

VELOSTRATA VM MIGRATION AND OPERATIONS

Table of Contents

Migration Workflow and Planning	4
Migration Workflows	5
Operating Systems Adaptations.....	6
UEFI Support for Windows Migrations	8
Cloud Instance Rightsizing Overview	9
Monitoring VM Usage	10
Setting Bandwidth Throttling for Migration.....	12
VM Migration Operations	14
Running a VM in the Cloud	15
Running a VM Back On-Prem/On Source	37
Running a Test Clone	41
Delete a Test Clone	57
Running the Migration Wizard.....	60
Detaching the VM.....	81
Cancelling the Detach.....	86
Starting the Detach Cleanup.....	88
VM Migration - Advanced Operations	92
Migrating VM Storage to the Cloud.....	93
Preparing to Detach the VM	96
Reconfiguring a VM.....	103
Shutting Down a VM in the Cloud	106
Powering on a VM in the Cloud	108
Restarting a VM in the Cloud	110
Monitoring a VM when Running in Cloud	111
Migrating Physical Servers	112
Using Offline Migration	122
Monitoring Velostrata	132
Understanding Velostrata Health Checks	133
Monitoring the Cloud Extension	135
High Availability Overview.....	137

Viewing the Cloud Extension Status	138
Viewing Velostrata vCenter Alarms and Events	143
Viewing the Velostrata vSphere Connectivity Alarm in the Velostrata Manager	145
Viewing the Cloud Instance Console Log or Screenshot.....	147
Saving a Support Bundle in the Velostrata Manager.....	149
Automatically Moving a Terminated VM to On-Premises	151
Troubleshooting Cloud Edge Components.....	152
Understanding the Velostrata Telemetry Service	153
Deploying Velostrata Prep Package for Linux Virtual Machines	157
Supported Linux Distributions and Versions.....	158
How-to: Red Hat Enterprise Linux (RHEL) 6/7 and CentOS 6/7 Prep for Run in GCP/AWS/ Azure.....	159
How-to: SUSE Enterprise Linux Server (SLES) 11/12 Prep for Run in GCP/AWS/Azure.....	161
How-to: Ubuntu 14/16/18 Prep for Run in GCP/AWS/Azure	162
Light Transformation Scripts.....	163
Customization Scripts Overview.....	164
Platform and Environment Detection	165
Windows.....	166
Linux	168
Environment Setting.....	170
Multiple IP Support in GCP Cloud	171
External DNS in GCP Cloud	173

Migration Workflow and Planning

Migration Workflows

Velostrata enables you to rapidly perform migration operations on single or multiple VMs directly from vCenter. These operations can include run-in-cloud, migrate, test clone, etc. Using the vCenter UI to accomplish these tasks is fast and only requires a few clicks. Plus, these operations complete quickly, often in a matter of minutes, empowering fast, simple migrations.

Alternatively, for more complex applications, you can also use our runbook automation feature which lets you take an inventory of available VMs, then define a very specific order for those migrations to take place. This is valuable when you are looking to automate the migration of a more complex app with dependencies.

Here is the general overview of the phases you are likely to encounter while using Velostrata:

Phase 1: Model (For more complex applications)

- Capture VM inventory using Velostrata's Runbook Automation.

Phase 2: Test before you migrate (Optional)

- Create a copy of a running on-premises Workload and run it in cloud. This enables you to test an application in cloud without disrupting the live production system. The clone can be fully operational within minutes. See [Running a Test Clone](#).

Phase 3: Fast cutover to cloud

Once you have completed testing on the clone, get the application and data live in the cloud in minutes. Data syncs back to on-prem as a safety net. The remaining data is migrated in the background.

1. While your VM is on-premises or at source cloud, make any necessary adjustments, for example, lower the TTL on the DNS, consider any IP address issues, and so on.
2. Move the VM to destination cloud. See [Running a VM in the Cloud](#). Once this is completed, perform any validation/sanity tests and deploy any fixes.
3. Migrate the storage to the destination cloud. See [Migrating VM Storage to the Cloud](#).
4. Prepare to detach the VM. This takes the data from the cloud storage and writes it to cloud drives. See [Preparing to Detach](#).

Note: Steps 2 to 4 (above) can be accomplished all together by [Running the Migration Wizard](#) or using [Runbook Automation](#).

Phase 4: Detach

1. Once the preparing to detach task completes successfully, you can detach the VM. You must assign a scheduled downtime slot for detaching. See [Detaching the VM](#).
2. After detaching the VM, perform any required validation, and then either cleanup or rollback (if you do not want to detach the VM from Velostrata). See [Starting the Detach Cleanup](#)

Operating Systems Adaptations

This topic describes the changes performed by the Velostrata RPM, as well as the VM modifications made for the run-in-cloud and detach operations for both Windows VMs and Linux VMs.

Changes Performed by Velostrata RPM

The Velostrata RPM prepares the Linux machine for booting in cloud using the Velostrata solution. The package can remain installed when the VM is running in VMware on-premises/Source cloud, as changes are activated only when detecting a run-in-cloud operation. Upon removal of the package, all changes are reverted.

The set of changes made to the system are:

- Enable boot in-cloud integration.
- Enable serial console log integration.
- Cloud-specific changes for the Velostrata storage channel.
- Hardware-specific adaptations for cloud migration.

For more detailed technical information, contact Velostrata support.

VM Modification for Run in Cloud – Windows VM

When you move a VM to the cloud, Velostrata shuts down the VM gracefully, and takes a safe point snapshot of the VM prior to its move to the cloud.

Modifications to the networking and storage drivers are then made to allow the VM to boot in the cloud.

- Install driver: NETKVM driver installation for GCP.
- Change network configuration.
- System tuning for iSCSI and MPIO access.
- Change license/edition.
- Disable VMware tools.
- Change page file location.
- Ensure hibernation is disabled.
- Change recovery options.
- Enable RDP.
- Deploy Velostrata framework that allows you to run custom actions

VM Modification for Run in Cloud – Linux VM

The Velostrata RPM is required to be installed before migrating to the cloud.

When you move a VM to the cloud, Velostrata shuts down the VM gracefully (if it is running this requires VMware Tools to be installed in the VM), and takes a safe point snapshot of the VM prior to its move to the cloud. Modifications to the networking and storage drivers are then made to allow the VM to boot in the cloud.

- Make the necessary changes to the boot sequence in order to boot in cloud (initrd).
- Enable serial console log integration.
- Make changes specific to GCP as needed.
- The following modifications are dynamically applied in the cloud:
 - Remount mounts with the `_netdev` option to support the proper shutdown sequence.
 - Remap swap files.
 - Start Velostrata keep-alive service.
 - Perform disk optimizations.
 - Perform network configuration adaptation including the following:
 - **Remove static IPs and routes:** Most migrated systems are preconfigured to static network environments, which includes pre-defined IPs, gateways, routes, network cards, etc. Cloud environments, however, only allow DHCP configuration with network topology managed outside of the VM itself. RPM contains built-in actions to remove all static configuration and reconfigure the default network interface (typically `eth0`) with DHCP.
 - **Primary IP of hostname is updated in `/etc/hosts`:** Some migrated applications rely on `/etc/hosts` to extract local IP address based on the `/etc/host` entry. When the VM/application is moved to cloud this involves, among other changes, change of the IP address. RPM contains built-in actions to correct `/etc/hosts` with the new IP address to preserve compatibility with migrated applications.

VM Modification for Detach – Windows VM

During detach of a Windows VM, Velostrata performs a cloud agent installation as recommended by GCP, via a VM agent for Windows

Note: These changes are in addition to those made for the run-in-cloud operation.

VM Modification for Detach – Linux VM

To ensure proper Linux boot and functionality after detach, the framework includes the following built-in actions for detached VMs:

- Further tuning of the network configuration.

Note: These changes are in addition to those made for the run-in-cloud operation.

UEFI Support for Windows Migrations

UEFI (Unified Extensible Firmware Interface) replaces the basic BIOS firmware originally present in most Windows PCs. Utilizing UEFI offers the user various advantages around security and disk management. VMware introduced support for UEFI with vSphere 5.0. As a result, it is possible you are utilizing UEFI on some of the VMs running in your datacenter.

Cloud providers, however, do not support UEFI, so we have developed a special transformation process that will automatically convert UEFI systems to the MBR format during migration. This process, however, has some limitations that are important:

1. This process is only currently supported on Windows systems
2. This process supports a maximum of 4 visible partitions on the source system.
 1. *Additional details:* GPT layouts typically include four partitions: Recovery, EFI (BCD), Reserved (hidden), and at least one user data partition. During our conversion, the reserved partition will be removed. As a result, migrated systems can support two user partitions on the boot disk (for example, a C and a D drive).
3. Supports drives up to 2TB
4. Software RAID and Dynamic Disks are not supported.
5. Systems will be migrated in write-isolation mode, which means any changes to the data is not synchronized back with the on-prem system.
6. You can still perform a rollback to on-premises operation, but it is no longer stateful. As in, the system in the cloud will turn off, and the system on-prem will boot back up, but the data changes made in the cloud will not persist to the on-prem system.

When systems meet the requirements above, the conversion will take place automatically when a user selects a system to migrate to the cloud. If the requirements are not met, you will receive an appropriate error message for diagnosis.

Important Note: as mentioned in step 5, it is important to re-iterate that write back is ***not*** supported when migrating machines that are configured with UEFI at source.

Cloud Instance Rightsizing Overview

When moving a virtual machine to the cloud, the question of instance rightsizing comes up - out of the many different instance types and sizes offered, which should you choose? Velostrata has developed a rightsizing feature to help answer this question. The feature includes built-in usage monitoring and a recommendation engine that provides cost- and performance-optimized cloud instance type and size recommendations.

Based on the user indicating which of the virtual machines to watch, the Velostrata virtual appliance on-premises starts collecting and analyzing utilization statistics, at a fine resolution, from VMware vSphere. The observed activity patterns are then classified into utilization buckets, based on which memory and CPU needs are estimated.

For better recommendation accuracy, Velostrata recommends at least 7 active days as a watch period, or a typical business cycle for the monitored workloads. A warning is shown when the activity period recorded is insufficient in order to provide a recommendation with an adequate confidence level. Nevertheless, a cost-optimized recommendation is still offered based on the available observation.

Cost-optimized recommendations are based on the observed utilization and activity classification. Performance-optimized recommendations are based on the provisioned VM's characteristics. Such recommendations are available in the Run In Cloud, Test Clone, Migrate and Offline Migration operations, and are accessible in the vCenter Web Client user interface, PowerShell module, REST API, and Automation Runbook Tool for mass migration planning.

For each operation where recommendations are presented, the virtual machine's provisioned vCPUs, RAM and number of disks are indicated, as well as the observed CPU and RAM usage classification. Recommendations include three options performance-optimized cloud instance options, as well as three cost-optimized options. The cumulative monitoring and active durations are indicated in days. In the vCenter Web Client wizards, the lowest cost performance-optimized option is selected by default. Clicking any other option sets the target instance selection accordingly. Only relevant options are presented, based on the number of disks, storage type and supported types by region as applicable to the target cloud in which the previously selected Velostrata CloudExtension resides.

Presented options also include expected monthly costs. These are to be used as relative cost indicators and not used for actual billing forecasting purposes. The expected cost uses on-demand compute price lists only, and does not include disk and network costs, and does not consider reduced cost options such as discount agreements, pre-purchased compute and reserved instances, spot and pre-emptive instances, or other price reduction plans. If the online price list is not accessible (internet access required), no cost-optimized recommendations are provided.

Monitoring VM Usage

Velostrata has a built-in recommendation engine that provides cost- and performance-optimized recommendations when:

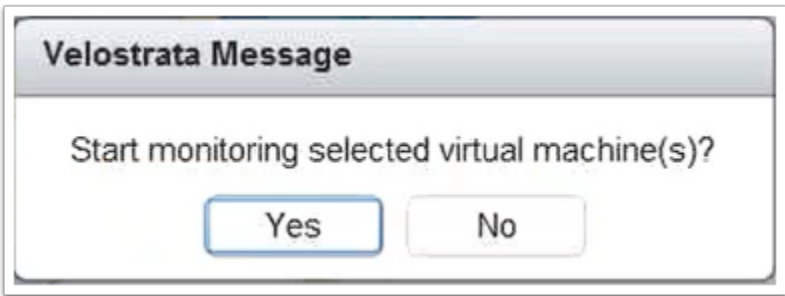
- Running a VM in the cloud.
- Running a test clone.
- Migrating a VM to cloud.

This functionality is available for AWS, Azure and GCP.

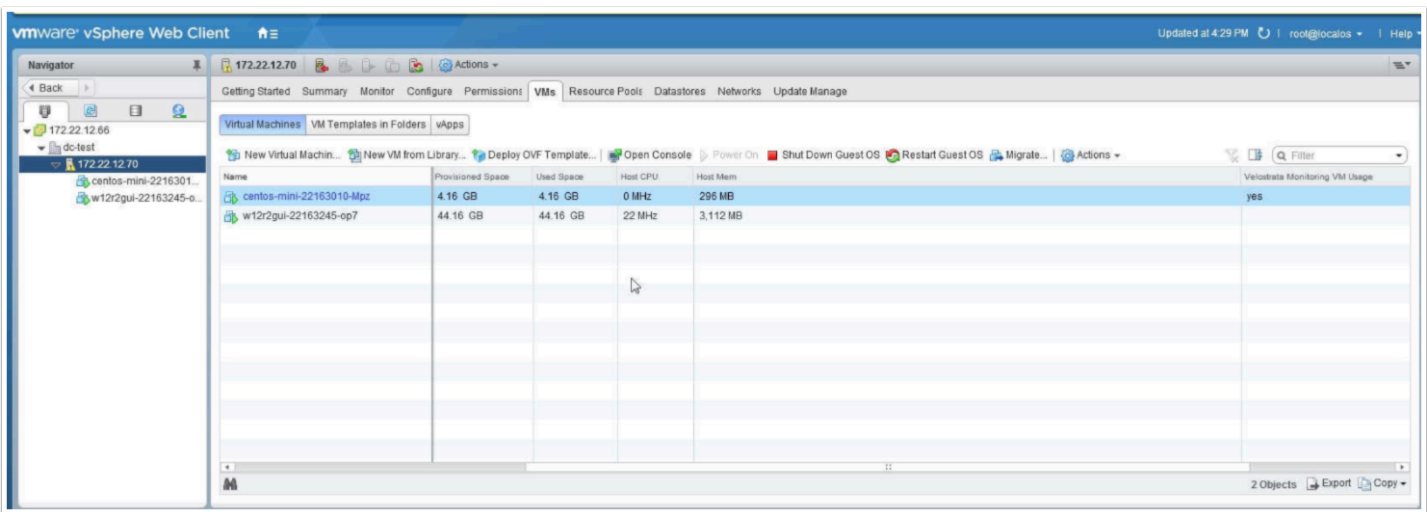
In order to provide an effective recommendation, Velostrata recommends monitoring the VM usage for at least 7 active days.

To start monitoring a VM:

1. On the vSphere Web Client, select the desired VM or VMs.
2. Right-click on the VM or VMs and select **Velostrata Operations > Start Monitoring Usage**.

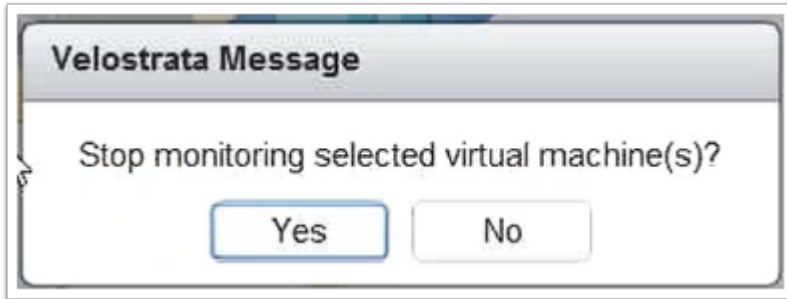


3. Click **Yes**. A **yes** appears in the **Velostrata Monitoring VM Usage** column.



To stop monitoring a VM:

1. On the vSphere Web Client, select the desired VM or VMs.
2. Right-click on the VM or VMs and select **Velostrata Operations > Stop Monitoring Usage**.



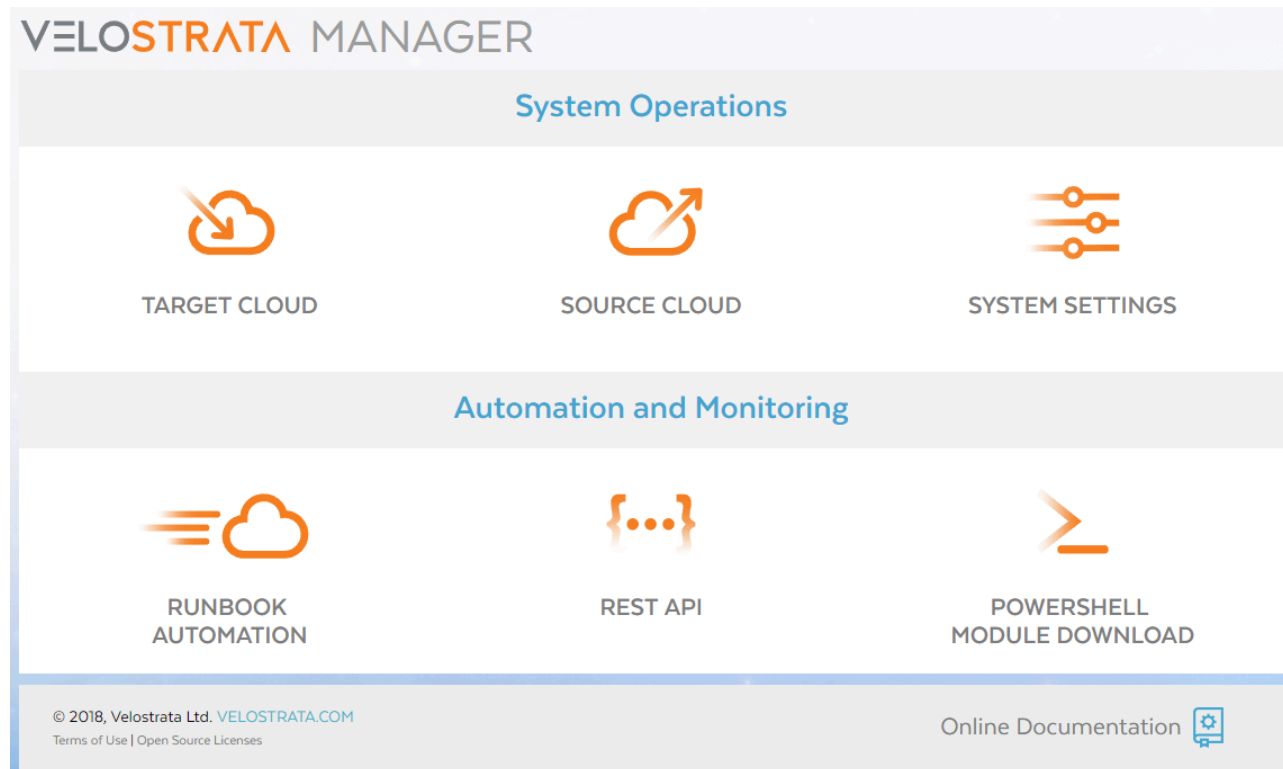
3. Click **Yes**.

Setting Bandwidth Throttling for Migration

You can prevent network saturation for migration loads by setting bandwidth throttling for migration traffic (this does not apply to on-demand traffic).

Via Velostrata Web Management

1. Open a Web browser and navigate to the Velostrata Manager Virtual Appliance IP address.



2. Click **System Settings**.

3. Login with username 'localsupport' and use your Velostrata Subscription ID (or GCP billing ID) as your password.

4. Click the **Network settings** tab.

[Logs](#)
[vCenter Plugin](#)
[Network Settings](#)

eth0

Raw configuration: iface eth0 inet dhcp

[eth1 configuration](#)
☐ Set storage migration rate limit to Mbps

Save



5. Check the box next to **Set storage migration rate limit to**
6. Enter the limit in megabits per second (maximum value of 10000000).
7. Click **Save**.

VM Migration Operations

Running a VM in the Cloud

When you move a VM from on-prem to the cloud, Velostrata shuts down the VM gracefully if it is running (requires VMware Tools to be installed in the VM), and takes a safe point snapshot of the VM prior to its move to the cloud. While moving a VM to the cloud you can:

- Scale up the VM and assign it more CPU and RAM resources by selecting an appropriate cloud instance type.
- Select a storage policy.

Velostrata includes a built-in rightsizing engine that provides cost- and performance-optimized recommendations. In order to provide an effective recommendation, Velostrata recommends monitoring the VM usage for at least 7 active days.

To run a VM in GCP from on-premises or another cloud, follow the appropriate steps, below:

Run on-prem VM in GCP

1. On the vSphere Web Client, select the desired **Virtual Machine**.
2. Right-click on the VM and select **Velostrata Operations > Run in Cloud**.



3. Select the **Velostrata Cloud Extension**.
4. The Cloud VM Name is filled in automatically from the VM. Modify the **Cloud VM Name** as required.

Note: From version 3.1, the random trailing suffix is no longer added to the name.

Run In Cloud - centos-mini-12125557-s3u

Velostrata Cloud Extension

Cloud Instance
Storage Policy
Networking
Summary

Velostrata Cloud Extension

Velostrata Cloud Extension: gcp_datacenter-2_1520852157_xpl

Cloud VM Name: centos-mini-12125557-s3u

Back Next Finish Cancel

Note: If you select a Cloud Extension that is impaired, (Impaired) is appended to the Velostrata Cloud Extension name. It is not recommended to move a VM to run in an impaired Cloud Extension. For more information, see [High Availability Overview](#).

5. Click **Next**.
6. Select the **Project** and **Instance Type** (VM size). Three options are recommended for performance-optimized VMs, and three options are recommended for cost-optimized VMs.
Note: The prices are for compute cost only and do not include disk and network costs.
Note: If the VM has not been monitored for a sufficient period (7 days), a message appears indicating that the activity duration may be insufficient for accurate recommendations.
Note: If the online price list is not available, no cost-optimized recommendations are provided.

Run In Cloud - centos-mini-04135336-30y

✓ Velostrata Cloud Extension

Cloud Instance

Storage Policy

Networking

Summary

Cloud Instance

Source VM	Provisioned	Observed Usage	Monitoring Duration:	Not monitored
CPU:	2	No information	Active Duration:	Not monitored
RAM:	2GB	No information		
Disks:	1			

Recommended Options:

Performance Optimized	Monthly Cost (Pay-As-You-Go)
n1-standard-2 (2 CPUs 7.5 GB RAM)	\$52.70
n1-highmem-2 (2 CPUs 13 GB RAM)	\$65.59
n1-highcpu-4 (4 CPUs 3.6 GB RAM)	\$78.62

Project:

Instance Type:

Back Next Finish Cancel

7. Click **Next**.

Run In Cloud - centos-mini-12125557-s3u

✓ Velostrata Cloud Extension

✓ Cloud Instance

Storage Policy

Networking

Summary

Storage Policy

Storage Policy: ☒ Write Back ☐ Write Isolation

Back Next Finish Cancel

8. Select the **Storage Policy**, that is, either **Write Back** or **Write Isolation**. The choice of Storage Policy need to be carefully reviewed, as this will affect the data changes done while running in cloud:

1. **Write back (default option):** When running in cloud using the write back policy, all changes in the cloud will be written to the on-premises storage, this write-back activity happens in background, in an interval of 5GB accumulated changes or 1 hour (whichever comes first).
2. **Write isolation:** When using write isolation policy, all changes done while running in cloud are kept in cloud on the Velostrata Cloud Edge and are not persisted back on-premises. When moving the VM back to run on-premises, it will go back to its state and data point in time captured in the base snapshot. Related Virtual Machines that are moved to cloud together using the Write Isolation policy should be moved back on-premises together to maintain state alignment.

9. Click **Next**.

Run In Cloud - centos-mini-09192712-q54-clone1531154073

✓ Velostrata Cloud Extension
✓ Cloud Instance
✓ Storage Policy
Networking
Summary

Networking

Subnet: 10.60.0.0/20

Network Tags (comma separated): velostrata

Instance Service Account (optional): cloud-edge-permanent

Configure Private IP: Auto

Edge Node: Node A

External IP: None

Back Next Finish Cancel

10. Select a cloud **Subnet**. Typically, the selection here would be of a private network subnet.
11. Enter the required Network Tags (comma separated), for example, **velostrata**. Network tags are used by networks to identify which instances are subject to certain firewall rules and network routes. For example, if you have several VM instances that are serving a large website, tag these instances with a shared word or term and then use that tag to apply a firewall rule that allows HTTP access to those instances.
12. Select the **Instance Service Account** (optional).
13. From the **Configure Private IP** drop-down list, select **Auto** to allow an available address on the subnet to be automatically assigned, or **Static** if a specific address assignment is required.
 1. If you select **Static**, a **Static IP** field appears. Enter the required static IP for the instance or specify an ENI ID (e.g. **eni-xxxxxx**) to associate a reserved Elastic Network Interface.
14. From the **Edge Node** drop-down list, select the required node.

15. For External IP, select **None, Static** and enter the **External IP address name** (this is the name for an external IP address created on the GCP console previously) or **Ephemeral** (the external IP is assigned by Google).
1. This IP appears as the **Public IP Address** in the Velostrata Cloud Extension portlet.
 2. If you select **Ephemeral** (the external IP is assigned by Google), the same setting persists when you detach, cleanup or cancel detach.
 3. If you select **static**, you will need to populate the external IP address name, too.
16. Click **Next**.

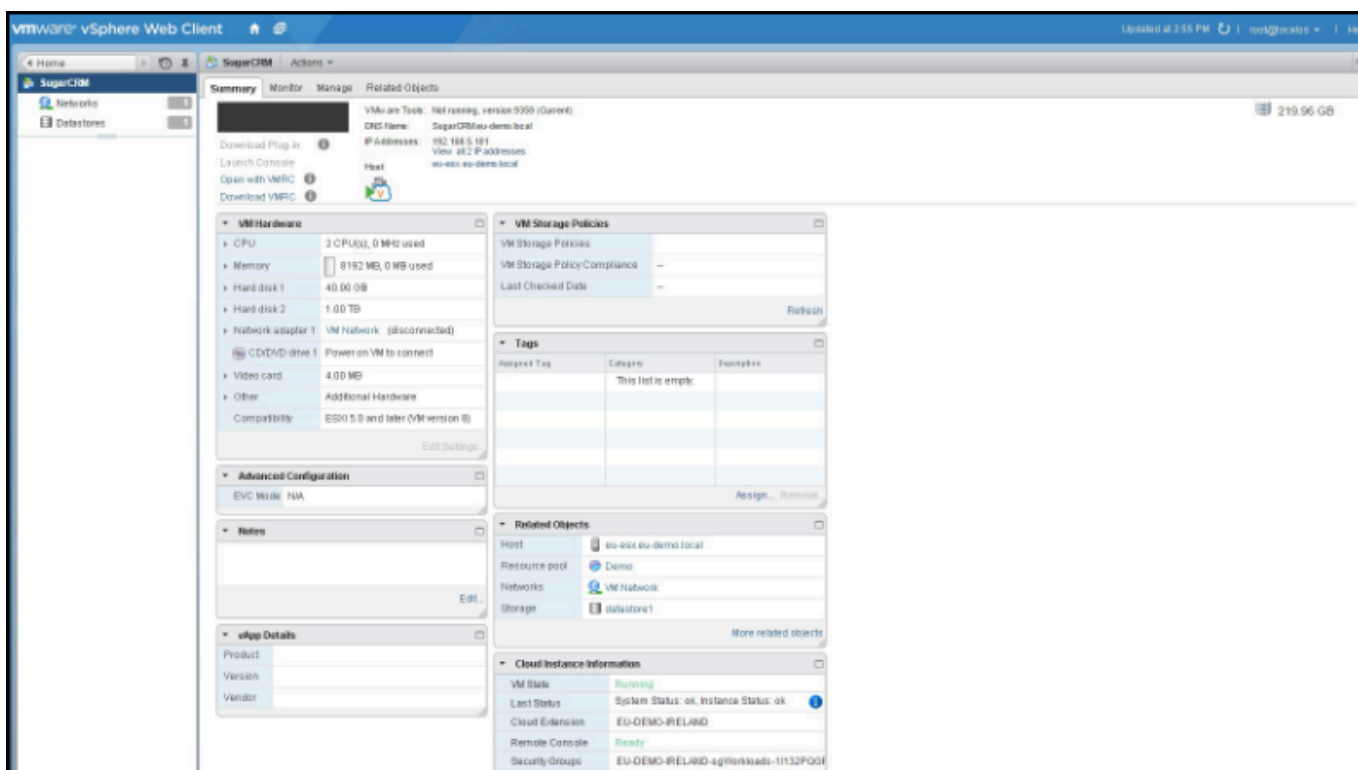
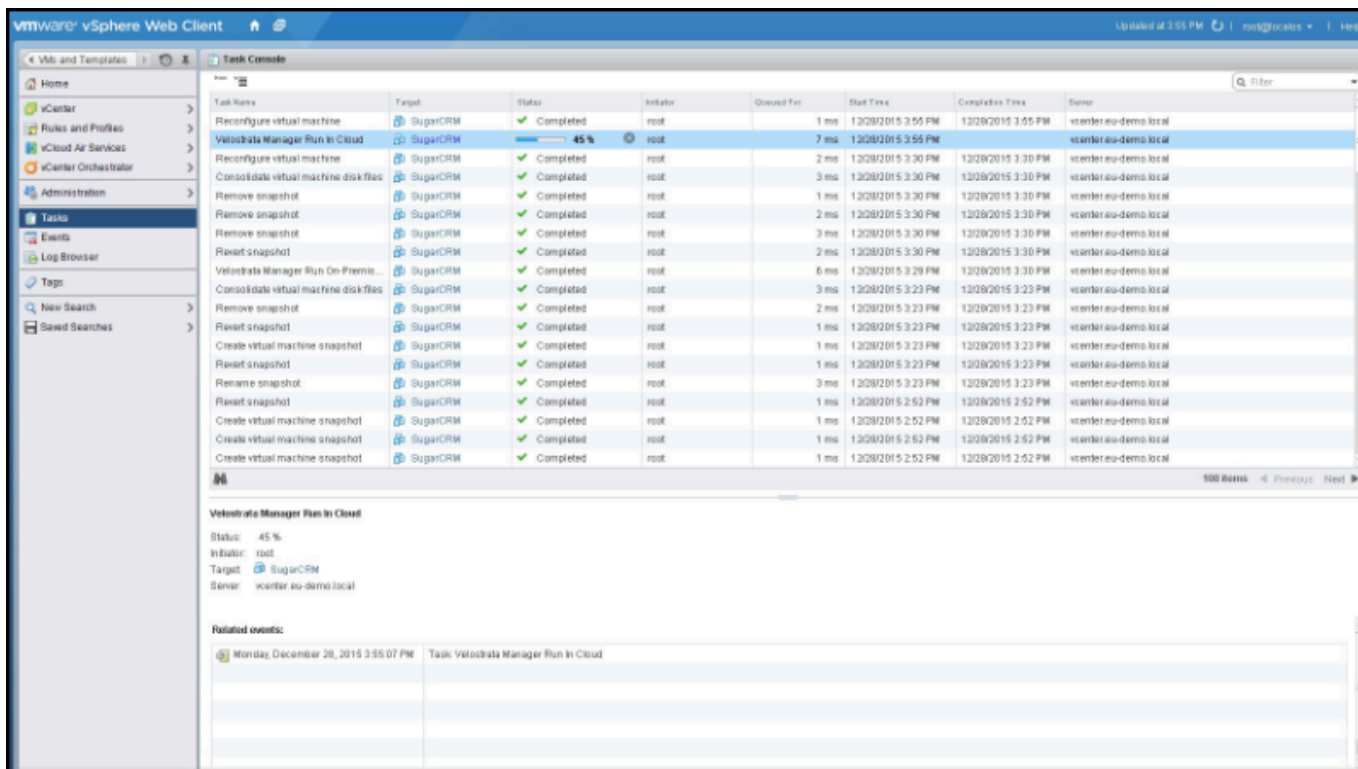
The screenshot shows a web interface titled "Run In Cloud - centos-mini-09192712-q54-clone1531154073". On the left is a sidebar with a list of steps: "Velostrata Cloud Extension", "Cloud Instance", "Storage Policy", "Networking", and "Summary". The "Summary" step is selected and highlighted. The main area displays a "Summary" table with the following details:

Velostrata Cloud Extension:	gcp_datacenter-2_1531153632_bGW
Cloud Instance Type:	f1-micro (1 CPU 0.6 GB RAM)
Cloud VM Name:	centos-mini-12125557-s3u
Project:	velos-auto-1
Service Account for Instance:	cloud-edge-permanent
Storage Policy:	Write Back
Network Tags:	velostrata
Subnet:	10.60.0.0/20
Edge Node:	Node A
Static IP:	Auto
External IP:	Ephemeral

At the bottom right of the interface are four buttons: "Back", "Next", "Finish", and "Cancel".

17. Review the summary and then click **Finish**.

The process of running the VM in the cloud can be viewed in the **Cloud Instance Information** portlet on the **VM Summary** page, and by monitoring the created vSphere task.



You can connect to the VM when the **Remote Console** field in the Cloud Instance Information portlet turns green and reads **"Ready"**. You can connect to the VM using the private IP address or FQDN.

Run AWS VM in GCP

During migration of an instance from AWS to GCP, Velostrata takes ownership of the instance disks at AWS. At the end of the process, the original AWS instance remains intact and powered off.

- Stops the source VM in AWS
- Creates the Velostrata VM Importer at AWS
- Attaches the disk from the source VM to the Velostrata worker service account (velos-worker-sa).
- Creates an instance in GCP
- Streams data from the importer to the GCP Cloud Extension
- Terminates the importer and re-attaches the disks to the source VM

Note: During cloud-to-cloud migrations, the VMs will be moved in **write isolation** mode, which means the data is **not** synchronized between AWS and GCP during the migration.

For detailed instructions on how to run VMs from AWS in GCP, please refer to our [Runbook Automation section](#).

Note: When you run a VM in the cloud and the instance does not start up in a healthy way, Velostrata uses VM auto healing to fix the problem and restart the instance. If this does not succeed, the Run in Cloud task is rolled back.

To view the related events, view the **Monitor > Tasks** tab, like below:

centos-mini-18201524-OAP-clone14/0811249

Gettng StartedSummaryMonitorManageRelated Objects

IssuesPerformancePoliciesTasksEventsUtilizationVelostrata Cloud Instance

Task Name	Target	Status	Initiator	Start Time	Completion Time
Velostrata Manager Start In Cloud	centos-mini-18201524-OAP-clone14/0811249	Completed	Automation	10/18/2016 8:37:35 PM	10/18/2016 8:46:37 PM
Velostrata Manager Stop In Cloud	centos-mini-18201524-OAP-clone14/0811249	Completed	Automation	10/18/2016 8:38:19 PM	10/18/2016 8:37:21 PM
Create virtual machine snapshot	centos-mini-18201524-OAP-clone14/0811249	Completed	hcl476809487	10/18/2016 8:21:02 PM	10/18/2016 8:21:02 PM
Consolidate virtual machine disk files	centos-mini-18201524-OAP-clone14/0811249	Completed	hcl476809487	10/18/2016 8:20:59 PM	10/18/2016 8:20:59 PM
Reconfigure virtual machine	centos-mini-18201524-OAP-clone14/0811249	Completed	hcl476809487	10/18/2016 8:20:55 PM	10/18/2016 8:20:55 PM
Velostrata Manager Run In Cloud	centos-mini-18201524-OAP-clone14/0811249	Completed	Automation	10/18/2016 8:20:55 PM	10/18/2016 8:25:19 PM

Velostrata Manager Start In Cloud

Status: Completed

Initiator: Automation

Target: centos-mini-18201524-OAP-clone1478011249

Server: 172.22.1.230

Related events:

10/18/2016 8:40:41 PM	Issue detected for centos-mini-18201524-OAP-clone1478011249 on 172.22.1.240 in dc-test: Event by Velostrata: Boot retry failed. Info: ProvisioningStateUpdating, Status: Updating, Info: PowerState deactivating, Status: VM deactivating.
10/18/2016 8:40:49 PM	Issue detected for centos-mini-18201524-OAP-clone1478011249 on 172.22.1.240 in dc-test: Event by Velostrata: VM vm-16 did not boot successfully. Retrying.
10/18/2016 8:27:24 PM	Task Velostrata Manager Start In Cloud

For clouds that were previously supported in other versions:

On-prem-to-AWS: To run a VM in the cloud:

AWS Spot Prices Overview

When you run a VM in the cloud on AWS, you can choose to pay on-demand pricing or select to spot market bid.

Spot instances let you bid on spare Amazon EC2 instances to name your own price for compute capacity. The spot price fluctuates based on the supply and demand of available EC2 capacity.

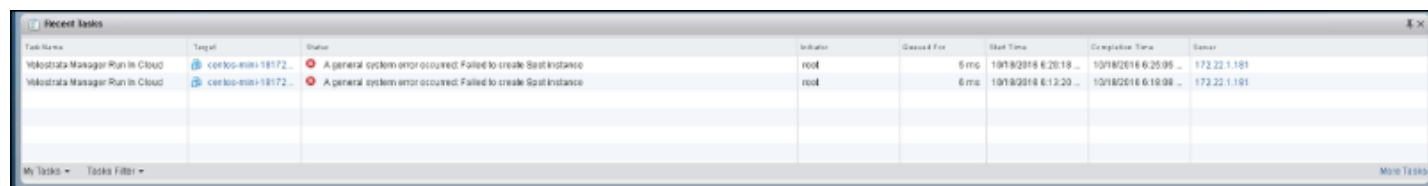
You can select the defined duration for the run in cloud instance, by choosing no reservation (AWS can take back the instance) or reserve the instance for between 1 and 6 hours.

When you move an instance into the cloud using a spot market instance, the full migration wizard is not available for the instance. It is also not possible to shutdown or reconfigure a spot market instance. You are able to restart a spot market instance.

For more information, see <https://aws.amazon.com/ec2/spot/pricing/>.

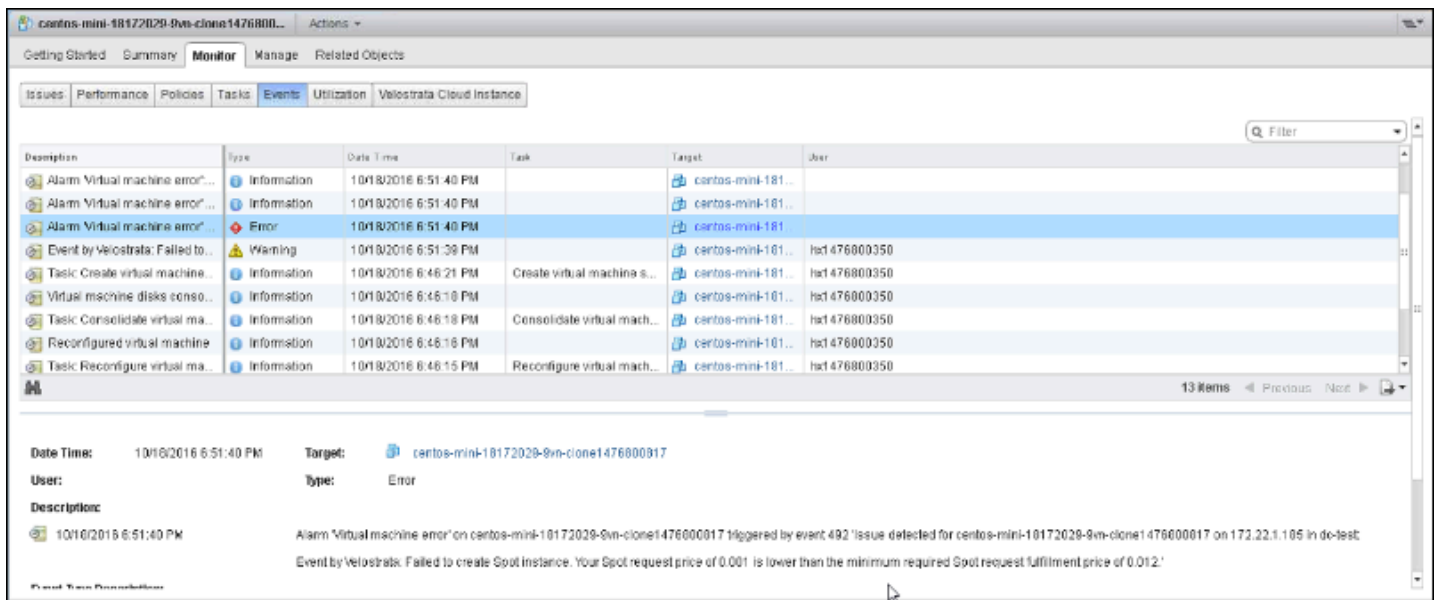
AWS Spot Instance

If the spot market bid is unsuccessful for an AWS VM an error message appears.



Task Name	Target	Status	Initiator	Desired For	Start Time	Completion Time	Error
Velostrata Manager Run in Cloud	centos-min-18172	Failed	root	6 mps	10/18/2016 6:20:18	10/18/2016 6:25:06	172.22.1.181
Velostrata Manager Run in Cloud	centos-min-18172	Failed	root	6 mps	10/18/2016 6:12:20	10/18/2016 6:16:08	172.22.1.181

To view the related events, view the **Monitor > Tasks** tab.



For an AWS instance, the Cloud Instance Information pane shows the Pricing Model (or Spot Market Bid or On-demand).

Cloud Instance Information	
VM State	Running
Last Status	--
Pricing Model	Spot Market Bid
Cloud Status Checks	System Status: initializing, Instance Status: initializing
Cloud Extension	datacenter-2_vpc-1410ff71_1476858632
Storage Migration	Cache On Demand
Remote Console	Ready
Security Groups	Test hosts
Private IP Address	172.31.10.181
Public IP Address	--
Edge Node	NodeA
CPU	1 CPU
Memory	3.75 GB
Cloud Instance Id	i-0cee0e0ebe953de4e
Instance Type	m3.medium
Storage Mode	Write Back
Network Adapter	eni-8a21b7d4

AWS: To run a VM in the cloud:

1. On the vSphere Web Client, select the desired **Virtual Machine**.
2. Right-click on the VM and select **Velostrata Operations > Run in Cloud**.



3. Select the **Velostrata Cloud Extension** and enter a **Cloud VM Name**.

Run In Cloud - centos-mini-18174114-809

Velostrata Cloud Extension

Cloud Instance

Storage Policy

Security Groups

Networking

Summary

Velostrata Cloud Extension

Velostrata Cloud Extension: datacenter-2_vpc-1410ff71_152138...

Cloud VM Name: centos-mini-18174114-809

Back Next Finish Cancel

Note: If you select a Cloud Extension that is impaired, (Impaired) is appended to the Velostrata Cloud Extension name. It is not recommended to move a VM to run in an impaired Cloud Extension. For more information, see [High Availability Overview](#).

Note: If you select to run your VM in a CE that is in the AWS Marketplace, a message appears indicating that you may incur usage costs according to the subscription terms.

4. Click **Next**.
5. Select the **Instance Type** (VM size). Three options are recommended for performance-optimized VMs, and three options are recommended for cost-optimized VMs.
Note: The prices are for compute cost only and do not include disk and network costs. Spot and reserved instances may also have price reduction plans.
Note: If the VM has not been monitored for a sufficient period (7 days), a message appears indicating that the activity duration may be insufficient for accurate recommendations.
Note: If the online price list is not available, no cost-optimized recommendations are provided.
6. Select **On-Demand** or **Spot Market Bid** for the **Pricing Model**.
7. If you select **Spot Market Bid**, select the **Defined Duration** (**No reservation** or between 1 and 6 hours) and enter the **\$USD** maximum price you are willing to pay for the spot.

Note: If you want to review the spot pricing history on the AWS site, click **Pricing History**.

Run In Cloud - centos-mini-18174114-809

✓ Velostrata Cloud Extension

Cloud Instance

Storage Policy

Security Groups

Networking

Summary

Cloud Instance

Source VM	Provisioned	Observed Usage	Monitoring Duration:	Not monitored
CPU:	2	No information		
RAM:	2GB	No information	Active Duration:	Not monitored
Disks:	1			

Recommended Options:

Performance Optimized	Monthly Cost (Pay-As-You-Go)
t2.medium (2 CPUs 4 GB RAM)	\$36.0
t2.large (2 CPUs 8 GB RAM)	\$72.57
m4.large (2 CPUs 8 GB RAM)	\$79.92

Instance Type:

Pricing Model:

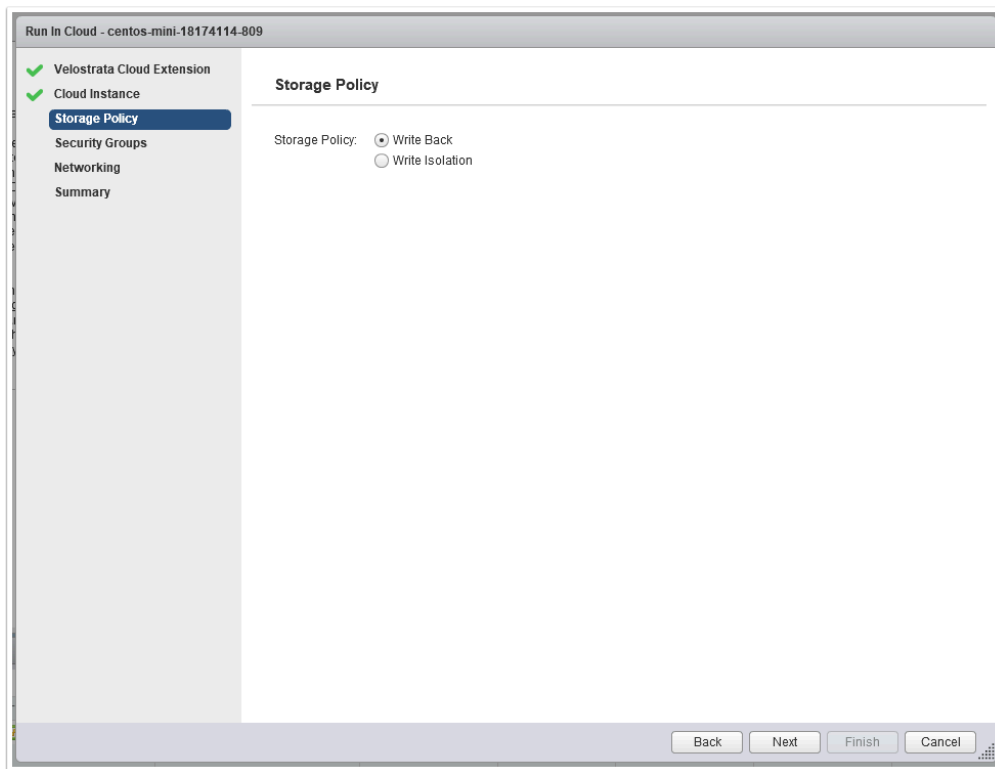
Instance Type:

Pricing Model:

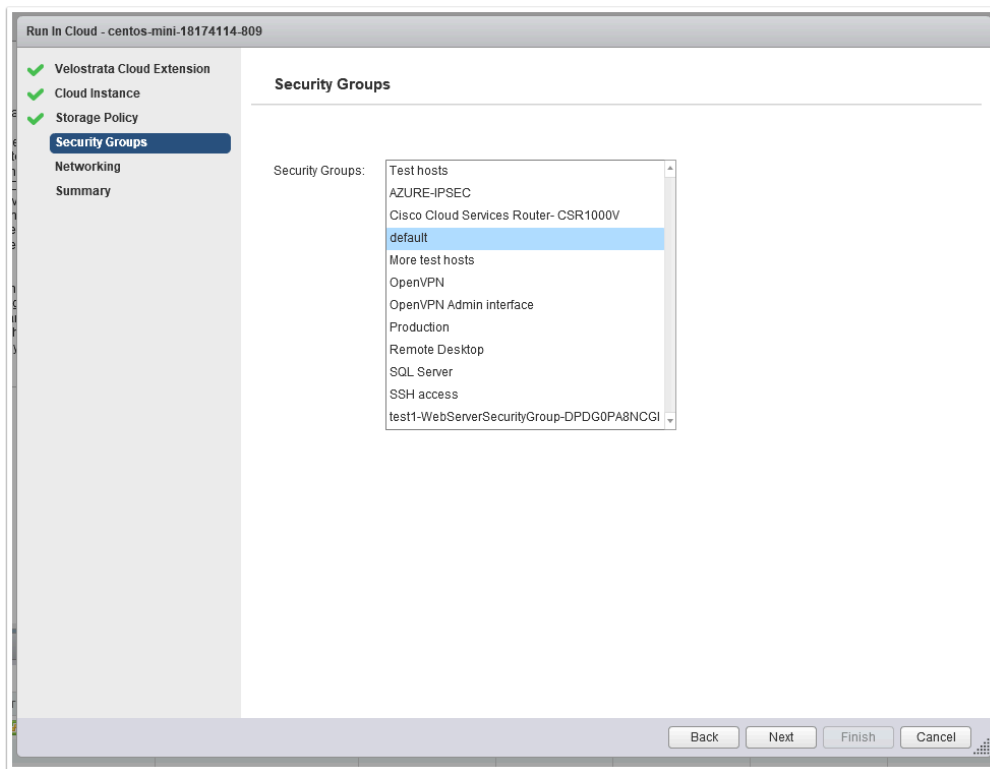
Defined Duration:

Maximum Price Set your max price (per instance/hour)

8. Click **Next**.



9. Select the **Storage Policy**, that is, either **Write Back** or **Write Isolation**. The choice of Storage Policy need to be carefully reviewed, as this will affect the data changes done while running in cloud:
 - **Write back (default option):** When running in cloud using the write back policy, all changes in the cloud will be written to the on-premises storage, this write-back activity happens in background, in an interval of 5GB accumulated changes or 1 hour (whatever comes first).
 - **Write isolation:** When using write isolation policy, all changes done while running in cloud are kept in cloud on the Velostrata Cloud Edge and are not persisted back on-premises. When moving the VM back to run on-premises, it will go back to its state and data point in time captured in the base snapshot. Related Virtual Machines that are moved to cloud together using the Write Isolation policy should be moved back on-premises together to maintain state alignment.
10. Click **Next**.



