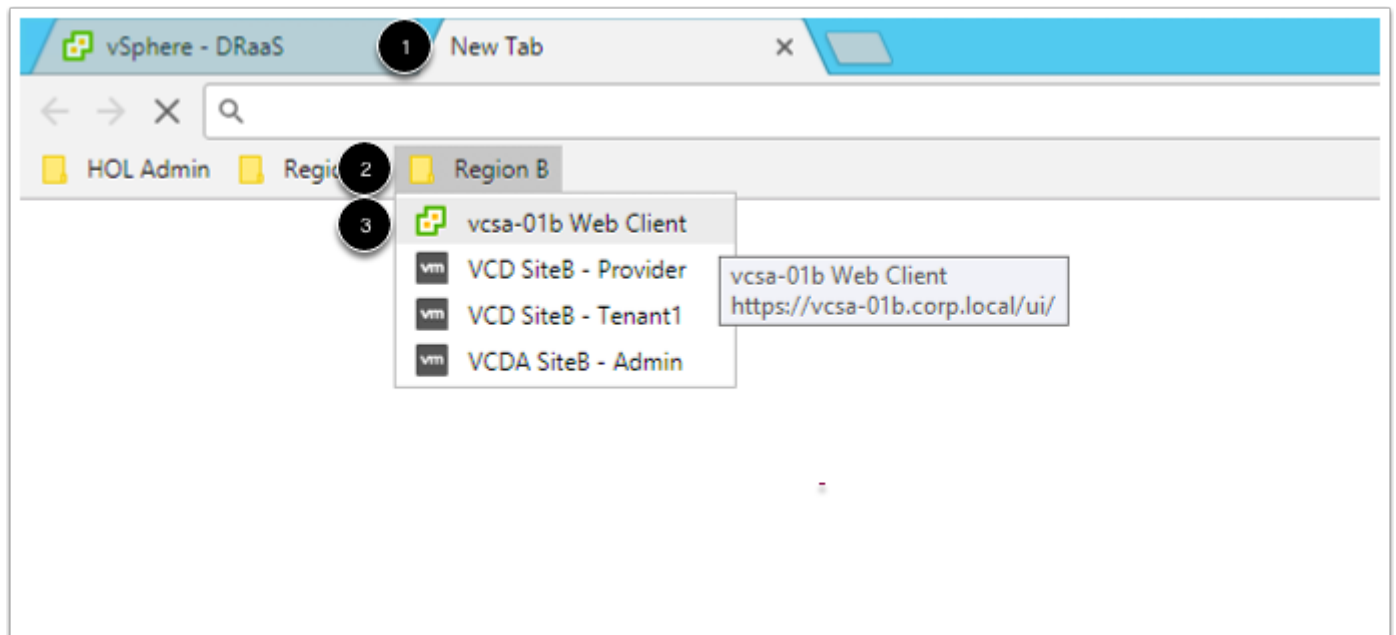
2 *****

☐ Use Windows session authentication

3 LOGIN

1. Enter Username: **administrator@corp.local**
2. Enter Password: **VMware1!**
3. Click on **LOGIN**

Open RegionB vCenter



1. Open a new tab on the browser.
2. Click on **RegionB**
3. Click on vcsa-01b Web Client. Verify the address as :
<https://vcsa-01b.corp.local/>

Login to RegionB vCenter

The screenshot shows a web browser window with two tabs: 'vSphere - DRaaS' and 'Login'. The address bar displays the URL: <https://vcsa-01b.corp.local/webssso/SAML2/SSO/regiona.local?SAMLRequest=zVTljpswFN33K5D3YCCZPKyQU>. Below the address bar, there are three tabs: 'HOL Admin', 'Region A', and 'Region B'. The main content area displays the 'VMware® vSphere' logo. Below the logo, there are two input fields for login credentials. The first field is labeled '1' and contains the text 'administrator@corp.local'. The second field is labeled '2' and contains a series of dots representing a password. Below the password field, there is a checkbox labeled 'Use Windows session authentication'. At the bottom, there is a blue button labeled '3' and 'LOGIN'. The right side of the page features a decorative graphic with overlapping blue and teal triangles.

VMware® vSphere

1 administrator@corp.local

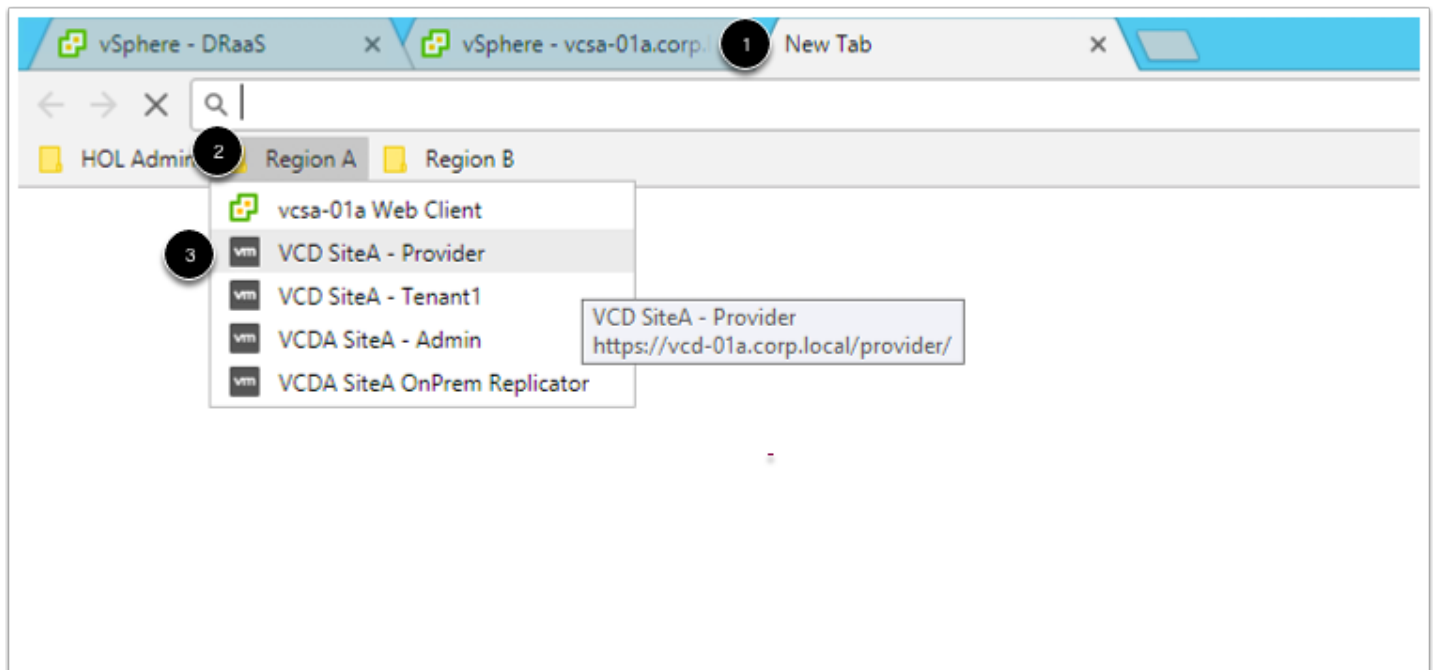
2

☐ Use Windows session authentication

3 LOGIN

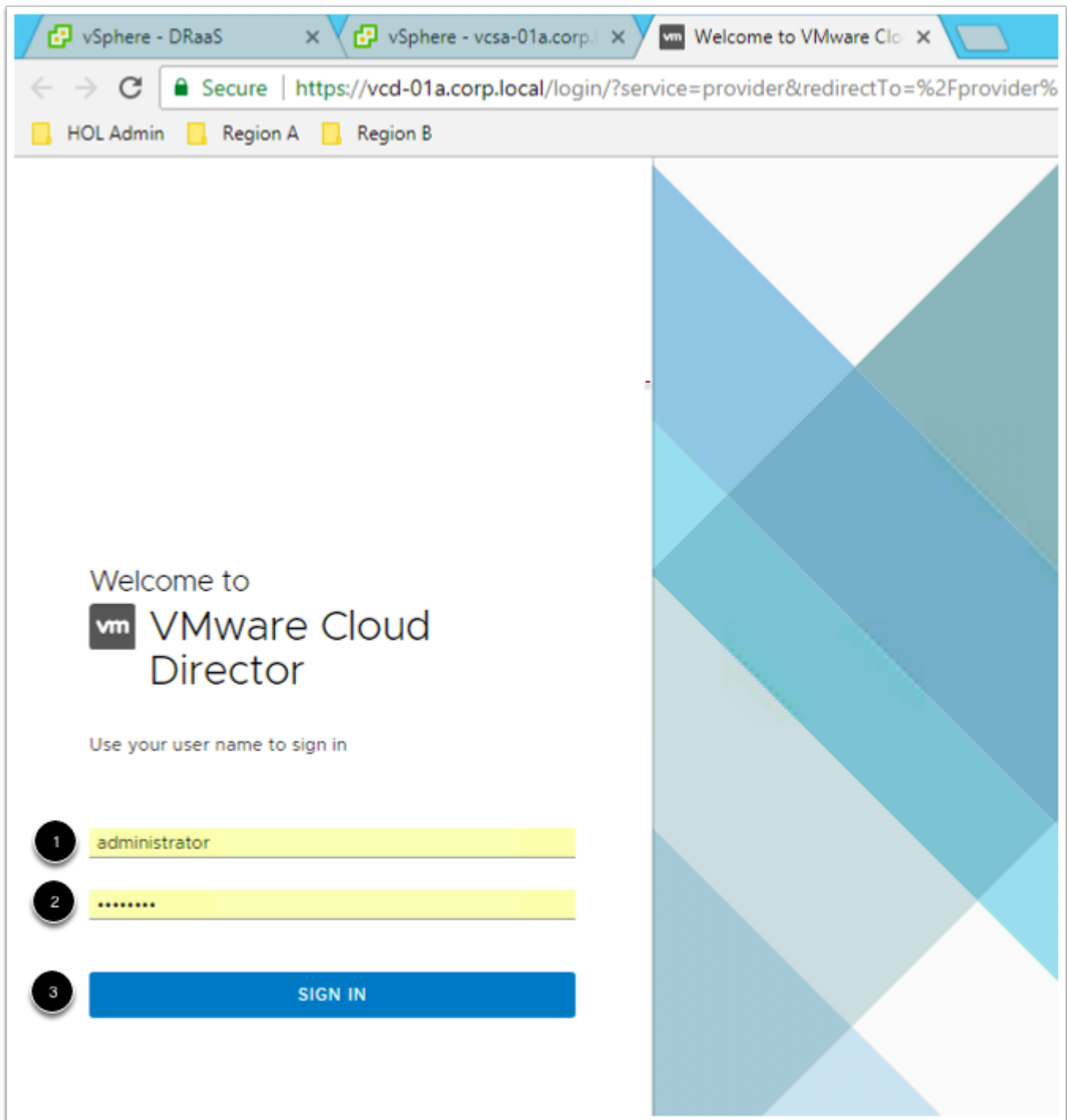
1. Enter Username: **administrator@corp.local**
2. Enter Password: **VMware1!**
3. Click on **LOGIN**

Open SiteA VMware Cloud Director Provider



1. Open a new tab on the browser.
2. Click on **RegionA**
3. Click on VCD SiteA - Provider . Verify the address as :
<https://vcd-01a.corp.local/>

Login to SiteA VMware Cloud Director Provider



The screenshot shows a web browser window with three tabs: 'vSphere - DRaaS', 'vSphere - vcsa-01a.corp.local', and 'Welcome to VMware Cloud Director'. The address bar shows a secure connection to 'https://vcd-01a.corp.local/login/?service=provider&redirectTo=%2Fprovider%'. Below the address bar, there are three tabs: 'HOL Admin', 'Region A', and 'Region B'. The main content area displays the 'Welcome to VMware Cloud Director' message. Below this, it says 'Use your user name to sign in'. There are three numbered steps: 1. Username: administrator, 2. Password: (masked with dots), and 3. Click on SIGN IN.

Welcome to
vm VMware Cloud Director

Use your user name to sign in

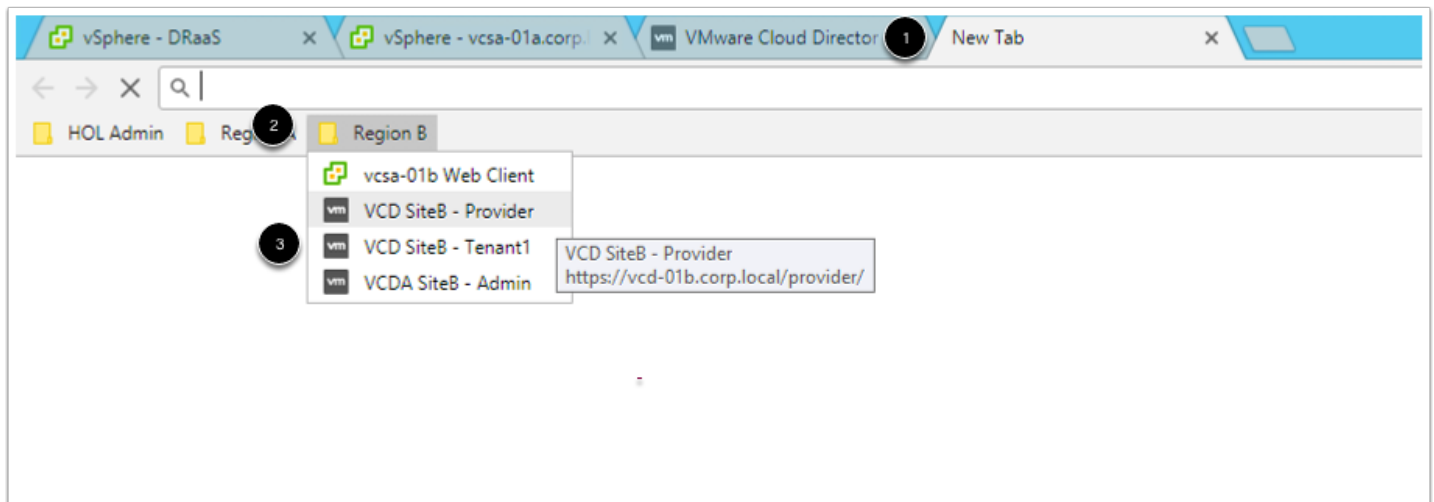
1 administrator

2

3 SIGN IN

1. Username: **administrator**
2. Password: **VMware1!**
3. Click on **SIGN IN**

Open SiteB VMware Cloud Director Provider



1. Open a new tab on the browser.
2. Click on **RegionB**
3. Click on VCD SiteB - Provider. Verify the address as :
<https://vcd-01b.corp.local/>

Login to SiteB VMware Cloud Director Provider

Browser tabs: vSphere - DRaaS, vSphere - vcsa-01a.corp.local, VMware Cloud Director, Welcome to VMware Cloud Director

Address bar: Secure | https://vcd-01b.corp.local/login/?service=provider&redirectTo=%2Fprovider%2F

