Understanding the Relationship with Domain Managers

Prime Central for HCS reports the events generated by underlying domain managers. Domain managers may also discover topology and relationships between components within its domain, which offer set of diagnostic and tracing tools to assist operator with troubleshooting issues within technology domain.

It may be often necessary to log on to the specific domain manager to understand and analyze the problem in detail. The cross-launch functionality allows the user to log on to the domain manager. Prime Central for HCS supports single sign-on for CUOM and DCNM-SAN. When you cross-launch Infrastructure Monitoring, DCNM-LAN or UCSM, you must sign in by entering the appropriate username and password. The following domain managers are supported:

- Cisco Unified Operations Manager—A product from the Cisco Unified Communications Management Suite. It provides a comprehensive and efficient solution for network management and allows you to monitor Cisco Unified Communications deployments.
- Cisco Unified Computing System Manager—It provides unified, embedded management of all software and hardware components of the Cisco Unified Computing System, across multiple chassis and thousands of virtual machines.
- Data Center Network Manager—It is a management solution that increases overall data center infrastructure uptime and reliability. In this way it improves business continuity and provides the following capabilities:
  - Automates the provisioning process
  - Proactively monitors the SAN and LAN by detecting performance degradation
  - Secures the network
  - Streamlines the diagnosis of dysfunctional network elements.

Note DCNM is an optional component in Prime Central for HCS 9.2.1. If you are not using DCNM in your deployment, skip tasks and sections related to DCNM.

This chapter contains the following sections:

Prime Central for HCS uses the limited version of the IBM Tivoli Netcool/OMNIbus technology. Some of the windows in the Alarm Browser and Alarm Report portlets have a Help button that launches the IBM Tivoli Netcool online help. Please see the Cisco license agreement for the limitations.

The following table outlines the software and hardware details of the domain managers managed by Prime Central for HCS:

Table 4-1 Domain Manager—Prerequisites

Domain Manager	Software Version	Hardware Version	Other Requirements
Cisco Prime Unified Operations Manager	9.0	UCS 5108/ VMWare	Windows Server 2008, 32-bit
Cisco Unified Computing System Manager	2.0	UCS 5108/ VMWare	None
vCenter	4.x	UCS 5108/ VMWare	MySQL or Microsoft SQL (refer to VMWare site for supported versions) - run on dedicated VM Windows 200x Server (refer to VMWare site for supported versions)

The following table outlines the software and hardware details of DCNM:

Table 4-2 DCNM-SAN and LAN—Prerequisites

Domain Manager	Software version	Hardware version	Other requirements
DCNM-SAN	6.1.2	UCS 5108/ VMWare	64 bit or Red Hat Linux 5.5, 64 bit. Optional Oracle 11g Enterprise or RAC (PostgreSQL 8.x comes with DCNM). Client can run on Windows or Linux based PC.
DCNM-LAN	6.1.2	UCS 5108/ VMWare	64 bit or Red Hat Linux 5.5, 64 bit. Optional Oracle 11g Enterprise or RAC (PostgreSQL 8.x comes with DCNM); Oracle recommended for DCNM federation and large deployments. Client can run on Windows or Linux based PC.

Note DCNM is an optional component in Prime Central for HCS 9.2.1. If you are not using DCNM in your deployment, skip tasks and sections related to DCNM.

For more information on Domain Managers, see http://preview.cisco.com/en/US/partner/docs/voice_ip_comm/hcs/9_0_1/Assurance_Reference_Guide.pdf

Cross Launching to Domain Managers

Prime Central for HCS supports cross-launch of underlying domain managers. To enable domain manager cross-launch, each domain manager must first be manually added in HCM-Fulfillment.

Your privilege to launch the domain manager is similar to the privilege that you have in Prime Central for HCS. Table 4-3 lists the mapping between the roles in Prime Central for HCS and the roles in domain managers. HTTP and HTTPS protocol-based cross launching to multiple versions of domain managers is supported. You can access the domain managers from Prime Central for HCS in either of these ways:

- From Domain Manager Global Cross Launch portlet:

  To view the Domain Manager Global Cross Launch portlet, go to **Assure > Global Cross Launch.**

  The portlet displays the list of domain managers configured in Prime Central for HCS. Select a domain manager and then select the cross-launch option. Depending on the option you choose, the corresponding domain manager is cross-launched. The names of domain managers are listed the way they are entered in HCS-F. UCSM and DCNM-LAN uses JNLP-based client; if you are cross launching UCSM and DCNM-LAN, you are prompted to open a JNLP file. Choose the default option (Open with: Java (TM) Web Start Launcher) and click OK.

