Introduction to Cloud Server Snapshots

Description

Provides an overview of the Cloud Server Snapshot feature available in some MCP 2.0 locations. To identify if this feature is currently available in a particular MCP 2.0 location, see How do I Identify Hardware Specifications and Capabilities Available in a Data Center Location.

Overview

Cloud Server Snapshots provides a hypervisor-enabled backup solution that shares many of the characteristics of traditional VM snapshots. Cloud Server Snapshots provides the user the benefits of a backup solution which can be enabled without loading any software agents into a Cloud Server, and at the same time provides the ability to instantly restore to a known-good previous state of a Cloud Server in circumstances such as the need to recover quickly from a failed change. Cloud Server Snapshots is a feature that can be enabled for a given Cloud Server. Once the feature is enabled, the system takes periodic "snapshots" of the Cloud Server. Each snapshot is a copy of a Cloud Server's hardware and storage state at a *given point in time*. Cloud Server Snapshots include the current state of all components of the Cloud Server, including server hardware configuration elements (Number of CPU, CPU Speed, RAM, Network Adapters, Storage Controllers, etc.) as well as the state of all local storage disks.

There are two types of Snapshots:

1. **System Generated Snapshot -** The system takes a daily "system-generated" snapshot periodically during a pre-determined window. The pre-determined window is chosen by the user when the Cloud Server Snapshot is enabled. When provisioning the service, users will choose an available window from a pool of windows made available on a first-come / first-served basis. Users cannot delete the system generated snapshots. The retention of System Generated Snapshots is based on the Snapshot Plan. See the Cloud Server Snapshot Plans section below for more details
2. **Manual Snapshots (User Initiated) -** Manual snapshots allow users to take a snapshot of a Cloud Server outside the time of their weekly window. For example, a user preparing for a maintenance event on a Cloud Server might take a manual snapshot prior to the maintenance to have a copy of the server state. Users can request a manual snapshot at any time but can only have a single snapshot in progress at any one time for each Cloud Server. Unlike system-generated Snapshots, manual Snapshots can be deleted. Manual Snapshots are automatically deleted by the system after 14 days. See How to Take a Manual Cloud Server Snapshot and How to View and Manage Snapshots for a Cloud Server

Once a Snapshot is created, the snapshot is stored for a given period of time (which varies depending on the snapshot "service plan" and the type of snapshot - see **Cloud Server Snapshot Plans** section below). So long as the Snapshot is stored, users can create new Cloud Server(s) from those Cloud Server Snapshots. The new server or servers have the same hardware configuration and storage state as the historical snapshot, giving users the ability to "roll back" to a previous state, for example back to a time *before* a failure or fault occurred.

Cloud Server Snapshots are useful for a variety of use cases such as:

- Creating a snapshot for "rollback" or protection prior to initiating maintenance or making major changes to a server.
- Recovering to a historical state after corruption of a server
- Review of historical states to recover lost files or to identify server state

These are simply a subset of potential ways the system can be used. There are too many potential use cases and variables to provide "best practices" around all the options, but it is helpful to provide a sample use case to get a better feel of how the Cloud Snapshot functions tie together.

- User initiates a Manual Snapshot per How to Take a Manual Cloud Server Snapshot
- User can identify Snapshot is in progress as described in How to Take a Manual Cloud Server Snapshot

- User ensures Manual Snapshot <u>successfully completed</u> by checking the snapshot list per How to View and Manage Snapshots for a Cloud Server
    - This step is important since it is possible for a Manual Snapshot to fail!
- User performs the upgrade or change to the server.
- User tests new application and determines something is not working correctly
- User creates a new Snapshot Preview Server from the Manual Snapshot created prior to the event per How to Create a Snapshot Preview Server from a Local Snapshot
- User may then choose to:
    - Access the newly created server via Console and identify the information/configurations from the server prior to the event
    - Copy information or configurations from the newly created Snapshot Preview server back to the server which was modified in order to correct information.
        - Note this may involve re-IP'ing and reconnecting NICs such that the servers can communicate without an IP conflict
- Alternately, the user may choose to power down or disconnect the NICs on the original server and begin using the Snapshot Preview server to replace the original, since it represents the same state as prior to the change. In this case:
    - User would want to migrate the Snapshot Preview server to Normal per How to Migrate a "Snapshot Preview" Server to a Normal Cloud Server.
    - User may want to re-enable add-on services on the new server.
    - User may want to maintain the "original" server for troubleshooting to determine what may have caused the upgrade to fail.
- For additional redundancy, you can enable Snapshot Replication and the system will replicate System Snapshots to an available secondary location within the same Geographic Location.
    - In the event of a Data Center failure, you can restore Snapshots to the secondary location from the Replicated Snapshot

