



Deploying the F5 Management Plug-In for VMware vSphere

Table of Contents

Introducing the F5 plug-in for VMware vSphere

Prerequisites and configuration notes	1
Installing the plug-in	3
Performing the initial configuration	4
Managing users of the plug-in	5
Managing the vCenter Parameters	6
Managing BIG-IP Definitions	7
Defining Rules for VM Membership in BIG-IP Pools	9
Approving and Denying Pending Changes	11
Managing virtual machines gracefully with the BIG-IP system	12

Appendix A: Frequently Asked Questions	16
--	----

Appendix B: Additional Software Components	20
--	----

Introducing the F5 Management Plug-In for VMware vSphere

Welcome to the F5 Management Plug-In™ installation and deployment guide for VMware® vSphere™. The F5 Management Plug-In for VMware vSphere provides integration between F5 Networks BIG-IP Local Traffic Manager (LTM) and VMware vSphere environments with the intent of reducing redundant tasks to operations performed in the vSphere client connected to a VMware vCenter™ instance.

The F5 Management Plug-In enables you to simplify the following tasks:

- ◆ **Adding virtual machines to pools on a BIG-IP system**

By defining policies that allow the plug-in to associate virtual machines with a pool on a BIG-IP system, the process of provisioning new servers for a load balanced application becomes much simpler.

- ◆ **Performing maintenance on a virtual machine**

Historically, when a server required maintenance an administrator had to either accept degradation of its performance, or to reach out to each application delivery controller that made use of the server and disable the corresponding objects to allow active sessions to gracefully finish.

Using this plug-in, an administrator simply indicates maintenance will be performed. Each BIG-IP system managed by the plug-in which uses that virtual machine will have the appropriate nodes disabled, allowing for existing sessions to continue operating. An administrator can then perform maintenance or other tasks on the server, before enabling it again, which returns it to service on the BIG-IP devices.

- ◆ **Shutting down a virtual machine gracefully**

Similar to the maintenance situation, if a virtual machine needs to be shutdown (perhaps as part of installing updates), it is best practice to allow existing sessions to close gracefully before initiating the shutdown, and for the shutdown to be initiated automatically once the connections reach a chosen level, or after a configurable timeout. The plug-in facilitates that workflow as well as booting it back up again and enabling it on the BIG-IP devices once it is available again.

The plug-in was written in Perl and only makes use of publicly available APIs such as F5's iControl™ and the VMware vSphere SDK for Perl. The source code for the application has not been obfuscated in any way and customers/partners are encouraged to modify or extend the plug-in.

- ◆ **Note**

The F5 Management Plug-In was created, tested, and published entirely by F5 Networks. VMware was not involved in the creation of the plug in and does not endorse it.

To provide feedback on this deployment guide or other F5 solution documents, contact us at solutionsfeedback@f5.com.

Prerequisites and configuration notes

The plug-in has the following requirements:

- ◆ One VMware vCenter 4.0 instance per plug-in installation.
- ◆ One or more VMware ESX/ESXi 4.0 hosts managed by each vCenter instance.
- ◆ One VMware Management Assistant (vMA) 4.0 virtual machine per plug-in.
- ◆ One or more F5 Networks BIG-IP Local Traffic Manager (LTM) systems (can be BIG-IP appliances, chassis, or Virtual Edition)
- ◆ It is assumed that the BIG-IP devices, vCenter, and ESX/ESXi hosts are already installed and initially configured. Refer to the appropriate documentation for each product for assistance with performing the necessary preparation.
- ◆ Installation of the plug-in is performed on top of a VMware Management Assistant (vMA) instance, which can be obtained from VMware's website. Download the OVF image and its documentation from: <http://www.vmware.com/support/developer/vima/>

As part of the installation of vMA, an IP address can be assigned manually or dynamically. It's recommended that a static address is used to avoid issues with the address changing once the plug-in is registered with vCenter. This address must be accessible from the systems that will be running the VMware vSphere client, and must be able to communicate with the vCenter system as well as any BIG-IPs (management IP or Self IP with port-lockdown allowing HTTPS).

For any assistance with vMA, refer to its documentation. It is not supported for the vMA instance hosting the plug-in to be used for any other purposes.

- ◆ The plug-in resides on F5's DevCentral (<http://devcentral.f5.com/labs/vsphereplugin/>), which requires a free registration

See *Appendix A: Frequently Asked Questions*, on page 16 and *Appendix B: Additional Software Components*, on page 20 for more information.

Installing the F5 Management Plug-In

The F5 Management Plug-In installs on top of a VMware Management Assistant (vMA) virtual machine which should not be used for any other purposes than hosting the plug-in.