- From a specific event listed in event portlets:

  From an event enlisted in the events portlet, you can cross-launch to the respective domain manager. Prime Central for HCS supports single sign-on for Cisco Prime Unified Operations Manager and DCNM-SAN. When you cross-launch Infrastructure Monitoring, DCNM-LAN or Cisco Unified Computing System Manager, you must sign in by entering the appropriate username and password. You must cross-launch the Infrastructure Monitoring domain manager by using only the option available in the menu bar. Do not cross-launch from the Global Cross-launch portlet.

  When you click a domain manager listed in the portlet, the following pages open, depending on the domain manager you are trying to launch:

  - Cisco Prime Unified Operations Manager—Cross-launches to the main event page.
  - DCNM-LAN—Cross-launches to the main application.
  - DCNM-SAN—Cross-launches to the main page.
  - Cisco Unified Computing System Manager—Cross-launches to the main application.

Table 4-3 User Roles Mapping between Prime Central for HCS and Domain Managers

Domain Manager	Prime Central for HCS Operator	Prime Central for HCS Administrator
Cisco Prime Unified Operations Manager	Network Operator	Super Admin
DCNM-SAN (Optional)	Network Operator	SAN Admin
DCNM-LAN (Optional)	JNLP-based cross-launch; credentials have to be manually entered.	
Cisco Unified Computing System Manager	JNLP-based cross-launch; credentials have to be manually entered.	
Infrastructure Monitoring	JNLP-based cross-launch; credentials have to be manually entered.	

For more information, see
http://cisco.com/en/US/partner/docs/voice_ip_comm/hcs/9_0_1/Assurance_Reference_Guide.pdf

CUOM Third-Party Monitoring

Prime Central for HCS is compatible with third-party monitoring support provided by Cisco Prime Unified Operations Manager. The prerequisites for third-party monitoring are as follows:

- Host-Resource-MIB for resource monitoring—Implementation is widely available and can be enabled on any Windows or Linux server.
- SYSAPPL-MIB (for process monitoring)—Available only in UC applications such as HCM-F and ELM. The process monitoring feature is enabled only when this MIB is available.
- Devices must be available in Cisco Prime Unified Operations Manager for monitoring.

The following events are generated by Cisco Prime Unified Operations Manager for third-party monitoring:

Table 4-4 Third-Party Events Supported by Cisco Prime Unified Operations Manager

CUOM Event	Domain Manager Severity	EventTypeID
HighCollisionRate	Critical	OM_Gen_App_Resources
HighBroadcastRate	Critical	OM_Gen_App_Resources
HighErrorRate	Critical	OM_Gen_App_Resources
HighDiscardRate	Critical	OM_Gen_App_Resources
HighBufferUtilization	Critical	OM_Gen_App_Resources
HighBufferMissRate	Critical	OM_Gen_App_Resources
HighBackplaneUtilization	Critical	OM_Gen_App_Resources
ServiceDown	Critical	OM_Gen_Processes
OperationallyDown	Critical	OM_Gen_Serviceability
InsufficientFreeHardDisk	Critical	OM_Gen_App_Resources

Table 4-4 Third-Party Events Supported by Cisco Prime Unified Operations Manager (continued)

CUOM Event	Domain Manager Severity	EventTypeID
HighUtilization (Processor)	Critical	OM_Gen_App_Resources
Unresponsive	Critical	OM_Gen_Servicability
InsufficientFreeVirtualMemory	Critical	OM_Gen_App_Resources
InsufficientFreeMemory	Critical	OM_Gen_App_Resources

Cross-Launching to Infrastructure Monitoring

Infrastructure Monitoring (IM) monitors Contact Center, vCenter, Cisco Prime Unified Operations Manager, Cisco Unified Computing System Manager, and vCenter VMs and ESXi hosts. The Contact Center is made up of four primary components (UCCE, CVP, CCMP, and CUIC). Both UCCE and CVP are monitored by Cisco Prime Unified Operations Manager. CUIC and CCMP will be monitored via Infrastructure Monitoring, and monitoring will be limited to critical service down only. Infrastructure Monitoring is based on a client-server-agent architecture. You have to log in using Infrastructure Monitoring credentials. Infrastructure Monitoring does not support single sign-on.

