IBM Tivoli NetView for z/OS
Version 6 Release 1

User's Guide: NetView Enterprise Management Agent

IBM

SC27-2876-00

IBM Tivoli NetView for z/OS
Version 6 Release 1

User's Guide: NetView Enterprise Management Agent

SC27-2876-00

Note

Before using this information and the product it supports, read the information in "Notices" on page 153.

This edition applies to version 6, release 1 of IBM Tivoli NetView for z/OS (product number 5697-NV6) and to all subsequent versions, releases, and modifications until otherwise indicated in new editions.

Contents

Figures

About this publication

The IBM® Tivoli® NetView® for z/OS® product provides advanced capabilities that you can use to maintain the highest degree of availability of your complex, multi-platform, multi-vendor networks and systems from a single point of control. This publication, the *IBM Tivoli NetView for z/OS User's Guide: NetView Enterprise Management Agent*, provides information about using the NetView Enterprise Management Agent.

Intended audience

This publication is for operators and system programmers who use or are responsible for the NetView Enterprise Management Agent.

Publications

This section lists publications in the IBM Tivoli NetView for z/OS library and related documents. It also describes how to access Tivoli publications online and how to order Tivoli publications.

IBM Tivoli NetView for z/OS library

The following documents are available in the IBM Tivoli NetView for z/OS library:

- *Administration Reference*, SC27-2869, describes the NetView program definition statements required for system administration.
- *Application Programmer's Guide*, SC27-2870, describes the NetView program-to-program interface (PPI) and how to use the NetView application programming interfaces (APIs).
- *Automation Guide*, SC27-2846, describes how to use automated operations to improve system and network efficiency and operator productivity.
- *Command Reference Volume 1 (A-N)*, SC27-2847, and *Command Reference Volume 2 (O-Z)*, SC27-2848, describe the NetView commands, which can be used for network and system operation and in command lists and command procedures.
- *Customization Guide*, SC27-2849, describes how to customize the NetView product and points to sources of related information.
- *Data Model Reference*, SC27-2850, provides information about the Graphic Monitor Facility host subsystem (GMFHS), SNA topology manager, and MultiSystem Manager data models.
- *Installation: Configuring Additional Components*, GC27-2851, describes how to configure NetView functions beyond the base functions.
- *Installation: Configuring Graphical Components*, GC27-2852, describes how to install and configure the NetView graphics components.
- *Installation: Configuring the GDPS Active/Active Continuous Availability Solution*, SC14-7477, describes how to configure the NetView functions that are used with the GDPS Active/Active Continuous Availability solution.
- *Installation: Configuring the NetView Enterprise Management Agent*, GC27-2853, describes how to install and configure the NetView for z/OS Enterprise Management Agent.
- *Installation: Getting Started*, GI11-9443, describes how to install and configure the base NetView functions.

- *Installation: Migration Guide*, GC27-2854, describes the new functions that are provided by the current release of the NetView product and the migration of the base functions from a previous release.
- *IP Management*, SC27-2855, describes how to use the NetView product to manage IP networks.
- *Messages and Codes Volume 1 (AAU-DSI)*, GC27-2856, and *Messages and Codes Volume 2 (DUI-IHS)*, GC27-2857, describe the messages for the NetView product, the NetView abend codes, the sense codes that are included in NetView messages, and generic alert code points.
- *Programming: Assembler*, SC27-2858, describes how to write exit routines, command processors, and subtasks for the NetView product using assembler language.
- *Programming: Pipes*, SC27-2859, describes how to use the NetView pipelines to customize a NetView installation.
- *Programming: PL/I and C*, SC27-2860, describes how to write command processors and installation exit routines for the NetView product using PL/I or C.
- *Programming: REXX and the NetView Command List Language*, SC27-2861, describes how to write command lists for the NetView product using the Restructured Extended Executor language (REXX) or the NetView command list language.
- *Resource Object Data Manager and GMFHS Programmer's Guide*, SC27-2862, describes the NetView Resource Object Data Manager (RODM), including how to define your non-SNA network to RODM and use RODM for network automation and for application programming.
- *Security Reference*, SC27-2863, describes how to implement authorization checking for the NetView environment.
- *SNA Topology Manager Implementation Guide*, SC27-2864, describes planning for and implementing the NetView SNA topology manager, which can be used to manage subarea, Advanced Peer-to-Peer Networking, and TN3270 resources.
- *Troubleshooting Guide*, GC27-2865, provides information about documenting, diagnosing, and solving problems that occur in the NetView product.
- *Tuning Guide*, SC27-2874, provides tuning information to help achieve certain performance goals for the NetView product and the network environment.
- *User's Guide: Automated Operations Network*, SC27-2866, describes how to use the NetView Automated Operations Network (AON) component, which provides event-driven network automation, to improve system and network efficiency. It also describes how to tailor and extend the automated operations capabilities of the AON component.
- *User's Guide: NetView*, SC27-2867, describes how to use the NetView product to manage complex, multivendor networks and systems from a single point.
- *User's Guide: NetView Enterprise Management Agent*, SC27-2876, describes how to use the NetView Enterprise Management Agent.
- *User's Guide: NetView Management Console*, SC27-2868, provides information about the NetView management console interface of the NetView product.
- *Licensed Program Specifications*, GC31-8848, provides the license information for the NetView product.
- *Program Directory for IBM Tivoli NetView for z/OS US English*, GI11-9444, contains information about the material and procedures that are associated with installing the IBM Tivoli NetView for z/OS product.
- *Program Directory for IBM Tivoli NetView for z/OS Japanese*, GI11-9445, contains information about the material and procedures that are associated with installing the IBM Tivoli NetView for z/OS product.

- *Program Directory for IBM Tivoli NetView for z/OS Enterprise Management Agent*, GI11-9446, contains information about the material and procedures that are associated with installing the IBM Tivoli NetView for z/OS Enterprise Management Agent.
- *IBM Tivoli NetView for z/OS V6R1 Online Library*, LCD7-4913, contains the publications that are in the NetView for z/OS library. The publications are available in PDF, HTML, and BookManager® formats.

Technical changes that were made to the text since Version 6.1 are indicated with a vertical bar (|) to the left of the change.

Related publications

You can find additional product information on the NetView for z/OS web site at http://www.ibm.com/software/tivoli/products/netview-zos/.

For information about the NetView Bridge function, see *Tivoli NetView for OS/390 Bridge Implementation*, SC31-8238-03 (available only in the V1R4 library).

Accessing terminology online

The IBM Terminology web site consolidates the terminology from IBM product libraries in one convenient location. You can access the Terminology web site at http://www.ibm.com/software/globalization/terminology/.

For NetView for z/OS terms and definitions, see the IBM Terminology web site. The following terms are used in this library:

NetView
For the following products:
- Tivoli NetView for z/OS version 6 release 1
- Tivoli NetView for z/OS version 5 release 4
- Tivoli NetView for z/OS version 5 release 3
- Tivoli NetView for z/OS version 5 release 2
- Tivoli NetView for z/OS version 5 release 1
- Tivoli NetView for OS/390® version 1 release 4

CNMCMD
For the CNMCMD member and the members that are included in it using the %INCLUDE statement

CNMSTYLE
For the CNMSTYLE member and the members that are included in it using the %INCLUDE statement

PARMLIB
For SYS1.PARMLIB and other data sets in the concatenation sequence

MVS™ For z/OS operating systems

MVS element
For the base control program (BCP) element of the z/OS operating system

VTAM®
For Communications Server - SNA Services

IBM Tivoli Network Manager
For either of these products:
- IBM Tivoli Network Manager
- IBM Tivoli OMNIbus and Network Manager

IBM Tivoli Netcool/OMNIbus

For either of these products:
- IBM Tivoli Netcool/OMNIbus
- IBM Tivoli OMNIbus and Network Manager

Unless otherwise indicated, references to programs indicate the latest version and release of the programs. If only a version is indicated, the reference is to all releases within that version.

When a reference is made about using a personal computer or workstation, any programmable workstation can be used.

Using NetView for z/OS online help

The following types of NetView for z/OS mainframe online help are available, depending on your installation and configuration:
- General help and component information
- Command help
- Message help
- Sense code information
- Recommended actions

Using LookAt to look up message explanations

LookAt is an online facility that you can use to look up explanations for most of the IBM messages you encounter, and for some system abends and codes. Using LookAt to find information is faster than a conventional search because, in most cases, LookAt goes directly to the message explanation.

You can use LookAt from the following locations to find IBM message explanations for z/OS elements and features, z/VM®, VSE/ESA, and Clusters for AIX® and Linux systems:

- The Internet. You can access IBM message explanations directly from the LookAt web site at http://www.ibm.com/systems/z/os/zos/bkserv/lookat/.
- Your z/OS TSO/E host system. You can install code on your z/OS or z/OS.e system to access IBM message explanations, using LookAt from a TSO/E command line (for example, TSO/E prompt, ISPF, or z/OS UNIX System Services running OMVS).
- Your Microsoft Windows workstation. You can install LookAt directly from the *z/OS Collection* (SK3T-4269) or the *z/OS and Software Products DVD Collection* (SK3T-4271) and use it from the resulting Windows graphical user interface (GUI). The command prompt (also known as the DOS command line) version can still be used from the directory in which you install the Windows version of LookAt.
- Your wireless handheld device. You can use the LookAt Mobile Edition from http://www.ibm.com/systems/z/os/zos/bkserv/lookat/lookatm.html with a handheld device that has wireless access and an Internet browser.

You can obtain code to install LookAt on your host system or Microsoft Windows workstation from the following locations:

- A CD in the *z/OS Collection* (SK3T-4269).
- The *z/OS and Software Products DVD Collection* (SK3T-4271).
- The LookAt web site. Click **Download** and then select the platform, release, collection, and location that you want. More information is available in the LOOKAT.ME files that is available during the download process.

Accessing publications online

The documentation DVD, *IBM Tivoli NetView for z/OS V6R1 Online Library*, SK2T-6175, contains the publications that are in the product library. The publications are available in PDF, HTML, and BookManager formats. Refer to the readme file on the DVD for instructions on how to access the documentation.

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli Information Center web site at http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp.

Note: If you print PDF documents on other than letter-sized paper, set the option in the **File → Print** window that enables Adobe Reader to print letter-sized pages on your local paper.

Ordering publications

You can order many Tivoli publications online at http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, contact your software account representative to order Tivoli publications. To locate the telephone number of your local representative, perform the following steps:

1. Go to http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss.
2. Select your country from the list and click **Go**.
3. Click **About this site** to see an information page that includes the telephone number of your local representative.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. Standard shortcut and accelerator keys are used by the product and are documented by the operating system. Refer to the documentation provided by your operating system for more information.

For additional information, see the Accessibility appendix in the *User's Guide: NetView*.

Tivoli technical training

For Tivoli technical training information, refer to the following IBM Tivoli Education web site at http://www.ibm.com/software/tivoli/education.

Tivoli user groups

Tivoli user groups are independent, user-run membership organizations that provide Tivoli users with information to assist them in the implementation of Tivoli Software solutions. Through these groups, members can share information and learn from the knowledge and experience of other Tivoli users.

Access the Tivoli Users Group at http://www.tivoli-ug.org.

Downloads

Clients and agents, NetView product demonstrations, and several free NetView applications can be downloaded from the NetView for z/OS support web site:

http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliNetViewforzOS.html

In the "IBM Tivoli for NetView for z/OS support" pane, click **Download** to go to a page where you can search for or select downloads.

These applications can help with the following tasks:

- Migrating customization parameters and initialization statements from earlier releases to the CNMSTUSR member and command definitions from earlier releases to the CNMCMDU member.
- Getting statistics for your automation table and merging the statistics with a listing of the automation table
- Displaying the status of a job entry subsystem (JES) job or canceling a specified JES job
- Sending alerts to the NetView program using the program-to-program interface (PPI)
- Sending and receiving MVS commands using the PPI
- Sending Time Sharing Option (TSO) commands and receiving responses

Support information

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

Online

Access the Tivoli Software Support site at http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman. Access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html.

IBM Support Assistant

The IBM Support Assistant is a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. The Support Assistant provides quick access to support-related information and serviceability tools for problem determination. To install the Support Assistant software, go to http://www.ibm.com/software/support/isa/.

Troubleshooting information

For more information about resolving problems with the NetView for z/OS product, see the *IBM Tivoli NetView for z/OS Troubleshooting Guide*. Additional support for the NetView for z/OS product is available through the NetView user group on Yahoo at http://groups.yahoo.com/group/NetView/. This support is for NetView for z/OS customers only, and registration is required. This forum is monitored by NetView developers who answer questions and provide guidance. When a problem with the code is found, you are asked to open an official problem management record (PMR) to obtain resolution.

Conventions used in this publication

This publication uses several conventions for special terms and actions and for operating system-dependent commands and paths.

Typeface conventions

This publication uses the following typeface conventions:

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as **Tip:**, and **Operating system considerations**:)
- Keywords and parameters in text

Italic

- Citations (examples: titles of publications, diskettes, and CDs
- Words defined in text (example: a nonswitched line is called a *point-to-point line*)
- Emphasis of words and letters (words as words example: "Use the word *that* to introduce a restrictive clause."; letters as letters example: "The LUN address must start with the letter *L*.")
- New terms in text (except in a definition list): a *view* is a frame in a workspace that contains data.
- Variables and values you must provide: ... where *myname* represents...

`Monospace`

- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

Operating system-dependent variables and paths

For workstation components, this publication uses the UNIX convention for specifying environment variables and for directory notation.

When using the Windows command line, replace **$***variable* with **%***variable***%** for environment variables and replace each forward slash (**/**) with a backslash (\) in directory paths. The names of environment variables are not always the same in the Windows and UNIX environments. For example, %TEMP% in Windows environments is equivalent to $TMPDIR in UNIX environments.

Note: If you are using the bash shell on a Windows system, you can use the UNIX conventions.

Part 1. NetView Enterprise Management Agent Introduction

Chapter 1. NetView Enterprise Management Agent Overview

Use the IBM Tivoli NetView for z/OS Enterprise Management Agent to manage your network from the Tivoli Enterprise Portal. Both sampled and real-time NetView data is available in the Tivoli Enterprise Portal with this agent. With the NetView for z/OS Enterprise Management Agent and the OMEGAMON® XE performance agents, you can manage and view availability and performance data for your network from a single interface.

Note: The NetView for z/OS Enterprise Management Agent is frequently referred to as the NetView agent.

You can perform the following kinds of tasks:
- Monitor NetView applications
- Monitor NetView task status and performance statistics
- Monitor the status of your TCP/IP stacks
- Monitor DVIPA configuration, workload balance, connections, connection routing, and VIPA routes
- Monitor and diagnose problems with TCP/IP connections
- Monitor the configuration and status of your Telnet servers
- Monitor the configuration and status of OSA channels and ports
- Monitor the configuration and status of HiperSockets™ interfaces
- Monitor active SNA sessions
- Issue commands to manage your network
- Support for the GDPS® Active/Active Continuous Availability solution

The NetView agent runs on a z/OS system in its own address space and requires the Tivoli Management Services, which is provided by IBM Tivoli Monitoring. The NetView program communicates with the NetView agent using the NetView program-to-program interface (PPI), which provides a secure communication layer between the NetView program and the agent.

The NetView agent is disabled by default. It is enabled by using the TEMA tower and associated subtower statements in the CNMSTUSR or C*xx*STGEN member. For information about changing CNMSTYLE statements, see *IBM Tivoli NetView for z/OS Installation: Getting Started*. Note that the CNMSTYLE member contains all of the values that can be customized for the NetView agent.

Enabling the TEMA tower starts the PPI receiver connection to the NetView agent by issuing the NACMD command. Data collectors provide sampled or real-time data. The collected data is stored in a data space and is retrieved by the NetView agent when a user requests data for the associated workspace in the Tivoli Enterprise Portal. The PPI receiver is stopped with the STOPNA command.

Tivoli Enterprise Portal Overview

The NetView for z/OS program uses the Tivoli Enterprise Portal to provide a view of your enterprise from which you can drill down to more closely examine components of each system being monitored. The application window for the Tivoli Enterprise Portal consists of a Navigator and a workspace.

The Physical Navigator displays all the systems in your enterprise where Tivoli Enterprise Monitoring Agents are installed. It shows the hierarchy of your monitored enterprise, from the top level (Enterprise) down to individual groupings of information collected by the NetView agent. When you click an item in the Navigator, the default workspace for that item is displayed.

The workspace is the work area of the Tivoli Enterprise Portal window and consists of one or more views of the resources being monitored. A view is a pane in the workspace, typically a chart or table, showing data collected by the NetView agent or other Tivoli Enterprise Monitoring Agents. Each view has a set of properties associated with it. You can customize the workspace by using the Properties Editor to change the style and content of each view. You can also add and delete views in a workspace.

Access the Tivoli Enterprise Portal in one of the following modes:

Desktop
The application software is installed on your system.

Browser
The software is downloaded to your system the first time you log on to Tivoli Enterprise Portal, and, after that, whenever the software is updated. Access is through a supported browser using the Web address of the Tivoli Enterprise Portal Server.

For more information about the Tivoli Enterprise Portal, see the Tivoli Enterprise Portal user assistance and the *IBM Tivoli Monitoring: Tivoli Enterprise Portal User's Guide*.

Workspace Overview

The NetView for z/OS Enterprise Management Agent workspaces contain views that report information about enterprise resources that you are monitoring.

Each workspace contains a navigation tree view and at least one other view. Many workspaces contain table views. Table rows can contain links to related workspaces that provide more detailed information. A workspace can contain other views, such as a bar chart, notepad, or take action view. A take action view can be used to send commands to the NetView host.

Many of the agent workspaces provide data that is either sampled at an interval or that is a combination of sampled and event-driven. Some workspaces contain data that is command-based; that is, they require a take action command to be issued to provide data.

All of the workspaces that are included with the NetView agent are read-only. To change these workspaces, save them using a different name.

The following sections provide general information about the NetView agent workspaces.
- "Access to Workspaces" on page 5
- "Cross-Product Workspace Links" on page 5
- "Data Collection for Workspaces" on page 6
- "Historical Data" on page 7

For descriptions of the NetView agent workspaces, see Part 2, "NetView Enterprise Management Agent Workspaces," on page 17. For detailed information about the workspaces, see the online help. Note that these workspace descriptions apply to the default settings of the original configuration. Changes and additions that you make to a workspace are not described in the online help or in this book.

Access to Workspaces

To access many of the NetView agent workspaces from the Navigator in the Tivoli Enterprise Portal, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **NetView** > *domain*; and then click the workspace name. The workspace descriptions describe how to access each workspace.

Note: To access most of the workspaces for the GDPS Active/Active Continuous Availability solution, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **Active/Active Sites** > *node*:**ACTACT**; and then click the workspace name.

For the links to some filtered workspaces, a filter window opens. In the filter window, specify or change values for one or more of the fields. For information about the fields, see the online help. You must specify a value for at least one field. You can include one or more wildcard characters (*) anywhere within a value that you specify. You can also specify a lone wildcard character for one or more fields, but you cannot specify a lone wildcard character for all the fields. Leaving a field blank is the same as specifying a lone wildcard character. Click **OK** to display the filtered data in the target workspace.

Notes:

1. When you click **OK**, the values you specified are saved, and the target workspace is displayed using the specified values.
2. If you click **Cancel**, any changes that you made are discarded and the target workspace is displayed with no data.

Cross-Product Workspace Links

Dynamic workspace linking provides easy navigation between workspaces for different products. By providing additional information about resources that are being monitored by other monitoring agents, this linking helps in problem determination and improves integration across the monitoring products, so that you can quickly determine the root cause of a problem.

When you right-click a link, a list of links is displayed. The list can contain links to workspaces provided by other monitoring products. For a cross-product workspace link to work, the target product must be installed and configured and your Tivoli Enterprise Portal user ID must be authorized to access the target product.

Choose a workspace from the list to navigate to that workspace. By linking to the target workspace in context, attributes in the source row can be used to locate the target workspace in the navigation tree or to filter the data that is displayed in the target workspace.

If you choose a target workspace that is not available, the following message is displayed; for more information, see the *IBM Tivoli NetView for z/OS Troubleshooting Guide*.

```
KFWITM081E The link target can not be found.
```

Table 1 on page 6 summarizes the cross-product workspace links that are available when this product ships. See the workspace descriptions in the online help for information about the predefined links provided with each workspace.

Table 1. Cross-Product Workspace Links

NetView Agent Workspace	Target Application or Monitoring Agent	Workspace in Target Application or Monitoring Agent	Attributes Used to Locate Target Workspace	Attributes Used to Filter Data in Target Workspace
DVIPA Connections	IBM Tivoli OMEGAMON XE for Mainframe Networks version 4.1.0 or later	TCP Connections Link	System ID	• Connection Start Time • Local IP Address • Local Port • Remote IP Address • Remote Port
Session Data	IBM Tivoli OMEGAMON XE for Mainframe Networks version 4.1.0 or later	HPR Connections	System ID	• Primary Name • Secondary Name
TCPIP Connection Data	IBM Tivoli OMEGAMON XE for Mainframe Networks version 4.1.0 or later	TCP Connections Link	System ID	• Connection Start Time • Local IP Address • Local Port • Remote IP Address • Remote Port
TCPIP Connection Data	IBM Tivoli OMEGAMON XE for CICS® on z/OS version 4.1.0 or later	TCPIP Statistics	System ID	Local Port (converted to an integer in the link expression)
TCPIP Connection Data	IBM Tivoli OMEGAMON XE on z/OS version 4.1.0 or later	System CPU Utilization	Managed system name (Sysplex Name:System ID:"MVSSYS")	None
Telnet Server Configuration and Status	IBM Tivoli OMEGAMON XE for Mainframe Networks version 4.2.0 or later	TN3270 Server Sessions	System ID	Telnet Server Job Name

Data Collection for Workspaces

Data collection for much of the data that is displayed in the Tivoli Enterprise Portal for the NetView agent is controlled outside of the TEMA subtowers. For information about which functions require a TEMA subtower to be enabled for data collection, see the data collection and display table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*. Data collection that is initiated by TEMA subtowers begins after an NACMD command completes successfully. After that, the NetView agent address space is active and ready for communication.

After communication is established between the NetView program and the agent, data is collected unless an operator action or unexpected error occurs. You might need to change the data collectors that are running at a given time or want to change some of the data collector parameters.

You can manually stop and start any of the NetView agent data collectors using the following commands, if the data collector subtower is enabled:

- NACTL STOP or NACTL START command for collecting NetView task (HEALTH), active (CONNACT) or inactive (CONINACT) TCP/IP connection, or active session (SESSACT) data
- COLLCTL STOP or COLLCTL START command for collecting DVIPA definition and status (DVDEF), distributed DVIPA (DVTAD), DVIPA connection

(DVCONN), VIPA route (DVROUT), OSA or HiperSockets (INTERFACES), Telnet server and port (TELNET), or NetView application (APPL) data

- ACTVCTL STOP or ACTVCTL START command for collecting GDPS Active/Active Continuous Availability solution (LIFELINE, DB2®, and IMS™) data

You can change any of the data collector statements by using the ROWS*xxx* and INT*xxx* statements in the CNMSTUSR or C*xx*STGEN member, and issue the RESTYLE NACMD command to pick up the changes. For these changes to take effect, the NACMD command must be stopped and reissued. For information about changing CNMSTYLE statements, see *IBM Tivoli NetView for z/OS Installation: Getting Started*.

Note: If you are changing only the intervals for a subtower, issuing the NACTL STOP and NACTL START commands for the subtower causes the changes to take effect.

Historical Data

Both real-time and historical data are available within the NetView agent workspaces. After historical data is configured, enabled, and collected, you can display historical reports, which are useful in finding the root cause of problems that evolved over a period of time and debugging problems that occurred in a prior time period. Capacity planners can also use historical reports to identify trends and correct imbalances in network load distribution.

Historical Data Collection

To generate reports containing historical data, historical collection must be configured and enabled and data must be collected. Use the Tivoli Enterprise Portal support to configure and enable collection of data in a historical database. The two types of historical data are short-term and long-term. Short-term historical data collection must be configured and enabled if you want to perform long-term historical data collection.