To install the plug-in

1. Download the plug-in from F5's DevCentral (requires free registration)
<http://devcentral.f5.com/labs/vsphereplugin/>
2. Using SCP or SFTP, copy the plug-in archive to the vMA (once it is available) using the vi-admin user account.
3. Using SSH, log into the vMA using the vi-admin account.
4. At the prompt, type the following command:

```
# sudo sh F5_Management_Plug-in-1.0.shar
```

Type the password for the vi-admin user when prompted.

The self-extracting installer launches and gathers some necessary information, installs all of the necessary components to run the plug-in, enables necessary services in the system's firewall, and register the plug-in with a vCenter server instance.

5. When prompted, complete the following:
 - *IP Address or hostname of the plug-in*
This is pre-populated with the IP of the first ethernet interface (eth0), and in most cases does not have to be changed.
In the event of network address translation between the plug-in and vCenter or the users, it may be necessary to provide a different address or host name. This is used by vCenter as well as vSphere clients to connect to the plug-in.

Type the new IP address, or press Return to accept the default.

Note: We recommend you use either the IP address or the full host name of the vMA system hosting the plug-in. Accessing the vMA with a shortened host name can cause issues if the vCenter or client running the vSphere client has a different DNS suffix search order.

- *Administrator Email Address*
This is the email address of the administrative contact for the vCenter system targeted by the plug-in.

Type the email address and press Return.

- *vCenter Host*
DNS hostname or IP address of the vCenter system that the plug-in should assist in managing.

Type the host name or IP address of the vCenter.

- *vCenter Username and password*
A set of credentials that are used to initially register the plug-in with vCenter. These credentials are also stored for use by background tasks in the plug-in such as polling it for new virtual machines and shutting down VMs. These credentials are obfuscated but not encrypted on disk.

Type the user name and password.

Once the registration process is complete, the plug-in is available using the vSphere client as described in the following sections.

Performing the initial configuration

When you next connect to the vCenter with a vSphere client, the plug-in is available to users in the **Home** section of the application, under Inventory.

Click **F5 Management Plug-In** to access the plug-in.

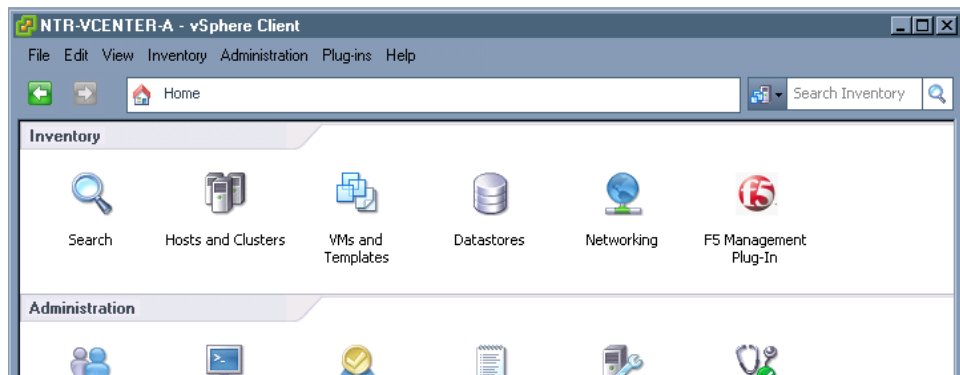


Figure 1 Home screen of the vSphere client

Managing users of the plug-in

The first screen you see when accessing the plug-in is a login form. The plug-in requires its own authentication to prevent users of the vSphere client with limited privileges from modifying policies or performing potentially damaging tasks.

Immediately after an installation, the authentication database is populated with a user that corresponds to the user name and password used to register the plug-in with vCenter. This account can be removed once others are created.