11. Select the required **Security Groups**.

Note: If you do not enter a Network Security Group, the default Network Security Group configured for the Cloud Extension is used.

Note: If public access is required from the internet to the VM, a DMZ is required with an associated security group, including appropriate inbound and outbound rules.

12. Click **Next**.

Run in Cloud - centos-mini-18174114-809

- ✓ Velostrata Cloud Extension
- ✓ Cloud Instance
- ✓ Storage Policy
- ✓ Security Groups
- Networking**
- Summary

Networking

Subnet: 172.31.0.0/20

Configure Private IP: Static

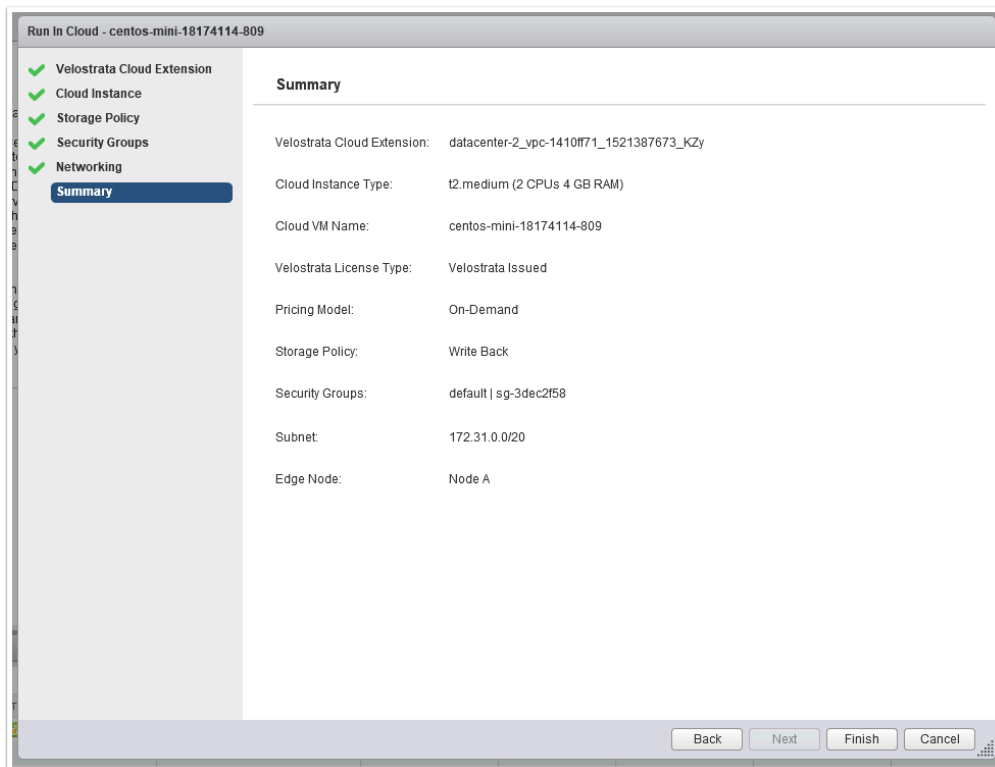
Static IP or ENI ID: *

Edge Node: Node A

Note: ENI option overrides subnet and security groups selection

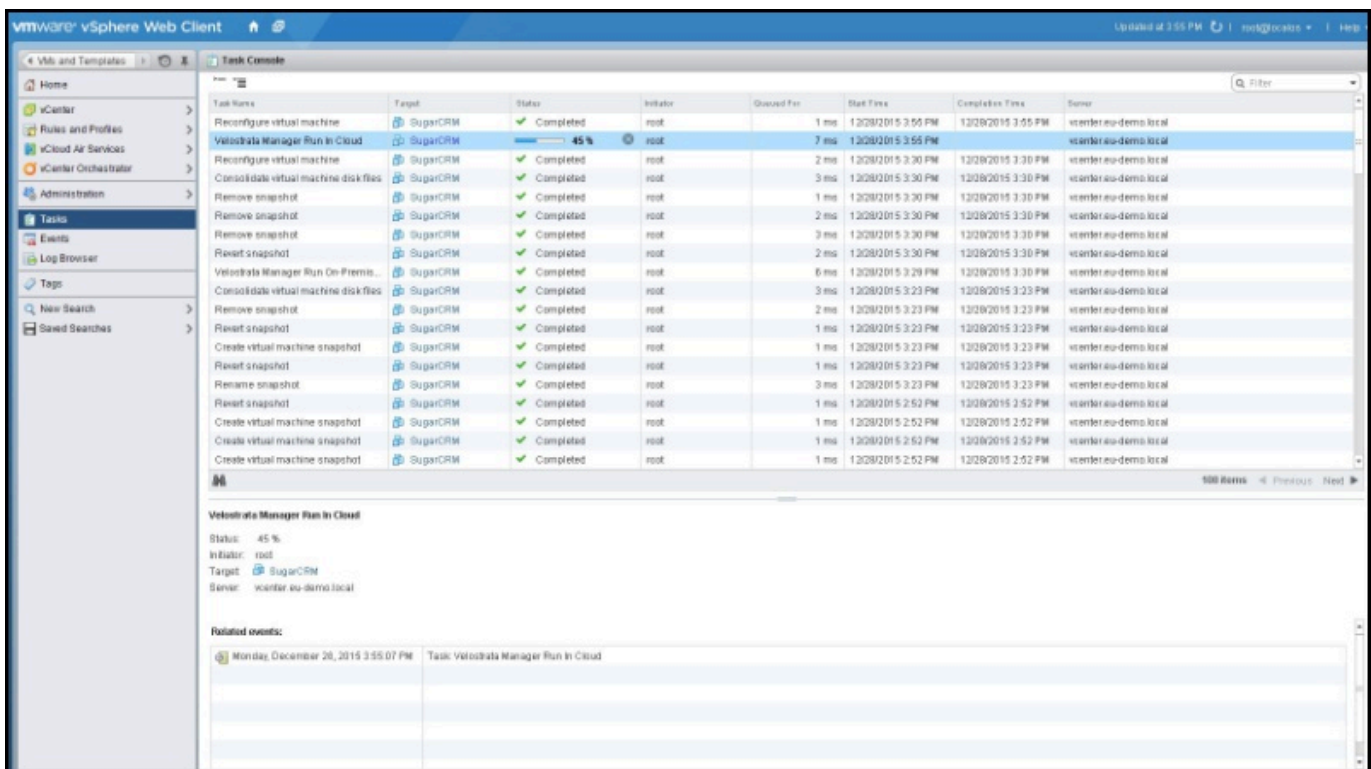
Back Next Finish Cancel

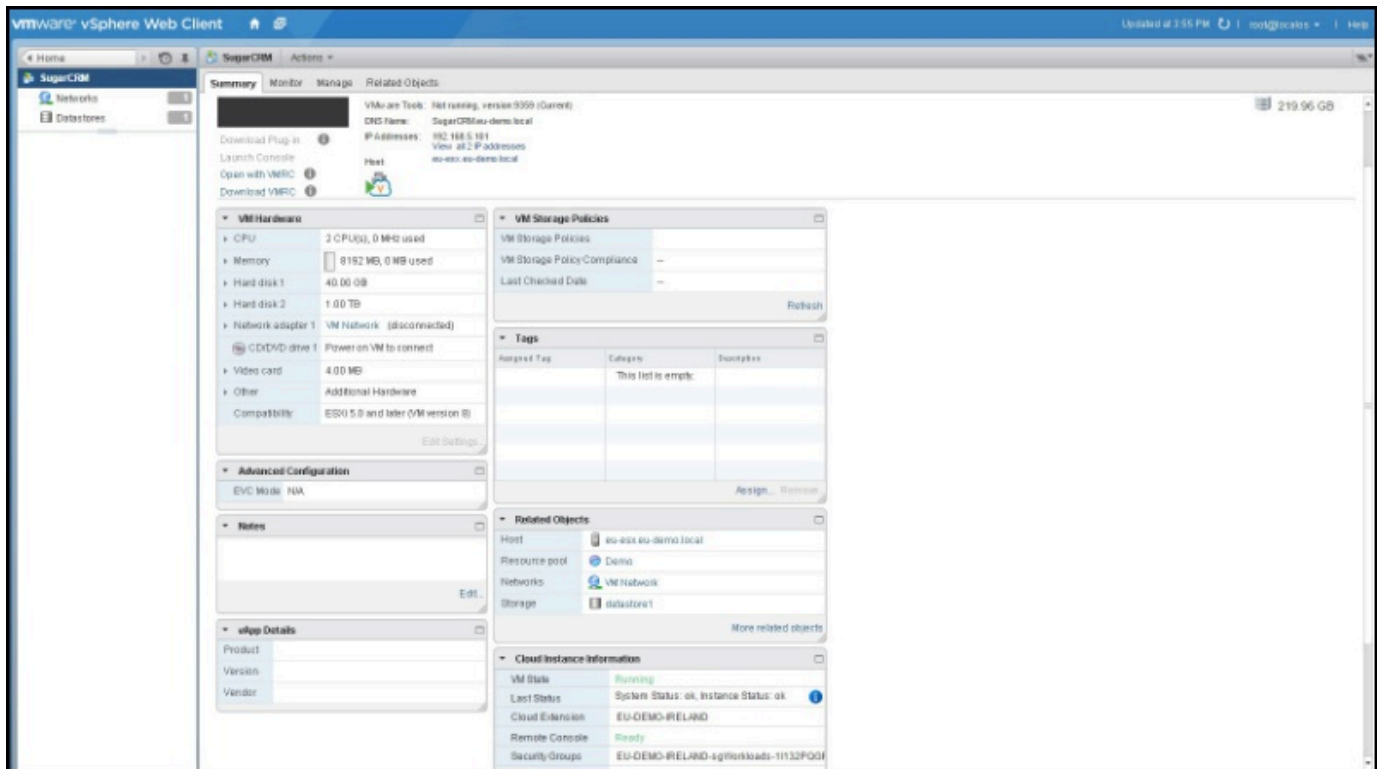
13. Select a cloud **Subnet**. Typically, the selection here would be of a private network subnet. When Cloud Edge nodes (A, B) are placed in different AZs, the Cloud Edge node in the same AZ as the selected subnet is automatically used, otherwise a manual node selection is required.
14. From the **Configure Private IP** drop-down list, select **Auto** to allow an available address on the subnet to be automatically assigned, or **Static** if a specific address assignment is required.
15. If you select **Static**, a **Static IP** field appears. Enter the required static IP for the instance or specify an ENI ID (e.g. **eni-xxxxxx**) to associate a reserved Elastic Network Interface.
16. From the **Edge Node** drop-down list, select the required node. When Cloud Edge nodes are placed in the same Availability Zone (AZ), a manual selection of the **Cloud Edge node** to use is required.
17. Click **Next**.
18. **Note:** If you select to run your VM in a CE that is in the AWS Marketplace, the **License Type** is **Marketplace**.



18. Review the summary and then click **Finish**.

The process of running the VM in the cloud can be viewed in the **Cloud Instance Information** portlet on the **VM Summary** page, and by monitoring the created vSphere task.





You can connect to the VM when the **Remote Console** field in the Cloud Instance Information portlet turns green and reads **"Ready"**. You can connect to the VM using the private IP address or FQDN.

On-prem-to-Azure: To run a VM in the cloud:

For Azure, select the type of Windows license to use, that is, either reuse your on-premises license (Azure Hybrid Use Benefit) or use a cloud-provided license:

- The Azure Hybrid Use Benefit is designed to help you to migrate to Azure without paying twice for the Windows license. If you have an existing on-premises Windows Server/Client license with active Software Assurance (SA), select to apply the Azure Hybrid Use Benefit. This enables you to reuse your on-prem license in the cloud.
- When using the cloud-provided license, the Windows license is included in the instance charges, and may be as much as 40% of the instance cost.

1. On the vSphere Web Client, select the desired **Virtual Machine**.
2. Right-click on the VM and select **Velostrata Operations > Run in Cloud**.



3. Select the **Velostrata Cloud Extension**.
4. The Cloud VM Name is filled in automatically from the VM. Modify the **Cloud VM Name** as required.

Note: From version 3.1, the random trailing suffix is no longer added to the name.

Run In Cloud - centos-mini-19110824-gkm

Velostrata Cloud Extension

Cloud Instance

Storage Policy

Security Groups

Networking

Summary

Velostrata Cloud Extension: datacenter-2_1521450507_hVs

Cloud VM Name: centos-mini-19110824-gkm

Back Next Finish Cancel

Note: If you select a Cloud Extension that is impaired, (Impaired) is appended to the Velostrata Cloud Extension name. It is not recommended to move a VM to run in an impaired Cloud Extension. For more information, see [High Availability Overview](#).

5. Click **Next**.
6. Select the **Instance Type** (VM size). Three options are recommended for performance-optimized VMs, and three options are recommended for cost-optimized VMs.
Note: The prices are for compute cost only and do not include disk and network costs.
Note: If the VM has not been monitored for a sufficient period (7 days), a message appears indicating that the activity duration may be insufficient for accurate recommendations.
Note: If the online price list is not available, no cost-optimized recommendations are provided.
7. Select whether to **Show only types supporting premium storage**.
Note: Instances that use premium storage may have a different cost.
8. Select the **Resource Group** and **Availability Set**.
9. (Windows) Select whether to use a **Cloud-provided license**, or if you have an existing on-premises Windows Server/Client license with active Software Assurance (SA), select **Hybrid Use Windows Server** or **Hybrid Use Windows Client** to apply the Azure Hybrid Use Benefit.

Run In Cloud - centos-mini-19110824-gkm

✓ Velostrata Cloud Extension

Cloud Instance

Storage Policy

Security Groups

Networking

Summary

Cloud Instance

Source VM	Provisioned	Observed Usage	Monitoring Duration:	Not monitored
CPU:	2	No information		
RAM:	2GB	No information	Active Duration:	Not monitored
Disks:	1			

Recommended Options:

Show only types supporting premium storage ☐

Performance Optimized	Monthly Cost (Pay-As-You-Go)
standard_a2_v2 (2 CPUs 4 GB RAM)	\$62.64
standard_d2_v3 (2 CPUs 8 GB RAM)	\$77.03
standard_d2_v2_promo (2 CPUs 7 GB RAM)	\$79.92

Instance Type:

Resource Group:

Availability Set:

Back Next Finish Cancel

10. Click **Next**.

Run In Cloud - centos-mini-19110824-gkm

✓ Velostrata Cloud Extension

✓ Cloud Instance

Storage Policy

Security Groups

Networking

Summary

Storage Policy

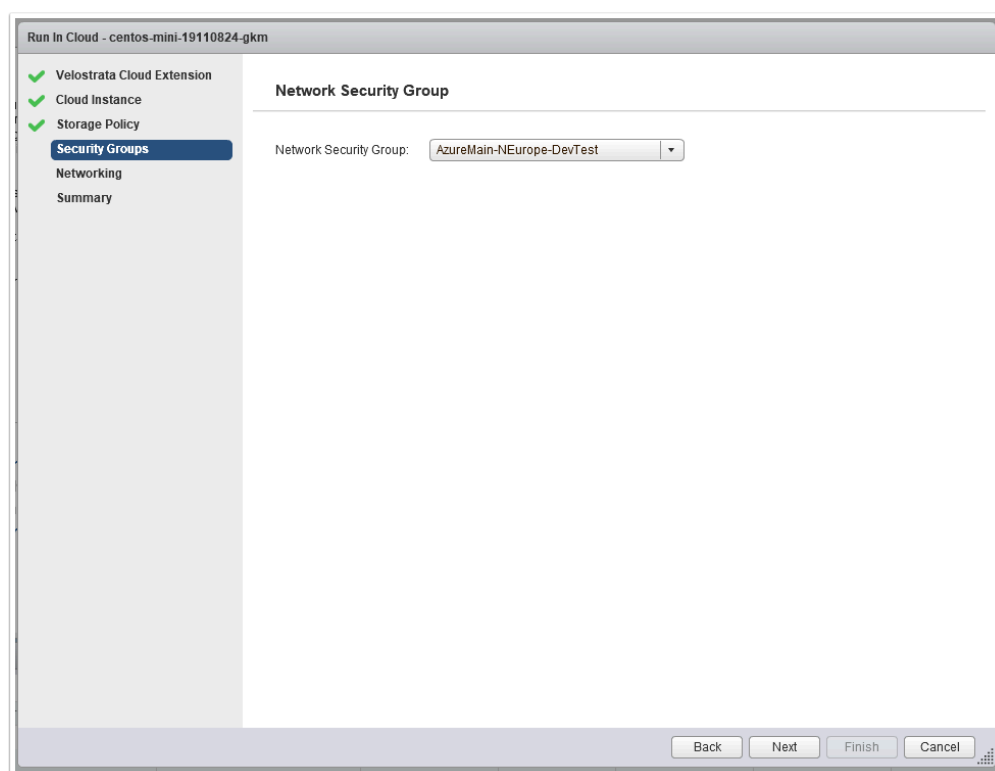
Storage Policy: ☒ Write Back ☐ Write Isolation

Back Next Finish Cancel

11. Select the **Storage Policy**, that is, either **Write Back** or **Write Isolation**. The choice of Storage Policy need to be carefully reviewed, as this will affect the data changes done while running in cloud

- **Write back (default option):** When running in cloud using the write back policy, all changes in the cloud will be written to the on-premises storage, this write-back activity happens in background, in an interval of 5GB accumulated changes or 1 hour (whichever comes first).
- **Write isolation:** When using write isolation policy, all changes done while running in cloud are kept in cloud on the Velostrata Cloud Edge and are not persisted back on-premises. When moving the VM back to run on-premises, it will go back to its state and data point in time captured in the base snapshot. Related Virtual Machines that are moved to cloud together using the Write Isolation policy should be moved back on-premises together to maintain state alignment.

12. Click **Next**.



13. Select the required **Network Security Group**.

Note: If you do not enter a Network Security Group, the default Network Security Group configured for the Cloud Extension is used.

14. Click **Next**.

Run in Cloud - centos-mini-19110824-gkm

- ✓ Velostrata Cloud Extension
- ✓ Cloud Instance
- ✓ Storage Policy
- ✓ Security Groups
- Networking**
- Summary

Networking

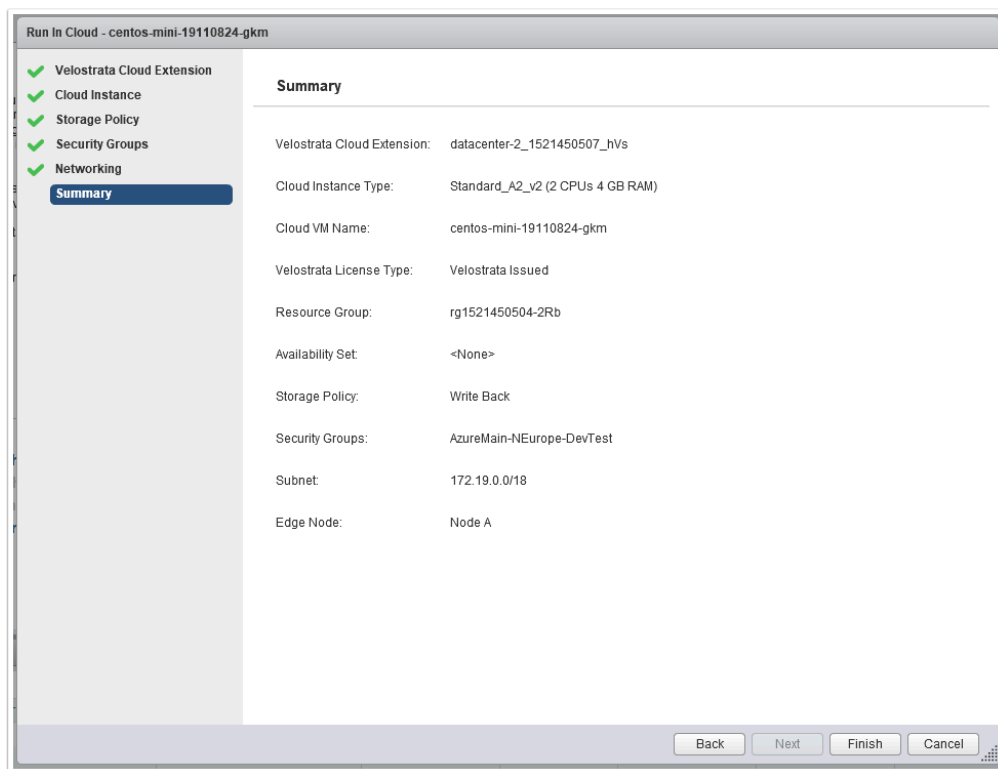
Subnet: 172.19.0.0/18

Configure Private IP: Auto

Edge Node: Node A

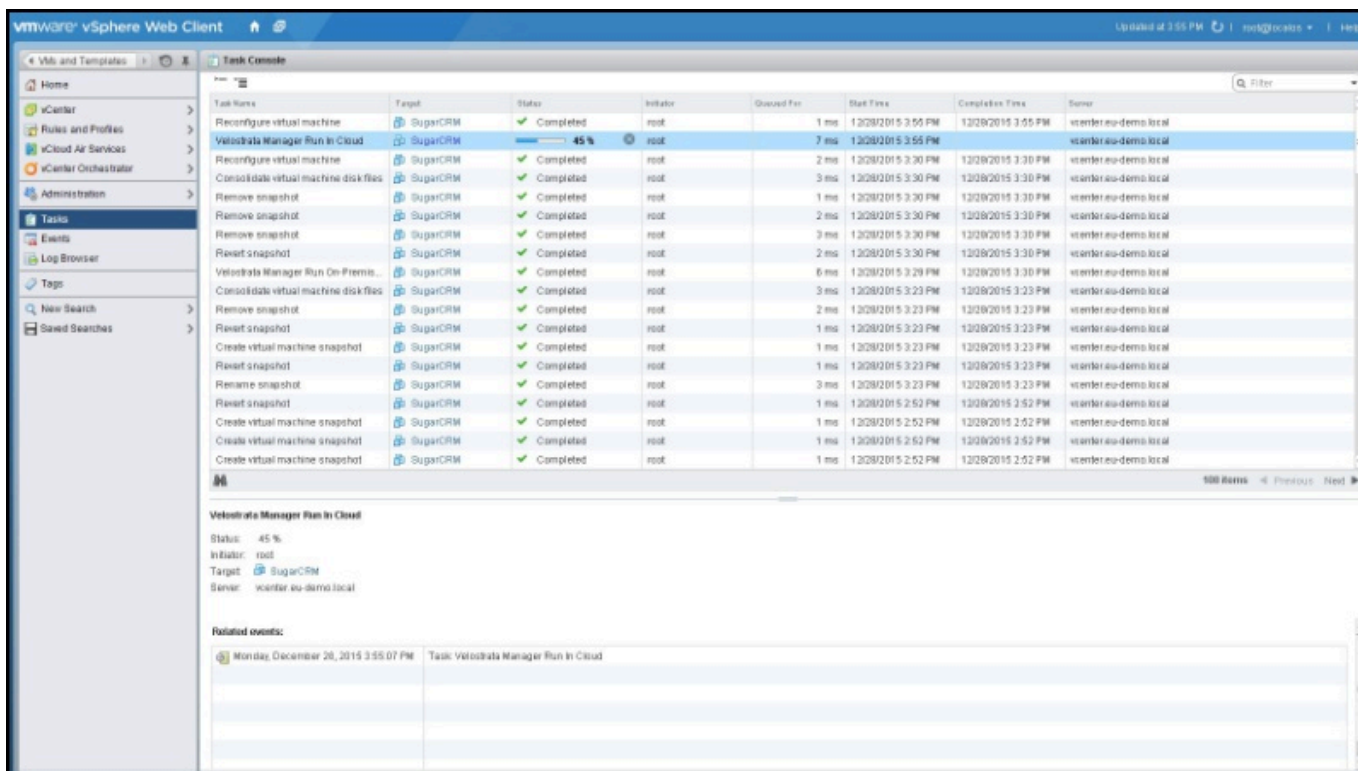
Back Next Finish Cancel

15. Select a cloud **Subnet**. Typically, the selection here would be of a private network subnet.
16. From the **Configure Private IP** drop-down list, select **Auto** to allow an available address on the subnet to be automatically assigned, or **Static** if a specific address assignment is required.
17. If you select **Static**, a **Static IP** field appears. Enter the required static IP for the instance or specify an ENI ID (e.g. **eni-xxxxxx**) to associate a reserved Elastic Network Interface.
18. From the **Edge Node** drop-down list, select the required node. A manual selection of the **Edge Node** to use is required. Select **Node A** or **Node B**. The default selection is **Node A**.
19. Click **Next**.



20. Review the summary and then click **Finish**.

The process of running the VM in the cloud can be viewed in the **Cloud Instance Information** portlet on the **VM Summary** page, and by monitoring the created vSphere task.



Running a VM Back On-Prem/On Source

When a VM is moved to run in cloud a base snapshot is taken. When the VM is moved to run back on the source, different behaviors will take place, depending on the storage policy used for that VM.

- **Write Isolation:** When using write isolation policy, the VM is moved back on-premises to the same point in time captured in the base snapshot. To maintain state alignment across related VMs when they use the write isolation policy, all related VMs should be moved back together.
- **Write Back:** When running in cloud using the write back policy, and as long as new or changed data is available, a new snapshot (consistency checkpoint) is taken and saved on-premises on every write back cycle (1 hour or 5GB changes, whatever comes first). When you choose to run such a VM on-premises, the remaining data changes are written back and the VM is then moved back on-premises. When the move back is complete, all interim snapshots taken by Velostrata are deleted and the virtual disks are consolidated.
- **Forced move back:** If there is a sustained cloud outage you may choose to force the VM to run on-premises or on the source. For VMs that use the Write Back policy, this moves the VM back to on-premises using its latest consistency checkpoint. This will result in data loss up to the last stored checkpoint.

Note: As a safety measure, the base snapshot of a VM that runs in cloud using the Write Back policy is not deleted automatically, when the Force option is used. The base snapshot can be deleted manually when verified to be no longer needed.

Note: In the cloud-to-cloud scenario, the source machine is shut down, the storage policy is write isolation, and when moving the VM back to the source, it is returned to the state that it was in when the migration operation started.

Using Web Manager

1. Login to your Velostrata Web Manager at [HTTPS://IP_OF_VELO_MANAGER](https://IP_OF_VELO_MANAGER)
2. Click the Runbook Automation tab.
3. When prompted for a username and password, use 'apiuser' as the username and your password is your Velostrata subscription ID or your GCP billing ID.
4. Click the monitor icon for one of the runbook automation jobs.

5. Select the VM you wish to return on-premises and click the 'Move Back' button on top.

VELOSTRATA

JOB MONITORING

Home

Runbook Automation

Virtual Machines

Start

Stop

Reboot

Move Back

Search

VmID	Target Instance Name	Project	Zone	Private IP	Power State	Run Group	Migration Status
i-001778a82f04f3401				-	-	200	-
i-056d81826efe94c53				-	-	200	-
i-092aedcb644848a2d				-	-	200	-
i-099bd38d8d4832f8a				-	-	300	-
i-0eable274197ae70f				-	-	100	-

© 2018, Velostrata Ltd. VELOSTRATA.COM

Terms of Use | Open Source Licenses

Show 10 entries

Showing 1-5 of 5

First

←

1

→

Last

Using vCenter

To run a VM back on-prem:

1. On the vSphere Web Client, select the desired **Virtual Machine**.
2. Right-click on the required VM and select **Velostrata Operations > Run On-Premises**.



Run On-Premises

Set selected virtual machine(s) to run on-premises?

☐ Force run on-premises. This option may be used in case of a prolonged cloud outage.

Warning: Forcing may result in data loss up to last stored checkpoint. This action may affect application state in related virtual machines.

To avoid accidental use of this feature, please type in the following number in the box below:

9557

OK

Cancel

3. If there has been a prolonged cloud outage, and you want to force a run on-premises, select **Force run on-premises**.
4. Type in the displayed confirmation code to approve the action.
5. Click **OK**. VMs returning from the cloud are automatically started on premises.

The process of running the VM on source can be viewed on the **Cloud Instance Information** portlet on the **VM Summary** page, and by monitoring the created vSphere task.

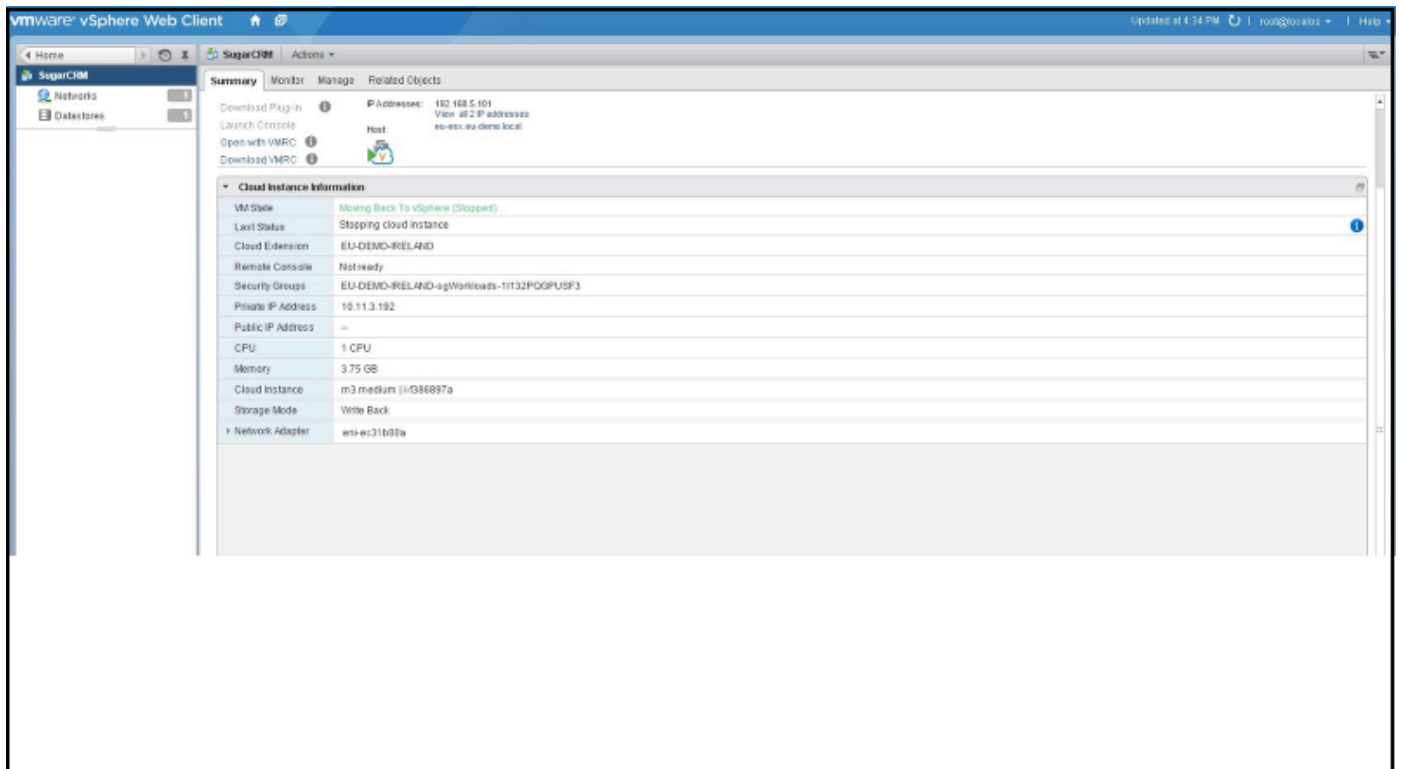
Task Name	Target	Status	Initiator	Quoted For	Start Time	Completion Time	Server
Velostrata Manager Run On-Premises	SuperCRM	50 %	root		5 ms	12/28/2015 4:28 PM	vcenter-au-demo.local
Consolidate virtual machine disk files	SuperCRM	Completed	root		1 ms	12/28/2015 4:28 PM	vcenter-au-demo.local
Remove snapshot	SuperCRM	Completed	root		2 ms	12/28/2015 4:28 PM	vcenter-au-demo.local
Revert snapshot	SuperCRM	Completed	root		3 ms	12/28/2015 4:28 PM	vcenter-au-demo.local
Create virtual machine snapshot	SuperCRM	Completed	root		5 ms	12/28/2015 4:28 PM	vcenter-au-demo.local
Revert snapshot	SuperCRM	Completed	root		2 ms	12/28/2015 4:28 PM	vcenter-au-demo.local
Rename snapshot	SuperCRM	Completed	root		3 ms	12/28/2015 4:25 PM	vcenter-au-demo.local
Velostrata Manager Reconfigure VM	SuperCRM	Completed	root		10 ms	12/28/2015 4:20 PM	vcenter-au-demo.local
Revert snapshot	SuperCRM	Completed	root		0 ms	12/28/2015 3:55 PM	vcenter-au-demo.local
Create virtual machine snapshot	SuperCRM	Completed	root		1 ms	12/28/2015 3:55 PM	vcenter-au-demo.local
Create virtual machine snapshot	SuperCRM	Completed	root		1 ms	12/28/2015 3:55 PM	vcenter-au-demo.local
Create virtual machine snapshot	SuperCRM	Completed	root		1 ms	12/28/2015 3:55 PM	vcenter-au-demo.local
Consolidate virtual machine disk files	SuperCRM	Completed	root		3 ms	12/28/2015 3:55 PM	vcenter-au-demo.local
Reconfigure virtual machine	SuperCRM	Completed	root		1 ms	12/28/2015 3:55 PM	vcenter-au-demo.local
Velostrata Manager Run In Cloud	SuperCRM	Completed	root		7 ms	12/28/2015 3:55 PM	vcenter-au-demo.local
Reconfigure virtual machine	SuperCRM	Completed	root		2 ms	12/28/2015 3:30 PM	vcenter-au-demo.local
Consolidate virtual machine disk files	SuperCRM	Completed	root		3 ms	12/28/2015 3:30 PM	vcenter-au-demo.local
Remove snapshot	SuperCRM	Completed	root		1 ms	12/28/2015 3:30 PM	vcenter-au-demo.local
Remove snapshot	SuperCRM	Completed	root		2 ms	12/28/2015 3:30 PM	vcenter-au-demo.local

Velostrata Manager Run On-Premises

Status: 50 %
Initiator: root
Target: SuperCRM
Server: vcenter-au-demo.local

Related events:

Time	Event
Monday, December 28, 2015 4:28:13 PM	Task: Velostrata Manager Run On-Premises



To run a VM back on source:

- To move a workload back from GCP to AWS, run the PowerShell command, run: **Move-VelosVm [-Id] <String[]> [-Destination] Origin [Confirm:\$false] [-Force]**

Where:

[Confirm:\$false] disables the dialog box warning message.

-Force forces the move back.

For example: **Move-VelosVm i-123abc -Destination Origin -confirm:\$false**

Running a Test Clone

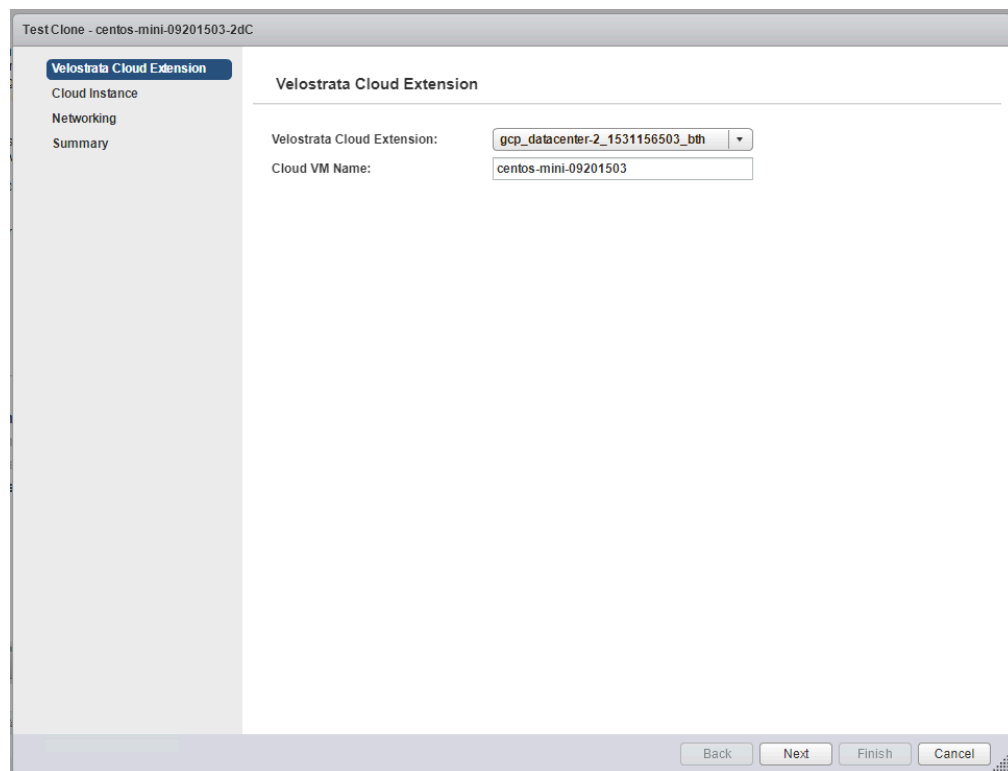
A workload can be tested in cloud using a Test Clone.

This is especially useful prior to migration as a Test Clone leaves the on-premises VM running, moves an identical clone (snapshot) of the VM to the cloud of choice, and similar to the Run In Cloud operation, the workload is up and running in the cloud within minutes. Some additional notes:

- It is highly recommended that a Test Clone be used in an isolated environment, to prevent network collisions with the on-premises live workload.
- The Test Clone cloud instance is created in write-isolation storage mode (all changes are committed only in cloud and are not persisted back on-premises).
- Only one Test Clone can be used for any specified VM at a time.

Run a Test Clone in GCP

1. On the vSphere Web Client, select the desired **Virtual Machine**.
2. Right-click on the VM and select **Velostrata Operations > Test Clone**.
3. Select the **Velostrata Cloud Extension** from the drop-down menu.
4. Give the Test Clone a new VM Name (optional, can use default populated value if desired).
5. Click **Next**.



The screenshot shows a window titled "Test Clone - centos-mini-09201503-2dC". On the left is a sidebar with a tree view containing "Velostrata Cloud Extension" (highlighted in blue), "Cloud Instance", "Networking", and "Summary". The main area is titled "Velostrata Cloud Extension" and contains two fields: "Velostrata Cloud Extension:" with a dropdown menu showing "gcp_datacenter-2_1531156503_bth", and "Cloud VM Name:" with a text box containing "centos-mini-09201503". At the bottom right are four buttons: "Back", "Next", "Finish", and "Cancel".

6. Select the **Instance Type** (VM size) using the rightsizing recommendations as desired and click **Next**.

Additional notes:

- The prices are for compute cost only and do not include disk and network costs.
- If the VM has not been monitored for a sufficient period (7 days), a message appears indicating that the activity duration may be insufficient for accurate recommendations.
- If the online price list is not available, no cost-optimized recommendations are provided.

Test Clone - centos-mini-09201503-2dC

Velostrata Cloud Extension

Cloud Instance

Networking

Summary

Cloud Instance

Source VM	Provisioned	Observed Usage	Monitoring Duration:
CPU:	2	No information	0 days
RAM:	2GB	No information	Active Duration: 0 days
Disks:	1		

Recommended Options:

Performance Optimized	Monthly Cost (Pay-As-You-Go)
custom-2-2048 (2 CPUs 2 GB RAM)	\$41.68
custom-2-3072 (2 CPUs 3 GB RAM)	\$44.20
custom-2-4096 (2 CPUs 4 GB RAM)	\$46.65

Cost Optimized	Monthly Cost (Pay-As-You-Go)
No information	No information
No information	No information
No information	No information

Project:

Instance Type:

Back Next Finish Cancel

7. Select the desired subnet from the drop-down menu.

8. Enter the required **Network Tags** (comma separated), for example, **velostrata**. Network tags are used by networks to identify which instances are subject to certain firewall rules and network routes. For example, if you have several VM instances that are serving a large website, tag these instances with a shared word or term and then use that tag to apply a firewall rule that allows HTTP access to those instances.

9. Select the **Instance Service Account** (if desired) from the drop-down menu.

10. From the **Configure Private IP** drop-down list, select **Auto** to allow an available address on the subnet to be automatically assigned, or **Static** if a specific address assignment is required.

A. If you select **Static**, a **Static IP** field appears. Enter the required static IP for the instance or specify an ENI ID (e.g. **eni-xxxxxx**) to associate a reserved Elastic Network Interface.

11. From the **Edge Node** drop-down list, select the required node.

12. Enter the **External IP address name**. This is the name for an external IP address created on the GCP console previously. If you select static, define that in the field that appears.

13. Click **Next**.

Test Clone - centos-mini-09201503-2dC

✓

Velostrata Cloud Extension

✓

Cloud Instance

Networking

Summary

Networking

Subnet: 10.60.0.0/20

Network Tags (comma separated): velostrata

Instance Service Account (optional):

Configure Private IP: Auto

Edge Node: Node A

External IP: None

Back

Next

Finish

Cancel

14. Review the summary and then click **Finish**.

Test Clone - centos-mini-09201503-2dC

✓

Velostrata Cloud Extension

✓

Cloud Instance

✓

Networking

Summary

Note: Velostrata will attempt to quiesce the guest OS using VMware Tools, before taking a snapshot. Crash-consistent snapshot will be used for guests that do not support quiescing. Please consult with the VMware Tools documentation for more information on snapshot support.

Summary

Velostrata Cloud Extension: gcp_datacenter-2_1531156503_bth

Cloud Instance Type: custom-2-2048 (2 CPUs 2 GB RAM)

Cloud VM Name: centos-mini-09201503

Project: velos-auto-1

Service Account for Instance:

Network Tags: velostrata

Subnet: 10.60.0.0/20

Edge Node: Node A

Static IP: Auto

External IP: None



Back

Next

Finish

Cancel

The process of running the VM in the cloud can be viewed in the **Cloud Instance Information** portlet on the **VM Summary** page (or by monitoring the created vSphere task).