Short-term historical data is, by default, the most recent 24 hours of data. It is stored in the persistent data store on z/OS systems or in files on distributed systems. The persistent data store is configured using the z/OS Configuration Tool.

Long-term historical data can be defined for as long as you want to store the data: days, weeks, months, or years. It is periodically exported from short-term history and is stored in Tivoli Data Warehouse. The Warehouse Proxy must be installed and configured with a supported database manager (for example, DB2 Universal Database™) before you can configure warehousing using the Historical Collection dialog.

Table 2 on page 8 shows, for the NetView workspaces that are defined to the **NetView** subnode, which workspaces and views can display historical data and the corresponding attribute groups to configure for historical data collection.

Table 2. NetView Subnode Workspaces and Views That Display Historical Data

Attribute Group	**Workspaces and Views**
NA DDVIPA Server Health	Distributed DVIPA Server Health: • All views Distributed DVIPA Server Health Details: • All views Distributed DVIPA Unhealthy Servers: • All views
NA DDVIPA Targets	Distributed DVIPA Targets: • All views DVIPA Stack Summary: • Local Distributed Targets Defined
NA DVIPA Sysplex Distributors	DVIPA Stack Summary: • Sysplex Distributors Defined DVIPA Sysplex Distributors: • DVIPA Sysplex Distributors Summary
NA Inactive TCPIP Connection Data	Inactive TCPIP Connection Data: • All views except Inactive TCPIP Connection Count
NA NetView Applications	NetView Applications: • All views
NA NetView Tasks	NetView Tasks: • All views NetView Task Details: • All views
NA Session Count	Session Data: • Active Session Count
NA TCPIP Connection Count	TCPIP Connection Data: • Active TCPIP Connection Count
NA TCPIP Connection Data	TCPIP Connection Data: • All views except Active TCPIP Connection Count

Table 3 shows, for the NetView agent workspaces that are defined to the **Active/Active Sites** subnode, which workspaces and views can display historical data and the corresponding attribute groups to configure for historical data collection. The Active/Active Sites subnode is displayed only with the GDPS Active/Active Continuous Availability solution.

Table 3. Active/Active Sites Subnode Workspaces and Views That Display Historical Data

Attribute Group	**Workspaces and Views**
NA DB2 Replication Apply Server	DB2 Replication Details: • Q Apply Details
NA DB2 Replication Apply Workload	DB2 Replication Details: • Q Apply: Receive Queue Details • Q Percent Full
NA DB2 Replication Capture Server	DB2 Replication Details: • Q Capture Details
NA DB2 Replication Capture Workload	DB2 Replication Details: • Q Capture: Send Queue Details

Table 3. Active/Active Sites Subnode Workspaces and Views That Display Historical Data (continued)

Attribute Group	Workspaces and Views
NA IMS Replication Capture Details	IMS Replication Details: • Capture Cache Size • Capture Queue Percent Full • IMS Capture Server Details
NA IMS Replication Apply Details	IMS Replication Details: • Apply Cache Size • Apply Queue Percent Full • IMS Apply Server Details
NA Replication Servers	Replication Servers: • All views
NA Workload Servers	Workload Server Details: • All views Workload Servers: • All views
NA Workload Sites	Workload Site Details: • All views Workload Sites: • All views

For more information about configuring historical data collection and reporting, see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Historical Reports

After historical data collection is enabled, a **Time Span** button (displayed as a clock in front of a calendar) is shown in the upper left corner of qualifying views in Tivoli Enterprise Portal workspaces. Click this icon to extend any existing Tivoli Enterprise Portal view (also called a report) to include historical data. Tivoli Enterprise Portal reports automatically pull data from both short-term and long-term history, based on the time period you specify.

You can create summarization data tables (hourly, daily, weekly, quarterly, monthly, and yearly) to reduce the data overload when creating reports. You can also define pruning intervals to ensure that you save only the data that is needed.

For more information about creating historical reports, see the *IBM Tivoli Monitoring: Tivoli Enterprise Portal User's Guide*.

You can use Tivoli Common Reporting, a reporting tool common across Tivoli products, to automatically generate reports. The NetView program provides a set of predefined reports that you can use with the Tivoli Common Reporting tool. For more information about the NetView reports, see *IBM Tivoli NetView for z/OS Installation: Configuring the NetView Enterprise Management Agent*.

Attribute Overview

Use the NetView for z/OS Enterprise Management Agent attributes to build views that display the availability of your network. Attributes can be used to define situations to test for specific conditions. When the conditions for a situation are met, situation event indicators are displayed in the Navigator.

A direct relationship usually exists between the NetView agent attributes and the table views. An attribute group corresponds to a table view, or, occasionally, to several table views within a workspace. Each attribute group has one or more attribute items, which correspond to the columns in a table view.

For general information about an attribute group or to see the names of the attributes in each attribute group, see Appendix C, “Attributes,” on page 91.

Situation Overview

The IBM Tivoli NetView for z/OS Enterprise Management Agent provides a set of situations that you can use to monitor the systems in your network. Situations are used to identify monitored resources that meet certain performance criteria and to raise an event when the criteria are met. A situation definition includes a sampling frequency, a set of conditions, and a list of monitored systems. These have implications for processor and storage consumption, and the cumulative effect of all the active situations has implications for performance.

All the situations provided for the NetView agent are defined such that they are not automatically started. When planning for the agent, evaluate the provided situations. Determine the situations that you want to start automatically, and eliminate situations that are not relevant for your environment. If necessary, modify existing situations or create new situations to meet the needs of your enterprise.

A policy is a logical expression that describes a series, or workflow, of automated steps, called activities, for which you can control the order of processing. An activity can be an activity program, a situation, or another policy. The NetView agent provides a policy for the GDPS Active/Active Continuous Availability solution that you can use to automate a response when a situation is resolved. By default, the policy is defined such that it is not automatically started.

For descriptions of the situations and policy that are provided with the NetView agent, see Appendix A, “Situations,” on page 69. For more information about situations and policies, see the *IBM Tivoli Monitoring Tivoli Enterprise Portal User's Guide*.

Take Action Command Overview

Use the NetView for z/OS Enterprise Management Agent take action commands to interact with your applications and operating system.

A take action command that is issued from the Tivoli Enterprise Portal is received by the NetView agent and sent to the NetView program over the PPI. The command is processed, and the command responses are stored in a data space. When the Tivoli Enterprise Portal user selects or refreshes the workspace for the command issued, the data is retrieved from the data space and displayed in the Tivoli Enterprise Portal.

For more information about the take action commands, see Appendix B, “Take Action Commands,” on page 81.

Chapter 2. Enterprise Management Agent Changes

The following changes are available with the Tivoli NetView for z/OS Enterprise Management Agent for Version 6 Release 1:

- All queries and workspaces that are new or changed for the Version 6 Release 1 Tivoli NetView for z/OS Enterprise Management Agent include the qualifier `(V610)` in the query and workspace descriptions. The identification of the version, release, and modification level for queries and workspaces began with Version 5 Release 4. Queries and workspaces that were part of the product before V5R4 do not include a qualifier.
- Table 4 shows the changes to existing workspaces.

Table 4. Workspace Changes

Workspaces	Changes
Distributed DVIPA Connection Routing	• The following integer attributes are added: – Source Port – Destination Port • The caption for the existing Source Port attribute, which is a string, is changed to Source Port String. This attribute is filtered out of the table view by default. • The caption for the existing Destination Port attribute, which is a string, is changed to Destination Port String. This attribute is filtered out of the table view by default.
Distributed DVIPA Server Health Distributed DVIPA Server Health Details Distributed DVIPA Unhealthy Servers Filtered Distributed DVIPA Server Health Filtered Distributed DVIPA Unhealthy Servers	• The following integer attribute is added: – DVIPA Port • The caption for the existing DVIPA Port attribute, which is a string, is changed to DVIPA Port String. This attribute is filtered out of the table view by default.
Distributed DVIPA Targets DVIPA Workloads Filtered Distributed DVIPA Targets	• The following integer attributes are added: – DVIPA Port – Hot Standby Rank – Hot Standby Server Status – Hot Standby Server Type • The caption for the existing DVIPA Port attribute, which is a string, is changed to DVIPA Port String. This attribute is filtered out of the table view by default.

Table 4. Workspace Changes (continued)

Workspaces	Changes
DVIPA Connections Filtered DVIPA Connections	• The following integer attributes are added: – DVIPA Port – Remote Port • The following long integer attributes are added: – Bytes Received – Bytes Sent – Bytes Sent or Received – Total Bytes – Total Bytes Received – Total Bytes Sent • The caption for the existing Bytes Received attribute, which is a string, is changed to Bytes Received String. This attribute is filtered out of the table view by default. • The caption for the existing Bytes Sent attribute, which is a string, is changed to Bytes Sent String. This attribute is filtered out of the table view by default. • The caption for the existing Bytes Sent or Received attribute, which is a string, is changed to Bytes Sent or Received String. This attribute is filtered out of the table view by default. • The caption for the existing DVIPA Port attribute, which is a string, is changed to DVIPA Port String. This attribute is filtered out of the table view by default. • The caption for the existing Remote Port attribute, which is a string, is changed to Remote Port String. This attribute is filtered out of the table view by default. • The caption for the existing Total Bytes attribute, which is a string, is changed to Total Bytes String. This attribute is filtered out of the table view by default. • The caption for the existing Total Bytes Received attribute, which is a string, is changed to Total Bytes Received String. This attribute is filtered out of the table view by default. • The caption for the existing Total Bytes Sent attribute, which is a string, is changed to Total Bytes Sent String. This attribute is filtered out of the table view by default.
DVIPA Stack Summary	• The following integer attributes are added to the Local Distributed Targets Defined table view: – DVIPA Port – Hot Standby Rank – Hot Standby Server Status – Hot Standby Server Type • The following integer attributes are added to the Sysplex Distributors Defined table view: – Auto Switch Back – DVIPA Port – Health Switch • The caption for the existing DVIPA Port attribute, which is a string, is changed to DVIPA Port String in both the Local Distributed Targets Defined and Sysplex Distributors Defined table views. This attribute is filtered out of the table views by default.

Table 4. Workspace Changes (continued)

Workspaces	Changes
DVIPA Sysplex Distributors Filtered DVIPA Sysplex Distributors	• The following integer attributes are added: – Auto Switch Back – DVIPA Port – Health Switch • The following value for the existing Distribution Method attribute is added: – hotStandBy (6) • The caption for the existing DVIPA Port attribute, which is a string, is changed to DVIPA Port String. This attribute is filtered out of the table view by default.
Inactive TCPIP Connection Data Filtered Inactive TCPIP Connection Data	• The following integer attributes are added: – Local Port – Remote Port • The following long integer attributes are added: – Total Bytes – Total Bytes Received – Total Bytes Sent • The caption for the existing Local Port attribute, which is a string, is changed to Local Port String. This attribute is filtered out of the table view by default. • The caption for the existing Remote Port attribute, which is a string, is changed to Remote Port String. This attribute is filtered out of the table view by default. • The caption for the existing Total Bytes attribute, which is a string, is changed to Total Bytes String. This attribute is filtered out of the table view by default. • The caption for the existing Total Bytes Received attribute, which is a string, is changed to Total Bytes Received String. This attribute is filtered out of the table view by default. • The caption for the existing Total Bytes Sent attribute, which is a string, is changed to Total Bytes Sent String. This attribute is filtered out of the table view by default.
NetView Applications	• The following integer attribute is added: – RMTCMD Port • The caption for the existing RMTCMD Port attribute, which is a string, is changed to RMTCMD Port String. This attribute is filtered out of the table view by default.
NetView Audit Log	• The following timestamp attribute is added: – Message Time • The existing Date and Time attributes are filtered out of the table view by default.

Table 4. Workspace Changes (continued)

Workspaces	Changes
NetView Log	• The caption for the existing Code attribute is changed to Routing Code. • The caption for the existing Date attribute is changed to First Record Date. • The caption for the existing Log attribute is changed to Network Log. • The caption for the existing MTYPE attribute is changed to HDRMTYPE. • The caption for the existing OperID attribute is changed to Operator ID. • The caption for the existing RecordCount attribute is changed to Record Count. • The caption for the existing SeqNum attribute is changed to Sequence Number. • The caption for the existing Time attribute is changed to Message Time.
OSA Channels and Ports	• The following integer attribute is added: – Channel Type
TCPIP Connection Data Filtered TCPIP Connection Data	• The following integer attributes are added: – Local Port – Remote Port • The following long integer attributes are added: – Bytes Received – Bytes Sent – Bytes Sent or Received – Total Bytes – Total Bytes Received – Total Bytes Sent • The caption for the existing Bytes Received attribute, which is a string, is changed to Bytes Received String. This attribute is filtered out of the table view by default. • The caption for the existing Bytes Sent attribute, which is a string, is changed to Bytes Sent String. This attribute is filtered out of the table view by default. • The caption for the existing Bytes Sent or Received attribute, which is a string, is changed to Bytes Sent or Received String. This attribute is filtered out of the table view by default. • The caption for the existing Local Port attribute, which is a string, is changed to Local Port String. This attribute is filtered out of the table view by default. • The caption for the existing Remote Port attribute, which is a string, is changed to Remote Port String. This attribute is filtered out of the table view by default. • The caption for the existing Total Bytes attribute, which is a string, is changed to Total Bytes String. This attribute is filtered out of the table view by default. • The caption for the existing Total Bytes Received attribute, which is a string, is changed to Total Bytes Received String. This attribute is filtered out of the table view by default. • The caption for the existing Total Bytes Sent attribute, which is a string, is changed to Total Bytes Sent String. This attribute is filtered out of the table view by default.

Table 4. Workspace Changes (continued)

Workspaces	Changes
Telnet Server Configuration and Status Filtered Telnet Server Configuration and Status	• The following integer attribute is added: – Port • The caption for the existing Port attribute, which is a string, is changed to Port String. This attribute is filtered out of the table view by default.

- Sixteen new workspaces and fourteen new attribute groups are added for monitoring the status of workloads and other managed elements in the GDPS Active/Active Continuous Availability solution. For information, see documentation about the solution. Table 5 shows the workspaces that are new and the associated attribute group or groups.

Table 5. New Workspaces

Workspace	Attribute Group
DB2 Replication Details	DB2 Replication Apply Server DB2 Replication Apply Workload DB2 Replication Capture Server DB2 Replication Capture Workload
Filtered Replication Servers	Replication Servers
Filtered Workload Servers	Workload Servers
Filtered Workloads	Workloads
IMS Replication Details	IMS Replication Apply Details IMS Replication Capture Details
Load Balancer Groups	Load Balancer Groups
Load Balancer Workloads	Load Balancer Groups
Load Balancers	Load Balancers
Replication Servers	Replication Servers
Workload Lifeline Advisors	Workload Lifeline Advisors
Workload Lifeline Agents	Workload Lifeline Agents
Workload Server Details	Workload Servers
Workload Servers	Workload Servers
Workload Site Details	Workload Sites
Workload Sites	Workload Sites
Workloads	Workloads

- The following situations for the GDPS Active/Active Continuous Availability solution are new:
  - NAS_AA_DB2_QPctFull
  - NAS_AA_IMS_AppQPctFull_Crit
  - NAS_AA_IMS_AppQPctFull_Warn
  - NAS_AA_IMS_CapQPctFull_Crit
  - NAS_AA_IMS_CapQPctFull_Warn
  - NAS_AA_LB_Status
  - NAS_AA_RS_AppServerStatus
  - NAS_AA_RS_CapServerStatus
  - NAS_AA_RS_DB2WorkloadState
  - NAS_AA_RS_IMSWorkloadState
  - NAS_AA_RS_LatencyExceeded

  - NAS_AA_WLA_Agents
  - NAS_AA_WLA_LBs
  - NAS_AA_WLA_NetWeight
  - NAS_AA_Workload_Status
- The following policy for the GDPS Active/Active Continuous Availability solution is new:
  - NAP_AA_RS_LatencyReset
- The following take action commands for the GDPS Active/Active Continuous Availability solution are new:
  - View Data Collection Statistics for Active/Active Sites
  - View DB2 Replication Details
  - View IMS Replication Details
  - View Load Balancer Groups
  - View Load Balancer Workloads
  - View Load Balancers
  - View Replication Servers
  - View Workload Lifeline Advisors
  - View Workload Lifeline Agents
  - View Workload Servers
  - View Workload Sites
  - View Workloads

Part 2. NetView Enterprise Management Agent Workspaces

Chapter 3. DVIPA Workspaces

The DVIPA workspaces provide information about your DVIPA configuration and the use of the configuration within your network. The data in the DVIPA workspaces is provided by sampling and events. You can also issue take action commands to retrieve real-time DVIPA information.

The following DVIPA workspaces, which are listed in alphabetical order, are provided:

Application-Instance DVIPA Workspace

The Application-Instance DVIPA workspace displays the configuration and status of the application-instance DVIPAs that are activated with an ioctl or bind() socket call.

To display this workspace, expand **z/OS Systems >** *system* **> NetView Agent >** *subagent* **> NetView >** *domain*, and then click **DVIPA Application-Instance**.

If the NetView domain node that is shown in the navigator view represents the master NetView program, this workspace can contain sysplex-wide data. Otherwise, the workspace contains data for the z/OS image on which the NetView program resides.

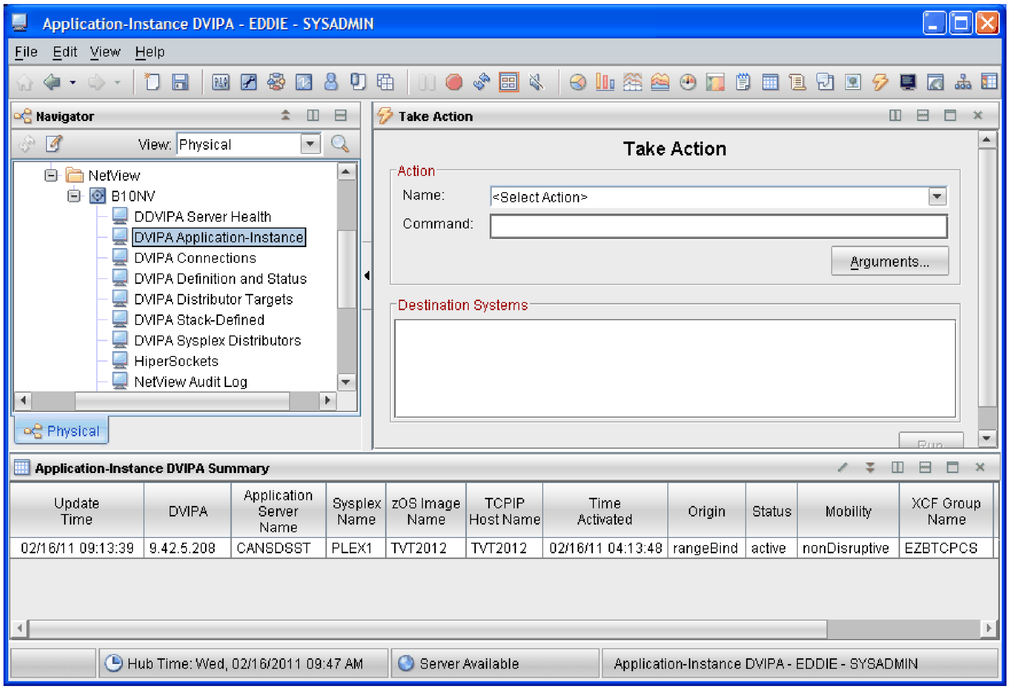
This workspace provides data that is updated by using sampling and events.

The queries for this workspace use the Origin attribute to filter the rows that can be retrieved for display. All data that matches Origin=rangeBind or Origin=rangeIoctl is displayed in the workspace.

Historical data is not enabled in this workspace.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 1.



Name: <Select Action>

Command:

Update Time	DVIPA	Application Server Name	Sysplex Name	zOS Image Name	TCPIP Host Name	Time Activated	Origin	Status	Mobility	XCF Group Name
02/16/11 09:13:39	9.42.5.208	CANSDSST	PLEX1	TVT2012	TVT2012	02/16/11 04:13:48	rangeBind	active	nonDisruptive	EZBTCPCS

Hub Time: Wed, 02/16/2011 09:47 AM

Server Available

Application-Instance DVIPA - EDDIE - SYSADMIN

Figure 1. Application-Instance DVIPA Workspace

Distributed DVIPA Connection Routing Workspace

The Distributed DVIPA Connection Routing workspace displays detailed information about distributed DVIPA connection routing. This information is available only for z/OS V1R11 Communications Server or later.

To display this workspace, click the link icon from a row in one of the following views:

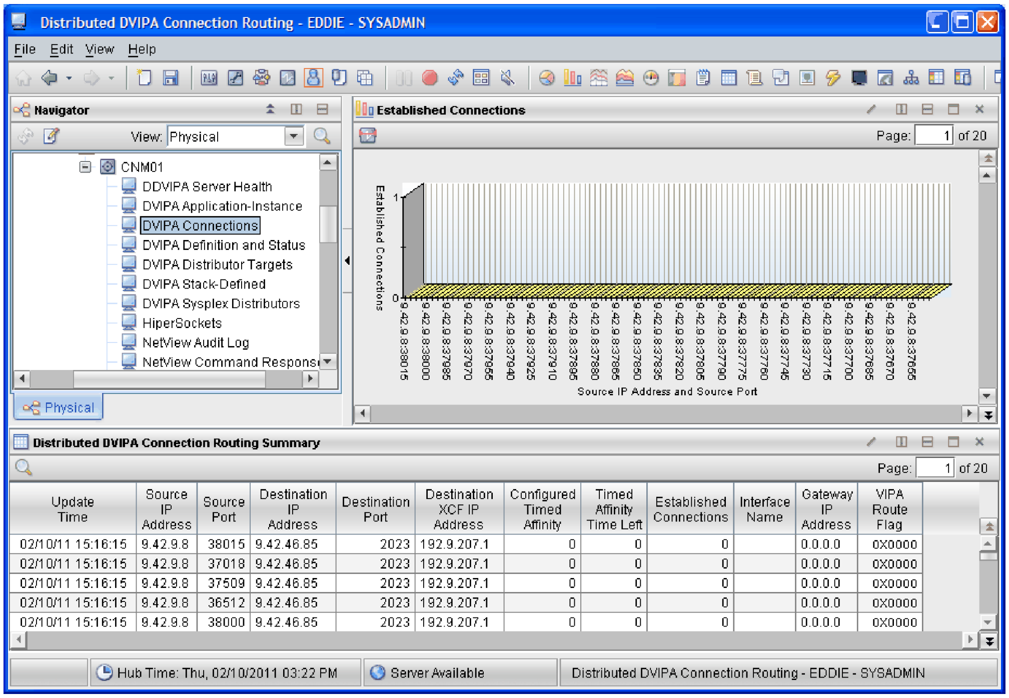
- DVIPA Connections and Filtered DVIPA Connections workspaces, the DVIPA Connections Summary table. See “DVIPA Connections Workspace” on page 25.
- DVIPA Sysplex Distributors and Filtered Sysplex Distributors workspaces, the DVIPA Sysplex Distributors Summary table. See “DVIPA Sysplex Distributors Workspace” on page 28.

This workspace provides data that is updated by using sampling.

Historical data is not enabled in this workspace.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 2 on page 21.