Infrastructure Monitoring Components

Client

The Infrastructure Monitoring client is a Java-based user interface for viewing and monitoring your enterprise network. The monitoring client will be started as a Java Webstart application, which downloads the installable software from the Infrastructure Monitoring Server, installs it, and then makes it available as a desktop application.

Server

The Infrastructure Monitoring client connects to its application server, the Infrastructure Monitoring Server. The Infrastructure Monitoring Server is a collection of software services for the client that enables retrieval, manipulation and analysis of data from the monitoring agents on your enterprise. This server connects to the IM Server, which acts as a collection and control point for alerts received from the monitoring agents, and collects performance and availability data. The main, or hub, IM Server correlates the monitoring data collected by agents and remote servers and passes it to the Infrastructure Monitoring Server for presentation and your evaluation.

Agent

IM Agents are installed on the systems whose applications or resources you want to monitor. The monitoring agent collects the monitored data, and passes it to the IM Server to which it is connected. The client gathers the current values of the monitored properties, or attributes, and displays them in views. It can also test the values against a threshold and display an event indicator when that threshold is exceeded.

Infrastructure Monitoring Window

Use this topic to familiarize yourself with the elements of the Infrastructure Monitoring window. The Infrastructure Monitoring window displays information about monitored resources in your enterprise. On the left is the Navigator, which shows the arrangement of your monitored network and allows you to

access information collected by different agents on your monitored systems. On the right is a workspace. The workspace can be divided into as many smaller frames, or panes, as you can reasonably fit inside the window. When you select an item in the Navigator, a new workspace opens with a set of views for that item.

Title bar

In browser mode, the title bar shows the name of the workspace. In desktop mode, the title bar shows the name of the workspace, the name and port number of the Infrastructure Monitoring Server, and the user name. For example, NT Cache Details - mars:14000 - JONDO tells us that the NT Cache Details workspace is open and the user JONDO is connected to the Infrastructure Monitoring Server named mars through port number 14000.

Menu bar

Infrastructure Monitoring has a menu bar that includes the following four menus: File The File menu has options for working with workspaces, setting a trace, and exiting the Infrastructure Monitoring.

- Edit—The Edit menu has editing options for workspace properties, historical data collection configuration, policies, situations, user IDs, queries, and object groups.
- View—The View menu has options for opening other workspaces for a Navigator item, hiding or showing the toolbars and status bar, refreshing the data in this workspace, turning off sound for events, and for opening other Navigator views.
- Help—The Help menu opens the Infrastructure Monitoring Help, a 10-minute tour to give you some hands-on experience

Also available are menus that open when you right-click an item in the Navigator or a view in the workspace. If your user ID does not have View or Modify permission for a function or does not have Workspace Author Mode permission, you will not see certain items in the menus, including the pop-up menus. For example, if you have no Workspace Author Mode permission, the Properties menu item is not displayed.

Toolbar

Your user ID requires Workspace Author Mode permission to create and maintain workspaces, including links. The toolbar has four tool groupings and they are listed below:

Icon	Description
	Returns to the previous workspace. Click the list button to see and select from a history of workspaces as they were opened. The selected workspace refreshes with the most recent sampling data from the agent. This icon is not available in browser mode. Use the Back tool in your browser instead.
	Forward Arrow—Moves forward to the next workspace. Click the list button to see and select from a history of workspaces that were opened after this one. The selected workspace refreshes with the most recent sampling data from the agent. This icon is not available in browser mode. Use the Forward tool in your browser instead.
	Desktop mode only: Opens a new Infrastructure Monitoring window. Keyboard shortcut: Ctrl + N.
	Saves the current workspace properties, including any changes to views and links. Keyboard shortcut: Ctrl + S.
	Opens the Properties editor for this workspace. Keyboard shortcut: Ctrl + R.
	Opens the History Collection Configuration window to define and start historical collection for the specified monitoring agents and attribute groups. Keyboard shortcut: Ctrl + H.
	Opens the Workflow editor to customize policies for automation. Keyboard shortcut: Ctrl + W.
	Opens the Situation editor for viewing, editing, and creating situations that alert you when the conditions they describe have been met. When you use this method to open the Situation editor instead of through the Navigator item pop-up menu, the situation is not associated with any Navigator item. Keyboard shortcut: Ctrl + E.

