MCP 1.0 to 2.0 Self-Service Migration

Description

This article describes how users can migrate servers from MCP 1.0 to MCP 2.0 using the **DRS for Cloud** feature described in Introduction to DRS for Cloud

The functionality described here can be utilized when users have Cloud Servers deployed in MCP 1.0 locations where DRS is enabled to support replication to a corresponding MCP 2.0 location. Users can identify if their MCP 1.0 location has such a DRS pairing available as described in How do I Identify Hardware Specifications and Capabilities Available in a Data Center Location.

This process is ideal for small to mid-sized clients who do not have a complex setup* and/or do not have any physical devices paired to their MCP 1.0 Server.

Recommended reading:

- Understanding MCP 1.0 vs. MCP 2.0 Data Center Locations
- Introduction to SSL Offload, including SSL Domain Certificate, SSL Certificate Chain, and SSL Offload Profiles

Prerequisites

1. Users must enable IPv6 locally on their MCP 1.0 servers, as IPv6 is utilized for the Client-to-Site VPN functionality in MCP 1.0 as described in How to Connect to a VPN with Single-Factor or Multi-Factor VPN Authentication
    a. This is a TCP/IP property in the Guest OS, which must be enabled locally to utilize IPv6
2. VM Tools should be be up-to-date and running on All MCP 1.0 Source Servers ***that will be migrated***
    a. See How to Update VMware Tools on a Cloud Server
3. Source and Target Locations must be enabled for DRS for Cloud
    a. See How do I Identify Hardware Specifications and Capabilities Available in a Data Center Location

What cannot be migrated using this procedure?

- Organizations with ***Complex Setups** (refer to FAQ), including MCP 1.0 CPNC connections, are more likely to need Cloud Support team assistance.
    - Please contact us well in advance of your planned migration for assistance.
- Some Virtual Appliances do not support replication
    - Some virtualization appliances do not support the disk replication used by DRS for Cloud. If testing indicates this does not work, clients will need to re-import any appliance as a fresh device
- Windows 2003 Guest OS Customization Images will not work in MCP 2.0. See What Operating Systems are Currently Supported on CloudControl?

Steps to Prepare for Self-Service Migration

1. **Review your MCP 1.0 environment and eliminate unnecessary assets**
    a. Review current Cloud Servers in the MCP 1.0 location. Delete any that you do not require on MCP 2.0
    b. Review any Client Images that you have deployed in the MCP 1.0 location. Delete any that do not require on MCP 2.0
    c. Consider your MCP 1.0 ACL Rules and any firewall rules that may be implemented directly on your Cloud Servers. It is likely that a subset (or all) of these will need to be recreated as MCP 2.0 Firewall Rules in a later step.
2. **Assess your downtime requirements**
    a. Identify your mission-critical systems and calculate the downtime you can take
    b. Follow step 6 to migrate any machine(s) that can be shut down or which might require a longer downtime
3. **Create a Network Domain in the corresponding MCP 2.0 location** (this will be your "Target" location)
    a. Deploy an MCP 2.0 Network Domain in the Target MCP 2.0 location as described in How to Deploy a Network Domain in a MCP 2.0 Data Center Location
        i. MCP 2.0 supports multiple VLANs in the same Network Domain so for most users, only a single MCP 2.0 Cloud Network Domain will be required
    b. For each MCP 1.0 Network, deploy a VLAN in the MCP 2.0 Network Domain to support your Cloud Servers
        i. You can configure each VLAN to match the Source Cloud Network's IPv4 Addressing. Unlike MCP 1.0, MCP 2.0 allows users to define their IPv4 address space. For details, see Introduction to IP Addressing in MCP 2.0
    c. Add Public IPv4 Blocks to support your needs. See How to Manage Public IPv4 Addresses on a Network or Network Domain
        i. Unlike MCP 1.0, a Cloud Network Domain does not include any public IPv4 addresses by default.
4. **Create Equivalent Firewall Rules on Your MCP 2.0 Target**