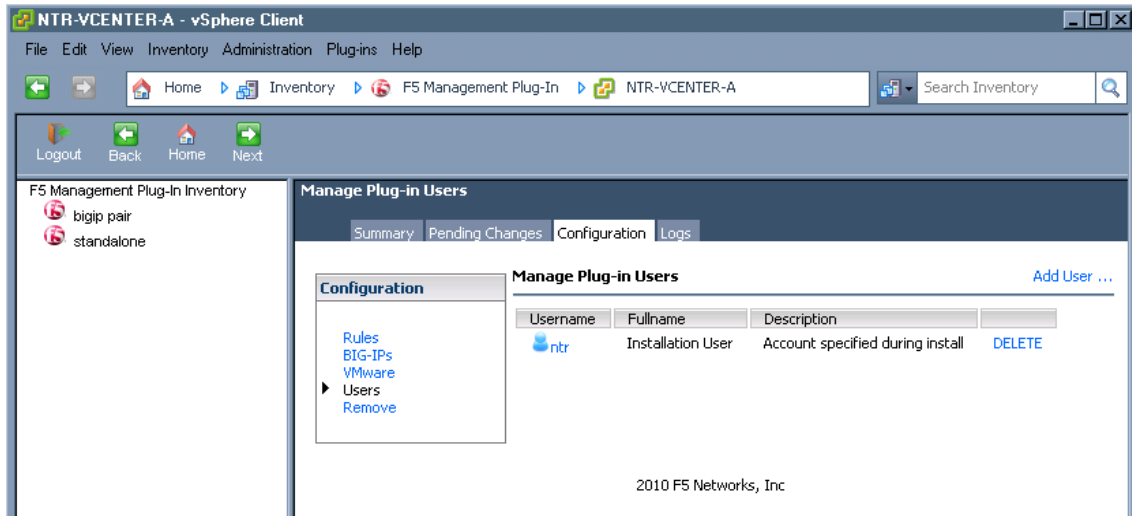


Figure 2 Manage plug-in Users page

To manage plug-in users

1. Open vCenter from a vSphere client.
2. From the **Home** page, in the Inventory section, click **BIG-IP Manager**.
3. If this is the first time you are accessing the plug-in, login with the same credentials you used to register it with vCenter.
4. Click the Configuration tab.
5. In the Configuration box, click **Users**. A list of users who can use the plug-in from within the vSphere client opens.
6. To manage the users, you have the following options:
 - **Edit an existing user**
To edit a user, from the Username column, click the user name you want to edit. A short edit user wizard opens. Modify the settings as applicable.
 - **Add a User**
To add a new user, click the **Add User** link. The Add User wizard opens.
 - **Delete a User**
To delete a user, click **DELETE** in the right column for that user and then confirm you want to permanently delete that user.

Notes about user names and passwords:

User names can contain:

- capital letters
- lowercase letters
- digits
- symbols, -_.

Passwords can contain:

- capital letters
- lower case letters
- decimal digits
- spaces
- symbols, !@#\$%^&*()-_+=[]{};,.

Both fields can be up to 16 characters long and neither can be blank.

Users in this database exist solely for using the plug-in and do not gain any capabilities to the vMA system hosting the plug-in, or to the rest of vCenter or the vSphere environment.

Once an additional user is created, the account that was created as part of the install can be removed.

Managing the vCenter Parameters

Each installation of the plug-in can only manage one instance of vCenter. The parameters to communicate with vCenter are stored during the initial registration of the plug-in with a vCenter and so it's likely these parameters will not need to be additionally changed.

However, if the user name or password necessary to login to vCenter or the address of the vCenter changes, it may be necessary to alter this information.

◆ **Note**

Because the plug-in can only manage one vCenter at a time and the credential store is initialized with a value, it is not possible to add additional vCenters.

To manage the vCenter parameters

1. In the vSphere client, open the BIG-IP Manager plug-in.
2. Click the Configuration tab.
3. In the **Configuration** box, click **VMware**.
4. You can modify the existing vCenter Parameters or Test connectivity to the vCenter:

- **Modifying the vCenter parameters**

Click the name of the existing vCenter server and complete the wizard. Remember this is the system and credentials that are used for background tasks such as polling for new virtual machines, retrieving information about VMs such as their names, IP addresses, and custom attributes, and for performing shutdown and reboot operations. Because of this, an account must be provided with sufficient privileges within vCenter to accomplish these tasks.

Important: Use extreme care in modifying any of the parameters in the wizard. When the plug-in was installed, a valid set of credentials had to be entered and these are automatically used afterward. Entering the wrong information in this wizard can result in the plug-in not functioning.

- **Testing Connectivity to vCenter**

Click **TEST** from the table to initiate an attempt to communicate with the vCenter. If successful, you are presented with information about the vCenter. If unable to connect or login, you are presented with such information.

Managing BIG-IP Definitions

In order for the plug-in to operate, you must define BIG-IP systems either as single units or HA pairs. This consists of a name for the system/pair, host names or IP addresses of the units, and a user name and password to use when communicating via iControl with the systems.

◆ **Note**

These names and passwords are stored in a database on the plug-in's server and are not encrypted.