Icon	Description
	Opens the Administer Users window for adding and removing user IDs and changing user permissions. Keyboard shortcut: Ctrl + U.
	Opens the Query editor. When you use this method to open the Query editor (instead of opening the Query editor through the Properties editor), you can view and customize queries but you cannot assign them to table and chart views. Keyboard shortcut: Ctrl + Q.
	Opens the Object Group editor for creating and working with groups, such as managed systems and situations. Keyboard shortcut: Ctrl + G.
	Pauses or resume automatic refresh of the data in the workspace views. The tool is disabled if no refresh interval has been set for the workspace (View Refresh Every). Keyboard shortcut: Shift + Esc.
	Reloads the saved workspace and refreshes the data in the workspace views. Keyboard shortcut: F5.
	Stops loading the workspace. If the workspace is set to refresh at intervals (View Refresh Every), the refresh stops until the next interval. Keyboard shortcut: Shift + Esc.
	Turns sound off or on for open events. Enabling or disabling sound for an event is controlled through the Situation editor.
	The IM event viewer integrates events from the IM Console Server with those from the IM Server.
	The table view shows a column for each attribute requested by the query and one or more rows of data. You can also get table views to show data samplings over a period of time.
	Replaces the view you click next with a pie chart, the properties of which you can customize for the data you want to include.
	Replaces the view you click next with a bar chart, the properties of which you can customize for the data you want to plot.

Icon	Description
	Replaces the view you next click inside with a plot chart, which you can then customize for the data you want to include.
	Replaces the view you next click inside with an area chart, which you can then customize for the data you want to include.
	Replaces the view you next click with a circular gauge chart, which you can then customize for the data you want to show.
	Replaces the view you next click with a linear gauge chart, which you can then customize for the data you want to show.
	The notepad view is a simple text editor for writing notes about the workspace. The message log view shows the status of events that have been opened on the entire monitored enterprise and can include up to 100 row entries at a time.
	The message log view shows the status of events that have been opened on the entire monitored enterprise and can include up to 100 row entries at a time.
	The situation event console view shows the status of events that have been opened on this branch of the Navigator, such as the state and how long the event has been open.
	The universal message console view displays situation and policy activities as they happen, such as when a situation has been created or deleted or a policy has been activated.
	The graphic view places Navigator items and their alerts as icons on a map or a picture to represent your monitored environment. Alerts show on these icons just as they do in the Navigator.
	The take action view enables you to send a command to a managed system.
	The terminal view starts a 3270 or 5250 session for working with z/OS applications, or a Telnet session for working with the TCP/IP network.

Icon	Description
	The browser view opens the Infrastructure Monitoring integrated browser for accessing Web pages and Web applications.
	A topology view can be added to a workspace to show the arrangement of monitored components associated with its Navigator item. Most Navigator items have at least one topology source available for the topology view, and some have multiple topology sources from which to chose.
	The common event console view is able to integrates events from multiple event repositories.
	For performance analysis, you can specify a time span to use for the workspaces that get opened. Historical navigation mode is easily started and stopped, and you can adjust the time span.
Each view in the workspace also has a title bar that includes these buttons:	
	Brings up the Properties editor for the view. This button does not display if the view has no properties.
	Shows or hides the view toolbar. This button does not display if the view has no toolbar.
	Splits the view horizontally into two separate views.
	Splits the view vertically into two separate views.
	Maximizes the view, at which time the button becomes a Restore button so you can restore the view to its original size.
	Removes the view from the workspace.

Many views have a toolbar of functions that are applicable to that view.

For example, the Time Span tool is displayed for table views, bar charts, and plot charts that query attribute groups that are historical in nature or that have been configured for historical data collection.

You can turn off the display of both the view title bar and toolbar through **View > View Toolbars**.

Navigator

The Navigator Physical view shows the hierarchy of your monitored enterprise, from the top level down to individual groupings of information collected by monitoring agents. Every item in the Navigator has at least one workspace associated with it. When you click an item in the Navigator the default workspace is displayed in the application window.

The Navigator provides a physical view of your monitored network, organized by operating system platform, system type, Infrastructure Monitoring product (agents), and the attribute groups from which the agents can collect information.

Small colored event indicator icons overlay Navigator icons when a situation (a test of certain conditions) becomes true. As you move up the Navigator hierarchy, multiple events are consolidated to show only the indicator with the highest severity.

You might see More... indicators in the Navigator. These indicators keep the tree compact so you can see more alerts in the viewable area without having to scroll. Click More... to expand that branch of the tree.

The Navigator toolbar has an Update tool that is enabled when monitoring agents have been added or removed from the managed network and the tree needs to be updated to show them.