    a. Create Firewall Rules on the MCP 2.0 Target Network Domain to match the MCP 1.0 Source Network's intent as described in How to Create a Firewall Rule on a Network Domain.
        i. Note firewall behavior is different in MCP 2.0. The default rules are different - traffic between VLANs is denied by default. For more details, see Introduction to Firewall Rules for Cloud Network Domains in MCP 2.0
5. **Copy Client Images from MCP 1.0 Source location to MCP 2.0 Target location**
    a. This function does not use the DRS for Cloud feature as it applies only to Cloud Servers. Instead, use the function described at How to Copy a Client Image between Locations in the Same Geographic Region
6. **Copy powered off MCP 1.0 Servers from MCP 1.0 Source Network to MCP 2.0 Target Network Domain**
    a. If the server isn't running, the DRS for Cloud feature isn't needed. Instead, use the function described at How to Copy a Stopped MCP 1.0 Cloud Server to an MCP 2.0 Data Center Location
7. **For each powered on MCP 1.0 Source Server, Create a DRS Target Server attached to the associated VLAN**
    a. Details on this function are available at How to Create a DRS Target Server. Make sure you assign the DRS Target Server the same private IPv4 address as the Source Server. This ensures that the CloudControl IPv4 record will be accurate when the **DRS Preview** step is implemented below.
    b. MCP 2.0 supports multiple NIC's but since you're migrating an MCP 1.0 Cloud Server, it will only have one NIC.
8. **Create Consistency Group(s) that Pairs your MCP 1.0 "Source" Servers to the MCP 2.0 "Target" Servers**
    a. Details on this function are available at How to Create a DRS Consistency Group
    b. Identify the servers that need to be migrated with the server state as of the same period in time and group them together in the same Consistency Group.
9. **You will need to wait for the Consistency Group to replicate, which can take several hours**
    a. You can monitor the state as described in How to View and Clean your Consistency Groups
10. **You can test your migration by putting the Consistency Group(s) in DRS Preview mode using a DRS snapshot**
    a. This brings up your Target Servers with the same disk state as the Source Servers as of the snapshot time. Details on this function are at How to Start a DRS Preview for a Consistency Group
        i. Use the most recent available DRS Snapshot
        ii. Once the Consistency Group is in Preview Mode, you can log into any Target Server using the console option and verify its configuration.
        iii. If you configure the NIC in the Target Server Guest OS with IPv6, you will be able to use that IPv6 to log in via the Client-to-Site VPN described in How to Connect to a VPN with Single-Factor or Multi-Factor VPN Authentication
        iv. We recommend confirming the NIC configuration in the Target Server's Guest OS with the CloudControl record.
    b. Note that if your application leverages inbound public IP traffic, you'll need to configure equivalent connectivity to your new public IP addresses:
        i. MCP 2.0 NAT functionality is similar to MCP 1.0. See How to Create a NAT Rule on a Network or Network Domain
        ii. MCP 2.0 uses Virtual Listeners instead of MCP 1.0 VIP functionality. For an overview, see Introduction to Virtual Listeners / VIPs in MCP 2.0
        iii. You should ensure your DNS entries are prepared to support a migration to the new MCP 2.0 public addresses by making sure the TTL (Time to Live) is short

Steps to Implement Self-Service Migration

When you are ready to migrate, the actual migration is multi-step, one-way process:

1. **Put your MCP 1.0 assets into maintenance.**
2. **Put the Consistency Group(s) in DRS Preview mode, in the same manner, you did for testing.**
3. **Apply IPv6 addresses to the Target Servers as was done in testing**.
4. **Confirm the application is ready to migrate prior to the next step!**
5. **Commit the DRS Preview State** as described in How to Initiate a Failover for a DRS Consistency Group
    a. The workload on the MCP 2.0 Target Server will be powered on and the corresponding workload in MCP 1.0 will be powered off
    b. The Consistency Group will be removed as part of this process, so it's a one-way change.
        i. If for some reason you need to fail back, you can power off the Server in MCP 2.0 and power the MCP 1.0 Server back on but to re-initiate migration, you will need to re-configure all of the Consistency Group(s)
6. **Optional but recommended, consider your SSL Certificate configuration**
    a. MCP 2.0 offers a convenient means of SSL certificate management through the SSL Offload feature, which removes the need to apply your certificates directly on your Cloud Servers. For full information please refer to Introduction to SSL Offload, including SSL Domain Certificate, SSL Certificate Chain, and SSL Offload Profiles, which includes links to articles describing how to set up an SSL Offload configuration in addition to explaining how the feature works.
7. **As needed, update DNS records to the new Public IPv4 on the MCP 2.0 side**
    a. You will need to work with your DNS provider support team to change the DNS setting
8. **If you use Cloud Monitoring, disable Cloud Monitoring on the MCP 1.0 Source Server and enable on the MCP 2.0 side**.
    a. To disable to MCP 1.0 side, see How to Disable Cloud Monitoring for a Server
        i. Stopping Cloud Monitoring will delete historical data. You can download reports before you disable in case you need to preserve the historical data.
    b. To enable the MCP 2.0 side, see How to Enable Cloud Monitoring for a Server
9. **If you use Cloud Backup**
    a. Backup history or retention cannot be moved to MCP 2.0
    b. If you do not need a backup history of the MCP 1.0 server, simply delete backups from MCP 1.0 as described in How to Delete a Backup Client on a Cloud Server and How to Disable Cloud Backup for a Server
    c. If you wish to keep the backup history available for a period of time, you can detach the history as described in Detaching a Backup Set. However, you cannot restore onto the MCP 2.0 server in a self-service manner. To restore onto MCP 2.0, you will need to open a ticket with backup support to perform a restore on your behalf
    d. In either case, you may want to change your backup approach on MCP 2.0:
        i. Many MCP 2.0 locations support a newer alternative called Cloud Server Snapshots. See Introduction to Cloud Server Snapshots
        ii. Alternately, you can enable the same Cloud Backup feature on MCP 2.0 as described in:
            1. How to Enable Cloud Backup on a Cloud Server
            2. How to Install the Backup Client on a Linux Server and How to Install the Backup Client on a Windows Server
            3. Additional Steps to Enable Application Backups once Client is Installed

10. **When complete, delete your MCP 1.0 assets and take advantage of the new capabilities MCP 2.0 offers.**

FAQ

- **The current MCP 1.0 Cloud environment meets all my needs. As such, why would I want to migrate to the MCP 2.0 environment?**

There are several compelling reasons to migrate to the MCP 2.0 environment. MCP 2.0 utilizes the latest in “best-of-breed" technologies to service its many cloud customers. In addition, there are several services and features available in the MCP 2.0 environment that are not available in MCP 1.0. These include, but are not limited to the following: Cloud Server Snapshots, Provisioned IOPS, various Network Domain Options, and reduced compute pricing. In addition, there are more pricing options available to customers in MCP 2.0. Finally, as part of NTTC CIS's guiding principle of continuous improvement, we will be retiring the MCP 1.0 platform.

- **Can I actively use my MCP 1.0 environment during the migration?**

Customers cannot modify the hardware assets during the migration process, however, customers can make changes to the operating systems (OS).

- **Is the migration process encrypted?**

Yes, the migration process is encrypted. The source and destination storage arrays are encrypted, and the data is transferred via encrypted tunnels.

- **What are the risks to the client in migrating from MCP 1.0 to MCP 2.0?**

Risk is minimal as the Source MCP 1.0 environment will exist until the customer deletes it post migration validation. Clients will have the ability to validate their MCP 2.0 location servers prior to final cutover.

- **When will the MCP 1.0 platform be retired?**

Timelines for the inevitable retirement of MCP 1.0 are still being confirmed. Meanwhile, we are engaging with our clients early on so we can provide appropriate support and allow time to schedule the migration to lessen the burden on the client.

- **Who is the target audience for Migration?**

All customers on MCP 1.0 infrastructure (Public Cloud, Hosted Private Cloud, Provider Cloud) are part of the target Migration audience.

- ***What is a Complex Setup?**

Any client that has multiple CPNC or interconnects, significant numbers of Servers in multiple Data Centers and/or Geographic Regions, Static Route configurations, or physical devices.

Recently Updated

- What Happens to a Source Server when it is added to a Consistency Group?
- Introduction to DRS for Cloud
- How to Start a DRS Preview for a Consistency Group
- How to Set Re-IP Address Rules for a Target Server in a DRS Server Pair
- How to Delete Re-IP Address Rules for the Target Server in a DRS Server Pair