Cloud Instance Information		
	VM State	Running
	Last Status	--
Run Mode	Test Clone	
Cloud Extension	gcp_datacenter-2_1531156503_	
Storage Migration	Cache On Demand	
Remote Console	Ready	
Network tags	velostrata	
Private IP Address	10.60.0.14	
Public IP Address	--	
Preferred Edge Node	NodeA	
Actual Edge Node	NodeA	
CPU	2 CPUs	
Memory	2 GB	
Cloud Instance Id	centos-mini-09201503	
Project	velos-auto-1	
Zone	europe-west1-d	
Service Account	--	
Instance Type	custom-2-2048	
Storage Policy	Write Isolation	
Network Adapter	--	

For clouds supported in previous editions of Velostrata:

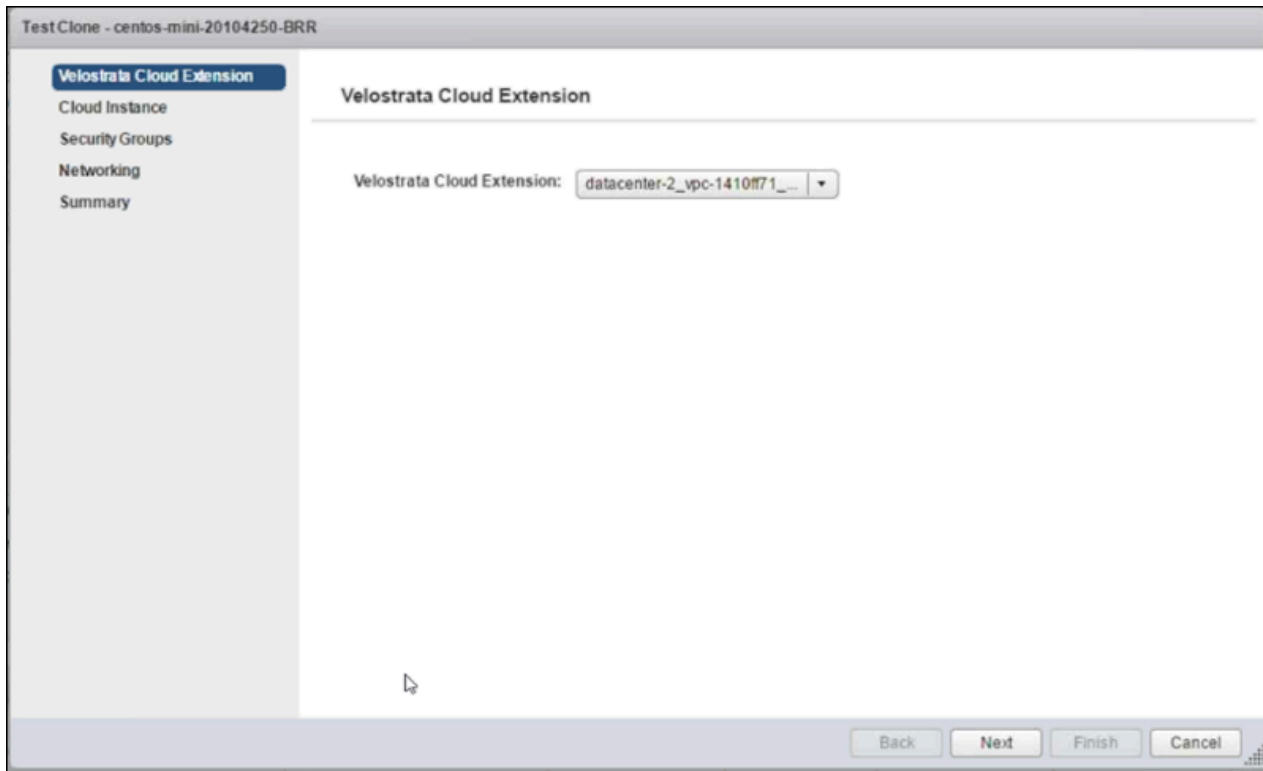
AWS: To run a test clone:

Select the type of Windows license to use, that is, either reuse your on-premises license (Azure Hybrid Use Benefit) or use a cloud-provided license:

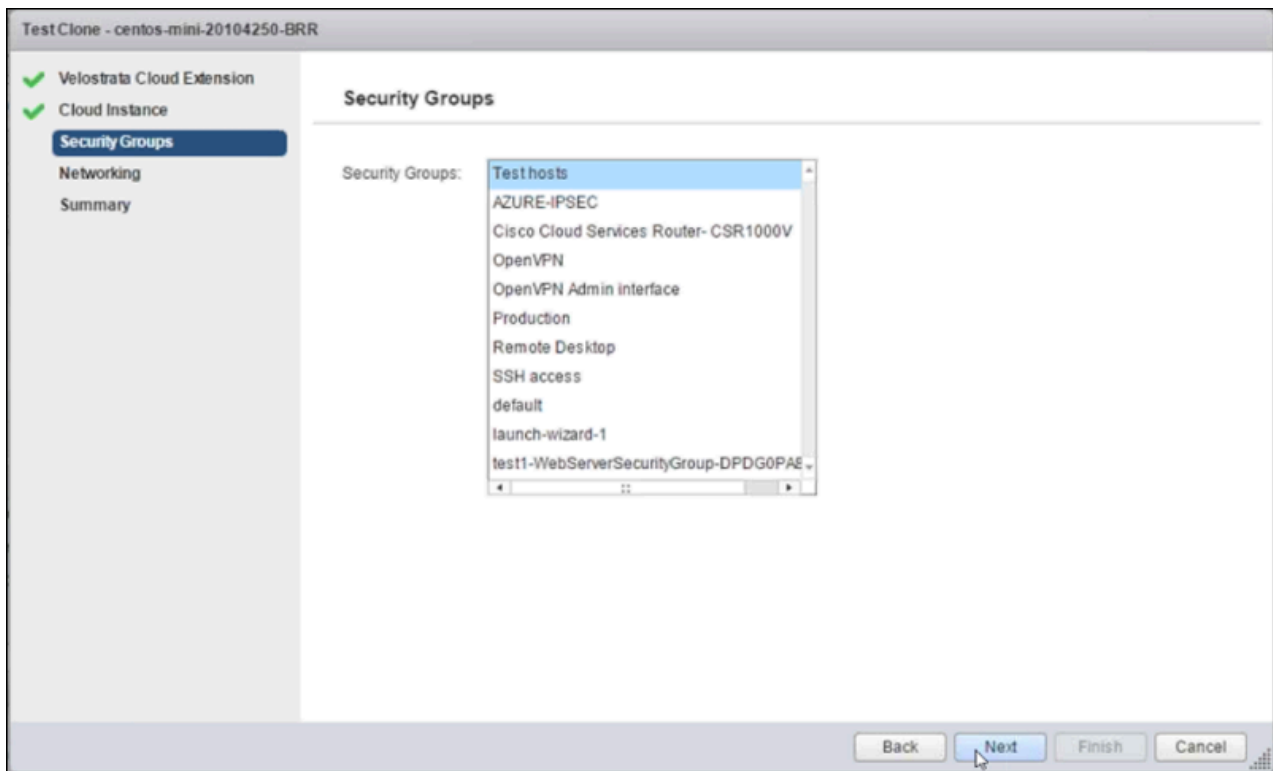
- The Azure Hybrid Use Benefit is designed to help you to migrate to Azure without paying twice for the Windows license. If you have an existing on-premises Windows Server/Client license with active Software Assurance (SA), select to apply the Azure Hybrid Use Benefit. This enables you to reuse your on-prem license in the cloud.
- When using the cloud-provided license, the Windows license is included in the instance charges, and may be as much as 40% of the instance cost.

There is a built-in recommendation engine that provides cost- and performance-optimized recommendations. In order to provide an effective recommendation, Velostrata recommends monitoring the VM usage for at least 7 active days. For more information, see [Monitoring VM Usage](#).

1. On the vSphere Web Client, select the desired **Virtual Machine**.
2. Right-click on the VM and select **Velostrata Operations > Test Clone**.
3. Select the **Velostrata Cloud Extension**.



4. Click **Next**.
5. Select the **Instance Type** (VM size). Three options are recommended for performance-optimized VMs, and three options are recommended for cost-optimized VMs.
Note: The prices are for compute cost only and do not include disk and network costs. Spot and reserved instances may also have price reduction plans.
Note: If the VM has not been monitored for a sufficient period (7 days), a message appears indicating that the activity duration may be insufficient for accurate recommendations.
Note: If the online price list is not available, no cost-optimized recommendations are provided.
6. Select **On-Demand** or **Spot Market Bid** for the **Pricing Model**. If you select **Spot Market Bid**, select the **Defined Duration (No reservation)** or between 1 and 6 hours) and enter the **\$USD** maximum price you are willing to pay for the spot.
Note: If you want to review the spot pricing history on the AWS site, click **Pricing History**.



8. Select the required **Network Security Group**.

Note: If you do not enter a Network Security Group the default Network Security Group configured for the Cloud Extension is used.

Note: If public access is required from the internet to the VM, a DMZ is required with an associated security group, including appropriate inbound and outbound rules.

9. Click **Next**.

Test Clone - w12r2gui-25120444-6zc

- ✓ Velostrata Cloud Extension
- ✓ Cloud Instance
- ✓ Security Groups
- Networking**
- Summary

Networking

Subnet: 172.29.1.0/24

Configure Private IP: Auto

Edge Node: Node A

Back Next Finish Cancel

10. Select a **Subnet**. Typically, the selection here would be of a private network subnet. When Cloud Edge nodes (A, B) are placed in different AZs, the Cloud Edge node in the same AZ as the selected subnet is automatically used, otherwise a manual node selection is required.

Test Clone - w12r2gui-25120444-6zc

- ✓ Velostrata Cloud Extension
- ✓ Cloud Instance
- ✓ Security Groups
- Networking**
- Summary

Networking

Subnet: 172.29.1.0/24

Configure Private IP: Static

Static IP: *

Edge Node: Node A

Back Next Finish Cancel

11. From the **Configure Private IP** drop-down list, select **Auto** to allow an available address on the subnet to be automatically assigned, or **Static** if a specific address assignment is required.
12. If you select **Static**, a **Static IP** field appears. Enter the required static IP for the instance or specify an ENI ID (e.g. **eni-xxxxxx**) to associate a reserved Elastic Network Interface.
13. From the **Edge Node** drop-down list, select the required node. When Cloud Edge nodes are placed in the same Availability Zone (AZ), a manual selection of the **Cloud Edge node** to use is required.
14. Click **Next**.

Note: If you select to run your VM in a CE that is in the AWS Marketplace, the **License Type** is **Marketplace**.

The screenshot shows a configuration window titled "Test Clone - centos-mini-20104250-BRR". On the left, there is a sidebar with a list of configuration steps: "Velostrata Cloud Extension", "Cloud Instance", "Security Groups", "Networking", and "Summary". The "Summary" step is currently selected and highlighted. A yellow warning box at the top right states: "Note: Velostrata will attempt to quiesce the guest OS using VMware Tools, before taking a snapshot. Crash-consistent snapshot will be used for guests that do not support quiescing. Please consult with the VMware Tools documentation for more information on snapshot support". The main area displays the "Summary" of the configuration with the following details:

Velostrata Cloud Extension:	datacenter-2_vpc-1410ff71_1476949369
Cloud Instance Type:	t2.micro 1 vCPU 1 GB RAM
License Type:	Bring Your Own License
Pricing Model:	On-Demand
Security Groups:	Test hosts sg-48539e2d
Subnet:	172.31.0.0/20
Edge Node:	Node A

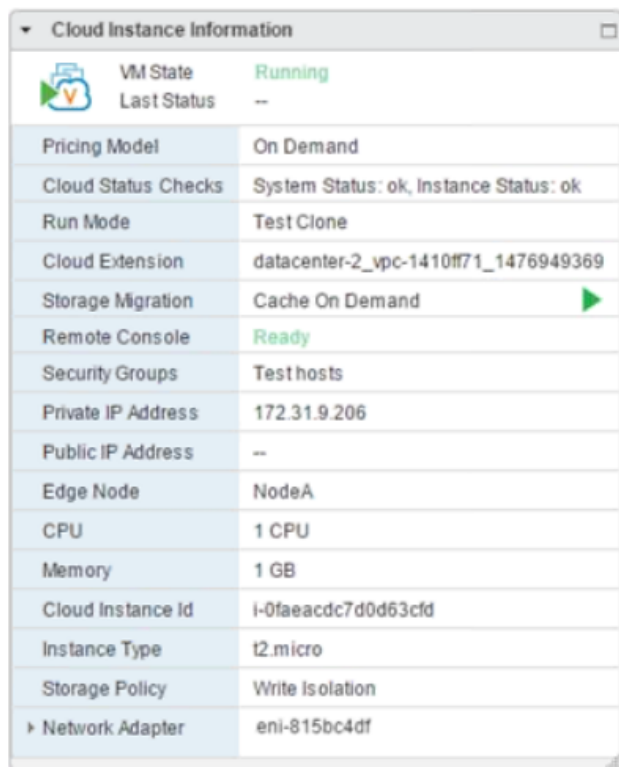
At the bottom of the window, there are four buttons: "Back", "Next", "Finish", and "Cancel". The "Next" button is highlighted with a mouse cursor.

15. Review the summary and then click **Finish**.

The process of running the VM in the cloud can be viewed in the **Cloud Instance Information** portlet on the **VM Summary** page, and by monitoring the created vSphere task.

Recent Tasks		
Task Name	Target	Status
Velostrata Manager Test Clone	w2008-20105002-GJY	<div><div></div></div> 45 %

You can connect to the VM when the **Remote Console** field in the Cloud Instance Information portlet turns green and reads "**Ready**". You can connect to the VM using the private IP address or FQDN.



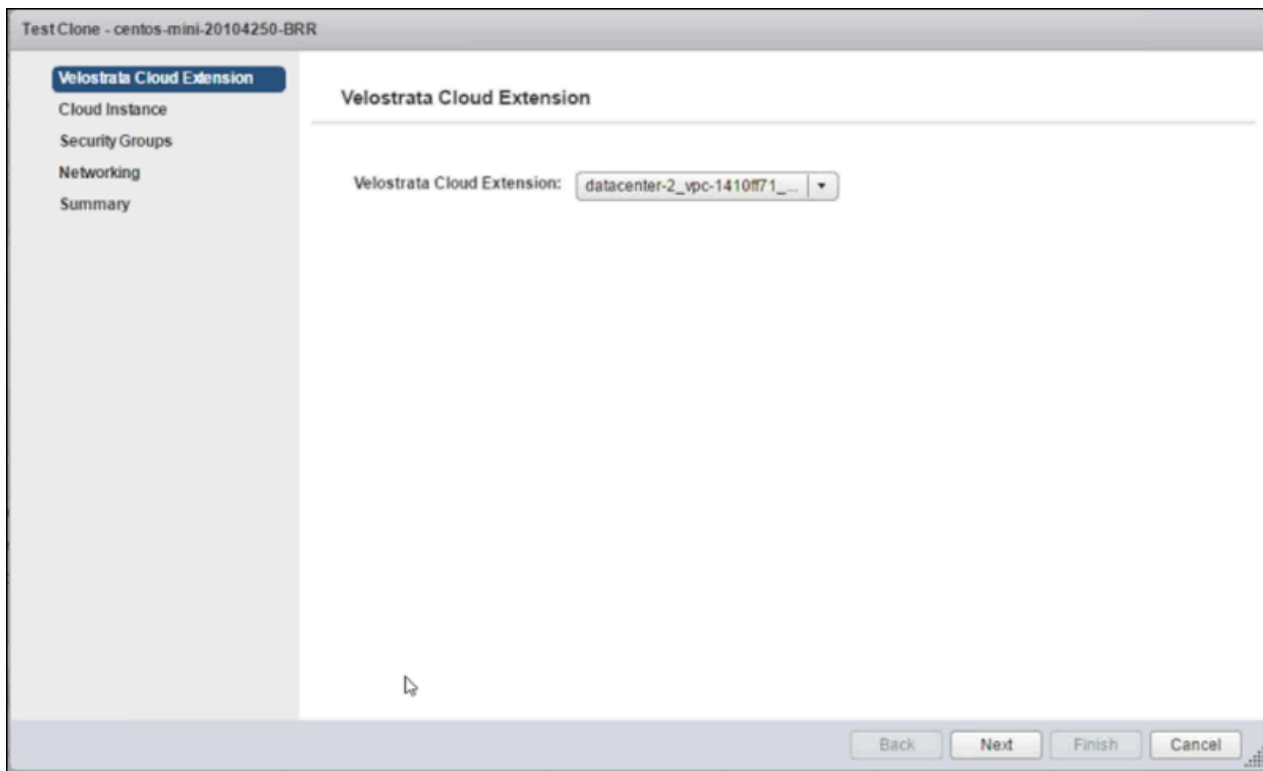
The screenshot shows a 'Cloud Instance Information' portlet with a table of VM details. The 'VM State' is 'Running' and the 'Remote Console' status is 'Ready' in green. The table lists various attributes such as Pricing Model, Cloud Status Checks, Run Mode, Cloud Extension, Storage Migration, Security Groups, Private IP Address, Public IP Address, Edge Node, CPU, Memory, Cloud Instance Id, Instance Type, Storage Policy, and Network Adapter.

Cloud Instance Information	
VM State	Running
Last Status	--
Pricing Model	On Demand
Cloud Status Checks	System Status: ok, Instance Status: ok
Run Mode	Test Clone
Cloud Extension	datacenter-2_vpc-1410ff71_1476949369
Storage Migration	Cache On Demand
Remote Console	Ready
Security Groups	Test hosts
Private IP Address	172.31.9.206
Public IP Address	--
Edge Node	NodeA
CPU	1 CPU
Memory	1 GB
Cloud Instance Id	i-0faeacdc7d0d63cfd
Instance Type	t2.micro
Storage Policy	Write Isolation
Network Adapter	eni-815bc4df

Azure: To run a test clone:

There is a built-in recommendation engine that provides cost- and performance-optimized recommendations. In order to provide an effective recommendation, Velostrata recommends monitoring the VM usage for at least 7 active days. For more information, see [Monitoring VM Usage](#).

1. On the vSphere Web Client, select the desired **Virtual Machine**.
2. Right-click on the VM and select **Velostrata Operations > Test Clone**.
3. Select the **Velostrata Cloud Extension**.



4. Click **Next**.
5. Select the **Instance Type** (VM size). Three options are recommended for performance-optimized VMs, and three options are recommended for cost-optimized VMs.
Note: The prices are for compute cost only and do not include disk and network costs. Spot and reserved instances may also have price reduction plans.
Note: If the VM has not been monitored for a sufficient period (7 days), a message appears indicating that the activity duration may be insufficient for accurate recommendations.
Note: If the online price list is not available, no cost-optimized recommendations are provided.
6. Select the **Resource Group** and **Availability Set**.
7. Select whether to use a **Cloud-provided license**, or if you have an existing on-premises Windows Server/Client license with active Software Assurance (SA), select **Hybrid Use Windows Server** or **Hybrid Use Windows Client** to apply the Azure Hybrid Use Benefit.
8. (Windows) Select whether to use a **Cloud-provided license**, or if you have an existing on-premises Windows Server/Client license with active Software Assurance (SA), select **Hybrid Use Windows Server** or **Hybrid Use Windows Client** to apply the Azure Hybrid Use Benefit.

Test Clone - w12core-11181341-JXb

✓ Velostrata Cloud Extension

Cloud Instance

Security Groups

Networking

Summary

Note: Activity duration may be insufficient for accurate recommendations

Cloud Instance

Source VM	Provisioned	Observed Usage	Monitoring Duration:
CPU:	2	10%	0 days
RAM:	2GB	0.25GB	Active Duration: 0 days
Disks:	1		

Recommended Options:

Show only types supporting premium storage ☐

Performance Optimized	Monthly Cost (Pay-As-You-Go)
basic_a2 (2 CPUs 3.5 GB RAM)	\$81.36
standard_a2_v2 (2 CPUs 4 GB RAM)	\$93.60
standard_a2 (2 CPUs 3.5 GB RAM)	\$129.6

Cost Optimized	Monthly Cost (Pay-As-You-Go)
basic_a0 (1 CPU 0.75 GB RAM)	\$12.95
standard_a0 (1 CPU 0.75 GB RAM)	\$14.39
standard_a1_v2 (1 CPU 2 GB RAM)	\$44.64

Instance Type:

Resource Group:

Availability Set:

Windows License:

Back Next Finish Cancel

Test Clone - rhel72-11162321-UIC

✓ Velostrata Cloud Extension

Cloud Instance

Networking

Security Groups

Summary

Cloud Instance

Source VM	Provisioned	Observed Usage	Monitoring Duration:
CPU:	1	No information	Not monitored
RAM:	2GB	No information	Active Duration: Not monitored
Disks:	1		

Recommended Options:

Performance Optimized	Monthly Cost (Pay-As-You-Go)
t2.small (1 CPU 2 GB RAM)	\$18.0
t2.medium (2 CPUs 4 GB RAM)	\$36.0
m3.medium (1 CPU 3.75 GB RAM)	\$52.56

Instance Type:

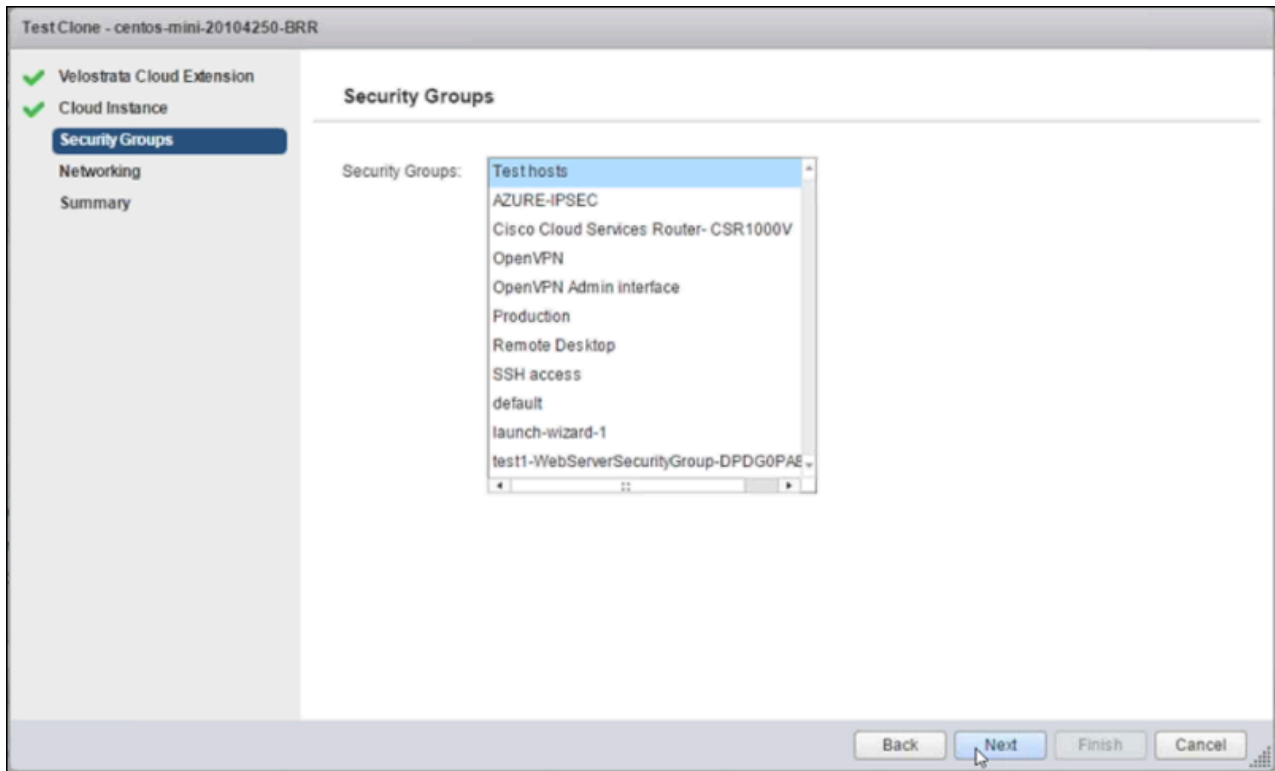
Pricing Model:

Defined Duration:

Maximum Price: Set your max price (per instance/hour)

Back Next Finish Cancel

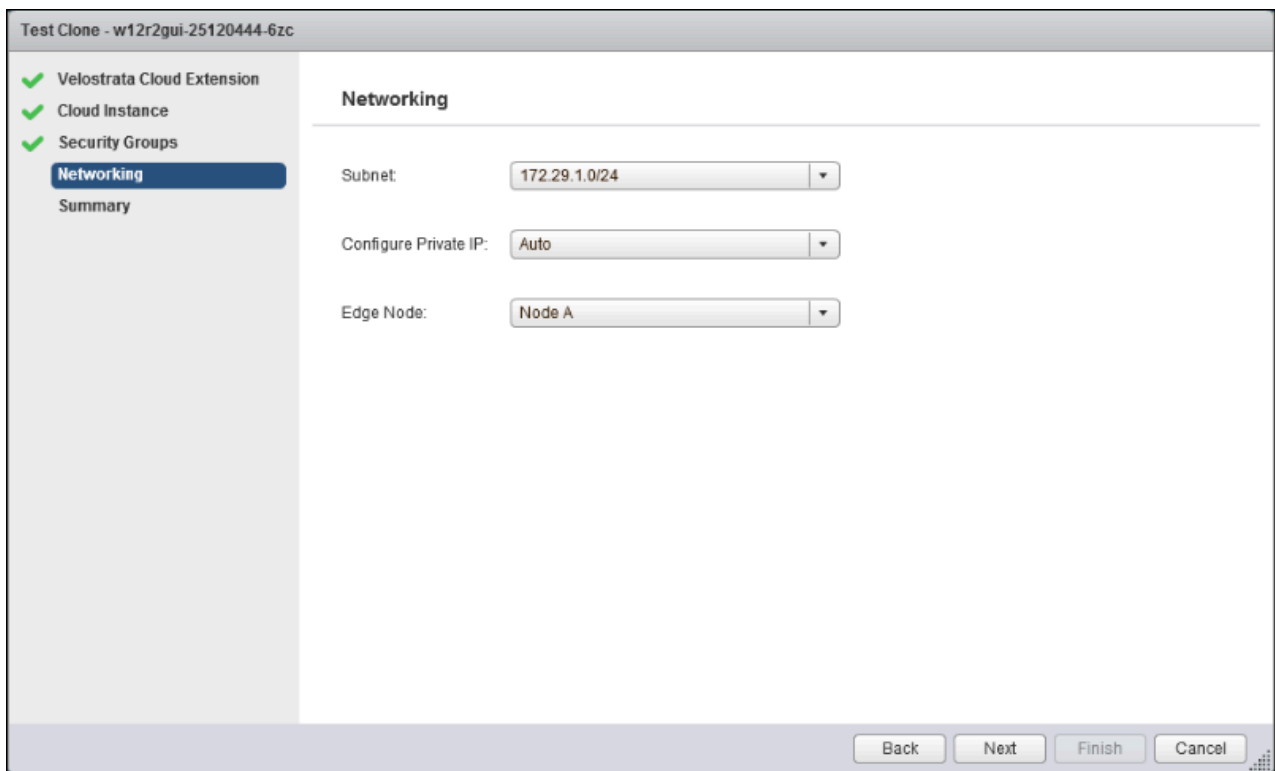
9. Click **Next**.



10. Select the required **Network Security Group**.

Note: If you do not enter a Network Security Group the default Network Security Group configured for the Cloud Extension is used.

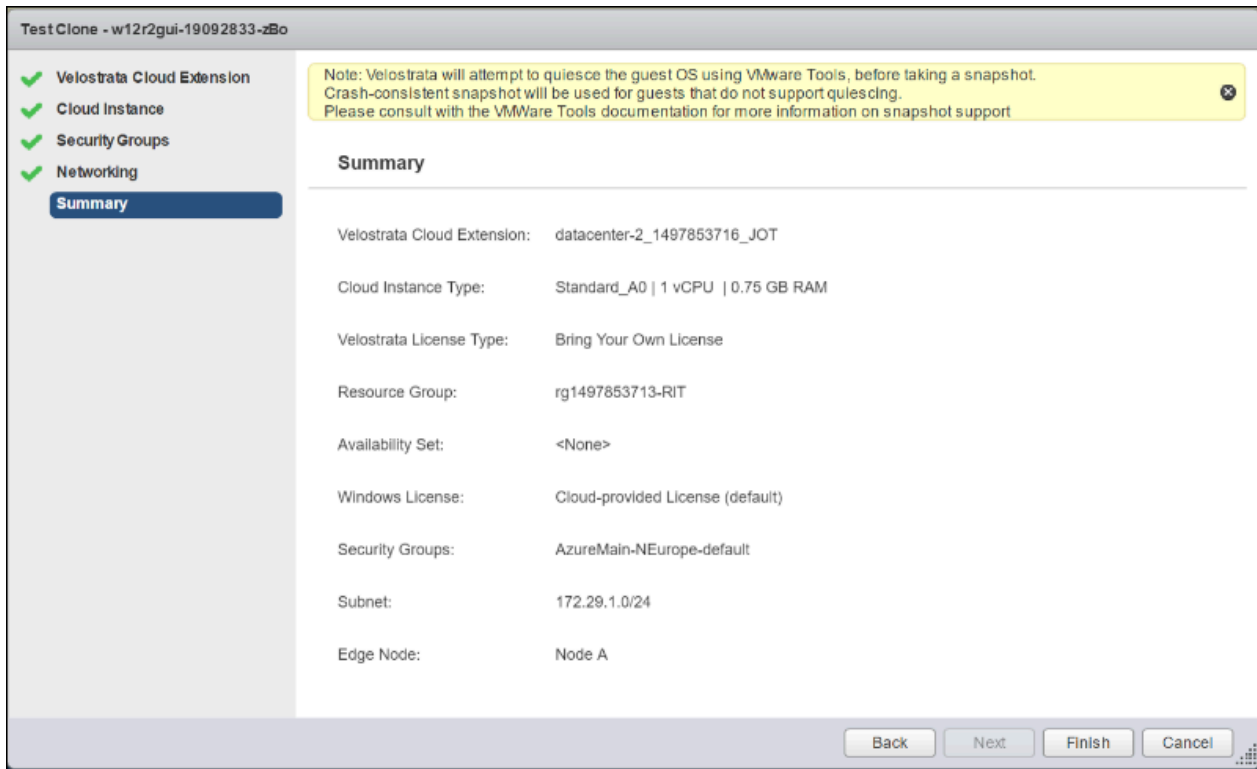
11. Click **Next**.



12. Select a **Subnet**. Typically, the selection here would be of a private network subnet.

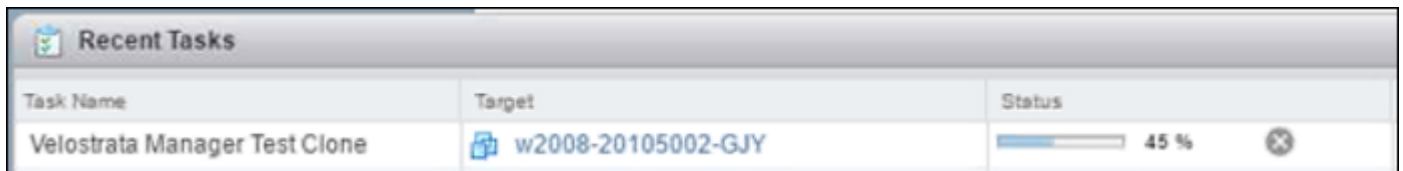
The screenshot shows a software window titled "Test Clone - w12r2gui-25120444-6zc". On the left is a sidebar with a list of steps: "Velostrata Cloud Extension", "Cloud Instance", "Security Groups", "Networking" (which is highlighted with a blue bar), and "Summary". The main content area is titled "Networking" and contains four configuration items: "Subnet" with a dropdown menu showing "172.29.1.0/24", "Configure Private IP:" with a dropdown menu showing "Static", "Static IP:" with a red asterisk icon and an empty text input field, and "Edge Node:" with a dropdown menu showing "Node A". At the bottom right of the window are four buttons: "Back", "Next", "Finish", and "Cancel".

13. From the **Configure Private IP** drop-down list, select **Auto** to allow an available address on the subnet to be automatically assigned, or **Static** if a specific address assignment is required.
14. If you select **Static**, a **Static IP** field appears. Enter the required static IP for the instance or specify an ENI ID (e.g. **eni-xxxxxx**) to associate a reserved Elastic Network Interface.
15. From the **Edge Node** drop-down list, select the required node. A manual selection of the **Edge Node** to use is required. Select **Node A** or **Node B**. The default selection is **Node A**.
16. Click **Next**.





17. Review the summary and then click **Finish**.

The process of running the VM in the cloud can be viewed in the **Cloud Instance Information** portlet on the **VM Summary** page, and by monitoring the created vSphere task.



You can connect to the VM when the **Remote Console** field in the Cloud Instance Information portlet turns green and reads "**Ready**". You can connect to the VM using the private IP address or FQDN.

Cloud Instance Information	
	<div>VM State Running</div> <div>Last Status --</div>
Pricing Model	On Demand
Cloud Status Checks	System Status: ok, Instance Status: ok
Run Mode	Test Clone
Cloud Extension	datacenter-2_vpc-1410ff71_1476949369
Storage Migration	Cache On Demand 
Remote Console	Ready
Security Groups	Test hosts
Private IP Address	172.31.9.206
Public IP Address	--
Edge Node	NodeA
CPU	1 CPU
Memory	1 GB
Cloud Instance Id	i-0faeacdc7d0d63cfd
Instance Type	t2.micro
Storage Policy	Write Isolation
▶ Network Adapter	eni-815bc4df

Delete a Test Clone

Once you have completed your testing with your test clone, you can delete it. Deleting the test clone will have no impact whatsoever on your live system or data. The test clone was running in an isolated test bubble in the cloud, so that it performs like the real application (and data), but without affecting it. Any changes you made to the data in the test clone will not reflect back to your live system on-prem.

Deleting Test Clone via Web Manager

1. Login to your Velostrata Web Manager at [HTTP://VELO_IP](http://VELO_IP)
2. Click the Runbook Automation tab.
3. Login with 'apiuser' for the username and use your GCP Billing ID for the password.
4. Click Start New Job
5. Define a job name, select your runbook inventory CSV file (which lists the test clone instances you are about to stop).
6. Select Delete Test Clones from the drop down.
7. Click Start.

For more information on using Runbooks, please visit [this section](#).

Start New Job

Job Name:

Runbook CSV: No file chosen

Operation:

Select...

Run in cloud

Test clone

Move back

Delete clone

Full migration

Offline migration

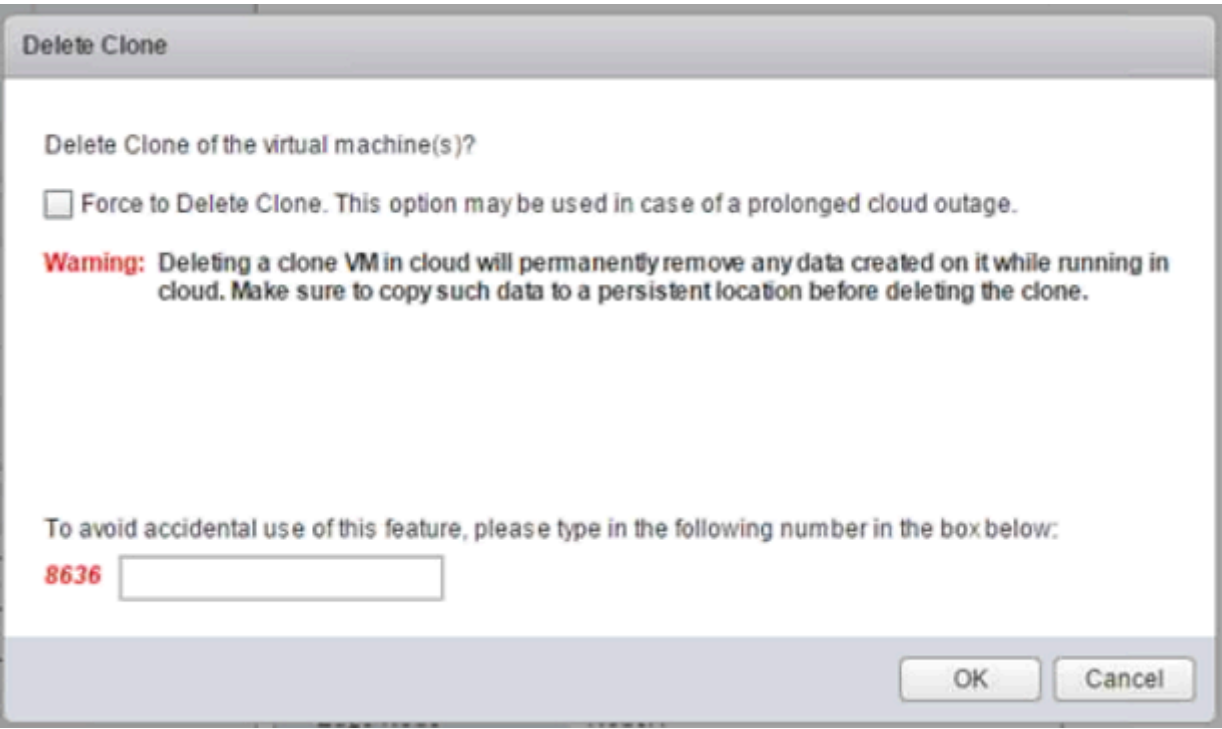
Detach

Cleanup

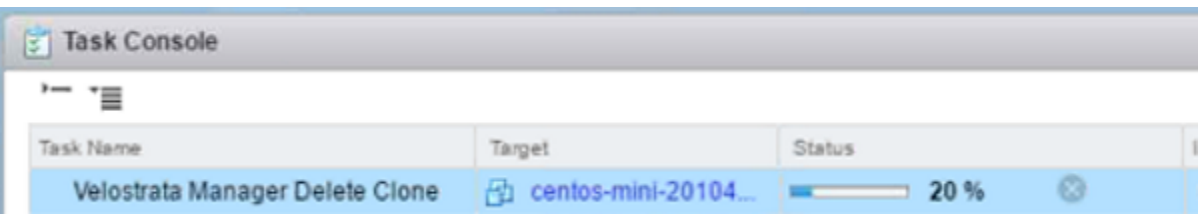
Deleting Test Clone via vCenter

To delete a Test Clone:


- 1. On the vSphere Web Client, select **Datacenter > Velostrata > Delete Clone**
- 2. Enter the number that appears in the box and click **OK**.



The process of deleting the Test Clone can be viewed on the Task Console by monitoring the created vSphere task:



The process can also be monitored via the Velostrata portlet:

Cloud Instance Information	
	<div>VM State</div> <div>Moving Back To vSphere (Running)</div> <div>Last Status</div> <div>Stopping cloud instance</div>
Pricing Model	On Demand
Cloud Status Checks	--
Run Mode	Test Clone
Cloud Extension	datacenter-2_vpc-1410ff71_147694
Storage Migration	Cache On Demand
Remote Console	Ready
Security Groups	Test hosts
Private IP Address	172.31.9.206
Public IP Address	--
Edge Node	NodeA
CPU	1 CPU
Memory	1 GB
Cloud Instance Id	i-0faeacdc7d0d63cfd
Instance Type	t2.micro
Storage Policy	Write Isolation
Network Adapter	eni-815bc4df

Running the Migration Wizard

The Migrate wizard in vSphere does the following steps:

1. Moves the VM to the cloud.
2. Migrates the storage to the cloud while the VM is running in cloud.
3. Prepare to detach the VM. This takes the data from the AWS S3 object, Azure blob, or GCP cloud storage and writes it to dedicated disks for the server.

Once the Migrate wizard is completed after several hours, the VM is **Ready to Detach**. See [Detaching the VM](#).

For Azure, AWS and GCP, there is a built-in recommendation engine that provides cost- and performance-optimized recommendations. In order to provide an effective recommendation, Velostrata recommends monitoring the VM usage for at least 7 active days. For more information, see [Monitoring VM Usage](#).

On-prem VMware to GCP

1. On the vSphere Web Client, select the desired **Virtual Machine**.
2. Right-click on the required VM and select **Velostrata Operations > Migrate**.
3. Select the **Velostrata Cloud Extension**.
4. Define a new name for the Cloud VM (if desired).
5. Click **Next**.

Full Migration - centos-mini-01111642-i0m

Velostrata Cloud Extension

Cloud Instance
Storage Policy
Networking
Migration
Summary

Velostrata Cloud Extension

Velostrata Cloud Extension: gcp_datacenter-2_1522570602_vLN

Cloud VM Name: centos-mini-01111642-i0m

Back Next Finish Cancel

6. Select the **Project** and **Instance Type** (VM size).

Three options are recommended for performance-optimized VMs, and three options are recommended for cost-optimized VMs. Additional notes:

- The prices are for compute cost only and do not include disk and network costs.
- If the VM has not been monitored for a sufficient period (7 days), a message appears indicating that the activity duration may be insufficient for accurate recommendations.
- If the online price list and/or sufficient monitoring periods are not available, no cost-optimized recommendations are provided.

7. Click **Next**.

Full Migration - centos-mini-04135336-30y

✓ Velostrata Cloud Extension

Cloud Instance

Storage Policy
Networking
Migration
Summary

Cloud Instance

Source VM	Provisioned	Observed Usage	Monitoring Duration:	Not monitored
CPU:	2	No information	Active Duration:	Not monitored
RAM:	2GB	No information		
Disks:	1			

Recommended Options:

Performance Optimized	Monthly Cost (Pay-As-You-Go)
n1-standard-2 (2 CPUs 7.5 GB RAM)	\$52.70
n1-highmem-2 (2 CPUs 13 GB RAM)	\$65.59
n1-highcpu-4 (4 CPUs 3.6 GB RAM)	\$78.62

Project: velos-auto-1

Instance Type: n1-standard-2 (2 CPUs 7.5 GB RAM)

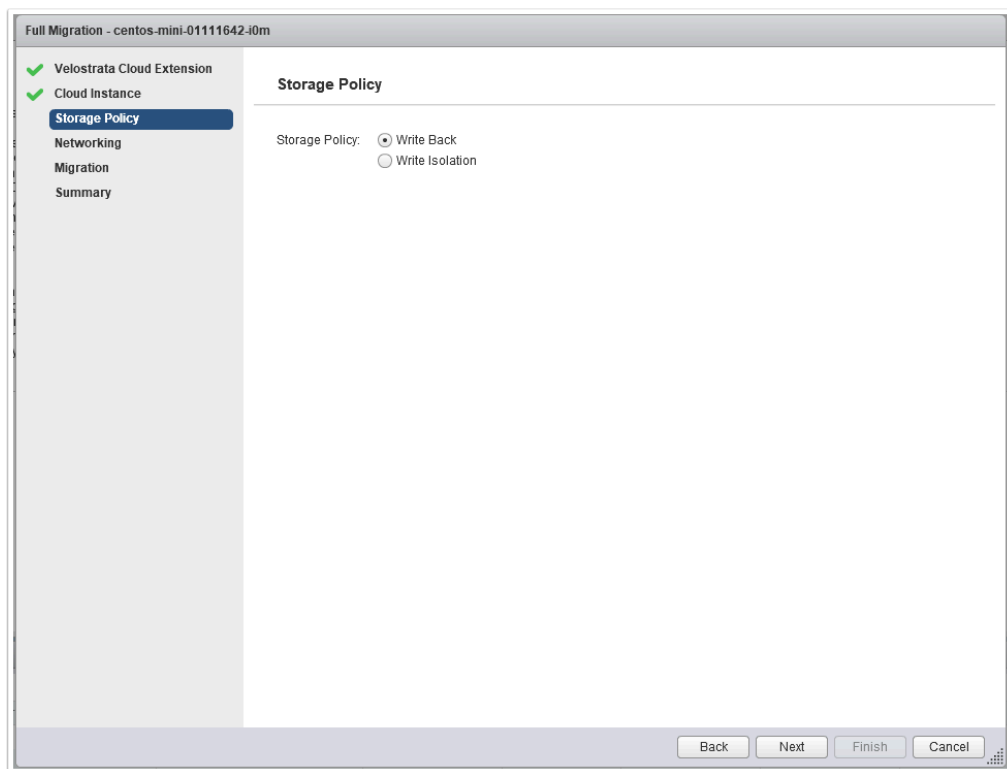
Back Next Finish Cancel

8. Select the **Storage Policy**, that is, either **Write Back** or **Write Isolation**. The choice of Storage Policy need to be carefully reviewed, as this will affect the data changes done while running in cloud:

- **Write back (default option):** When running in cloud using the write back policy, all changes in the cloud will be written to the on-premises storage. This write-back activity happens in background, in an interval of 5GB accumulated changes or 1 hour (whatever comes first).
- **Write isolation:** When using write isolation policy, all changes done while running in cloud are kept in cloud on the Velostrata Cloud Edge and are not persisted back on-premises. When moving the VM back to run on-premises, it will go back to its state and data point in time captured in the base snapshot. Related Virtual Machines that are moved to cloud together using the Write Isolation policy should be moved back on-premises together to maintain state alignment.

Note: Once the VM is running in cloud, the storage policy may be switched between Write Back and Write Isolation. To do this, right-click the VM and select **Reconfigure virtual machine**.

9. Click **Next**.



7. Select the **Storage Policy**, that is, either **Write Back** or **Write Isolation**. The choice of Storage Policy need to be carefully reviewed, as this will affect the data changes done while running in cloud:

- **Write back (default option):** When running in cloud using the write back policy, all changes in the cloud will be written to the on-premises storage. This write-back activity happens in background, in an interval of 5GB accumulated changes or 1 hour (whatever comes first).
- **Write isolation:** When using write isolation policy, all changes done while running in cloud are kept in cloud on the Velostrata Cloud Edge and are not persisted back on-premises. When moving the VM back to run on-premises, it will go back to its state and data point in time captured in the base snapshot. Related Virtual Machines that are moved to cloud together using the Write Isolation policy should be moved back on-premises together to maintain state alignment.

Note: Once the VM is running in cloud, the storage policy may be switched between Write Back and Write Isolation. To do this, right-click the VM and select **Reconfigure virtual machine**.

8. Click **Next**.

The screenshot shows the 'Full Migration' wizard for a VM instance. The left sidebar lists the steps: Velostrata Cloud Extension, Cloud Instance, Storage Policy, **Networking** (selected), Migration, and Summary. The main area is titled 'Networking' and contains the following fields:

- Subnet:** A dropdown menu showing '10.60.0.0/20'.
- Network Tags (comma separated):** A text input field containing 'velostrata'.
- Instance Service Account (optional):** A dropdown menu.
- Configure Private IP:** A dropdown menu showing 'Auto'.
- Edge Node:** A dropdown menu showing 'Node A'.
- External IP:** A dropdown menu showing 'None'.

At the bottom right, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

9. Select a cloud **Subnet**. Typically, the selection here would be of a private network subnet.

10. Enter the required Network Tags (comma separated), for example, **velostrata**. Network tags are used by networks to identify which instances are subject to certain firewall rules and network routes. For example, if you have several VM instances that are serving a large website, tag these instances with a shared word or term and then use that tag to apply a firewall rule that allows HTTP access to those instances.

11. Select the **Instance Service Account** (optional).

12. From the **Configure Private IP** drop-down list, select **Auto** to allow an available address on the subnet to be automatically assigned, or **Static** if a specific address assignment is required.

A. If you select **Static**, a **Static IP** field appears. Enter the required static IP for the instance or specify an ENI ID (e.g. **eni-xxxxxx**) to associate a reserved Elastic Network Interface.

13. From the **Edge Node** drop-down list, select the required node.

14. For External IP, select **None**, **Static** and enter the **External IP address name** (this is the name for an external IP address created on the GCP console previously) or **Ephemeral** (the external IP is assigned by Google). Notes:

- This IP appears as the **Public IP Address** in the Velostrata Cloud Extension portlet.
- If you select **Ephemeral** (the external IP is assigned by Google), the same setting persists when you detach, cleanup or cancel detach.
- If you select **static**, you will need to populate the external IP address name, too.

15. Click **Next**.

Full Migration - centos-mini-04135336-30y

- ✓ Velostrata Cloud Extension
- ✓ Cloud Instance
- ✓ Storage Policy
- ✓ Networking
- Migration**
- Summary

Migration

Disk Type:

Service Account:

Back Next Finish Cancel

16. Select the **Disk Type** and **Service Account**.
17. Click **Next**.

Full Migration - centos-mini-09201503-2dc-clone1531156775

- ✓ Velostrata Cloud Extension
- ✓ Cloud Instance
- ✓ Storage Policy
- ✓ Networking
- ✓ Migration
- Summary**

Summary

Velostrata Cloud Extension:	gcp_datacenter-2_1531156503_bth
Cloud Instance Type:	custom-2-2048 (2 CPUs 2 GB RAM)
Cloud VM Name:	centos-mini-09201503-2dc-clone1531156775
Project:	velos-auto-1
Service Account for Instance:	cloud-edge-permanent
Storage Policy:	Write Back
Network Tags:	velostrata
Subnet:	10.60.0.0/20
Edge Node:	Node A
Static IP:	Auto
External IP:	None
Disk Type:	SSD
Service Account:	cloud-edge-permanent

Back Next Finish Cancel

18. Review the summary and then click **Finish**.

The process of running the VM in the cloud and then migrating the VM can be viewed in the **Cloud Instance Information** portlet on the **VM Summary** page, and by monitoring the created vSphere task.