Navigation bar: HOL Admin, Region A, Region B

Welcome to
vm VMware Cloud Director

Use your user name to sign in

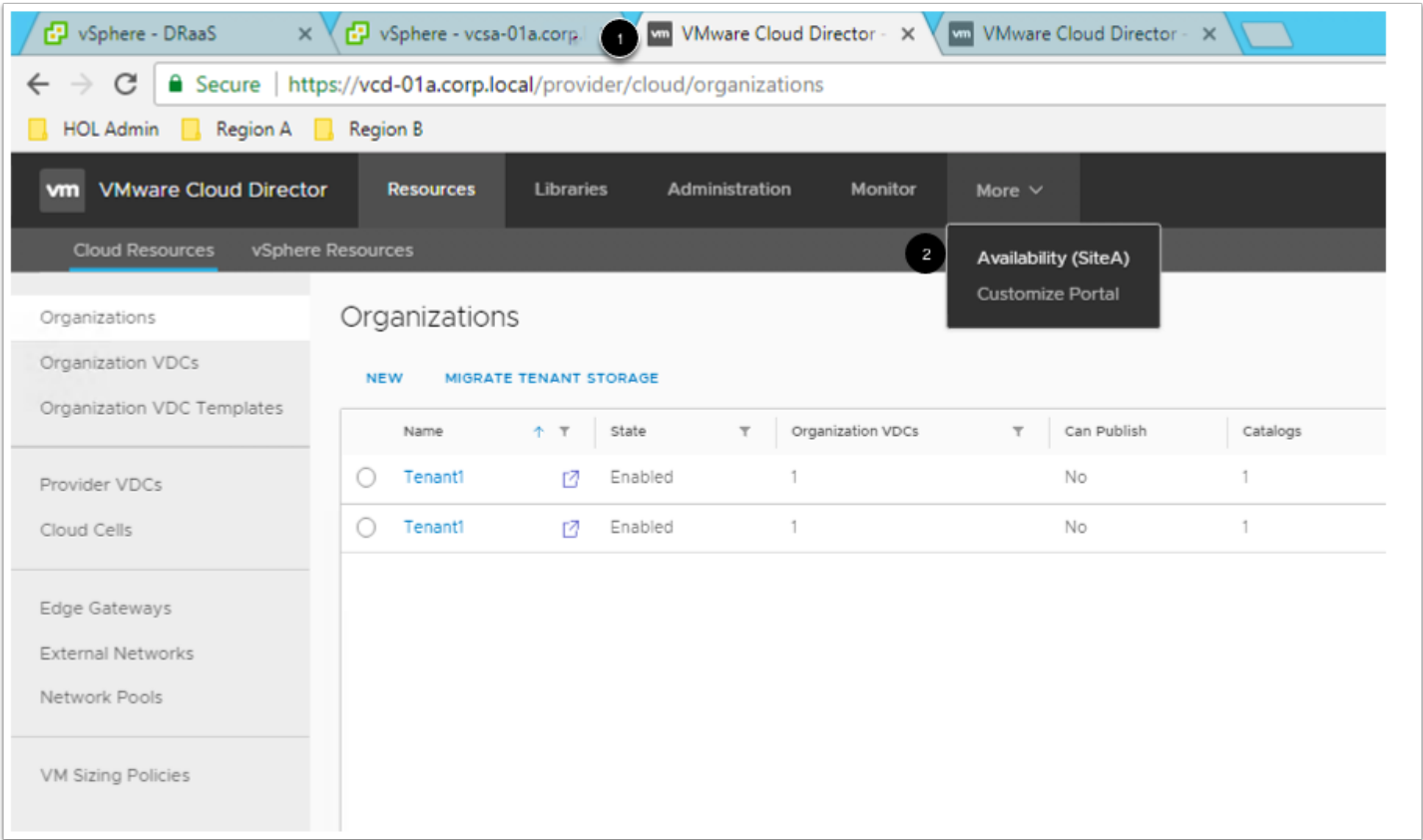
1 administrator

2

3 SIGN IN

1. Username: **administrator**
2. Password: **VMware1!**
3. Click on **SIGN IN**

Open Availability menu at SiteA Provider



- 1. Switch to tab **Site A Provider**
- 2. Expand More
- 3. Click on **Availability (Site A)**

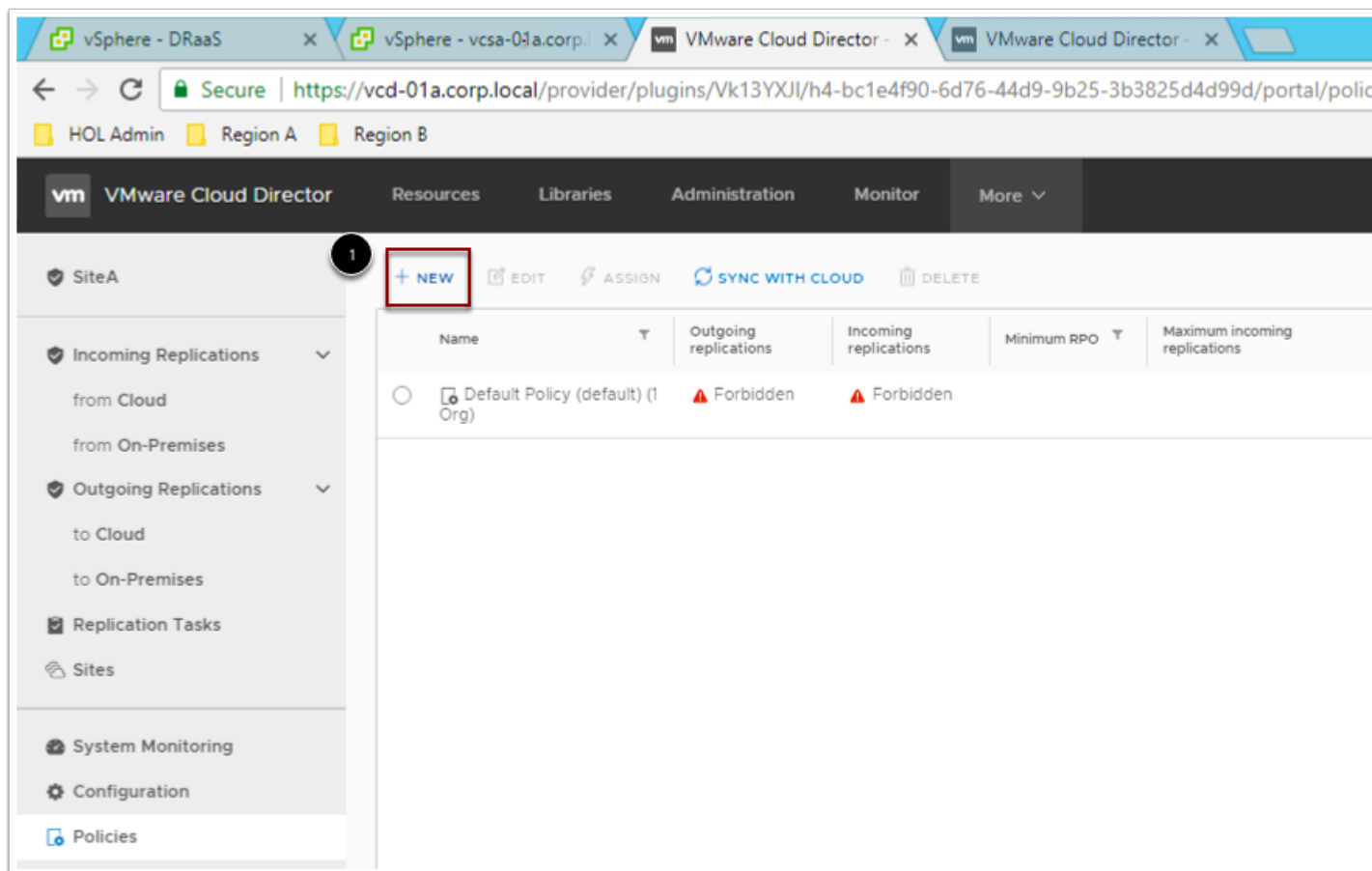
Review Topology and System Health at vCD SiteB

The screenshot displays the VMware Cloud Director web interface for SiteA. The top navigation bar includes links for Resources, Libraries, Administration, Monitor, and More. The left sidebar lists various SiteA components, with 'Policies' highlighted. The main content area is divided into three sections:

- Topology (1):** A diagram showing '0 On-Premises sites' and '0 Cloud sites' connected by bidirectional arrows. A 'CONFIGURE' link is present in the top right corner of this section.
- System health (2):** A section showing the status of services. 'Cloud Service' is 'Online' with a green checkmark, and 'Lookup Service' is 'Online' with a green checkmark.
- On-Premises VM replication status (3):** A section showing 'Incoming VMs' with a circular gauge at 0 and 'No replications'.

1. **Topology:** There are no sites paired and no Replications
2. **System health:** Confirm there are green check marks and everything is healthy and green
3. From the left panel, click **Policies**

Add a new Replication Policy



Replication policies are sets of rules that define and control the replication attributes on a VMware Cloud Director organization level. To control the replication settings allowed for replications on a VMware Cloud Director organization level, the service providers can create replication policies.

When configuring a protection or a migration, the New Replication wizard validates the replication attributes of the policy that is assigned to the organization. Lets add a new policy at SiteA Provider that will be validated while configuring replication.

1. Click on **+ NEW** to add a new Policy

Add a new Policy

New Policy

Policy name: * **1** T1-PolicyA

☒ Allow custom SLA settings

☒ Allow outgoing replications

☒ Allow incoming replications

2 Maximum number of vm replications: * ☐ Unlimited ☒ 10

Max point-in-time instances per replication: ⓘ * 24

Max stored instances per replication: ⓘ * 24

☐ Enable bandwidth throttling

Max throughput per On-Premises Replicator Appliance: * 512 (1 - 10000 mbit/s)

Minimum allowed RPO:

5 min | 30 min | 2 hours | 8 hours | 24 hours

5m

3

CANCEL CREATE

A brief overview for each parameter in this wizard-

- Enter a unique, case-sensitive name for the replication policy.
- Select whether to allow custom SLA settings per replication or only to allow SLA profiles to set the SLA settings.
- Select whether to allow incoming and outgoing replications.
- If incoming replications are enabled, enter the maximum number of virtual machines replications.
- If incoming replications are enabled, enter the maximum number of point-in-time instances per replication.

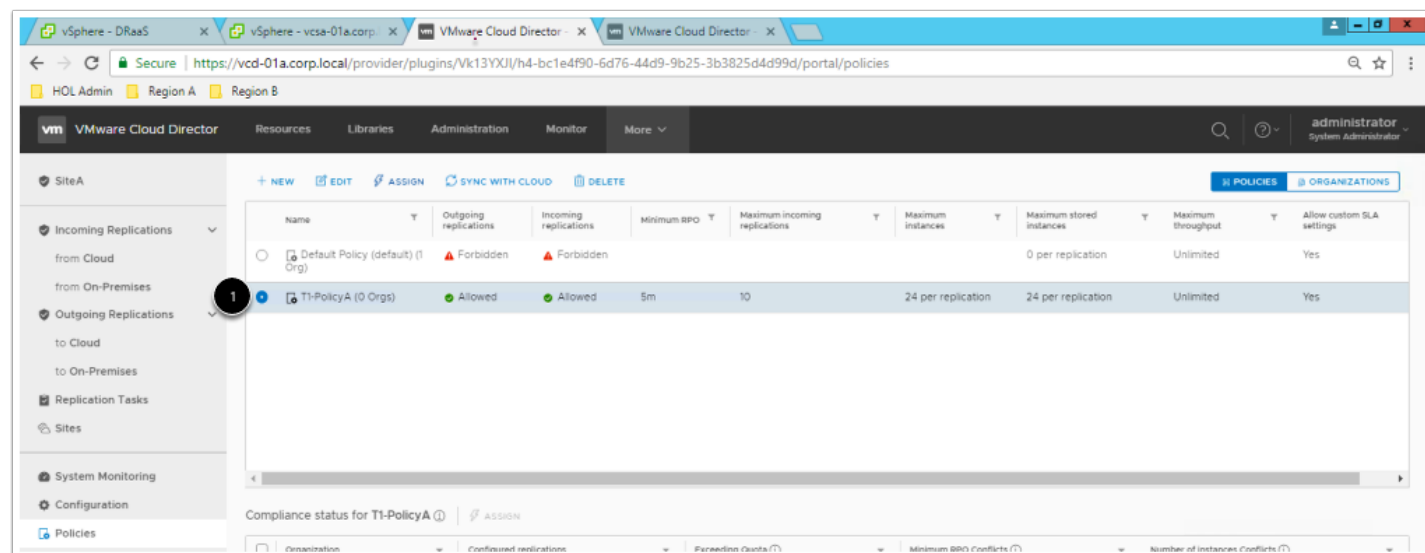
-If incoming replications are enabled, enter the maximum number of stored instances per replication.

-Select whether to allow bandwidth throttling and if enabled enter the maximum throughput per VMware Cloud Director Availability On-Premises Appliance.

-If incoming replications are enabled, set the minimum allowed RPO by using the Recovery Point Objective (RPO) slider or by clicking the time ranges.

1. Enter Policy name: **T1-PolicyA**
2. Leave everything as default
3. Click on **CREATE**

Confirm the Policy is created



1. Confirm policy **T1-PolicyA** is created successfully

Assign the Policy

The screenshot shows the VMware Cloud Director interface. The left sidebar contains navigation options like SiteA, Incoming Replications, Outgoing Replications, Replication Tasks, Sites, System Monitoring, Configuration, and Policies. The main area displays a table of policies. The 'T1-PolicyA' policy is selected, and the 'ASSIGN' button is highlighted.

Name	Outgoing replications	Incoming replications	Minimum RPO	Maximum incoming replications	Maximum instances	Maximum stored instances	Maximum throughput	Allow custom SLA settings
Default Policy (default) (1 Org)	Forbidden	Forbidden				0 per replication	Unlimited	Yes
T1-PolicyA (0 Orgs)	Allowed	Allowed	5m	10	24 per replication	24 per replication	Unlimited	Yes

1. Click on **T1-PolicyA**
2. Click on **ASSIGN**

Assign the Policy (contd..)

The screenshot shows the 'Assign Policy' dialog for 'T1-PolicyA'. It prompts the user to 'Check all organizations to be included to the policy.' A table lists organizations and their associated policies. 'Tenant1' is checked, and its policy is 'Default Policy'. The 'ASSIGN' button is highlighted.

Organization	Policy
☒ Tenant1	Default Policy

1. Check the checkbox **Tenant1**
2. Click on **ASSIGN**

Confirm the Policy is assigned to Org

The screenshot shows the VMware Cloud Director interface. The left sidebar has a 'Policies' link. The main area displays a table of policies. A circled '1' points to the 'T1-PolicyA (1 Org)' row.

Name	Outgoing replications	Incoming replications	Minimum RPO	Maximum incoming replications	Maximum instances	Maximum stored instances	Maximum throughput	Allow custom SLA settings
Default Policy (default) (0 Orgs)	Forbidden	Forbidden				0 per replication	Unlimited	Yes
T1-PolicyA (1 Org)	Allowed	Allowed	5m	10	24 per replication	24 per replication	Unlimited	Yes

Below the table, there is a 'Compliance status for T1-PolicyA' section with an 'ASSIGN' button.