To add a BIG-IP system to the plug in

1. In the vSphere client, open the BIG-IP Manager plug-in.
2. Click the Configuration tab.
3. In the **Configuration** box, click **BIG-IPs**.
4. Click the **Add BIG-IP** link on the far right. The Add BIG-IP wizard opens.
5. In the **Name** box, type a unique name for this BIG-IP system.
6. In the **Hostname/IP Address** box, type the host name or IP address of the BIG-IP device.
7. In the **Peer Hostname/IP Address** box, if you are using the BIG-IP system in a redundant pair, type the host name or IP address of the peer BIG-IP device.

8. In the **Username** box, type a user name on the BIG-IP system that has access the resources that will be managed.
9. In the **Password** box, type the associated password.

Figure 3 Add BIG-IP system wizard

10. Click **Next**.
11. Review the information. If you need to make changes, click the **Back** button. Otherwise, click **Next**.
12. Click **Close** to add the BIG-IP system.

Other options on the BIG-IP configuration page:

- ◆ *Modify an existing BIG-IP definition*
Click the name of the system in the table to run the wizard; modifying any of the settings as applicable. Just like when creating a definition, leave the peer host blank if it represents a standalone BIG-IP.
- ◆ *Delete an existing BIG-IP definition*
Click **DELETE** to the right of the system you want to delete, and then confirm the deletion.
- ◆ *Testing Connectivity and Configuration*
Click **Test** to the right of the system you want to test. This initiates a connection test to the BIG-IP systems. If successful, a message displays showing some information about the system. If unsuccessful, an error message displays.

Defining Rules for VM Membership in BIG-IP Pools

The most useful feature of the plug-in is its ability to automatically add members to pools on BIG-IP devices based on information learned from virtual machines managed by vCenter. To accomplish this, an administrator must first define the policies that will govern the operation of the plug-in. This is done through the creation of rules. Once a rule is created, every 5 minutes the vCenter system is polled in the background by the plug-in and the rules are compared against the current contents of the vCenter.

Adding a New Rule

A rule is needed for each policy governing how VMs should be added to pools on BIG-IPs.

To add a new rule

1. In the vSphere client, open the BIG-IP Manager plug-in.
2. Click the Configuration tab.
3. In the **Configuration** box, click **Rules**.
4. Click Add Rule on the far right. The Add Rule wizard opens.
5. In the **Descriptive Name** box, type a name.
Click **Next**.
6. From the **BIG-IP** list, select the BIG-IP system (you added in *Managing BIG-IP Definitions*, on page 7) that includes the pool to which you want to add members.
Click **Next**.
7. From the **Pool** list (populated by all pools on the BIG-IP system you selected in the previous step), select the pool to which you want to add matching virtual machines.
8. In the **Service Port** box, type the TCP/UDP port to associate with the IP of any virtual machines added to the pool. Must be between 1 and 65535.
This is necessary because the listening services of a particular VM are not exposed to the plug-in.
Click **Next**.
9. From the Match Type list, select the criteria to use when determining whether a VM matches the rule. The options are:
 - *VM Name Regular Expression*
A regular expression to apply to the name of the VM. If it matches, all IP addresses of the VM are added to the pool.
 - *VM IP Against Network*
Accepts CIDR notation for a match. Any IP addresses of a VM that satisfy the mask operation are added to the pool.

- *VM IP Within Range*
Accepts two IP addresses separated with a dash and no whitespace. Any IP addresses that fall between the two addresses are added to the pool.
 - *Custom Attribute*
Accepts a name/value pair separated by an equals (=) sign and no whitespace. If a virtual machine has a custom attribute and value that matches the provided criteria, all IP addresses for the VM are added to the pool.
10. In the **Match Criteria** box, type the criteria to apply based on the Match Type you selected in the previous step. The following list contains simple examples for each Match Type:
- *VM Name Regular Expression*
http
 - *VM IP Against Network*
192.0.2.0/24
 - *VM IP Within Range*
192.0.2.1-192.0.2.100
 - *Custom Attribute*
webservers=true
11. In the Queue Changes section, click the appropriate button (For more information on this process, see the following section: *Approving and Denying Pending Changes.*):
- a) Click the **Require changes to be approved** button if the results of a rule match should be added to a pending list.
 - b) Click the **Make Changes automatically** button if the results of a rule match should be applied immediately.
- For testing the plug-in, we recommend **Require changes to be approved**. We also recommend this option if you anticipate a VM will have multiple IP addresses present but only one should be added to a pool, and a match type that doesn't use the IP address is used.
Click **Next**.
12. Review the summary and then click **Next**.
The Rule is created.
13. Click **Close**.