Once the Migrate wizard is completed after several hours, the VM is **Ready to Detach**. See [Detaching the VM](#).

AWS to GCP

During migration of an instance from AWS to GCP, Velostrata takes ownership of the instance disks at AWS. At the end of the process, the original AWS instance remains intact and powered off.

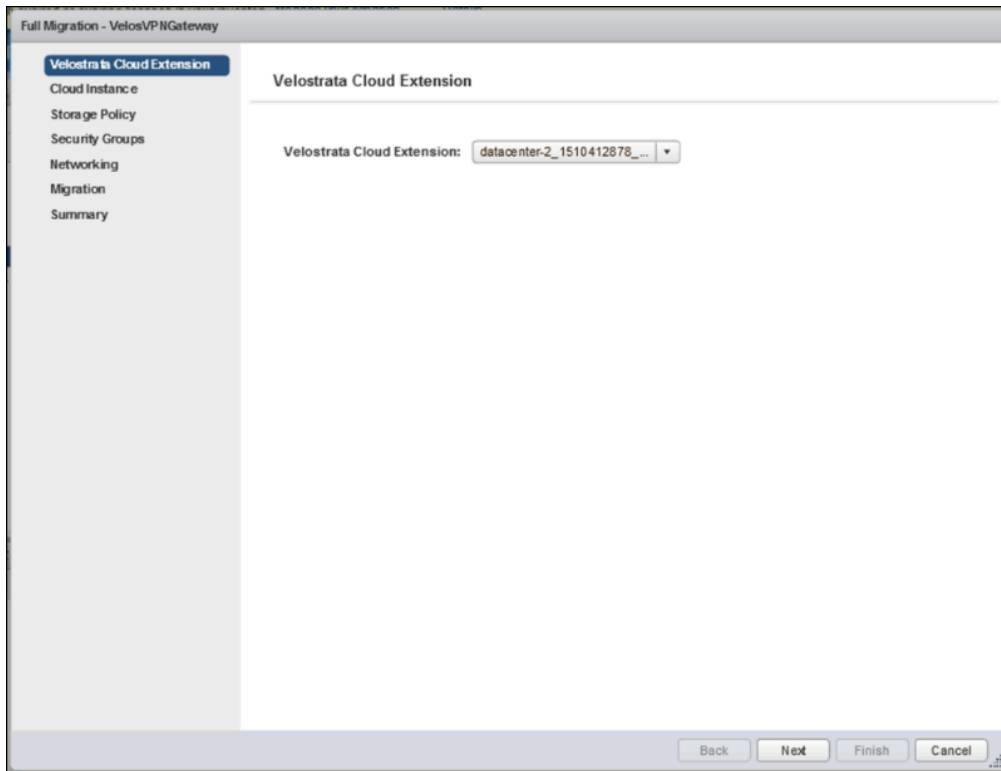
- Stops the source VM in AWS
- Creates the Velostrata VM Importer at AWS
- Attaches the disk from the source VM to the Importer
- Creates an instance in GCP
- Streams data from the importer to the GCP Cloud Extension
- Terminates the importer and re-attaches the disks to the source VM

For detailed instructions on how to migrate VMs from AWS in GCP, please refer to our [Runbook Automation section](#).

For clouds and operations supported in previous versions:

On-prem-to-AWS: To run the migration wizard from vSphere:

1. On the vSphere Web Client, select the desired **Virtual Machine**.
2. Right-click on the required VM and select **Velostrata Operations > Migrate**.



3. Select the **Velostrata Cloud Extension**.
4. Click **Next**.
5. Select the **Instance Type** (VM size). Three options are recommended for performance-optimized VMs, and three options are recommended for cost-optimized VMs.
Note: The prices are for compute cost only and do not include disk and network costs. Spot and reserved instances may also have price reduction plans.
Note: If the VM has not been monitored for a sufficient period (7 days), a message appears indicating that the activity duration may be insufficient for accurate recommendations.
Note: If the online price list is not available, no cost-optimized recommendations are provided.

Full Migration - VelosVPNGateway

✓ Velostrata Cloud Extension

Cloud Instance

Storage Policy

Security Groups

Networking

Migration

Summary

Cloud Instance

Source VM	Provisioned	Observed Usage	Monitoring Duration:	Not monitored
CPU:	2	No information		
RAM:	2GB	No information	Active Duration:	Not monitored
Disks:	1			

Recommended Options:

Performance Optimized	Monthly Cost (Pay-As-You-Go)
t2.medium (2 CPUs 4 GB RAM)	\$36.0
t2.large (2 CPUs 8 GB RAM)	\$72.57
m4.large (2 CPUs 8 GB RAM)	\$79.92

Instance Type: t2.medium (2 CPUs 4 GB RAM) ▼

Back Next Finish Cancel

6. Click **Next**.

Full Migration - VelosVPNGateway

✓ Velostrata Cloud Extension

✓ Cloud Instance

Storage Policy

Security Groups

Networking

Migration

Summary

Storage Policy

Storage Policy: ☒ Write Back ☐ Write Isolation

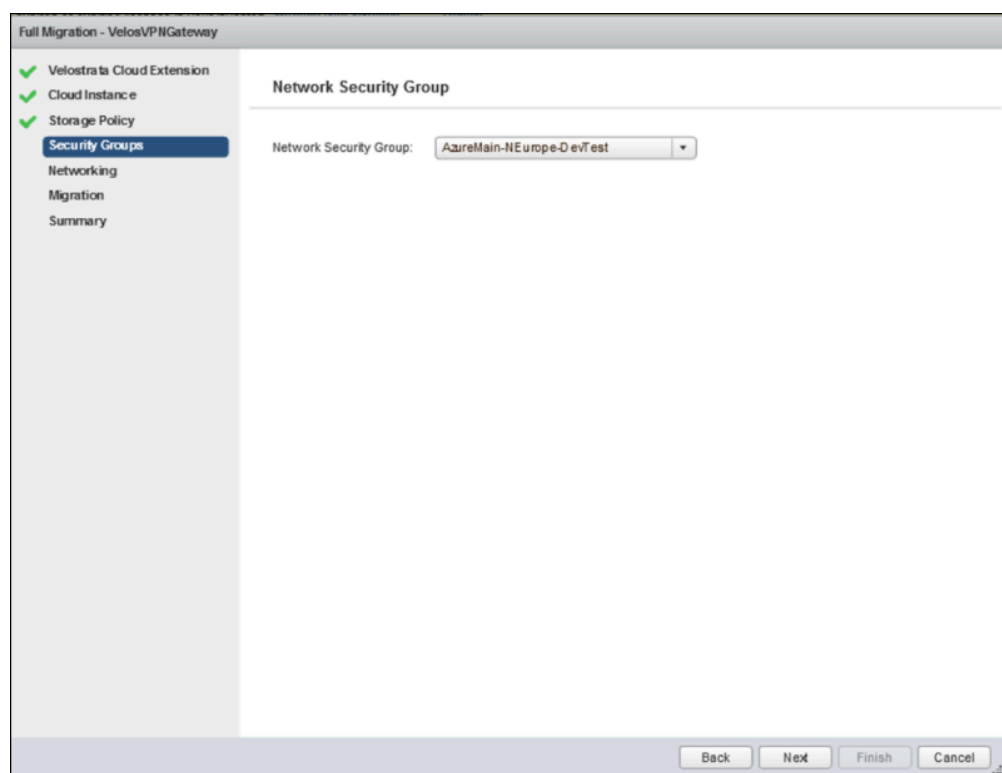
Back Next Finish Cancel

7. Select the **Storage Policy**, that is, either **Write Back** or **Write Isolation**. The choice of Storage Policy need to be carefully reviewed, as this will affect the data changes done while running in cloud:

- **Write back (default option):** When running in cloud using the write back policy, all changes in the cloud will be written to the on-premises storage. This write-back activity happens in background, in an interval of 5GB accumulated changes or 1 hour (whichever comes first).
- **Write isolation:** When using write isolation policy, all changes done while running in cloud are kept in cloud on the Velostrata Cloud Edge and are not persisted back on-premises. When moving the VM back to run on-premises, it will go back to its state and data point in time captured in the base snapshot. Related Virtual Machines that are moved to cloud together using the Write Isolation policy should be moved back on-premises together to maintain state alignment.

Note: Once the VM is running in cloud, the storage policy may be switched between Write Back and Write Isolation. To do this, right-click the VM and select **Reconfigure virtual machine**.

8. Click **Next**.



9. Select the required **Network Security Group**.

Note: If you do not enter a Network Security Group the default Network Security Group configured for the Cloud Extension is used.

Note: If public access is required from the internet to the VM, a DMZ is required with an associated security group, including appropriate inbound and outbound rules.

10. Click **Next**.

Full Migration - VelosVPN Gateway

- ✓ Velostrata Cloud Extension
- ✓ Cloud Instance
- ✓ Storage Policy
- ✓ Security Groups
- Networking**
- Migration
- Summary

Networking

Subnet:

Configure Private IP:

Edge Node:

Back Next Finish Cancel

Full Migration - VelosVPN Gateway

- ✓ Velostrata Cloud Extension
- ✓ Cloud Instance
- ✓ Storage Policy
- ✓ Security Groups
- Networking**
- Migration
- Summary

Networking

Subnet:

Configure Private IP:

Static IP: *

Edge Node:

Back Next Finish Cancel

11. Select a **Subnet**. Typically, the selection here would be of a private network subnet. When Cloud Edge nodes (A, B) are placed in different AZs, the Cloud Edge node in the same AZ as the selected subnet is automatically used, otherwise a manual node selection is required. If left blank, the **default** selection for this field is the **Default Workload Subnet** configured for the Cloud Extension.

12. From the **Configure Private IP** drop-down list, select **Auto** to allow an available address on the subnet to be automatically assigned, or **Static** if a specific address assignment is required.
13. If you select **Static**, a **Static IP** field appears. Enter the required static IP for the instance or specify an ENI ID (e.g. **eni-xxxxxx**) to associate a reserved Elastic Network Interface.
14. From the **Edge Node** drop-down list, select the required node. When Cloud Edge nodes are placed in the same Availability Zone (AZ), a manual selection of the **Cloud Edge node** to use is required.
15. Click **Next**.

Full Migration - centos-mini

✓ Velostrata Cloud Extension
✓ Cloud Instance
✓ Storage Policy
✓ Security Groups
✓ Networking
Migration
Summary

Migration

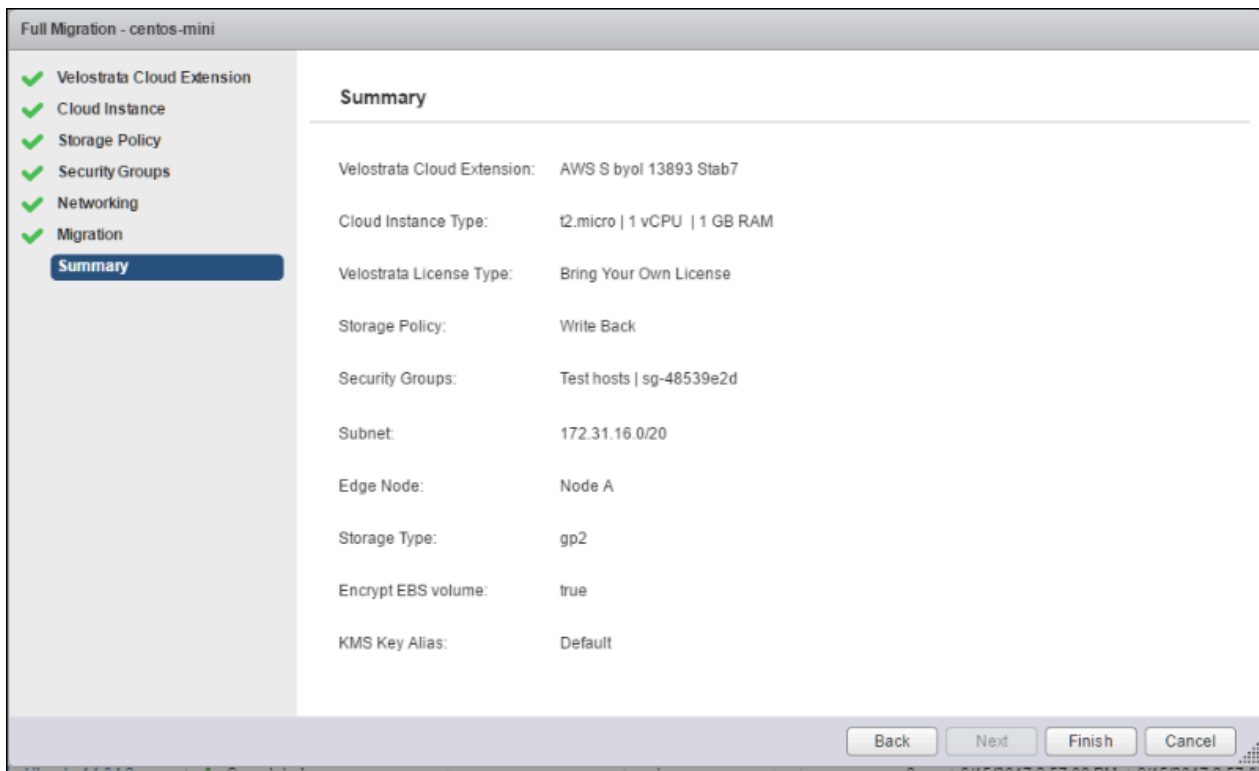
Storage Type:

Encrypt EBS volume: ☒

KMS Key ID:

Back Next Finish Cancel

16. Select the **Storage Type**.
17. Select **Encrypt EBS volume**, if you are using EBS encryption for native volumes, and from **KMS Key ID**, select the encryption key alias to be used. If this is not specified, the default key is used.
18. Click **Next**.



19. Review the summary and then click **Finish**.

The process of running the VM in the cloud and then migrating the VM can be viewed in the **Cloud Instance Information** portlet on the **VM Summary** page, and by monitoring the created vSphere task.

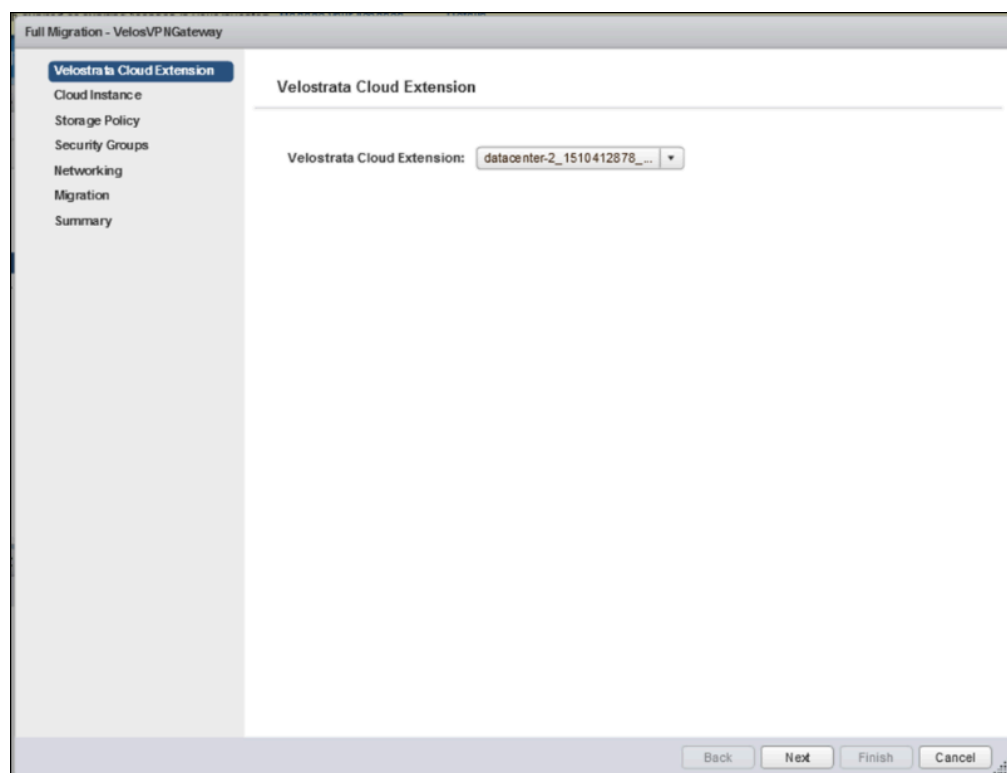
Cloud Instance Information	
VM State	Running
Last Status	Running Migrate To Cloud task
Cloud Status Checks	System Status: ok, Instance Status: ok
Cloud Extension	AWS-Ireland
Storage Migration	<div><div></div></div> Migrating (29GB of 40GB) ⏏ i
Remote Console	Ready
Security Groups	Ben-Demo-EU-N-sgWorkloads-1XQTDXLFI0D
Private IP Address	111.0.3.202

Once the Migrate wizard is completed after several hours, the VM is **Ready to Detach**. See [Detaching the VM](#).

On-prem-to-Azure: To run the migration wizard from vSphere:

1. On the vSphere Web Client, select the desired **Virtual Machine**.

2. Right-click on the required VM and select **Velostrata Operations > Migrate**.



3. Select the **Velostrata Cloud Extension**.
4. Click **Next**.
5. Select the **Instance Type** (VM size). Three options are recommended for performance-optimized VMs, and three options are recommended for cost-optimized VMs.
Note: The prices are for compute cost only and do not include disk and network costs. Spot and reserved instances may also have price reduction plans.
Note: If the VM has not been monitored for a sufficient period (7 days), a message appears indicating that the activity duration may be insufficient for accurate recommendations.
Note: If the online price list is not available, no cost-optimized recommendations are provided.
6. Select whether to **Show only types supporting premium storage**.
Note: Instances that use premium storage may have a different cost.
7. Select the **Resource Group** and **Availability Set**.
8. (Windows) Select whether to use a **Cloud-provided license**, or if you have an existing on-premises Windows Server/Client license with active Software Assurance (SA), select **Hybrid Use Windows Server** or **Hybrid Use Windows Client** to apply the Azure Hybrid Use Benefit.

Full Migration - w12core-11181341-DB

✓ Velostrata Cloud Extension

Cloud Instance

Storage Policy

Security Groups

Networking

Migration

Summary

Note: Activity duration may be insufficient for accurate recommendations

Cloud Instance

Source VM	Provisioned	Observed Usage	Monitoring Duration:
CPU:	2	10%	0 days
RAM:	2GB	0.25GB	Active Duration: 0 days
Disks:	1		

Recommended Options:

Show only types supporting premium storage ☐

Performance Optimized	Monthly Cost (Pay-As-You-Go)
basic_a2 (2 CPUs 3.5 GB RAM)	\$81.36
standard_a2_v2 (2 CPUs 4 GB RAM)	\$93.60
standard_a2 (2 CPUs 3.5 GB RAM)	\$129.6

Cost Optimized	Monthly Cost (Pay-As-You-Go)
basic_a0 (1 CPU 0.75 GB RAM)	\$12.95
standard_a0 (1 CPU 0.75 GB RAM)	\$14.39
standard_a1_v2 (1 CPU 2 GB RAM)	\$44.64

Instance Type:

Resource Group:

Availability Set:

Windows License:

Back Next Finish Cancel

9. Click **Next**.

Full Migration - VelosVPNGateway

✓ Velostrata Cloud Extension

✓ Cloud Instance

Storage Policy

Security Groups

Networking

Migration

Summary

Storage Policy

Storage Policy: ☒ Write Back ☐ Write Isolation

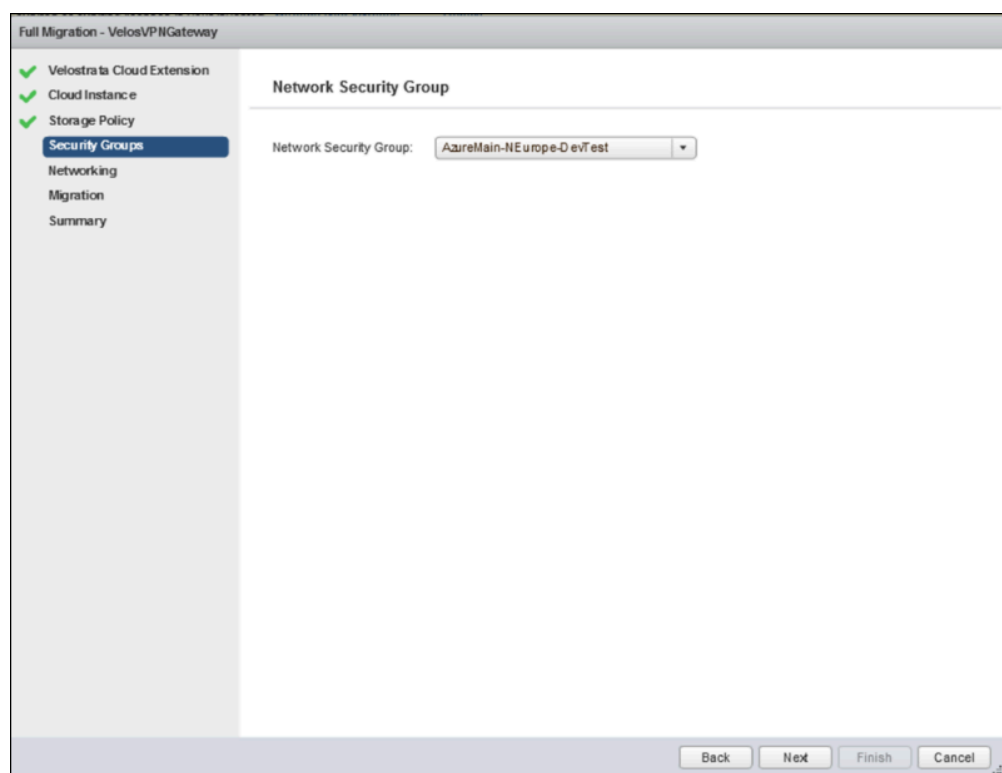
Back Next Finish Cancel

10. Select the **Storage Policy**, that is, either **Write Back** or **Write Isolation**. The choice of Storage Policy need to be carefully reviewed, as this will affect the data changes done while running in cloud:

- **Write back (default option):** When running in cloud using the write back policy, all changes in the cloud will be written to the on-premises storage. This write-back activity happens in background, in an interval of 5GB accumulated changes or 1 hour (whichever comes first).
- **Write isolation:** When using write isolation policy, all changes done while running in cloud are kept in cloud on the Velostrata Cloud Edge and are not persisted back on-premises. When moving the VM back to run on-premises, it will go back to its state and data point in time captured in the base snapshot. Related Virtual Machines that are moved to cloud together using the Write Isolation policy should be moved back on-premises together to maintain state alignment.

Note: Once the VM is running in cloud, the storage policy may be switched between Write Back and Write Isolation. To do this, right-click the VM and select **Reconfigure virtual machine**.

11. Click **Next**.



12. Select the required **Network Security Group**.

Note: If you do not enter a Network Security Group the default Network Security Group configured for the Cloud Extension is used.

13. Click **Next**.

Full Migration - VelosVPN Gateway

- ✓ Velostrata Cloud Extension
- ✓ Cloud Instance
- ✓ Storage Policy
- ✓ Security Groups
- Networking**
- Migration
- Summary

Networking

Subnet:

Configure Private IP:

Edge Node:

Back Next Finish Cancel

Full Migration - VelosVPN Gateway

- ✓ Velostrata Cloud Extension
- ✓ Cloud Instance
- ✓ Storage Policy
- ✓ Security Groups
- Networking**
- Migration
- Summary

Networking

Subnet:

Configure Private IP:

Static IP: *

Edge Node:

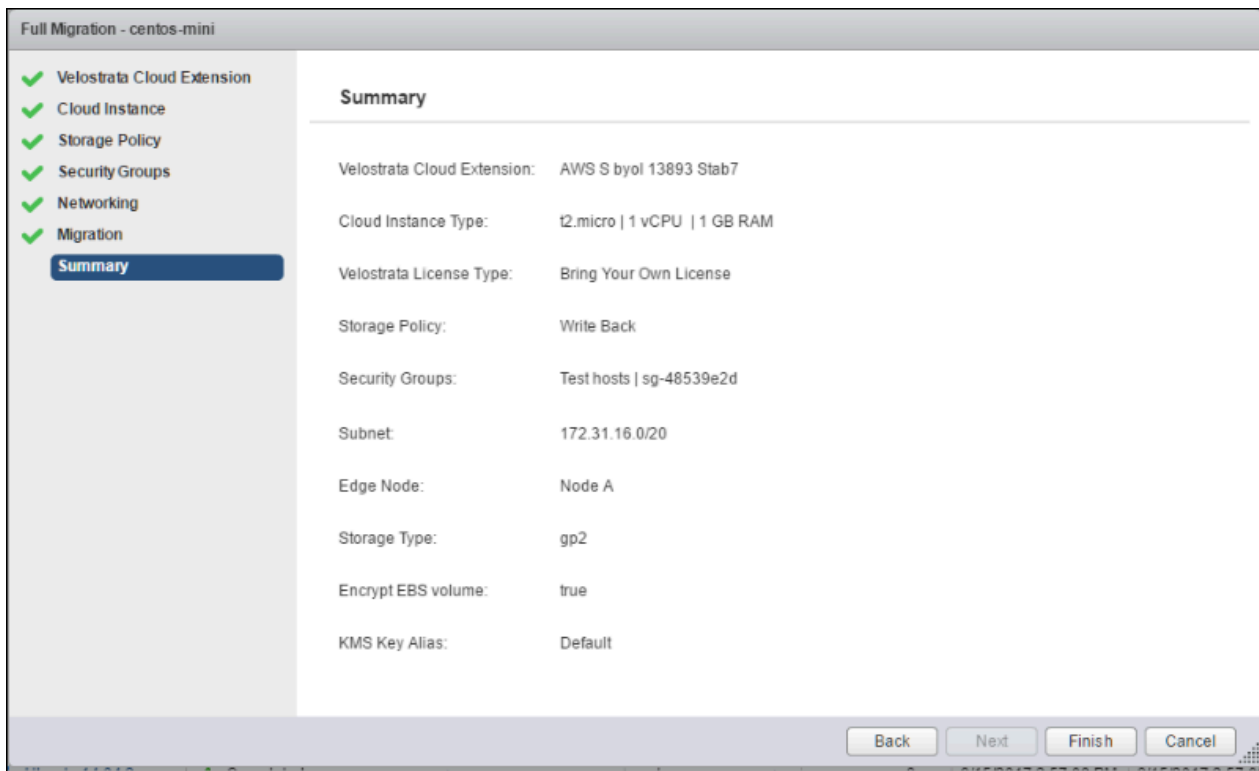
Back Next Finish Cancel

14. Select a **Subnet**. Typically, the selection here would be of a private network subnet. When Cloud Edge nodes (A, B) are placed in different AZs, the Cloud Edge node in the same AZ as the selected subnet is automatically used, otherwise a manual node selection is required. If left blank, the **default** selection for this field is the **Default Workload Subnet** configured for the Cloud Extension.

13. From the **Configure Private IP** drop-down list, select **Auto** to allow an available address on the subnet to be automatically assigned, or **Static** if a specific address assignment is required.
14. If you select **Static**, a **Static IP** field appears. Enter the required static IP for the instance or specify an ENI ID (e.g. **eni-xxxxx**) to associate a reserved Elastic Network Interface.
15. From the **Edge Node** drop-down list, select the required node. A manual selection of the **Edge Node** to use is required. Select **Node A** or **Node B**. The default selection is **Node A**.
16. Click **Next**.

The screenshot shows a window titled "Full Migration - centos-mini". On the left is a sidebar with a checklist of components: "Velostrata Cloud Extension", "Cloud Instance", "Storage Policy", "Security Groups", "Networking", "Migration" (highlighted in blue), and "Summary". The main content area is titled "Migration" and contains three settings: "Storage Type" set to "gp2", "Encrypt EBS volume" checked with a checkbox, and "KMS Key ID" set to "Default". At the bottom right of the window are four buttons: "Back", "Next", "Finish", and "Cancel".

17. Select the **Storage Type**.
18. Click **Next**.



19. Review the summary and then click **Finish**.

The process of running the VM in the cloud and then migrating the VM can be viewed in the **Cloud Instance Information** portlet on the **VM Summary** page, and by monitoring the created vSphere task.

Cloud Instance Information	
VM State	Running
Last Status	Running Migrate To Cloud task
Cloud Status Checks	System Status: ok, Instance Status: ok
Cloud Extension	AWS-Ireland
Storage Migration	<div><div></div></div> Migrating (29GB of 40GB) i
Remote Console	Ready
Security Groups	Ben-Demo-EU-N-sgWorkloads-1XQTDXLFI0D
Private IP Address	111.0.3.202

Once the Migrate wizard is completed after several hours, the VM is **Ready to Detach**. See [Detaching the VM](#).

To run the migration using PowerShell:

1. In PowerShell, connect to the Velostrata Manager by running **Connect-VelostrataManager**.

```

PS C:\Users\Administrator> Connect-VelostrataManager

cmdlet Connect-VelostrataManager at command pipeline position 1
Supply values for the following parameters:
Server: 192.168.15.124
Username: apiuser
Password: *****

Server          Port      Username
-----
192.168.15.124  443      apiuser

PS C:\Users\Administrator>

```

2. When prompted enter details for the **Server**, **Username** (**apiuser**) and **Password** (the subscription ID).
3. To start the migration run:

```

Invoke-VelosMigration -StorageSpec <String> [-Id] <String[]> [-StoragePolicy <String>] [-
PricingModelType <String>] [-MaxPriceUSD <Nullable`1[Double]>] [-
DefinedDurationHours<Nullable`1[Int32]>] -CloudExtension
<CloudExtensionDescriptionWrapper> -InstanceType <String> [-SecurityGroupIds
<List`1[String]>] [-NetworkTags <List`1[String]>] [-SubnetId <String>] [-
TargetInstanceName <String>] [-CloudDetailsName <String>] [-StaticAddress <String>]
[-EdgeNode <String>] [-ResourceGroupId <String>] [-AvailabilitySetId <String>] [-
AzureHubLicenseType <AzureHubLicenseType>] [-EncryptDisk <SwitchParameter>] [-
DiskEncryptionKey <String>] [<CommonParameters>]

```

The cmdlet invokes the combined actions of **Move-VelosVm**, **Start-VelosStorageMigration** and **Start-VelosPrepareToDetach**.

Invoke-VelosMigration

SYNOPSIS

This cmdlet invokes combined actions of Move-VelosVm, Start-VelosStorageMigration and Start-VelosPrepareToDetach.

Aws parameters:

EncryptDisk - will create an encrypted EBS disk during prepare to detach stage. When selected, you can provide an alias key ID using -DiskEncryptionKey, or let the system use the default CMK DiskEncryptionKey - when using -EncryptDisk, you can specify a KMS key alias. Please note that the Key should be created in the KMS prior to the operation and velosMgrGroup should be added to the list of users which can assign the KMS key.

SYNTAX

```
Invoke-VelosMigration -StorageSpec <String> [-Id] <String[]> [-StoragePolicy <String>] [-PricingModelType <String>] [-MaxPriceUSD <Double>] [-DefinedDurationHours <Int32>] -CloudExtension <CloudExtensionDescriptionWrapper> -InstanceType <String> [-SecurityGroupIds <List`1[String]>] [-NetworkTags <List`1[String]>] [-SubnetId <String>] [-TargetInstanceName <String>] [-CloudDetailsName <String>] [-StaticAddress <String>] [-EdgeNode <String>] [-ResourceGroupId <String>] [-AvailabilitySetId <String>] [-AzureHubLicenseType <AzureHubLicenseType>] [-EncryptDisk <SwitchParameter>] [-DiskEncryptionKey <String>] [<CommonParameters>]
```

DESCRIPTION

The cmdlet invokes combined actions of Move-VelosVm, Start-VelosStorageMigration and Start-VelosPrepareToDetach. For detailed information about parameters please see respective help.

RELATED LINKS

Unknown
Velostrata website: <http://www.velostrata.com>

REMARKS

To see the examples, type: "get-help Invoke-VelosMigration -examples".
For more information, type: "get-help Invoke-VelosMigration -detailed".
For technical information, type: "get-help Invoke-VelosMigration -full".
For online help, type: "get-help Invoke-VelosMigration -online"

Detaching the VM

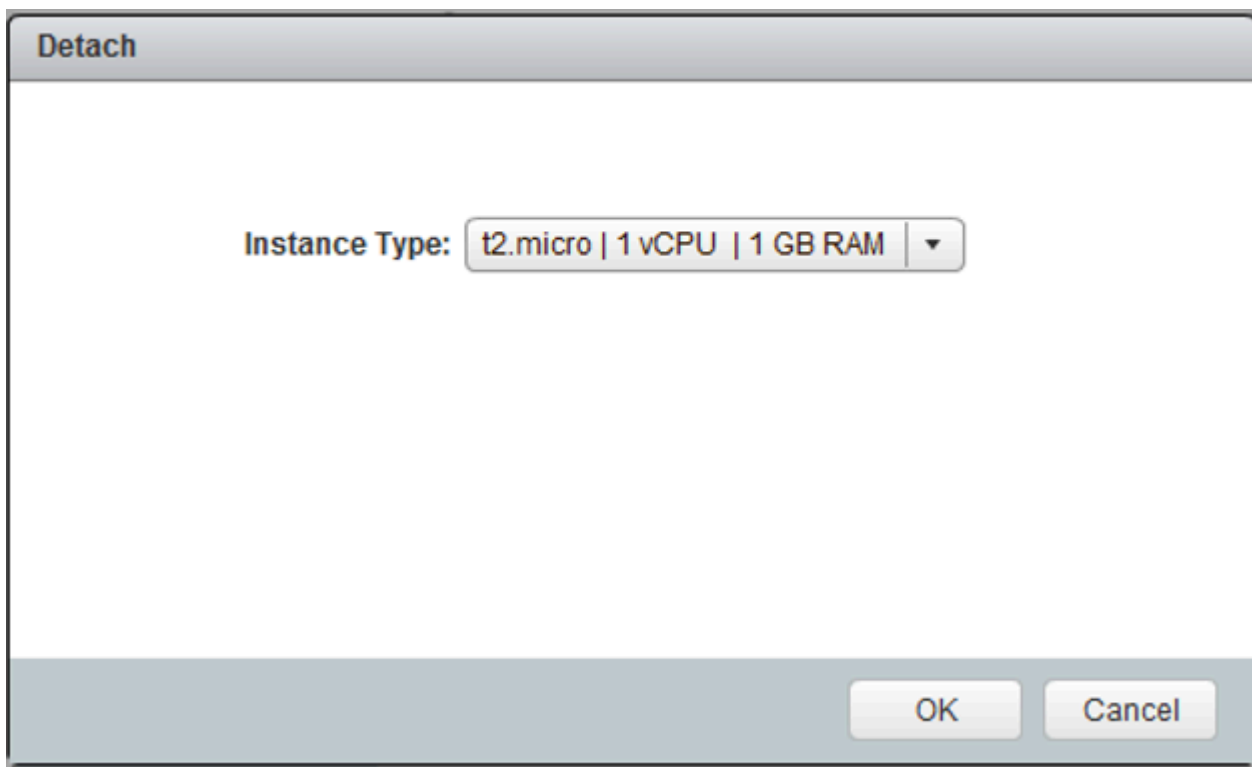
Once the VM is "Ready to detach" and the preparing to detach task completes successfully, you can detach the VM. You must assign a scheduled downtime slot for detaching.

Detaching is a sequence in which the VM will shut down, perform necessary last synchronization including adjusting instance size, attach the native disks to the instance, and start the instance.

After detaching the VM, perform any required validation that the VM is functioning correctly, and then either cleanup or rollback (if you do not want to detach the VM from Velostrata). See [Starting the Detach Cleanup](#)

On-prem-to-Cloud: To detach in vSphere:

1. On the vSphere Web Client, select the desired **Virtual Machine**.
2. Right-click on the required VM and select **Velostrata Operations > Migration Operations > Detach**.
3. Select a new instance type (optional) and click OK.



You can monitor the detach progress from vCenter:

Cloud Instance Information	
VM State	Stopping
Last Status	--
Cloud Extension	gcp_datacenter-2_1531156503_bth
Storage Migration	Detaching
Remote Console	Ready
Network tags	velostrata
Private IP Address	10.60.0.2
Public IP Address	--
Preferred Edge Node	NodeA
Actual Edge Node	NodeA
CPU	2 CPUs
Memory	2 GB
Cloud Instance Id	centos-mini-09201503-2dc-clone1531156775
Project	velos-auto-1
Zone	europa-west1-d
Service Account	cloud-edge-permanent@velos-auto-1.iam.gserviceaccount.com
Instance Type	custom-2-2048
Storage Policy	Write Back (uncommitted: 4.2MB)
Network Adapter	--

After the detach process is completed, the VM state will be listed as **Detached**.

On-prem-to-Cloud: To detach the VM using PowerShell:

1. In Powershell, connect to the Velostrata Manager by running **Connect-VelostrataManager**.

```
PS C:\Users\Administrator> Connect-VelostrataManager
cmdlet Connect-VelostrataManager at command pipeline position 1
Supply values for the following parameters:
Server: 192.168.15.124
Username: apiuser
Password: *****

Server          Port          Username
-----
192.168.15.124  443          apiuser

PS C:\Users\Administrator>
```

2. When prompted enter details for the **Server**, **Username** (**apiuser**) and **Password** (the subscription ID).
3. To detach the VM, run **get-vm myserver | Start-VelosDetach -InstanceType string**.

Note: To find the **InstanceType** you can use the **Get-VelosCeInstanceType** command.

```
PS C:\Users\Administrator> get-vm mytestvm |Start-VelosDetach -InstanceType Standard_DS1
```

Id	EntityId	Type	Initiator	ExternalTaskId	State	Start
t-7	vm-122	DetachVm	powershell_192.168.15.50		Running	6/21/

4. To check the state of the task, run **Get-Velostask [ID]** and optionally **Get-Velostask [ID] | fl ***

```
PS C:\Users\Administrator> Get-VelosTask t-7 |fl *
```


Id : t-7
EntityId : vm-122
Type : DetachVm
IsCancelled : False
Initiator : powershell_192.168.15.50
ExternalTaskId : task-4356
State : Running
ErrorMessage :
ErrorDetails :
Progress : 8
ProgressMessage : Stopping workload instance
StartTime : 6/21/2016 10:58:50 AM
EndTime :
AdditionalInfo : {[DetachProcessedRecords, 0], [DetachTotalRecords, 0], [ExporterInstanceId, /subscriptions/1836565f-4796-bed1-6dc575e4de1f/resourceGroups/Velostrata-Azure-WestEU-2958cd-4907/providers/MicrosoftCompute/virtualMachines/Velostrata-Exporter-2958cd-0539]}

5. Monitor the created vSphere Cloud Instance Information and task. The **VM State** is **Stopped** and the **Storage Migration** is **Detaching**.

Recent Tasks							
Task Name	Target	Initiator	Status	Queued For	Start Time	Completion Time	Server
Velostrata Manager Detach VM	myTestVM	powershell_192.16...	51 %	8 ms	6/21/2016 1:58:58 PM		192.168.15.103

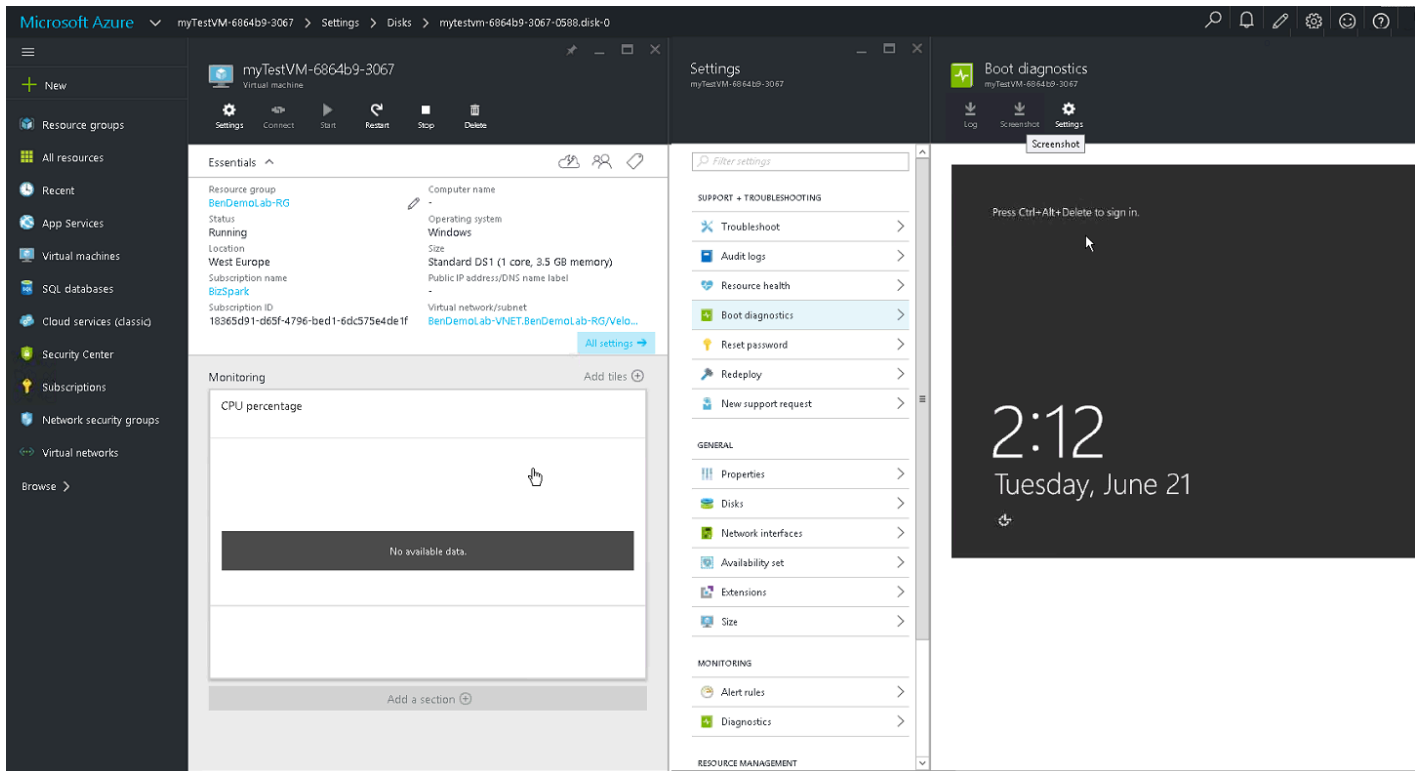
Cloud Instance Information	
VM State	Stopped
Last Status	--
Cloud Extension	Azure-WestEU
Storage Migration	Detaching
Remote Console	Not ready
Security Groups	poc.sgWorkloads.BenDemoLab
Private IP Address	222.222.0.4
Public IP Address	--
Edge Node	NodeA
CPU	--
Memory	--
Cloud Instance Id	myTestVM-6864b9-3067
Instance Type	Standard_DS1
Availability Set	--
Resource Group	/subscriptions/18365d91-d65f-4
Storage Mode	--
Network Adapter	--

Once the task completes successfully the **VM State** is **Running** and the **Storage Migration** is **Detached**.

Recent Tasks			
Task Name	Target	Initiator	Status
Velostrata Manager Detach VM	 myTestVM	powershell_192.16...	✔ Completed

Cloud Instance Information	
VM State	Running
Last Status	--
Cloud Extension	Azure-WestEU
Storage Migration	Detached
Remote Console	Ready
Security Groups	poc.sgWorkloads.BenDemoLab-RG
Private IP Address	222.222.0.4
Public IP Address	--
Edge Node	NodeA
CPU	--
Memory	--
Cloud Instance Id	myTestVM-6864b9-3067
Instance Type	Standard_DS1

6. Connect to the VM and perform the necessary validations. For example, in Azure you can use **"Boot Diagnostics"** to see the VM has been booted.



Cloud-to-Cloud: To detach the VM using PowerShell:

This cmdlet starts the detach sequence for the specified workload in the target cloud. The workload must be in the "Ready to Detach" state in order to perform this operation. Once finished, the workload boots and runs natively in the target cloud. You must assign a scheduled downtime slot for detaching.

- To detach the VM, run **Start-VelosDetach -ID i-123abcd -InstanceType string**.

Note for AWS Marketplace Users:

If the VM was created in an AWS marketplace Cloud Extension, when the instance is detached from Velostrata, it is detached from the marketplace CE, a new instance is created with a bring your own license, and the volumes are attached to this new instance. Although the instance ID has changed, this has no impact on the operation of the instance as it has the same ENI ID and Private IP. The routing rules are also still valid. If the detach is canceled, the instance may or may not have the original instance ID. Nevertheless, the instance will have the same IP and tagging.

Cancelling the Detach

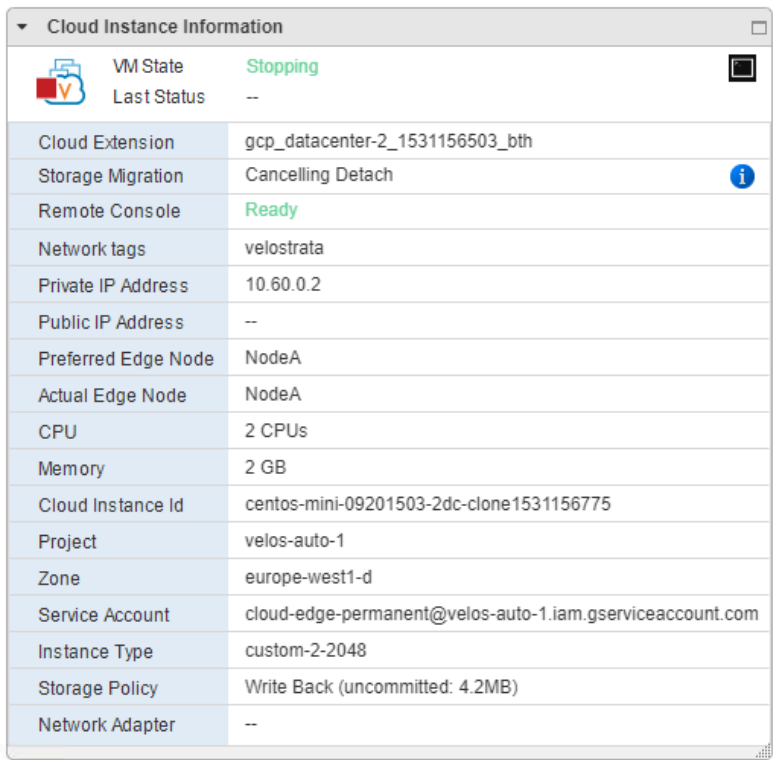
Once the VM is detached (and when the VM is showing as **Ready for Detach**) and for some reason you wish to go back to use the Velostrata cache, you can stop or cancel the detach process. This deletes the AWS EBS or Azure storage, and moves the system back to the state it was before the detach started - fully cached. In vSphere the menu option is **Cancel Detach**.


