



**nworks**

Smart Plug-in for VMware  
for HP OpenView Operations for Windows  
Version 3 Upgrade Guide

Edition 1.0.01

July 2007



---

# Contents

---

<b>1</b>	<b>Introduction .....</b>	<b>5</b>
<b>2</b>	<b>Upgrade Process .....</b>	<b>5</b>
2.1	To Upgrade the SPI for VMware for OVOW Version 2 to Version 3 .....	6
2.2	To Upgrade the SPI for VMware for OVOW Version 3.x to Version 3.1.4 .....	10



---

# 1 Introduction

---

This document outlines the steps necessary to upgrade the nworks Smart Plug-in for VMware for HP OpenView Operations for Windows (SPI for VMware for OVOW) from Version 2 to Version 3.

Keep the following points in mind:

- The Virtual Infrastructure Collector (VIC) implements new performance classes. Old coda data classes are preserved, but not updated by the VIC. The effect is that the 2.x historical data is not deleted, but is not updated or accessible through the graphs or reports.

**Note:** Please note that the new reports include only data from the 3.x Collector, and will not contain data collected by the 2.x version. You can save the reports generated before the upgrade to another location so that they are available after the upgrade. The reports are located here:  
`%OvDataDir%webpages\VM`

- All of the information associated with the managed ESX Servers (Version 2 and Version 3.0.1) and VirtualCenter Server (Version 1) must be validated using the Virtual Infrastructure Collector Configuration Component (VICConfig) before the VIC will manage them.

---

## 2 Upgrade Process

---

This section contains the following two upgrade procedures:

- To Upgrade the SPI for VMware for OVOW  
Version 2 to Version 3
- To Upgrade the SPI for VMware for OVOW  
Version 3.x to Version 3.1.4

## 2.1 To Upgrade the SPI for VMware for OVOW Version 2 to Version 3

### 1. For each VEM, do the following:

- a. Save the SPI for VMware license key.
  - i. Start the Configuration component.
  - ii. Select the **Licensing** tab.
  - iii. Copy the existing license key to a file for later use.
  - iv. Exit the Configuration component.
- b. Use Add/Remove programs to uninstall the nworks Virtual Infrastructure Collector (VIC). This process could take up to 5 minutes, depending on where the Collector is in the collection cycle.

**Note:** You can monitor the nworksVIC process with Windows Task Manager to know when it exits. This process takes a few minutes.

- c. Install the new Virtual Infrastructure Collector (VIC). When prompted for a license key, use the license key that you saved in step 1a.
- d. Install the new Virtual Infrastructure Collector Configuration Component (VICConfig). On the last installation screen, select the option to start VICConfig.

**Note:** VICConfig is a windows application that must be run on the VEM.

- e. In VICConfig, select the **System Config** tab to display a list of systems, ESX Servers, and VirtualCenter Servers. This is the list of all systems managed by the Version 2 Virtual Infrastructure Collector (VIC). You must validate the system before the VIC will manage them.

At this point, there are several choices on how to manage the ESX Servers. Your choice depends on what type of data you want from the ESX Servers and ease of administration. You can:

- Continue to directly manage ESX Servers (Version 2 and Version 3).

If you choose to directly manage the ESX Servers, you must maintain username/password information for each ESX Server using VICConfig. By directly connecting to the ESX Servers, you can gather file system information and manage ESX Server processes. This is not possible when managing an ESX Server through VirtualCenter. It is not possible to collect VMware Cluster or VMware Resource Pool information through directly managed ESX Servers. Furthermore, if you manage an ESX Server directly and through VirtualCenter, you must turn off Metrics and Events for the ESX Server. If you don't, the VIC will get duplicate information from the ESX Server and the VirtualCenter Server managing the ESX Server.

- Manage ESX Servers through VirtualCenter Server (Version 2 only).

If you choose to manage the ESX Servers through a VirtualCenter Server, then you only need to maintain username/password information for the VirtualCenter Server password. VirtualCenter takes care of all authentications to the individual ESX Servers. Using VirtualCenter Servers to manage ESX Servers does not allow you to manage non-VMFS file systems or ESX Server process on the ESX Servers themselves.