Cloud Server Snapshot Plans

We currently offer three Cloud Server Snapshot plans: **One Month**, **Three Month**, and **Twelve Month**. All three Snapshot plans offer the same Cloud Server Snapshot features:

- **Servers will have a Daily "System" snapshot taken during a user-specified UTC window**
    - Users can choose from a pool of available UTC windows, broken into 12 two-hour times during the day.
    - Note that some daily UTC windows may be identified as "OVERLAPS_WITH_MAINTENANCE". This means that time overlaps with one of our Operational maintenance windows on a particular day of the week. The System does not block a snapshot from occurring during this timeframe, however, if Operations is performing hypervisor or snapshot maintenance in the location during the selected time, the System snapshot may be unsuccessful on that particular day. Such failed system snapshots are visible as described in How to View and Manage Snapshots for a Cloud Server.
        - In order for the System to determine whether a System snapshot failed:
            - CloudControl checks once an hour for the list of <u>all</u> snapshots, including System ones
            - If CloudControl does not identify a System snapshot within 12 hours of the scheduled window, it inserts a failed record with a 31-day expiry time
            - However, we have seen some cases where the underlying infrastructure takes more than 12 hours to complete the scheduled snapshot, in that case, the system will show <u>both</u> the failed record and the successful one with the same Snapshot start time.
- **Users can take Manual Snapshots "on-demand" in addition to scheduled System snapshots**
    - For details, see the ***Manual Snapshots*** section below
- **Users can choose to have their System Snapshots replicated to another location (where available)**
    - For details, see the ***Snapshot Replication*** section below
- **Users can define local OS-level scripts that run before and after the vSphere snapshot used during the snapshot process**

    - For details, see the ***Pre and Post Snapshot Scripts Feature*** section below.
- **Users can create a *new* Cloud Server from a Snapshot at any time**
    - For details, see the ***Using Cloud Server Snapshots to Create a New Cloud Server*** section below
- **Users can restore files or directories from a Local Snapshot directly onto the protected server**
    - For details, see the ***Performing a File or Directory Restore from a Cloud Server Snapshot*** section below

The difference between the plans relates to the retention period for these system snapshots. Each plan offers a different retention period:

Id	Plan Name	System Snapshot Retention Period	Retention Notes
ONE_MONTH	One Month: 7d-4w	Daily - 7 days Weekly - 31 Days	- Every 7 Days, one daily Snapshot will be "promoted" to a weekly Snapshot with a 31 day retention period.
THREE_MONTH	Three Month: 14d-12w	Daily - 14 Days Weekly - 90 Days	- Every 7 Days, one daily Snapshot will be "promoted" to a weekly Snapshot with a 90 day retention period.
TWELVE_MONTH	Twelve Month: 31d-12w-12m	Daily - 31 Days Weekly - 90 Days Monthly - 365 days	- Every 7 days, one daily snapshot will be "promoted" to a weekly Snapshot with a 90 Day retention Period, - Every 30 days, one weekly snapshot will be "promoted" to a monthly Snapshot with 365 Day retention period.

⚠

⚠️ **Details on Previously Available Plans**

Prior to October 24, 2019, the system offered **Essentials** and **Advanced** Cloud Server Snapshot plans. For details on these plans and the end-of-sale details, see October 2019 Changes to Cloud Server Snapshot Plans.

Enabling the Cloud Server Snapshot feature

The Cloud Server Snapshot feature is not available in all locations. To identify if it is available in a given location, and to see system constraints around the service, see How do I Identify Hardware Specifications and Capabilities Available in a Data Center Location.

Where available, users can enable the service as described in How to Enable Cloud Server Snapshots on a Server. A few notes on this:

1. All Snapshot Window times are listed in UTC, so the local time may change with daylight savings time, where applicable. For example, if the Server is located in the NA9 location which follows US-Eastern Time Zone and you pick the 02:00 UTC window, the Snapshot may be taken at either 9:00 PM or 10:00 PM local time depending on whether the location is currently following daylight savings time. The UI will show this conversion based on the current daylight savings time status.
2. There is a maximum number of total servers that can be assigned to each window in a given location. When all of these "slots" are used, the system will not allow additional servers to choose that window. Slots may become available again in the future if a Cloud Server using the slot disables the feature or if the infrastructure is expanded to provide additional slots. The UI will display the current number of available slots as described in How to Enable Cloud Server Snapshots on a Server in order to allow you to ensure there are enough slots to support multiple servers for which you want to share the same window.
3. The initial System Generated snapshot taken after a Cloud Server is enabled can be a long-running process taking hours (especially if the amount of local storage is large). This is true only of the initial System snapshot - after the initial System snapshot is taken, any future Manual or System snapshots are much quicker as the system only needs to identify changes since the previous snapshot. This means that even if you choose to **Create Initial Snapshot immediately** as described in How to Enable Cloud Server Snapshots on a Server, this initial Manual Snapshot will also be a long-running process and you will be prevented from performing a number of Server actions while a Manual Snapshot is in progress, as detailed in the **Restrictions While Snapshots are Taking Place** section below.
4. There is a limitation on the maximum amount of storage that can be attached to a Cloud Server in order to enable the Cloud Server Snapshot feature. For more information see **Maximum Total Snapshot Storage** on How do I Identify Hardware Specifications and Capabilities Available in a Data Center Location

🚫 **Some Server Configurations Not Supported or Are Not Fully Restored**

Some Cloud Server hardware configurations are incompatible with the Cloud Server Snapshot Service. For example, Cloud Servers with ISO files attached to CD-ROM cannot be enabled for Snapshots. Similarly, although Snapshot enablement of servers with "empty" SATA Controllers without ISO or Local Drives is allowed, users should be aware that when creating a "Snapshot Preview" server as described in How to Create a Snapshot Preview Server from a Local Snapshot, the SATA controller will not appear as part of the Snapshot Preview server.

For complete details on all unusual configurations, see preconditions in How to Enable Cloud Server Snapshots on a Server

Users can switch between Snapshot plans. For instructions on switching plans, see How to View and Manage Snapshots for a Cloud Server.

Snapshot Replication Feature

Snapshot Replication allows you to replicate System Snapshots to a secondary site in the same Geographic Region. Only System-Generated Snapshots can be replicated (not Manual Snapshots). Replication is not available in all Snapshot locations. To identify if it is available and to which locations replications can be made, see How do I Identify Hardware Specifications and Capabilities Available in a Data Center Location.

Once Snapshot Replication has been enabled on a Cloud Server, It can take anywhere from 30 minutes to several hours for the Snapshots to be replicated to the secondary location. Replicated system snapshots are retained for the same retention time as Primary (Source) snapshots. In the secondary location, you will incur "Replicated Snapshot Hours" based on your Snapshot plan once replication is enabled.

Snapshots are replicated asynchronously to the replicated location. Once the snapshot is replicated, you will be able to create Snapshot Preview servers in the secondary location using the Replicated Snapshots. However, there are some differences in the process when creating a Snapshot Preview Server from a Replicated Snapshot:

1. You will need to specify a unique VLAN to which to connect each NIC on the Server. This means that the secondary location must have the same number of available VLANs as the Network Domain of the Source server.
2. If a Disk speed is not available in the replicated location, the Disk Speed will automatically be changed to the *default* Disk Speed for that Data Center Location, which in currently always the Standard Disk Speed.

For details, see:

- How to Manage Snapshot Replication on a Cloud Server
- How to Create a Snapshot Preview Server from a Replicated Snapshot

Pre and Post Snapshot Scripts Feature

The Pre and Post Snapshots feature can help ensure your snapshots can be used to create a usable server. At a technical level, taking a Cloud Server Snapshot is a two-step process:

1. The System first uses VMWare's native **Virtual Machine Snapshot** capability to take a local snapshot of the server. This process usually lasts a few seconds.
2. The system then offloads a "copy" of that Virtual Machine Snapshot to the external snapshot infrastructure where it is stored. This is a longer-running process, especially on the initial Snapshot.

Cloud Server Snapshots can be created either while a server is running or in a stopped state. However, the Virtual Machine Snapshot performed in step #1 is taken with the Quiesce and Memory settings set to OFF, so there are no actions taken within the Guest OS to prepare for the Virtual Machine Snapshot if the server is running. To address this limitation, the system supports the ability to configure the system to run a local script on the Cloud Server prior to taking the Virtual Machine Snapshot and to run another local script and immediately after the Virtual Machine Snapshot has been taken. Users can opt to run a Pre-Snapshot Script, a Post-Snapshot script, or both a Pre and Post Snapshot script.