Note: Potential data loss may occur if the VM disks were changed when the VM was already in "Detached" state and the VM wrote on the native disks.

You cannot rollback if you have run the detach cleanup.

To cancel the detach in vSphere:

1. On the vSphere Web Client, select the desired **Virtual Machine**.
2. Right-click on the required VM and select **Velostrata Operations > Migration Operations > Cancel Detach**.
3. You will be prompted to type in four digits to confirm you want to cancel.
4. Once you confirm, the storage migration state will change to "Cancelling Detach".
5. When the cancellation is complete, the storage migration state will change back to "Fully Cached".



Cloud Instance Information		
	VM State	Stopping
	Last Status	--
Cloud Extension	gcp_datacenter-2_1531156503_bth	
Storage Migration	Cancelling Detach	
Remote Console	Ready	
Network tags	velostrata	
Private IP Address	10.60.0.2	
Public IP Address	--	
Preferred Edge Node	NodeA	
Actual Edge Node	NodeA	
CPU	2 CPUs	
Memory	2 GB	
Cloud Instance Id	centos-mini-09201503-2dc-clone1531156775	
Project	velos-auto-1	
Zone	europe-west1-d	
Service Account	cloud-edge-permanent@velos-auto-1.iam.gserviceaccount.com	
Instance Type	custom-2-2048	
Storage Policy	Write Back (uncommitted: 4.2MB)	
Network Adapter	--	

To rollback the detach via PowerShell, run the follwing command:

get-vm myserver | Stop-VelosDetach

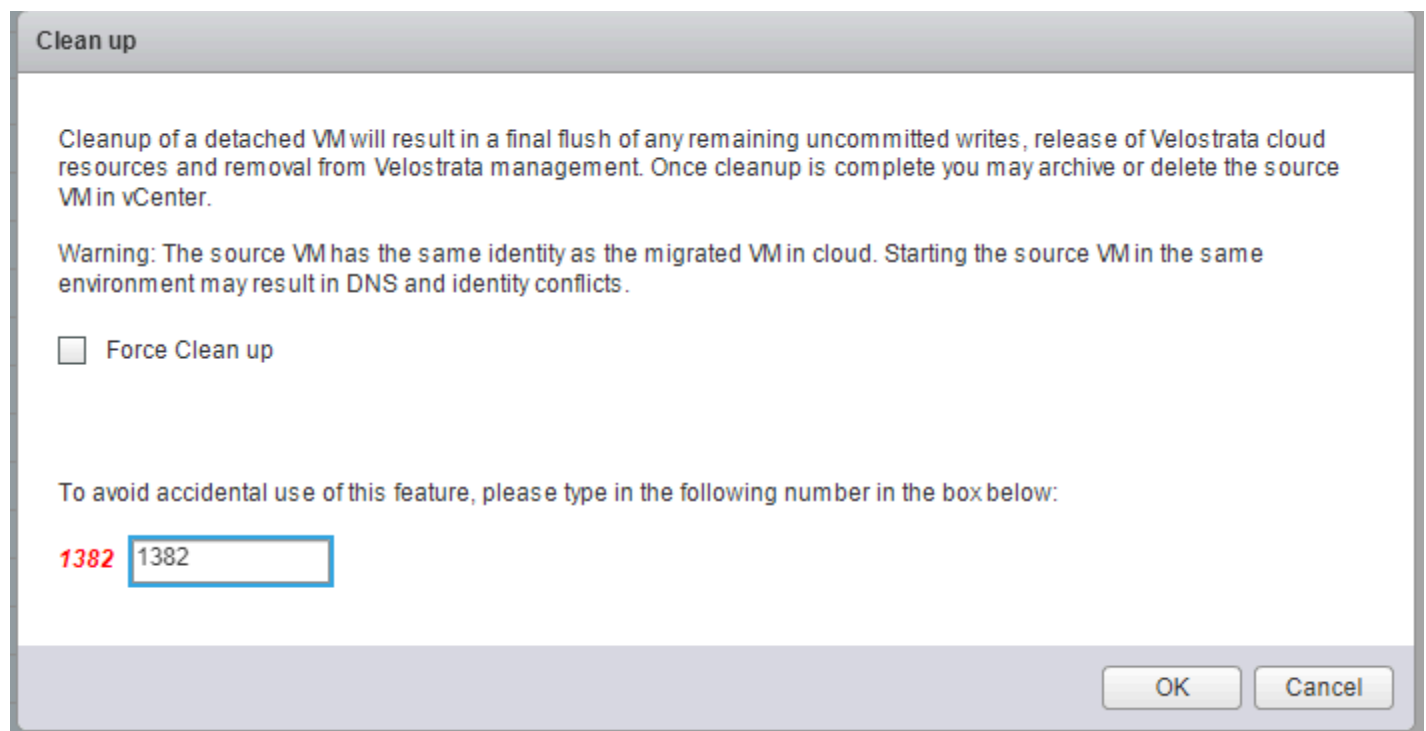
Starting the Detach Cleanup

Once the VM is detached and you have completed any required validation, you can start the detach cleanup. This marks the VM as unmanaged by Velostrata and removes the (temporary) storage objects. Once you have run the detach cleanup, the VM is managed by vCenter.

If for some reason you do not want to complete the detach cleanup and you want to revert back, you can move the VM back to fully cached. See [Rolling Back the Detach](#).

On-prem-to-Cloud: To start the detach cleanup in vSphere:

1. On the vSphere Web Client, select the desired **Virtual Machine**.
2. Right-click on the required VM and select **Velostrata Operations > Migration Operations > Cleanup**.



Clean up

Cleanup of a detached VM will result in a final flush of any remaining uncommitted writes, release of Velostrata cloud resources and removal from Velostrata management. Once cleanup is complete you may archive or delete the source VM in vCenter.

Warning: The source VM has the same identity as the migrated VM in cloud. Starting the source VM in the same environment may result in DNS and identity conflicts.


☐ Force Clean up

To avoid accidental use of this feature, please type in the following number in the box below:

1382

OK Cancel

3. Enter the number and then click **OK**. If you want to force a clean up, select **Force Clean up**.
4. The storage migration state will change to "Cleaning Up".
5. After the clean up process is completed, the VM is no longer managed by Velostrata, and is instead once again managed by vSphere.

Cloud Instance Information		
	VM State	Unmanaged
	Last Status	--
Cloud Extension	--	
Storage Migration	--	
Remote Console	Ready	
Security Groups	--	
Private IP Address	--	
Public IP Address	--	
Preferred Edge Node	--	
Actual Edge Node	--	
CPU	--	
Memory	--	
Cloud Instance Id	--	
Instance Type	--	
Storage Policy	--	
Network Adapter	--	

Onprem-to-Cloud: To start the detach cleanup using PowerShell:

1. In Powershell, connect to the Velostrata Manager by running **Connect-VelostrataManager**.

```
PS C:\Users\Administrator> Connect-VelostrataManager

cmdlet Connect-VelostrataManager at command pipeline position 1
Supply values for the following parameters:
Server: 192.168.15.124
Username: apiuser
Password: *****

Server          Port      Username
-----
192.168.15.124  443      apiuser

PS C:\Users\Administrator>
```

2. When prompted enter details for the **Server**, **Username** (**apiuser**) and **Password** (the subscription ID).
3. To start the detach cleanup, run **get-vm myserver | Start-VelosDetachCleanup**.
4. When prompted, enter **Y**.

```
PS C:\Users\Administrator> get-vm mytestvm | Start-VelosDetachCleanup

Confirm
Are you sure you want to perform this action?
Performing operation "Start-VelosDetachCleanup" on Target "vm-122".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y

Id      EntityId      Type      Initiator      ExternalTaskId      State      StartTime
--      -
t-8     vm-122         CleanupVm powershell_192.168.15.50      Running      6/21/20...
```

5. To check the state of the task, run **Get-Velostask [ID]** and optionally **Get-Velostask [ID] | fl ***

```
PS C:\Users\Administrator> Get-VelosTask t-8

Id      EntityId      Type      Initiator      ExternalTaskId      State      StartTime
--      -
t-8     vm-122         CleanupVm powershell_192.168.15.50      task-4362      Running      6/21/20...

PS C:\Users\Administrator> Get-VelosTask t-8 | fl *

Id           : t-8
EntityId     : vm-122
Type         : CleanupVm
IsCancelled  : False
Initiator    : powershell_192.168.15.50
ExternalTaskId : task-4362
State        : Running
ErrorMessage :
ErrorDetails :
Progress     : 65
ProgressMessage : Deleting unneeded workload resources
StartTime    : 6/21/2016 11:35:46 AM
EndTime      :
AdditionalInfo : {}
```

6. Monitor the created vSphere Cloud Instance Information and task. The **VM State** is **Running** and the **Storage Migration** is **Cleaning Up**.

Recent Tasks			
Task Name	Target	Initiator	Status
Reconfigure virtual machine	myTestVM	VSPHERE.LOCAL\...	✓ Completed
Consolidate virtual machine disk files	myTestVM	VSPHERE.LOCAL\...	✓ Completed
Remove snapshot	myTestVM	VSPHERE.LOCAL\...	✓ Completed
Remove snapshot	myTestVM	VSPHERE.LOCAL\...	✓ Completed
Velostrata Manager Cleanup VM	myTestVM	powershell_192.16...	<div> <div></div> 85 % </div>

▼ Cloud Instance Information	
VM State	Running
Last Status	--
Cloud Extension	Azure-WestEU
Storage Migration	Cleaning Up
Remote Console	Ready
Security Groups	poc.sgWorkloads.BenDemoLab-RG
Private IP Address	222.222.0.4
Public IP Address	--
Edge Node	NodeA
CPU	--
Memory	--
Cloud Instance Id	myTestVM-6864b9-3067
Instance Type	Standard_DS1

Cloud-to-Cloud: To start the detach cleanup using PowerShell:

1. In Powershell, connect to the Velostrata Manager by running **Connect-VelostrataManager**.
2. When prompted enter details for the **Server**, **Username** (**apiuser**) and **Password** (the subscription ID).
3. To start the detach cleanup, run **Start-VelosDetachCleanup -ID i-123abcd**.
4. When prompted, enter **Y**.

VM Migration - Advanced Operations

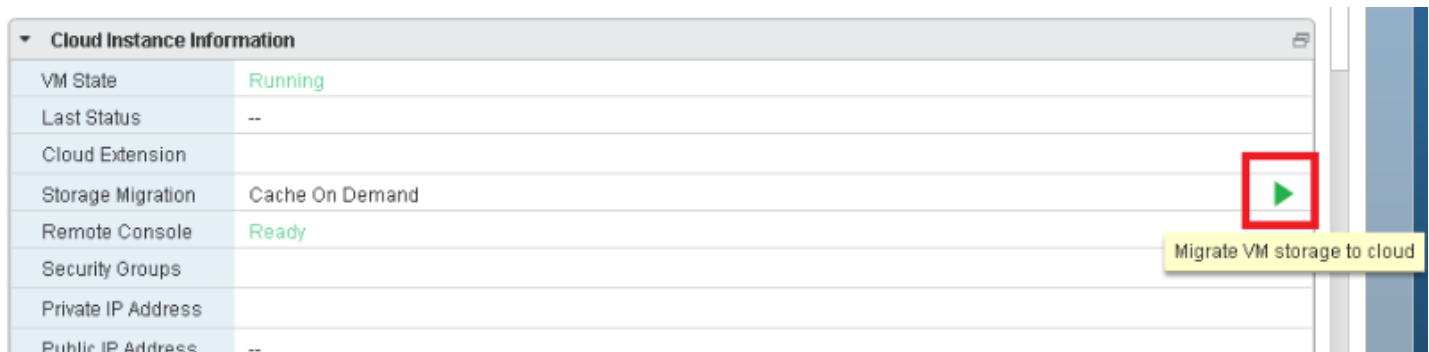
Migrating VM Storage to the Cloud

When a VM is running in cloud using the "Run in Cloud" operation, it uses the Velostrata intelligent "Cache on Demand" mechanism, which takes into account various sophisticated algorithms to efficiently predict and stream any needed storage from source VM to the destination cloud. At any point in time you can initiate full storage migration which will start the process of full data migration to destination cloud.

The storage migration allows for a fully migrated server that can be detached for a permanent cloud instance, which is no longer dependent on the source VM storage. Storage migration can also be used for a VM running in the cloud temporarily, and in this case the storage migration offers additional data redundancy point (backup), reduced network traffic, and better handling of WAN outages.

To migrate on-prem source VM storage to the cloud:

1. On the VSphere Web Client, select the desired **Virtual Machine**.
2. If the VM is still running on-premises, follow the steps in [Running the Migration Wizard](#).
3. If the VM is already running in the cloud, view the **Summary** tab, and in the **Storage Migration** row, click on the green arrow and select **Migrate VM storage to Cloud**. Alternatively, right-click the VM and select **Velostrata Operations** > **Migration Operations** > **Start Storage Migration**. The data migration starts.



The migration can take minutes to hours depending on various parameters like the size of the virtual machine, the bandwidth to the cloud, and the current utilization etc.

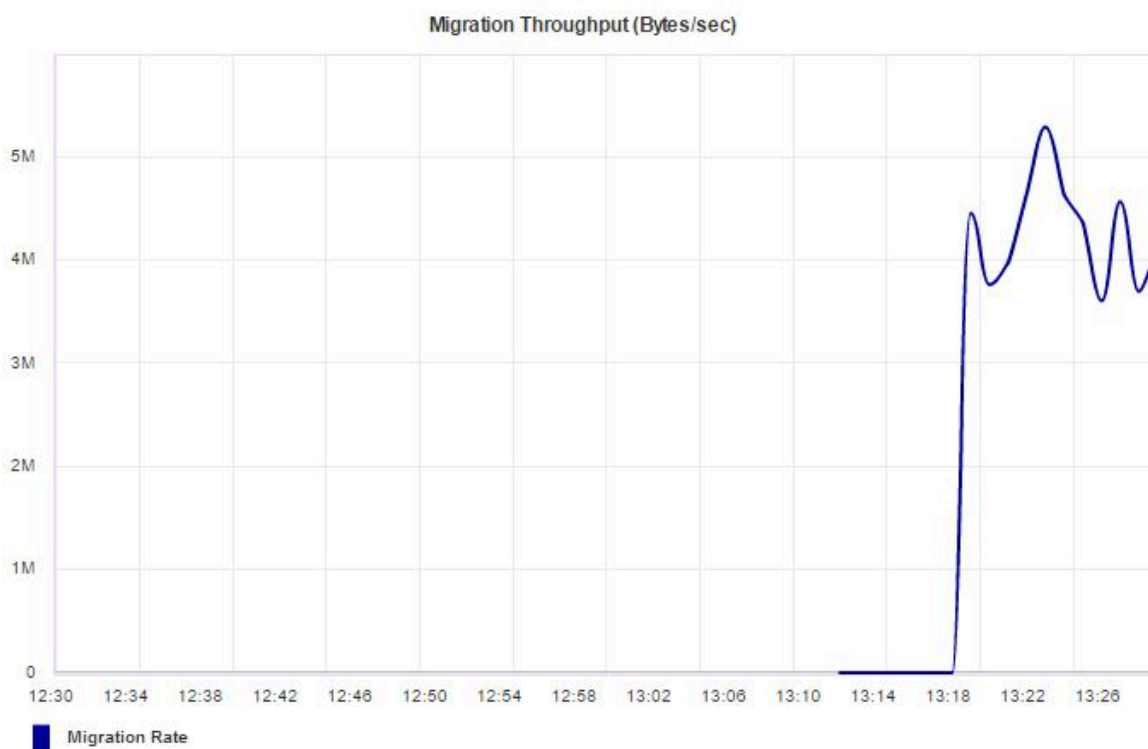
It is important to note that the storage migration activity is de-prioritized versus the regular storage reads of the VM, and the storage migration will occur primarily in idle times. This prevents any performance degradation for the production VMs running in cloud.

Migration can be monitored in the VM portlet on vSphere Web Client, this can also be used to pause the migration if desired.

Cloud Instance Information	
VM State	Running
Last Status	--
Cloud Extension	
Storage Migration	<div> <div></div> <div>Migrating (5GB of 40GB)</div> </div>
Remote Console	Ready
Security Groups	
Private IP Address	

In addition, you can also view a **Migration Throughput** graph.

- On the VSphere Web Client, select the desired **Datacenter** linked to the cloud extension.
- In the **Monitor** tab, select the **Velostrata Service** tab, choose the specific cloud extension and the time range to view the graph.



When storage migration is complete, the VM shows as **Fully Cached**.

Cloud Instance Information	
VM State	Running
Last Status	--
Cloud Extension	
Storage Migration	Fully Cached
Remote Console	Ready
Security Groups	

In this state, all VM disks are stored in an GCP Bucket (or AWS S3 object/Azure blob) and are accessible by our Cloud Edge appliances for all reads and writes. VM writes may still replicate back to the on-premises datastore if the original storage mode policy indicated that it should (“write back” as opposed to “write isolation”).

To migrate cloud source VM Storage to destination cloud:

1. In PowerShell, connect to the Velostrata Manager by running **Connect-VelostrataManager**.
2. When prompted enter details for the **Server**, **Username** (**apiuser**) and **Password** (the subscription ID).
3. To detach the cloud source VM storage, run **Start-VelosStorageMigration [-Id] <string[]>**.

Preparing to Detach the VM

After the VM is "Fully Cached" and you want to start the detach process, the first task required is "Prepare to detach" the VM from Velostrata. This task takes the VM disks from the Velostrata cache and object store and creates the native data drives in the target cloud. A Velostrata exporter is deployed automatically in the cloud to perform this task.

The exporter runs through all data disks and converts them to native cloud disks, after this first iteration is completed, the exporter continues to write the changes committed since its previous execution. This task runs in cycles.

After sufficient progress has been achieved (3 cycles), the VM is marked as "Ready to Detach".

The VM can then be detached from Velostrata in minutes. The Velostrata exporter continues to synchronize the VM disks from cache into the native cloud storage until detached or until manually stopped (stop prepare to detach). Once the VM is in the "Ready to Detach" state you will effectively have to "cut over" and will need to schedule a downtime slot for the actual detach action.

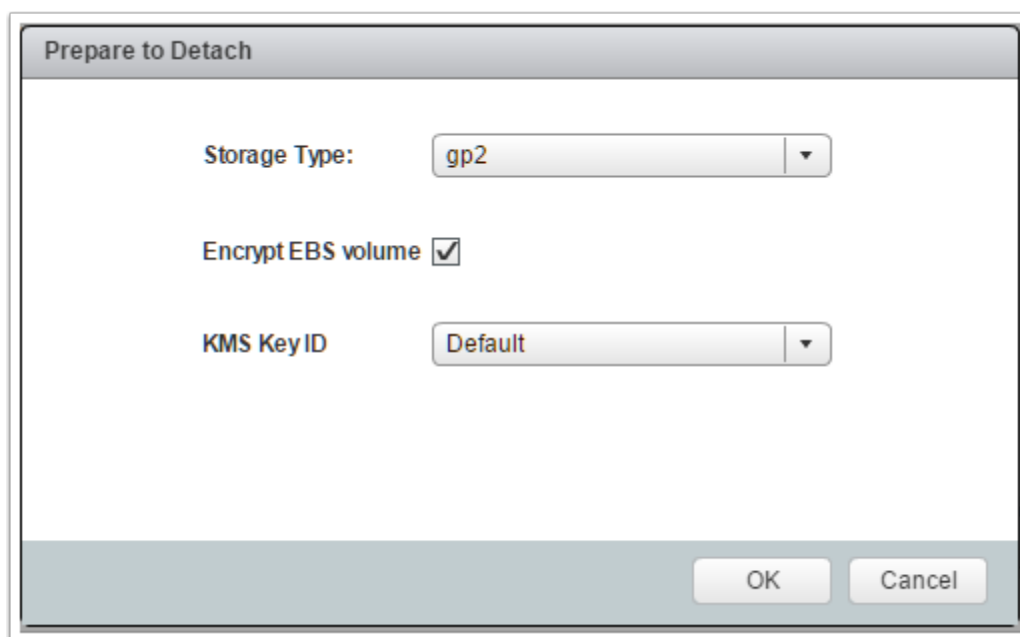
The VM must be in the **Fully Cached** state prior to running the prepare to detach operation. If the VM is not in the **Fully Cached** state, first run the procedure to migrate the VM storage to the cloud.

Note: If you want to stop (revert back) after the preparing to detach process has finished, you can stop or rollback the detach process.

When working in cache mode, all cached data is stored in encrypted disks attached to the Velostrata Cloud Extension. During detach, you can choose if you want to use encrypted disks or not, and can optionally specify the key to be used. For more information, see [EBS Encryption Key Preparation](#).

On-prem-to-Cloud: To prepare to detach in vSphere:

1. On the vSphere Web Client, select the desired **Virtual Machine**.
2. Right-click on the required VM and select **Velostrata Operations > Migration Operations > Prepare Detach**.



The image shows a 'Prepare to Detach' dialog box. It contains three fields: 'Storage Type' with a dropdown menu showing 'gp2', 'Encrypt EBS volume' with a checked checkbox, and 'KMS KeyID' with a dropdown menu showing 'Default'. At the bottom right are 'OK' and 'Cancel' buttons.

3. Select the **Storage Type** and then click **OK**.
4. For AWS, if you wish to use EBS encryption for native volumes, select **Encrypt EBS volume**, and select the encryption key alias to be used. If this is not specified, an AWS-generated KMS default key is used.

Note: If you want to use a specific KMS key for encryption, add the AWS Velostrata service user to the list of users who can assign the KMS key.

Cloud Instance Information	
VM State	Running
Last Status	--
Cloud Status Checks	System Status: ok, Instance Status: ok
Cloud Extension	AWS-Ireland
Storage Migration	Preparing To Detach (0 of 5,444 Records) i
Remote Console	Ready
Security Groups	Ben-Demo-EU-N-sgWorkloads-1XQTDXLFI0D
Private IP Address	111.0.3.147
Public IP Address	--
Edge Node	NodeA
CPU	1 CPU
Memory	1 GB
Cloud Instance Id	i-02e9cff02193e695a
Instance type	t2.micro

After the ready to detach process is completed, the VM is **Ready to Detach**.

Cloud Instance Information	
VM State	Running
Last Status	--
Cloud Status Checks	System Status: ok, Instance Status: ok
Cloud Extension	AWS-Ireland
Storage Migration	Ready To Detach
Remote Console	Ready
Security Groups	Ben-Demo-EU-N-sgWorkloads-1XQTDXLFI0D
Private IP Address	111.0.3.147
Public IP Address	--
Edge Node	NodeA
CPU	1 CPU
Memory	1 GB
Cloud Instance Id	i-02e9cff02193e695a
Instance type	t2.micro

GCP-to-Cloud: To prepare to detach in vSphere:

1. On the vSphere Web Client, select the desired **Virtual Machine**.
2. Right-click on the required VM and select **Velostrata Operations > Migration Operations > Prepare Detach**.

The screenshot shows a 'Prepare to Detach' dialog box. It contains two configuration options: 'Disk Type' set to 'SSD' and 'Service Account' which is currently empty. The dialog has 'OK' and 'Cancel' buttons at the bottom right.

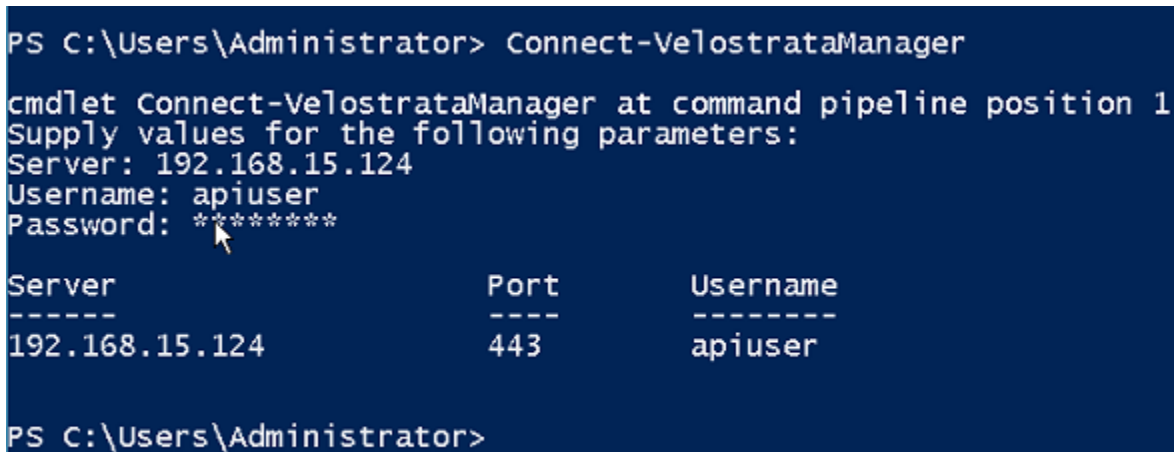
3. Select the **Disk Type**.
4. Select the **Service Account**.

5. Click **OK**.

After the ready to detach process is completed, the VM is **Ready to Detach**.

On-prem-to-Cloud: To prepare to detach the VM using PowerShell:

1. In PowerShell, connect to the Velostrata Manager by running **Connect-VelostrataManager**.



```
PS C:\Users\Administrator> Connect-VelostrataManager

cmdlet Connect-VelostrataManager at command pipeline position 1
Supply values for the following parameters:
Server: 192.168.15.124
Username: apiuser
Password: *****

Server          Port          Username
-----
192.168.15.124  443          apiuser

PS C:\Users\Administrator>
```

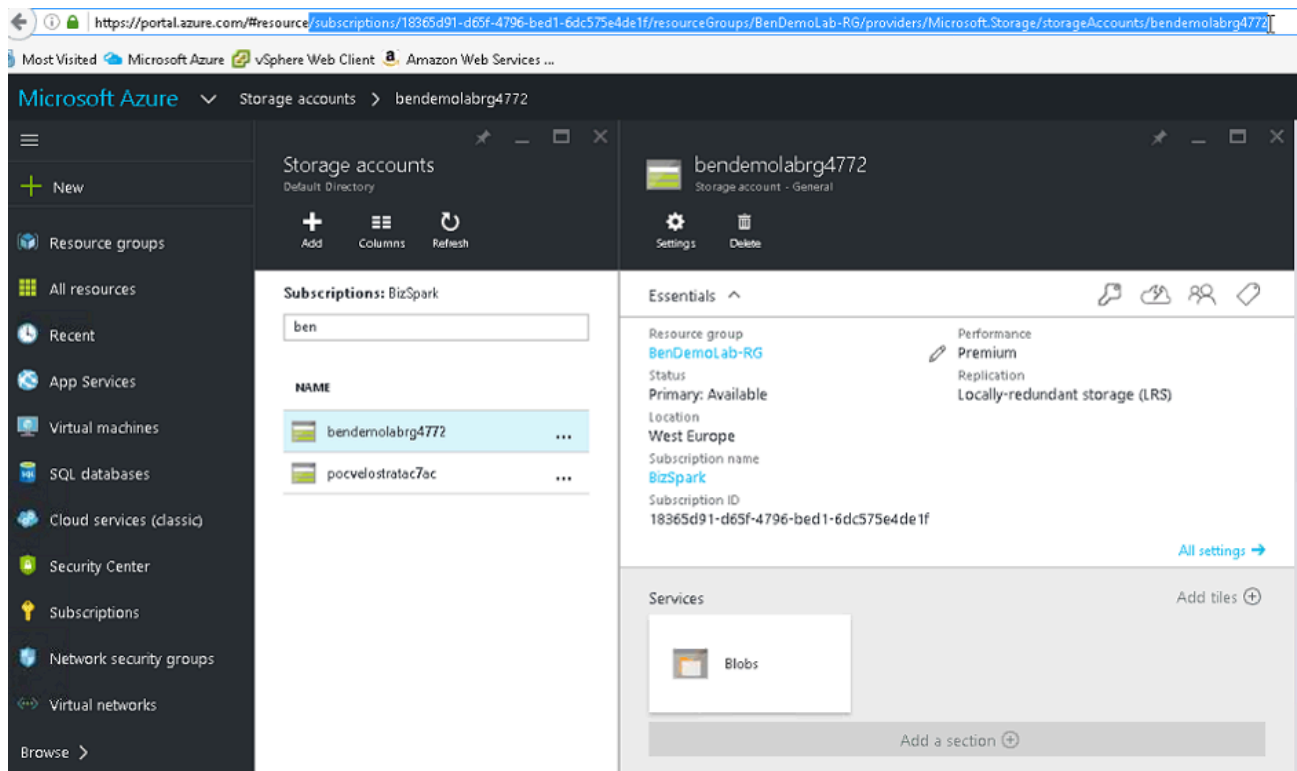
- When prompted enter details for the **Server**, **Username** (**apiuser**) and **Password** (the subscription ID).
- To prepare to detach, run **get-vm myserver | Start-VelosPrepareToDetach -StorageSpec "string"** or for AWS, run **get-vm myserver | Start-VelosPrepareToDetach -StorageSpec "string" -EncryptDisk -DiskEncryptionKey "string"**.

The command requires a **StorageSpec** string value:

- For AWS, this is the volume type, for example, SSD-based EBS volumes are type **gp2**.
- For Azure, this is the storage account ID. In Azure, select the required Storage account, and copy the partial URL after the **https://portal.azure.com/#resource**.

For AWS, you can create an encrypted EBS disk during the prepare to detach stage:

- EncryptDisk** - will create an encrypted EBS disk during prepare to detach stage. When selected, you can provide an alias key ID, or let the system use the default CMK.
- DiskEncryptionKey** - when using -EncryptDisk, you can specify a KMS key alias. Note that the key should be created in the KMS prior to the operation and the VelosMgrGroup must be added to the list of users which can assign the KMS key.



```
PS C:\Users\Administrator> get-vm mytestvm | Start-VelosPrepareToDetach -StorageSpec "/subscriptions/18365d91-d65f-4796-bed1-6dc575e4de1f/resourceGroups/BenDemoLab-RG/providers/Microsoft.Storage/storageAccounts/bendemolabrg4772"
```

Id	EntityId	Type	Initiator	ExternalTaskId	State	Start
t-4	vm-122	PrepareToDetach	powershell_192.168.15.50		Running	6/21/

4. To check the state of the task, run **Get-Velostask [ID]** and optionally **Get-Velostask [ID] | fl**

```
PS C:\Users\Administrator> Get-VelosTask t-4
```

Id	EntityId	Type	Initiator	ExternalTaskId	State	Start
t-4	vm-122	PrepareToDetach	powershell_192.168.15.50	task-4346	Running	6/21/


```
PS C:\Users\Administrator> get-velostask t-4 |fl
```

```
Id           : t-4
EntityId     : vm-122
Type         : PrepareToDetach
Initiator    : powershell_192.168.15.50
ExternalTaskId : task-4346
State        : Running
StartTime    : 6/21/2016 10:40:40 AM
EndTime      :
```

5. Monitor the created vSphere Cloud Instance Information for progress.

NOTE: The vCenter task may be completed before the VM is actually ready for detaching. Monitor the portlet and the task in Powershell as reliable sources of information.

Cloud Instance Information	
VM State	Running
Last Status	--
Cloud Extension	Azure-WestEU
Storage Migration	Preparing To Detach
Remote Console	Ready
Security Groups	poc.sgWorkloads.BenDemoLab-

```
PS C:\Users\Administrator> Get-VelosTask t-4
```

Id	EntityId	Type	Initiator	ExternalTaskId	State	Start
----	-----	----	-----	-----	-----	-----
t-4	vm-122	PrepareToDetach	powershell_192.168.15.50	task-4346	Succeeded	6/21/

Cloud-to-Cloud: To prepare to detach the VM using PowerShell:

1. In PowerShell, connect to the Velostrata Manager by running **Connect-VelostrataManager**.
2. When prompted enter details for the **Server**, **Username** (**apiuser**) and **Password** (the subscription ID).
3. To prepare to detach, run **Start-VelosPrepareToDetach [-Id] <String[]> -StorageSpec <String>**

- 4. For example, run: **Start-VelosPrepareToDetach -id i-0029a39f53eb73818 -StorageSpec Standard**
- 5. The example starts the detach preparation for an AWS Workload **i-0029a39f53eb73818**. The data disks are created in GCP (volume type: Standard).

Id		EntityId	Type	Initiator	ExternalTaskId
State		StartTime			
--		-----	----	-----	-----
-		-----			
t-26		i-0029a39f53eb73818	PrepareToDetach	powershell_192.168.0.1	
Success		5/18/20...			

Reconfiguring a VM

When a VM is running in cloud, its settings can be changed using the "Reconfigure Cloud Instance" wizard in the Velostrata plug-in for vCenter Web Client. You can change the instance type (for example, select an instance that performs better for this workload, or an instance that costs less, and so on). When changing the instance type, a reboot is required, however the instance Private IP address and other identifiers remain the same. You can also reconfigure the storage policy from Write Back to Write Isolation, and vice-versa.

All virtual machine state and data created in cloud in write-isolation mode will be lost when machines are moved back on-premises. Related virtual machines, which are part of the same application, should be moved together to align application state. Make sure to copy out to a persistent location any data you wish to keep prior to moving such machines back to on-premises.

A typical scenario for changing the storage from Write Isolation to Write Back is for a Dev-Test environment or a project that is nearing an end. By changing the VM to run from Write Isolation to Write Back, the data is written back to on-premises. Once the data is backed up, you can then run the VM back on-premises.

When switching from Write Back to Write Isolation, the edge node stops transferring the data from the cloud instance. This may result in an inconsistent snapshot.

To reconfigure a VM:

1. On the vSphere Web Client, select the desired **Virtual Machine**.
2. Right-click on the required VM and select **Velostrata Operations > Reconfigure virtual machine**.

Reconfigure Virtual Machine - centos-mini-11075814-BAX

Cloud Instance
Storage Policy
Networking
Summary

Cloud Instance

Source VM	Provisioned	Observed Usage	Monitoring Duration:	Not monitored
CPU:	2	No information		
RAM:	2GB	No information	Active Duration:	Not monitored
Disks:	1			

Recommended Options:

Performance Optimized	Monthly Cost (Pay-As-You-Go)
n1-standard-2 (2 CPUs 7.5 GB RAM)	\$75.31
n1-highmem-2 (2 CPUs 13 GB RAM)	\$93.74
n1-highcpu-4 (4 CPUs 3.6 GB RAM)	\$112.32

Instance Type: n1-standard-2 (2 CPUs 7.5 GB RAM)

Back
Next
Finish
Cancel

3. Select new **Instance Type**.
4. Click **Next**.

Reconfigure Virtual Machine - centos-mini-11075814-BAX

✓ Cloud Instance
Storage Policy
Networking
Summary

Storage Policy

Storage Policy: ☐ Write Back ☒ Write Isolation

Warning: All virtual machine state and data created in cloud in write-isolation mode will be lost when machines are moved back on-premises.

Related virtual machines, which are part of the same application, should be moved together to align application state.

Make sure to copy out to a persistent location any data you wish to keep prior to moving such machines back to on-premises.

Back
Next
Finish
Cancel

Note: You cannot reconfigure the storage on a cloned VM or on a spot instance.

5. To change the storage policy, select either **Write Back** or **Write Isolation** and then click **Next**.

The screenshot shows the 'Reconfigure Virtual Machine' window for 'centos-mini-11075814-BAX'. The left sidebar has four items: 'Cloud Instance' (checked), 'Storage Policy' (checked), 'Networking' (selected and highlighted in blue), and 'Summary'. The main area is titled 'Networking' and contains a label 'Network Tags (comma separated):' followed by a text input field containing 'velostrata'. A small blue information icon is to the right of the input field. At the bottom right, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

6. For GCP, enter the **Network Tags** (in a comma-separated list) and click **Next**.

The screenshot shows the 'Reconfigure Virtual Machine' window for 'centos-mini-11075814-BAX'. The left sidebar has four items: 'Cloud Instance' (checked), 'Storage Policy' (checked), 'Networking' (checked), and 'Summary' (selected and highlighted in blue). The main area is titled 'Summary' and displays the following configuration details:

Velostrata Cloud Extension:	gcp_datacenter-2_1520747894_6aR
Cloud Instance Type:	n1-standard-2 (2 CPUs 7.5 GB RAM)
Storage Policy:	Write Back i
Network Tags:	velostrata
Subnet:	10.132.0.0/20
Edge Node:	Node A
External IP:	None

At the bottom right, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'. A mouse cursor is pointing at the 'Next' button.

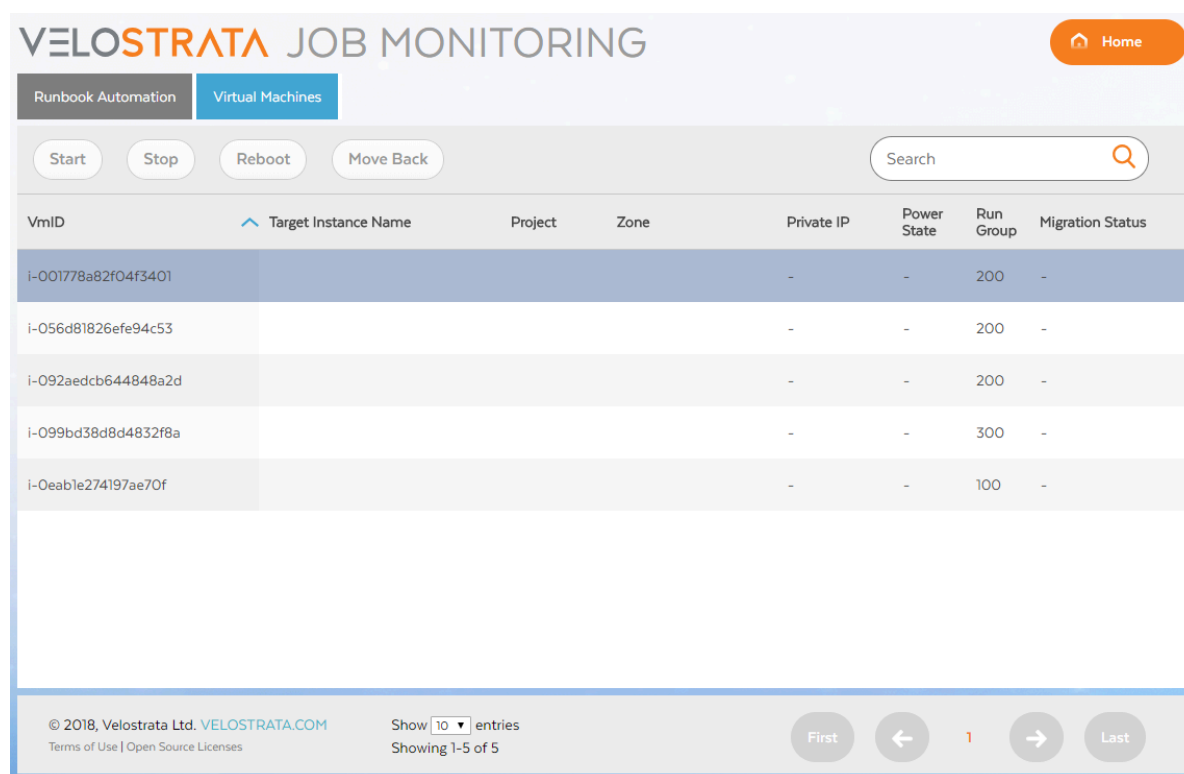
7. Review the summary (where changes are noted with the small blue icon) and then click **Finish** (or click **Cancel** to leave the current VM configuration as is).

Shutting Down a VM in the Cloud

Note: You cannot shut down a VM via the Cloud Portal.

Using Web Manager

1. Login to your Velostrata Web Manager at [HTTPS://IP_OF_VELO_MANAGER](https://ip_of_velo_manager)
2. Click the Runbook Automation tab.
3. When prompted for a username and password, use 'apiuser' as the username and your password is your Velostrata subscription ID or your GCP billing ID.
4. Click the monitor icon for one of the runbook automation jobs.
5. Select the VM you wish to return on-premises and click the 'Stop' button on top.



The screenshot shows the VELOSTRATA JOB MONITORING interface. At the top, there's a header with the VELOSTRATA logo and 'JOB MONITORING' text. Below the header, there are two tabs: 'Runbook Automation' and 'Virtual Machines'. The 'Virtual Machines' tab is active. Below the tabs, there are four buttons: 'Start', 'Stop', 'Reboot', and 'Move Back'. To the right of these buttons is a search bar. Below the buttons and search bar is a table with the following columns: 'VmID', 'Target Instance Name', 'Project', 'Zone', 'Private IP', 'Power State', 'Run Group', and 'Migration Status'. The table contains five rows of data. At the bottom of the interface, there is a footer with copyright information, a 'Show 10 entries' dropdown, and pagination controls.

VmID	Target Instance Name	Project	Zone	Private IP	Power State	Run Group	Migration Status
i-001778a82f04f3401				-	-	200	-
i-056d81826efe94c53				-	-	200	-
i-092aedcb644848a2d				-	-	200	-
i-099bd38d8d4832f8a				-	-	300	-
i-0eable274197ae70f				-	-	100	-

Using vCenter

1. On the vSphere Web Client, select the desired **Virtual Machine**.
2. Right-click the VM and select **Velostrata Operations > Shutdown**.



Using PowerShell:

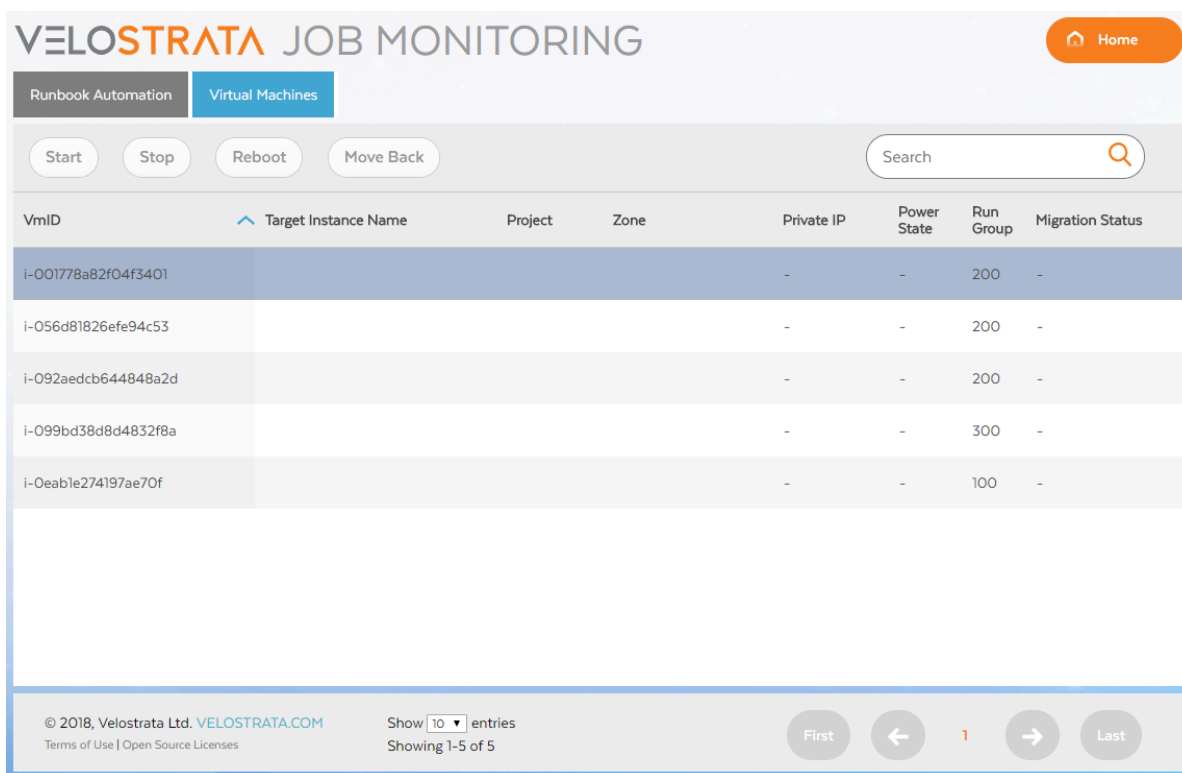
1. In PowerShell, connect to the Velostrata Manager by running **Connect-VelostrataManager**.
2. When prompted enter details for the **Server**, **Username** (**apiuser**) and **Password** (the subscription ID).
3. To shut down a VM, run **Stop-VelosVm [-Id] <string[]>**.

Powering on a VM in the Cloud

Note: If the instance was launched with the Assign Public IP option, a new public IP is assigned on each power on.

Using Web Manager

1. Login to your Velostrata Web Manager at [HTTPS://IP_OF_VELO_MANAGER](https://IP_OF_VELO_MANAGER)
2. Click the Runbook Automation tab.
3. When prompted for a username and password, use 'apiuser' as the username and your password is your Velostrata subscription ID or your GCP billing ID.
4. Click the monitor icon for one of the runbook automation jobs.
5. Select the VM you wish to return on-premises and click the 'Start' button on top.



The screenshot shows the VELOSTRATA JOB MONITORING interface. At the top, there's a header with the logo and a 'Home' button. Below the header, there are two tabs: 'Runbook Automation' and 'Virtual Machines'. The 'Virtual Machines' tab is active. Below the tabs, there are four buttons: 'Start', 'Stop', 'Reboot', and 'Move Back'. To the right of these buttons is a search bar. Below the buttons and search bar is a table with the following columns: 'VmID', 'Target Instance Name', 'Project', 'Zone', 'Private IP', 'Power State', 'Run Group', and 'Migration Status'. The table contains five rows of data. At the bottom of the interface, there is a footer with copyright information, a 'Show 10 entries' dropdown, and pagination controls.

VmID	Target Instance Name	Project	Zone	Private IP	Power State	Run Group	Migration Status
i-001778a82f04f3401				-	-	200	-
i-056d81826efe94c53				-	-	200	-
i-092aedcb644848a2d				-	-	200	-
i-099bd38d8d4832f8a				-	-	300	-
i-0eable274197ae70f				-	-	100	-

Using vCenter

1. On the vSphere Web Client, select the desired **Virtual Machine**.
2. Right-click the VM and select **Velostrata Operations > Power On**.



Using PowerShell:

1. In PowerShell, connect to the Velostrata Manager by running **Connect-VelostrataManager**.
2. When prompted enter details for the **Server**, **Username** (**apiuser**) and **Password** (the subscription ID).
3. To power on a VM, run **Start-VelosVm [-Id] <string[]>**.

Restarting a VM in the Cloud

Note: If the instance was launched with the assign Public IP option, a new public IP might be assigned on each restart.

When you run restart a VM in the cloud and the instance does not restart up in a healthy way, Velostrata uses VM auto healing to fix the problem and restart the instance.

To restart a VM in the cloud:

1. On the vSphere Web Client, select the desired **Virtual Machine**.
2. Right-click the VM and select **Velostrata Operations > Restart**.



To restart a VM using PowerShell:

1. In PowerShell, connect to the Velostrata Manager by running **Connect-VelostrataManager**.
2. When prompted enter details for the **Server**, **Username** (**apiuser**) and **Password** (the subscription ID).
3. To restart on a VM, run **Restart-VelosVm [-Id] <String[]>**.