- Do both.  
If you choose to manage the ESX Servers directly and through a VirtualCenter Server, Metrics and Events must be unchecked at the ESX Server level to avoid duplicate performance and event information.
- f. For each system in the list:
  - i. Select the system.
  - ii. Click **Edit**.
  - iii. Click **Validate**.
  - iv. After validation has completed, select the types of data to be collected by VIC from the system:
    - **Metrics**—Performance data (no VMware Cluster or VMware Resource Pool data from directly managed ESX Servers).
    - **Events**—Event data.
    - **File system**—File system data (only VMFS file system data available from VirtualCenter servers).
    - **Process Monitor**—Processes running on the ESX Server Console OS. This option is only available for directly managed ESX Servers.
  - v. Click **OK** to update the configuration.
- g. To add new systems such as VirtualCenter Servers running version 2.0.1 or later:
  - i. Click **Add**.
  - ii. In the Server Name field, enter the IP address or fully qualified domain name.
  - iii. In the User Name field, enter the user name to access the server.  
For directly managed ESX Servers, this can be any valid user.  
For VirtualCenter Servers, this can be any valid user.
  - iv. In the two Password fields, enter the password.
  - v. In the Communication Port field, enter the number of the communication port the VIC uses to communicate with the server. Generally speaking, these are:
    - **902**—ESX Server Version 2
    - **443**—ESX Server Version 3
    - **8443**—VC Server Version 1
    - **443**—VC Server Version 2 (clean install)
    - **8443**—VC Server Version 2 (upgraded from VC Server Version 1)
    - **0**—Collector will check standard ports
  - vi. Click **Validate**.
  - vii. Make any adjustments to the Metrics, Events, Filesystem, or Process Monitor check boxes.
  - viii. Click **OK** to save the configuration.

- h. At this point, the VIC is not running. Before starting the VIC, the OVOW Management Server must be updated with the SPI for VMware OVOW Version 2 policies. Once the OVOW Management Server has been configured correctly and the Version 3 policies are deployed to the VEM, the VIC is started.

## 2. Upgrade the OVOW Management Server using the following steps:

You can upgrade the OVOW Management Server in two ways.

One approach is to remove all of the elements of the SPI for VMware Version 2 from the Management Server. This includes policies, tools, and other items as described in the SPI for VMware Administrator Guide under “Uninstalling the Management Server Component from OVOW.”

Another approach is to remove the policies deployed to the VEMs and replace them with the new policies. Although they are no longer being used, all SPI for VMware Version 2 policies remain on the Management Server. This is the approach outlined in the following procedure.

- a. On the OVOW Management Server, install **VMSPiOVOWSetup.msi**.
- b. Open the OVOW console and navigate to **Nodes > SPI for VMware Collectors**. For each VEM listed in the OVOW console tree:
  - i. Select the VEM.
  - ii. Right click and select **View > Policy Inventory**.
  - iii. You are going to remove all of the SPI for VMware policies from the VEM. There are several ways to find all of the SPI for VMware policies. The easiest way is to sort the policy inventory by version from highest to lowest version number by clicking on the column header twice. The SPI for VMware policies will be in the 200-230 range.
  - iv. Select all of the SPI for VMware policies, right click, and select **All Tasks > Remove from node**.
  - v. In the Confirm policy removal dialog box, click **Yes**.
  - vi. Select the VEM, right click, and select **View > Active Messages**.
- c. Once you have removed all of the SPI for VMware policies from each VEM, open the Node Configuration Editor. The SPI for VMware Version 3 installs a new node group: SPI for VMware VEM. Using the Node Configuration Editor, remove each Version 2 VEM from the SPI for VMware Collectors node group and add each Version 3 VEM to the SPI for VMware VEM.

The process of adding Version 3 VEMs to the SPI for VMware VEM node group triggers the deployment of SPI for VMware Version 3 policies to the VEM.

- i. In the Node Configuration Editor, add each Version 3 VEM to the SPI for VMware VEM and remove each Version 2 VEM from SPI for VMware Collectors. If you have upgraded a Version 2 VEM to a Version 3 VEM, simply drag the VEM from one group to the other.
  - ii. When you are satisfied that you have reconfigured the node list correctly, click **OK** to commit the changes.
  - iii. At this point, all nodes placed in the SPI for VEM are updated with SPI for VMware Version 3 policies required to manage the VIC on the VEM.
- d. With the SPI for VMware Version 2 policies removed from the VEMs and the SPI for VMware Version 3 policies deployed to the VEMs, configuration, performance, event, and state information starts flowing from the VEMs to the OVOW Management Server. Now it is time to start the VIC on the each VEM.

**3. Start the VIC on each VEM.**

- a. Open VICConfig.
- b. Click the Global Settings tab.
- c. Click **Resend**, which tells the VIC to resend the configuration XML to the OVOW Management Server.
- d. Click the Collector tab.
- e. Click **Start**.