Once this feature is enabled, the system will attempt to run these scripts on all Snapshots (Manual and System) for that Cloud Server. Pre and/or Post Snapshot scripts can be enabled when a Cloud Server is initially enabled for Snapshots or added on to an existing Snapshot-enabled Cloud Server. Users are required to provide Server credentials, file/path name for the script to be run, along with additional parameters when enabling this feature. Note there are limitations on supported OS and VMware Tools must be installed and running in order to use the feature. For details, see:

- [How to Set Pre and Post Snapshot Scripts on a Cloud Server](#)

Manual Snapshot Feature

The Manual Snapshot function allows users to take a snapshot at any time outside the time of their weekly window as described in [How to Take a Manual Cloud Server Snapshot](#).

- The maximum number of Manual snapshots that can be stored on can be identified as described in [How do I Identify Hardware Specifications and Capabilities Available in a Data Center Location](#). Users at the limit can delete a manual snapshot at any time in order to have the ability to generate a new Manual Snapshot
  - *NOTE: As of October 8, 2019, the limit is 5 Manual Snapshots per server in all locations.*
- Manual Snapshots are automatically deleted by the system after the Manual Snapshot Retention period is listed in the Data Center Specifications section of the Data Center Dashboard. See [How do I Identify Hardware Specifications and Capabilities Available in a Data Center Location](#).
  - *NOTE: As of October 8, 2019, the retention period is 14 days in all locations.*

Cloud Server System Snapshot Archiving

> (i) **System Snapshot Archival In Process of Being Rolled Out**
>
> We are in the process of rolling out the archival of system snapshots as described below. It is expected that most locations with Cloud Server Snapshots will eventually have archiving enabled. Announcements will be made on the status page before archiving is enabled, but users should be aware that even if a location currently does not show archiving is in place, it may be added later.

In data centers where Snapshot Archiving has been enabled after a System Snapshot has been successfully taken it will be moved from local Snapshot storage infrastructure to Archived Storage infrastructure after a certain number of days. Manual Snapshots are not archived. The time between the successful completion of the System Snapshot and when it is moved to Archived Storage can vary by Data Center. You can identify whether snapshot archival is currently being used and the specific archival policy by looking at the Data Center Specifications section of the Data Center Dashboard as described in [How do I Identify Hardware Specifications and Capabilities Available in a Data Center Location](#). Specifically, see the sections "**Snapshot Archive Enabled**" (True or False) and "**Snapshot Retention Before Archive (Days)**". If replication is enabled in a location, the replication policy applies to all System Snapshots stored in that location - including if that location is used as a Replication Target location by a server in another data center location.

You can identify if a System Snapshot is currently archived when viewing the list of Snapshots. The Snapshot tab of the Server dashboard will display the Archive Status of each Snapshot, indicating whether it is archived, available locally or is in the process of being downloaded from the archive.

For more details, see Navigating the Server Dashboard

Creating a Snapshot Preview Server from a Snapshot that currently resides on Archived Storage will take significantly longer than creating one from a Snapshot that is not archived as the process requires an extra step where the Snapshot is first copied ("rehydrated") from the Archival Storage infrastructure to local Snapshot storage infrastructure before a Snapshot Preview Server can be created. The timeframe to rehydrate a Snapshot depends on a number of factors, including the size of the snapshot, connectivity to the archival storage, and overall load on the Snapshot infrastructure. Be sure to allow for this extra time if you plan to create a Snapshot Preview Server from an archived Snapshot. Once successfully rehydrated from the archival storage, a Snapshot will reside on the local storage for up to 24 hours. It is important to note that only one archived Snapshot can be brought back to local storage (re-hydrated) at a time for a given Cloud Server.

File or Directory Restore operations do not require the rehydration step but may also take longer if restoring from an archived System Snapshot. See How to Restore a File or Directory from a Cloud Server Snapshot to the Cloud Server.

Snapshot Long-Term Snapshot Retention Feature

Many organizations have a need to retain backups for an extended period of time to meet compliance requirements, in some cases for up to 7 years. Snapshot Long-Term Retention is an add-on feature of Cloud Server Snapshot Service that allows users to specify that they want to keep a System Snapshot for a longer period than what is allowed under the Snapshot Service Plans (i.e. longer than 1 year). This feature provides a solution for Cloud Server Snapshots which is not tied to proprietary vendor formats. Long-Term Retention Images are stored using standard vSphere datastores, meaning that if the underlying technology of Cloud Server Snapshots is changed, Long-term Retention Images will not be "stuck" in a legacy vendor format.