Monitoring a VM when Running in Cloud

The basic instance status for the cloud instance information are presented in the **Summary** page portlet added by the Velostrata plug-in. When the **Remote Console** field is **Ready**, the instance is reachable from the Velostrata Virtual Machine on-prem. The remote console probe tests the RDP port (TCP/3389) for Windows VMs and the SSH port (TCP/22) for Linux VMs.

While running in cloud, further performance and operational statistics are available for the VM in the **Monitoring > Cloud Instance** tab. You can review details about storage IOs in cloud vs. those affecting the vSphere Datastore storage on-prem, as well as other operational statistics such as IO latency and throughput.

Graphs are offered at pre-canned periods of Hour, Day, 7 days, 30 days as well as a user-defined custom range.

The following metrics are available:

- **Workload:**
 - **IOPS:** Storage IO operations that the VM has generated over the Cloud Edge node.
 - **IO Latency (ms):** Average storage IO operation latency (1 min interval) for this VM's operations.
 - **Throughput (Bytes/sec):** Storage throughput utilized for this VM.
- **Uncommitted Writes (Bytes):** The amount of write data acknowledged in cloud for this VM, and still pending a commit to the vSphere datastore on-prem.
- **vSphere Datastore:**
 - **IOPS:** Backend IOPs generated against the vSphere datastore for this VM's activity.
 - **vSphere Datastore Bytes (cumulative):** Total bytes read from on-prem datastore or written to during this VMs run in cloud. This graph slope can be used to identify active working set converges and transitions.
 - **Throughput (Bytes/sec):** Total throughput of vSphere datastore storage access, as generated by the VM's activity in cloud.
 - **IO Offload %:** Based on the ratio between IO operations handled in cloud vs IO operations generated against the vSphere datastore on prem.
- **Change set Compaction Ratio %:** Efficiency metric for overlapping writes compaction. Pre compression.

Migrating Physical Servers

Migrating a Physical Server

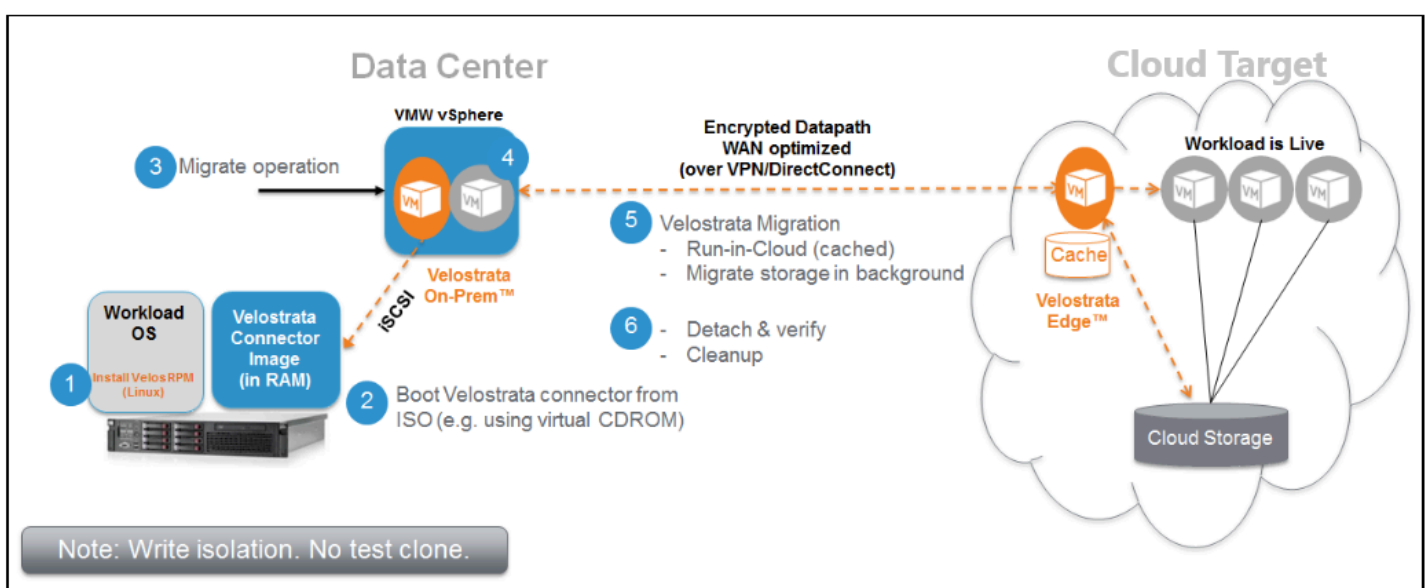
Migrating a physical server to the cloud is done by booting a Velostrata Connector ISO image into RAM from a virtual or physical DVDROM/CDROM device. The Velostrata connector maps the local storage and creates a Stub VMware VM as a management object for Velostrata cloud migration operations. From that point forward, the migration is done in a similar way to the migration of other VMs except here it takes place in write isolation mode, meaning data changes made in the cloud are not synced back to on-prem.

Notes:

- The Stub VM created in the process is intended for Velostrata management operations only, and not set up for local execution on vSphere. It is set up with no network interface, and a minimal CPU/RAM setting.
- Test clone is not supported for physical servers.

System requirements:

- Disk types supported include SAS, SATA, SSD, virtual disks presented by hardware controller, and SAN volumes mounted on physical HBAs.
 - PATA/IDE disks are not supported.
- Minimum of 4GB RAM is recommended
 - For machines with less than 4GB RAM, press any key during the boot splash screen (one with the keyboard icon) and choose the Velostrata Connector (low memory) option from the menu. This uses an on-demand copy from the CD image.
- Physical DVDROM/CDROM or virtual CDROM to boot the Velostrata Connector ISO from.



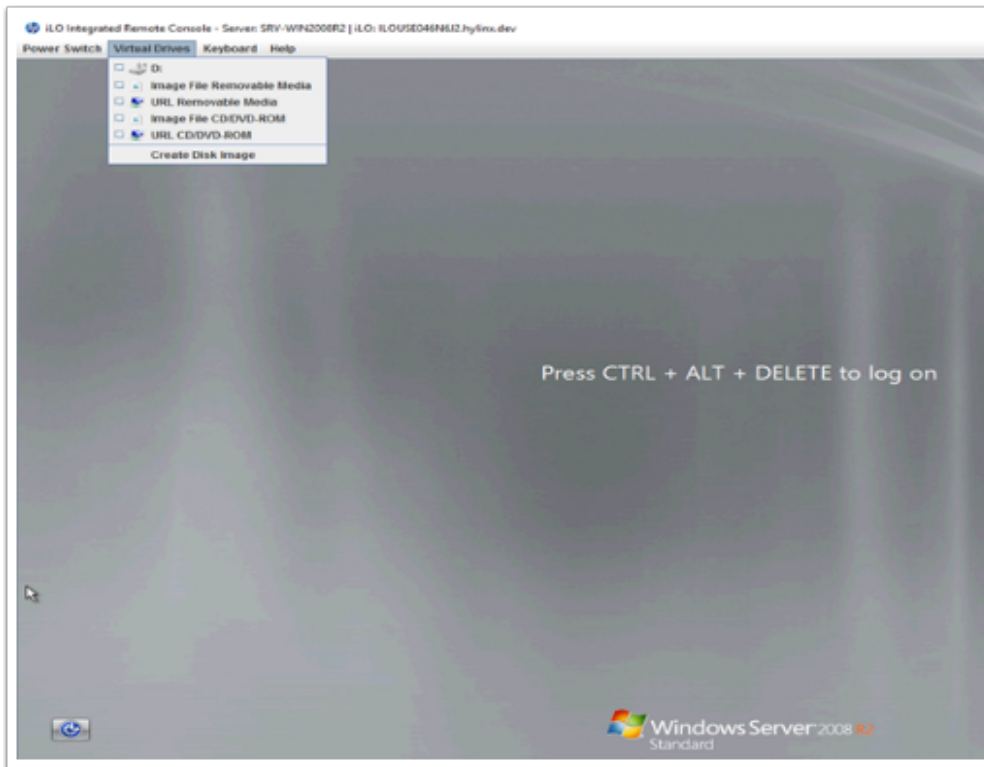
Instructions

1. Check OS compatibility in the Velostrata [release notes](#).
2. For Linux OS install the Velostrata-Prep RPM, as described in the relevant chapter [here](#).
3. Download the Velostrata Connector ISO: <http://tiny.cc/VelosPhysicalConnector>
4. Boot from the Velostrata ISO.

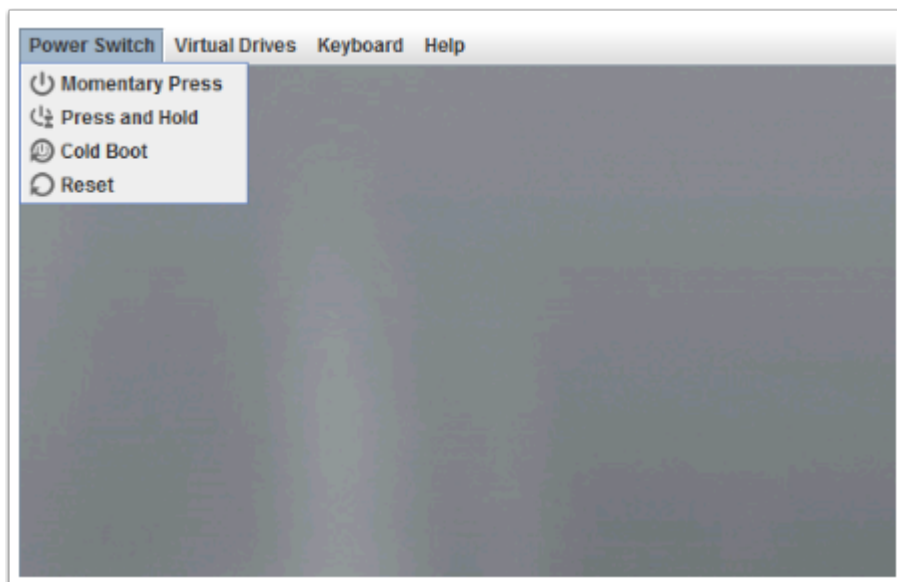
Note: This can be done by using ILO (HP Enterprise servers) or iDRAC (Dell servers).

The steps below use HP ILO:

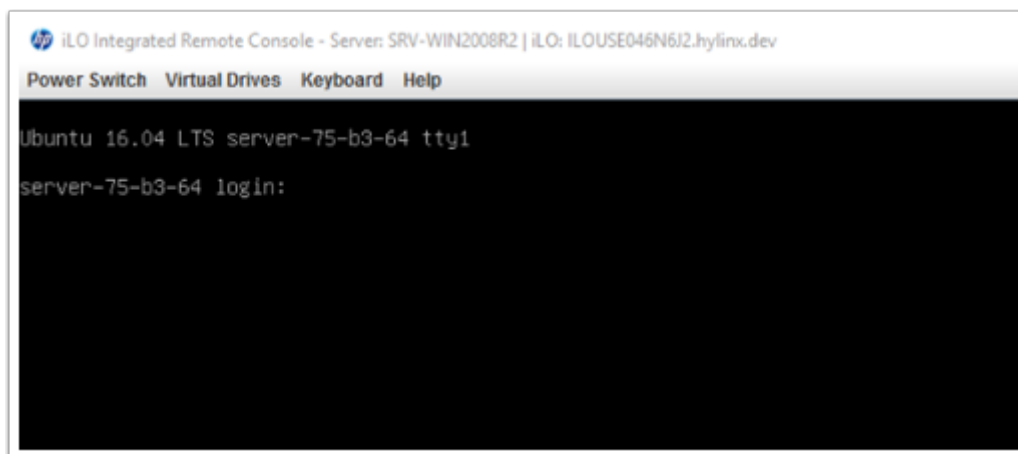
5. Launch the remote console.
6. Select **Virtual Drives > Image File CD/DVD-ROM**, and select the Velostrata Connector ISO that you downloaded.



7. Select **Power Switch > Reset**.

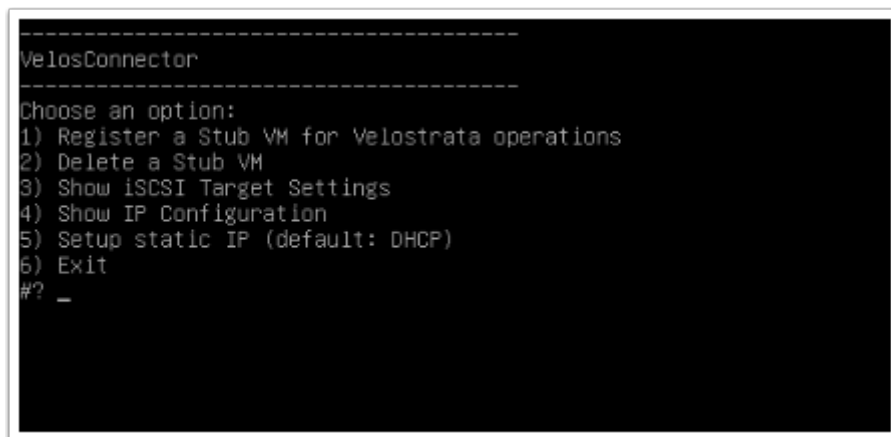


8. Once the server is up, ensure that it boots from the ISO.



9. Log in to the ISO using the following credentials: ubuntu>Welcome01

10. Run **./VelosConnector.sh** script to view the menu.



11. In vCenter, check for an **iSCSI Software Adapter**. If you do not have one, follow these steps:

11A. Navigate to **Configure > Storage Adapters** and add an iSCSI Software Adapter.

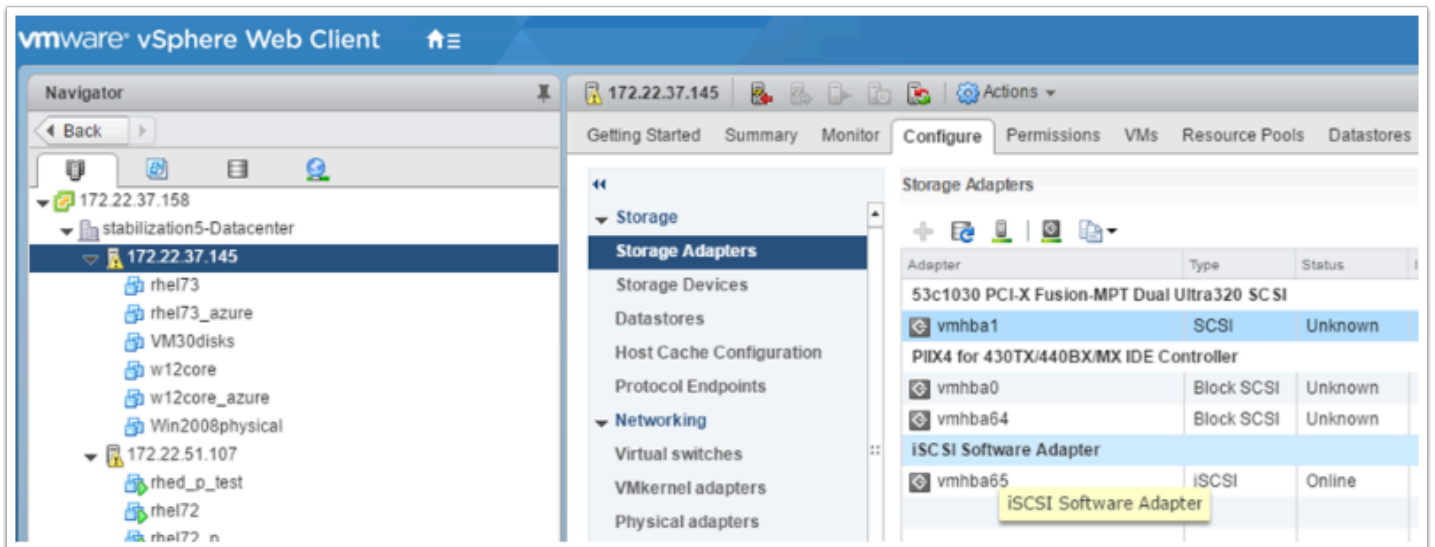
11B. Under **Networking**, select **VMKernel adapters** and click the **edit icon**.

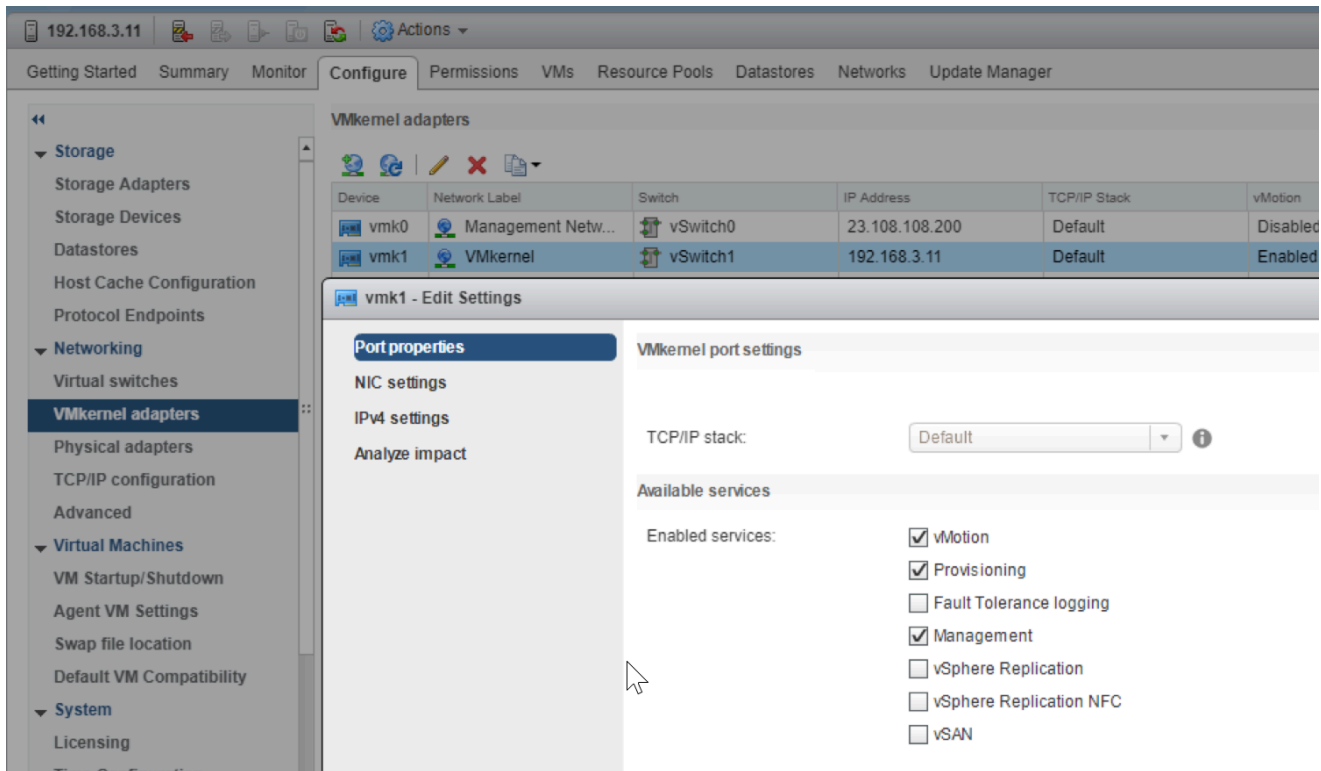
11C. Click **Port properties** option.

11D. Under the **Enable services** area, check the **Provisioning** checkbox and click **OK**.

Note: we recommend a 1:1 relationship between a VM and an iSCSI Target.

(See screen shots below for reference):





12. Select 1) **Register a Stub VM for Velostrata operations** and follow the instructions. Note that registering the OS properly is required in order to create the correct AML in the cloud and enable proper migration.

```

-----
VelosConnector  BETA2.7.1
-----
Choose an option:
1) Register a Stub VM for Velostrata operations
2) Delete a Stub VM
3) Show iSCSI Target Settings
4) Show IP Configuration
5) Setup static IP (default: DHCP)
6) Exit
#?

```



```

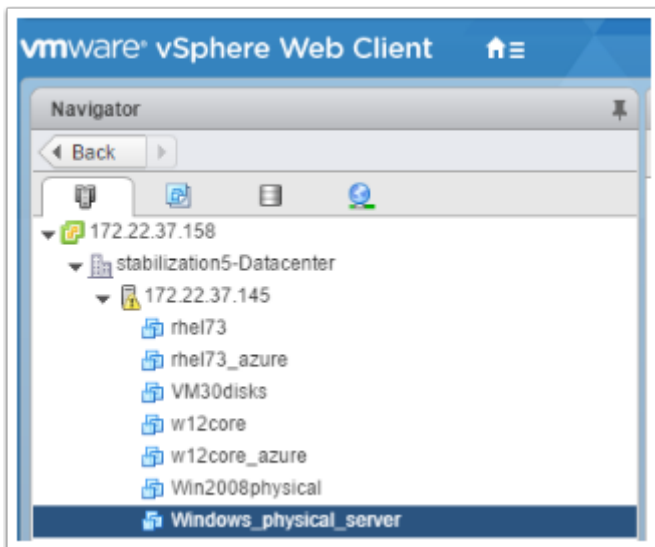
#? 1
Enter vCenter Server IP: 172.22.34.224
Verifying connectivity...OK
Enter ESX host IP: 172.22.34.225
Verifying connectivity...OK
Enter VM name to create: rhel73
Target vSphere Datastore: datastore-2
NOTE: Using local IP: 172.22.35.102 for iSCSI target connection setup.
Creating iSCSI Target portal on 172.22.35.102 for IQN: iqn.2017-02.com.velostrata.server-bb-e7-14:ta
rget
Using default IP port 3260
This NetworkPortal already exists in configFS.
Select guest operating system to register:
1) Windows
2) Linux
3) Other
#? 2
Select architecture:
1) 64bit
2) 32bit
#? 1
Select Linux version:
1) RHEL/CentOS 5 3) RHEL/CentOS 7 5) SLES 11 7) Other Linux
2) RHEL/CentOS 6 4) SLES 10 6) SLES 12
#? 3
You have selected: RHEL/CentOS 7 64bit
Confirm? (y/n)y

vCenter Login
-----
Username: root
Password:

Executing...OK
VM: rhel73 , created with ID: vm-1603

```

The VM appears in vCenter.



13. Now that the VM is in vCenter, you can perform the migration using the standard process as outlined [here](#).

Deleting a Stub VM

You can delete the VM and the iSCSI target configuration on the ESX side after your migration is complete.

Note: If you create more than one VM using the same iSCSI Target, when you delete any of those VMs, it will automatically delete the iSCSI Target as well. Therefore, you must manually delete any additional VMs that were tied to that iSCSI Target.

To delete a Stub VM

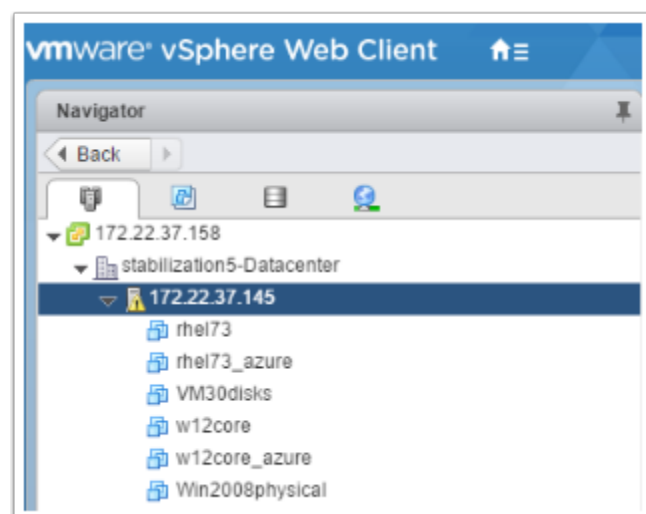
1. Select **2) Delete a Stub VM**.
2. Follow the on-screen instructions.

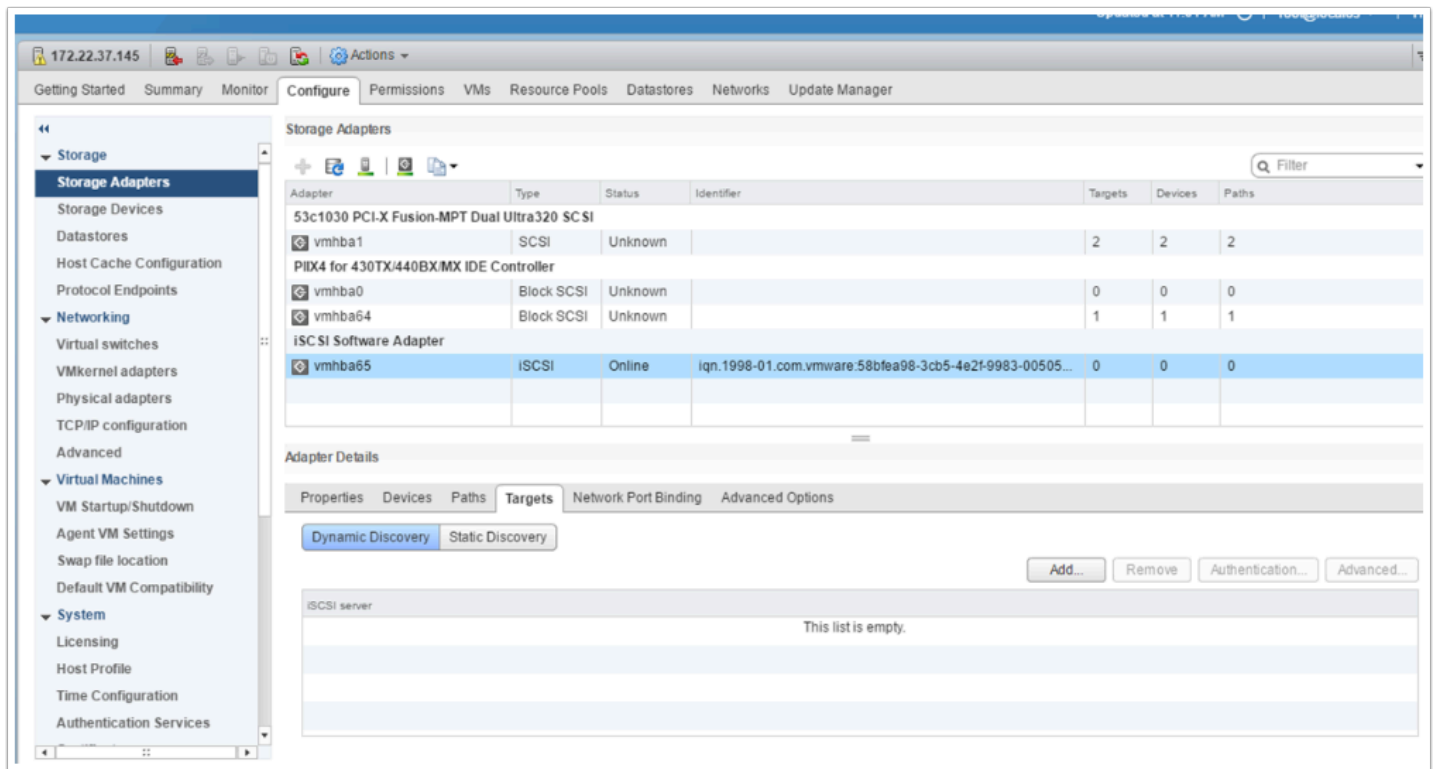
```
-----
VelosConnector BETA2.7.1
-----
Choose an option:
1) Register a Stub VM for Velostrata operations
2) Delete a Stub VM
3) Show iSCSI Target Settings
4) Show IP Configuration
5) Setup static IP (default: DHCP)
6) Exit
#? 2
Enter vCenter Server IP/FQDN: 172.22.34.224
Verifying connectivity...OK
NOTE: Using local IP: 172.22.35.102 for iSCSI target.
Enter VM name to delete: rhelp2c

vCenter Login
-----
Username: root
Password:

Executing...
OK
VM: rhelp2c , has been deleted.
root@server-bb-e7-14:~# _
```

3. On vCenter, check that the VM and the iSCSI target no longer exist.





Showing the iSCSI Target Settings

You can view the iqn, portals and luns that will be migrated to the cloud.

To show the iSCSI Target Settings

- Select **3) Show iSCSI Target Settings**. Ensure that you can see all the disks of the server.

```

-----
VeloConnector DEMO3
-----
Choose an option:
1) Register a Stub VM for Velostrata operations
2) Delete a Stub VM
3) Show iSCSI Target Settings
4) Show IP Configuration
5) Setup static IP (default: DHCP)
6) Exit
#? 3
iSCSI Target configuration:
Warning: Could not load preferences file /home/ubuntu/.targetcli/prefs.bin.
o- / ..... [..]
  o- backstores ..... [..]
    o- fileio ..... [0 Storage Object]
    o- iblock ..... [2 Storage Objects]
      o- 0 ..... [/dev/sda, in use]
      o- 1 ..... [/dev/sdb, in use]
    o- pscsi ..... [0 Storage Object]
    o- rd_mcp ..... [0 Storage Object]
  o- ib_srpt ..... [0 Targets]
  o- iscsi ..... [1 Target]
    o- iqn.2017-02.com.velostrata.server-75-b3-64:target ..... [1 TPG]
      o- tpg1 ..... [enabled]
        o- acls ..... [0 ACLs]
        o- luns ..... [2 LUNs]
          o- lun0 ..... [iblock/0 (/dev/sda)]
          o- lun1 ..... [iblock/1 (/dev/sdb)]
        o- portals ..... [1 Portal]
          o- 192.168.10.98:3260 ..... [OK, user disabled]
  o- loopback ..... [0 Targets]
  o- qla2xxx ..... [0 Targets]
  o- tcm_fc ..... [0 Targets]
  o- usb_gadget ..... [0 Targets]
  o- vhost ..... [0 Targets]
ubuntu@server-75-b3-64:~$ _

```

Managing the IP Configuration

You can view the IP of the server that will be used for the iSCSI target configuration. The ISO gets the IP from DHCP by default, but you can configure a static IP. It is necessary to have a valid IP before the stub can be registered.

To manage the IP configuration

1. Select **4) Show IP Configuration**.

```

-----
VelosConnector
-----
Choose an option:
1) Register a Stub VM for Velostrata operations
2) Delete a Stub VM
3) Show iSCSI Target Settings
4) Show IP Configuration
5) Setup static IP (default: DHCP)
6) Exit
#? 4
Active Network Interfaces:
2: enp3s0f0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether d4:85:64:75:b3:64 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.98/24 brd 192.168.10.255 scope global enp3s0f0
        valid_lft forever preferred_lft forever
    inet6 fe80::d685:64ff:fe75:b364/64 scope link
        valid_lft forever preferred_lft forever
3: enp3s0f1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether d4:85:64:75:b3:66 brd ff:ff:ff:ff:ff:ff
4: enp4s0f0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether d4:85:64:75:b3:68 brd ff:ff:ff:ff:ff:ff
5: enp4s0f1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether d4:85:64:75:b3:6a brd ff:ff:ff:ff:ff:ff
ubuntu@server-75-b3-64:~$ _

```

2. **Select 5) Setup Static IP** to configure a static IP.

Using Offline Migration

Velostrata enables you to migrate workloads with operating systems that are not currently supported by Velostrata's streaming technology.

During the offline migration process, the VM storage is migrated to the cloud first, and the VM is started in the cloud only after the migration is completed. Velostrata automatically performs the detach and cleanup of residue data associated with this VM.

Offline migration can also be used for “storage only migration”. Old VMs (e.g. RedHat 4) can be migrated to the cloud with offline migration, even when unsupported by the cloud provider. Administrator can then reattach a data disk to a newer and supported cloud instance.

For AWS, you may select to encrypt the native volumes and optionally, specify the key to be used. See [EBS Encryption Key Preparation](#).

Important notes:

- After the migration, the VM is located in the cloud with the name of the VM as defined on-premises.
- Preparation of the VM is required, before the offline migration starts.

Preparations Before the Offline Migration Process

RHEL 5.11+

- Edit **/etc/sysconfig/network-scripts/ifcfg-eth0** and change the primary interface name to **eth0** and make sure it is set to **DHCP**:

```
BOOTPROTO=dhcp
ONBOOT=yes
STARTMODE=onboot
DEVICE=eth0
TYPE=Ethernet
DEFROUTE=yes
```

Ubuntu 12.x

- Edit **/etc/network/interfaces** and change the primary interface name to **eth0** and make sure that it is set to **DHCP**:

```
# The primary network interface
auto eth0
iface eth0 inet dhcp
```

Windows Server 2003, Windows Server 2003 R2, Windows Server 2008 (non-R2) to AWS

Install the following packages:

- .Net 3.5 redistributable - dotnetfx35setup.exe - [Download link](#)
- Windows Management Framework Core 2.0. Reference - [Download link](#)
Note: The specific package depends on the exact OS version, for OS - Windows 2003 - Service pack 2 is a prerequisite.
- EC2Install.zip - [Download link](#)
- CITRIX-Win_PV.zip - [Download link](#)
 1. Extract the zip file to a temporary folder destination.
 2. Execute **Citrix_xensetup.exe** in the extracted folder. During the installation process, a warning message appears notifying you that the workload platform on which the installation is running is not a Citrix Xen platform, and prompts you for approval.
 3. Click **OK** to approve.

Windows 2008 non-R2 to GCP

No special preparation required prior to offline migration for Windows Server 2008 64 bit version.

Windows Server 2008 32 bit version requires package installation before initiating offline migration, please contact Velostrata support for further details

Windows 2008 non-R2 to Azure

- No special preparation required prior to offline migration.

Windows Server 2003, Windows Server 2003 R2 to Azure

Complete the following preparation prior to performing an offline migration for a Windows 2003-based VM to Azure.

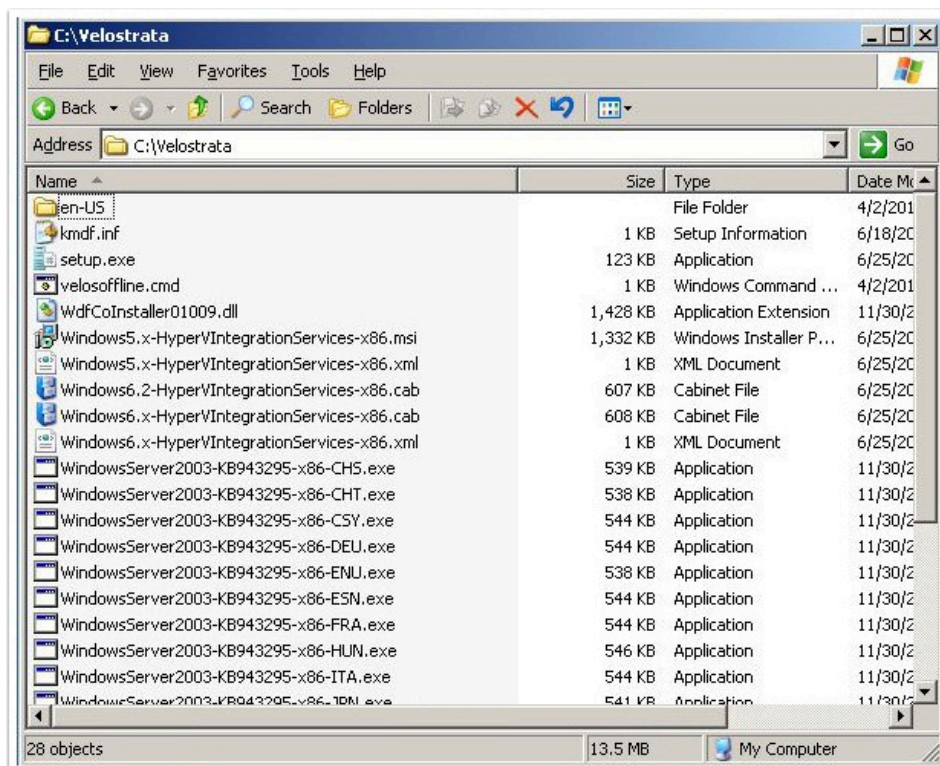
1. Copy (and extract) the Velostrata Offline for 2003 package to the GuestOS root of the c:\ drive.

[Windows 2003 x86 package](#)

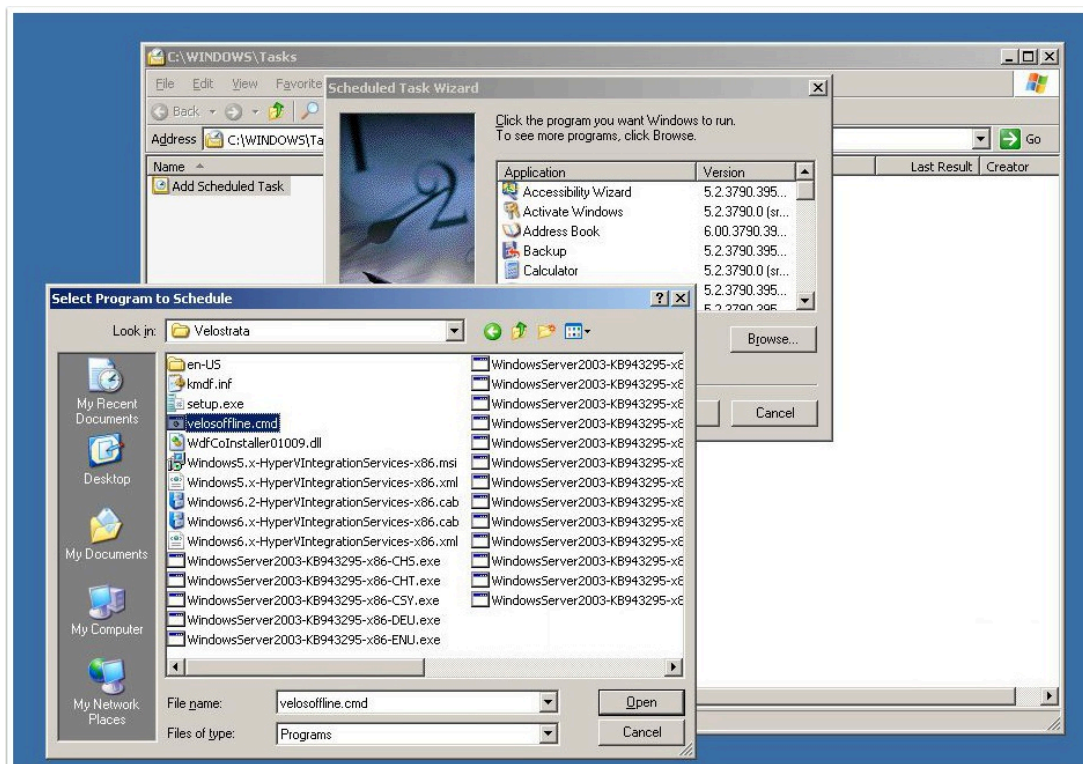
[Windows 2003 x64 package](#)

The extracted package folder includes the **velosoffline.cmd** script which runs the following:

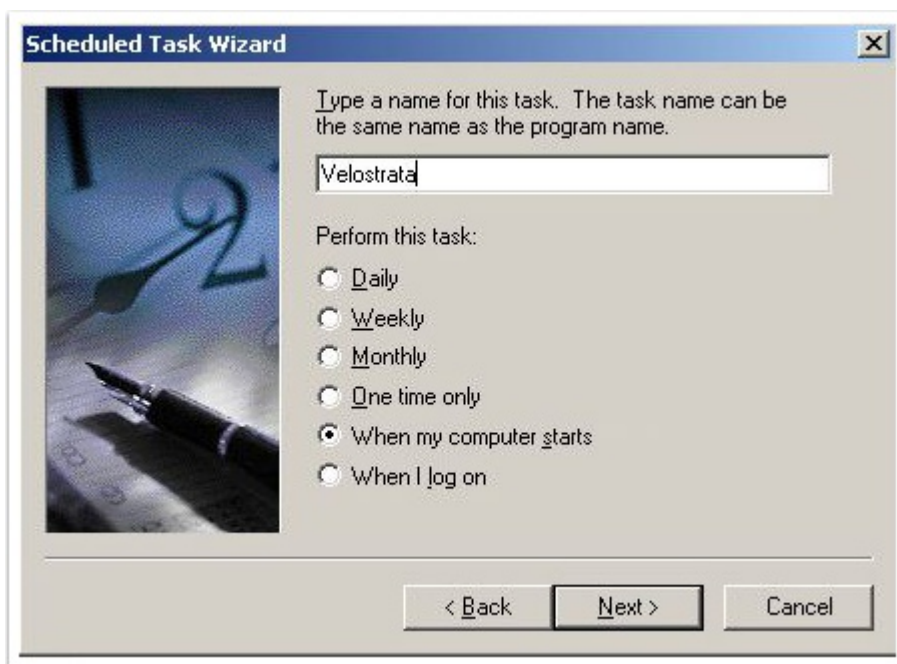
- Disables hibernate.
- Enables system restart on BSOD.
- Installs Hyper-V integration tools post detach at Windows start up.



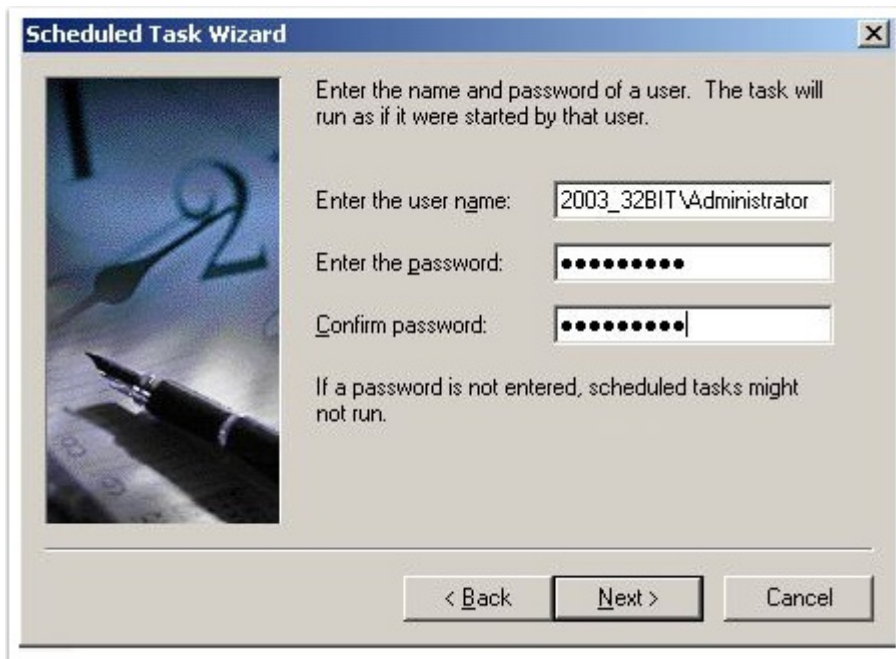
2. Create a scheduled task to run the script at Windows start up.



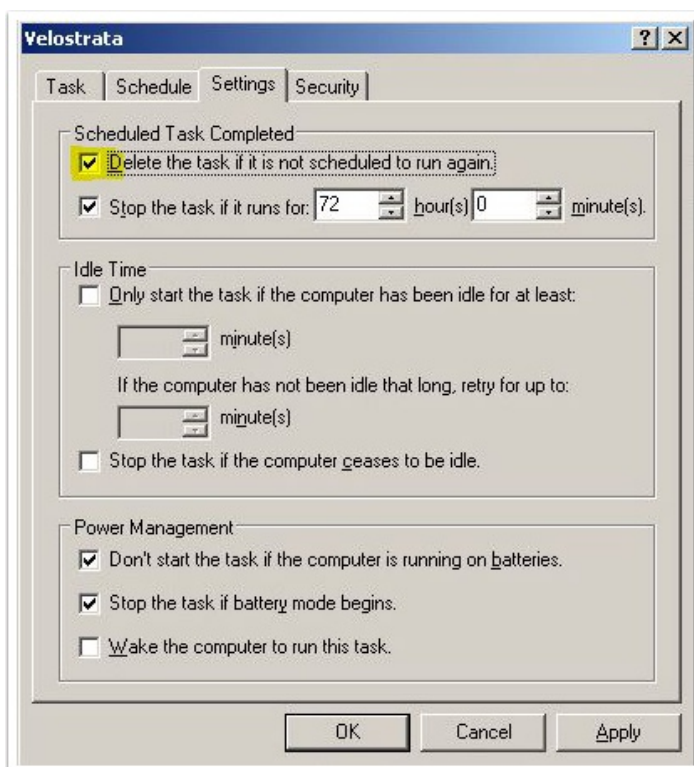
3. Set the task to run **When my computer starts**.



4. Enter the user name and password of an administrative user for the GuestOS.



5. For the task, select the **Settings** tab, and select **Delete the task if it is not scheduled to run again.**



6. Migrate the VM offline (as described below).
7. After the Detach, delete the scheduled task created before the migration.

Windows 2003 to GCP

- No special preparation required prior to offline migration.

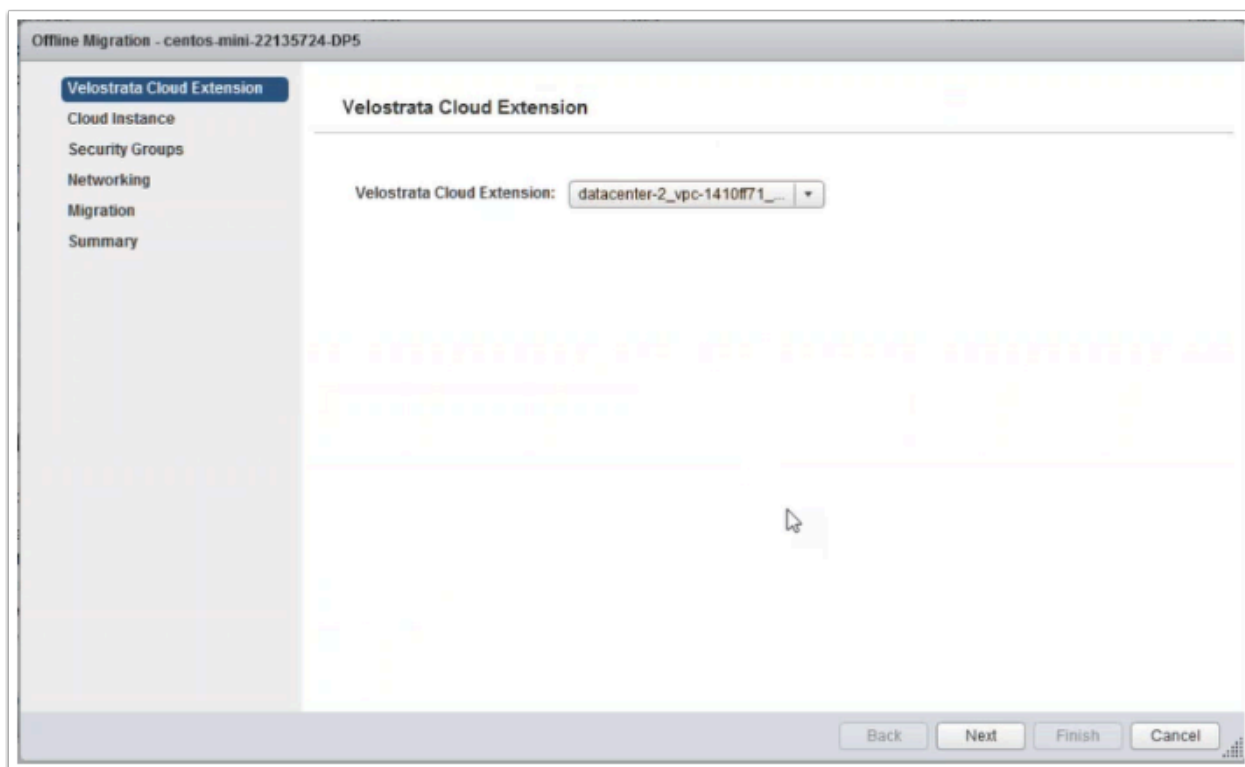
Onprem-toCloud: To migrate a VM offline:

1. Perform the offline preparation as explained in previous section, exact procedure depends on specific OS.
2. On the vSphere Web Client, select the desired **Virtual Machine**.
3. Right-click on the VM and select **Velostrata Operations > Offline Migrate**.