Other options on the BIG-IP configuration page:

- ◆ *Modify an existing Rule*
Click the name of the rule in the table to run the wizard; modifying any of the settings as applicable.
Note: Modifying a rule does not result in previously added pool members from being removed if they no longer match a rule.

- ◆ *Delete an existing Rule*

Click **DELETE** to the right of the rule you want to delete, and then confirm the deletion.

Note: Deleting a rule does not remove pool members from pools on BIG-IP systems that were previously added by it.

Approving and Denying Pending Changes

If you defined a rule that requires approval of matches before performing an action, when a match is found it is added to a queue. You can manage this queue from the plug-in.

To approve or deny changes

1. In the vSphere client, open the BIG-IP Manager plug-in.
2. Click the Pending Changes tab.
A list of Queued changes opens.
3. To approve or deny changes (you can approve or deny multiple changes at the same time):
 - a) Click the green checkmark (✓) in each box next to the entry you want to approve.
 - b) Click the red X (✗) in each box next to the entry you want to deny.
This moves the change to the Blacklist (to prevent future matches from queuing it again).
4. Click the **Submit** button.

◆ Note

Accepting changes can take a few moments due to the synchronization of configuration that occurs after making changes.

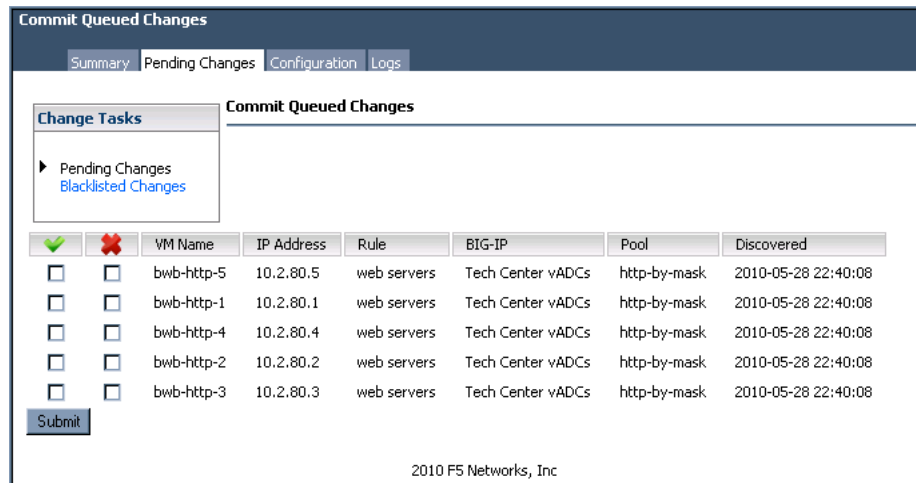


Figure 4 Pending changes page

After declining a change, an entry in the blacklist is added for that match which prevents subsequent polls of vCenter from showing that match.

If you want to allow a virtual machine to be added to a pool in the future that was previously blacklisted, click the **Blacklisted Changes** link to review the list. You can remove items from the Blacklisted Changes list by clicking the red X (x).

Once removed from the Blacklisted changes list, the virtual machine should be matched on the next polling operation and either added to the appropriate pool automatically if the rule is configured to do so, or added to the queue of pending changes again for approval.

Managing virtual machines gracefully with the BIG-IP system

In this section, we show you two options for managing virtual machines with the BIG-IP system without disrupting existing users.

Disabling a virtual machine for maintenance

Using the plug-in, you can easily stop the BIG-IP from sending new connections to a virtual machine (for maintenance or other tasks) without having to powering down the virtual machine. The BIG-IP allows existing connections to continue, but new connections are next to other virtual machines.

To disable a virtual machine for maintenance

1. In the vSphere client, from the **Home** menu, click **Hosts and Clusters**.

-
2. In the navigation pane, right-click a virtual machine that was previously added to a BIG-IP system by rule matching. You should see two additional menu items; *Graceful Shutdown via BIG-IP* and *Disable via BIG-IP* (see Figure 5).
 3. Click **Disable via BIG-IP**. A new window opens to confirm your selection.
 4. Review the virtual machine name and IP information. If this is the correct virtual machine you want to disable, click **Next**. Otherwise, click **Cancel**.

The plug-in instructs all BIG-IP systems to disable the node objects matching any interface IP addresses learned from the virtual machine. This allows existing connections to continue, but new ones to be load balanced to other members of the appropriate pools to which it may belong. When the administrator is content with the state of the VM, the desired actions can be performed on the VM (including rebooting it).

5. When you are ready to add the virtual machine back to service, return to the **Hosts and Clusters** in the vSphere client, right-click the virtual machine, and select **Enable via BIG-IP**. This enables the nodes corresponding to this VM on all BIG-IP devices.

