Brocade Virtual Traffic Manager (Brocade vTM) Quick Start Guide for Hitachi Content Platform (HCP)

HCP Technology Team

Intro .......................................................................................................................... 2
Assumptions .............................................................................................................. 2
Documentation Reference ......................................................................................... 2
Overview .................................................................................................................... 2
Step 1: Creating the Brocade vTM Boot Disk ......................................................... 3
Step 2: Install the Brocade vTM Base OS ................................................................. 3
Step 3: Setting the initial IP ...................................................................................... 5
Step 4: Running the initial configuration Wizard ..................................................... 5
Step 5: Joining a Brocade vTM to a cluster ............................................................... 13
Step 6: Configure services ....................................................................................... 16
Step 7: Create a Traffic IP Group ............................................................................. 35
Step 8: Create a Virtual Server for HCP ................................................................. 37
A.1: Configure Data Plane Acceleration ................................................................. 47
A.2: Create The Search Console Pool .................................................................... 48
Intro
This document is intended for anyone who is looking to configure a Brocade vTM load balancer with Hitachi Content Platform. Brocade Virtual Traffic Manager (vTM) is part of the Brocade Virtual Application Delivery Controller (vADC) product family. There are a number of other components in the Brocade vADC family, but the Hitachi Content Platform only needs to install the Brocade vTM component.

The most current version of this guide can always be downloaded from at:

https://hcpanywhere.hds.com/u/yYrhB92K4oTbiuEH/Brocade%20vTM%20HCP%20Quickstart.pdf?

Assumptions
This quick start guide assumes the following has been completed:

- Hardware is setup and functional
- Networking is configured for servers which will host the Brocade vTM (10GB network recommended)
- Brocade Software and documentation has been downloaded.
  - If you have not yet downloaded your Brocade vTM software, please refer to the email from Brocade that is included on the Media Kit DVD sent to you. That email provides complete instructions for downloading your software including the required “Tokens” and “Token Serial Numbers”.

Documentation Reference
The Brocade vTM 11.0 Hardware document is referenced in the first several steps of this document.

Overview
The install and configuration process involves multiple steps. First a boot disk must be created and the Brocade vTM OS needs to be installed on every node. Next an initial setup is completed, followed by adding each node into the cluster. Lastly monitors, pools, and traffic IP groups are created for each HCP service.

Note: Steps 1 & 2 can be ignored if running as a virtual machine. Please follow the vTM Deployment Guide for Hypervisor deployment instructions.
Step 1: Creating the Brocade vTM Boot Disk
In order to create the Brocade vTM Boot Disk, reference Chapter 3 of the Brocade Virtual Traffic Manager: Appliance image installation and Getting Started Guide, v11.0. Follow the steps to create an installation Disk or USB Flash Drive.

Step 2: Install the Brocade vTM Base OS
To install the Brocade vTM Base OS:

1. Boot the physical or virtual system off the installation media which was created in Step 1.
2. At the Brocade Installer screen, enter Yes to start the installation.
3. If you are prompted to unmount partitions, select yes. The existing partition disks are unmounted, and the vTM base OS begins to install.

4. Once the installation completes, remove the Installation media and select Continue.
Step 3: Setting the initial IP

Extra details of these steps can also be found in chapter 4 of the Brocade vTM: Application image installation and getting started guide.

To set the initial IP address from the console of the newly installed node:

1. Type Alt+F2 to switch to the alternative console display "tty2".
2. When prompted for the username, enter admin.
3. When prompted for the password, enter admin.
4. Run the following command: z-set-initial-address
5. Enter your IP address EX 192.168.1.10
6. Enter your netmask. EX: 255.255.255.0
7. Once the command completes, enter logout to log out of the console.
8. Switch back to "tty1" by pressing Alt+F1.
9. Verify that the IP address in the URL for “Administration Interface” has changed to your new IP address.

Step 4: Running the initial configuration Wizard.