**4. Verify operation on the OVOW Management Server console.**

- a. Open the OVOW console.
- b. Review events in the events browser.
- c. Review the service map.
- d. Review performance graphs.

**5. Update reports**

The approach on reports depends on if you are using OVOW Reporter Lite or Reporter.

- a. For OVOW Reporter Lite:
  - i. On the OVOW console, use Add/Remove Programs to remove the SPI for VMware Reports Component.
  - ii. Install **VMSPIReports.msi**.
- b. For Reporter:
  - i. On the Reporter server, use Add/Remove Programs to remove the SPI for VMware Reports Component.
  - ii. Install **VMSPIReports.msi**.

## 2.2 To Upgrade the SPI for VMware for OVOW Version 3.x to Version 3.1.4

**Special Instructions for Upgrading from 3.0.x to 3.1.x:** In VIC version 3.1.0, nworks added, changed names, and changed lengths of some Coda class elements to prevent data truncation and improve compatibility with OVPA. Therefore, if you have installed version 3.0.0 to 3.0.9 of the Collector at any point, you are required to delete the VMSPI Coda classes to avoid problems (usually expressed as OV110 alerts in OVO). Deleting the VMSPI Coda classes will not have any impact on other Coda classes.

To preserve as much VMSPI Coda class data as possible, gather the Coda data into OVOW Reporter-Lite or Reporter using `gathercoda` with the `-h` option for each VEM (Collector system). The `-h` option gathers all Coda data from the OVO agent up until the last hour. Normally, OVOW Reporter-Lite and Reporter gather Coda data up until midnight of the previous day. The `gathercoda` command is on the PATH, so it can be executed anywhere on the command line on the OVOW management server or Reporter system:

```
gathercoda -h <vem-hostname>
```

Graphing and OVPM use data stored in Coda classes. Deleting the VMSPI Coda classes resets the starting point of the graphs.

### 1. On the VEM, remove the Collector component, the Configuration component, and the VMSPI Coda classes:

- a. Open the Configuration UI and copy the license key to a text file for use on the installation of the new version of the Collector component.
- b. Uninstall the Collector using Add/Remove Programs.
- c. Uninstall the Configuration GUI using Add/Remove Programs.
- d. Remove the VMSPI metrics and classes. In order to do this, you need to find the `ddf1bd.mwc` file.
  - i. Search the VEM system for the `ddf1bd.mwc` file. With OVOW deployed agents, the default is in `%OvAgentDir%\conf\dsi2ddf`.
  - ii. Use Notepad to open `ddf1bd.mwc`. Look for a line starting with `DATASOURCE=VMSPI LOGFILE=` and copy the information following `LOGFILE=` for use in the `ddfutil` command.
  - iii. Open a command window and navigate to the directory containing `ddfutil`. On OVOW systems, this will be in the following directory:  
`%ovagentdir%\bin\instrumentation`
  - iv. Execute the following command using the exact line from the `DATASOURCE=VMSPI LOGFILE=` entry of `ddf1bd.mwc`. Quote the log file name:  
`ddfutil "fully qualified name of LOGFILE from ddf1bd.mwc" -rm all`

**Note:** The log file does not exist on the system. It is a required parameter and must match the name in `ddf1bd.mwc`.

2. **On the OVOW management server, perform the following steps to update the VMSPI components:**
  - a. Install the updated version of the OVOW management component.
  - b. Open the OVOW console.
  - c. Navigate the console tree to **Nodes > SPI for VMware VEM** and, for each VEM listed in the node group, do the following:
    - i. Select the node and view the Policy Inventory.
    - ii. Sort the Policy Inventory by Version. The version numbers of the VMSPI policies are 3XX. This groups all of the SPI for VMware policies together.
    - iii. Select the SPI for VMware policies and use the shortcut menu **Remove from node**.
  - d. Navigate the console tree to **Policy Management > Policy groups > SPI for VMware > VMware Enterprise Monitor (VEM)**
  - e. Select the Auto-Deploy policy group and deploy to each VEM.
  - f. Select any other SPI for VMware policies that you want to deploy to the VEMs.
3. **Back on the VEM, install the Collector component and the Configuration component.**
  - a. Install the latest version of the Collector component. Use the license key saved in the previous step.
  - b. Install the latest version of the Configuration component.
  - c. Use Configuration component to verify the configuration and start the Collector component.