Update Time	Source IP Address	Source Port	Destination IP Address	Destination Port	Destination XCF IP Address	Configured Timed Affinity	Timed Affinity Time Left	Established Connections	Interface Name	Gateway IP Address	VIPA Route Flag
02/10/11 15:16:15	9.42.9.8	38015	9.42.46.85	2023	192.9.207.1	0	0	0		0.0.0.0	0X0000
02/10/11 15:16:15	9.42.9.8	37018	9.42.46.85	2023	192.9.207.1	0	0	0		0.0.0.0	0X0000
02/10/11 15:16:15	9.42.9.8	37509	9.42.46.85	2023	192.9.207.1	0	0	0		0.0.0.0	0X0000
02/10/11 15:16:15	9.42.9.8	36512	9.42.46.85	2023	192.9.207.1	0	0	0		0.0.0.0	0X0000
02/10/11 15:16:15	9.42.9.8	38000	9.42.46.85	2023	192.9.207.1	0	0	0		0.0.0.0	0X0000

Figure 2. Distributed DVIPA Connection Routing Workspace

Distributed DVIPA Server Health Workspace

The Distributed DVIPA Server Health workspace displays health statistics for all application servers that reside on distributed DVIPA targets.

To display this workspace, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **NetView** > *domain*, and then click **DDVIPA Server Health**.

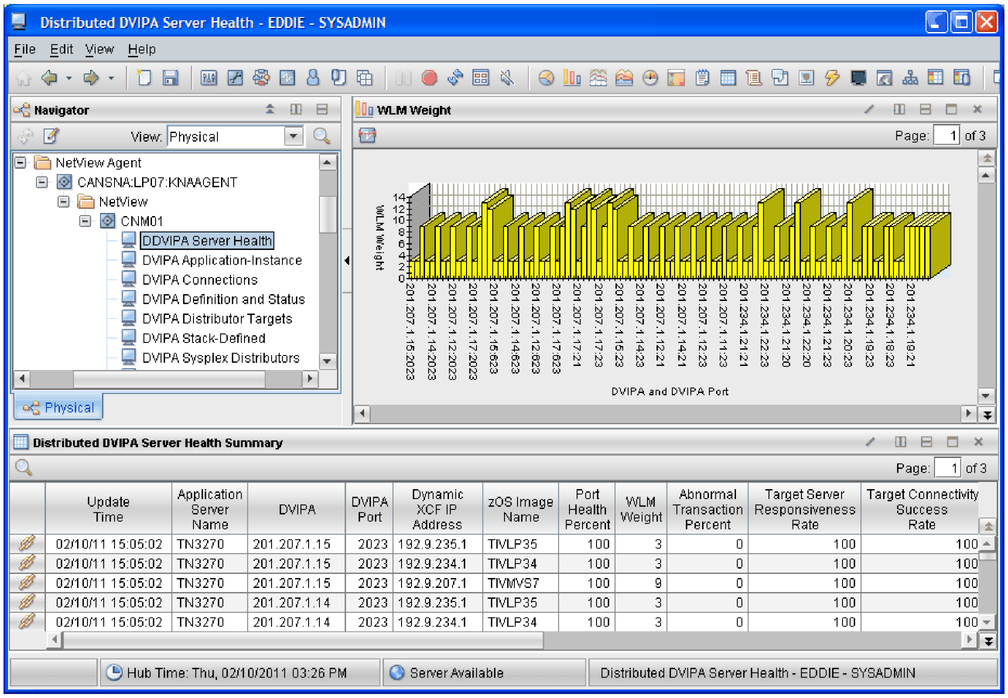
If the NetView domain node that is shown in the navigator view represents the master NetView program, this workspace can contain sysplex-wide data. Otherwise, the workspace contains data for the z/OS image on which the NetView program resides.

This workspace provides data that is updated by using sampling and events.

Historical data is enabled in this workspace.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 3 on page 22.



Update Time	Application Server Name	DVIPA	DVIPA Port	Dynamic XCF IP Address	zOS Image Name	Port Health Percent	WLM Weight	Abnormal Transaction Percent	Target Server Responsiveness Rate	Target Connectivity Success Rate
02/10/11 15:05:02	TN3270	201.207.1.15	2023	192.9.235.1	TIVLP35	100	3	0	100	100
02/10/11 15:05:02	TN3270	201.207.1.15	2023	192.9.234.1	TIVLP34	100	3	0	100	100
02/10/11 15:05:02	TN3270	201.207.1.15	2023	192.9.207.1	TIVMVS7	100	9	0	100	100
02/10/11 15:05:02	TN3270	201.207.1.14	2023	192.9.235.1	TIVLP35	100	3	0	100	100
02/10/11 15:05:02	TN3270	201.207.1.14	2023	192.9.234.1	TIVLP34	100	3	0	100	100

Hub Time: Thu, 02/10/2011 03:26 PM | Server Available | Distributed DVIPA Server Health - EDDIE - SYSADMIN

Figure 3. Distributed DVIPA Server Health Workspace

Distributed DVIPA Server Health Details Workspace

The Distributed DVIPA Server Health Details workspace displays information about health statistics for application servers that reside on distributed DVIPA targets over time.

To display this workspace, click the link icon from a row in one of the following views:

- Distributed DVIPA Server Health and Filtered Distributed DVIPA Server Health workspaces, the Distributed DVIPA Server Health Summary table. See "Distributed DVIPA Server Health Workspace" on page 21.
- Distributed DVIPA Unhealthy Servers and Filtered Distributed DVIPA Unhealthy Servers workspaces, the Distributed DVIPA Unhealthy Servers Summary table. See "Distributed DVIPA Unhealthy Servers Workspace" on page 24.

The data in this workspace is provided by using historical data collection. When you view historical data in this workspace, all rows with collection times in the specified time span are displayed. If historical data is available and you specified a valid time span, the workspace displays a series of points for the historical data within the specified time span. Otherwise, only one point representing the most recent collection is displayed in the workspace.

Historical data is enabled in this workspace.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 4 on page 23.

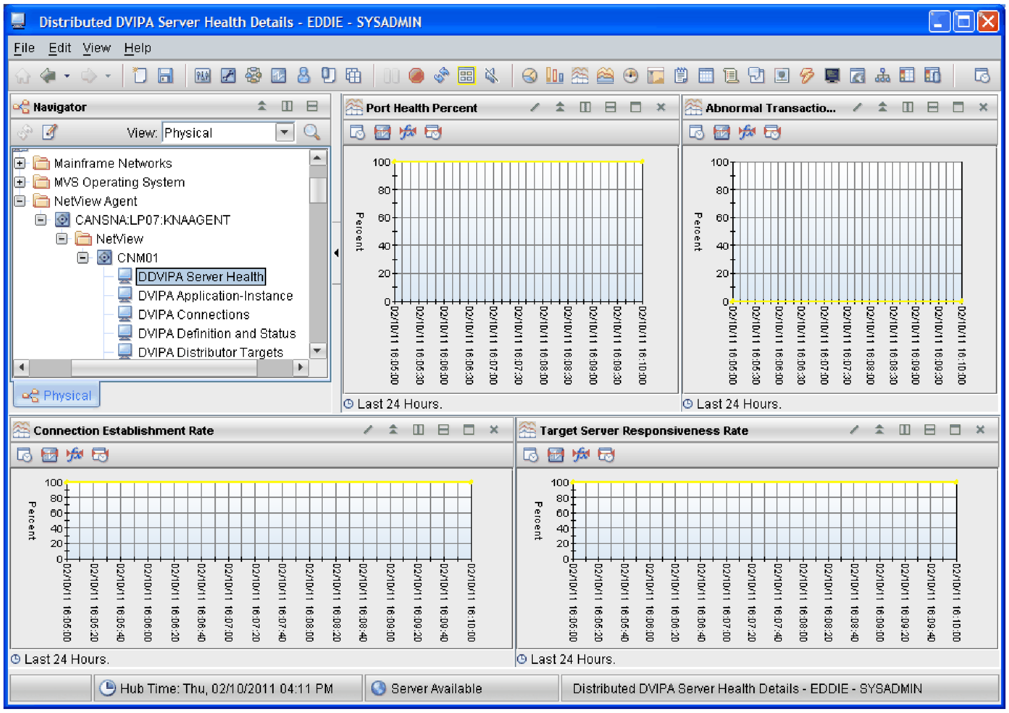

Distributed DVIPA Server Health Details - EDDIE - SYSADMIN
File Edit View Help
Navigator
View: Physical
Mainframe Networks
MVS Operating System
NetView Agent
CANSNA:LP07:KNAAGENT
NetView
CNM01
DDVIPA Server Health
DVIPA Application-Instance
DVIPA Connections
DVIPA Definition and Status
DVIPA Distributor Targets
Physical
Port Health Percent
Abnormal Transactio...
Connection Establishment Rate
Target Server Responsiveness Rate
Percent
100
80
60
40
20
0
Last 24 Hours.
Hub Time: Thu, 02/10/2011 04:11 PM
Server Available
Distributed DVIPA Server Health Details - EDDIE - SYSADMIN

Figure 4. Distributed DVIPA Server Health Details Workspace

Distributed DVIPA Targets Workspace

The Distributed DVIPA Targets workspace displays information about the distributed DVIPA targets.

To display this workspace, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **NetView** > *domain*, and then click **DVIPA Distributor Targets**.

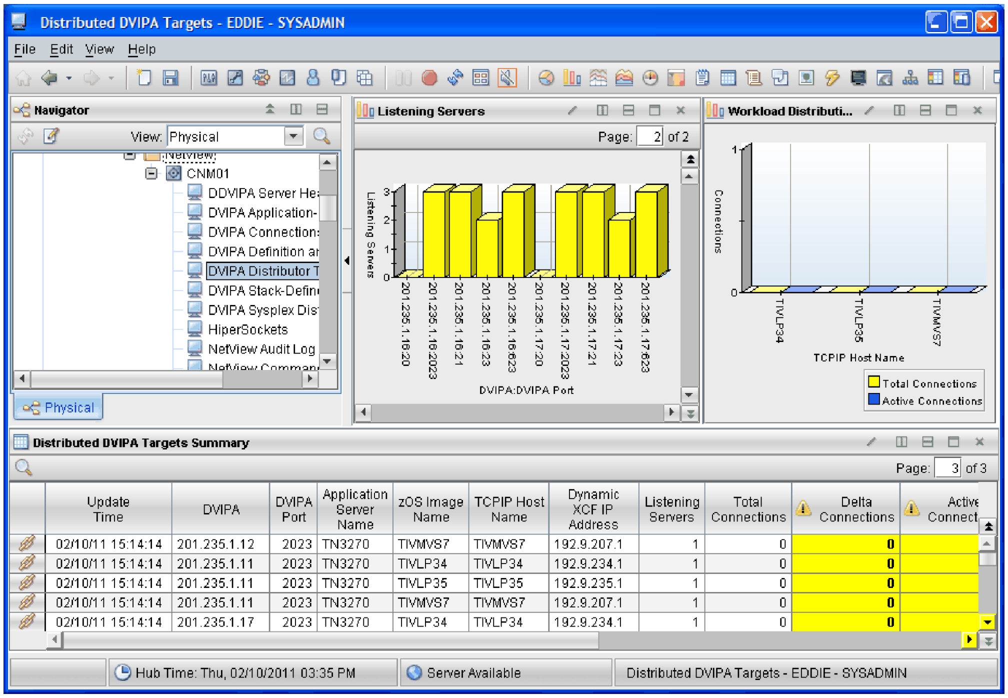
If the NetView domain node that is shown in the navigator view represents the master NetView program, this workspace can contain sysplex-wide data. Otherwise, the workspace contains data for the z/OS image on which the NetView program resides.

This workspace provides data that is updated by using sampling and events.

Historical data is enabled in this workspace.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 5 on page 24.



	Update Time	DVIPA	DVIPA Port	Application Server Name	zOS Image Name	TCPIP Host Name	Dynamic XCF IP Address	Listening Servers	Total Connections	Delta Connections	Active Connect
	02/10/11 15:14:14	201.235.1.12	2023	TN3270	TIVMVS7	TIVMVS7	192.9.207.1	1	0	0	
	02/10/11 15:14:14	201.235.1.11	2023	TN3270	TIVLP34	TIVLP34	192.9.234.1	1	0	0	
	02/10/11 15:14:14	201.235.1.11	2023	TN3270	TIVLP35	TIVLP35	192.9.235.1	1	0	0	
	02/10/11 15:14:14	201.235.1.11	2023	TN3270	TIVMVS7	TIVMVS7	192.9.207.1	1	0	0	
	02/10/11 15:14:14	201.235.1.17	2023	TN3270	TIVLP34	TIVLP34	192.9.234.1	1	0	0	

Hub Time: Thu, 02/10/2011 03:35 PM | Server Available | Distributed DVIPA Targets - EDDIE - SYSADMIN

Figure 5. Distributed DVIPA Targets Workspace

Distributed DVIPA Unhealthy Servers Workspace

The Distributed DVIPA Unhealthy Servers workspace displays health statistics for application servers that reside on distributed DVIPA targets that are considered to be unhealthy.

To display this workspace, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **NetView** > *domain*, select and right-click **DDVIPA Server Health**, click **Workspace**, and then click **Distributed DVIPA Unhealthy Servers**.

If the NetView domain node that is shown in the navigator view represents the master NetView program, this workspace can contain sysplex-wide data. Otherwise, the workspace contains data for the z/OS image on which the NetView program resides.

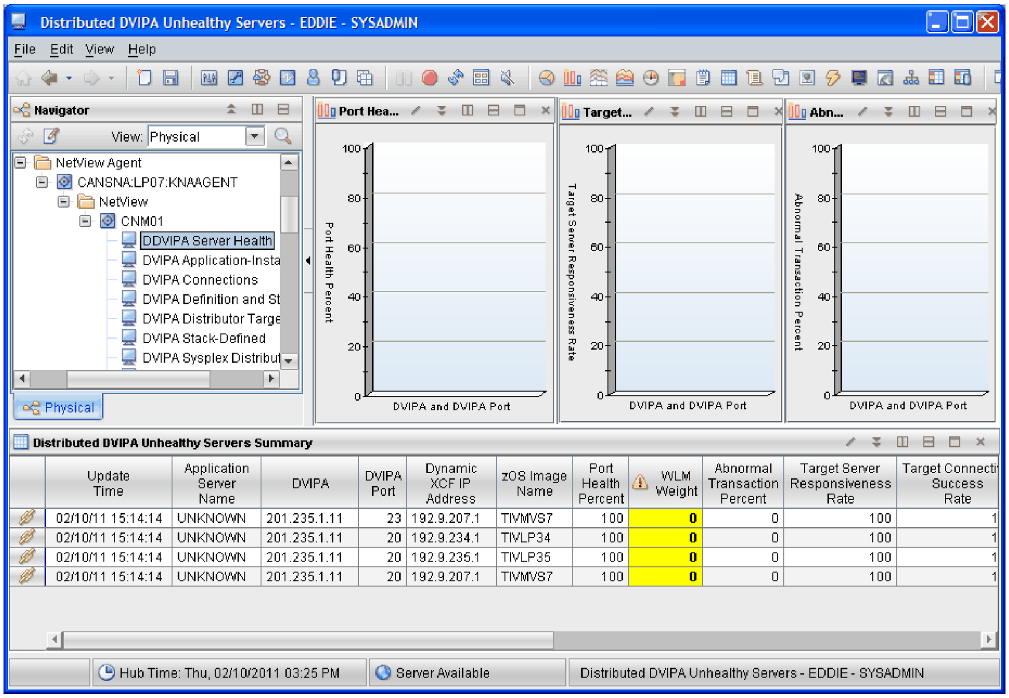
This workspace provides data that is updated by using sampling and events.

The queries for this workspace use the WLM Weight attribute to filter the rows that can be retrieved for display. Because of the default filter, you might not see all your application servers. You can modify the query to display more or fewer connections than the default filter allows.

Historical data is enabled in this workspace.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 6 on page 25.



Update Time	Application Server Name	DVIPA	DVIPA Port	Dynamic XCF IP Address	zOS Image Name	Port Health Percent	WLM Weight	Abnormal Transaction Percent	Target Server Responsiveness Rate	Target Connecti Success Rate
02/10/11 15:14:14	UNKNOWN	201.235.1.11	23	192.9.207.1	TIVMVS7	100	0	0	100	1
02/10/11 15:14:14	UNKNOWN	201.235.1.11	20	192.9.234.1	TIVLP34	100	0	0	100	1
02/10/11 15:14:14	UNKNOWN	201.235.1.11	20	192.9.235.1	TIVLP35	100	0	0	100	1
02/10/11 15:14:14	UNKNOWN	201.235.1.11	20	192.9.207.1	TIVMVS7	100	0	0	100	1

Hub Time: Thu, 02/10/2011 03:25 PM | Server Available | Distributed DVIPA Unhealthy Servers - EDDIE - SYSADMIN

Figure 6. Distributed DVIPA Unhealthy Servers Workspace

DVIPA Connections Workspace

The DVIPA Connections workspace displays connections involving a dynamic virtual IP address (DVIPA) and a DVIPA port.

To display this workspace, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **NetView** > *domain*, and then click **DVIPA Connections**.

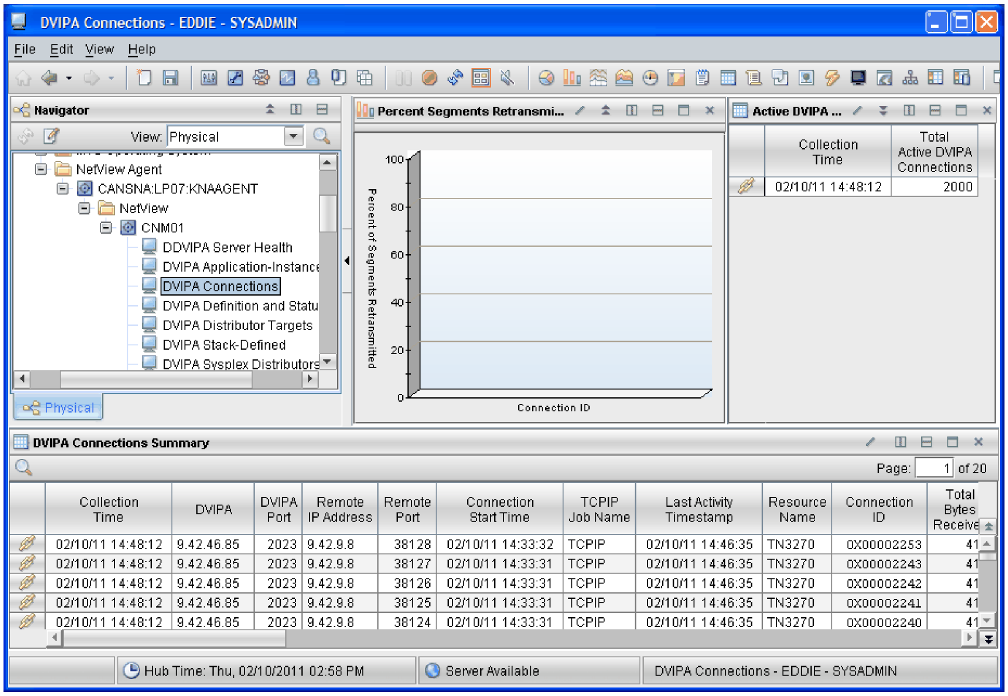
This workspace provides data that is updated by using sampling.

The queries for this workspace use the Byte Rate attribute to filter the rows that can be retrieved for display. Because of the default filter, you might not see all your connections. You can modify the query to display more or fewer connections than the default filter allows.

Historical data is not enabled in this workspace.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 7 on page 26.


DVIPA Connections - EDDIE - SYSADMIN
File Edit View Help
Navigator
View: Physical
NetView Agent
CANSNA:LP07:KNAAGENT
NetView
CNM01
DDVIPA Server Health
DVIPA Application-Instance
DVIPA Connections
DVIPA Definition and Statu
DVIPA Distributor Targets
DVIPA Stack-Defined
DVIPA Sysplex Distributors
Physical
Percent Segments Retransmi...
Percent of Segments Retransmitted
100
80
60
40
20
0
Connection ID
Active DVIPA ...
DVIPA Connections Summary
Page: 1 of 20
Hub Time: Thu, 02/10/2011 02:58 PM
Server Available
DVIPA Connections - EDDIE - SYSADMIN

Collection Time	Total Active DVIPA Connections
02/10/11 14:48:12	2000

Collection Time	DVIPA	DVIPA Port	Remote IP Address	Remote Port	Connection Start Time	TCPIP Job Name	Last Activity Timestamp	Resource Name	Connection ID	Total Bytes Receive
02/10/11 14:48:12	9.42.46.85	2023	9.42.9.8	38128	02/10/11 14:33:32	TCPIP	02/10/11 14:46:35	TN3270	0X00002253	41
02/10/11 14:48:12	9.42.46.85	2023	9.42.9.8	38127	02/10/11 14:33:31	TCPIP	02/10/11 14:46:35	TN3270	0X00002243	41
02/10/11 14:48:12	9.42.46.85	2023	9.42.9.8	38126	02/10/11 14:33:31	TCPIP	02/10/11 14:46:35	TN3270	0X00002242	41
02/10/11 14:48:12	9.42.46.85	2023	9.42.9.8	38125	02/10/11 14:33:31	TCPIP	02/10/11 14:46:35	TN3270	0X00002241	41
02/10/11 14:48:12	9.42.46.85	2023	9.42.9.8	38124	02/10/11 14:33:31	TCPIP	02/10/11 14:46:35	TN3270	0X00002240	41

Figure 7. DVIPA Connections Workspace

DVIPA Definition and Status Workspace

The DVIPA Definition and Status workspace displays the definition and status of the dynamic virtual IP addresses (DVIPAs).

To display this workspace, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **NetView** > *domain*, and then click **DVIPA Definition and Status**.

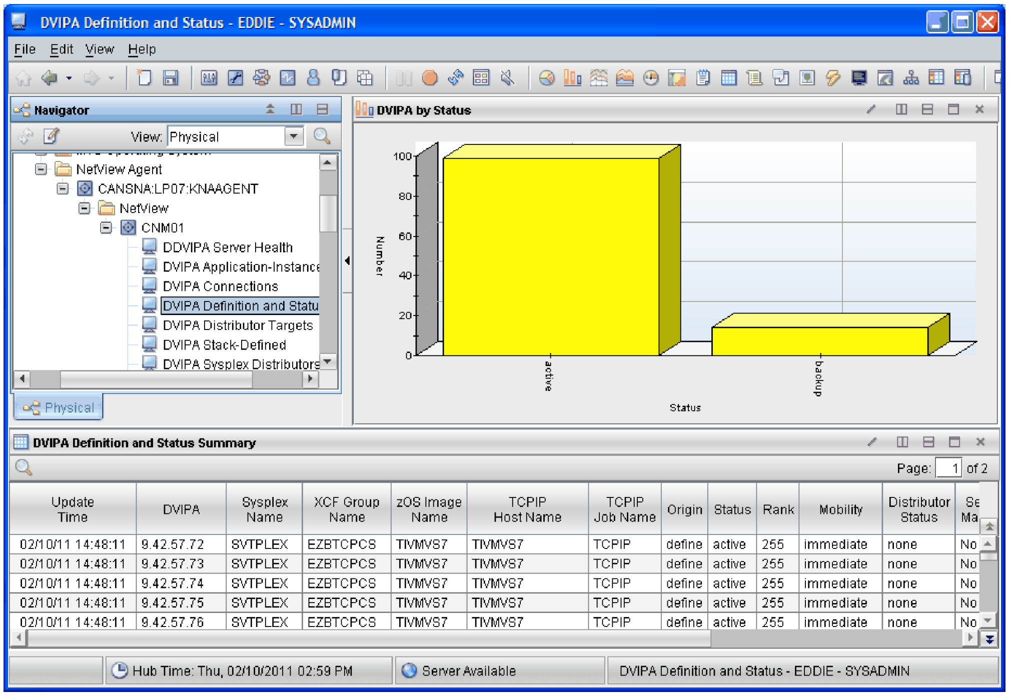
If the NetView domain node that is shown in the navigator view represents the master NetView program, this workspace can contain sysplex-wide data. Otherwise, the workspace contains data for the z/OS image on which the NetView program resides.

This workspace provides data that is updated by using sampling and events.

Historical data is not enabled in this workspace.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 8 on page 27.