Open your internet browser and navigate to the IP address configured in step 3. Details of these steps can be found in chapter 4 of the Brocade vTM: Application image installation and getting started guide.
Click Next

Initial configuration, step 1 of 9

1. Welcome to your Brocade Virtual Traffic Manager

The following pages will guide you through the process of setting up your Brocade Virtual Traffic Manager Appliance for basic operation. This should only take a few minutes. Some initial networking settings will be required - please contact your support provider if you need any help.

Accept the License agreement. Click Next

Initial configuration, step 2 of 9

2. Brocade Terms and Conditions of Sale

Use of this software is subject to the Brocade Terms and Conditions of Sale. Please review these terms, published at http://www.brocade.com/legal/index.page before proceeding.

I accept the license agreement
Configure Management IP address for Brocade vTM. Click Next.

3. Networking

Please provide the basic network configuration for this appliance. The configuration may be changed at a later date using the user interface.

The hostname that this appliance will be known by. This can be provided as 'hostname' or 'hostname.domainname'.

Hostname: vadc2.denver.lab (required)

Please enter a valid IPv4 address and netmask for at least one network card.
IPv6 addresses can be configured on the System > Networking page.

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP address</th>
<th>Netmask</th>
<th>Management IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>172.19.22.191</td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>eth1 (unplugged)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth2 (unplugged)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth3 (unplugged)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth4 (unplugged)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth5 (unplugged)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth6 (unplugged)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth7 (unplugged)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth8 (unplugged)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth9 (unplugged)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth10 (unplugged)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth11 (unplugged)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The appliance can be configured to only allow management on one specific IP address. This restricts all admin server access, SOAP management, REST API access and other control information to this IP address. This setup is useful if you want to completely separate your public and private networks. If you wish to do this, tick the box below and select an IP address using the Management IP address option buttons above.

- Use a single Management IP address

To use trunking, give interfaces the same IP address. All interfaces in a trunk must be connected to the same switch and the switch must have IEEE 802.3ad support enabled.

**Note:** Unplugged interfaces should not be assigned IP addresses on the management network.

The gateway IP address for this appliance.

Gateway: 172.19.22.1
Configure a DNS server for Brocade vTM. Click Next

Initial configuration, step 4 of 9

4. DNS/Search Domain Settings

Please provide the DNS and Search Domain configuration for this appliance. DNS settings are optional. However, without access to a Name Server, hostnames won’t be able to be automatically converted to IP addresses.

The Name Server(s) that the appliance will use. Please provide a space separated list of your Name Servers’ IP addresses.

Name Servers: 172.19.22.100

The default domain name used when looking up unqualified hostnames in the DNS.

Search Domain: denver.lab

Set a time Zone. Click Next
Set an Admin Password. Click Next.

Initial configuration, step 6 of 9

6. Security

A master 'admin' user is created that you can use to log in to the Administration Server and SSH console. Please choose a password for this user.

Enter Password: ******
Confirm Password: ******

Brocade vTM Appliances come with a tool pre-installed to help prevent brute-force SSH attacks. This will block remote hosts that have made multiple failed connection attempts for a set time. The specific parameters, including the time spent blocked and the number of permissible failed attempts, can be configured on the Security page when you have completed the initial configuration.
Would you like to enable this tool now?

- Enable SSH Intrusion Prevention

Optionally, set IPMI information. Click Next.

Initial configuration, step 7 of 9

7. IPMI settings

You can modify the IPMI configuration for this appliance, or leave these settings blank to use the current IPMI configuration.

You may choose to disable IPMI LAN access entirely.

- Disable IPMI LAN access

You may create an IPMI 'admin' user to access IPMI remotely using the IPMI LAN channel.

- Create an IPMI admin user
Upload a Brocade vTM License. Click Next. Review the configuration settings and complete the Initial setup. Click Complete.

Once the initial configuration is finished, enter the IP address you configured in step 4 into the URL.

**Initial configuration, finished**

Setup finished

Your traffic manager is now being reconfigured with the settings that you have provided.