Organization	Configured replications	Exceeding Quota	Minimum RPO Conflicts	Number of instances Conflicts
Tenant1	0	0	0	0

1. Confirm T1-PolicyA is now assigned to 1 Org

Switch to SiteB Cloud Provider tab

The screenshot shows the VMware Cloud Director interface. The left sidebar has a 'Cloud Resources' link. The main area displays a table of organizations. Annotations 1, 2, and 3 point to the 'More' dropdown menu, which is expanded to show 'Customize Portal' and 'Availability (SiteB)'.

Name	State	Organization VDCs	Can Publish	Catalogs	vApps	Running VMs	Users	Site
Tenant1	Enabled	1	No	1	2	1	1	192.168.210.40
Tenant1	Enabled	1	No	1	1	1	1	192.168.110.40

1. Switch to tab **SiteB Provider**
2. Expand **More**
3. Click on **Availability (SiteB)**

Verify/Create Replication Policy for SiteB

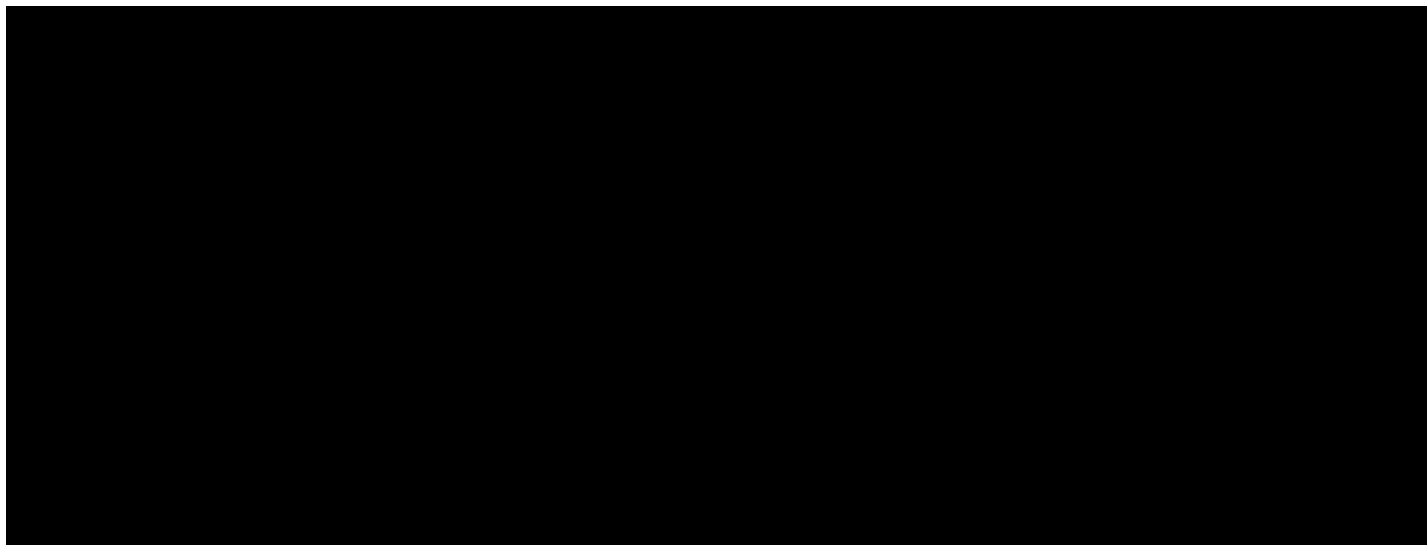
The screenshot shows the VMware Cloud Director interface for SiteB. The left sidebar contains a navigation menu with the following items: SiteB (selected), Incoming Replications (with a dropdown arrow), from Cloud, from On-Premises, Outgoing Replications (with a dropdown arrow), to Cloud, to On-Premises, Replication Tasks, Sites, System Monitoring, Configuration, Policies (highlighted in blue), and SLA Profiles. The main content area has a top bar with buttons: + NEW, EDIT, ASSIGN, SYNC WITH CLOUD, and DELETE. Below this is a table of replication policies.

Name	Outgoing replications	Incoming replications	Minimum RPO
☐ Default Policy (default) (0 Orgs)	Forbidden	Forbidden	
☐ T1-Policy (1 Org)	Allowed	Allowed	5m

If you went through Module 2 before this module, you should already have a replication policy created and assigned. You can go to the next page.

If you do NOT already have a replication policy created and assigned, please use the steps you just completed for SiteA to create and assign a replication policy for SiteB.

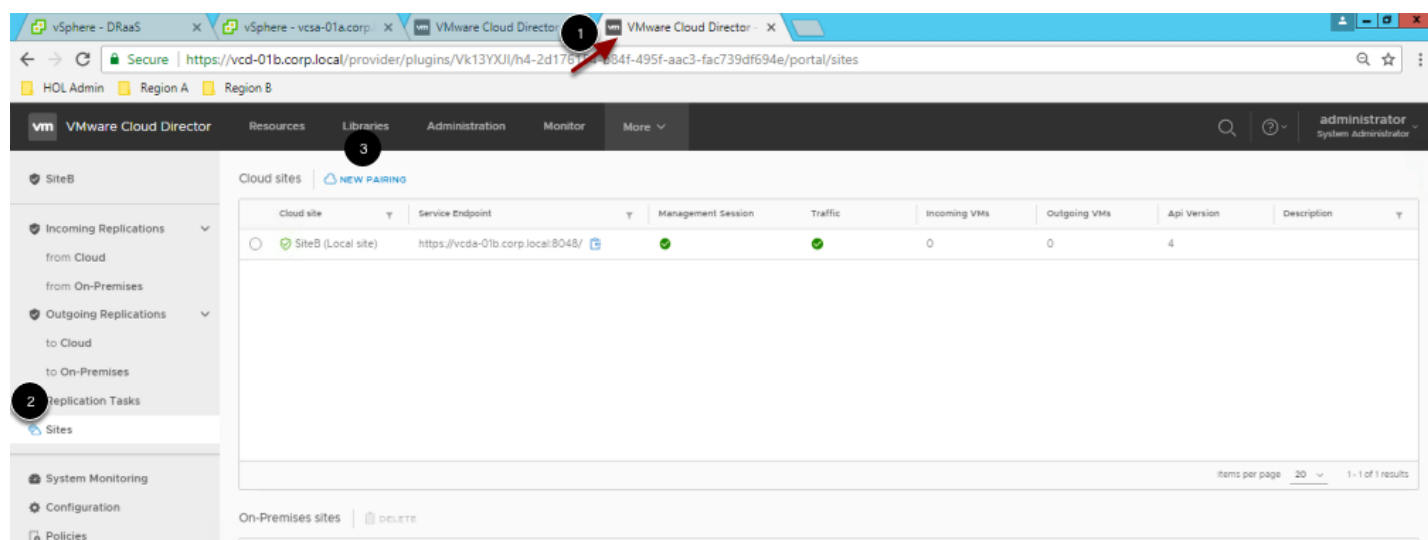
Copy Public API Endpoint from SiteA Cloud Provider



Before we pair the 2 sites, we need the Public API Endpoint from SiteA

1. Switch to SiteA Cloud Provider tab
2. From left panel, click on **Sites**
3. Copy Public API Endpoint: **https://vcda-01a.corp.local:8048/**

Configure New Pairing between Cloud Provider Sites



1. Switch back to **SiteB Cloud Provider**
2. From left panel, Click on **Sites**
3. Click on **NEW PAIRING**

Enter New Pairing details

New Pairing

Enter name, description and connection details for the cloud site.

Site name ⓘ * **1** SiteA

Service Endpoint ⓘ * **2** <https://vcda-01a.corp.local:8048/>

Description

3

CANCEL PAIR

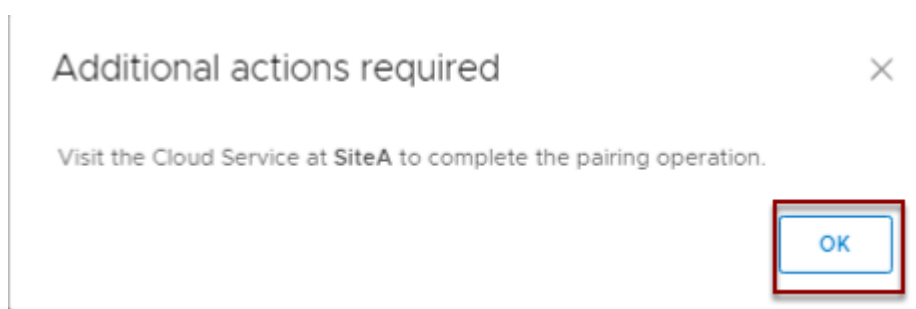
1. Enter Site name : **SiteA**
2. **Service Endpoint** - Paste the Public API Endpoint url we copied from Site A cloud provider: <https://vcda-01a.corp.local:8048/>
3. Click on **PAIR**

Accept the Server Certificate



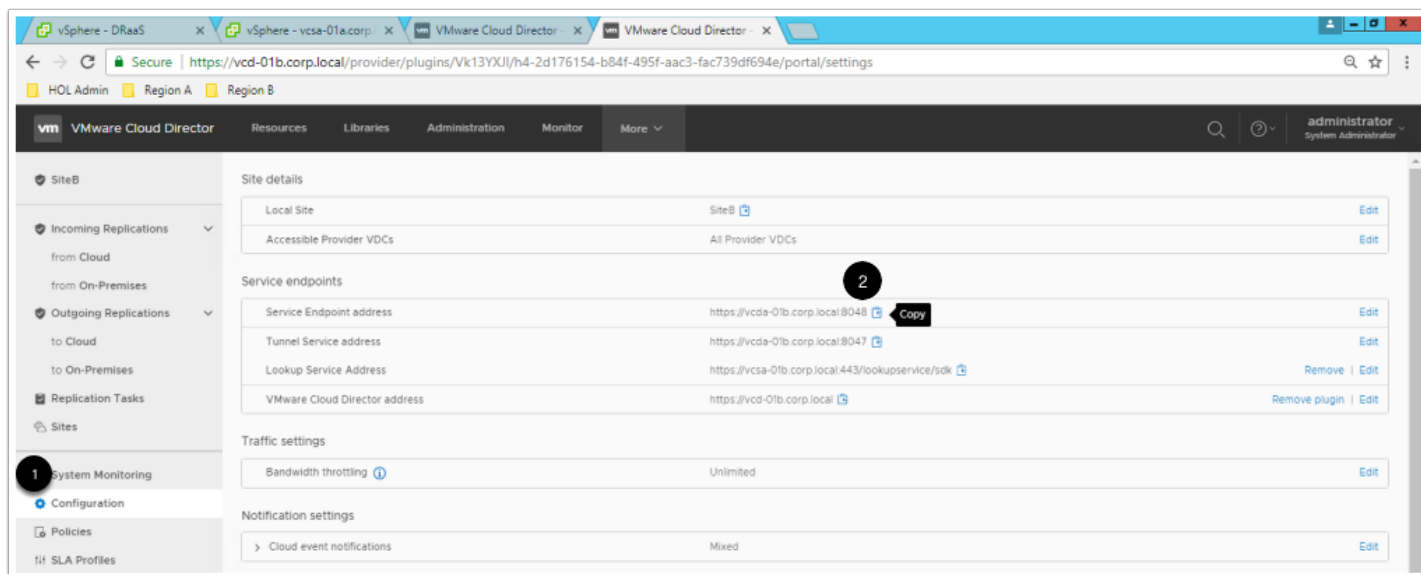
1. Click on **ACCEPT** to accept the SSL certificate from the paired site and you should be able to successfully pair the sites

Additional Action is Required to Complete the Pairing Between 2 Cloud Provider Sites



To complete the pairing between 2 cloud provider sites, additional action is required. Click on OK

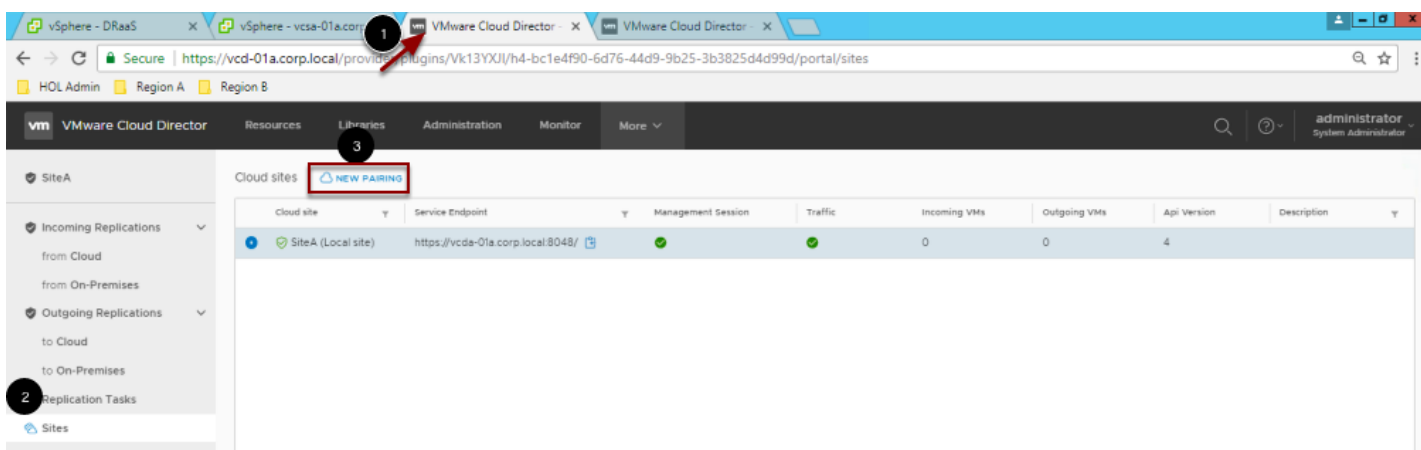
Copy Public API Endpoint from SiteB Cloud Provider



Before we complete pairing the 2 cloud sites, we need the Public API Endpoint from SiteB as well

1. From Left panel, Click on **Configuration**
2. Copy the Service Endpoint address using the icon
https://vcda-01b.corp.local:8048/

Switch to SiteA Cloud Provider



1. Switch to tab **SiteA Cloud Provider**.
2. From left panel, Click on **Sites**
3. Click on **NEW PAIRING**

Enter New Pairing details

New Pairing

Enter name, description and connection details for the cloud site.