For more information on Long-Term Snapshot Replication, see Introduction to Cloud Server Snapshot Long-Term Retention Images

Application-Specific Considerations when Configuring Snapshot Service

Since there is no guarantee write state of the server at the time of snapshot, some applications such as databases and Active Directory servers will need additional configuration in order to ensure a restorable state based on the snapshot. Here are overview of the approach to address common scenarios:

- Using Windows Server Backup to Protect Active Directory (AD) with the Cloud Server Snapshot Feature
- Using Volume Shadow Copy Service (VSS) to Protect SQL Server with the Cloud Server Snapshot Feature
- Using FLUSH TABLES WITH READ LOCK to Protect MySQL databases with the Cloud Server Snapshots Feature

Viewing and Understanding Cloud Server Snapshots

Once enabled, you can view the Cloud Server Snapshots associated with a server as described in How to View and Manage Snapshots for a Cloud Server. The View Snapshots function allows you to view the detailed configuration of the Cloud Server at the time the snapshot was taken, as well as Snapshots that have been replicated to a secondary location.

Cloud Server Snapshot Consistency Levels

> ⊘ **VMWare Tools Required for Some Consistency Levels**
>
> Note that the "consistency level" provided by the Cloud Server Snapshot service varies depending on:
>
> - Whether VMware Tools is installed and Running
> - Operating System capabilities

When a Cloud Server Snapshot is taken, it is possible that the system, at that moment, is making changes to files on the disk at the time of the snapshot. It's also possible that the application is in the middle of a thread or transaction where it is making changes across multiple files or transactions. To avoid problems when creating a Snapshot Preview server from a snapshot, you want some level of "consistency" in the snapshot - avoiding complications where the file state is "incomplete".

The Cloud Snapshot Service supports multiple levels of consistency depending on the server and application configuration:

- **INCONSISTENT** - Inconsistent means the disk state is not guaranteed to be consistent on any level. This level occurs when neither VMware Tools nor Open VM Tools is running on the Cloud Server at the time of the snapshot. This includes times when the server is in a stopped state since Tools isn't running. The system requires VMware Tools or Open VM Tools to be running in order to have visibility into the Operating System, which is needed to identify or ensure any information about consistency.
- **CRASH_CONSISTENT** - Crash Consistent means the system was able to confirm that all the data captured on the local disks is representative of the state of the storage as of the **start time** of the snapshot. This means the OS will boot but application data cannot be guaranteed. This level can be provided when Open VM Tools is running on the Cloud Server at the time of the snapshot or the server is running an out-of-date version of VMware Tools. This is currently the highest level of guaranteed consistency supported with servers running Open VM Tools.
- **FILE_SYSTEM_CONSISTENT** - This indicates the file system state is consistent as of the **start time** of the snapshot, meaning that any writes to specific files are complete. The level can be provided when VMware Tools is up-to-date and the OS does not support application consistency.
- **APP_CONSISTENT** - This value is returned for some LINUX OS variants but effectively means the same thing as FILE_SYSTEM_CONSISTENT
- **VSS_CONSISTENT** *(NOT YET AVAILABLE)* - With a VSS_CONSISTENT snapshot, you can ensure some level of application consistency for applications taking advantage of Microsoft's **Volume Shadow Copy Service** as the service ensures the application is in a consistent state when the snapshot is taken. Note that VSS_CONSISTENT is not a guarantee of full application consistency. It merely indicates the snapshot was consistent with the Microsoft's Volume Shadow Copy Service
  - *Support for VSS Consistent Snapshots is not yet available* but is expected to be added in the future. It will require a special software agent that interfaces with the Cloud Server Snapshot service.

Snapshot Index State

When a Snapshot is initiated (whether Manual or System), the Snapshot will be indexed based on the state of the snapshot. In order for a snapshot to be used for a file or directory restore operation, the Index State <u>must</u> be Valid. There are 3 possible index states:

1. **Valid** – This indicates that indexing has completed successfully, and the Snapshot <u>can</u> be used for File or Directory restores
   - **Note**: If the Index State is Valid, the Index State icon will be black ≡. Hovering your mouse over the icon will indicate that the state is Valid.
2. **Incomplete** – This indicates that the indexing has not yet completed. You cannot use a Snapshot in this state for a File or Directory restore at this time.
   - **Note:** The system automatically sets the index state of Snapshots to this value during the Snapshot process. It may take some time to update, depending on the size and complexity of the file and directory structure
   - **Note**: If the Index State is Incomplete, the Index State icon will be gray ≡. Hovering your mouse over the icon will indicate whether the state is Incomplete or Invalid.
3. **Invalid** – Snapshots cannot be used for file or directory restores. This could be because of any of the following reasons:
   - Indexing has failed
   - The Operating System could be unsupported
   - The file system on the Operating System could be unsupported
     - **Note**: If the Index State is Invalid, the Index State icon will be red ≡. Hovering your mouse over the icon will indicate that the state is Invalid.