◆ **Note**

If a node was disabled by hand prior to a disable action from the plug-in, a subsequent enable action re-enables it. If this is undesired, the plug-in should not be used to perform the maintenance.

Shutting Down a VM Gracefully

When a virtual machine needs to be shutdown, but it is actively servicing connections it received from a BIG-IP as part of a pool, you can use the plug-in to help perform this operation without significantly impacting users.

This allows existing connections to continue to operate, but causes new connections to load balance to other members of the pools to which the virtual machine belongs. Once per minute, a background process checks all BIG-IPs for the number of active connections to that node and if the sum of those connections is less than the value provided in the following procedure or if the timeout period is met, the VM is gracefully powered off.

To gracefully shutdown a virtual machine

1. In the vSphere client, from the **Home** menu, click **Hosts and Clusters**.
2. In the navigation pane, right-click a virtual machine that was previously added to a BIG-IP system by rule matching. You should see two additional menu items; *Graceful Shutdown via BIG-IP* and *Disable via BIG-IP* (see Figure 5).

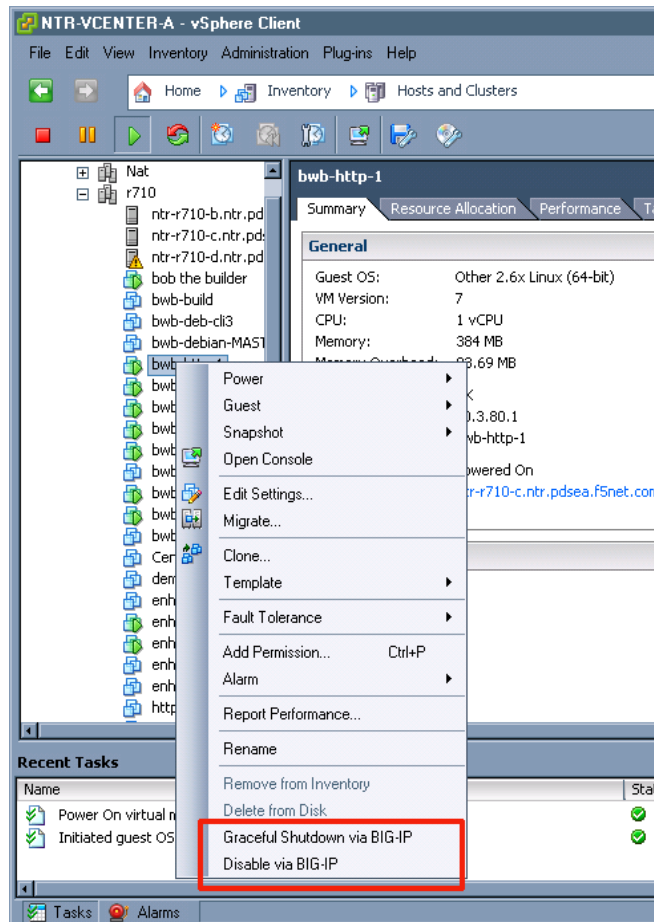


Figure 5 BIG-IP options when right-clicking a virtual machine

3. Click **Graceful Shutdown via BIG-IP**. The Graceful Shutdown wizard opens.
4. Review the VM Name and IP address. If they are not correct, click the Cancel button.
5. In the **Wait for connections to drop below** box, type the maximum number of active connections to the VM that can be tolerated before a shutdown should be initiated.
6. In the **Timeout in minutes before performing action**, type a number of minutes to allow the connections to drop to the level you specified in the previous step before shutting down anyway.
7. Click **Next**.
8. Review the settings, and then click the Next button.
9. Click **Close**.

To gracefully boot and enable via BIG-IP

1. In the vSphere client, from the **Home** menu, click **Hosts and Clusters**.
2. In the navigation pane, right-click the virtual machine that was previously shutdown, and then click **Gracefully Boot and Enable via BIG-IP**. The Boot and Enable wizard opens.
3. Verify that the right virtual machine was selected, and complete the wizard.
4. The virtual machine is booted, and then once per minute, a background process checks whether the VM is booted (whether VMware tools is running and providing IP address information). Once IP information is available for the VM, the plug-in will enable matching node objects for the VM.

◆ Note

Any previously disabled nodes matching this VM are enabled again after booting using the BIG-IP. If this is undesired, do not use the plug-in to manage this shutdown and boot procedure.