Please make a note of the new Administration Server location:

https://172.19.22.191:9090/

It can take up to a minute for the network to adjust to the new settings, so the new Administration Server may not be available immediately. You can log in with the username 'admin' and the password that you chose.
Using the admin user and password configured in step 4, log into the vTM.
Configure the Brocade vTM for Active Active (LACP) networking, to do this configure a second interface with the same IP address.
IMPORTANT!!! Set the management port on the Brocade vTM to 9091, if you do not this will conflict with the HCP MAPI port.

Repeat steps 2 and 3 for each Brocade vTM in your environment.

Step 5: Joining a Brocade vTM to a cluster

A Brocade vTM cluster needs a. minimum of two hosts and can be configured in an Active/Backup or Active/Active configuration. We will configure four Brocade vTM hosts in an active/active configuration.
1. Connect to the IP address of the second Brocade vTM, select the **join a cluster** from the **Wizards** drop down menu.

To join a cluster click the Select existing cluster radio button. Click Next.
Cluster Joining wizard, step 2 of 5

2. Cluster selection

Please select the cluster you wish to join:

Cluster 1: vadc1.denver.lab:9090

Cluster Joining wizard, step 3 of 5

3. Authentication

The admin server you are clustering with is using an SSL certificate with the following SHA-1 fingerprint:

vadc1.denver.lab:9090

5D:05:70:91:51:10:B5:45:84:5F
46:C9:00:60:C4:E9:B1:E1:BC:70

Unfold to view full certificate details ...

Please check the box beside the fingerprint above to indicate that you have verified it or that you trust the network between it and this system.

If you do not already have this fingerprint on record you can get it by logging into the target admin server and visiting the System > Security page. (Refer to the product documentation for further information on cluster security.)

Enter the username and password of a user in the target cluster with permission to add and remove traffic managers.

Username: admin
Password: ********

Cluster Joining wizard, step 4 of 5

4. Additional Settings

If the cluster has Traffic IP groups, should the new machine join them?

- Yes, and allow it to host Traffic IPs immediately
- Yes, but make it a passive machine
- No, do not add it to any Traffic IP groups
Repeat the above steps for each Brocade vTM in your environment, when completed you should see all of the Brocade vTM’s listed as traffic managers from the home page.

**Step 6: Configure services**

For each of the services on HCP (Management, Data Access, and MAPI), we will create a monitor, Pool, TrafficIP group, then Virtual Server.
6A: Create HCP Specific Monitors

Navigate to Catalogs > Monitors and scroll down to Create new monitor.

Enter HCP –Data and select HTTP Monitor, then select Create Monitor.
Once created, select back off = No, scroll down to additional settings and select the path and status regex as seen below.
Select Use SSL = Yes, In the path textbox enter /node_status and in the status_regex textbox enter 204

Next, create a monitor for HCP-Management
Select Backoff = No

Custom, Pool-node HTTP monitor
You can edit all of its parameters.

HCP-Management is currently not being used by any pools.

Last Modified: 1 Aug 2016 19:14

<table>
<thead>
<tr>
<th>▼ Basic Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: HCP-Management</td>
</tr>
</tbody>
</table>

The minimum time between calls to a monitor.

| delay: 50 | seconds |

The maximum runtime for an individual instance of the monitor.

| timeout: 3 | seconds |

The number of times in a row that a node must fail execution of the monitor before it is classed as unavailable.

| failures: 3 |

Should the monitor slowly increase the delay after it has failed?

| back_off: Yes, No |

Whether or not the monitor should emit verbose logging. This is useful for diagnosing problems.

| verbose: Yes, No |
Change use_ssl=“yes” , Path = “/” and Status regex = 302

Next Create a monitor for HCP-MAPI
Monitor: HCP-MAPI

Custom, Pool-node TCP Connect monitor
You can edit all of its parameters.

HCP-MAPI is currently not being used by any pools.