DVIPA Definition and Status - EDDIE - SYSADMIN
File Edit View Help
Navigator
View: Physical
NetView Agent
CANSNA:LP07:KNAAGENT
NetView
CNM01
DDVIPA Server Health
DVIPA Application-Instance
DVIPA Connections
DVIPA Definition and Statu
DVIPA Distributor Targets
DVIPA Stack-Defined
DVIPA Sysplex Distributors
Physical
DVIPA by Status
100
80
60
40
20
0
Number
active
backup
Status
DVIPA Definition and Status Summary
Page: 1 of 2
Hub Time: Thu, 02/10/2011 02:59 PM
Server Available
DVIPA Definition and Status - EDDIE - SYSADMIN

Update Time	DVIPA	Sysplex Name	XCF Group Name	zOS Image Name	TCPIP Host Name	TCPIP Job Name	Origin	Status	Rank	Mobility	Distributor Status	Se Ma
02/10/11 14:48:11	9.42.57.72	SVTPLEX	EZBTCPCS	TIVMVS7	TIVMVS7	TCPIP	define	active	255	immediate	none	No
02/10/11 14:48:11	9.42.57.73	SVTPLEX	EZBTCPCS	TIVMVS7	TIVMVS7	TCPIP	define	active	255	immediate	none	No
02/10/11 14:48:11	9.42.57.74	SVTPLEX	EZBTCPCS	TIVMVS7	TIVMVS7	TCPIP	define	active	255	immediate	none	No
02/10/11 14:48:11	9.42.57.75	SVTPLEX	EZBTCPCS	TIVMVS7	TIVMVS7	TCPIP	define	active	255	immediate	none	No
02/10/11 14:48:11	9.42.57.76	SVTPLEX	EZBTCPCS	TIVMVS7	TIVMVS7	TCPIP	define	active	255	immediate	none	No

Figure 8. DVIPA Definition and Status Workspace

DVIPA Stack Summary Workspace

The DVIPA Stack Summary workspace displays DVIPA information for a specific stack (TCPIP Job Name) and z/OS image name.

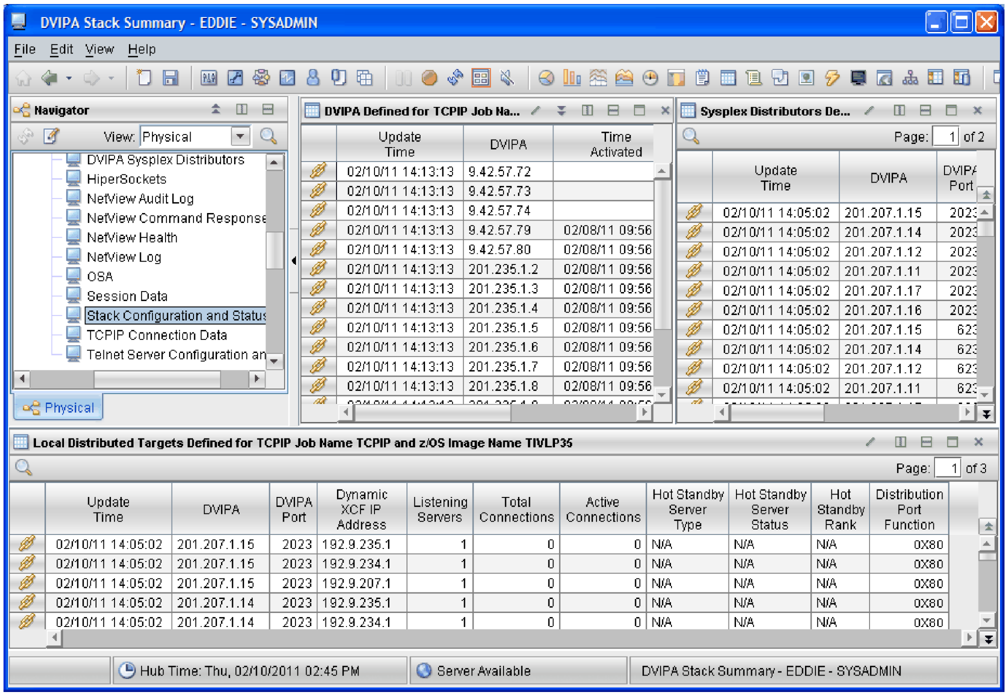
To display this workspace, click the link icon from a row in the Stack Configuration and Status workspace, the Stack Configuration and Status Summary table. See “Stack Configuration and Status Workspace” on page 49.

This workspace provides data that is updated by using sampling and events.

Historical data is enabled in this workspace for the Sysplex Distributors Defined and Local Distributed Targets Defined table views.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 9 on page 28.


DVIPA Stack Summary - EDDIE - SYSADMIN
File Edit View Help
Navigator
View: Physical
DVIPA Sysplex Distributors
HiperSockets
NetView Audit Log
NetView Command Response
NetView Health
NetView Log
OSA
Session Data
Stack Configuration and Status
TCPIP Connection Data
Telnet Server Configuration an
Physical
DVIPA Defined for TCPIP Job Na...
Sysplex Distributors De...
Page: 1 of 2
Local Distributed Targets Defined for TCPIP Job Name TCPIP and z/OS Image Name TIVLP35
Page: 1 of 3
Hub Time: Thu, 02/10/2011 02:45 PM
Server Available
DVIPA Stack Summary - EDDIE - SYSADMIN

DVIPA Defined for TCPIP Job Na...

Update Time	DVIPA	Time Activated
02/10/11 14:13:13	9.42.57.72	
02/10/11 14:13:13	9.42.57.73	
02/10/11 14:13:13	9.42.57.74	
02/10/11 14:13:13	9.42.57.79	02/08/11 09:56
02/10/11 14:13:13	9.42.57.80	02/08/11 09:56
02/10/11 14:13:13	201.235.1.2	02/08/11 09:56
02/10/11 14:13:13	201.235.1.3	02/08/11 09:56
02/10/11 14:13:13	201.235.1.4	02/08/11 09:56
02/10/11 14:13:13	201.235.1.5	02/08/11 09:56
02/10/11 14:13:13	201.235.1.6	02/08/11 09:56
02/10/11 14:13:13	201.235.1.7	02/08/11 09:56
02/10/11 14:13:13	201.235.1.8	02/08/11 09:56

Sysplex Distributors De...

Update Time	DVIPA	DVIPA Port
02/10/11 14:05:02	201.207.1.15	2023
02/10/11 14:05:02	201.207.1.14	2023
02/10/11 14:05:02	201.207.1.12	2023
02/10/11 14:05:02	201.207.1.11	2023
02/10/11 14:05:02	201.207.1.17	2023
02/10/11 14:05:02	201.207.1.16	2023
02/10/11 14:05:02	201.207.1.15	623
02/10/11 14:05:02	201.207.1.14	623
02/10/11 14:05:02	201.207.1.12	623
02/10/11 14:05:02	201.207.1.11	623

Local Distributed Targets Defined for TCPIP Job Name TCPIP and z/OS Image Name TIVLP35

Update Time	DVIPA	DVIPA Port	Dynamic XCF IP Address	Listening Servers	Total Connections	Active Connections	Hot Standby Server Type	Hot Standby Server Status	Hot Standby Rank	Distribution Port Function
02/10/11 14:05:02	201.207.1.15	2023	192.9.235.1	1	0	0	N/A	N/A	N/A	0X80
02/10/11 14:05:02	201.207.1.15	2023	192.9.234.1	1	0	0	N/A	N/A	N/A	0X80
02/10/11 14:05:02	201.207.1.15	2023	192.9.207.1	1	0	0	N/A	N/A	N/A	0X80
02/10/11 14:05:02	201.207.1.14	2023	192.9.235.1	1	0	0	N/A	N/A	N/A	0X80
02/10/11 14:05:02	201.207.1.14	2023	192.9.234.1	1	0	0	N/A	N/A	N/A	0X80

Figure 9. DVIPA Stack Summary Workspace

DVIPA Sysplex Distributors Workspace

The DVIPA Sysplex Distributors workspace displays information about DVIPA sysplex distributors.

To display this workspace, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **NetView** > *domain*, and then click **DVIPA Sysplex Distributors**.

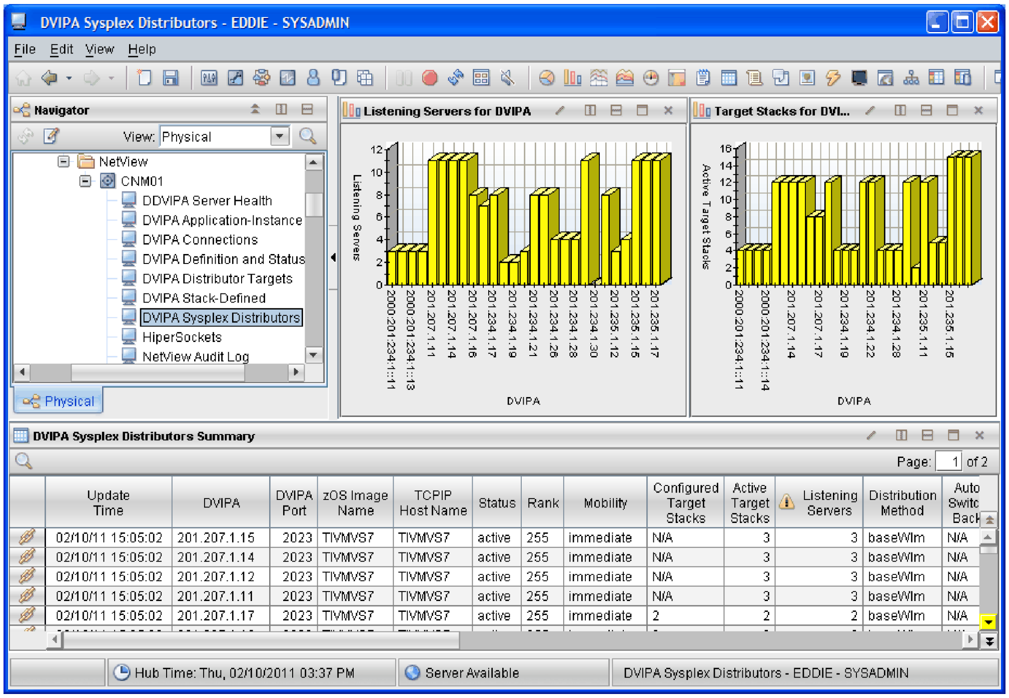
If the NetView domain node that is shown in the navigator view represents the master NetView program, this workspace can contain sysplex-wide data. Otherwise, the workspace contains data for the z/OS image on which the NetView program resides.

This workspace provides data that is updated by using sampling and events.

Historical data is enabled in this workspace.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 10 on page 29.



	Update Time	DVIPA	DVIPA Port	zOS Image Name	TCPIP Host Name	Status	Rank	Mobility	Configured Target Stacks	Active Target Stacks	⚠ Listening Servers	Distribution Method	Auto Switc Back
	02/10/11 15:05:02	201.207.1.15	2023	TIVMVS7	TIVMVS7	active	255	immediate	N/A	3	3	baseWlm	N/A
	02/10/11 15:05:02	201.207.1.14	2023	TIVMVS7	TIVMVS7	active	255	immediate	N/A	3	3	baseWlm	N/A
	02/10/11 15:05:02	201.207.1.12	2023	TIVMVS7	TIVMVS7	active	255	immediate	N/A	3	3	baseWlm	N/A
	02/10/11 15:05:02	201.207.1.11	2023	TIVMVS7	TIVMVS7	active	255	immediate	N/A	3	3	baseWlm	N/A
	02/10/11 15:05:02	201.207.1.17	2023	TIVMVS7	TIVMVS7	active	255	immediate	2	2	2	baseWlm	N/A

Figure 10. DVIPA Sysplex Distributors Workspace

DVIPA Workload

The DVIPA Workload workspace displays information about the distributed DVIPA targets for the selected distributed DVIPA and distributed DVIPA port.

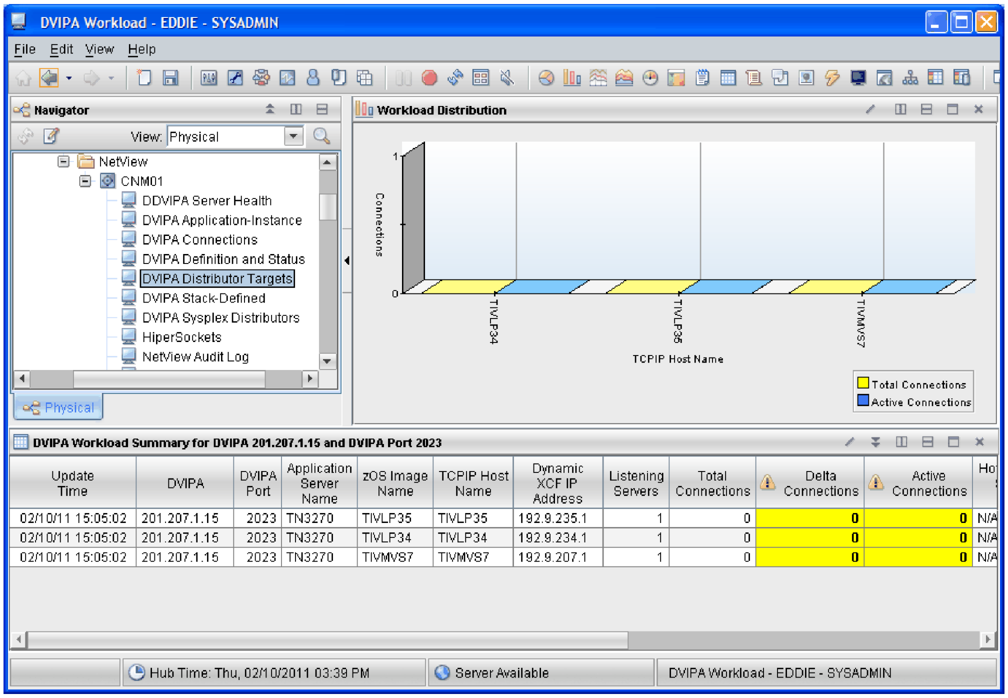
To display this workspace, click the link icon from a row in the Distributed DVIPA Targets and Filtered Distributed DVIPA Targets workspaces, the Distributed DVIPA Targets Summary table. See “Distributed DVIPA Targets Workspace” on page 23.

This workspace provides data that is updated by using sampling.

Historical data is enabled in this workspace.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 11 on page 30.



DVIPA Workload Summary for DVIPA 201.207.1.15 and DVIPA Port 2023

Update Time	DVIPA	DVIPA Port	Application Server Name	zOS Image Name	TCPIP Host Name	Dynamic XCF IP Address	Listening Servers	Total Connections	Delta Connections	Active Connections	Ho
02/10/11 15:05:02	201.207.1.15	2023	TN3270	TIVLP35	TIVLP35	192.9.235.1	1	0	0	0	N/A
02/10/11 15:05:02	201.207.1.15	2023	TN3270	TIVLP34	TIVLP34	192.9.234.1	1	0	0	0	N/A
02/10/11 15:05:02	201.207.1.15	2023	TN3270	TIVMVS7	TIVMVS7	192.9.207.1	1	0	0	0	N/A

Figure 11. DVIPA Workload Workspace

Filtered Distributed DVIPA Server Health Workspace

The Filtered Distributed DVIPA Server Health workspace displays health statistics for all application servers that reside on distributed DVIPA targets.

To display this workspace, click the link icon from a row in one of the following views:

- Distributed DVIPA Targets and Filtered Distributed DVIPA Targets workspaces, the Distributed DVIPA Targets Summary table. See “Distributed DVIPA Targets Workspace” on page 23.
- DVIPA Stack Summary workspace, the Local Distributed Targets Defined table. See “DVIPA Stack Summary Workspace” on page 27.

This workspace provides the same views, thresholds, and links that are provided in the Distributed DVIPA Server Health workspace. See “Distributed DVIPA Server Health Workspace” on page 21.

Filtered Distributed DVIPA Targets Workspace

The Filtered Distributed DVIPA Targets workspace displays information about the distributed DVIPA targets.

To display this workspace, click the link icon from a row in one of the following views:

- DVIPA Sysplex Distributors and Filtered DVIPA Sysplex Distributors workspaces, the DVIPA Sysplex Distributors Summary table. See “DVIPA Sysplex Distributors Workspace” on page 28.

- DVIPA Stack Summary workspace, the Sysplex Distributors Defined table or the Local Distributed Targets Defined table. See “DVIPA Stack Summary Workspace” on page 27.

This workspace provides the same views, thresholds, and links that are provided in the Distributed DVIPA Targets workspace. See “Distributed DVIPA Targets Workspace” on page 23.

Filtered Distributed DVIPA Unhealthy Servers Workspace

The Filtered Distributed DVIPA Unhealthy Servers workspace displays health statistics for application servers that reside on distributed DVIPA targets that are considered to be unhealthy.

To display this workspace, click the link icon from a row in one of the following views:

- Distributed DVIPA Targets and Filtered Distributed DVIPA Targets workspaces, the Distributed DVIPA Targets Summary table. See “Distributed DVIPA Targets Workspace” on page 23.
- DVIPA Stack Summary workspace, the Local Distributed Targets Defined table. See “DVIPA Stack Summary Workspace” on page 27.

This workspace provides the same views that are provided in the Distributed DVIPA Unhealthy Servers workspace. See “Distributed DVIPA Unhealthy Servers Workspace” on page 24.

Filtered DVIPA Connections Workspace

The Filtered DVIPA Connections workspace displays connections involving a dynamic virtual IP address (DVIPA) and a DVIPA port.

To display this workspace, click the link icon from a row in one of the following views:

- DVIPA Connections workspace, the Active DVIPA Connection Count table or the DVIPA Connections Summary table. See “DVIPA Connections Workspace” on page 25.
- Distributed DVIPA Targets and Filtered Distributed DVIPA Targets workspaces, the Distributed DVIPA Targets Summary table. See “Distributed DVIPA Targets Workspace” on page 23.

Note: If you display this workspace using a link filter window, the summary table is titled "Filtered DVIPA Connections Summary". Otherwise, the summary table is titled "DVIPA Connections Summary".

This workspace provides the same views and thresholds that are provided in the DVIPA Connections workspace. However, the only link provided from the Filtered DVIPA Connections Summary table is the **Distributed DVIPA Connection Routing** link. See “DVIPA Connections Workspace” on page 25.

Filtered DVIPA Definition and Status Workspace

The Filtered DVIPA Definition and Status workspace displays the status of the dynamic virtual IP addresses (DVIPAs).

To display this workspace, click the link icon from a row in the DVIPA Stack Summary workspace, the DVIPA Defined table. See “DVIPA Stack Summary Workspace” on page 27.

This workspace provides the same views and thresholds that are provided in the DVIPA Definition and Status workspace. See “DVIPA Definition and Status Workspace” on page 26.

Filtered DVIPA Sysplex Distributors Workspace

The Filtered DVIPA Sysplex Distributors workspace displays information about DVIPA sysplex distributors.

To display this workspace, click the link icon from a row in the DVIPA Stack Summary workspace, the Sysplex Distributors Defined table. See “DVIPA Stack Summary Workspace” on page 27.

This workspace provides the same the same views, thresholds and links that are provided in the DVIPA Sysplex Distributors workspace. See “DVIPA Sysplex Distributors Workspace” on page 28.

Stack-Defined DVIPA Workspace

The Stack-Defined DVIPA workspace displays the definition and status of the stack-defined DVIPA.

To display this workspace, expand **z/OS Systems >** *system* **> NetView Agent >** *subagent* **> NetView >** *domain*, and then click **DVIPA Stack-Defined**.

If the NetView domain node that is shown in the navigator view represents the master NetView program, this workspace can contain sysplex-wide data. Otherwise, the workspace contains data for the z/OS image on which the NetView program resides.

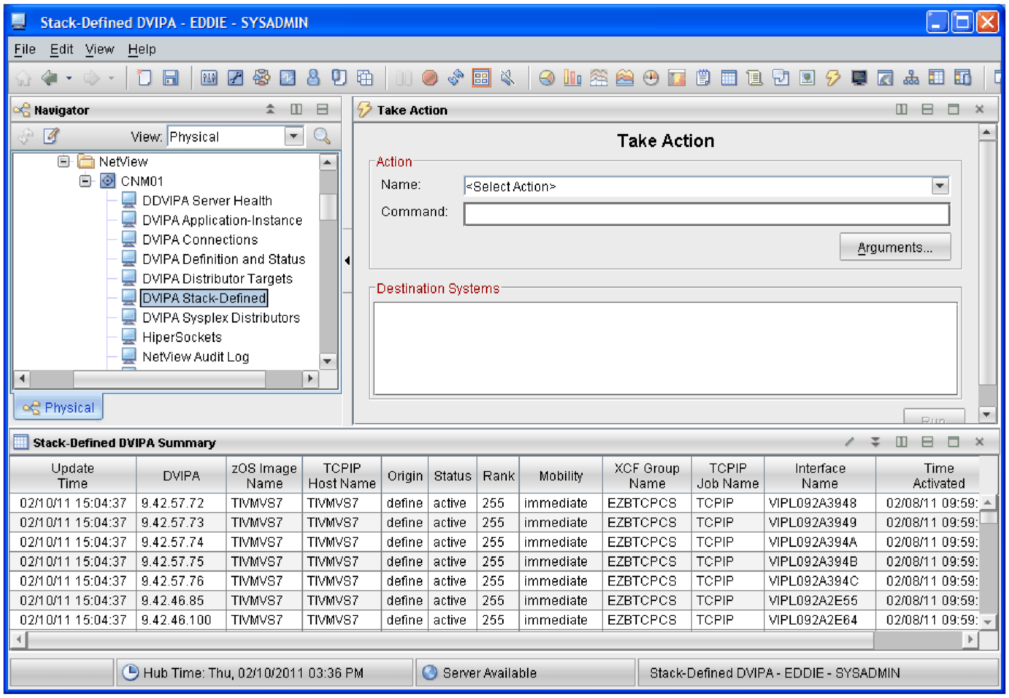
This workspace provides data that is updated by using sampling and events.

The queries for this workspace use the Origin and Distributor Status attributes to filter the rows that can be retrieved for display. All data that matches Origin=define or Origin=backup and matches Distributor Status=none is displayed in the workspace.

Historical data is not enabled in this workspace.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 12 on page 33.



Name: <Select Action>

Command:

Stack-Defined DVIPA Summary

Update Time	DVIPA	zOS Image Name	TCPIP Host Name	Origin	Status	Rank	Mobility	XCF Group Name	TCPIP Job Name	Interface Name	Time Activated
02/10/11 15:04:37	9.42.57.72	TIVMVS7	TIVMVS7	define	active	255	immediate	EZBTCPCS	TCPIP	VIPL092A3948	02/08/11 09:59:
02/10/11 15:04:37	9.42.57.73	TIVMVS7	TIVMVS7	define	active	255	immediate	EZBTCPCS	TCPIP	VIPL092A3949	02/08/11 09:59:
02/10/11 15:04:37	9.42.57.74	TIVMVS7	TIVMVS7	define	active	255	immediate	EZBTCPCS	TCPIP	VIPL092A394A	02/08/11 09:59:
02/10/11 15:04:37	9.42.57.75	TIVMVS7	TIVMVS7	define	active	255	immediate	EZBTCPCS	TCPIP	VIPL092A394B	02/08/11 09:59:
02/10/11 15:04:37	9.42.57.76	TIVMVS7	TIVMVS7	define	active	255	immediate	EZBTCPCS	TCPIP	VIPL092A394C	02/08/11 09:59:
02/10/11 15:04:37	9.42.46.85	TIVMVS7	TIVMVS7	define	active	255	immediate	EZBTCPCS	TCPIP	VIPL092A2E55	02/08/11 09:59:
02/10/11 15:04:37	9.42.46.100	TIVMVS7	TIVMVS7	define	active	255	immediate	EZBTCPCS	TCPIP	VIPL092A2E64	02/08/11 09:59:

Hub Time: Thu, 02/10/2011 03:36 PM

Server Available

Stack-Defined DVIPA - EDDIE - SYSADMIN

Figure 12. Stack-Defined DVIPA Workspace

VIPA Routes Workspace

The VIPA Routes workspace displays VIPA route information for a specific stack and z/OS image name. This information is available only for z/OS V1R11 Communications Server or later.