Infrastructure Monitoring also comes with a Navigator Logical view that initially shows one Navigator item. To change to the Navigator Logical view, select it from the Navigator view list. You can also edit the Logical view and define new Navigator views for any logical hierarchy.

For example, you might have a Navigator view for Manufacturing and another for Marketing.

The right border of the Navigator view has a button that hides the Navigator and expands the adjacent workspace views to fill the gap. Click to restore its original size. You can also click <*Navigator name*> in the right-most section of the status bar to restore the Navigator view; or right-click it to see a list of Navigator views to select from.

Sometimes, when you rename a blade in vCenter and launch Infrastructure Monitoring, the blade will be available in two names and the old name will be grayed out. To delete the blade, follow the steps below:

Step 1 Click the **Enterprise Navigator** item. The default workspace opens.

Step 2 Click **Workspace** gallery, scroll to **Managed System Status**, and click the workspace.

Step 3 Right-click an OFFLINE row, then click **Clear Offline Entry.**

Workspace

The workspace is the working area of the application window and consists of one or more views.

A view is a pane in the workspace, typically a chart or table showing data collected from a monitoring agent, such as the process detail running on the UNIX operating system. A view can be split either vertically or horizontally into two separate, independent views.

Every item in the Navigator has a default workspace associated with it.

Some items might have multiple workspaces, which are accessible from the Workspace gallery or from the Navigator item pop-up menu.

A workspace can be linked to other workspaces. A link can be context-sensitive, whereby you click a link in a table row or right-click a table row or a chart data series to link to more detailed information about one of the attributes in the row or data series.

Status bar—The status bar has several sections showing the following, starting from the left:

Hub Time, which is the local time at the hub monitoring server

Server Available (or offline if you see a red ?X? over the server icon), which is the status of the connection to the portal server

Workspace name, portal server name, and port number, and the user name. If the user is in workspace administration mode, *ADMIN MODE* is displayed.

If the Navigator view is minimized, a Navigator button is displayed for you to click to restore the named Navigator.

You can turn off the display of the status bar through the View menu.

Monitoring Agents

IM Agents are installed to monitor the resources. The agents and the operating system, subsystem or computer that they are running on are referred to as managed systems.

The Navigator Physical view shows the types of agents installed and running on each managed system.

Some agents also have subagents. In such instances the agent is the managing agent. The agent gathers the current values of the attributes (elements) specified in a view. Gathered attribute values can also be tested against a threshold and display an event indicator when conditions exceed the threshold.

Some agents have fewer than 100 attributes, and many have several hundred. These attribute values are displayed in the table and chart views of workspaces at the system, agent, and attribute group level of the Navigator Physical view. When an attribute value (or range of values) is specified in a situation, as a table threshold, or as a chart or table view filter, Infrastructure Monitoring compares the current value with the value specified and does the following:

If the comparison in the situation is met, then the situation is true and event indicators are displayed in the Navigator.

If the compared value exceeds the threshold specified for the table, the cell is highlighted in red, yellow, or blue.

If the compared value meets the filter condition, it is included in the chart or table display.

Predefined Workspaces and Situations

Predefined workspaces, situations open when you click a Navigator item or select from the Workspace Gallery, are predefined. They provide visual feedback of real-time values from managed systems, and historical values when historical data collection has been configured. They provide a starting point for designing your own workspaces.

Queries

The predefined workspaces are populated with data gathered as a result of queries, which are also predefined. Creating your own queries from these predefined queries enables you to add or remove attributes, apply a sort order, and pre-filter the data to keep data retrieval at a manageable level and to enable you to more easily see data of interest.

Take action commands

Some agents have predefined take action commands, such as the Windows OS agent Start Service and Stop Service commands. They are available for selection and they provide examples of the kinds of actions that you might want to define for maintaining managed systems.

Situations

The tests for conditions that you want to be alerted for are available in the predefined situations. To avoid an overwhelming number of events opening in a newly managed environment and, conversely to avoid missing important events because the comparison criteria was set too low, many of the predefined situations for an agent are not set to start automatically. They remain stopped until you either start them manually or set them to Run at startup. A good way to find out which situations are set to run at startup and which ones are not, is to filter the Situation editor tree with Show Situations, which is available when the Situation editor is opened from the Navigator pop-up menu. As agents report monitoring data, and especially when that data is being collected and stored in a IM Data Warehouse, you can better determine the values and circumstances that are worthy of an alert, such as high CPU activity on a transaction server at peak times.