Site name ⓘ *

1 SiteB

Service Endpoint ⓘ *

2 <https://vcda-01b.corp.local:8048>

Description

CANCEL

3 PAIR

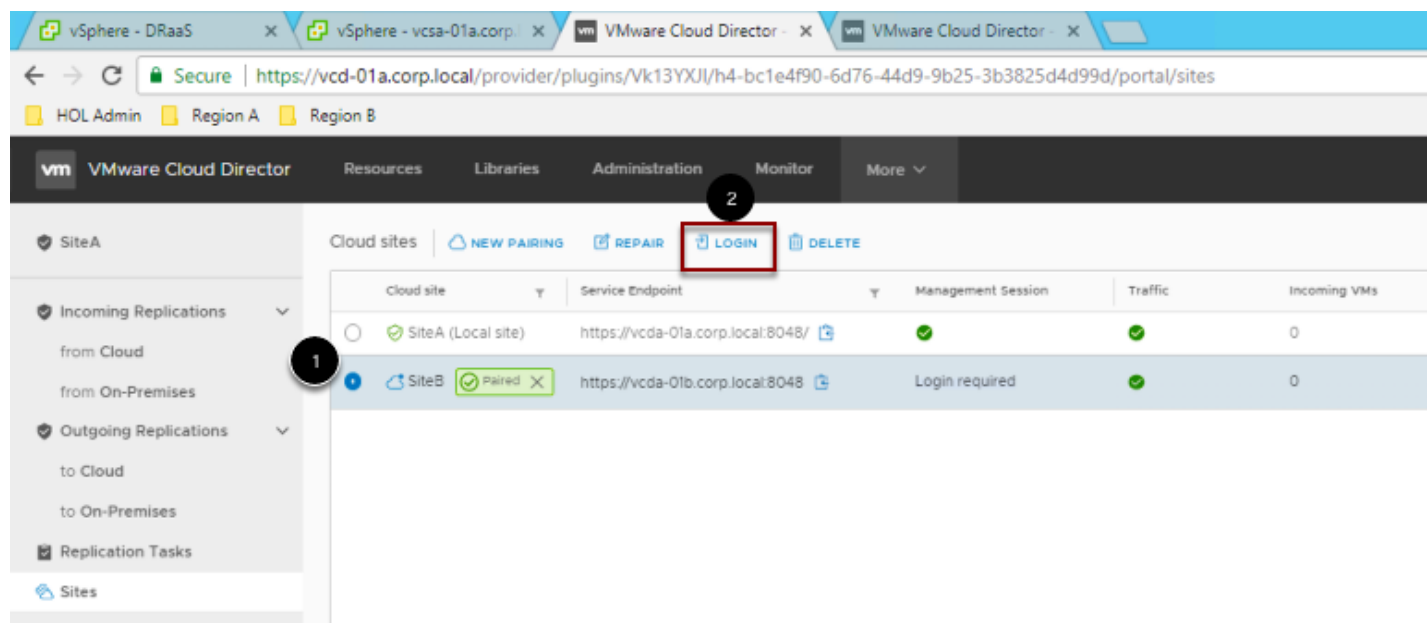
1. Enter Site name : **SiteB**
2. **Service Endpoint** - Paste the Public API Endpoint url we copied from Site B cloud provider: <https://vcda-01b.corp.local:8048/>
3. Click on **PAIR**

Accept the Server Certificate



1. Click on **ACCEPT** to accept the SSL certificate from the paired site and you should be able to successfully pair the sites

Login to SiteB to complete pairing



Once the pairing is completed, a login button appears allowing us to authenticate as our vCloud Director provider admin user (administrator@system) to the 2nd site. After successful authentication the 2 cloud provider sites should be paired and ready to run failover workflows.

1. Select **SiteB**
2. Click on **LOGIN**

Enter Login Credentials for SiteB

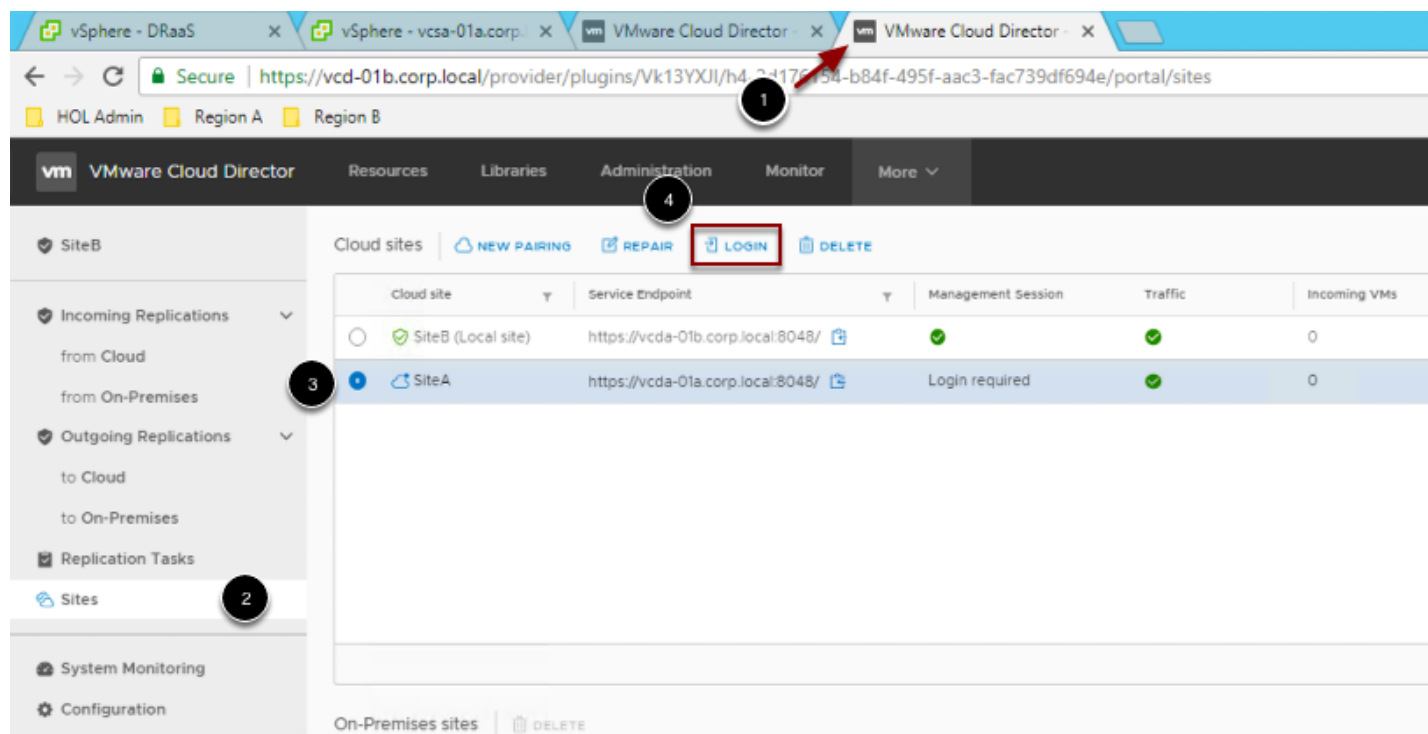
1. Enter Username: **administrator@system**
2. Enter Password: **VMware1!**
3. Click **LOGIN**

Confirm on vCD SiteA that the Pairing is complete

Cloud site	Service Endpoint	Management Session	Traffic	Incoming VMs	Outgoing VMs	Api Version	Description
SiteA (Local site)	https://vcda-01a.corp.local:8048/	✓	✓	0	0	4	
SiteB	https://vcda-01b.corp.local:8048	✓	✓	0	0	4	

Confirm that the pairing to SiteB is **Green** and **Healthy**

Verify the Pairing at vCD SiteB



Before we confirm the pairing between the sites, we need to login to SiteA

1. Switch to tab **SiteB Cloud Provider**
2. Select **Sites** in the left-hand navigation bar
3. Select the Cloud site **SiteA**
4. Click on **LOGIN**

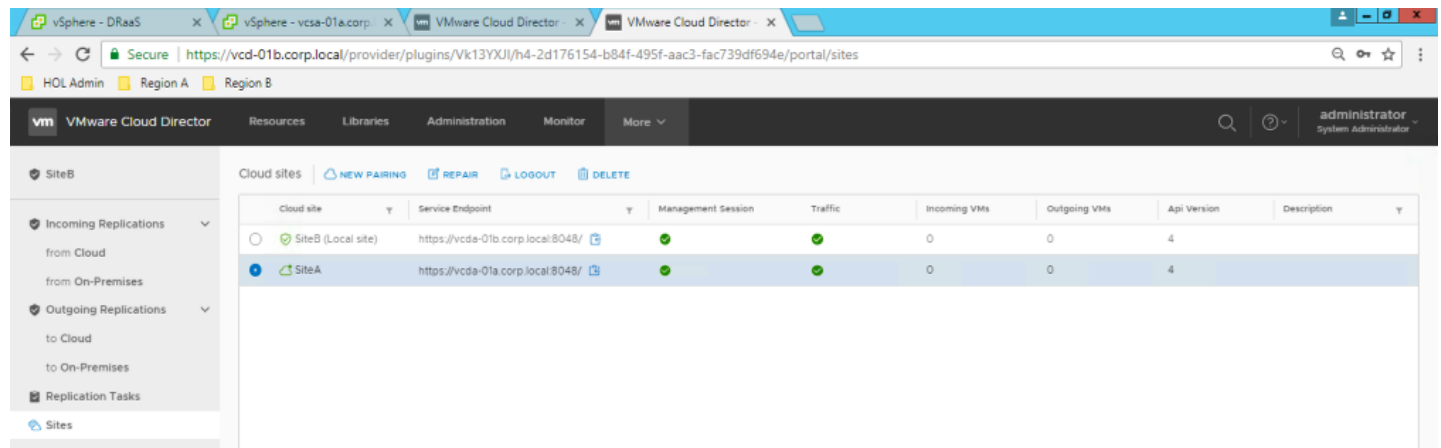
Enter Login Credentials for SiteA

The 'Log In | SiteA' dialog box is shown. It contains the text 'Provide credentials to manage replications on SiteA.' Below this are two input fields: 'Username' (callout 1) with the value 'administrator@system' and 'Password' (callout 2) which is masked with dots. At the bottom right are two buttons: 'CANCEL' and 'LOGIN' (callout 3, highlighted in green).

1. Enter Username: **administrator@system**
2. Enter Password: **VMware1!**

3. Click on **LOGIN**

Confirm the Pairing from SiteB to SiteA is successful

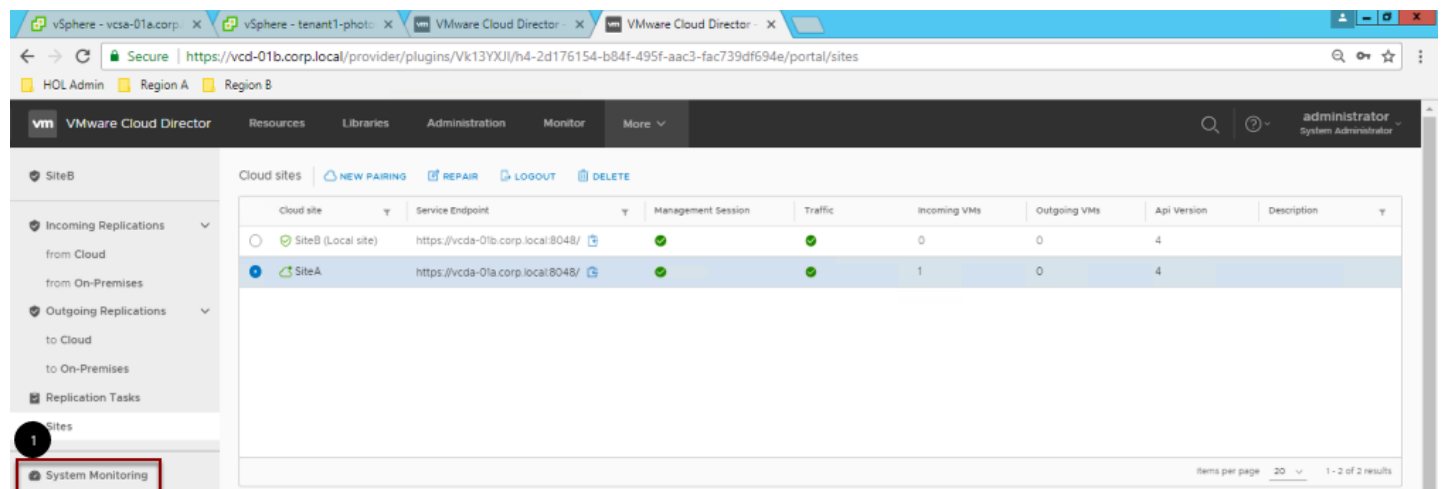


The screenshot shows the VMware Cloud Director interface. The left-hand navigation bar has 'Sites' selected. The main area displays 'Cloud sites' with a table of site pairings. The table has columns: Cloud site, Service Endpoint, Management Session, Traffic, Incoming VMs, Outgoing VMs, Api Version, and Description. Two sites are listed: SiteB (Local site) and SiteA. Both show a green status icon and a green checkmark in the Management Session column, indicating successful pairing.

Cloud site	Service Endpoint	Management Session	Traffic	Incoming VMs	Outgoing VMs	Api Version	Description
SiteB (Local site)	https://vcda-01b.corp.local:8048/	✓	✓	0	0	4	
SiteA	https://vcda-01a.corp.local:8048/	✓	✓	0	0	4	

Confirm that the pairing to SiteA is **Green** and **Healthy**

System Monitoring at SiteB Cloud Provider



The screenshot shows the VMware Cloud Director interface. The left-hand navigation bar has 'System Monitoring' selected, which is highlighted with a red box and a '1' in a circle. The main area displays 'Cloud sites' with a table of site pairings. The table has columns: Cloud site, Service Endpoint, Management Session, Traffic, Incoming VMs, Outgoing VMs, Api Version, and Description. Two sites are listed: SiteB (Local site) and SiteA. Both show a green status icon and a green checkmark in the Management Session column, indicating successful pairing.

Cloud site	Service Endpoint	Management Session	Traffic	Incoming VMs	Outgoing VMs	Api Version	Description
SiteB (Local site)	https://vcda-01b.corp.local:8048/	✓	✓	0	0	4	
SiteA	https://vcda-01a.corp.local:8048/	✓	✓	1	0	4	

1. Click on **System Monitoring** on the left-hand navigation bar

View Local and Remote Replicators at Cloud SiteB

The screenshot shows the VMware Cloud Director web interface. The left sidebar contains navigation menus for Sites, Incoming Replications, Outgoing Replications, Replication Tasks, System Monitoring, Configuration, Policies, SLA Profiles, Datastores, System Tasks, OpenAPI Client, Reports, Resources, Support, and About. The main content area is titled 'System health' and includes a 'Service status' table and a 'Manager Service status' table. Below these, there are sections for 'Local Replicator Services (1)' and 'Remote Replicator Services (2)'. The 'Remote Replicator Services (2)' section is highlighted with a red box, showing details for a service named 'Service connectivity (vSphere-OnPrem)'. The details include Address, Instance ID, Maintenance mode, and Site.

Service status	
Traffic	OK
Address	192.168.210.90
Instance ID	20170154-b84f-495f-aac3-fac739df694e
Server time	7/7/20, 11:45 PM GMT-7
Lookup Service connectivity	OK
Database connectivity	OK
VMware Cloud Director connectivity	OK
Tunnel Service connectivity	OK
NTP connectivity	OK

Manager Service status	
Service connectivity	OK
Address	https://192.168.210.90:8044
Instance ID	1ab8f545-c09c-4123-bf1c-a48ecd7dd2
Server time	7/7/20, 11:45 PM GMT-7
Lookup Service connectivity	OK
Replicators lookup service configuration	OK
Database connectivity	OK

1 Local Replicator Services (1)

Service connectivity (192.168.210.90)	
Service connectivity	OK

2 Remote Replicator Services (2)

Service connectivity (vSphere-OnPrem)	
Address	https://192.168.210.90:8044
Instance ID	ea5f8fb-cf4e-41c9-8721-c007243078e8
Maintenance mode	No
Site	vSphere-OnPrem

Scroll down to the bottom of the page to view Local and Remote Replicator details.