The index state of a Snapshot can be viewed in the Snapshot tab of the Server Dashboard. See Navigating the Server Dashboard

Using Cloud Server Snapshots to Create a New Cloud Server

The purpose of having Cloud Server Snapshots is to either get access to the data from a historical snapshot or to create a replica of the server based on a historical snapshot. This section explains how to create a replica of the server. You can also restore a directory onto the protected server as described in the next section **Performing a File or Directory Restore from a Cloud Server Snapshot**.

Creating a new Cloud Server from a Snapshot involves two phases: **Creating a Snapshot Preview Server** and **Migration of a Snapshot Preview Server to Production Disk Speeds.** Details on each phase are described below.

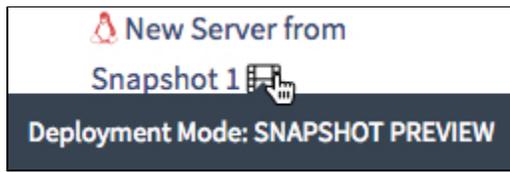## Creating a Snapshot Preview Server

The first step in the process is to create a "Snapshot Preview" server. The process differs slightly depending on whether you are creating a server from a "local" snapshot in the same data center as the original server or whether you are creating it from a "replicated" snapshot in a different data center. When using a local snapshot, the Snapshot Preview server is created on the same NIC VLANs as the original server. When using a replicated Snapshot, you must define the VLANs for each NIC.

For complete details, see:

- How to Create a Snapshot Preview Server from a Local Snapshot
- How to Create a Snapshot Preview Server from a Replicated Snapshot

In either case, this function allows you to bring up a new server that matches the state of the server represented by the **start time** of a successful snapshot. The goal is to allow you to quickly assess the snapshot to ensure it contains the data and server state you are looking for as well as to gain quick access to data and potentially replace the original server in production using this newly created server. Note that this process will take longer if Archive is enabled for the Location and the Snapshot chosen resides are Archive Storage (see **Snapshot Archiving** section above)

A "Snapshot Preview" server has the same virtual CPU and RAM performance as the original server and runs on a physical ESXi host in the production infrastructure. However, the "local storage" (i.e. disks) for a Snapshot Preview server is not running on the production storage infrastructure. Instead, it is

running on disks presented by the snapshot service itself. Snapshot Preview Servers are indicated by the ⬚ Snapshot Preview Server icon. You can hover your mouse over the icon to see that the Server is in Snapshot Preview mode:

Performance and Restrictions of Snapshot Preview Servers

While in Snapshot Preview mode, the server has some performance limitations and some other restrictions:

1. Since the disk is being presented by the snapshot infrastructure and mounted to the ESX hypervisor via NFS, the server will not achieve the I/O performance indicated associated with the "disk speed" of the local storage. To achieve normal performance, you need to initiate a "migration" to the normal storage infrastructure as described in the next step.
2. The "Snapshot Preview" server is tied to a specific physical ESXi host. If that physical ESXi host fails, the Snapshot Preview server state will be lost and will not immediately restart on another host as described in What Happens When the Physical Server Hosting my Cloud Server Crashes.
3. The following server actions are prohibited while the Cloud Server is in Snapshot Preview mode:
    a. Modifications to Storage Controllers or Disks, including:
        i. Add/Remove/Expand Local Disk
        ii. Add/Remove SCSI Controller
        iii. Change Disk Speed
        iv. Change the IOPS value on a variable IOPS disk speed disk
        v. Remove ISO/FLP
    b. Create Server Anti-Affinity Rule using Server
    c. Enabling other CloudControl Services such as Cloud Server Snapshots, Monitoring, or Backup
        i. This also includes a prohibition on creating a Security Group or DRS Consistency Group with a server while it is in "Snapshot Preview" state

Given those limitations (particularly the first two issues), the recommended best practice is to verify that the server represents a snapshot state you are looking for, make any necessary changes to it, and then to migrate the Snapshot Preview server to NORMAL as soon as possible. **Users must initiate migration of "Snapshot Preview" Servers to at the Production Disk Speeds as described in the next section within two hours after creation.** After two hours, the system will initiate the migration automatically**.**

Potential Configuration Issues with Snapshot Preview Servers

There are some minor caveats and potential Guest OS configuration issues with Snapshot Preview Server:

- When creating a Snapshot Preview from a Local Snapshot, the Snapshot Preview server is provisioned to the same VLANs as the original server. Therefore, it likely has many (if not all) of the same IP addresses as the original server. That means there is a high likelihood of IP conflict if the original server is running. **We recommend creating Snapshot Preview Servers with the NICs in a disconnected state and connecting them only after you are sure it will not cause a problem**.
    - For more details on "connected" and "disconnected" NICs, see Introduction to Cloud Server NICs in MCP 2.0
    - The system will prevent you from creating a Snapshot Preview server if any of the IP addresses from the time of the snapshot are "exclusively reserved". You will need to unreserve the IPs in order to create a Snapshot Preview server as described in How to Unreserve an IPv4 or IPv6 Address.
- On UNIX-based Operating Systems, failing to preserve the MAC address means the resulting server will require configuration changes as described in Enabling Network Connectivity to a Snapshot Preview Server using RHEL, CentOS, or Oracle if MAC Addresses Have Changed. However, keeping the MAC Addresses has the potential to cause a MAC address conflict when both the original Server and the Snapshot Preview server are powered on with their NICs connected, so Users should be aware of this possibility and similarly use the disconnected NIC option as described above. See How to Create a Snapshot Preview Server from a Local Snapshot and Introduction to IP Addressing in MCP 2.0 for more details.
- Any CD-ROM devices attached to the original Cloud Server as of the time of the snapshot are not restored on the Snapshot Preview server.
- **Servers with disks on IDE controller will have a new boot order**. See Addressing Boot Order Issues with a Snapshot Preview Server with an IDE Disk
- If the Cloud Server was using Cloud Backup at the time of the snapshot, the backup agent will still be installed and potentially running on the Snapshot Preview server even though it's not enabled for backups. We recommend disabling the agent so as not to result in the backup agent processing backup requests.

- Although Snapshot enablement of servers with "empty" SATA Controllers without ISO or Local Drives is allowed, users should be aware that when creating a "Snapshot Preview", the SATA controller will not appear as part of the Snapshot Preview server.

Migration of a Snapshot Preview Server to Production Disk Speeds

The second step in the process migrates the server's local storage onto the production disk infrastructure. This converts the server to a "normal" Cloud Server free of any performance limitations or restrictions. This is a potentially long-running process depending on the size of the local storage, as the process is the equivalent of initiating a "disk speed" change on all of the local disks attached to the Cloud Server. During this migration, the server will continue to run in the state it was in at the time of the migration. However:

- All CloudControl server changes are prohibited during the migration (i.e. the server is in a "Pending Change" state).
  - This includes the ability to start or stop the server, so ensure you have the server in the desired state prior to migration
  - However, OS-level and application-level changes can continue to be made while in this state. The prohibition applies only to CloudControl changes to the server.
- Until migration is complete, the performance restrictions of a Snapshot Preview continue to apply:
  - Since at least some disk is being presented by the snapshot infrastructure and mounted to the ESX hypervisor via NFS, the server will not achieve the I/O performance indicated associated with the "disk speed" of the local storage until the migration is complete.
  - The "Snapshot Preview" server is still tied to a specific physical ESXi host and if that host fails, the Snapshot Preview server will be lost and will not restart on another host.
- The server continues to incur normal usage charges except local storage which continues to be reported as Standard Disk Speed under Storage Hours

Once migration is complete, the server acts as a Normal Cloud Server and there are no restrictions on usage or changes. However, remember that the new server is not enabled with services such as Cloud Server Snapshots, Monitoring, etc. so you may want to enable those services on the new server if required.

Migration from a Snapshot Preview to a "Normal" server can be done in one of two ways:

- Users can initiate the migration, see How to Migrate a "Snapshot Preview" Server to a Normal Cloud Server
- If the server has been in Snapshot Preview for more than two hours, the System will initiate the migration automatically.

⚠️ **System Will Make Three System Initiated Migration Attempts**

If the System initiated migration fails, the System will retry the migration. If the migration fails after 3 retries, the System will stop trying to migrate the Server. The Server will remain in Snapshot Preview status but will be returned to a Normal state. At this point the User can either:

- Initiate the Migration Manually, see How to Migrate a "Snapshot Preview" Server to a Normal Cloud Server or
- Delete the Snapshot Preview Server, see How to Delete a Cloud Server

---

Performing a File or Directory Restore from a Cloud Server Snapshot

Another feature of Cloud Server Snapshots is the ability for a user to specify a file or file directory from a historical snapshot and have that particular file or directory copied or "restored" back onto the Cloud Server associated with the snapshot. This ability is useful when a single file or directory needs to be restored instead of creating an entirely new Server using Snapshot Preview.