Last Modified: 1 Aug 2016 19:16

▼ Basic Settings

Name: **HCP-MAPI**  
The minimum time between calls to a monitor.  
**delay**: 30 seconds

The maximum runtime for an individual instance of the monitor.  
**timeout**: 90 seconds

The number of times in a row that a node must fail execution of the monitor before it is classed as unavailable.  
**failures**: 3

Should the monitor slowly increase the delay after it has failed?  
**back_off**:  
- **Yes** 
- **No**  

Whether or not the monitor should emit verbose logging. This is useful for diagnosing problems.  
**verbose**:  
- **Yes** 
- **No**

▼ Notes

A description of the monitor.  
**note**: **HCP MAPI**

Apply changes

**Update**
You should now have a monitor for HCP-Data, HCP-Management and HCP-MAPI

6B: Create Pools for each HCP Service

Navigate to Services > Pools, Create a new pool for HCP01-Data.

Input the IP address of each node, followed by the port 443, and select the monitor of HCP-Data.
6C: Enable SSL Encryption
Optionally enable SSL encryption to re-encrypt data traffic between the Brocade vTM and HCP
Scroll down and edit SSL Settings.
For SSL_encrypt, select yes.

Now create a pool for HCP01-Mapi. Enter the IP address of each node followed by port 9090, select the HCP-MAPI monitor.
Scroll down and edit SSL Settings.
For SSL_encrypt, select yes.

Next create a pool for HCP01-Management, enter the IP address for each node with the port of 8000, select the HCP-Management Monitor and create the pool.
Scroll down and edit SSL Settings

- **Protocol Settings**
  - Configure settings specific to the protocol this pool is using to communicate with its nodes.

- **Load Balancing**
  - Load balancing controls how the pool distributes traffic across its nodes.

- **Session Persistence**
  - Session persistence controls how the pool ensures that client sessions are consistently directed to the same nodes.

- **Bandwidth Management**
  - A bandwidth management class in a pool limits the upstream bandwidth to the backend nodes.

- **Health Monitoring**
  - Adding monitors to a pool enables the status of backend nodes to be known more accurately.

- **SSL Settings**
  - Enable and configure SSL encryption between the pool and its back-end nodes.

- **IP Transparency**
  - Configure whether connections to back-end server appear to originate from the traffic manager or the remote client.

- **Autoscale**
  - Pods whose nodes are located in a cloud can be autoscaled; these settings control the details of how this is done.

- **DNS-derived autoscaling**
  - DNS-derived autoscaling queries DNS hostnames and grows and shrinks the nodes used in a pool as the DNS record changes.

- **Kerberos Protocol Transition**
  - Specialize Kerberos protocol transition for this pool.
For SSL_encrypt, select yes.

Now, create a pool for the HCP Search UI.
You have now created Pool’s for HCP Data, Monitor and Management.

6D: Enable Session Persistence
From the Services > Pools page, Click on HCP01 Management
Click on Session Persistence.

Click on Manage Session Persistence classes.
Create a new Session Persistence class called HCP-Persistence. Under Type, select **Transparent session affinity**.

Click the edit button on the first pool.

Select **Session Persistence** settings.
Select **HCP-Persistence Class** and click Update.
Step 7: Create a Traffic IP Group

Under Traffic IP groups, select Network Settings.

In the Add a network field, type a traffic IP Network.
Create the Traffic IP Group, this IP address will serve as the interface for the HCP on the load balancer.

Optional: Upon the creation of the Traffic IP Group, w/ Multi-Hosted mode ENABLED, the a static ARP entry may need to be created in the network. Attempt a ping of the Traffic IP group once created. If a response isn’t received, please identify the MAC address assigned & issue the following command to the network switches.

Issue the following commands on the switch(es) responsible for the HCP

1. Add the Static Mac Entry
   a. `#mac address table static <mac address> <vlan> <interface>`
   b. E.G: `#mac address-table static 0100.5E65.0101 vlan 225 interface po 1`
2. Add the ARP entry to the VLAN  
   a. E.G: `ip arp 172.18.225.105 0100.5E65.0101`

**Step 8: Create a Virtual Server for HCP**

Navigate to Services> Virtual Servers and create a Virtual Server for HCP Data

Once the HCP Data Virtual Server has been created, select the traffic IP group and click enabled.
Once you created the Virtual server for HCP, click the Edit button for **SSL Decryption**.
Enable SSL Decrypt and manage the SSL certificate.