1. Here, you should see that both the **Local** (to the site you are logged into) and **Remote** Replicators are shown and connected
2. The odd Address shown for the Remote replicator (boxed in red above) is correct since this is an internal address used to reach the remote replicator appliance via the Tunnel.

System Monitoring at Cloud SiteA

The screenshot shows the VMware Cloud Director web interface. The browser tabs include 'vSphere - vcsa-01a.corp', 'vSphere - tenant1-photo', and two 'VMware Cloud Director' tabs. The address bar shows the URL: <https://vcd-01a.corp.local/provider/plugins/Vk13YXJl/h4-bc1e4f90-6d76-44d9-9b25-3b3825d4d99d/portal/sites>. The navigation bar includes 'HOL Admin', 'Region A', and 'Region B'. The main navigation menu has 'vm VMware Cloud Director', 'Resources', 'Libraries', 'Administration', 'Monitor', and 'More'. The left sidebar shows 'SiteA' selected, with sub-items: 'Incoming Replications' (from Cloud, from On-Premises), 'Outgoing Replications' (to Cloud, to On-Premises), 'Replication Tasks', 'Sites', and 'System Monitoring' (highlighted with a red box and a black circle with the number 2). The main content area shows 'Cloud sites' with buttons for 'NEW PAIRING', 'REPAIR', 'LOGOUT', and 'DELETE'. A table lists the cloud sites:

Cloud site	Service Endpoint	Management Session	Traffic	Incoming VMs
SiteA (Local site)	https://vcd-01a.corp.local:8048/	✓	✓	0
SiteB	https://vcd-01b.corp.local:8048	✓	✓	0

Similar to Cloud SiteB, we will now review the local and remote replicators configured at Cloud SiteA

1. Switch back to tab **SiteA Cloud Provider**
2. Click on **System Monitoring**

View Local and Remote Replicators at Cloud SiteA

The screenshot shows the VMware Cloud Director interface for SiteA. The left sidebar contains navigation links for Incoming Replications, Outgoing Replications, Replication Tasks, Sites, System Monitoring, Configuration, Policies, SLA Profiles, Datastores, System Tasks, OpenAPI Client, Reports, Resources, Support, and About. The main content area displays the following tables:

Service status	
Traffic	OK
Address	192.168.110.90
Instance ID	bc1e4f90-6d76-44d9-9b25-3b3825d4d99d
Server time	7/7/20, 11:53 PM GMT-7
Lookup Service connectivity	OK https://vcsa-01a.corp.local
Database connectivity	OK
VMware Cloud Director connectivity	OK
Tunnel Service connectivity	OK https://vcsa-01a.corp.local
NTP connectivity	OK

Manager Service status	
Service connectivity	OK
Address	https://192.168.110.90:8044
Instance ID	8d04ba75-fe16-46bd-ab41-c4863bd8dabc
Server time	7/7/20, 11:53 PM GMT-7
Lookup Service connectivity	OK
Replicators lookup service configuration	OK
Database connectivity	OK

Local Replicator Services (1)

Service connectivity (192.168.110.90)	OK
---------------------------------------	----

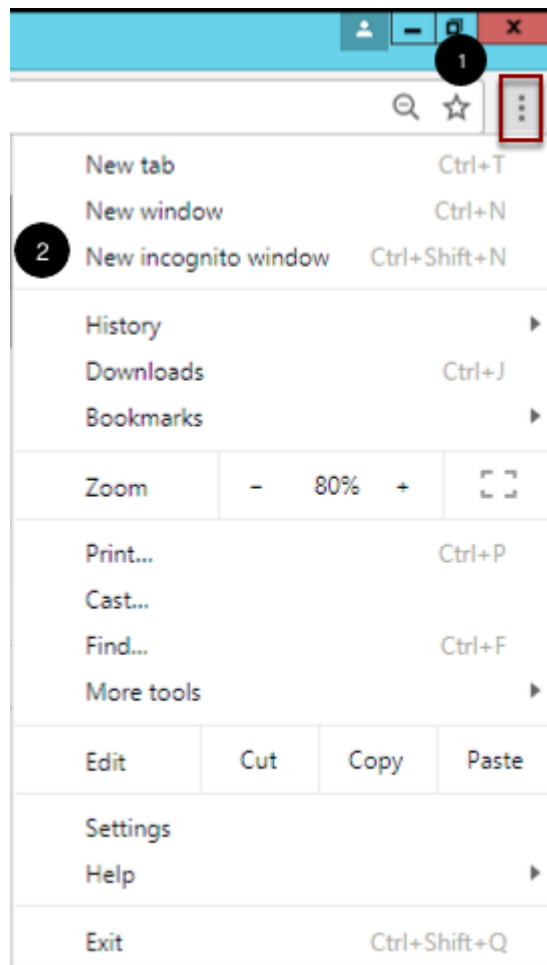
Remote Replicator Services (1)

Service connectivity (SiteB)	OK
Address	https://192.168.110.90:8044
Instance ID	a37c7b2e-75e3-40f6-ab6c-59c826e53ba2
Maintenance mode	NO
Site	SiteB

Scroll down to the bottom to the bottom of the page to view Local and Remote Replicator Services details.

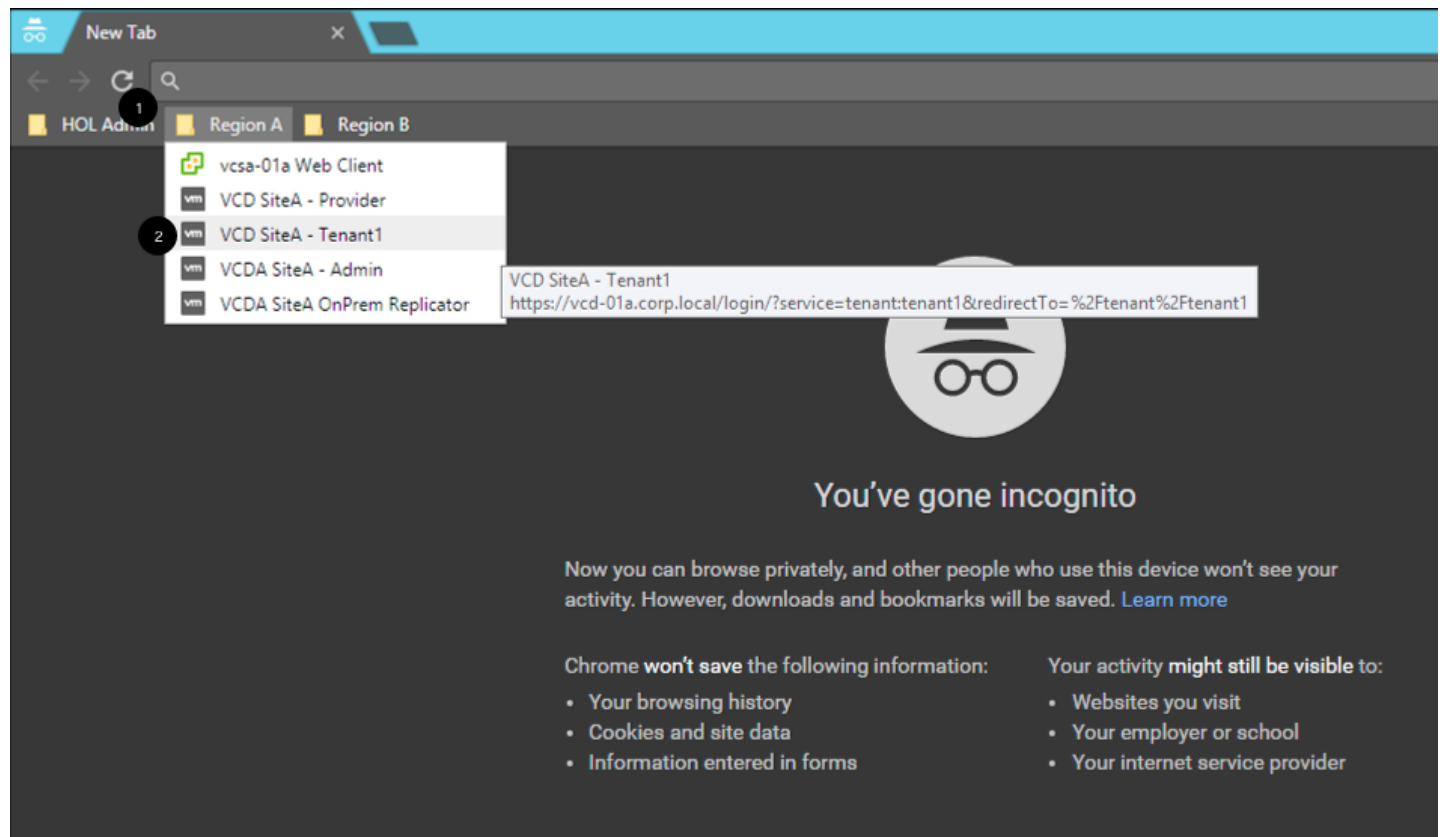
1. Here, you should see that both the **Local** (to the site you are logged in to) and **Remote** Replicators are shown and connected
2. The odd Address shown for the Remote replicator (boxed in red above) is correct this is an internal address used to reach the remote replicator appliance via the Tunnel.

Open new browser to Login as Tenant



1. Click on 3 dots at the top right corner to open Chrome in Incognito mode. We will login as Tenant in Incognito mode so the other Chrome browser tabs can remain open logged in as Administrator.
2. Click on **New incognito window**

Open Tenant Site A



1. In the bookmarks bar, open the folder named **Region A**
2. Click on **VCD SiteA - Tenant1**

Login as Tenant at Site A

vm Welcome to VMware Cloud Director

Secure | <https://vcd-01a.corp.local/login/?service=tenant:tenant1&redirectTo=%2F>

HOL Admin Region A Region B

Welcome to
vm VMware Cloud Director

Use your user name to sign in

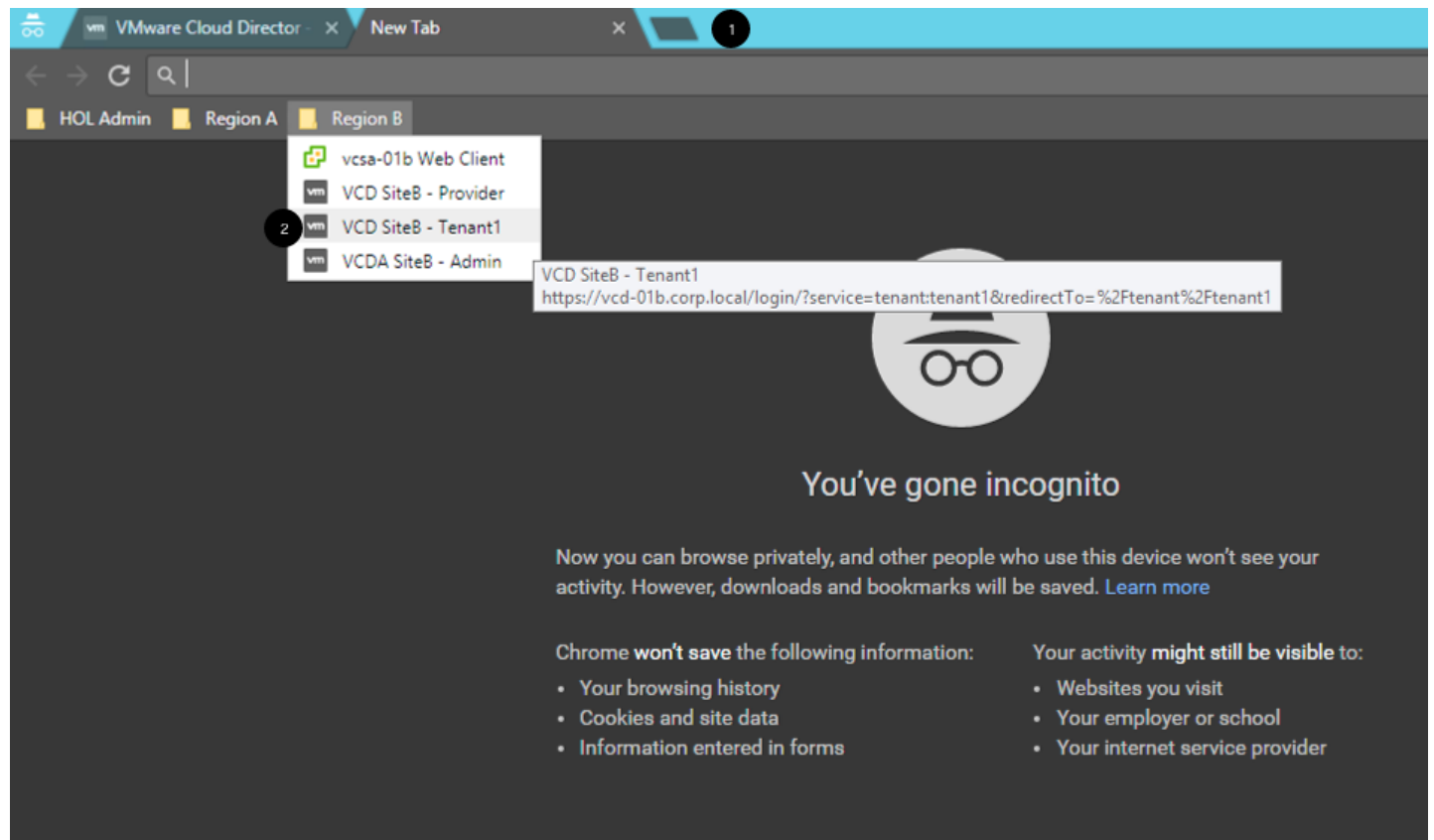
1 t1admin

2 *****

3 SIGN IN

1. Enter Username **t1admin**
2. Enter Password **VMware1!**
3. Click on **SIGN IN**

Open Tenant Site B



1. Click on Region B
2. Click on VCD SiteB - Tenant1

Login as Tenant at Site B

VMware Cloud Director - x Welcome to VMware Clo x

Secure | <https://vcd-01b.corp.local/login/?service=tenant:tenant1&redirectTo=%2Ftenant%2F>