To display this workspace, click the link icon from a row in the DVIPA Sysplex Distributors workspace, the DVIPA Sysplex Distributors Summary table. See "DVIPA Sysplex Distributors Workspace" on page 28.

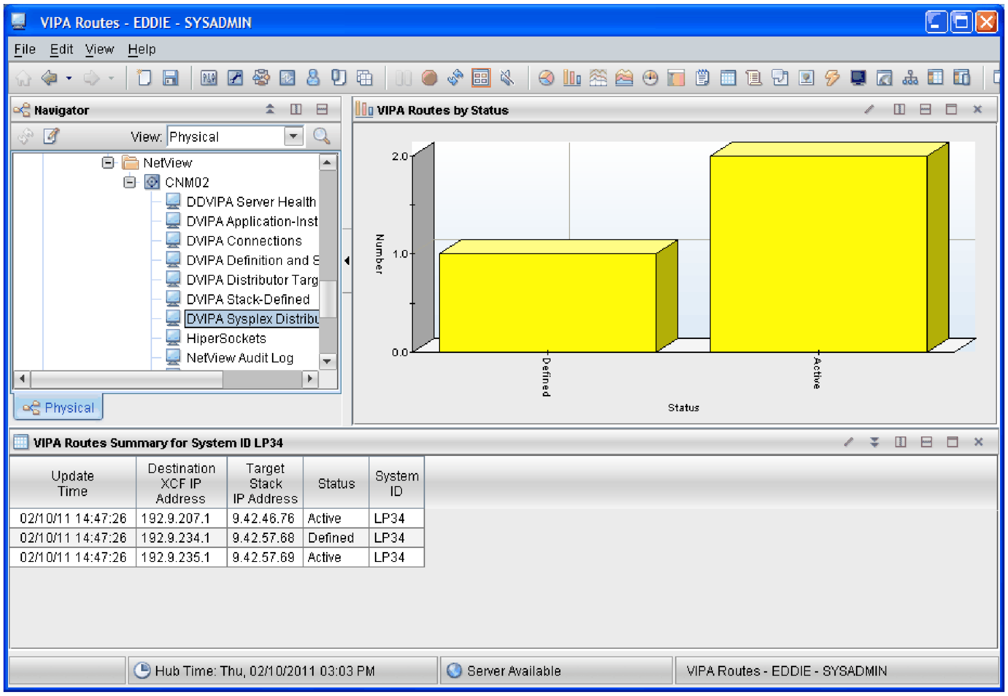
If the NetView domain node that is shown in the navigator view represents the master NetView program, this workspace can contain sysplex-wide data. Otherwise, the workspace contains data for the z/OS image on which the NetView program resides.

This workspace provides data that is updated by using sampling and events.

Historical data is not enabled in this workspace.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 13 on page 34.



Update Time	Destination XCF IP Address	Target Stack IP Address	Status	System ID
02/10/11 14:47:26	192.9.207.1	9.42.46.76	Active	LP34
02/10/11 14:47:26	192.9.234.1	9.42.57.68	Defined	LP34
02/10/11 14:47:26	192.9.235.1	9.42.57.69	Active	LP34

Figure 13. VIPA Routes Workspace

Chapter 4. TCP/IP Connection Workspaces

The TCP/IP connection workspaces provide information about active and inactive TCP/IP connections in your network. The following workspaces for TCP/IP connections, which are listed in alphabetical order, are provided:

- "Filtered Inactive TCPIP Connection Data Workspace"
- "Filtered TCPIP Connection Data Workspace"
- "Inactive TCPIP Connection Data Workspace"
- "TCPIP Connection Data Workspace" on page 37

Filtered Inactive TCPIP Connection Data Workspace

The Filtered Inactive TCPIP Connection Data workspace displays information about the inactive TCP/IP connections.

To display this workspace, click the link icon from a row in one of the following views:

- Inactive TCPIP Connection Data workspace, the Inactive TCPIP Connection Count table or the Inactive TCPIP Connection Data Summary table. See "Inactive TCPIP Connection Data Workspace."
- TCPIP Connection Data workspace, the TCPIP Connection Data Summary table. See "TCPIP Connection Data Workspace" on page 37.

This workspace provides the same views and thresholds that are provided in the Inactive TCPIP Connection Data workspace, except that no links are defined for this workspace. See "Inactive TCPIP Connection Data Workspace."

Filtered TCPIP Connection Data Workspace

The Filtered TCPIP Connection Data workspace displays information about the active TCP/IP connections.

To display this workspace, click the link icon from a row in the TCPIP Connection Data workspace, the Active TCPIP Connection Count table or the TCPIP Connection Data Summary table. See "TCPIP Connection Data Workspace" on page 37.

Note: If you are using the GDPS Active/Active Continuous Availability solution, you can also link to this workspace from the Workload Lifeline Advisors workspace.

This workspace provides the same views and thresholds that are provided in the TCPIP Connection Data workspace, except that no links are defined for this workspace. See "TCPIP Connection Data Workspace" on page 37.

Inactive TCPIP Connection Data Workspace

The Inactive TCPIP Connection Data workspace displays information about inactive TCP/IP connections. It displays the most recent inactive connections that you specified to keep on DASD for this LPAR.

To display this workspace, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **NetView** > *domain*, right-click **TCPIP Connection Data**, click **Workspace**, and then click **Inactive TCPIP Connection Data**.

Note: You can also link to this workspace from the TCPIP Connection Data workspace.

This workspace provides data that is updated by using sampling.

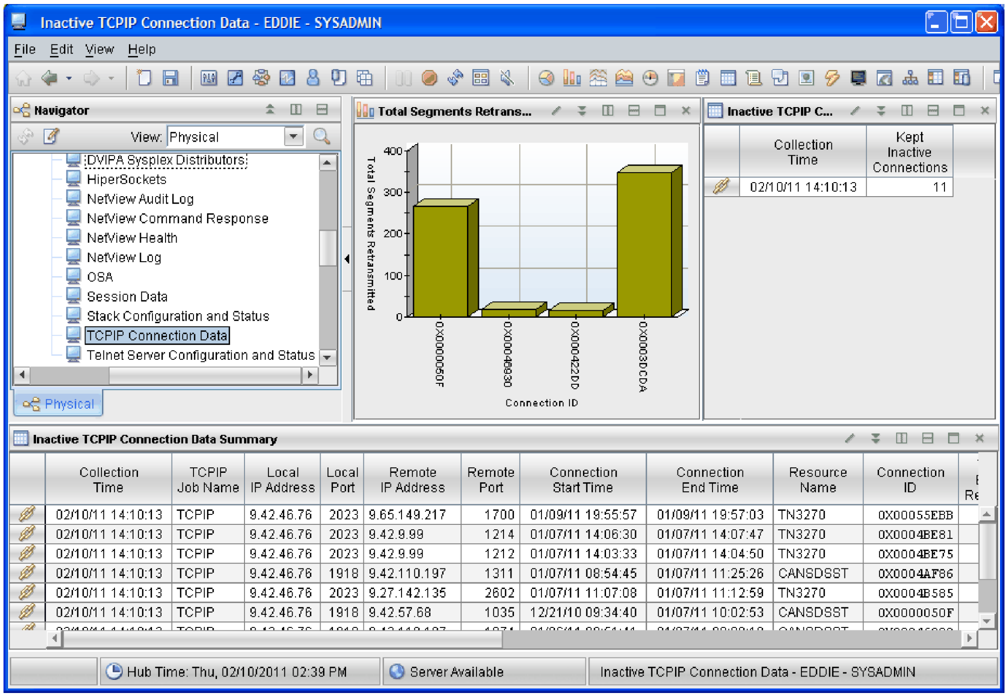
The queries for this workspace use the Byte Rate attribute to filter the rows that can be retrieved for display. Because of the default filter, you might not see all your connections. You can modify the query to display more or fewer connections than the default filter allows.

If you have a large installation, you might not be able to view all the available connections in the Tivoli Enterprise Portal. For more information, see the *IBM Tivoli NetView for z/OS Tuning Guide*.

Historical data is enabled in this workspace for all views except the Inactive TCPIP Connection Count view. When you view historical data in this view, all rows with collection times in the specified time span are displayed.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 14.



Collection Time	Kept Inactive Connections
02/10/11 14:10:13	11

Collection Time	TCPIP Job Name	Local IP Address	Local Port	Remote IP Address	Remote Port	Connection Start Time	Connection End Time	Resource Name	Connection ID
02/10/11 14:10:13	TCPIP	9.42.46.76	2023	9.65.149.217	1700	01/09/11 19:55:57	01/09/11 19:57:03	TN3270	0X00055EBB
02/10/11 14:10:13	TCPIP	9.42.46.76	2023	9.42.9.99	1214	01/07/11 14:06:30	01/07/11 14:07:47	TN3270	0X0004BE81
02/10/11 14:10:13	TCPIP	9.42.46.76	2023	9.42.9.99	1212	01/07/11 14:03:33	01/07/11 14:04:50	TN3270	0X0004BE75
02/10/11 14:10:13	TCPIP	9.42.46.76	1918	9.42.110.197	1311	01/07/11 08:54:45	01/07/11 11:25:26	CANSDSST	0X0004AF86
02/10/11 14:10:13	TCPIP	9.42.46.76	2023	9.27.142.135	2602	01/07/11 11:07:08	01/07/11 11:12:59	TN3270	0X0004B585
02/10/11 14:10:13	TCPIP	9.42.46.76	1918	9.42.57.68	1035	12/21/10 09:34:40	01/07/11 10:02:53	CANSDSST	0X0000050F

Hub Time: Thu, 02/10/2011 02:39 PM

Server Available

Inactive TCPIP Connection Data - EDDIE - SYSADMIN

Figure 14. Inactive TCPIP Connection Data Workspace

TCPIP Connection Data Workspace

The TCPIP Connection Data workspace displays information about the active TCP/IP connections. It displays information about active TCP/IP connections on this LPAR for stacks that you have defined on the TCPCONN.ROWSA.&CNMTCPN statement in the CNMSTYLE member.

To display this workspace, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **NetView** > *domain*, and then click **TCPIP Connection Data**.

This workspace provides data that is updated by using sampling.

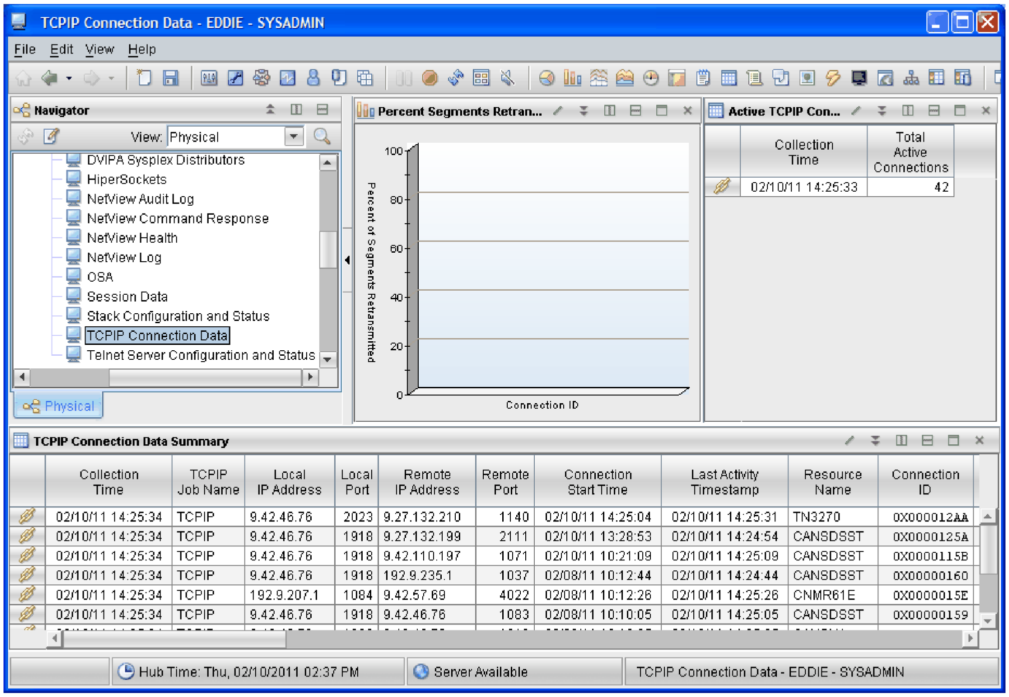
The queries for this workspace use the Byte Rate attribute to filter the rows that can be retrieved for display. Because of the default filter, you might not see all your connections. You can modify the query to display more or fewer connections than the default filter allows.

If you have a large installation, you might not be able to view all the available connections in the Tivoli Enterprise Portal. For more information, see the *IBM Tivoli NetView for z/OS Tuning Guide*.

Historical data is enabled in this workspace. When you view historical data in this workspace, all rows with collection times in the specified time span are displayed.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 15.


TCPIP Connection Data - EDDIE - SYSADMIN
File
Edit
View
Help
Navigator
View: Physical
DVIPA Sysplex Distributors
HiperSockets
NetView Audit Log
NetView Command Response
NetView Health
NetView Log
OSA
Session Data
Stack Configuration and Status
TCPIP Connection Data
Telnet Server Configuration and Status
Physical
Percent Segments Retran...
100
80
60
40
20
0
Percent of Segments Retransmitted
Connection ID
Active TCPIP Con...
TCPIP Connection Data Summary
Hub Time: Thu, 02/10/2011 02:37 PM
Server Available
TCPIP Connection Data - EDDIE - SYSADMIN

Collection Time	Total Active Connections
02/10/11 14:25:33	42

Collection Time	TCPIP Job Name	Local IP Address	Local Port	Remote IP Address	Remote Port	Connection Start Time	Last Activity Timestamp	Resource Name	Connection ID
02/10/11 14:25:34	TCPIP	9.42.46.76	2023	9.27.132.210	1140	02/10/11 14:25:04	02/10/11 14:25:31	TN3270	0X000012AA
02/10/11 14:25:34	TCPIP	9.42.46.76	1918	9.27.132.199	2111	02/10/11 13:28:53	02/10/11 14:24:54	CANSDSST	0X0000125A
02/10/11 14:25:34	TCPIP	9.42.46.76	1918	9.42.110.197	1071	02/10/11 10:21:09	02/10/11 14:25:09	CANSDSST	0X0000115B
02/10/11 14:25:34	TCPIP	9.42.46.76	1918	192.9.235.1	1037	02/08/11 10:12:44	02/10/11 14:24:44	CANSDSST	0X00000160
02/10/11 14:25:34	TCPIP	192.9.207.1	1084	9.42.57.69	4022	02/08/11 10:12:26	02/10/11 14:25:26	CNMR61E	0X0000015E
02/10/11 14:25:34	TCPIP	9.42.46.76	1918	9.42.46.76	1083	02/08/11 10:10:05	02/10/11 14:25:05	CANSDSST	0X00000159

Figure 15. TCPIP Connection Data Workspace

Chapter 5. NetView Health Workspaces

The NetView Health workspaces show the status and performance of NetView applications and tasks. The following workspaces for NetView health, which are listed in alphabetical order, are provided:
- "NetView Applications Workspace"
- "NetView Task Details Workspace" on page 40
- "NetView Tasks Workspace" on page 41

NetView Applications Workspace

The NetView Applications workspace displays information about the NetView applications.

To display this workspace, expand **z/OS Systems >** *system* **> NetView Agent >** *subagent* **> NetView >** *domain*, and then click **NetView Health**.

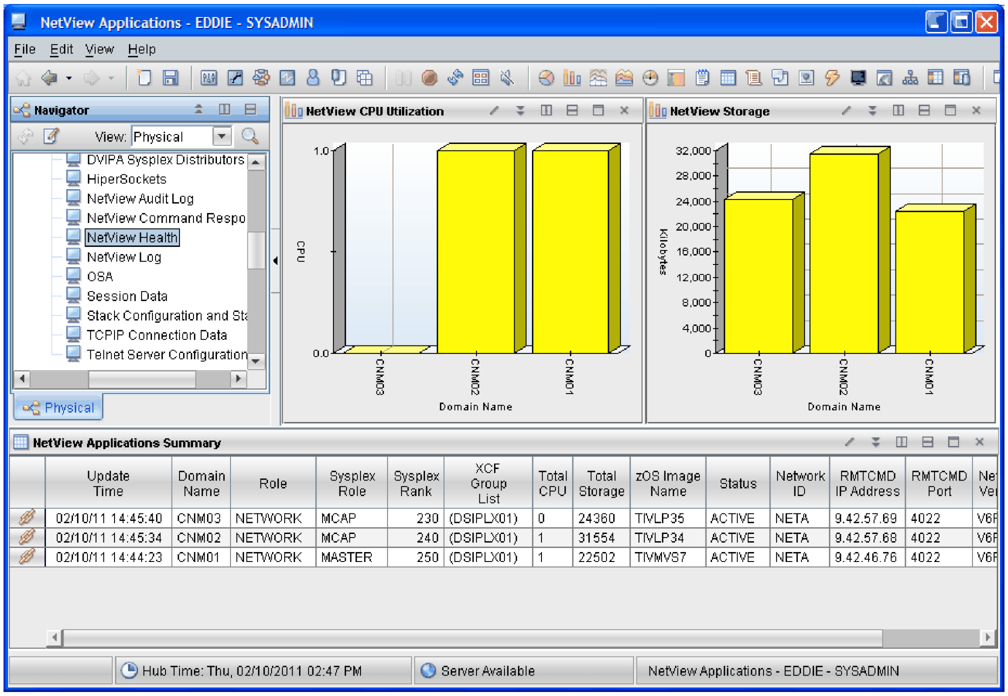
If the NetView domain node that is shown in the navigator view represents the master NetView program, this workspace can contain sysplex-wide data. Otherwise, the workspace contains data for the z/OS image on which the NetView program resides.

This workspace provides data that is updated by using sampling and events.

Historical data is enabled in this workspace.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 16 on page 40.



	Update Time	Domain Name	Role	Sysplex Role	Sysplex Rank	XCF Group List	Total CPU	Total Storage	zOS Image Name	Status	Network ID	RMTCMD IP Address	RMTCMD Port	Ne Ve
	02/10/11 14:45:40	CNM03	NETWORK	MCAP	230	(DSIPLX01)	0	24360	TIVLP35	ACTIVE	NETA	9.42.57.69	4022	V6F
	02/10/11 14:45:34	CNM02	NETWORK	MCAP	240	(DSIPLX01)	1	31554	TIVLP34	ACTIVE	NETA	9.42.57.68	4022	V6F
	02/10/11 14:44:23	CNM01	NETWORK	MASTER	250	(DSIPLX01)	1	22502	TIVMVS7	ACTIVE	NETA	9.42.46.76	4022	V6F

Figure 16. NetView Applications Workspace

NetView Task Details Workspace

The NetView Task Details workspace displays six performance statistics for the task over time. It displays line charts for the NetView task showing either historical data or a single point for the most recent collection.

To display this workspace, click the link icon for a row in the NetView Tasks workspace, the NetView Tasks Summary table. See “NetView Tasks Workspace” on page 41.

This workspace provides data that is updated by using sampling.

Historical data is enabled in this workspace.

The data in this workspace is provided using historical data collection. When you view historical data in this workspace, all rows with collection times that are in the specified time span are displayed. If historical data is available and you specified a valid time span, the workspace displays a series of points for the historical data within the specified time span. Otherwise, only one point representing the most recent collection is displayed in the workspace.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 17 on page 41.

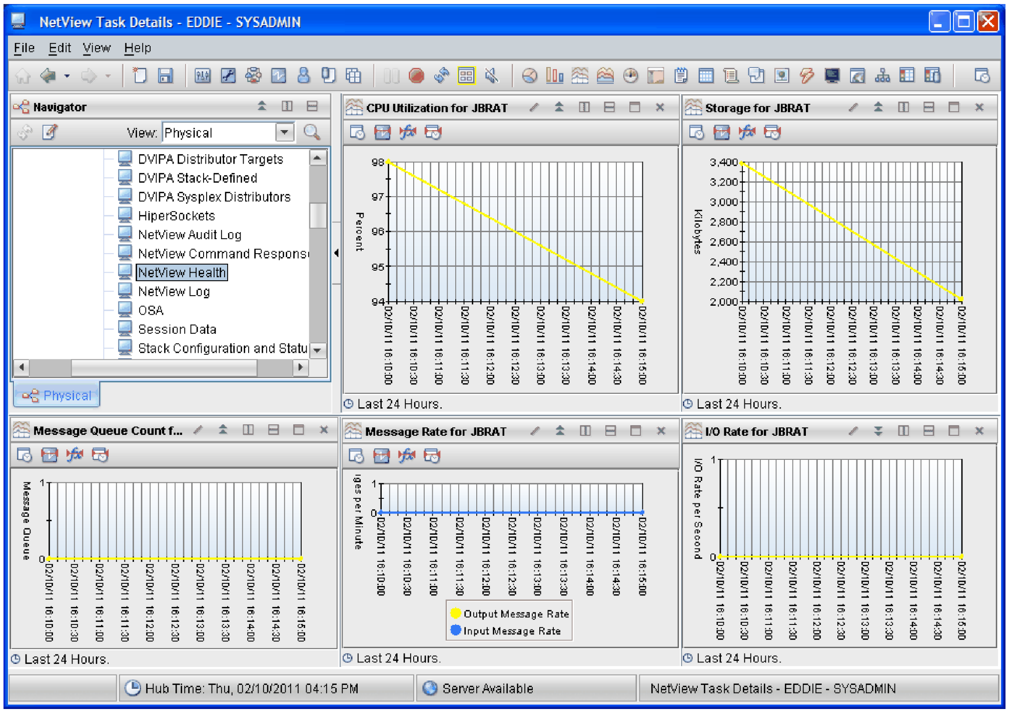


Figure 17. NetView Task Details Workspace

NetView Tasks Workspace

The NetView Tasks workspace provides task status and performance statistics for all NetView tasks.

To display this workspace, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **NetView** > *domain*, select and right-click **NetView Health**, click **Workspace**, and then click **NetView Tasks**.

You can also link to this workspace from the NetView Applications workspace.

This workspace provides data that is updated by using sampling.

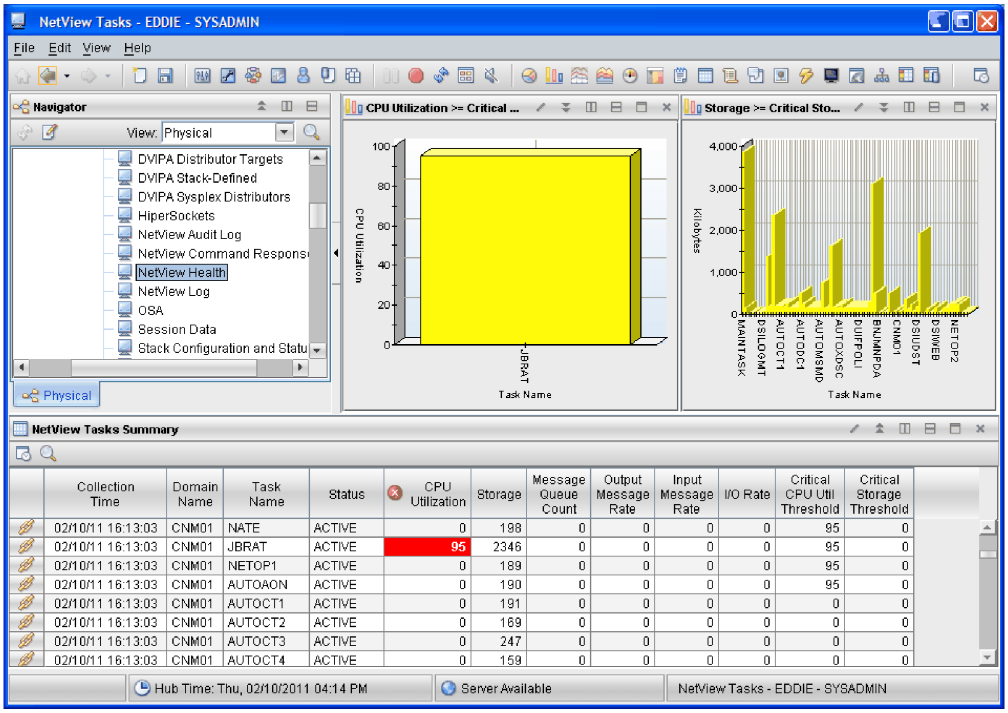
The tasks shown in the bar chart views (CPU Utilization >= Critical CPU Util Threshold and Storage >= Critical Storage Threshold) use values defined with the WRNCPU, WRNSTG, MAXCPU, and MAXSTG keywords of the DEFAULTS and OVERRIDE commands. If you specify one or more values for the WRNCPU or WRNSTG keywords, then the maximum of the specified values is compared to the current CPU or storage statistic for the task. If the current CPU or storage statistic is greater than or equal to the maximum WRNCPU or maximum WRNSTG value, the task is displayed in the appropriate view. If a WRNCPU or WRNSTG value was not specified for the task, then the MAXCPU and MAXSTG values are used to determine whether the task is displayed in the view.