The system will restore the specified file or directory from a source location on the Snapshot to a target location on the parent Cloud Server.

There are several preconditions that must be met in order to successfully perform a File or Directory restore. For a full list of preconditions, as well as instructions on how to use this function, see How to Restore a File or Directory from a Cloud Server Snapshot to the Cloud Server

Note that you **cannot** perform a File or Directory Restore from a Replicated Snapshot.

Cloud Server Snapshots and Usage Reporting

Enabling Cloud Server Snapshots on a server will cause the server to incur a new **(Snapshot Plan) Snapshot Service Hours** where **(Snapshot Plan)** represents either the Snapshot plan was enabled for the Cloud Server. If Snapshot Replication is enabled for a Server, additional usage will appear under **(Snapshot Plan) Replicated Snapshot Hours** beginning from the time Replication was enabled on the Server. In all cases, the usage charges are based on the aggregate size of *all of the local disks* attached to the Cloud Server. The charges apply to the total size of the disks, not the amount of local storage actually used by the Operating System becausethe stored snapshot includes the exact state of all local disks (even if unformatted) and any Disks that are replicated to a secondary location.

All Snapshot Service Hours usage is incurred *immediately upon service enablement* before any snapshots are taken or stored and usage will stop when the service is disabled. Note that disabling Snapshot Replication can take anywhere from 2 to 4 hours andusage will continue to be incurred until Replication is fully disabled. The "(Snapshot Plan) Snapshot Service Hours" and "(Snapshot Plan) Snapshot Hours usage charges are in addition to the normal Economy/Standard/High-Performance usage charges for local disks that are described in Introduction to Cloud Server Local Storage ("Disks") and Disk Speeds.

When a "Snapshot Preview" Cloud Server that is newly created from a Snapshot (Local or Replicated) as described in How to Create a Snapshot Preview Server from a Local Snapshot, the server incurs all local disks as Standard Disk Speed rates ("Storage Hours") while it is in Snapshot Preview mode. Local disks incur normal disk speed usage only after the server is migrated to a "Normal" server as described in How to Migrate a "Snapshot Preview" Server to a Normal Cloud Server.

For more information on Snapshot usage elements, please refer to the Cloud Server Snapshots section of Introduction to Usage Reporting

From a reporting perspective, details of Snapshot Usage (and Replicated Snapshot usage) are contained in the Snapshot Usage report as described in How to Generate a Snapshot Usage Report

Additional Details on Cloud Server Snapshot Service

Restrictions While Snapshots are Taking Place

While snapshots are in progress, you cannot modify any existing disks on the Cloud Server. Therefore:

1. When taking a Manual Snapshot, the system will prevent you from removing disks, changing disk speeds, and expanding disks until the Manual Snapshot is finished.
2. If you take these actions while a System Snapshot is occurring:
     - Attempting to removing a disk or change a disk speed on the Server will fail
     - Attempting to expand a disk on the Server will cause the System Snapshot to fail
     - *Unfortunately, the system does not provide a real-time view into when a system snapshot is occurring, so the best practice is to avoid such actions during your system window and schedule your system window when such actions are unlikely to occur.*

Notes about Snapshot Preview Servers

- Remember a Snapshot Preview server is a completely separate Cloud Server from the original server on which the snapshot was created. Changes made on this server are not reflected on the original Cloud Server or vice-versa.
    - The new server does not have the same services associated with it, so it is not enabled for Monitoring, Backup, Cloud Server Snapshots, or any other services. These will have to be enabled on the new server once it is migrated out of Snapshot Preview as described below.
- Snapshot Preview servers incur normal usage for all usage elements, meaning they are "billable" as new servers with the one exception that all local disk is reported as Standard Disk Speed under Storage Hours. For more details, see the **Cloud Server Snapshots and Usage Reporting** section above
- Any Priced Software that was associated with the Cloud Server at the time of the snapshot is inherited by the Snapshot Preview and will incur usage accordingly. For more details on Priced Software, see Introduction to Cloud ("Priced") Software
- You can create multiple Snapshot Preview servers from the same Snapshot, and the Snapshot remains available even after the server is migrated to "Normal" as described below.
- You can have a maximum of 10 Snapshot Preview servers deployed at one time in a given Data Center.

Recently Updated

- Introduction to Geographic Regions
- Migrating to the new RHUI Architecture
- New Features by Release
- Cloud Backup - Introduction
- Introducing the New Red Hat Update Infrastructure