HOL Admin Region A Region B

Welcome to
vm VMware Cloud Director

Use your user name to sign in

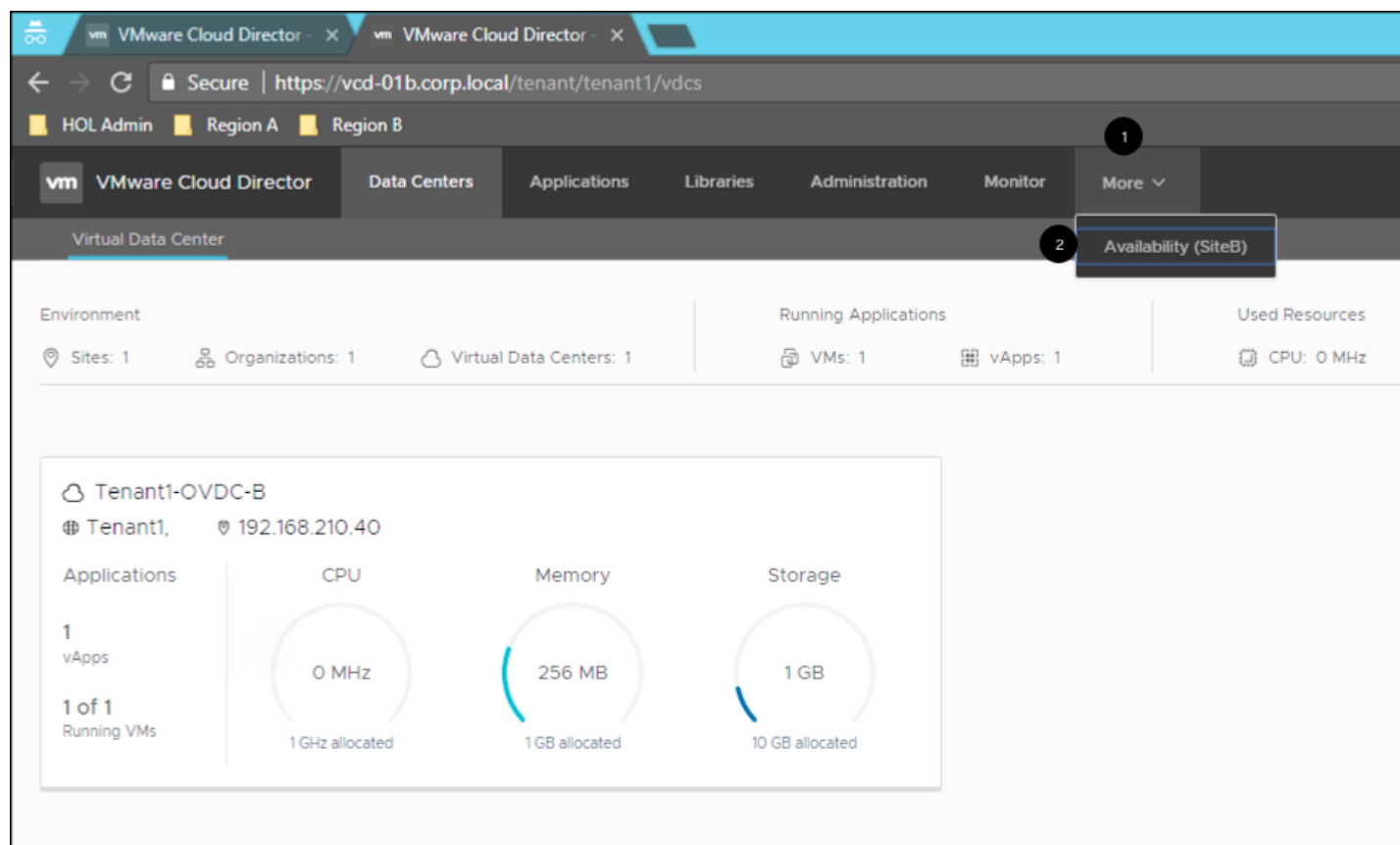
1 t1admin

2

3 SIGN IN

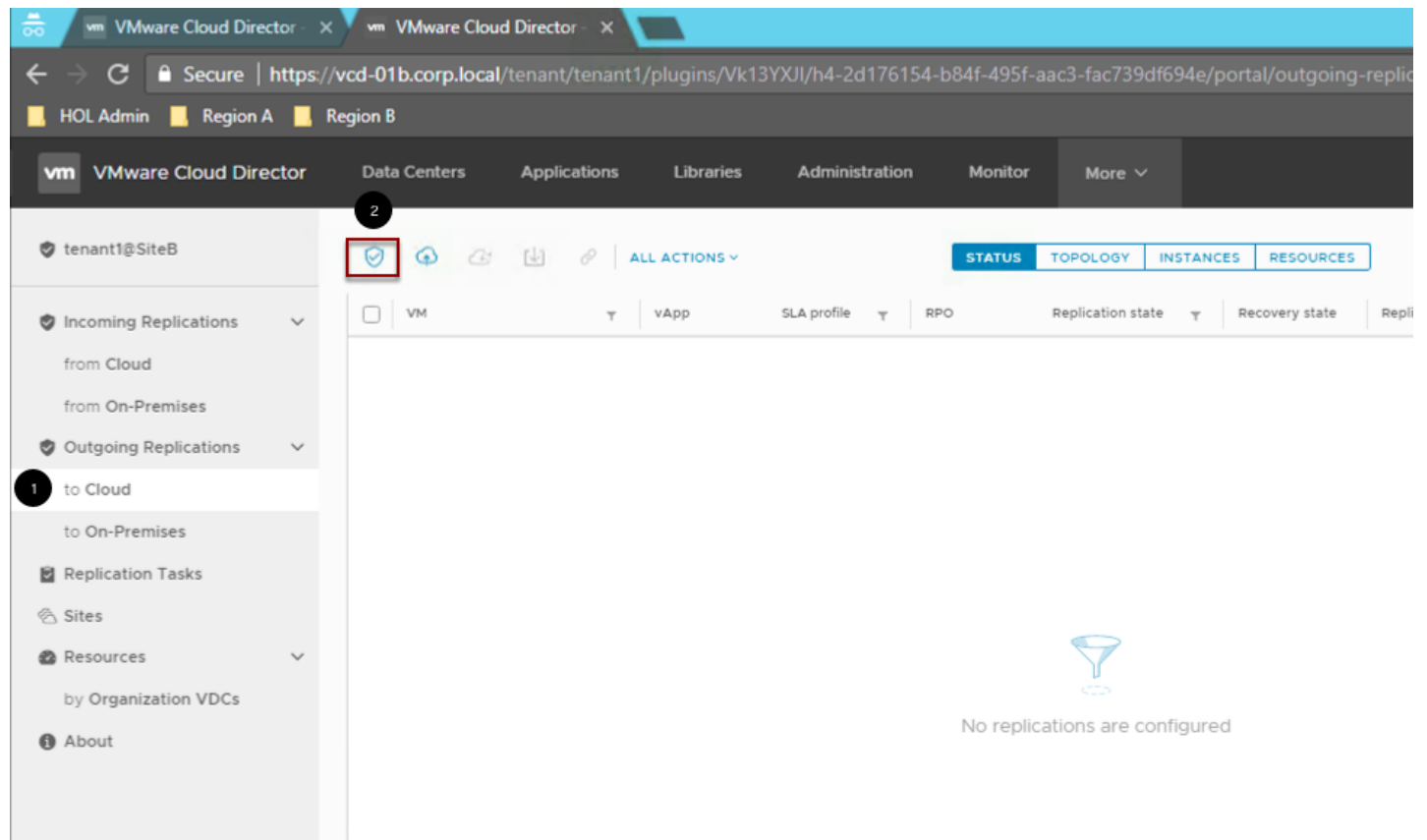
1. Enter Username **t1admin**
2. Enter Password **VMware1!**
3. Click on **SIGN IN**

Open Availability menu at SiteB Tenant



1. Expand **More**
2. Click on **Availability (SiteB)**

Configure New Replication as Tenant from Cloud SiteB to Cloud SiteA



We will now configure replication from Cloud Provider SiteB to Cloud Provider SiteA as Tenant

1. From left panel, Click on **Outgoing Replications to Cloud**
2. Click on **icon for New Protection**

Provide credentials to manage replication at SiteA

New Outgoing Replication

1 Cloud vApps and VMs

2 Destination VDC and Storage policy

3 Settings

4 Ready To Complete

Cloud vApps and VMs

Destination Site: SELECT SITE

EXPAND ALL MORE

vApp / VM	CPUs	Memory	VDC	State
☐ tenant1-photon-01b	(1 VMs)	1	256	Tenan... Ready

0 VMs CLEAR SELECTED

items per page: 20 1 - 1 of 1 results

CANCEL NEXT

1. Enter Username **t1admin@tenant1**
2. Enter Pass **VMware1!**

New Outgoing Replication - Cloud vApps and VMs

New Outgoing Replication

1 Cloud vApps and VMs

2 Destination VDC and Storage policy

3 Settings

4 Ready To Complete

Cloud vApps and VMs

Destination Site: SITEA

EXPAND ALL MORE

vApp / VM	CPUs	Memory	VDC	State
☒ tenant1-photon-01b	(1 VMs)	1	256	Tenan... Ready

0 VMs CLEAR SELECTED

items per page: 20 1 - 1 of 1 results

CANCEL NEXT

1. Check the checkbox for VM **tenant1-photon-01b**
2. Click on **NEXT**

New Outgoing Replication - Destination VDC and Storage policy

New Outgoing Replication

1 Cloud vApps and VMs

2 Destination VDC and Storage policy

3 Settings

4 Ready To Complete

Destination VDC and Storage policy

Select a virtual data center from SiteA to be used as replication target:

REFRESH

Name	Used CPU	Used memory	Used storage	VMs	Quota	Ongoing replications
Tenant1-O...	1000 M	256.00 MB	1.25 GB	1	Currently unavailable	0

Storage policy

Select the new storage policy placement for the recovered VMs

Name	Used	Limit
Any	1.25 GB	10.00 GB

CANCEL

BACK

NEXT

1. Review the defaults and Click on **NEXT**

New Outgoing Replication - Configure Settings

New Outgoing Replication

1 Cloud vApps and VMs

2 Destination VDC and Storage policy

3 Settings

4 Ready To Complete

Settings

SLA profile

SLA profiles are not available for "Tenant1"

Target recovery point objective (RPO)

5 min

30 min

2 hours

8 hours

24 hours

24h

Retention policy for point in time instances

Preserve

4

instances spread evenly over the last

4 days

Delay start synchronization

Set time that is convenient for the first synchronization.

Exclude disks

Save disk space on the target site by excluding disks that are not necessary.

Configure Seed VMs

Use an older copy of the protected VMs on the target site to reduce the data traffic.

CANCEL

BACK

NEXT

Here's brief overview of the parameters -

SLA Profile - The premise of a SLA Profile is to provide a grouping of target settings when protecting a workload. This minimizes the amount of time spent configuring for protection. Think of this as a logical grouping construct which is a single selection to

protect a workload. One does not need to think about what settings to configure. A SLA Profile consists of the following:

- Target Recovery Point Objective (target being the key word here)
- Retention Policy for Point in Time Instances
- Ability to Quiesce or Compress Replication Traffic
- Time select of the synchronization.

Just select SLA profile, and done. You can either use default or custom created SLA profile. SLA profiles are optional and only pertain to protections. They are not utilized for migrations at this time.

Target recovery point objective (RPO) -The RPO is the longest tolerable timeframe of data loss. For example, with one hour RPO the recovered virtual machine can have no more than one hour of data lost. Shorter RPO intervals, ensure less data loss during recovery, at the expense of consuming more network bandwidth to keep the replica up to date.

Retention Policy- Maximum number of retained snapshots per single virtual machine replication within an organization.

Delay start synchronization

- To schedule the start of the replication, select this option and enter the local date and time to start the replication.
- To start the replication when the wizard finishes, leave this option deselected.

Exclude disks - To exclude some hard disks of the virtual machines from replicating to the destination site, select this option.

Configure Seed VMs -For each new replication that you configure, an initial full synchronization operation is performed. During this operation, vCloud Availability copies the whole data from the source vApp or VM to a datastore in the target site. Due to the size of the vApp or VM or to the network bandwidth, an initial full synchronization might take a long time.

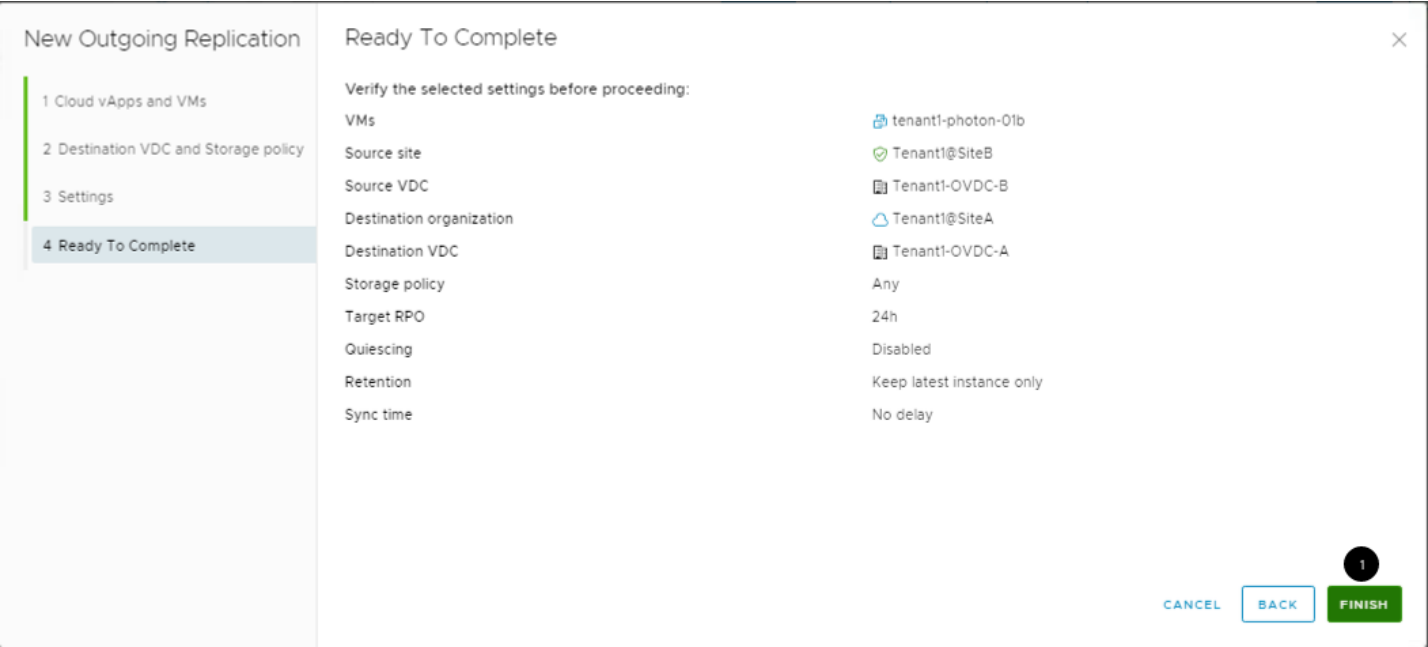
To reduce the initial synchronization time, you copy the source vApp or VM to the target site by using removable media, failover of a previous replication, or other means of data transfer. Then, in the target site, configure a replication that uses the vApp or VM copy as a replication seed.

When a replication uses a seed vApp or VM, vCloud Availability does not copy the whole source vApp or VM data to the target site. Instead, vCloud Availability copies only the different data blocks between the source vApp or VM and the seed and reuses the seed data in the target site as a basis for replication.