A situation for each performance statistic is provided for critical, warning, and informational levels. To provide a warning that a task is approaching the value when it might be penalized, the values for all of the situations should be below the maximum value specified for these statistics on the DEFAULTS and OVERRIDE commands.

Historical data is enabled in this workspace. When you view historical data in this workspace, all rows with collection times that are in the specified time span are displayed.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 18.



Collection Time	Domain Name	Task Name	Status	CPU Utilization	Storage	Message Queue Count	Output Message Rate	Input Message Rate	I/O Rate	Critical CPU Util Threshold	Critical Storage Threshold
02/10/11 16:13:03	CNM01	NATE	ACTIVE	0	198	0	0	0	0	95	0
02/10/11 16:13:03	CNM01	JBRAT	ACTIVE	95	2346	0	0	0	0	95	0
02/10/11 16:13:03	CNM01	NETOP1	ACTIVE	0	189	0	0	0	0	95	0
02/10/11 16:13:03	CNM01	AUTOAON	ACTIVE	0	190	0	0	0	0	95	0
02/10/11 16:13:03	CNM01	AUTOCT1	ACTIVE	0	191	0	0	0	0	0	0
02/10/11 16:13:03	CNM01	AUTOCT2	ACTIVE	0	169	0	0	0	0	0	0
02/10/11 16:13:03	CNM01	AUTOCT3	ACTIVE	0	247	0	0	0	0	0	0
02/10/11 16:13:03	CNM01	AUTOCT4	ACTIVE	0	159	0	0	0	0	0	0

Hub Time: Thu, 02/10/2011 04:14 PM

Server Available

NetView Tasks - EDDIE - SYSADMIN

Figure 18. NetView Tasks Workspace

Chapter 6. Other NetView Workspaces

The following additional NetView for z/OS Enterprise Management Agent workspaces, which are listed in alphabetical order, are provided:

- "Filtered Session Data Workspace"
- "Filtered Telnet Server Configuration and Status Workspace"
- "HiperSockets Configuration and Status Workspace"
- "NetView Audit Log Workspace" on page 44
- "NetView Command Response Workspace" on page 45
- "NetView Log Workspace" on page 46
- "OSA Channels and Ports Workspace" on page 47
- "Session Data Workspace" on page 48
- "Stack Configuration and Status Workspace" on page 49
- "Telnet Server Configuration and Status Workspace" on page 50

Filtered Session Data Workspace

The Filtered Session Data workspace displays information about the active SNA sessions.

To display this workspace, click the link icon from a row in the Session Data workspace, the Active Session Count table or the Session Data Summary table. See "Session Data Workspace" on page 48.

This workspace provides the same views and thresholds that are provided in the Session Data workspace, except that no links are defined for this workspace. See "Session Data Workspace" on page 48.

Filtered Telnet Server Configuration and Status Workspace

The Filtered Telnet Server Configuration and Status workspace displays information about Telnet servers.

To display this workspace, click the link icon from a row in the Stack Configuration and Status workspace, the Stack Configuration and Status Summary table. See "Stack Configuration and Status Workspace" on page 49.

This workspace provides the same views and thresholds that are provided in the Telnet Server Configuration and Status workspace, except that no links are defined for this workspace. See "Telnet Server Configuration and Status Workspace" on page 50.

HiperSockets Configuration and Status Workspace

The HiperSockets Configuration and Status workspace displays configuration and status information for HiperSockets. This information is available only for z/OS V1R11 Communications Server or later, and the data collection for this information requires Resource Object Data Manager (RODM).

To display this workspace, expand **z/OS Systems >** *system* **> NetView Agent >** *subagent* **> NetView >** *domain*, and then click **HiperSockets**.

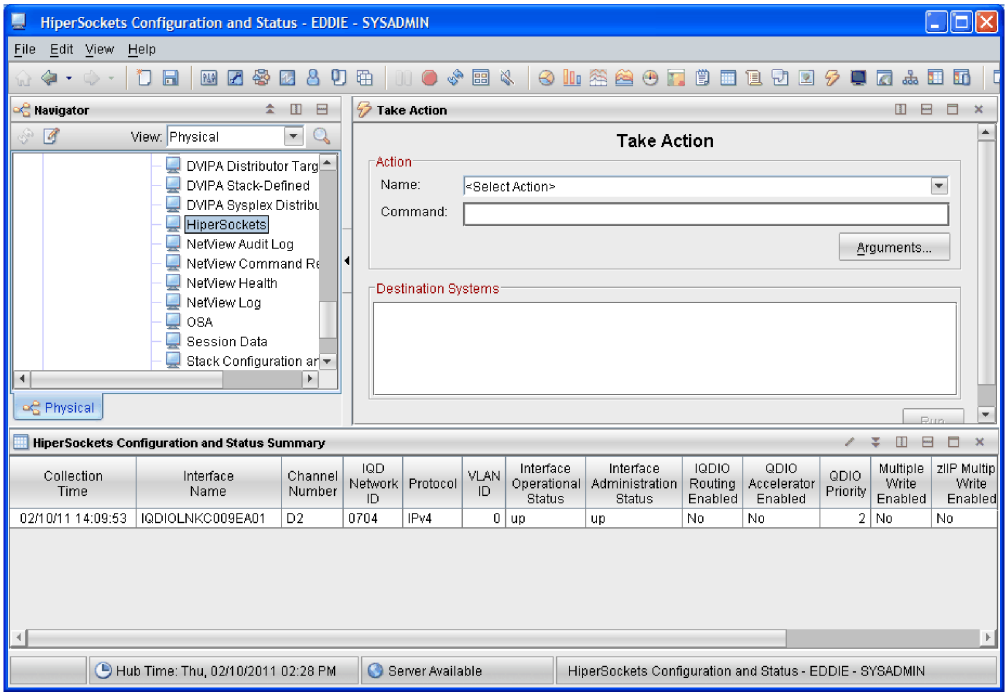
If the NetView domain node that is shown in the navigator view represents the master NetView program, this workspace can contain sysplex-wide data. Otherwise, the workspace contains data for the z/OS image on which the NetView program resides.

This workspace provides data that is updated by using sampling.

Historical data is not enabled in this workspace.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 19.



Collection Time	Interface Name	Channel Number	IQD Network ID	Protocol	VLAN ID	Interface Operational Status	Interface Administration Status	IQDIO Routing Enabled	QDIO Accelerator Enabled	QDIO Priority	Multiple Write Enabled	zIIP Multip Write Enabled
02/10/11 14:09:53	IQDIOLNKC009EA01	D2	0704	IPv4	0	up	up	No	No	2	No	No

Figure 19. HiperSockets Configuration and Status Workspace

NetView Audit Log Workspace

The NetView Audit Log workspace displays information about take action commands issued using the NetView for z/OS Enterprise Management Agent and the APSERV command receiver.

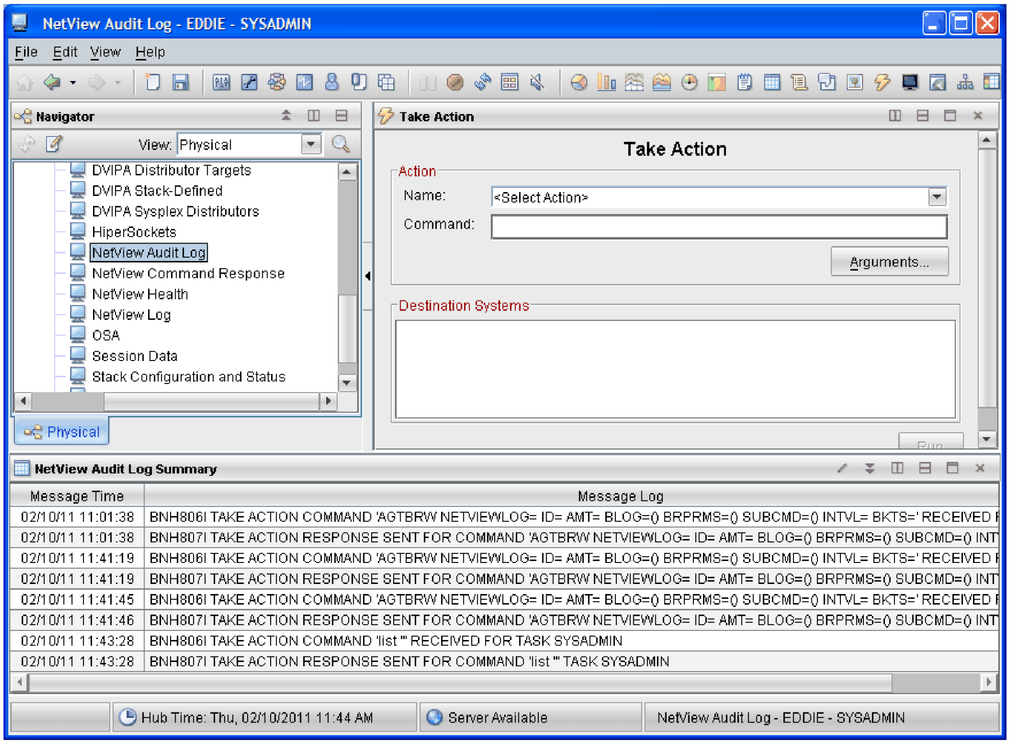
To display this workspace, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **NetView** > *domain*, and then click **NetView Audit Log**.

This workspace is empty unless take action commands are issued. The BNH806I and BNH807I audit trail messages provide information about the command and the NetView task that processed the command.

The amount of data that can be displayed in this workspace is controlled by the (TEMA)NACMD.ROWSAVLOG statement in the CNMSTYLE member. The data in this workspace wraps and is not cleared until the NACMD command is stopped and reissued.

Historical data is not enabled in this workspace.

This workspace is shown in Figure 20.



Message Time	Message Log
02/10/11 11:01:38	BNH806I TAKE ACTION COMMAND 'AGTBRW NETVIEWLOG= ID= AMT= BLOG=() BRPRMS=() SUBCMD=() INTVL= BKTS=' RECEIVED F
02/10/11 11:01:38	BNH807I TAKE ACTION RESPONSE SENT FOR COMMAND 'AGTBRW NETVIEWLOG= ID= AMT= BLOG=() BRPRMS=() SUBCMD=() INT
02/10/11 11:41:19	BNH806I TAKE ACTION COMMAND 'AGTBRW NETVIEWLOG= ID= AMT= BLOG=() BRPRMS=() SUBCMD=() INTVL= BKTS=' RECEIVED F
02/10/11 11:41:19	BNH807I TAKE ACTION RESPONSE SENT FOR COMMAND 'AGTBRW NETVIEWLOG= ID= AMT= BLOG=() BRPRMS=() SUBCMD=() INT
02/10/11 11:41:45	BNH806I TAKE ACTION COMMAND 'AGTBRW NETVIEWLOG= ID= AMT= BLOG=() BRPRMS=() SUBCMD=() INTVL= BKTS=' RECEIVED F
02/10/11 11:41:46	BNH807I TAKE ACTION RESPONSE SENT FOR COMMAND 'AGTBRW NETVIEWLOG= ID= AMT= BLOG=() BRPRMS=() SUBCMD=() INT
02/10/11 11:43:28	BNH806I TAKE ACTION COMMAND 'list '' RECEIVED FOR TASK SYSADMIN
02/10/11 11:43:28	BNH807I TAKE ACTION RESPONSE SENT FOR COMMAND 'list '' TASK SYSADMIN

Hub Time: Thu, 02/10/2011 11:44 AM | Server Available | NetView Audit Log - EDDIE - SYSADMIN

Figure 20. NetView Audit Log Workspace

NetView Command Response Workspace

The NetView Command Response workspace displays the commands and command responses for take action commands using the NetView for z/OS Enterprise Management Agent and the APSERV command receiver. It displays all take action commands and command output except for the Browse NetView Logs take action command.

Note: For security reasons, only commands and command responses issued by the current Tivoli Enterprise Portal user can be seen in this workspace.

To display this workspace, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **NetView** > *domain*, and then click **NetView Command Response**.

This workspace provides data that is based on commands. Data is present after a take action command is issued and the workspace is refreshed.

The amount of data that can be displayed in this workspace is controlled by the (TEMA)NACMD.ROWSNVCM statement in the CNMSTYLE member. The data in this workspace wraps and is not cleared until the NACMD command is stopped and reissued.

To find a text string in this view, click the **Find** icon. In the Find window, type the text you want to find, and click **Find**.

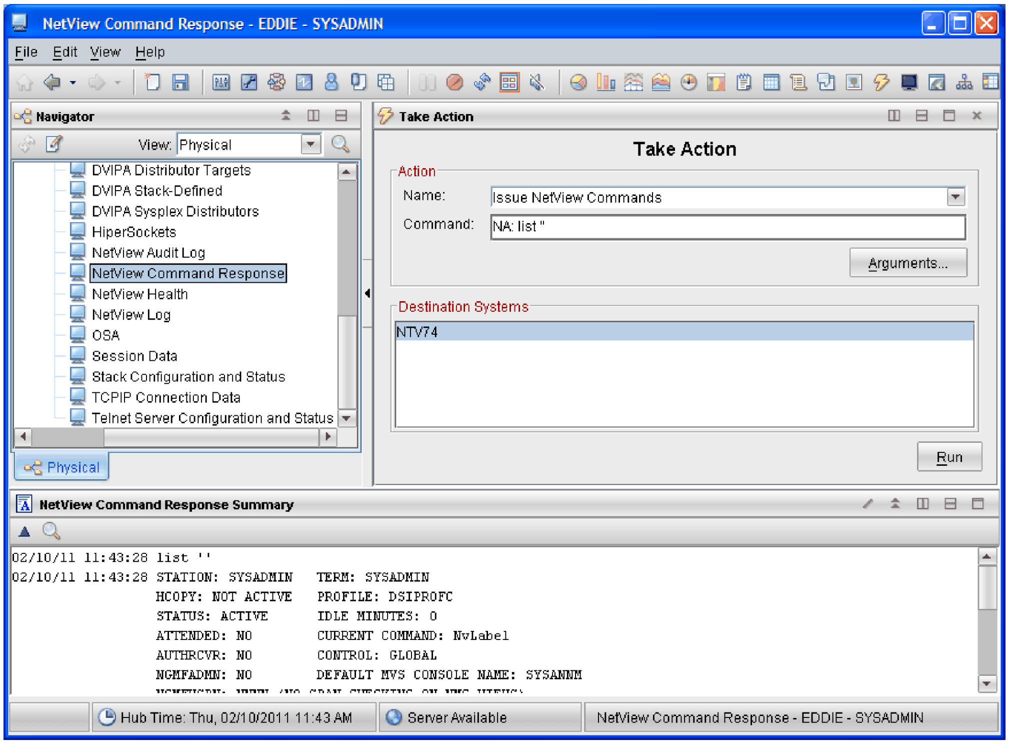
To reverse the order of the command responses in the view, click the **Sort** icon. The default order of the command responses is the oldest at the top and the newest at the bottom.

Notes:

1. The find and sort functions work only on the page that you are viewing. The default view-level page size is 100 rows of data. This value is specified in the properties for the NetView Command Response Summary view. If you are viewing more than 100 rows of data, by default, they are displayed in several pages. To use the find and sort functions for more than 100 rows of data, set the view-level page size to return all rows or increase the number of rows to return.
2. The data for this view can span several pages. If the workspace is refreshed while you are viewing any page other than the first page, the view is reset to display the first page.

Historical data is not enabled in this workspace.

This workspace is shown in Figure 21.


NetView Command Response - EDDIE - SYSADMIN
File
Edit
View
Help
Navigator
View:
Physical
DVIPA Distributor Targets
DVIPA Stack-Defined
DVIPA Sysplex Distributors
HiperSockets
NetView Audit Log
NetView Command Response
NetView Health
NetView Log
OSA
Session Data
Stack Configuration and Status
TCPIP Connection Data
Telnet Server Configuration and Status
Physical
Take Action
Take Action
Action
Arguments...
Destination Systems
Run
NetView Command Response Summary
Hub Time: Thu, 02/10/2011 11:43 AM
Server Available
NetView Command Response - EDDIE - SYSADMIN

Name: Issue NetView Commands

Command: NA: list ''

Destination Systems: NTV74

```
02/10/11 11:43:28 list ''
02/10/11 11:43:28 STATION: SYSADMIN   TERM: SYSADMIN
                  HCOPY: NOT ACTIVE   PROFILE: DSIPROFC
                  STATUS: ACTIVE      IDLE MINUTES: 0
                  ATTENDED: NO        CURRENT COMMAND: NvLabel
                  AUTHRCVR: NO        CONTROL: GLOBAL
                  NGMFADMN: NO        DEFAULT MVS CONSOLE NAME: SYSANNM
```

Figure 21. NetView Command Response Workspace

NetView Log Workspace

The NetView Log workspace displays information from the NetView log. It displays the NetView log records that are a result of the Browse NetView Logs take action command that you issued.

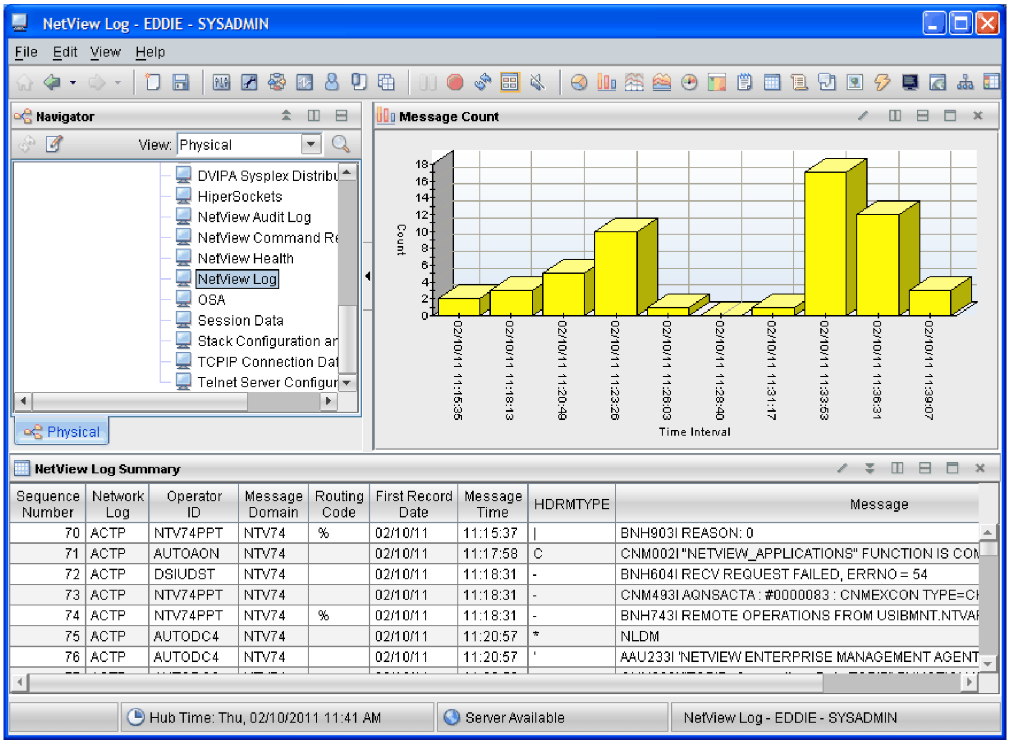
To display this workspace, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **NetView** > *domain*, and then click **NetView Log**.

This workspace provides data that is based on commands. Data is present after the Browse NetView Logs take action command is issued and the workspace is refreshed. Error messages related to this take action command are displayed in the NetView Audit Log workspace.

The amount of data that can be displayed in this workspace is controlled by the (TEMA)NACMD.ROWSNVLOG statement in the CNMSTYLE member.

Historical data is not enabled in this workspace.

This workspace is shown in Figure 22.



Sequence Number	Network Log	Operator ID	Message Domain	Routing Code	First Record Date	Message Time	HDRMTYPE	Message
70	ACTP	NTV74PPT	NTV74	%	02/10/11	11:15:37	|	BNH903I REASON: 0
71	ACTP	AUTOAON	NTV74		02/10/11	11:17:58	C	CNM002I "NETVIEW_APPLICATIONS" FUNCTION IS CON
72	ACTP	DSIUDST	NTV74		02/10/11	11:18:31	-	BNH604I RECV REQUEST FAILED, ERRNO = 54
73	ACTP	NTV74PPT	NTV74		02/10/11	11:18:31	-	CNM493I AQNSACTA : #0000083 : CNMEXCON TYPE=CI
74	ACTP	NTV74PPT	NTV74	%	02/10/11	11:18:31	-	BNH743I REMOTE OPERATIONS FROM USIBMNT.NTVAI
75	ACTP	AUTODC4	NTV74		02/10/11	11:20:57	*	NLDM
76	ACTP	AUTODC4	NTV74		02/10/11	11:20:57	'	AAU233I 'NETVIEW ENTERPRISE MANAGEMENT AGENT

Figure 22. NetView Log Workspace

OSA Channels and Ports Workspace

The OSA Channels and Ports workspace displays the configuration and status data for the OSA channels and ports. The data collection for this information requires Resource Object Data Manager (RODM).

To display this workspace, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **NetView** > *domain*, and then click **OSA**.

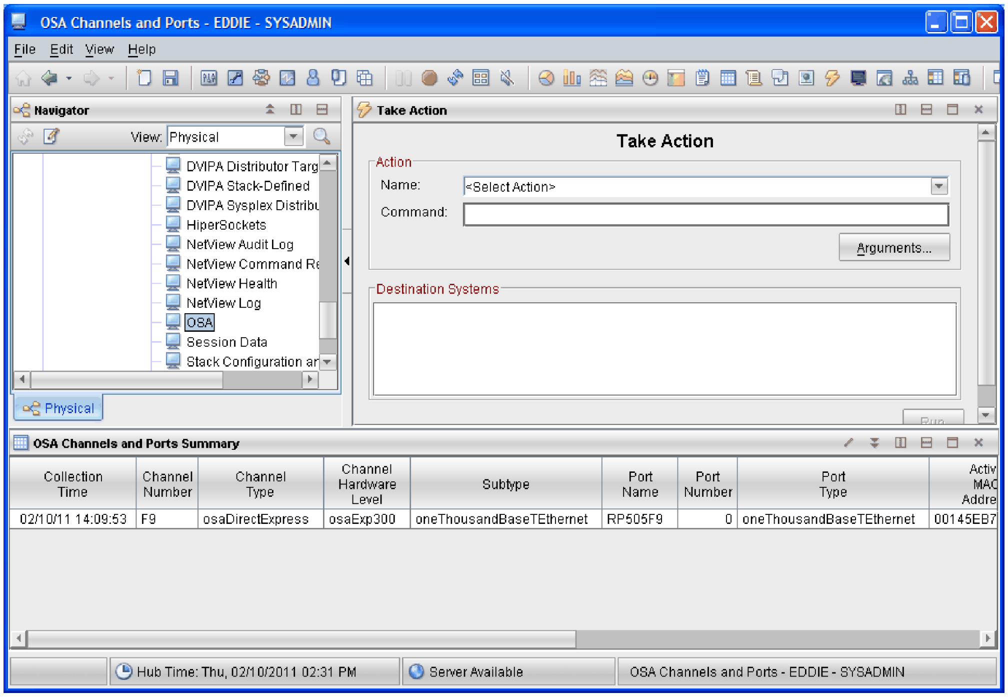
If the NetView domain node that is shown in the navigator view represents the master NetView program, this workspace can contain sysplex-wide data. Otherwise, the workspace contains data for the z/OS image on which the NetView program resides.