Note: The following AWS instance types support 32 bit: t2.nano, t2.micro, t2.small, t2.medium, and c3.large.

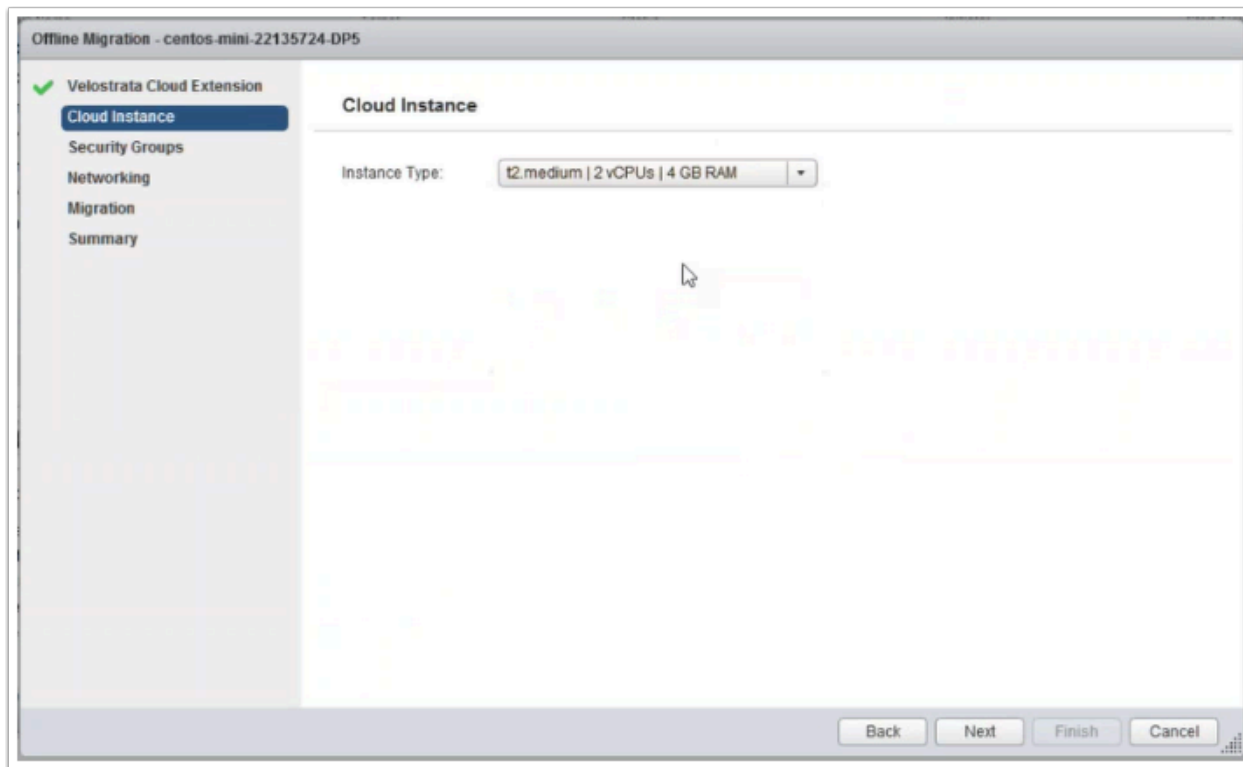


4. Select the **Velostrata Cloud Extension**.

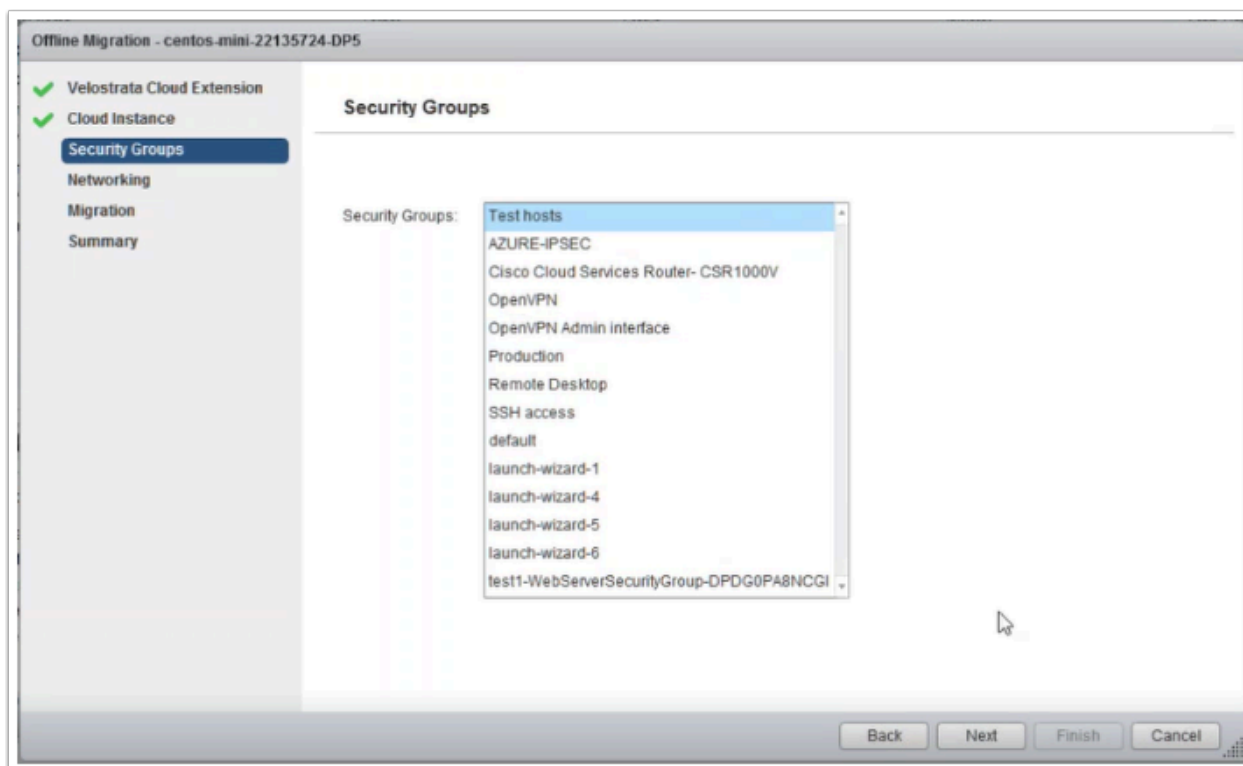


Note: If you select to run your VM in a CE that is in the AWS Marketplace, a message appears indicating that you may incur usage costs according to the subscription terms.

5. Click **Next**.



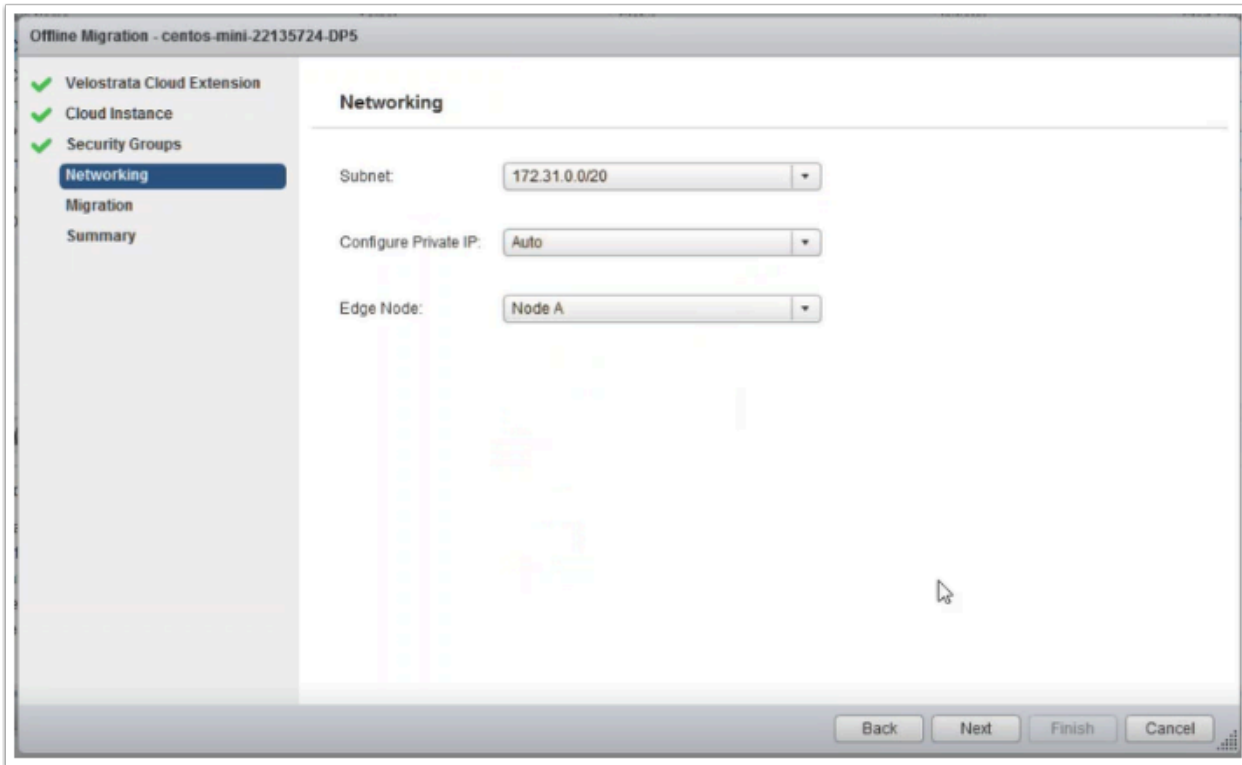
6. Select the **Instance Type** (VM size).
7. Click **Next**.



8. Select the required **Security Groups**.

Note: For AWS, if public access is required from the internet to the VM, a DMZ is required with an associated security group, including appropriate inbound and outbound rules.

9. Click **Next**.

The screenshot shows a software window titled "Offline Migration - centos-mini-22135724-DP5". On the left is a sidebar with a tree view containing "Velostrata Cloud Extension", "Cloud Instance", "Security Groups", "Networking" (which is highlighted with a blue bar), "Migration", and "Summary". The main content area is titled "Networking" and contains three dropdown menus: "Subnet:" with the value "172.31.0.0/20", "Configure Private IP:" with the value "Auto", and "Edge Node:" with the value "Node A". At the bottom right of the window are four buttons: "Back", "Next", "Finish", and "Cancel".

10. Select a **Subnet in the cloud**. Typically, the selection here would be of a private network subnet. AWS - When Cloud Edge nodes (A, B) are placed in different AZs, the Cloud Edge node in the same AZ as the selected subnet is automatically used, otherwise a manual node selection is required.
11. From the **Configure Private IP** drop-down list, select **Auto** to allow an available address on the subnet to be automatically assigned, or **Static** if a specific address assignment is required.
12. If you select **Static**, a **Static IP** field appears. Enter the required static IP for the instance or specify an ENI ID (e.g. **eni-xxxxxx**) to associate a reserved Elastic Network Interface.
13. From the **Edge Node** drop-down list, select the required node. For Azure, a manual selection of the **Edge Node** to use is required. Select **Node A** or **Node B**. The default selection is **Node A**. For AWS, when Cloud Edge nodes are placed in the same Availability Zone (AZ), a manual selection of the **Cloud Edge node** to use is required.
14. Click **Next**.

Offline Migration - win03

- ✓ Velostrata Cloud Extension
- ✓ Cloud Instance
- ✓ Security Groups
- ✓ Networking
- Migration**
- Summary

Migration

Storage Type:

Encrypt EBS volume: ☒

KMS Key ID:

- Default
- alias/autoTest
- alias/test

Back Next Finish Cancel

15. Select the **Storage Type**.
16. For AWS, select **Encrypt EBS volume**, if you are using EBS encryption for native volumes, and then from **KMS Key ID**, select the encryption key alias to be used. If this is not specified, the default key is used.
17. Click **Next**.

Offline Migration - win03

- ✓ Velostrata Cloud Extension
- ✓ Cloud Instance
- ✓ Security Groups
- ✓ Networking
- ✓ Migration
- Summary**

Summary

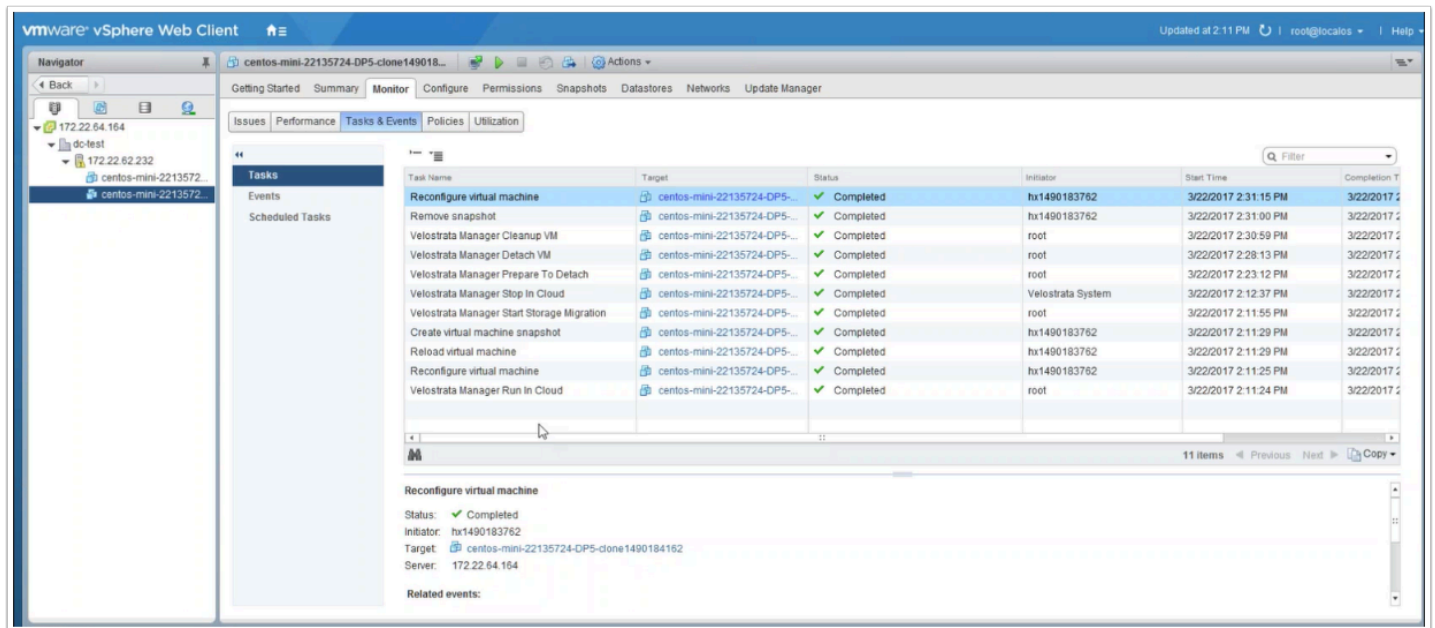
Velostrata Cloud Extension:	AWS S byol 13893 Stab7
Cloud Instance Type:	t2.medium 2 vCPUs 4 GB RAM
Velostrata License Type:	Bring Your Own License
Storage Policy:	Write Isolation
Security Groups:	Test hosts sg-48539e2d
Subnet:	172.31.16.0/20
Edge Node:	Node A
Storage Type:	gp2
Encrypt EBS volume:	true
KMS Key Alias:	alias/test

Back Next Finish Cancel

The Summary page differs slightly for AWS and Azure.

18. Review the summary and then click **Finish**.

19. To view the related migration tasks, view the **Monitor > Tasks & Events** tab.



After the offline migration is completed, you can connect to the VM using its private IP address or FQDN.

Cloud-to-Cloud: To migrate a VM offline:

- To perform offline migration, run **Invoke-VelosOfflineMigration [-Id] <String[]> -CloudExtension \$variable [-EdgeNode <String>] -StorageSpec <String> -InstanceType <string> -CloudDetailsName <string>**

For example:

```
Invoke-VelosOfflineMigration -Id i-04151a4a1067cfe9b -CloudExtension $gcpCe  
-EdgeNode NodeA -StorageSpec Standard -InstanceType n1-standard-1  
-CloudDetailsName aws
```

Monitoring Velostrata

Understanding Velostrata Health Checks

Velostrata health checks are performed periodically on the following components:

- Cloud Edge
- Exporter
- Backend

Velostrata Cloud Extension								
Name	Cloud Provider	License Type	Size	Region	VPC-ID / Virtual	Node A Availabi	Node B Availabi	Status
datacenter-2_vpc-1410ff71	Aws	Bring Your Own	Large	eu-west-1	vpc-1410ff71	eu-west-1c	eu-west-1c	Impaired

The screenshot shows a detailed view of a component's status. A blue box labeled "Status: Active//Impaired" points to the status field in the table. Another blue box labeled "Component" points to the component name "datacenter-2_vpc-1410ff71_1486473374_Xf6". A third blue box labeled "Error List (Code, Severity)" points to the error list in the detailed view.

datacenter-2_vpc-1410ff71_1486473374_Xf6

Last seen in 'Active' state at 02-08-2017 09:49:58 [UTC].

Edge A: Impaired:
Check Instance Not Terminated Failed (840, High)

Edge B: Active
On Premises Edge: Active
Windows Servicing Instance: Active
Cloud Api: Active
VPN: Active

Component	External Code	Description
CloudEdge1 / CloudEdge2	110	CloudEdge Process
	120	CloudEdge Functionality
	140	Storage Grid Process
	145	Object Store Availability
	150	Cloud Control Access
	160	VPN Access

Component	External Code	Description
	800	Instance Running
	170	iSCSI Layer
	820	Critical Disk Space Utilization
	830	Instance Availability
	840	Check Instance Not Terminated
	850	Internal Error
	860	SQS
Exporter	410	Exporter Process
	420	Exporter Functionality
	830	Instance Availability
	840	Check Instance Not Terminated
	140	Storage Grid Process
	145	Object Store Availability
	850	Internal Error
Backend	210	Backend Service
	220	Backend Functionality
	830	Instance Availability
	850	Internal Error
		Critical Local DiskSpace Utilization

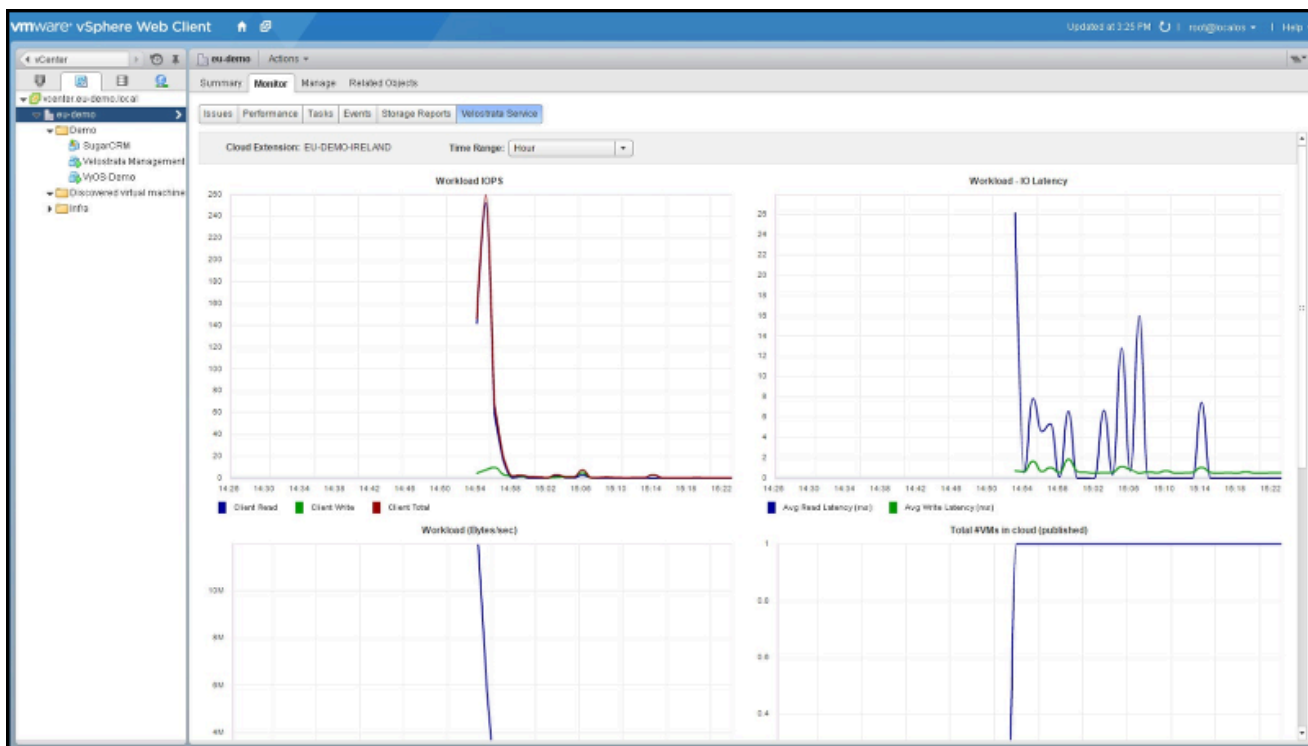
Monitoring the Cloud Extension

To monitor the current run state of the Cloud Extension, review the Velostrata **Cloud Extension** portlet added to the virtual Datacenter **Summary** page. If the Cloud Extension appears in an **Impaired** state, it cannot be used to run new VMs in cloud.

Remediation Tip: If a Cloud Extension appears impaired due to a cloud host health issue, stopping and starting the Cloud Extension may fix the issue as affected instances are restarted on a healthy host. Alternatively, repair the Cloud Extension. See [Repairing a Cloud Extension](#).

To monitor the Cloud Extension:

- To monitor performance and operational statistics for the Cloud Extension, click your datacenter and then use the **Monitor > Velostrata Service** tab. You can review performance and usage stats aggregated across all VMs and Cloud Edges associated with this Cloud Extension. You can also review the total number of VMs running in cloud, WAN usage, IOPS, IO latency and throughput as well as other efficiency metrics.



Graphs are offered at pre-canned periods of Hour, Day, 7 days, 30 days as well as a user-defined custom range.

The following metrics are available:

- **Workload:**
 - **IOPS:** Total IO operations per second generated by VMs in cloud, using this Cloud Extension (nodes A + B).
 - **IO Latency (ms):** Average IO latency for IO operations across all VMs in cloud, using this Cloud Extension.
 - **Throughput (Bytes/sec):** Total throughput across all VMs in cloud, using this Cloud Extension (nodes A + B).
- **WAN Usage (Bytes/sec):** Total WAN throughput in each direction for the Cloud Extension, as reported by nodes A + B.
- **Total #VMs in Cloud (running or stopped):** Total VMs in cloud, using this Cloud Extension.
- **Datastore IO Offload%:** Average IO offload across node A and B. This is based on the ratio of IO operations that were handled in cloud by nodes A and B, vs the total IO operations over the related vSphere Datastores on premises.

High Availability Overview

Velostrata Cloud Extension provides High Availability by using an active-passive model. Workloads use iSCSI multipath, and are connected to the primary and replica Cloud Edge nodes, but served only by the primary Cloud Edge node. When the primary Cloud Edge fails, the workloads failover to use the secondary Cloud Edge. Failback to the primary Cloud Edge is done once it becomes active again. For more information about the events that occur with failover and failback, see [Viewing the Cloud Extension Status](#).

A Cloud Extension with an **"impaired"** status functions differently depending on whether one, or both, Cloud Edge nodes have failed:

- If both Cloud Edge nodes are impaired, the Cloud Extension cannot be used to run new VMs in cloud, and will cause failures to VMs currently running in cloud. You can perform a forced move back, run the "prepare-to-detach" operation, and stop a VM.
- If one of the Cloud Edge nodes is impaired, and the other Cloud Edge node is active most of the usual operations are still available.

Similarly, if the VPN (access to CE), Cloud API, Backend or Management component fails, the Cloud Extension will be impaired and a limited set of actions will be available.

Use the tooltip to try and determine the reason for the failure. See [Viewing the Cloud Extension Status](#).

Note: When one of the Cloud Edge nodes is down, the Cloud Edge does not provide high availability, in order to avoid any chance of data loss, all data is written to the object store, which reduces the Cloud Extension performance. For that reason, it is not recommended to move more VMs from on-premise to a Cloud Extension where one of the Cloud Edge nodes is impaired. When you move a VM to the cloud, and the Cloud Extension is impaired, the Cloud Extension name includes an indication that it is impaired in the **Velostrata Cloud Extension** page in the **Run in Cloud** wizard. See [Viewing the Cloud Extension Status](#).

- If a Cloud Extension is impaired due to incomplete deployment or initial health checks that did not pass. This is most likely due to pre-requisites that are not met, after fixing the underlying causes, use [Repair Cloud Extension](#). Repairing the cloud extension attempts to re-create the missing components and/or run relevant health checks. Once the Cloud Extension is repaired, the status is set to **Active**.
- If a Cloud Extension is impaired due to a cloud host health issue, stopping and starting the Cloud Extension may remediate the issue as affected instances are restarted on a healthy host.

For more information on how to view the Cloud Extension status, and the events that occur, see [Viewing the Cloud Extension Status](#).

Viewing the Cloud Extension Status

To monitor the current run state of the Cloud Extension, review the Velostrata **Cloud Extension** portlet added to the virtual Datacenter **Summary** page.

A cloud extension state can be “Creating”, “Starting” “Stopping” “Deleting” “Active”, or “Impaired”.

For information on Velostrata High Availability, see [High Availability Overview](#).

Remediation Tip: If a Cloud Extension appears impaired due to a cloud host health issue, stopping and starting the Cloud Extension may re-mediate the issue as affected instances are restarted on a healthy host.

An impaired Cloud Extension can be caused due to components that were not successfully deployed failures during system operation. These are presented in the list of health checks that did not pass. After fixing the underlying causes, the Cloud Extension can be repaired. Repairing the cloud extension attempts to re-create the missing components and/or run relevant health checks. See [Repairing the Cloud Extension](#). Once the Cloud Extension is repaired, the status is set to **Active**.

The following health checks are performed every 1 minute to report on Cloud Extension status:

- Cache Store Accessibility
- Velostrata Storage Grid Service Status
- Velostrata Cloud Edge Service
- SCSI Target
- Cloud Edge Local Storage
- Cloud Edge Functionality
- Exporter Service
- Exporter Functionality
- On-Premises Edge Service
- SQS Service (if the AWS region supports the SQS Service)

Enhanced Degraded Mode

Velostrata 3.0+ supports an Enhanced Degraded Mode using the AWS SQS service. This delivers improved performance and is currently applicable in the following AWS regions:

- US East (N. Virginia)
- US East (Ohio)

- US West (Oregon)
- EU (Ireland)

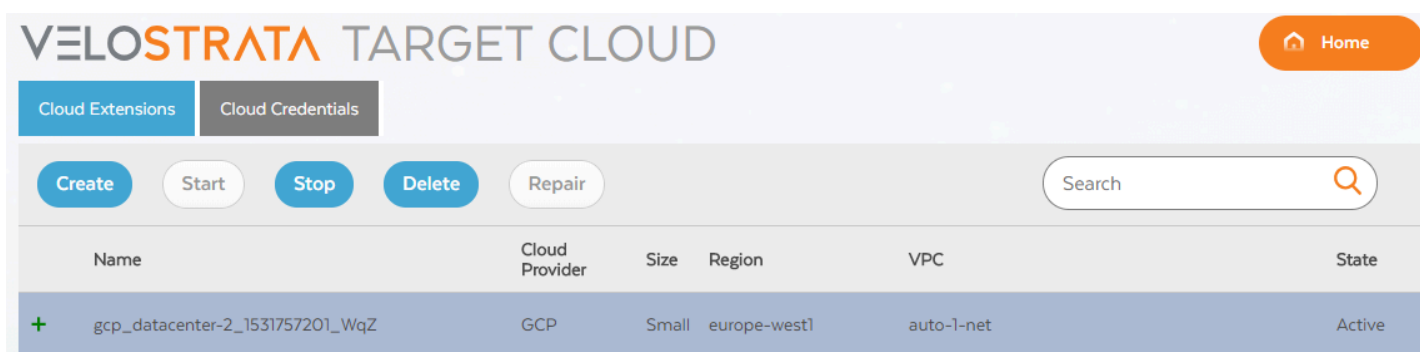
Additional AWS regions will automatically be added as soon as the SQS service is available. This Enhanced Degraded Mode is only applicable to VMs moved to the cloud in version 3.0.

Note: The new Enhanced Degraded Mode does not apply if the SQS service is unavailable in the region, or if the VM that went into Degraded Mode was upgraded from an older version. This impacts performance but does not impact on the service.

An SQS health check is run on the regions that support the SQS service. The health check will fail only in supported regions when there is an on-going disruption. Moreover, the health-check impact is marked as “Medium”, meaning the CE will not become Impaired due to the failure.

To view basic Cloud Extension status from the web:

1. Login to your Velostrata web management appliance via HTTPS://IP_OF_VELO_MGMT.
2. Click the Target Cloud icon.
3. A list of Cloud Extensions appear with their state listed on the far right.
4. You can perform limited operations on a Cloud Extension by selecting one and using the buttons at the top to start, stop, delete, or repair.



The screenshot shows the Velostrata Target Cloud web interface. At the top, there's a header with the Velostrata logo and 'TARGET CLOUD'. Below the header, there are two tabs: 'Cloud Extensions' (active) and 'Cloud Credentials'. Under the 'Cloud Extensions' tab, there are five buttons: 'Create', 'Start', 'Stop', 'Delete', and 'Repair'. To the right of these buttons is a search bar. Below the buttons and search bar is a table with the following columns: Name, Cloud Provider, Size, Region, VPC, and State. The table contains one entry: 'gcp_datacenter-2_1531757201_WqZ' with Cloud Provider 'GCP', Size 'Small', Region 'europe-west1', VPC 'auto-l-net', and State 'Active'.

Name	Cloud Provider	Size	Region	VPC	State
gcp_datacenter-2_1531757201_WqZ	GCP	Small	europe-west1	auto-l-net	Active

To view advanced Cloud Extension status from vCenter:

1. To view the Cloud Extension status, view the **Datacenter > Summary** tab.

[illegible]

Status

Active

Impaired

datacenter-2_vpc-1410ff71_1495543194_CDb

Last seen in 'Active' state at 05-23-2017 13:19:52 [UTC].

Edge A: Active

Edge B: Impaired:

Instance Not Stopped Failed (800, High)

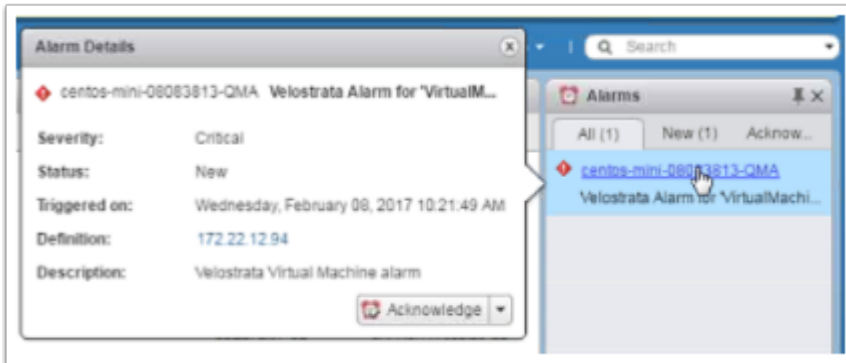
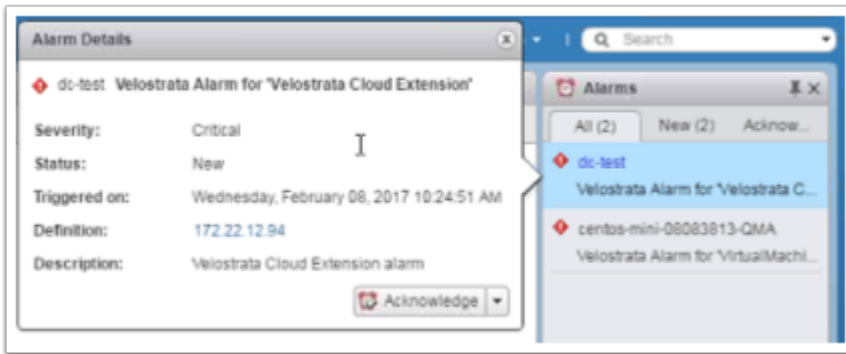
On Premises Edge: Active

Cloud Api: Active

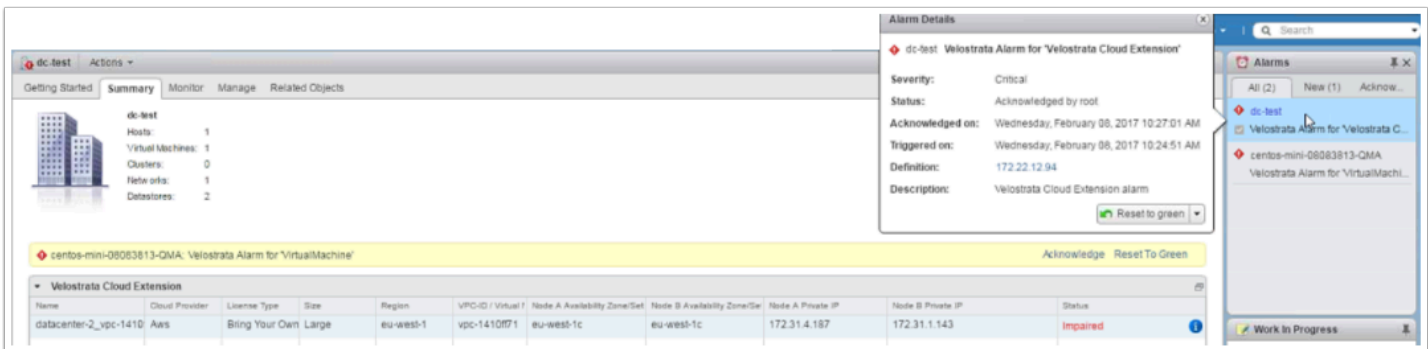
VPN: Active

The screenshot shows the Velocloud console interface. The main panel displays the 'Summary' tab for a resource named 'dc-test'. On the left, there's a summary of resources: Hosts: 1, Virtual Machines: 1, Clusters: 0, Networks: 1, and Datastores: 2. On the right, there are progress bars for CPU, MEMORY, and STORAGE usage. A red box highlights the 'Alarms' section, which contains two alarms: 'Velostrata Alarm for 'Velostrata Cloud Extension'' and 'centos-mini-06083813-QMA: 'Velostrata Alarm for 'VirtualMachine''. Below the alarms, there's a table for 'Velostrata Cloud Extension' with columns: Name, Cloud Provider, License Type, Size, Region, VPC ID / Virtual ID, Node A Availability Zone/Set, and Node B Availability Zone/Set. The table has one row: 'datacenter-2_vpc-1410' with 'Aws' provider, 'Bring Your Own' license, 'Large' size, 'eu-west-1' region, and 'vpc-1410f71' VPC ID. To the right of the table, there's a details panel for 'centos-mini-06083813-QMA' showing its status as 'Active' and a list of components: Edge A (Impaired), Edge B (Active), On Premises Edge (Active), Windows Servicing Instance (Active), Cloud Api (Active), and VPN (Active).

Name	Cloud Provider	License Type	Size	Region	VPC ID / Virtual ID	Node A Availability Zone/Set	Node B Availability Zone/Set
datacenter-2_vpc-1410	Aws	Bring Your Own	Large	eu-west-1	vpc-1410f71	eu-west-1c	eu-west-1c



5. To acknowledge the alarm, click **Acknowledge**.



6. To view the related events, select **Monitor > Events**. In this example, the Cloud Extension is degraded as Cloud Edge node A has failed. The VM is moved to Cloud Edge node B and the following events appear during failover.

Issues Performance **Tasks & Events** Velostrata Service

Tasks
Events
Scheduled Tasks

Filter

Description	Type	Date Time	Task	Target	User
Alarm 'Velostrata Alarm for V...	Information	5/28/2017 9:57:36 AM		centos-mini-280...	
Velostrata Event - vm-13 rais...	Warning	5/28/2017 9:57:35 AM		centos-mini-280...	hx1495953270
Velostrata VM (vm-13) error: ...	Error	5/28/2017 9:57:35 AM		centos-mini-280...	hx1495953270
General event: Event by Velo...	Information	5/28/2017 9:53:27 AM		centos-mini-280...	hx1495953270
Task: Create virtual machine...	Information	5/28/2017 9:48:51 AM	Create virtual machine s...	centos-mini-280...	hx1495953270
Task: Reload virtual machine	Information	5/28/2017 9:48:50 AM	Reload virtual machine	centos-mini-280...	hx1495953270
Virtual machine centos-mini-...	Information	5/28/2017 9:48:47 AM		centos-mini-280...	hx1495953270
Task: Consolidate virtual ma...	Information	5/28/2017 9:48:47 AM	Consolidate virtual mach...	centos-mini-280...	hx1495953270
Reconfigured centos-mini-2...	Information	5/28/2017 9:48:44 AM		centos-mini-280...	hx1495953270
Task: Reconfigure virtual ma...	Information	5/28/2017 9:48:43 AM	Reconfigure virtual mach...	centos-mini-280...	hx1495953270
Task: Velostrata Manager Ru...	Information	5/28/2017 9:48:43 AM	Velostrata Manager Run ...	centos-mini-280...	root

69 items Previous Next Export Copy

Date Time: 5/28/2017 9:57:35 AM Target: centos-mini-28093556-JAR
 User: hx1495953270 Type: Warning

Description:
 5/28/2017 9:57:35 AM Velostrata Event - vm-13 raised event of type VmFailover at 5/28/17 6:56 AM

Event Type Description:

Possible Causes:

Related events:
 There are no related events.

7. Once Cloud Edge node A is active, failback occurs and the VM is moved back to Cloud Edge node A and the following events appear.

Issues Performance **Tasks & Events** Velostrata Service

Tasks
Events
Scheduled Tasks

Filter

Description	Type	Date Time	Task	Target	User
Velostrata Event - vm-13 raised event of type VmFailback at 5/28/17 7:06 AM	Warning	5/28/2017 10:07:30 AM		centos-mini-280...	hx1495953270
Alarm 'Velostrata Alarm for VirtualMachine' on centos-mini-28093556-JAR chan...	Information	5/28/2017 10:06:26 AM		centos-mini-280...	
Velostrata VM (vm-13) error cleared: Degraded Mode	Information	5/28/2017 10:06:25 AM		centos-mini-280...	hx1495953270
Velostrata VM (vm-13) error cleared: Degraded Mode	Information	5/28/2017 10:06:25 AM		centos-mini-280...	hx1495953270
Alarm 'Velostrata Alarm for 'Velostrata Cloud Extension' on dc-test changed fro...	Information	5/28/2017 10:05:40 AM		dc-test	
Cloud Extension 'datacenter-2_vpc-1410ff71_1495953356_fm' is Active	Information	5/28/2017 10:05:39 AM		dc-test	hx1495953270
Cloud Extension 'datacenter-2_vpc-1410ff71_1495953356_fm' is Active	Information	5/28/2017 10:05:39 AM		dc-test	hx1495953270
Velostrata System Event - raised event of type FrontendStarted at 5/28/17 7:04 AM	Information	5/28/2017 10:05:20 AM		dc-test	hx1495953270
Alarm 'Velostrata Alarm for 'Velostrata Cloud Extension' on dc-test changed fro...	Information	5/28/2017 10:00:32 AM		dc-test	
Cloud Extension health check failed: 'datacenter-2_vpc-1410ff71_1495953356_...	Error	5/28/2017 10:00:31 AM		dc-test	hx1495953270
Alarm 'Velostrata Alarm for VirtualMachine' on centos-mini-28093556-JAR chan...	Information	5/28/2017 9:57:36 AM		centos-mini-280...	

79 items Previous Next Export Copy

Date Time: 5/28/2017 10:07:30 AM Target: centos-mini-28093556-JAR
 User: hx1495953270 Type: Warning

Description:
 5/28/2017 10:07:30 AM Velostrata Event - vm-13 raised event of type VmFailback at 5/28/17 7:06 AM

Event Type Description:

Possible Causes:

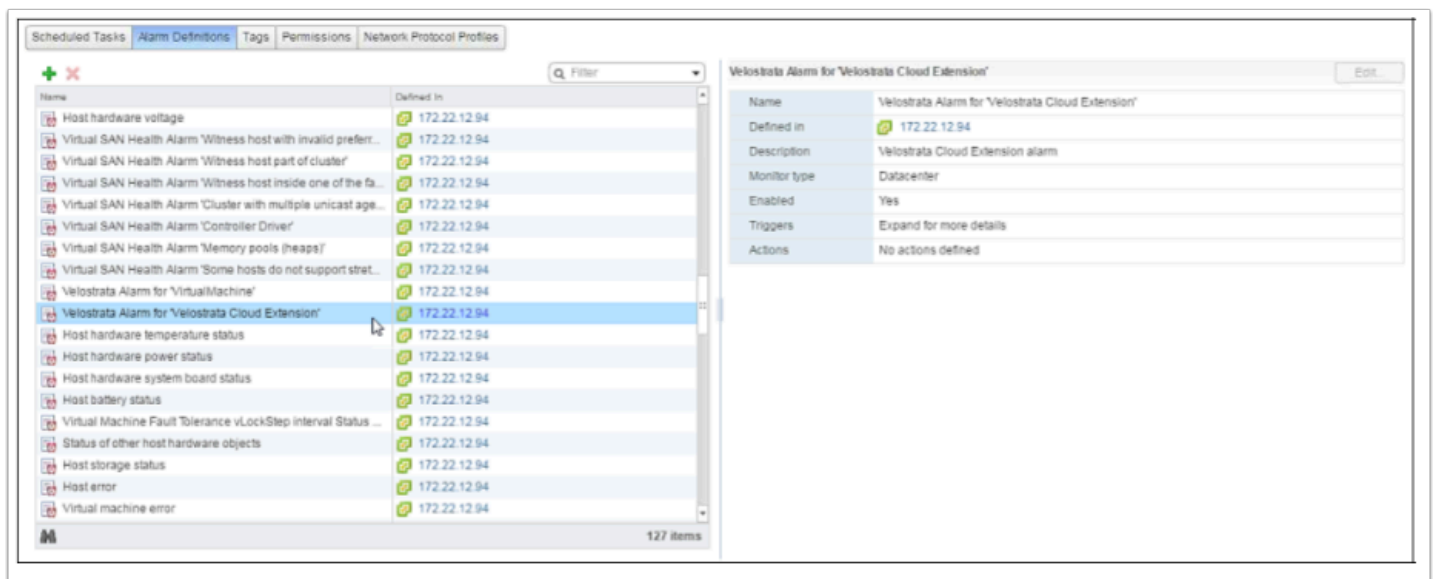
Related events:
 There are no related events.

Viewing Velostrata vCenter Alarms and Events

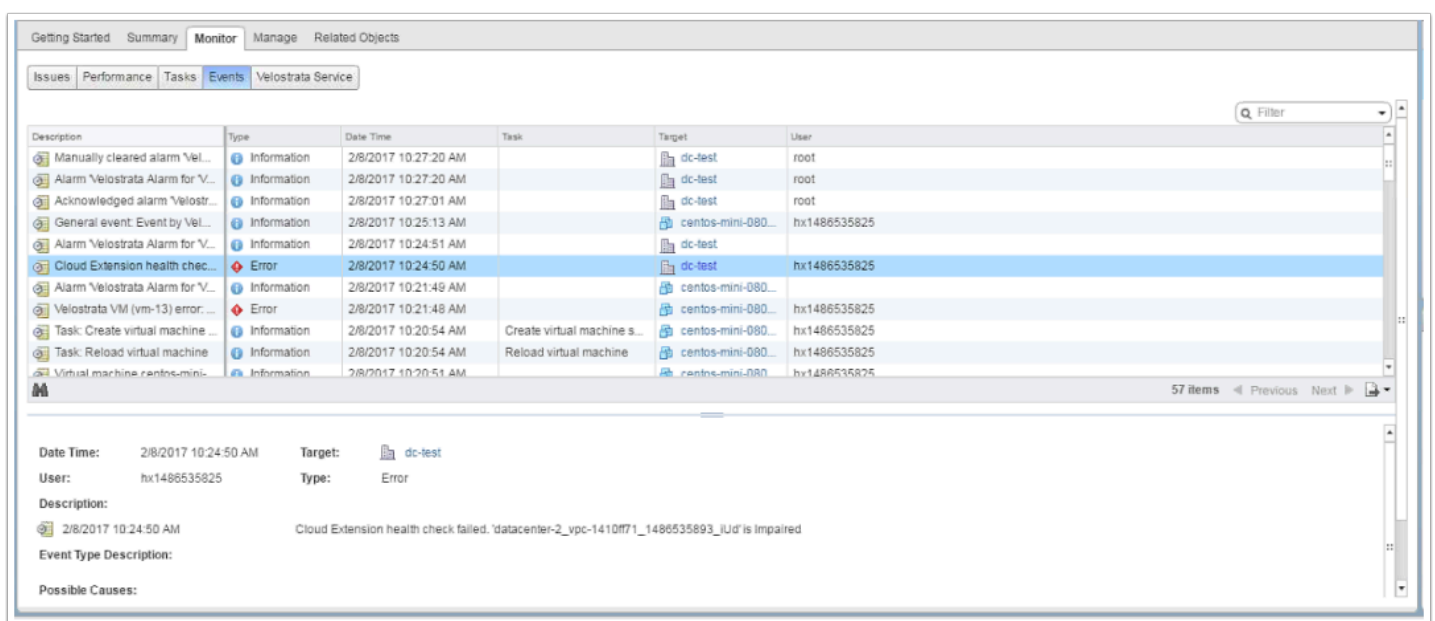
When the Velostrata plug-in is installed, two alarm definitions are added to vCenter:

1. **Velostrata Alarm for 'VirtualMachine'**
2. **Velostrata Alarm for 'Velostrata Cloud Extension'**

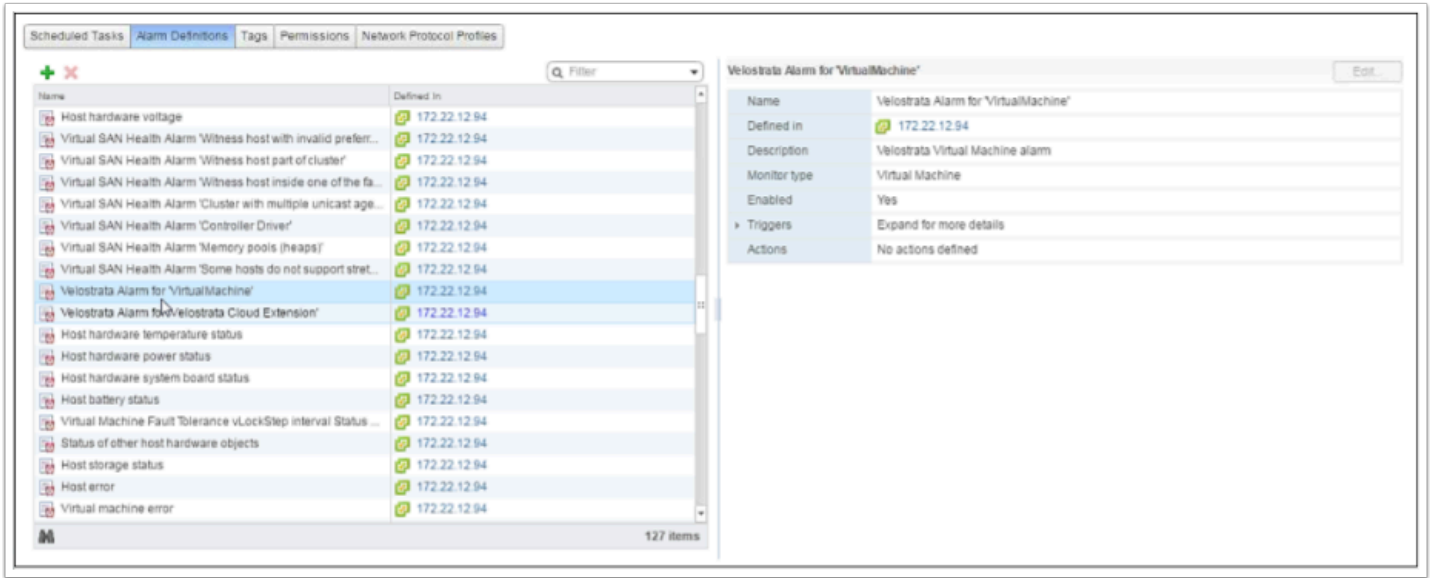
Velostrata triggers an alarm in vCenter whenever a Cloud Extension is in an **Impaired** state. The alarm is cleared when the Cloud Extension returns to an **Active** state. The alarm is triggered on the associated Datacenter.