We do not have Seed VM available at the target site for this exercise

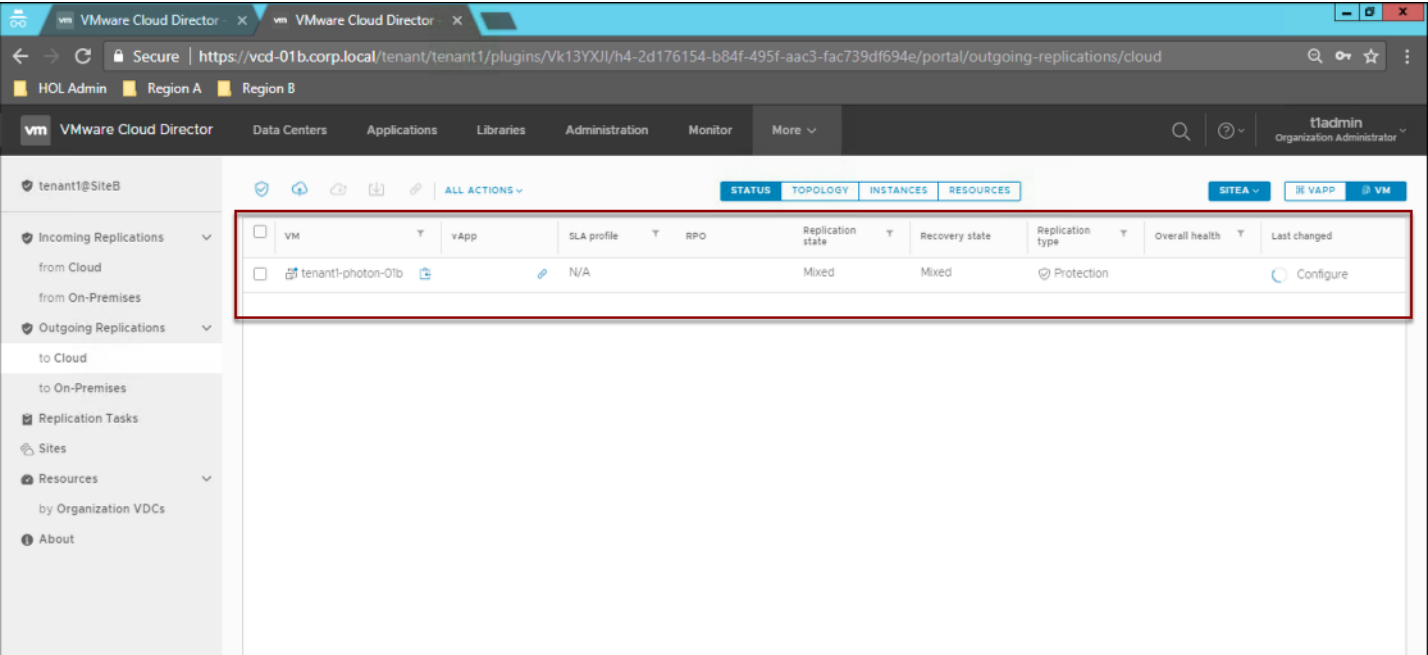
1. Leave everything as Default and Click **Next**

Ready to Complete the Replication



- 1. Review the replication details and click on **FINISH**

Replication in Progress



Review the replication details, it is in progress

Replication is Completed

The screenshot shows the VMware Cloud Director web interface. The left sidebar contains navigation options like 'Incoming Replications', 'Outgoing Replications', 'Replication Tasks', 'Sites', and 'Resources'. The main area displays a table of replication tasks. A red box highlights the first row of the table, which represents a completed replication for a VM named 'tenant1-photon-01b'. The table has columns for VM, vApp, SLA profile, RPO, Replication state, Recovery state, Replication type, Overall health, and Last changed. The 'Replication state' is 'Healthy', 'Recovery state' is 'Not started', 'Replication type' is 'Protection', and 'Overall health' is 'Green'.

VM	vApp	SLA profile	RPO	Replication state	Recovery state	Replication type	Overall health	Last changed
tenant1-photon-01b	tenant1-...	N/A	24h	Healthy	Not started	Protection	Green	7/29/20, 4:47 PM

Verify the Replication status, it may take few minutes to complete. Review the details and Confirm:

1. Replication state is **Healthy**
2. Replication type is **Protection**
3. Overall health is **Green**

Note: In case you see Unexpected vCloud Director error during replication, please retry. Due to the nested environment in Hands On Lab, sometimes the error is seen, in real world it should work seamlessly.

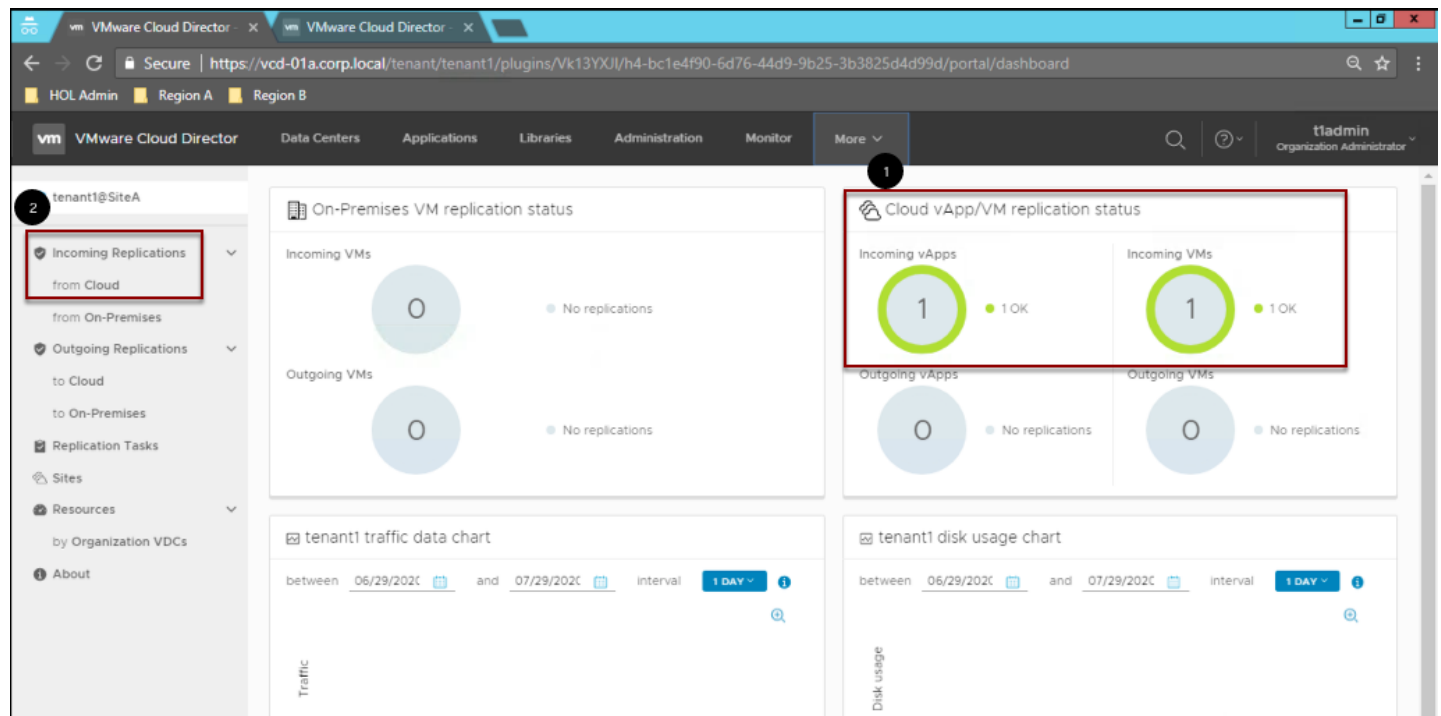
Verify Replication Status at SiteA Tenant

The screenshot displays the VMware Cloud Director web interface. The browser address bar shows the URL `https://vcd-01a.corp.local/tenant/tenant1/vdcs`. The navigation bar includes tabs for 'HOL Admin', 'Region A', and 'Region B'. Below this, a secondary navigation bar contains links for 'VMware Cloud Director', 'Data Centers', 'Applications', 'Libraries', 'Administration', 'Monitor', and a 'More' dropdown menu. The 'More' menu is expanded, revealing the 'Availability (SiteA)' option, which is highlighted by a blue box and a red arrow. The main content area shows a summary of the environment, including 'Sites: 1', 'Organizations: 1', 'Virtual Data Centers: 1', 'Running Applications: VMs: 1', 'vApps: 1', and 'Used Resources: CPU: 1 GHz'. Below this, a detailed view for 'Tenant1-OVDC-A' is shown, including a table of applications and their resource usage.

Applications	CPU	Memory	Storage
1 vApps	1 GHz	256 MB	1 GB
1 of 1 Running VMs	2 GHz allocated	1 GB allocated	10 GB allocated

1. Switch to tab **Cloud Site A**
2. Expand **More**
3. Click on **Availability (SiteA)**

Verify Incoming Cloud vApp/VM Replication Status at SiteA Tenant



1. You can notice **Incoming VM replication status as Green**
2. From left panel, click on **Incoming Replication from Cloud**

Confirm Incoming Cloud vApp/VM Replication Status at SiteA Tenant

The screenshot shows the VMware Cloud Director interface for the 'tenant1@SiteA' tenant. The left sidebar shows the navigation menu with 'Incoming Replications' selected. The main content area displays a table of incoming replications. A red box highlights the first row of the table, which represents a vApp named 'tenant1-photon-01b'.

VM	vApp	SLA profile	RPO	Replication state	Recovery state	Replication type	Overall health	Last changed
☐	tenant1-photon-01b	N/A	24h	Healthy	Not started	Protection	Green	7/29/20, 4:47 P...

Confirm the Replication State is Healthy and Overall health is Green

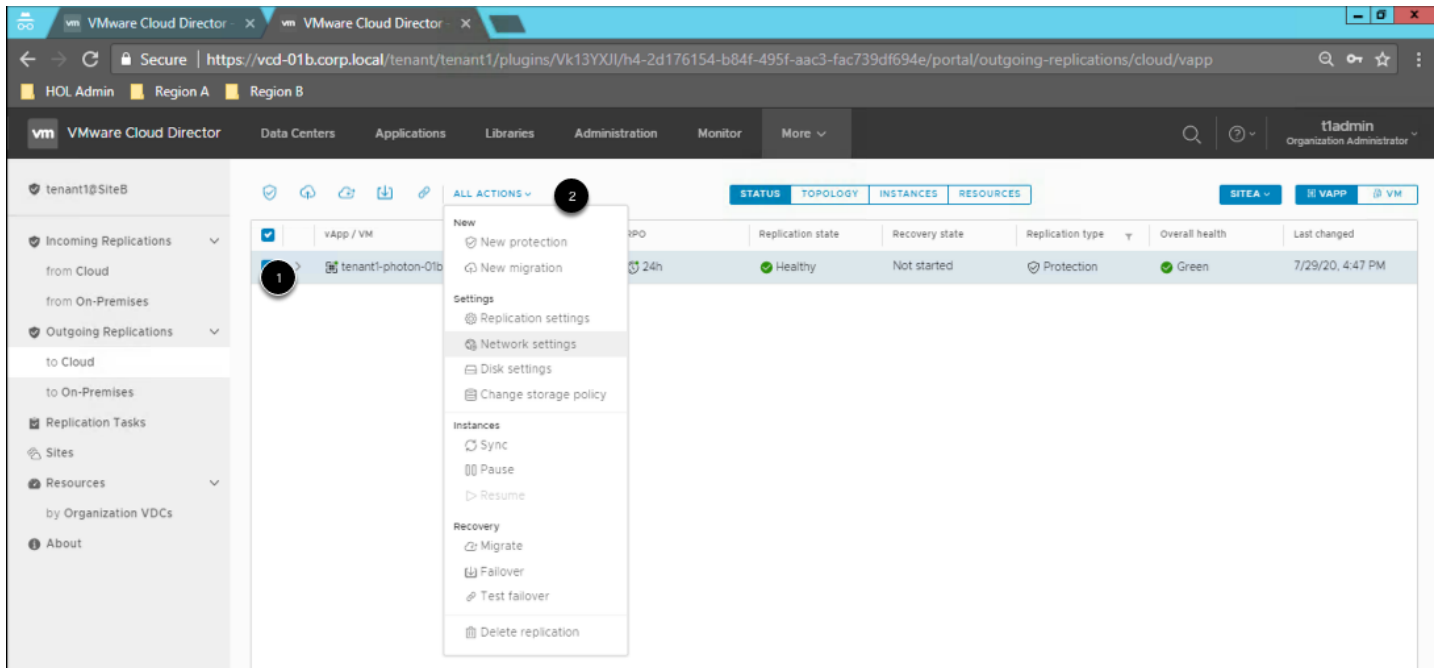
Switch to Cloud SiteB Tenant to configure network for Replicated VM

The screenshot shows the VMware Cloud Director interface for the 'tenant1@SiteB' tenant. The left sidebar shows the navigation menu with 'Outgoing Replications' selected. The main content area displays a table of outgoing replications. Red circles 1 and 2 highlight the tenant switch and the vAPP button respectively.

vApp / VM	SLA profile	RPO	Replication state	Recovery state	Replication type	Overall health	Last changed
> tenant1-photon-01b	N/A	24h	Healthy	Not started	Protection	Green	7/29/20, 4:47 PM

1. Switch back to **SiteB Tenant**
2. In the upper right-hand corner, click on **vAPP**

Configure Networks for Replicated VM



Before we can run Recovery of the replicated VM in Cloud, we need to configure a Test/Failover Network. This Network would be connected to the Recovered VM.

For the cloud to cloud replications, VMware Cloud Director Availability replicates all the types of source vApp networks in the target cloud site: Isolated, bridged (direct) and fenced (NAT-routed) networks. VMware Cloud Director Availability replicates the source networks settings like: IP pools, NAT routes, firewall rules, and DNS settings, in the target site.

1. Check the checkbox for **VM tenant1-photon-01b**
2. Expand **ALL ACTIONS**
3. Click on **Network Settings**

Configure Network Settings for Replicated VM

Network Settings | tenant1-photon-01b

Apply to all vApps NETWORK IP MODE MORE EXPAND ALL

Source vApp networks	Connect to target org VDC network	Connected	Primary nic	MAC address	Reset MAC	IP mode	IP address
tenant1-photon-01b	None	☒			☐	Static - IP Pool	192.168.245.101

CANCEL APPLY

In this screen, we can configure the target networks to be used for migration/failover as well as test failovers. For this lab, we will just configure the Migrate/Failover network.