Appendix A: Frequently Asked Questions

- ◆ *Does the plug-in remove nodes and pool members from BIG-IPs if a virtual machine is removed?*

No, the plug-in does not delete any objects on the BIG-IP devices. However, if a virtual machine is removed, any monitoring performed by a BIG-IP system should fail, causing traffic to be load balanced elsewhere.

- ◆ *Can the plug-in manage VMware ESX and ESXi hosts outside of a vCenter environment?*

No, the plug-in requires vCenter. Even though the APIs are the same between ESX/ESXi and vCenter, vSphere client plug-ins only work with vCenter.

- ◆ *Can the plug-in be accessed via HTTP outside of a vSphere client?*

No, the plug-in was written in such a way that it assumes it is running within the context of a vSphere client.

- ◆ *How can I replace the SSL key and certificate that is used by the plug-in so that users aren't warned when using the default self-signed certificate?*

The key and certificate are stored in `/var/lib/f5` as `plug-in.key` and `plug-in.crt`. If you replace those files and restart the web server (`sudo /etc/init.d/httpd restart`), the new key and certificate will be used.

- ◆ *Is the source code to the plug-in available?*

Yes, the source code is available as Perl scripts on the vMA host running the plug-in. Look in `/var/lib/f5/` and `/usr/lib/perl5/site_perl/5.8.8/F5plugin.pm`

- ◆ *If my virtual machines have more than one virtual interface and thus more than one IP address, and a rule matches the virtual machine that is not based on the IP (name regex or custom attribute), are all IP addresses added to the pools?*

If the rule is configured to automatically add the members, it will add all interface IP addresses that are learned. If configured to require confirmation, an entry will be added for each IP address and the different interfaces can be approved or denied as desired.

- ◆ *How often do background tasks run for the plug-in?*

VMware vCenter is polled for information about its virtual machines every 5 minutes. BIG-IP devices are polled for the number of connections to a node every minute.

When a VM is booted up via the plug-in, the availability of IP addresses via VMware Tools is polled once per minute. Every night at 2am, the logs older than 7 days are purged.

◆ *Can the frequency of background jobs be changed?*

Yes, but changing the periods of these jobs to be less than the default is not supported by F5. Also be warned that making these operations occur too quickly can lead to unpredictable results, and each environment will respond differently based on the size of the installation.

SSH to the vMA instance hosting the plug-in as the vi-admin user and run the following command: **gsudo crontab -e** and change the frequency as desired.

◆ *How do I change the level of logging that is performed by the plug-in?*

By default, the log level is 6 (informational). To change it to a different value, edit the **F5plugin.pm** and change the line for **\$MAX_DEBUG_LEVEL** to the desired level. Any calls to log with a debug level higher than the configured max will be discarded and thus not committed to the logs.

◆ *How do I manipulate the VMware credential store by hand outside of the plug-in?*

This action is not supported and should not be necessary, but should an unexpected issue occur where the credential store needs to be changed because the plug-in is unavailable, you can use the script provided by VMware in **/usr/lib/vmware-vcli/apps/general/credstore_admin.pl**.

◆ *Can I manipulate the plug-in's authentication database manually?*

This action is not supported, though an engineer with knowledge of basic SQL should be capable. **sqlite3 /var/lib/f5/f5.db** provides access to the database, and the **users** table contains this data.

◆ *What kind of an audit trail is left behind by changes made by the tool?*

Access to BIG-IP devices is performed using iControl, and all such calls are made using the username and password stored for a particular BIG-IP or pair of BIG-IP devices. Likewise, all changes and queries to VMware vCenter are made using the credentials stored in the VMware credential database for that system. Because of this, all changes that are logged will show up as one of these users and not as the user that is logged into vCenter or the plug-in.

◆ *Why does the plug-in require an additional login?*

It was decided the actions that are possible using the plug-in needed some additional authentication because they interacted with other devices outside of VMware vCenter. It was anticipated that some situations would arise where a user could authenticate to the vSphere client that wouldn't need access to the BIG-IP plug-in.

Also, because the plug-in is implemented over HTTP, for security reasons denying unauthorized users bypassing the vSphere client was necessary. Users of the plug-in and users within vSphere are handled separately.

◆ ***How are changes to the pools on pairs of BIG-IPs kept in sync?***

If a pair of BIG-IP devices is defined in the plug-in, changes are attempted against the first one that is defined. If that system does not respond or a login cannot occur, the change is attempted against the second system. No attempt is made to communicate with the active or the standby specifically. Once the change is finished, a configsync is initiated to keep the peer system current.