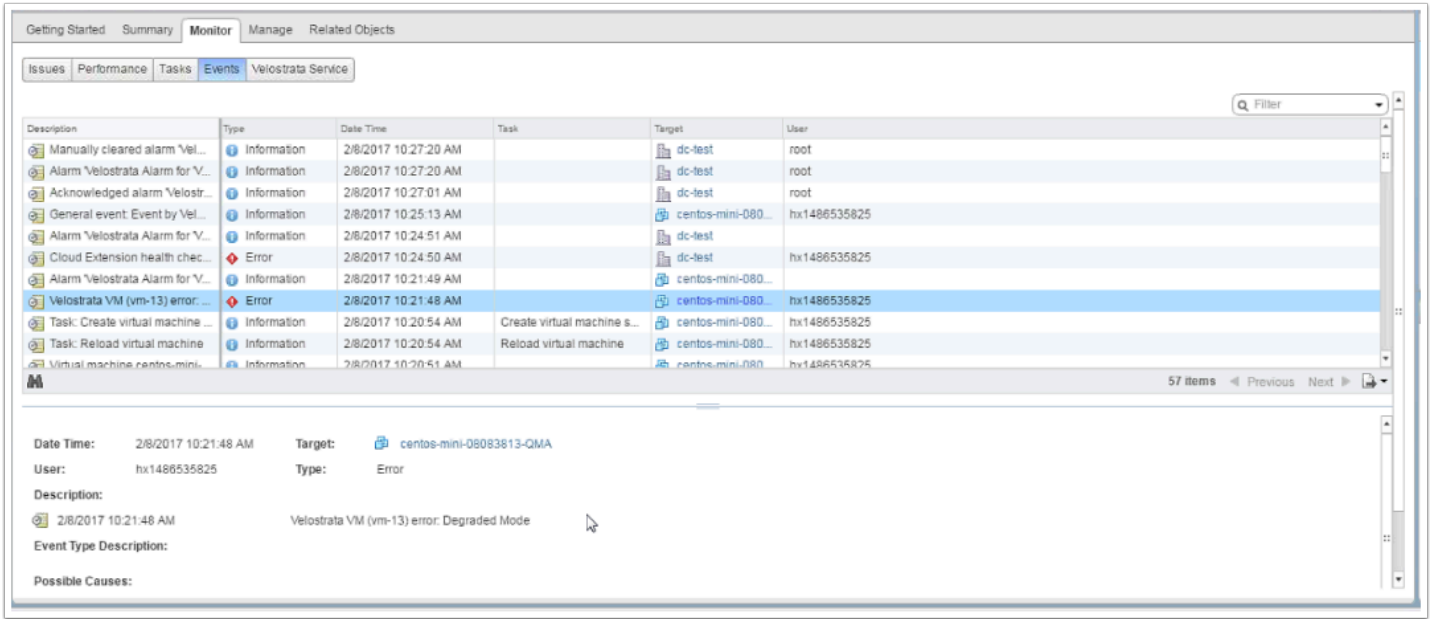
A corresponding **Error** event appears too.



If for example, a node in the Cloud Extension is stopped, an alarm is also raised for any VM running in the Cloud Extension, because although the VM is running, its performance is degraded.



More details appear in the events. For example, there is an **Error** event for the VM, showing that it is in **Degraded** mode.



Viewing the Velostrata vSphere Connectivity Alarm in the Velostrata Manager

You can view a connectivity to vSphere alarm in the Velostrata Manager. You can also create a support bundle from the configuration page.

To view the vSphere connectivity alarm in the Velostrata Web Manager:

1. Open a Web browser and navigate to the Velostrata Manager Virtual Appliance IP address, for example,
2. Click the **System Settings** icon.
3. Login when prompted with username 'localsupport'. Use your Velostrata Subscription ID or GCP Billing ID as your password.

VELOSTRATA SYSTEM SETTINGS

Home

Logs vCenter Plugin Network Settings

Download Support Bundle View System Alarms (0)

Enable Automatic Support Bundle Upload

Support bundle will be uploaded periodically to the Velostrata service.
Support bundles do not contain credentials or personally identifiable information

Enable Telemetry

Velostrata Telemetry collects and stores operational and performance metrics reported by Velostrata software components. This information provides:

- Performance graphs in the vSphere web client
- Activity Monitoring in the vSphere web client

All metrics collected are communicated over an encrypted connection and are identifiable only by the subscription ID of the system. No personally identifiable information, or private data is collected by the service.

Telemetry and log aggregation service location: EU

Apply

© 2018, Velostrata Ltd. VELOSTRATA.COM
Terms of Use | Open Source Licenses

4. Click the **View System Alarms (x)** button.
5. This brings up a prompt with all system alarms currently.

- Logs
- vCenter Plugin
- Network Settings

Download Support Bundle

View System Alarms (0)

Enable Automatic Support Bundle Upload

Support bundle will be uploaded periodically to the Velostrata service.

Support bundles do not contain credentials or personally identifiable information

☐ Yes ☒ No

Enable Telemetry

Velostrata Telemetry collects and stores operational and performance data from Velostrata software components. This information provides:

- Performance graphs in the vSphere web client
- Activity Monitoring in the vSphere web client

All metrics collected are communicated over an encrypted connection and are identifiable only by the subscription ID of the system. No personally identifiable information, or private data is collected by the service.

☒ Yes ☐ No

System Alarms

No internal alarms.

Telemetry and log aggregation service location:

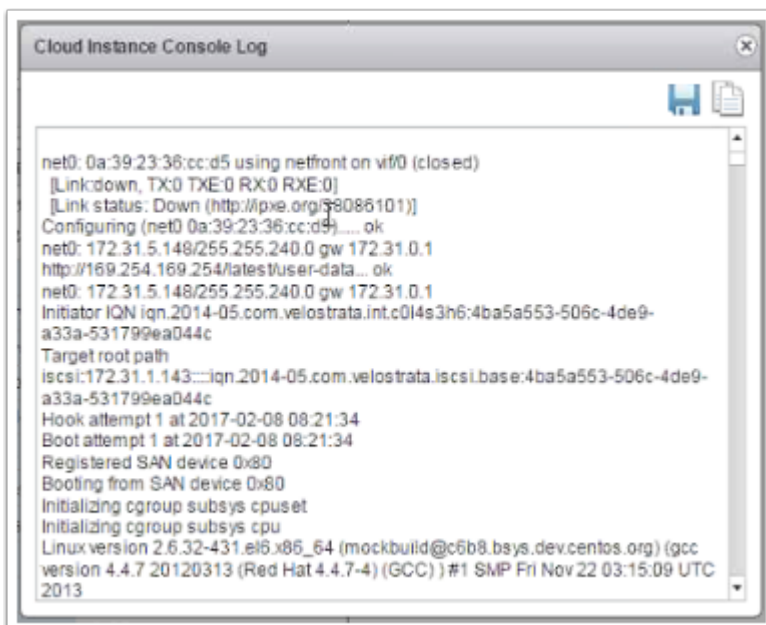
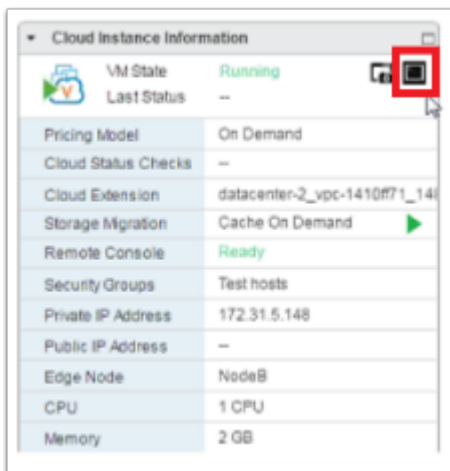
Apply

Viewing the Cloud Instance Console Log or Screenshot

You can view the Cloud Instance Console Log for a VM. You can either save the log or copy it to the clipboard. When requesting support, please supply a copy of the related logs. You can also save a copy of the cloud instance screenshot.

To view the Cloud Instance Console Log or screenshot:

1. In the Cloud Instance Information pane, click the **Collect cloud instance console log** icon.



2. To save the log, click **Save file to your local system**.
3. Name the file, select a location to save the file and click **Save**.
4. To copy the log, click **Save logs to Clipboard**.
5. To save a copy of the cloud instance screenshot, click **Collect cloud instance screenshot**.

6. To save the screenshot, click **Save file to your local system**.
7. Name the file, select a location to save the file and click **Save**.

Saving a Support Bundle in the Velostrata Manager

You can create a support bundle from the Velostrata Manager configuration page. Send this with your support request.

To save a support bundle in the Velostrata Web Manager:

1. Open a Web browser and navigate to the Velostrata Manager Virtual Appliance IP address, for example,
2. Click the **System Settings** icon.
3. Login when prompted with username 'localsupport'. Use your Velostrata Subscription ID or GCP Billing ID as your password.

VELOSTRATA SYSTEM SETTINGS

Home

Logs vCenter Plugin Network Settings

Download Support Bundle View System Alarms (0)

Enable Automatic Support Bundle Upload
Support bundle will be uploaded periodically to the Velostrata service.
Support bundles do not contain credentials or personally identifiable information

Yes No

Enable Telemetry
Velostrata Telemetry collects and stores operational and performance metrics reported by Velostrata software components. This information provides:
- Performance graphs in the vSphere web client
- Activity Monitoring in the vSphere web client
All metrics collected are communicated over an encrypted connection and are identifiable only by the subscription ID of the system. No personally identifiable information, or private data is collected by the service.

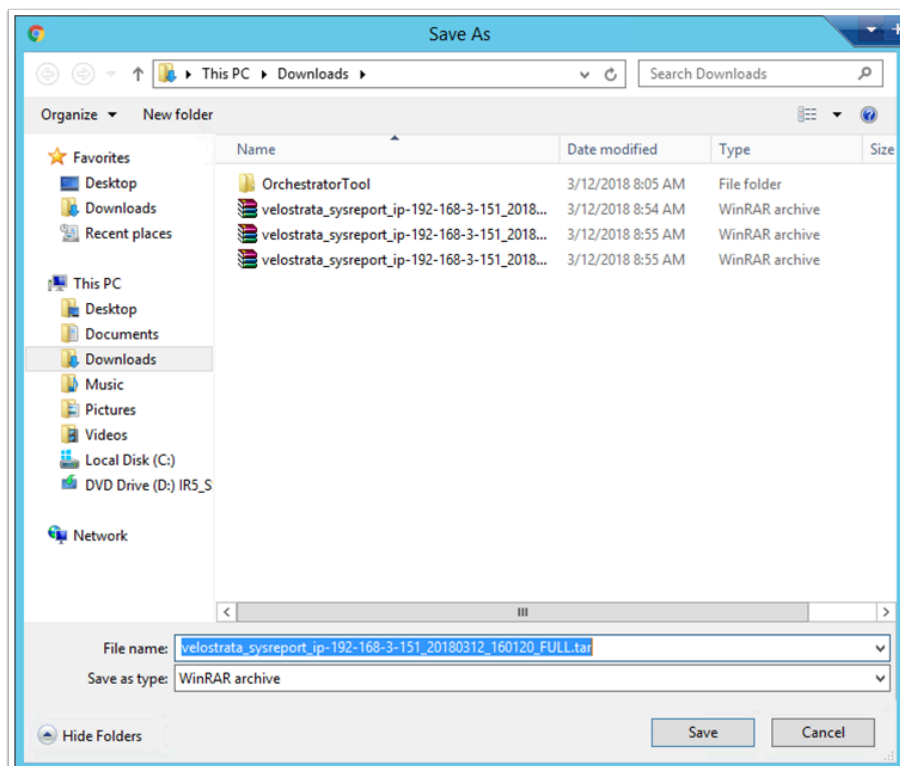
Yes No

Telemetry and log aggregation service location: EU

Apply

© 2018, Velostrata Ltd. VELOSTRATA.COM
Terms of Use | Open Source Licenses

4. Click the **Download Support Bundle**. The support bundle is generated and you will be prompted where you would like to save the tar file on your hard disk.




Automatically Moving a Terminated VM to On-Premises

If a VM is in a **Terminated** state, Velostrata automatically moves the VM back to on-premises (so that it is no longer managed by Velostrata). This applies to both spot and on-demand VMs. If the storage policy is **Write Back**, the uncommitted writes are written back to on-premises before the VM is moved backed to on-premises. This happens automatically.

When a non-spot terminated VM is moved to on-premise, a warning event appears.

vApp Details

Cloud Instance Information



VM State

Shutting Down

Last Status

--

Pricing Model	On Demand
Cloud Status Checks	--
Cloud Extension	datacenter-2_vpc-1410f71_1486535893_iUd
Storage Migration	Cache On Demand
Remote Console	Unavailable
Security Groups	--
Private IP Address	
Public IP Address	--
Edge Node	NodeB
CPU	1 CPU
Memory	2 GB
Cloud Instance Id	i-01b8dcdb96ddd2646
Instance Type	t2.small
Storage Policy	Write Back (uncommitted: 3.7MB)
Network Adapter	eni-1b582c4b

Troubleshooting Cloud Edge Components

The customer may contact the Velostrata Support Team to resolve specific issues that might require troubleshooting and inspection of the Cloud Edge appliances. In this case, the customer and the support representative will create temporary SSH access to access the Cloud Edge appliances. Access to the FE is then enabled using a combination of the certificate authority (CA) key pair - generated by the system admin, and a passphrase provided by Velostrata support. The generated key expires after 8 hours.

For more information, contact the Velostrata Support Team.

Understanding the Velostrata Telemetry Service

Velostrata Telemetry collects and stores operational and performance metrics reported by Velostrata software components. This information provides:

- Performance graphs in the vSphere web client (e.g. IOPS, IO latency, throughput)
- Activity Monitoring in the vSphere web client (e.g. - VMs in the cloud, migration activity, WAN utilization).
- Troubleshooting functional and performance issues and customer support.

All metrics collected and sent to Velostrata Telemetry are communicated over an encrypted connection and are identifiable only by the subscription ID configured by the customer during installation. Telemetry information includes operation metrics, such as network transfer volumes, I/O activity and response times, task type counters and API request statistics.

No personal names, birth dates, Social Security numbers or migrated server names are collected or stored by the Velostrata Telemetry service.

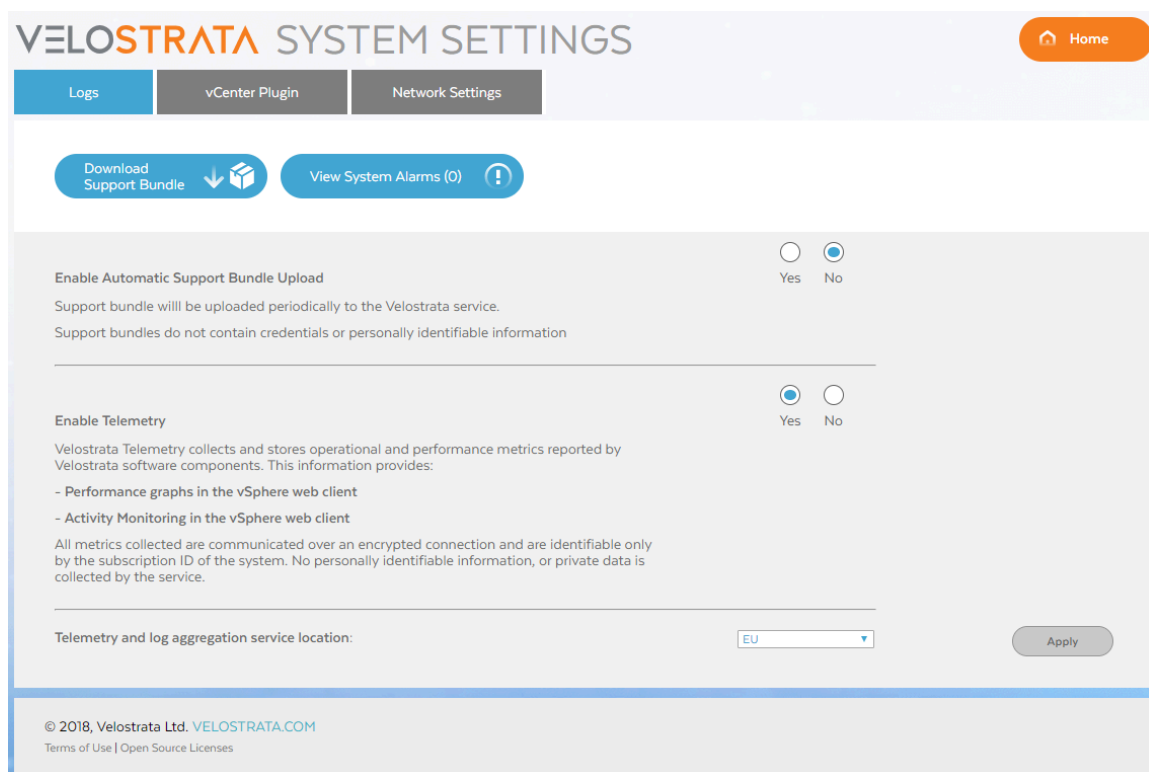


It is highly recommended to keep the telemetry service enabled for full functionality of the Velostrata product and to enable expedited customer support experience. However, if security or other reasons prohibit the use of the telemetry service, please notify and consult with Velostrata Support. You may also request the latest list of metrics collected.

Instructions for disabling telemetry reporting (if desired):

Disabling the Telemetry via Velostrata Web Manager

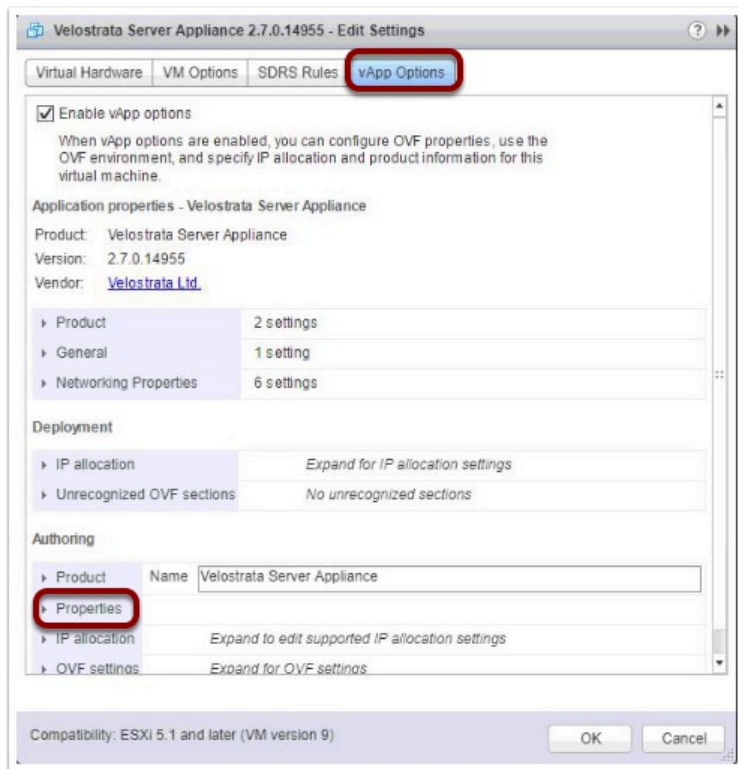
1. Open a Web browser and navigate to the Velostrata Manager Virtual Appliance IP address, for example,
2. Click the **System Settings** icon.
3. Login when prompted with username 'localsupport'. Use your Velostrata Subscription ID or GCP Billing ID as your password.



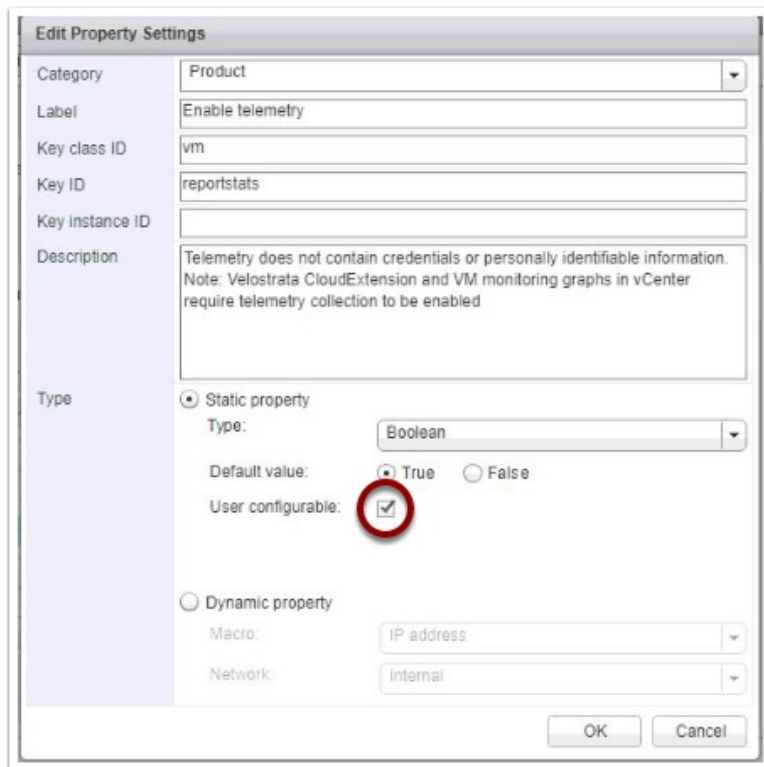
The screenshot shows the 'VELOSTRATA SYSTEM SETTINGS' interface. At the top, there are tabs for 'Logs', 'vCenter Plugin', and 'Network Settings'. Below these are buttons for 'Download Support Bundle' and 'View System Alarms (0)'. The main section contains two toggle switches: 'Enable Automatic Support Bundle Upload' (set to 'No') and 'Enable Telemetry' (set to 'No'). Below the 'Enable Telemetry' toggle, there is a list of features provided by telemetry: 'Performance graphs in the vSphere web client' and 'Activity Monitoring in the vSphere web client'. A note states that all metrics are communicated over an encrypted connection and are identifiable only by the subscription ID. At the bottom, there is a dropdown menu for 'Telemetry and log aggregation service location' set to 'EU' and an 'Apply' button. The footer contains copyright information for 2018 and links to 'Terms of Use' and 'Open Source Licenses'.

4. Toggle the **Enable Telemetry** option from YES to NO.

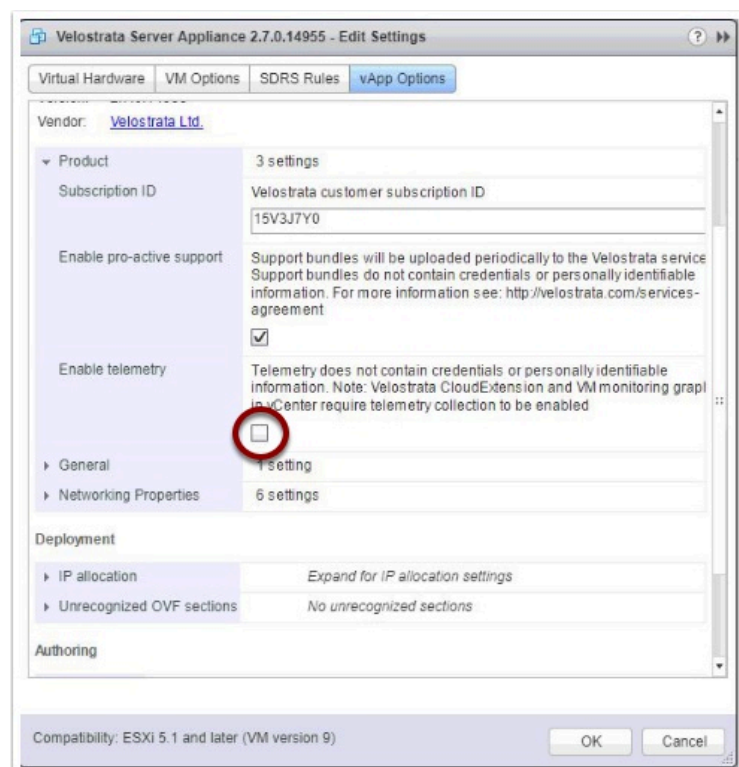
Disabling the Telemetry via vCenter



- 4. Under **Authoring**, expand **Properties**, select **vm.reportstats**, and click **Edit**.
- 5. Check **User configurable**, and click **OK**.



6. Back on the **vApp Options** tab, under **Application properties - Velostrata Server Appliance**, expand **Product** and verify that **Enable telemetry** is unchecked, then click **OK**.



7. Power on the Velostrata virtual appliance.

1. Shut down the Velostrata Management Virtual Appliance in vSphere.
2. In the vSphere web console, right-click the Velostrata virtual appliance and select **Edit Settings**.
3. Click on the **vApp Options** tab.

Deploying Velostrata Prep Package for Linux Virtual Machines

Supported Linux Distributions and Versions

The following Linux distributions and versions are currently supported:

- Red Hat Enterprise Linux / CentOS 6.x, 7.x
- SUSE Linux Enterprise Server (SLES) 11 SP2 - SP4; SLES 12
- Ubuntu 14.04., Ubuntu16.04, Ubuntu 17.10, Ubuntu 18.04.

You will need to install the pre-requisite Velostrata prep package and its dependencies on the virtual machine you intend to run in cloud. The Velostrata package can remain installed when the virtual machine running on-premises to allow a future impromptu run in-cloud.

- For RHEL/CentOS 6, 7, download and install the velostrata-prep RPM from: <http://tiny.cc/velos-v3-rhel6>
- For SUSE 11, 12, download and install the velostrata-prep RPM from: <http://tiny.cc/velos-v3-suse11>
- For Ubuntu, download and install the velostrata-prep deb package from: <http://tiny.cc/velos-v3-ubuntu>

Disk Device Mappings in Linux

For correct handling of disk device mount points when running in cloud or when performing full migration on either GCP, Azure or AWS, the Linux setup must reference logical disk reference - e.g. using LVM, or UUID. If disk mount points are using direct device mounts (e.g. /dev/sdaX) then these need to be modified to a logical reference, otherwise no action is needed.

The Velostrata RPM will automatically check for direct device mounts when installed and will automatically update /etc/fstab to use UUID based reference.

How-to: Red Hat Enterprise Linux (RHEL) 6/7 and CentOS 6/7 Prep for Run in GCP/AWS/Azure

Overview

A Red Hat Linux VM will require certain adaptation done in order to run in GCP, AWS, Azure using Velostrata.

Specifically, GCP, AWS and Azure are based on a different hypervisor platform which results different configuration, for instance - networking. In addition, when using Velostrata, the virtual machines are booting using the Velostrata Cloud Edge virtual appliance as their storage target and not a local virtual disk and this will be configured on-the-fly.

Installation Steps

There are two ways to install the Velostrata RPM package:

- Download and install the prerequisites, and then install the velostrata-prep RPM
 - Install the velostrata-prep RPM using yum. This automatically fetches and installs the required pre-requisites.
1. Log in to the workload VM.
 2. Download the latest velostrata-prep RPM from: <http://tiny.cc/velos-v3-rhel6>
 3. Check for the list of prerequisites by running:

```
rpm -qpR velostrata-prep-VERSION.redhat.x86_64.rpm
```



For example

```
rpm -qpR velostrata-prep-1.8-12.redhat.x86_64.rpm
```

4. Download and install the prerequisites.
5. Install the velostrata-prep RPM.

```
rpm -Uvh velostrata-prep-VERSION.redhat.x86_64.rpm
```

For example

```
rpm -Uvh velostrata-prep-1.8-12.redhat.x86_64.rpm
```

-or-

1. Log in to the workload VM.
2. Download the latest velostrata-prep RPM from: <http://tiny.cc/velos-v3-rhel6>
3. Install the velostrata-prep RPM (velostrata-prep-VERSION.redhat.x86_64.rpm) using yum.
This automatically fetches and installs the required pre-requisites.

NOTE: No reboot is required.

NOTE: If the installation is unsuccessful or if there are any warnings, ensure that you address them prior to executing the run-in-cloud operation.

How-to: SUSE Enterprise Linux Server (SLES) 11/12 Prep for Run in GCP/AWS/Azure

Overview

A SUSE Linux Enterprise Server 11 (SLES) and SLES 12 will require certain adaptation done in order to run in the cloud using Velostrata.

Specifically, GCP, AWS and Azure are based on a different hypervisor platform than the source hypervisor, which results in different configuration, for instance - networking. In addition, when using Velostrata, the virtual machines are booting using the Velostrata Cloud Edge virtual appliance as their storage target and not a local virtual disk and this will be configured on-the-fly.

Installation Steps

1. Login to the SLES virtual machine with root access user.
2. Install the SLES **xen-kmp-default** package:

```
zypper install xen-kmp-default
```

3. Reboot.
4. Install the **velostrata-prep** package (download from: <http://tiny.cc/velos-v3-suse11>)

```
zypper install velostrata-prep-VERSION.suse.x86_64.rpm
```

Example:

```
zypper install velostrata-prep-1.8-12.suse.x86_64.rpm
```

NOTE: No reboot is required after the Velostrata package is installed.

NOTE: If the installation is unsuccessful or if there are any warnings during the installation, ensure that you address them prior to the run-in-cloud operation.

How-to: Ubuntu 14/16/18 Prep for Run in GCP/AWS/Azure

Overview

An Ubuntu 14/16/18 virtual machine that is built and maintained on VMware platform will require certain adaptation done in order to be migrated using Velostrata.

Installation Steps

1. Login to the Ubuntu virtual machine with with sudo privileged access.
2. Install the **velostrata-prep** package (download from: <http://tiny.cc/velos-v3-ubuntu>)

```
sudo dpkg -i velostrata-prep-VERSION.deb
```

Example:

```
sudo dpkg -i velostrata-prep-1.8-12.deb
```

3. Install all required/missing pre-requisites for the velostrata-prep package.

```
sudo apt-get install -f -y
```

NOTE: No reboot is required after the Velostrata package is installed.

NOTE: If the installation is unsuccessful or if there are any warnings during the installation, ensure that you address them prior to the run-in-cloud operation.

Light Transformation Scripts

Customization Scripts Overview

When a VM is migrated to the cloud, various guest-level adaptations may need to be made for the VM to operate properly. Some required adaptations can be as a result of cloud environment constraints (for example, a VM will not be able to boot properly without them). These adaptations are handled by Velostrata out of the box, but other generic improvements or customer-specific adaptations may be desired.

To provide flexibility for defining those actions, Velostrata includes generic code to execute scripts based on the provided conditions and order. The scripts can be either provided by Velostrata (and deployed as a part of RPM/Velostrata service) or be deployed by customers.

Our model contains two entities - conditions and actions:

- Conditions are defined as “VM is started in cloud running with Velostrata” or “Detached VM is started in cloud”.
- Actions are the scripts that are executed when the condition holds.

Platform and Environment Detection

The framework detects the following environments:

- On-prem (VMware)
- Cloud (GCP + Velostrata, AWS + Velostrata, Azure + Velostrata)
- Detached (GCP Native, AWS native, Azure native)

Windows

With Windows, similar to Linux, some OS adaptation scripts are provided by Velostrata as default; additional ones can be added by users.

User scripts are placed here: "c:\Program Files\Velostrata\UserScripts"

The registry is updated to run the scripts ("UserTasks") on startup depending on the environment the VM is running at, referred to as MachineState. The three options are:

- **Origin** on premises environment
- **Velostrata** - the scripts will run when the VM is running in cached mode
- **Detach** - the scripts will run after the detach operation

The tasks are executed sequentially in alphabetic order. If the order of the tasks matter, it is recommended to use numerical prefixes to task names, e.g. "10_ResetWMI" and "20_ConfigKMS".

When writing the user script, absolute paths should be used as the script is copied to the UserScripts folder, which can cause relative paths to break.

In order for the tasks to be properly configured, scripts should be placed in the appropriate folder and the registry should be updated. The following section describes how this can be easily done using an assistance script. Note that only PowerShell scripts can be used for this purpose.

Powershell Assistance Script

Velostrata provides a PowerShell module that enables easy installation of a user script on a relevant VM. The script validates user input to prevent inconsistent states, copies the user script to the **UserScripts** directory, and creates its tree if it's missing. It also creates the relevant registry keys and their trees, and fills in the appropriate values.

Module name: **VelostrataUserScripts.psm1**

Available commands are **Install-VelosUserScript** and **Remove-VelosUserScript**.

How to use the assistance script:

1. Download the module from Velostrata S3 repository:

<https://storage.googleapis.com/velostrata-release/V3.5/20182/VelostrataUserScripts.zip>

2. Import the module (make sure to use relevant path):

```
Import-Module .\VelostrataUserScripts.psm1 -force
```

3. Run the assistance script per each OS adaptation script/task you wish to configure.

Example:

```
Install-VelosUserScript -FilePath .\resetWMI.ps1 -TaskName "10_ResetWMI"
```

-MachineState Detach -TaskType RunAlways -Platform Aws

Where:

- *FilePath*: The file name. Note that files run from the path of the user-scripts folder.
- *TaskName*: A unique name to be provided by the user. See note about sequencing above.
- *MachineState*: One of the following three options:
 - **Origin** - on-premises environment.
 - **Velostrata** - the scripts will run when the VM is running in cache mode.
 - **Detach** - the scripts will run after the detach operation.
- *TaskType*: one of two options:
 - **RunOnce** - This means the task will run once on the next boot and is then deleted,
 - **RunAlways** - The task will run on every boot.
- *Platform*: represents the environment in which the VM is running. May be either:
 - *Aws*
 - *Azure*
 - *All*

Note that the **Platform** parameter is optional and defaults to **All**.

4. The script removal command validates that a task exists and then deletes it from the registry, and optionally also for the scripts directory.

Usage:

Remove-VelosUserScript -TaskName "ResetWMI" -MachineState Detach -DeleteScriptFile

Where:

TaskName - should be similar to the one provided during scriptInstall

DeleteScriptFile an optional parameter

Examples:

Install-VelosUserScript -FilePath .\KMS\Config-Kms_AWS.ps1 -TaskName "10_configKMS"
-MachineState Velostrata -TaskType RunAlways

Remove-VelosUserScript -TaskName "10_configKMS" -MachineState Velostrata -DeleteScriptFile

Linux

Customization Script Modules and Execution Overview

Some Linux OS adaptation scripts are provided by Velostrata as default, as part of the Velostrata RPM installation. Rules for the Velostrata scripts are located here:

`/opt/velostrata/actions/<PHASE>.rules`

Additionally, a system admin can define custom scripts. The rules for these scripts would be located here:

`/etc/velostrata/actions/<PHASE>.rules`

Note: We will focus in this section on custom scripts, but the mechanism for Velostrata scripts is the same. Do not change the Velostrata scripts located in the `/opt/...` folder.

<PHASE> can be one of the following values and reflects the project phase of the VM:

- **origin** – the scripts will run when the VM is on-prem
- **velos** – the scripts will run when the VM is running in “cache on demand” mode
- **detach** – the scripts will run after the detach operation

Notes:

- The scripts are executed by the `velostrata.init` service, which is triggered on every boot. If you wish to avoid running the scripts multiple times, the script should manage this option.
- Linux is case-sensitive. Make sure to use lower-case for PHASE definitions

Rules Definitions

The actions that are run by the service are defined using a set of rules. The framework goes over the rules in a defined order and executes the rule based on the parameters provided.

Rule parameters:

- **NAME:** Unique rule name.
- **PLATFORM:** Cloud or platform to run rule on (aws, azure, any).
- **TEST:** Simple setting to test for a file's existence. If a path specified, the rule is only executed if the file/directory path exists. This could be leveraged to check if the script was already ran (i.e. by writing a file to signal that).
- **ACTION:** Bash script to run or an inline command.
- **REQUIRES:** optional field for required services for rule to run (currently, only "rc.local" is supported).

Example Rules:

adjust network settings

NAME="**fix-network-config**", PLATFORM="**any**", TEST="", ACTION="/usr/sbin/velostrata-fix-network-config"

#finetune machine to work optimally in Azure

NAME=" **Azure_tweaks**", PLATFORM="**azure**", TEST="", ACTION="/usr/sbin/velostrata-azure-tweaks"

Environment Setting

Multiple IP Support in GCP Cloud

In order to preserve multi-IP configuration when migrating to GCP, you can configure an additional Alias IP Range per instance in GCP. Velostrata adds all the IPs in the range to the instance NIC.

This feature is only supported after the VM is detached.

Velostrata supports ranges of up to 32 addresses/27 CIDR. GCP currently only supports a single CIDR mask, enabling you to specify one of the following:

- x.x.x.x/32 - single IP address
- x.x.x.x/31 - 2 addresses
- x.x.x.x/30 - 4 addresses
- x.x.x.x/29 - 8 addresses
- x.x.x.x/28 - 16 addresses
- x.x.x.x/27 - 32 addresses

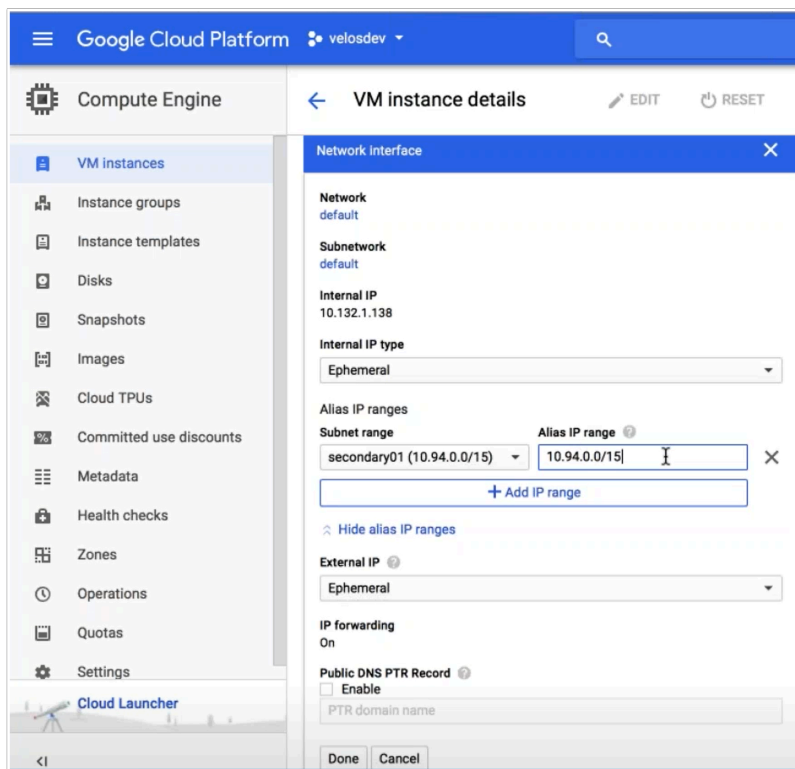
Note: This only applies to Linux machines.

You can either specify up to 32 IP addresses or specify just a CIDR mask up to /27 (32 IP address) to have a range of IPs assigned automatically. The range must belong to the specified subnet's range. The range you choose must not already be in use, even in part, by any other resource on the VPC network.

1. To enable multiple IP support, set one of the following:
 - In the project metadata, set the **apply-alias-ip-ranges** key to **true**, or
 - In the instance metadata set the **apply-alias-ip-ranges** key to **true**.

Note: The instance metadata has priority over the project metadata.

2. Go to the **VM instance** page in the Google Cloud Platform Console.
3. Select the required instance.
4. In the **VM instance details** page, click **Edit**.
5. Scroll down to the **Network interfaces** section.
6. Click **Show alias IP ranges**.
7. Enter a **Subnet range**.
8. Enter an **Alias IP range** in CIDR notation. This range must be an unused subrange of the primary range.



8. Click **Done**.

External DNS in GCP Cloud

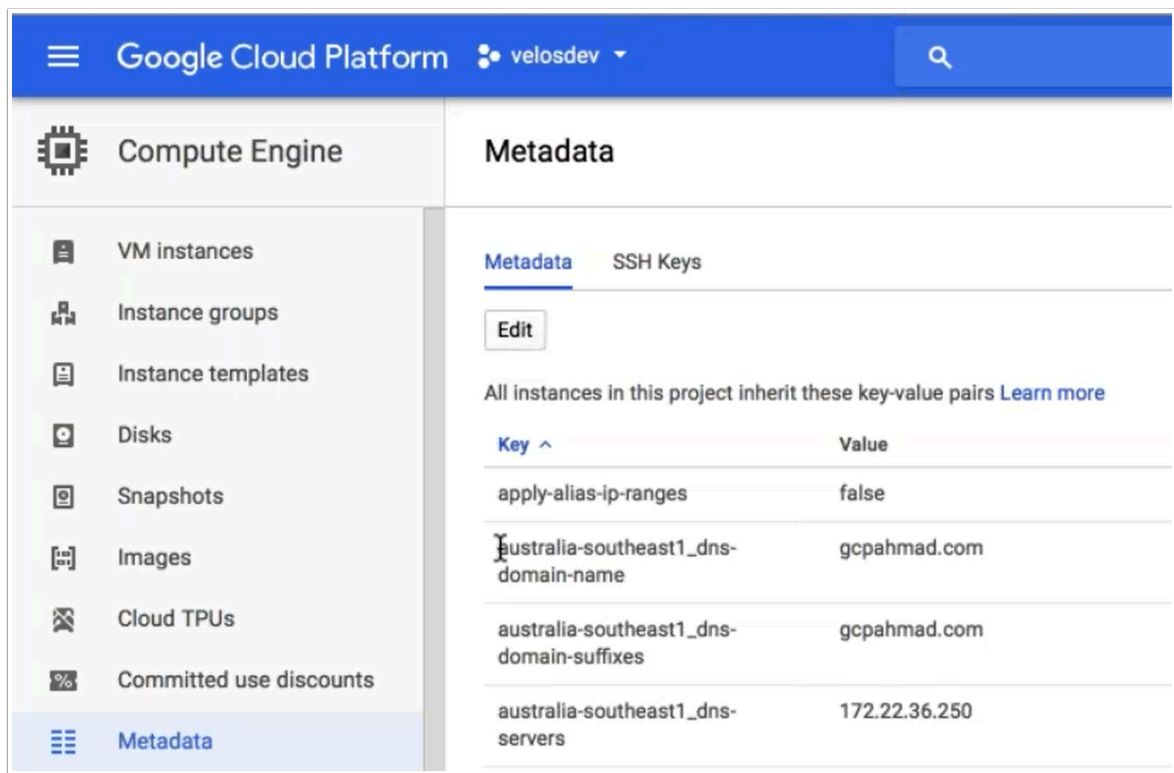
GCP VPC networks have an internal DNS service but do not support configuring an external DNS for an instance. Enterprise customers typically use various DNS servers within the organization and therefore require a mechanism to configure DNS server settings for migrated machines.

Velostrata provides a way to set and control the DNS settings of migrated machines in a persistent manner. You can configure the DNS settings in the GCP project (and region) as GCP Project Metadata. This will then apply to all instance migrated to GCP by Velostrata.

When empty DNS metadata is provided, for example, **default-dns-servers = ""**, the DNS configuration will be overwritten with values from DHCP.

To configure the external DNS in GCP:

1. In the Google Cloud Platform Console, go to the **Metadata** page for your project.
2. Under **Metadata**, click **Edit**.



3. Modify the project-wide keys.
 - **{region_name}_dns-domain-name: mydomain.com** - represents the connection-specific DNS suffix in Windows clients.
 - **{region_name}_dns-servers: {comma separated list of IPs}** - represents the list of DNS servers.

- **{region_name}_dns-domain-suffixes: mydomain.com, myseconddomain.com** - represents the list of DNS suffixes to add to Windows and Linux machines.

The system also supports the following key:values for a default configuration to machines without explicit region configuration:

- **default_dns-domain-name: mydomain.com**
- **default_dns-servers: {comma separated list of IPs}**
- **default_dns-domain-suffixes: mydomain.com, myseconddomain.com**

Note: A region setting takes priority over a default setting.

4. When you are done, click **Save** at the bottom of the page.

The settings are applied as followed:

For Windows clients, the key:values are applied to all NICs as follows:

- **dns-domain-name:** Replaces the “DNS suffix for this connection” setting per NIC.
- **dns-servers:** Replaces the list of DNS servers per NIC.
- **dns-domain-suffixes:** Replaces the list of DNS suffixes per NIC.

For Linux clients, the key:values are applied to all NICs as follows:

- **dns-servers:** Prepends the list of DNS servers in the **resolv.conf** file.
- **dns-domain-suffixes:** Prepends the list of DNS suffixes in the **resolv.conf** file.