1. In the dropdown for connect to target org VDC network, select **Tenant1-OVDC-A-OrgNet-Rtd**
2. Set IP Mode to **Static - IP Pool**
3. Click on **APPLY**

Run Failover to Cloud SiteA

tenant1@SiteB

Incoming Replications

from Cloud

from On-Premises

Outgoing Replications

to Cloud

to On-Premises

Replication Tasks

Sites

Resources

by Organization VDCs

About

tenant1-photon-01b

ALL ACTIONS

New

- New protection
- New migration

Settings

- Replication settings
- Network settings
- Disk settings
- Change storage policy

Instances

- Sync
- Pause
- Resume

Recovery

- Migrate
- Failover
- Test failover
- Delete replication

STATUS TOPOLOGY INSTANCES RESOURCES

SITEA VAPP VM

SPO	Replication state	Recovery state	Replication type	Overall health	Last changed
24h	Healthy	Not started	Protection	Green	7/29/20, 4:47 PM

Now that the VM is successfully replicated in Cloud, we will run Failover workflow such that VM will now run in Cloud SiteA

1. Check the checkbox for VM **tenant1-photon-01b**
2. Expand **ALL ACTIONS**
3. Click on **FAILOVER**

Failover in Cloud - Recovery Settings

Failover

- 1 Recovery Settings
- 2 Recovery Instance
- 3 Ready To Complete

Recovery Settings

Select configuration for the recovered VMs

☐ Consolidate VM disks

Turning on this option will consolidate all instances into the recovered disk.
This can improve the runtime performance of the recovered VM, but may greatly increase RTO.

☒ Power on recovered vApps

Network Settings

☒ Apply preconfigured network settings on failover

☐ Connect all VMs to network ▼

CANCEL **1** **NEXT**

Brief overview of the parameters on this page

Consolidate VM disks - Enable for a better performance of the recovered virtual machines at the expense of the failover task taking longer to complete.

Power on recovered vApps - Select to power on the virtual machines on the destination site after the task completes.

Network settings

-Apply preconfigured network settings on failover will assign the network configured during the virtual machine replication.

-Connect all VMs to network will allow you select a target network on the fly during a failover

1. Because we already configured a target network, leave the default setting and click **NEXT**

Failover - Recovery Instance

The screenshot shows a web interface for configuring a failover recovery instance. On the left is a sidebar titled 'Failover' with three steps: '1 Recovery Settings', '2 Recovery Instance' (which is highlighted), and '3 Ready To Complete'. The main area is titled 'Recovery Instance' and contains the instruction 'Select recovery point in time.' Below this, there is a light blue rectangular area representing a timeline. A blue dot is placed on this timeline, and below it, the text 'tenant1-photon-01b' is displayed. At the bottom left of the timeline area, the date and time '7/29/20, 4:47 PM' are shown. In the bottom right corner of the main area, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'. The 'NEXT' button is highlighted in blue and has a small black circle with the number '1' above it, indicating the current step.

1. Select the latest available Instance and click on **NEXT**

Ready to Complete the Failover Settings

Failover

1 Recovery Settings

2 Recovery Instance

3 Ready To Complete

Ready To Complete

Verify the selected settings before proceeding:

Recovered vApps

Recovery site

Recovery network

Synchronize VM changes

Power on recovered vApps

Consolidate VM disks

tenant1-photon-01b

SiteA

Preconfigured network settings

Manually selected instance

Enabled

Disabled

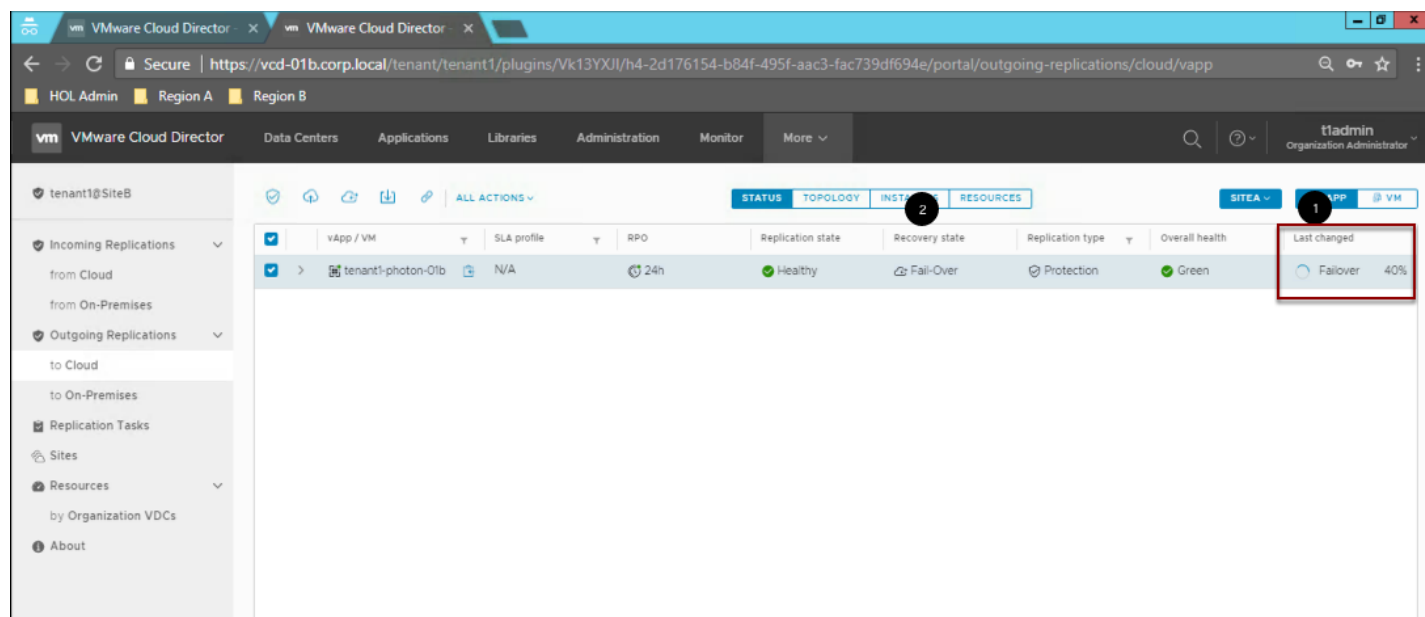
CANCEL

BACK

1FINISH

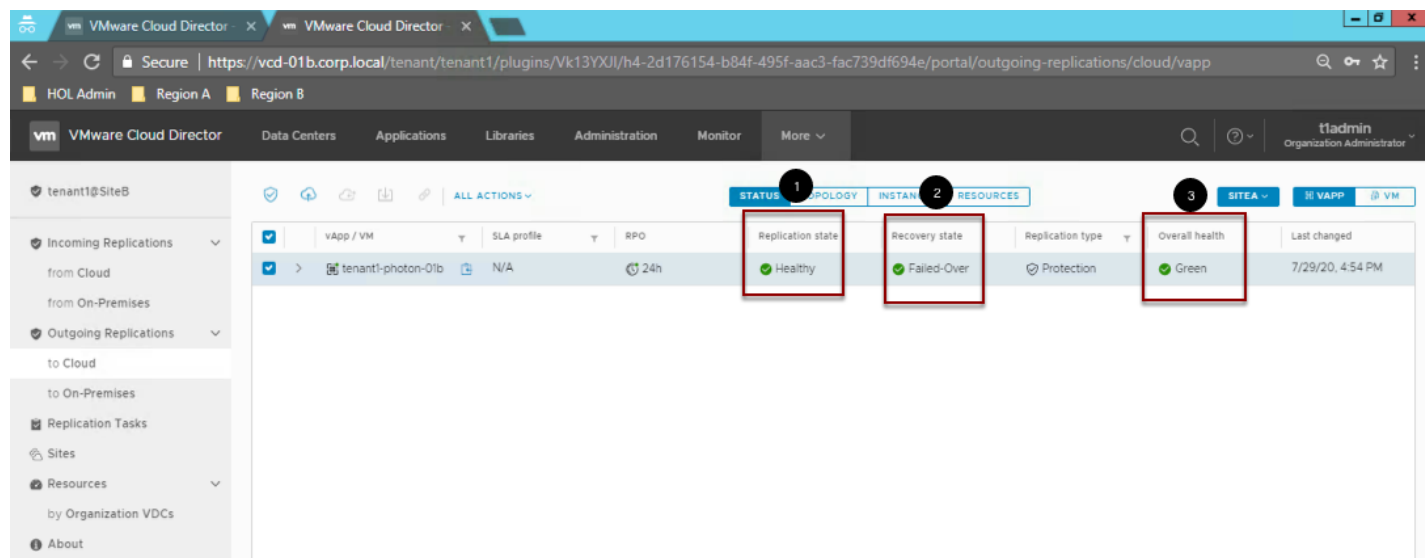
1. Review the Failover Settings and Click on **FINISH**

Failover to Cloud SiteA is in Progress



1. In the Detailed Status, you will notice **Failover in Progress**.
2. Recovery State is updated to **Fail-Over**

Failover completed successfully



This process will take a couple of minutes. Please be patient.

1. Replication State is **Healthy**
2. Recovery State shows **Failed-Over**.
3. Overall health is **Green**

Note: In case you see Unexpected vCloud Director error during failover, please retry. Due to the nested environment in Hands On Lab, sometimes the error is seen, in real world it should work seamlessly.

Verify Failover is successful at Cloud Provider SiteA

The screenshot shows the VMware Cloud Director web interface. The browser address bar indicates the URL: <https://vcd-01a.corp.local/tenant/tenant1/plugins/Vk13YXJl/h4-bc1e4f90-6d76-44d9-9b25-3b3825d4d99d/portal/incoming-replications/cloud>. The user is logged in as 't1admin' (Organization Administrator). The left sidebar shows the 'Incoming Replications' menu item selected. The main table displays the following data:

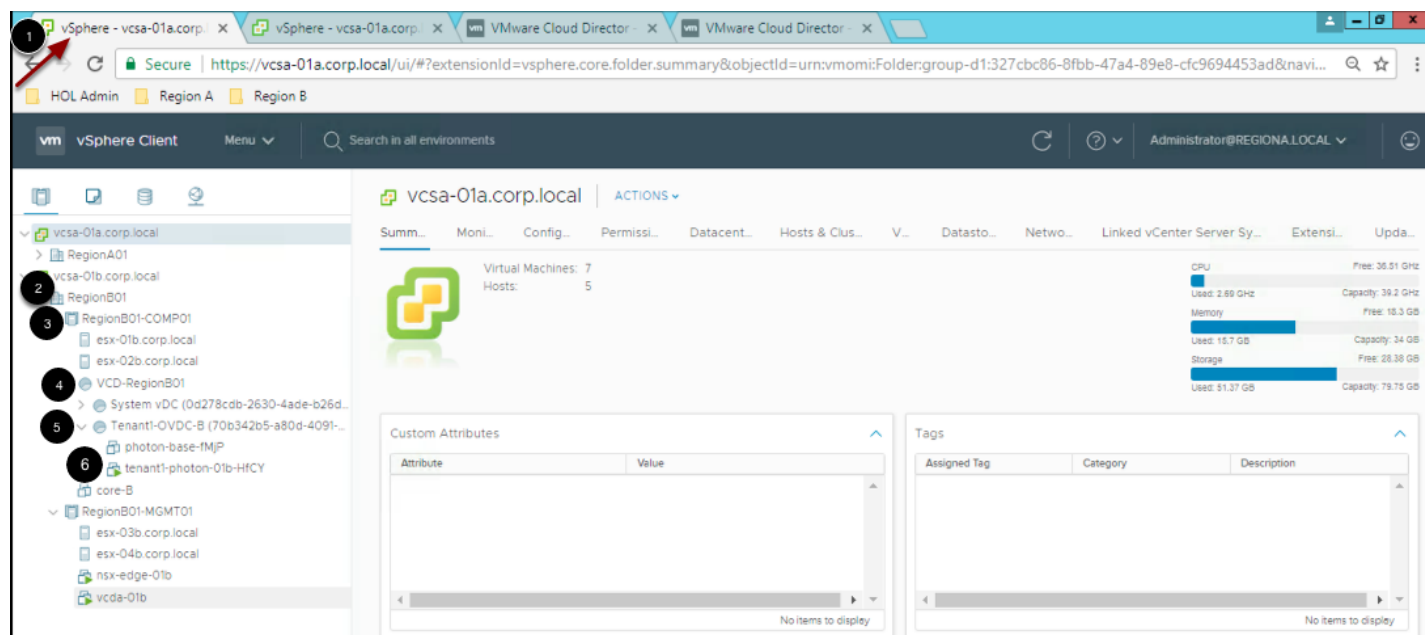
VM	vApp	SLA profile	RPO	Replication state	Recovery state	Replication type	Overall health	Last changed
tenant1-photon-01b	tenant1	N/A	24h	Healthy	Failed-Over	Protection	Green	7/29/20, 4:54 P...

Lets confirm that Failover is completed successfully from Cloud Provider SiteA

1. Switch to SiteA Tenant
2. Click on **Incoming Replications from Cloud**
3. Replication State is **Healthy**
4. Recovery State shows **Failed-Over**.
5. Overall health is **Green**

Note: In case you see Unexpected vCloud Director error during failover, please retry. Due to the nested environment in Hands On Lab, sometimes the error is seen, in real world it should work seamlessly.

Verify Failed-Over VM is now running in SiteA



1. Switch back to Chrome browser **vCenter SiteA**
2. On the left panel expand **RegionB01**
3. Expand **RegionB01-COMP01**
4. Expand **vCD-RegionB01**
5. Expand **Tenant1-OVDC-B**
6. Verify VM **tenant1-photon-01b-xxxx** is now powered on in SiteA inventory

Congratulations!! You completed the Tenant driven Pairing and Recovery Workflows between the Cloud Provider Sites.

Conclusion

In this module, we covered Tenant Self Service Replication and Failover workflows from Cloud to Cloud using VMware Cloud Director Availability

You've finished Module 4

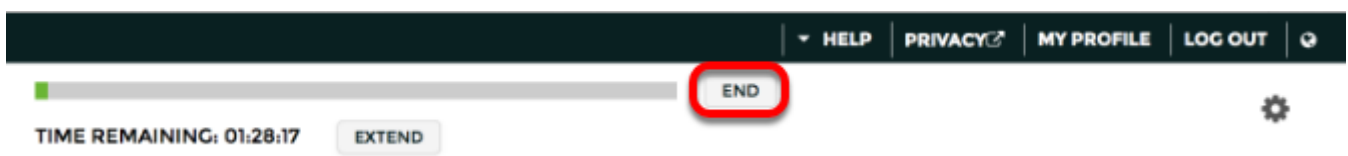


Congratulations on completing Module 4!!

Here are links to other modules in the lab you may be interested in:

- [Module 1 - VMware Cloud Director Availability Overview and Architecture](#) (15 minutes) (Basic) This module will show an overview of the architecture and deployment of VMware Cloud Director Availability 4.0
- [Module 2 - On-Prem DR and Migration to Cloud with VMware Cloud Director Availability](#) (45 Minutes) (Basic) This module will walk through the steps to pair On-Premises site with Cloud and how to use VMware Cloud Director Availability for disaster recovery and migration from on-prem to cloud.
- [Module 3 - Administrator-driven Cloud-to-Cloud DR with VMware Cloud Director Availability](#) (30 minutes) (Basic) This module will show how administrators can use Cloud Director Availability for cloud-to-cloud DR workflows.

How to End Lab



To end your lab click on the **END** button.

Conclusion

Thank you for participating in the VMware Hands-on Labs. Be sure to visit <http://hol.vmware.com/> to continue your lab experience online.

Lab SKU: HOL-2182-01-HBD

Version: 20200929-224906