Click create a Self-Signed certificate.
Enter the appropriate information for the SSL Certificate, the name should match the HCP’s domain name.

Name: Description of Certificate
Common Name (CN): wildcard entry matching HCP cluster name, e.g.: *.hcp1.denver.lab
Organization: Customer Org
OU: Optional
Location: City
State: Full State Name
Country: Country 2 Letter Code
Expiration: Recommended 10 years
Key Type: 2048 bit RSA

NOTE: Please see the vTM administration guide if a trusted certificate from an approved internal or external authority is required.
Enable SSL Decrypt.

Click **Create a HCP Management Virtual Server.**

V1.0.6 - Last update October 2016
Once the HCP Management Virtual Server has been created, select the traffic IP group and click enabled.
Then click the edit button for **SSL Decryption Setting**.
Select the previously created certificate, and enable SSL decrypt.

Create a Virtual Server for HCP01-Mapi.
Once the HCP Management Virtual Server has been created, select the traffic IP group and click enabled.
Click the edit button for **SSL Decryption Setting**.
Select the HCP1 certificate and enable SSL Decrypt by selecting yes.

You have now configured the Brocade vTM for HCP. Create a DNS record which resolves the host address specified in the certificate to the IP address created as the traffic IP group. The DNS record forwards HCP-Data, Management, and MAPI requests through the Brocade vTM to the HCP.

Appendix A

A.1: Configure Data Plane Acceleration

In order to provide additional performance & hardware acceleration to the HCP cluster traffic, thru the vTM, Brocade has provided a feature called Data Plane Acceleration that has been qualified to run against the intel 10Gb Ethernet adapters provided in the D51B & all VMware deployments. To enable this, please ensure that multiple processors are available to the vTM appliance as this required dedicated cores for data plane acceleration traffic.
Browse to System -> Data Plane Acceleration & choose `data_plane_acceleration_mode: YES`
Define the # of cores to dedicate to the data plane acceleration traffic.
Choose ‘Update’ to confirm setting.

Once applied, the vTM will need rebooted. *This will need to be done on each node of the cluster individually.*

**Warning:** There may be a problem. Please see below for details

```markdown
data_plane_acceleration_mode: A machine reboot is required to start Data Plane Acceleration Mode
```

System -> Traffic Manager -> REBOOT

**A.2: Create The Search Console Pool**

**A.2.1: Create a monitor for HCP MQE Search Interface**
In order to support the HCP MQE Search UI, a pool will need to be created.
Create a new HTTP monitor & call it ‘HCP-Search’, ensure that **Scope** is set to **NODE**

Ensure that **back_off** is set to **YES**
Ensure that `use_ssl` is enabled & set the `status_regex` to 302

A.2.2: Create the HCP-Search Session Persistence

Create the HCP-Search session persistence

Set the Session Persistence to Transparent Session Affinity, leave the rest of the settings `default`
A.2.3: Create the Search Resource Pool

**Services -> Pools**

Add each HCP node with the port :8888 appended to the address, e.g. 192.168.14.220:8888

Choose the HCP-Search Monitor

![Pool Configuration](image)

Edit the HCP01-Search Pool, setting `ssl_encrypt` to YES

![SSL Configuration](image)
Enable the Session Persistence option previously created

A.2.4: Create the HCP-Search Virtual Server
Create the Virtual Server responsible for terminating the HCP Search UI traffic

Name: HCP01-Search
Protocol: HTTP
Port: 8888
Default Traffic Pool: HCP01-SEARCH

Ensure that the Virtual Server is **ENABLED**
Assign to the correct Traffic IP Group
Enable SSL Decryption
Choose the correct Certificate for the HCP cluster

Confirm HCP Search UI is reachable via standard Internet Browser test.