◆ ***How are the connection counts retrieved for a graceful shutdown?***

In this case, whether a system is active or standby is considered when querying a BIG-IP device for stats. The status of the first unit is retrieved, and if active, its stats are collected, but if it is standby, the stats are retrieved from the peer unit.

This occurs for every pair of BIG-IPs and the sum of the current connections will be used to make the determination.

◆ ***What changes are made to the vMA by the plug-in?***

The installer lists what sorts of changes it is making as it performs them, but essentially the steps are:

1. Install additional RPMs
2. Install additional perl modules
3. Create necessary directories for the plug-in
4. Alter the local firewall policy to allow https connections
5. Generate a key and self-signed certificate for SSL
6. Configure the web server to start on every boot
7. Configure the web server for SSL
8. Register the plug-in with VMware vCenter

◆ ***What is the “bigip_managed” custom attribute used for and what do the different values represent?***

This virtual machine custom attribute is added by the plug-in for each virtual machine that is added to a pool by the plug-in. It is used by the plug-in to inform the vSphere client what extra menu items to show when a VM is right-clicked. A value of **1** means the VM is enabled and operating. A value of **2** means the VM has been disabled. A value of **3** means the VM has been disabled and powered off. Users should not need to change this value manually, but for VMs that already belong to pools before a rule matches them, it may be useful to set the custom attribute by hand to allow the plug-in to manage them.

◆ ***I previously registered a copy of the plug-in with my vCenter and now I want to do it again for another instance of vMA. How do I do that?***

First, the old plug-in must be unregistered from vSphere, as a second registration will not succeed. If the original plug-in is available still, this can be done through the plug-in in the vSphere client by accessing the Configuration tab and using the **Remove** option.

If the plug-in is not accessible but still registered, you can use a perl script to unregister the original plug-in. The script is originally distributed by VMware, and provided as a courtesy as part of the plug-in's installer at `/var/lib/f5/util/registerplug-in.pl`. To run it, run the following commands after opening an SSH connection to the plug-in's vMA host:

```
# export VI_USERNAME=<vcenter username>
# export VI_PASSWORD=<vcenter password>
# export VI_SERVER=<vcenter ip or hostname>
# /var/lib/f5/util/registerplug-in.pl --action remove --key \
com.f5net.pdsea.ntr.manager
```

Substitute an administrator's username and password as well as the vCenter hostname or IP address where appropriate. Once completed, log out to clear out your shell's environment that contains the sensitive data for vCenter.

◆ ***What happens when I remove the plug-in from my vCenter instance via the “Configuration-->Remove” option?***

When the plug-in is removed from vCenter using the functionality in the vSphere client, it unregisters the plug-in from vCenter, which causes any new connections to the vCenter via a vSphere client to not show the plug-in.

Additionally, the database of configuration for the plug-in is purged, as well as login details for vCenter and BIG-IP devices. The packages and files placed on the vMA as part of the installation are not deleted.

◆ ***Can the plug-in manage Virtual Edition BIG-IPs or is it restricted to appliances and chassis?***

The plug-in can manage any BIG-IP device running at least v9.0 of F5's TMOS software regardless of whether it is an appliance or a virtual machine.

Appendix B: Additional Software Components

In addition to the software provided with vMA (see the documentation for vMA for a complete listing of that software's components), the BIG-IP plug-in for VMware vSphere includes the following unmodified packages from the 5.0 repository of CentOS:

- apr-1.2.7-11.el5_3.1.x86_64.rpm
- apr-util-1.2.7-11.el5.x86_64.rpm
- distcache-1.4.5-14.1.x86_64.rpm
- httpd-2.2.3-43.el5.centos.x86_64.rpm
- mailcap-2.1.23-1.fc6.noarch.rpm
- mod_ssl-2.2.3-43.el5.centos.x86_64.rpm
- openssl-0.9.8e-12.el5_4.6.x86_64.rpm
- perl-DBI-1.52-2.el5.x86_64.rpm
- postgresql-libs-8.1.18-2.el5_4.1.x86_64.rpm

For licenses and source code, please consult with the CentOS project.

The following Perl modules are also provided, as taken from CPAN:

- HTML-Template-2.9
- NetAddr-IP-4.028

Their licenses and source code are provided at CPAN.

Due to requiring tools not present on vMA that themselves have significant prerequisites, an additional RPM providing Perl support for SQLite is provided from: <http://dag.wieers.com/rpm/packages/perl-DBD-SQLite/>

Specifically, the package is named

perl-DBD-SQLite-1.14-1.el5.rf.x86_64.rpm and is available under the same terms as the corresponding module on CPAN.

A summary of licensing details for included software is available at **/var/lib/f5/licenses.txt**.