This workspace provides data that is updated by using sampling.

Historical data is not enabled in this workspace.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 23.



Collection Time	Channel Number	Channel Type	Channel Hardware Level	Subtype	Port Name	Port Number	Port Type	Activ MAC Addre
02/10/11 14:09:53	F9	osaDirectExpress	osaExp300	oneThousandBaseTEthernet	RP505F9	0	oneThousandBaseTEthernet	00145EB7

Figure 23. OSA Channels and Ports Workspace

Session Data Workspace

The Session Data workspace displays information about active SNA sessions.

To display this workspace, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **NetView** > *domain*, and then click **Session Data**.

This workspace provides data that is updated by using sampling.

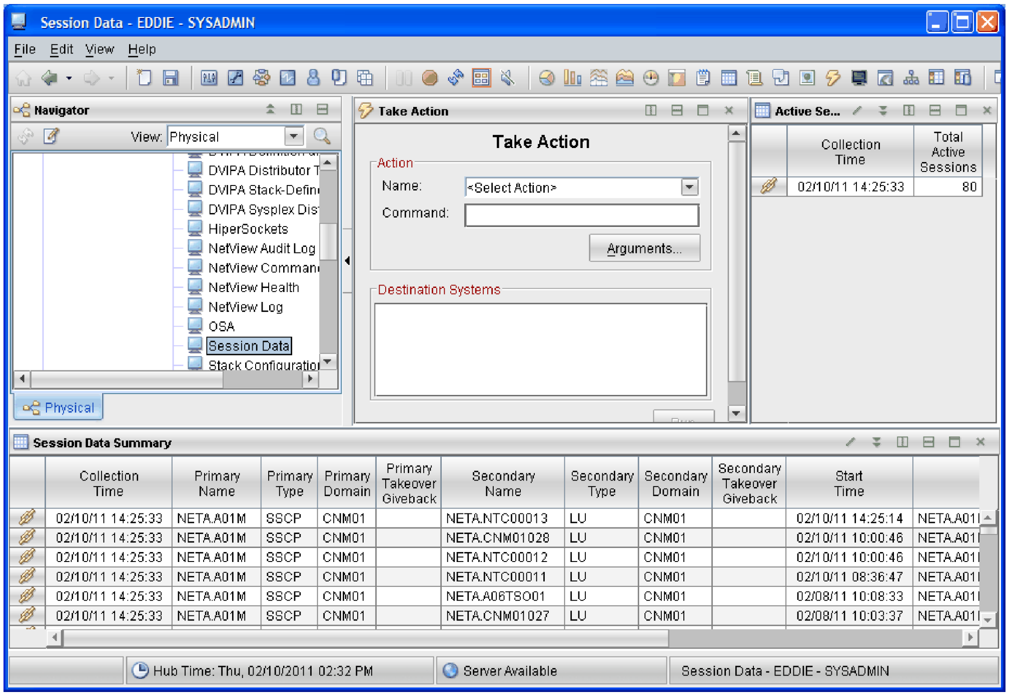
The queries for this workspace use the Primary Type attribute to filter the rows that can be retrieved for display. Because of the default filter, you might not see all your sessions. You can modify the query to display more or fewer sessions than the default filter allows.

If you have a large installation, you might not be able to view all the available sessions in the Tivoli Enterprise Portal. For more information, see the *IBM Tivoli NetView for z/OS Tuning Guide*.

Historical data is enabled in this workspace for the Active Session Count table view. When you view historical data in this view, all rows with collection times in the specified time span are displayed.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 24.



Name: <Select Action>

Command:

	Collection Time	Total Active Sessions
	02/10/11 14:25:33	80

	Collection Time	Primary Name	Primary Type	Primary Domain	Primary Takeover Giveback	Secondary Name	Secondary Type	Secondary Domain	Secondary Takeover Giveback	Start Time	
	02/10/11 14:25:33	NETA.A01M	SSCP	CNM01		NETA.NTC00013	LU	CNM01		02/10/11 14:25:14	NETA.A01
	02/10/11 14:25:33	NETA.A01M	SSCP	CNM01		NETA.CNM01028	LU	CNM01		02/10/11 10:00:46	NETA.A01
	02/10/11 14:25:33	NETA.A01M	SSCP	CNM01		NETA.NTC00012	LU	CNM01		02/10/11 10:00:46	NETA.A01
	02/10/11 14:25:33	NETA.A01M	SSCP	CNM01		NETA.NTC00011	LU	CNM01		02/10/11 08:36:47	NETA.A01
	02/10/11 14:25:33	NETA.A01M	SSCP	CNM01		NETA.A06TSO01	LU	CNM01		02/08/11 10:08:33	NETA.A01
	02/10/11 14:25:33	NETA.A01M	SSCP	CNM01		NETA.CNM01027	LU	CNM01		02/08/11 10:03:37	NETA.A01

Hub Time: Thu, 02/10/2011 02:32 PM | Server Available | Session Data - EDDIE - SYSADMIN

Figure 24. Session Data Workspace

Stack Configuration and Status Workspace

The Stack Configuration and Status workspace displays information about the z/OS Communications Server stacks.

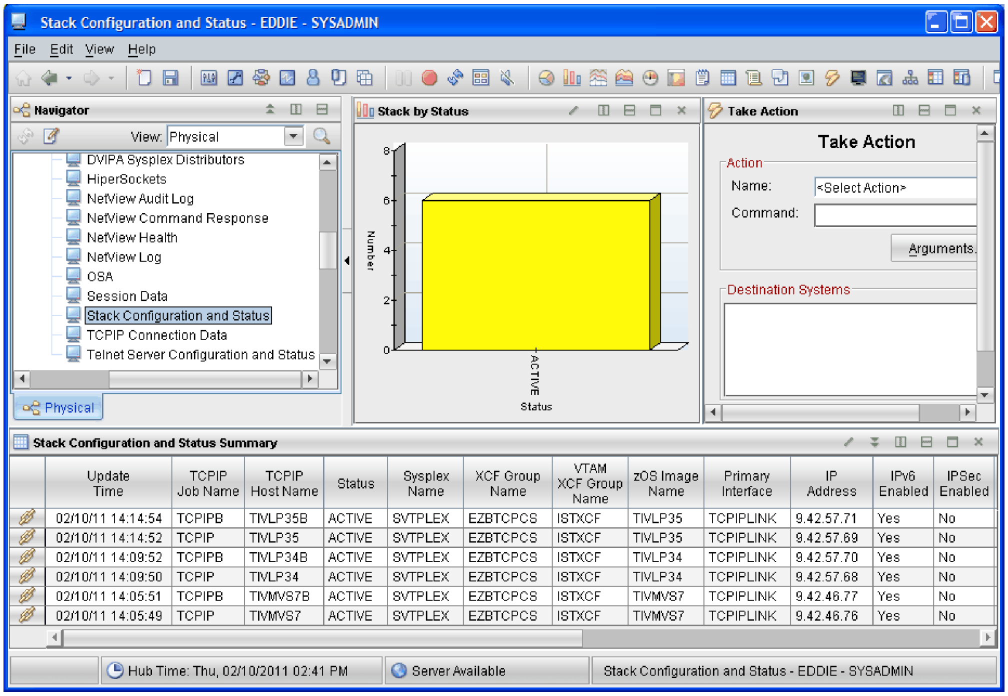
To display this workspace, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **NetView** > *domain*, and then click **Stack Configuration and Status**.

If the NetView domain node that is shown in the navigator view represents the master NetView program, this workspace can contain sysplex-wide data. Otherwise, the workspace contains data for the z/OS image on which the NetView program resides.

Historical data is not enabled in this workspace.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 25 on page 50.



Update Time	TCPIP Job Name	TCPIP Host Name	Status	Sysplex Name	XCF Group Name	VTAM XCF Group Name	zOS Image Name	Primary Interface	IP Address	IPv6 Enabled	IPSec Enabled
02/10/11 14:14:54	TCPIPB	TIVLP35B	ACTIVE	SVTPLEX	EZBTCPCS	ISTXCF	TIVLP35	TCPIPLINK	9.42.57.71	Yes	No
02/10/11 14:14:52	TCPIP	TIVLP35	ACTIVE	SVTPLEX	EZBTCPCS	ISTXCF	TIVLP35	TCPIPLINK	9.42.57.69	Yes	No
02/10/11 14:09:52	TCPIPB	TIVLP34B	ACTIVE	SVTPLEX	EZBTCPCS	ISTXCF	TIVLP34	TCPIPLINK	9.42.57.70	Yes	No
02/10/11 14:09:50	TCPIP	TIVLP34	ACTIVE	SVTPLEX	EZBTCPCS	ISTXCF	TIVLP34	TCPIPLINK	9.42.57.68	Yes	No
02/10/11 14:05:51	TCPIPB	TIVMVS7B	ACTIVE	SVTPLEX	EZBTCPCS	ISTXCF	TIVMVS7	TCPIPLINK	9.42.46.77	Yes	No
02/10/11 14:05:49	TCPIP	TIVMVS7	ACTIVE	SVTPLEX	EZBTCPCS	ISTXCF	TIVMVS7	TCPIPLINK	9.42.46.76	Yes	No

Figure 25. Stack Configuration and Status Workspace

Telnet Server Configuration and Status Workspace

The Telnet Server Configuration and Status workspace displays information about Telnet servers and Telnet server ports.

To display this workspace, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **NetView** > *domain*, and then click **Telnet Server Configuration and Status**.

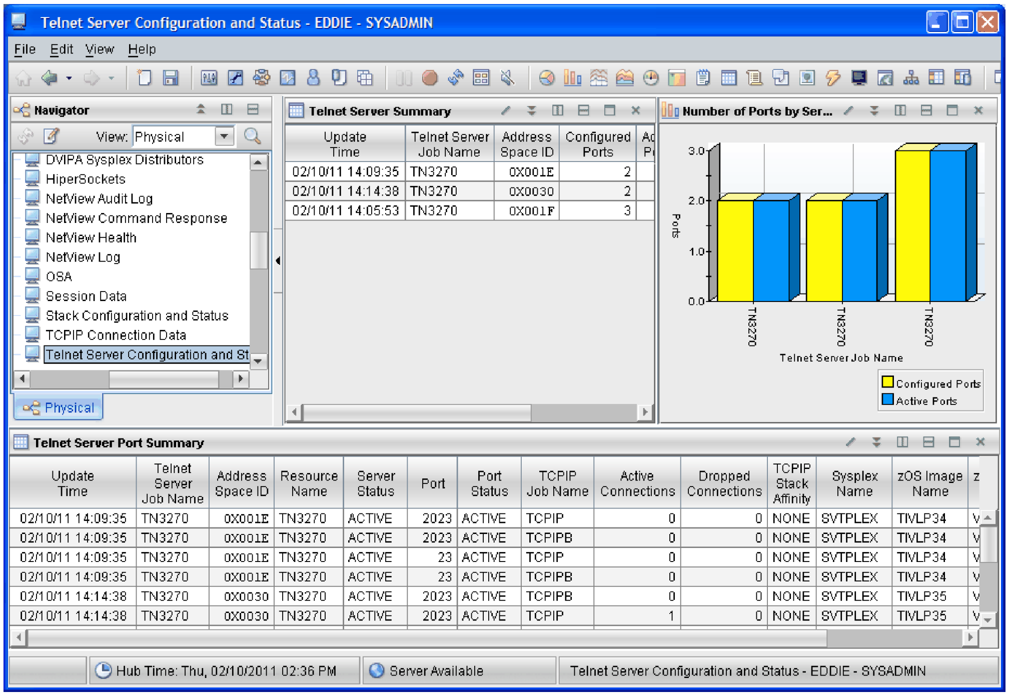
If the NetView domain node that is shown in the navigator view represents the master NetView program, this workspace can contain sysplex-wide data. Otherwise, the workspace contains data for the z/OS image on which the NetView program resides.

This workspace provides data that is updated by using sampling and events.

Historical data is not enabled in this workspace.

For information about data collection and data display for this workspace, see the table in *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

This workspace is shown in Figure 26 on page 51.



Telnet Server Summary

Update Time	Telnet Server Job Name	Address Space ID	Configured Ports	Ac P
02/10/11 14:09:35	TN3270	0X001E	2	
02/10/11 14:14:38	TN3270	0X0030	2	
02/10/11 14:05:53	TN3270	0X001F	3	

Telnet Server Port Summary

Update Time	Telnet Server Job Name	Address Space ID	Resource Name	Server Status	Port	Port Status	TCPIP Job Name	Active Connections	Dropped Connections	TCPIP Stack Affinity	Sysplex Name	zOS Image Name	z
02/10/11 14:09:35	TN3270	0X001E	TN3270	ACTIVE	2023	ACTIVE	TCPIP	0	0	NONE	SVTPLEX	TIVLP34	V
02/10/11 14:09:35	TN3270	0X001E	TN3270	ACTIVE	2023	ACTIVE	TCPIPB	0	0	NONE	SVTPLEX	TIVLP34	V
02/10/11 14:09:35	TN3270	0X001E	TN3270	ACTIVE	23	ACTIVE	TCPIP	0	0	NONE	SVTPLEX	TIVLP34	V
02/10/11 14:09:35	TN3270	0X001E	TN3270	ACTIVE	23	ACTIVE	TCPIPB	0	0	NONE	SVTPLEX	TIVLP34	V
02/10/11 14:14:38	TN3270	0X0030	TN3270	ACTIVE	2023	ACTIVE	TCPIPB	0	0	NONE	SVTPLEX	TIVLP35	V
02/10/11 14:14:38	TN3270	0X0030	TN3270	ACTIVE	2023	ACTIVE	TCPIP	1	0	NONE	SVTPLEX	TIVLP35	V

Hub Time: Thu, 02/10/2011 02:36 PM | Server Available | Telnet Server Configuration and Status - EDDIE - SYSADMIN

Figure 26. Telnet Server Configuration and Status Workspace

Chapter 7. GDPS Active/Active Continuous Availability Solution Workspaces

The workspaces for the GDPS Active/Active Continuous Availability solution show availability and performance metrics for workload distribution and replication capture and apply servers. The following workspaces, which are listed in alphabetical order, are provided:

- "DB2 Replication Details Workspace"
- "Filtered Replication Servers Workspace" on page 54
- "Filtered Workload Servers Workspace" on page 54
- "Filtered Workloads Workspace" on page 55
- "IMS Replication Details Workspace" on page 55
- "Load Balancer Groups Workspace" on page 56
- "Load Balancer Workloads Workspace" on page 56
- "Load Balancers Workspace" on page 57
- "Replication Servers Workspace" on page 58
- "Workload Lifeline Advisors Workspace" on page 59
- "Workload Lifeline Agents Workspace" on page 60
- "Workload Server Details Workspace" on page 61
- "Workload Servers Workspace" on page 62
- "Workload Site Details Workspace" on page 63
- "Workload Sites Workspace" on page 64
- "Workloads Workspace" on page 65

DB2 Replication Details Workspace

The DB2 Replication Details workspace displays DB2 replication details for a specific capture and apply server pair.

To display this workspace, click the link icon for a row in the Replication Servers and Filtered Replication Servers workspaces, the Replication Servers Summary table. See "Replication Servers Workspace" on page 58.

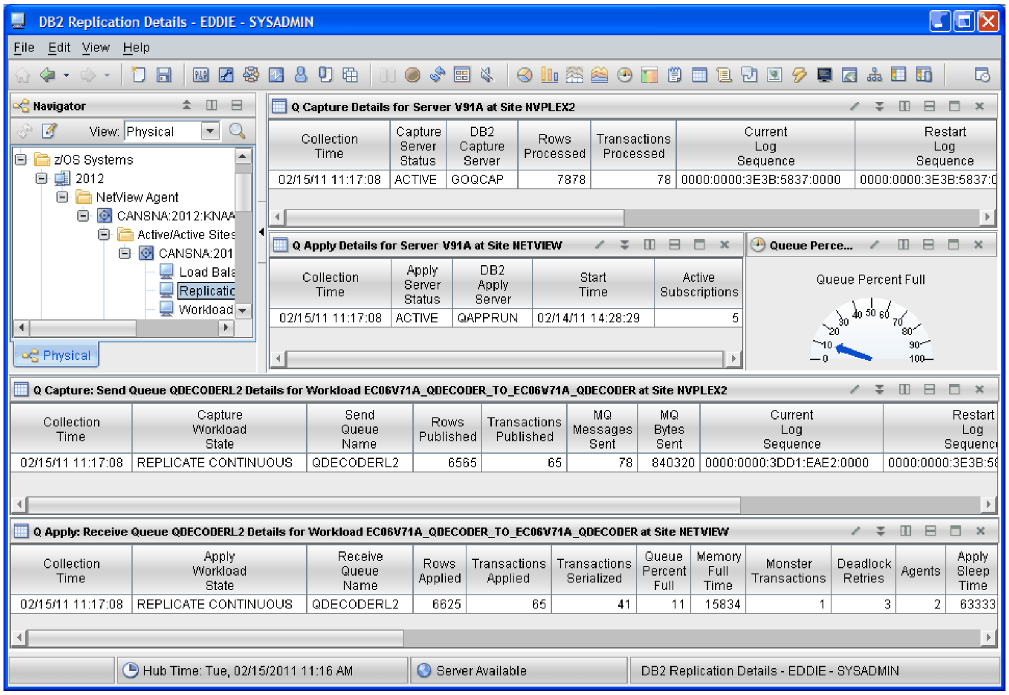
This workspace provides data that is updated by using sampling.

Historical data is enabled in this workspace.

You can also monitor DB2 replication by using the IBM InfoSphere® Replication Server Q Replication Dashboard. The Q Replication Dashboard is a customizable web tool for monitoring the health and performance of replication and event publishing and is available for download from the InfoSphere Replication Server support site. The dashboard summary can be used to quickly identify and troubleshoot problems, and shows at-a-glance status information on programs, queues, Q subscriptions, and other objects. You can use the Tivoli Enterprise Portal launch application feature to write and save definitions to start an application, such as the Q Replication Dashboard, for yourself or for all users in your monitored environment. See the *IBM Tivoli Monitoring: Tivoli Enterprise Portal User's Guide* for information about the launch application feature.

For information about data collection and data display for this workspace, see *IBM Tivoli NetView for z/OS Installation: Configuring the GDPS Active/Active Continuous Availability Solution*.

This workspace is shown in Figure 27.



Q Capture Details for Server V91A at Site NVPLEX2

Collection Time	Capture Server Status	DB2 Capture Server	Rows Processed	Transactions Processed	Current Log Sequence	Restart Log Sequence
02/15/11 11:17:08	ACTIVE	GOQCAP	7878	78	0000:0000:3E3B:5837:0000	0000:0000:3E3B:5837:0

Q Apply Details for Server V91A at Site NETVIEW

Collection Time	Apply Server Status	DB2 Apply Server	Start Time	Active Subscriptions
02/15/11 11:17:08	ACTIVE	QAPPRUN	02/14/11 14:28:29	5

Q Capture: Send Queue QDECODERL2 Details for Workload EC06V71A_QDECODER_TO_EC06V71A_QDECODER at Site NVPLEX2

Collection Time	Capture Workload State	Send Queue Name	Rows Published	Transactions Published	MQ Messages Sent	MQ Bytes Sent	Current Log Sequence	Restart Log Sequenc
02/15/11 11:17:08	REPLICATE CONTINUOUS	QDECODERL2	6565	65	78	840320	0000:0000:3DD1:EAE2:0000	0000:0000:3E3B:5

Q Apply: Receive Queue QDECODERL2 Details for Workload EC06V71A_QDECODER_TO_EC06V71A_QDECODER at Site NETVIEW

Collection Time	Apply Workload State	Receive Queue Name	Rows Applied	Transactions Applied	Transactions Serialized	Queue Percent Full	Memory Full Time	Monster Transactions	Deadlock Retries	Agents	Apply Sleep Time
02/15/11 11:17:08	REPLICATE CONTINUOUS	QDECODERL2	6625	65	41	11	15834	1	3	2	63333

Figure 27. DB2 Replication Details Workspace

Filtered Replication Servers Workspace

The Filtered Replication Servers workspace displays all the capture and apply server pairs that make up a specific workload for the GDPS Active/Active Continuous Availability solution.

To display this workspace, click the link icon from a row in the Workloads and Filtered Workloads workspaces, the Workloads Summary table. See “Workloads Workspace” on page 65.

This workspace provides the same views, thresholds, and links that are provided in the Replication Servers workspace. See “Replication Servers Workspace” on page 58.

Filtered Workload Servers Workspace

The Filtered Workload Servers workspace displays the servers that are reporting to a specific load balancer group, Multi-site Workload Lifeline Agent, or workload.

To display this workspace, click the link icon from a row in one of the following views:

- Workload Lifeline Agents workspace, the Workload Lifeline Agents Summary table. See “Workload Lifeline Agents Workspace” on page 60.
- Workloads and Filtered Workloads workspaces, the Workloads Summary table. See “Workloads Workspace” on page 65.

This workspace provides the same views, thresholds, and links that are provided in the Workload Servers workspace. See “Workload Servers Workspace” on page 62.

Filtered Workloads Workspace

The Filtered Workloads workspace displays the workloads for an external load balancer or sysplex distributor.

To display this workspace, click the link icon from a row in the Load Balancer Workloads workspace, the Load Balancer Workloads Summary table. See "Load Balancer Workloads Workspace" on page 56.

This workspace provides the same views, thresholds, and links that are provided in the Workloads workspace. See "Workloads Workspace" on page 65.

IMS Replication Details Workspace

The IMS Replication Details workspace displays IMS replication details for a specific capture and apply server pair.

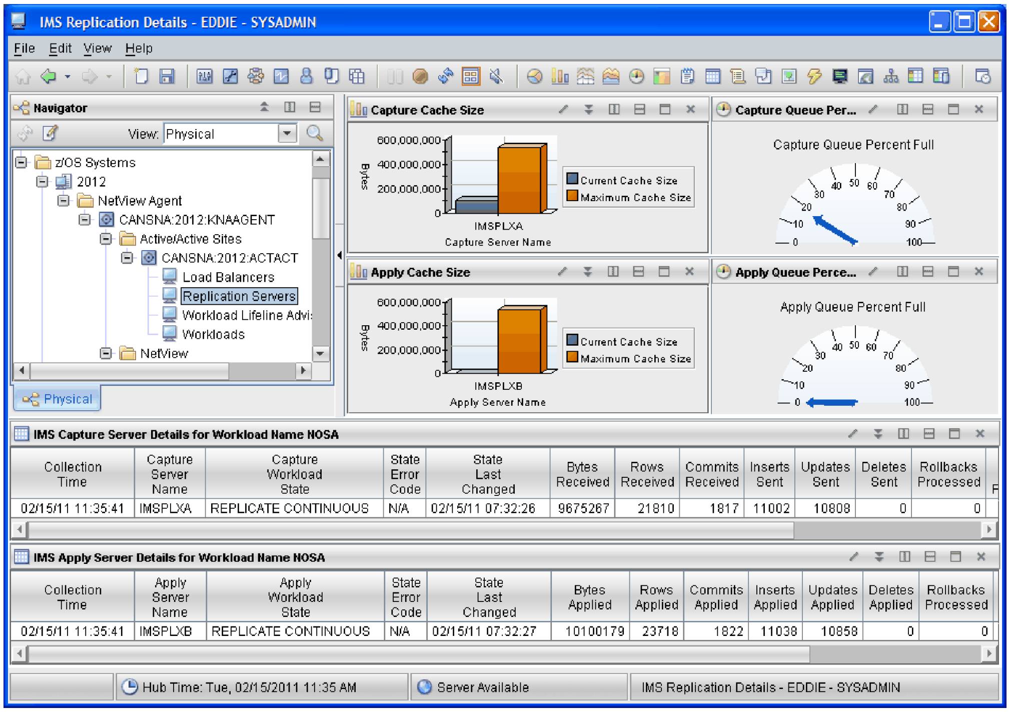
To display this workspace, click the link icon from a row in the Replication Servers and Filtered Replication Servers workspaces, the Replication Servers Summary table. See "Replication Servers Workspace" on page 58.

This workspace provides data that is updated by using sampling.

Historical data is enabled in this workspace.

For information about data collection and data display for this workspace, see *IBM Tivoli NetView for z/OS Installation: Configuring the GDPS Active/Active Continuous Availability Solution*.

This workspace is shown in Figure 28.



IMS Capture Server Details for Workload Name NOSA

Collection Time	Capture Server Name	Capture Workload State	State Error Code	State Last Changed	Bytes Received	Rows Received	Commits Received	Inserts Sent	Updates Sent	Deletes Sent	Rollbacks Processed
02/15/11 11:35:41	IMSPLXA	REPLICATE CONTINUOUS	N/A	02/15/11 07:32:26	9675267	21810	1817	11002	10808	0	0

IMS Apply Server Details for Workload Name NOSA

Collection Time	Apply Server Name	Apply Workload State	State Error Code	State Last Changed	Bytes Applied	Rows Applied	Commits Applied	Inserts Applied	Updates Applied	Deletes Applied	Rollbacks Processed
02/15/11 11:35:41	IMSPLXB	REPLICATE CONTINUOUS	N/A	02/15/11 07:32:27	10100179	23718	1822	11038	10858	0	0

Hub Time: Tue, 02/15/2011 11:35 AM

Server Available

IMS Replication Details - EDDIE - SYSADMIN

Figure 28. IMS Replication Details Workspace

Load Balancer Groups Workspace

The Load Balancer Groups workspace displays group configuration information for an external load balancer.

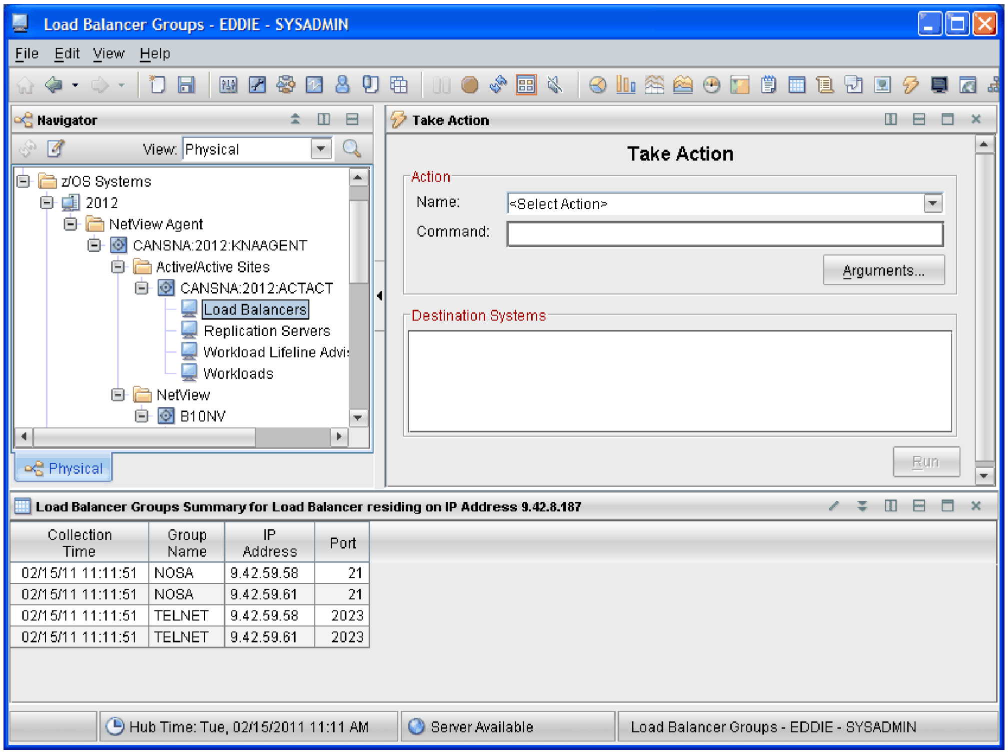
To display this workspace, click the link icon for a row in the Load Balancers workspace, the Load Balancers Summary table. See “Load Balancers Workspace” on page 57.

This workspace provides data that is updated by using sampling.

Historical data is not enabled in this workspace.

For information about data collection and data display for this workspace, see *IBM Tivoli NetView for z/OS Installation: Configuring the GDPS Active/Active Continuous Availability Solution*.

This workspace is shown in Figure 29.



View: Physical

Name: <Select Action>

Command:

Load Balancer Groups Summary for Load Balancer residing on IP Address 9.42.8.187

Collection Time	Group Name	IP Address	Port
02/15/11 11:11:51	NOSA	9.42.59.58	21
02/15/11 11:11:51	NOSA	9.42.59.61	21
02/15/11 11:11:51	TELNET	9.42.59.58	2023
02/15/11 11:11:51	TELNET	9.42.59.61	2023

Figure 29. Load Balancer Groups Workspace

Load Balancer Workloads Workspace

The Load Balancer Workloads workspace displays workload configuration information for an external load balancer or sysplex distributor.

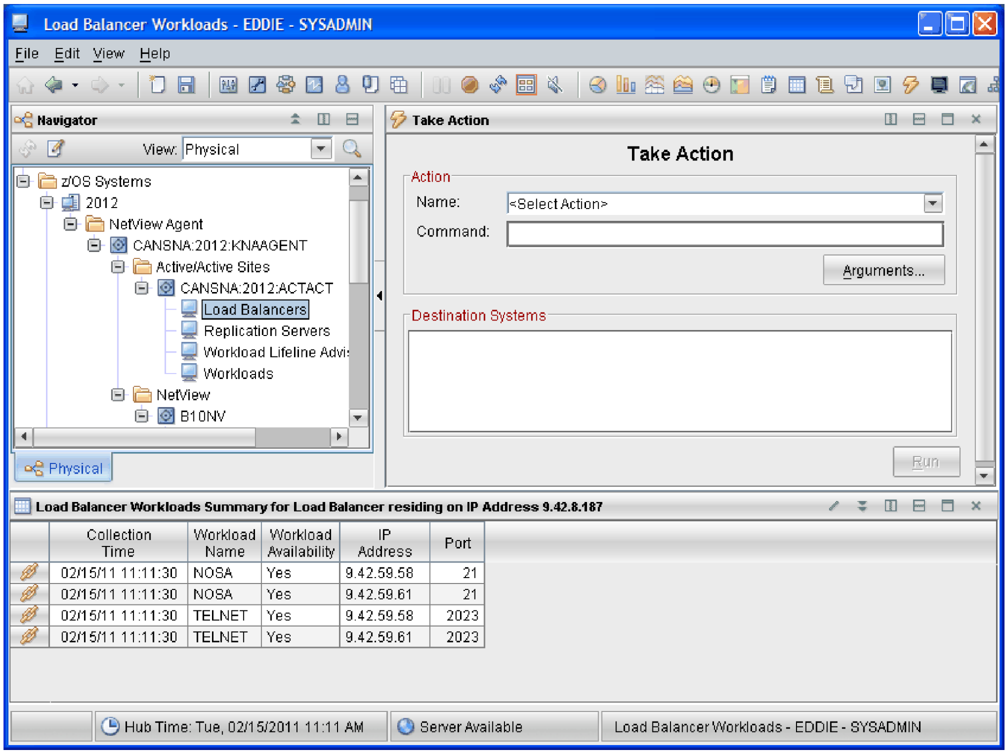
To display this workspace, click the link icon for a row in the Load Balancers workspace, the Load Balancers Summary table. See “Load Balancers Workspace” on page 57.

This workspace provides data that is updated by using sampling.

Historical data is not enabled in this workspace.

For information about data collection and data display for this workspace, see *IBM Tivoli NetView for z/OS Installation: Configuring the GDPS Active/Active Continuous Availability Solution*.

This workspace is shown in Figure 30.



View: Physical

Take Action

Name: <Select Action>

Command:

Load Balancer Workloads Summary for Load Balancer residing on IP Address 9.42.8.187

	Collection Time	Workload Name	Workload Availability	IP Address	Port
	02/15/11 11:11:30	NOSA	Yes	9.42.59.58	21
	02/15/11 11:11:30	NOSA	Yes	9.42.59.61	21
	02/15/11 11:11:30	TELNET	Yes	9.42.59.58	2023
	02/15/11 11:11:30	TELNET	Yes	9.42.59.61	2023

Hub Time: Tue, 02/15/2011 11:11 AM | Server Available | Load Balancer Workloads - EDDIE - SYSADMIN

Figure 30. Load Balancer Workloads Workspace

Load Balancers Workspace

The Load Balancers workspace displays the external load balancers and sysplex distributors that are defined to load balance workloads.

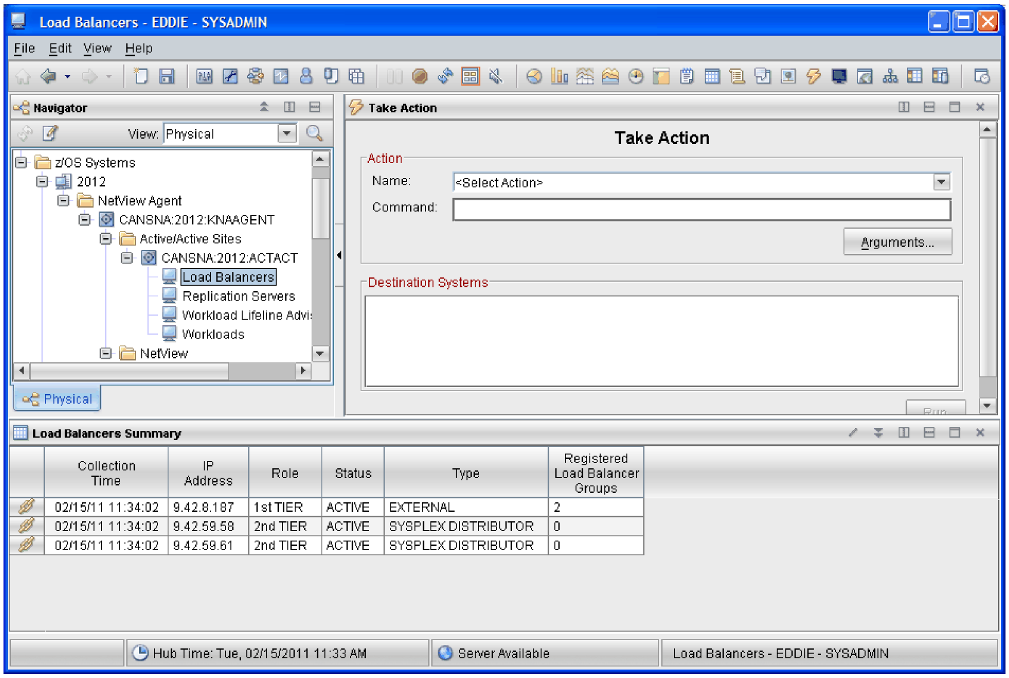
To display this workspace, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **Active/Active Sites** > *node*:**ACTACT**, and then click **Load Balancers**.

This workspace provides data that is updated by using sampling.

Historical data is not enabled in this workspace.

For information about data collection and data display for this workspace, see *IBM Tivoli NetView for z/OS Installation: Configuring the GDPS Active/Active Continuous Availability Solution*.

This workspace is shown in Figure 31 on page 58.



Collection Time	IP Address	Role	Status	Type	Registered Load Balancer Groups
02/15/11 11:34:02	9.42.8.187	1st TIER	ACTIVE	EXTERNAL	2
02/15/11 11:34:02	9.42.59.58	2nd TIER	ACTIVE	SYSPLEX DISTRIBUTOR	0
02/15/11 11:34:02	9.42.59.61	2nd TIER	ACTIVE	SYSPLEX DISTRIBUTOR	0

Figure 31. Load Balancers Workspace

Replication Servers Workspace

The Replication Servers workspace displays all capture and apply server pairs that make up the workloads for the GDPS Active/Active Continuous Availability solution.

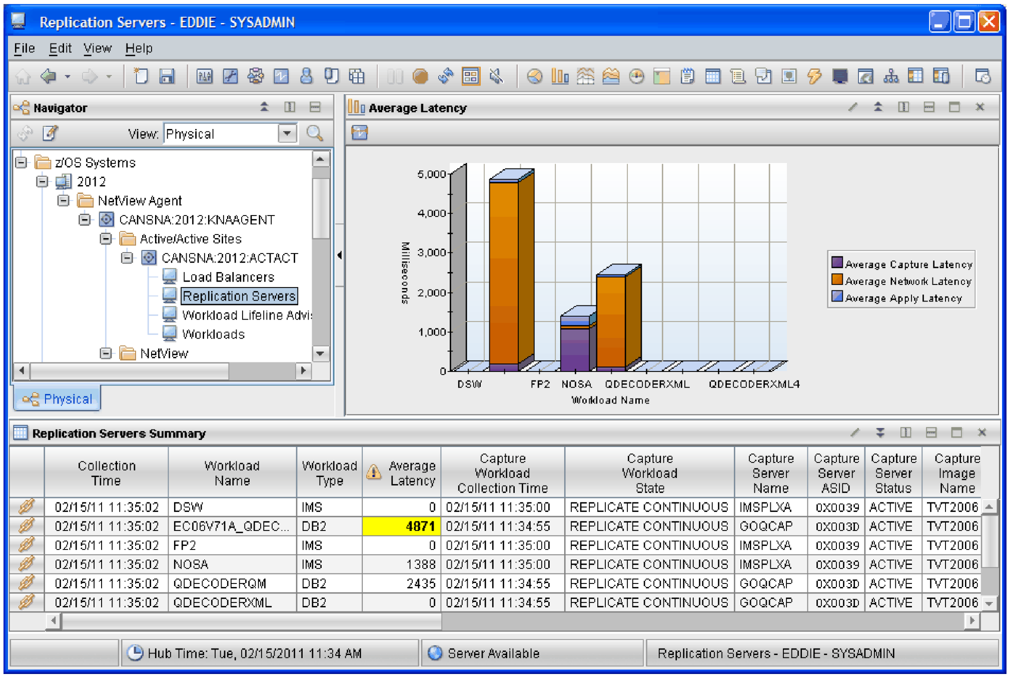
To display this workspace, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **Active/Active Sites** > *node*:**ACTACT**, and then click **Replication Servers**.

This workspace provides data that is updated by using sampling.

Historical data is enabled in this workspace.

For information about data collection and data display for this workspace, see *IBM Tivoli NetView for z/OS Installation: Configuring the GDPS Active/Active Continuous Availability Solution*.

This workspace is shown in Figure 32 on page 59.



	Collection Time	Workload Name	Workload Type	Average Latency	Capture Workload Collection Time	Capture Workload State	Capture Server Name	Capture Server ASID	Capture Server Status	Capture Image Name
	02/15/11 11:35:02	DSW	IMS	0	02/15/11 11:35:00	REPLICATE CONTINUOUS	IMSPLXA	0X0039	ACTIVE	TVT2006
	02/15/11 11:35:02	EC06V71A_QDEC...	DB2	4871	02/15/11 11:34:55	REPLICATE CONTINUOUS	GOQCAP	0X003D	ACTIVE	TVT2006
	02/15/11 11:35:02	FP2	IMS	0	02/15/11 11:35:00	REPLICATE CONTINUOUS	IMSPLXA	0X0039	ACTIVE	TVT2006
	02/15/11 11:35:02	NOSA	IMS	1388	02/15/11 11:35:00	REPLICATE CONTINUOUS	IMSPLXA	0X0039	ACTIVE	TVT2006
	02/15/11 11:35:02	QDECODERQM	DB2	2435	02/15/11 11:34:55	REPLICATE CONTINUOUS	GOQCAP	0X003D	ACTIVE	TVT2006
	02/15/11 11:35:02	QDECODERXML	DB2	0	02/15/11 11:34:55	REPLICATE CONTINUOUS	GOQCAP	0X003D	ACTIVE	TVT2006

Figure 32. Replication Servers Workspace

Workload Lifeline Advisors Workspace

The Workload Lifeline Advisor workspace displays the primary Multi-site Workload Lifeline Advisor that is used to calculate the best site for routing new TCP/IP connections. If configured, the secondary Multi-site Workload Lifeline Advisor is also displayed.

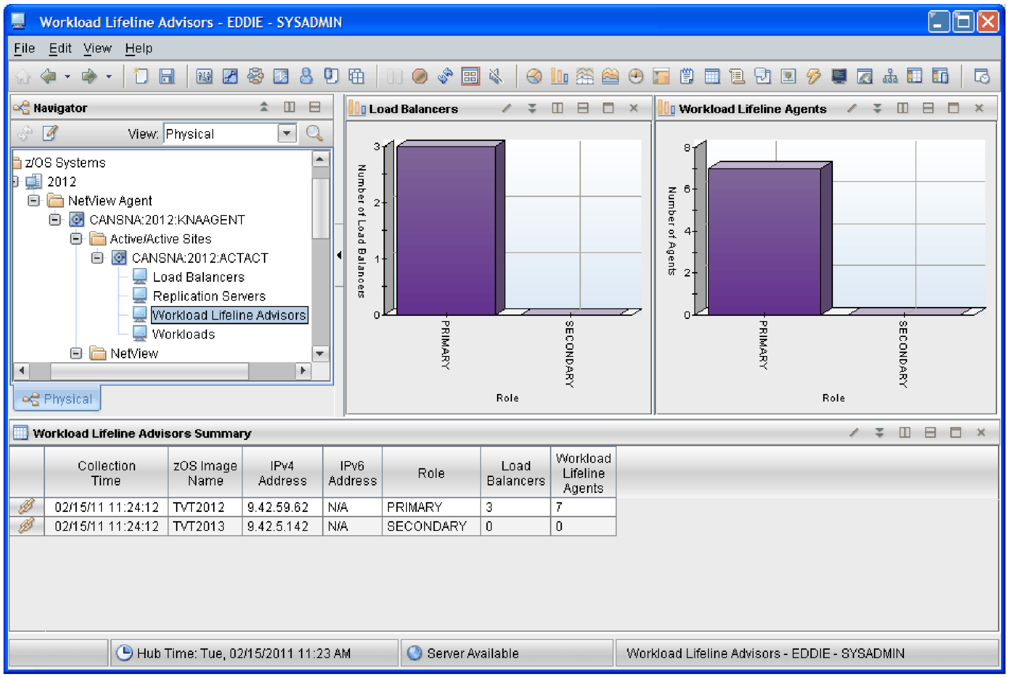
To display this workspace, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **Active/Active Sites** > *node*:**ACTACT**, and then click **Workload Lifeline Advisors**.

This workspace provides data that is updated by using sampling.

Historical data is not enabled in this workspace.

For information about data collection and data display for this workspace, see *IBM Tivoli NetView for z/OS Installation: Configuring the GDPS Active/Active Continuous Availability Solution*.

This workspace is shown in Figure 33 on page 60.



Collection Time	zOS Image Name	IPv4 Address	IPv6 Address	Role	Load Balancers	Workload Lifeline Agents
02/15/11 11:24:12	TVT2012	9.42.59.62	N/A	PRIMARY	3	7
02/15/11 11:24:12	TVT2013	9.42.5.142	N/A	SECONDARY	0	0

Figure 33. Workload Lifeline Advisors Workspace

Workload Lifeline Agents Workspace

The Workload Lifeline Agents workspace displays all Multi-site Workload Lifeline Agents in both the active and standby sites that are gathering server capacity and health information for registered servers and are reporting back to the primary Multi-site Workload Lifeline Advisor.

To display this workspace, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **Active/Active Sites** > *node*:**ACTACT**, select and right-click **Workload Lifeline Advisors**, click **Workspace**, and then click **Workload Lifeline Agents**.

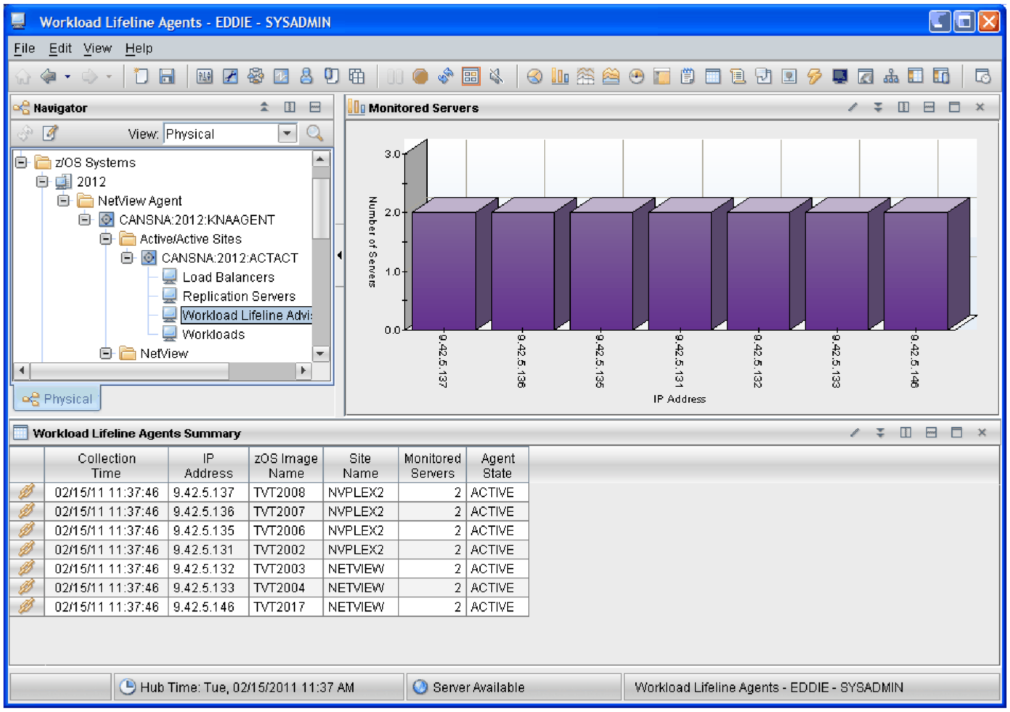
Note: You can also link to this workspace from the Workload Lifeline Advisors workspace.

This workspace provides data that is updated by using sampling.

Historical data is not enabled in this workspace.

For information about data collection and data display for this workspace, see *IBM Tivoli NetView for z/OS Installation: Configuring the GDPS Active/Active Continuous Availability Solution*.

This workspace is shown in Figure 34 on page 61.



Collection Time	IP Address	zOS Image Name	Site Name	Monitored Servers	Agent State
02/15/11 11:37:46	9.42.5.137	TVT2008	NVPLEX2	2	ACTIVE
02/15/11 11:37:46	9.42.5.136	TVT2007	NVPLEX2	2	ACTIVE
02/15/11 11:37:46	9.42.5.135	TVT2006	NVPLEX2	2	ACTIVE
02/15/11 11:37:46	9.42.5.131	TVT2002	NVPLEX2	2	ACTIVE
02/15/11 11:37:46	9.42.5.132	TVT2003	NETVIEW	2	ACTIVE
02/15/11 11:37:46	9.42.5.133	TVT2004	NETVIEW	2	ACTIVE
02/15/11 11:37:46	9.42.5.146	TVT2017	NETVIEW	2	ACTIVE

Figure 34. Workload Lifeline Agents Workspace

Workload Server Details Workspace

The Workload Server Details workspace displays the net weight and abnormal terminations for a specific workload server over time.

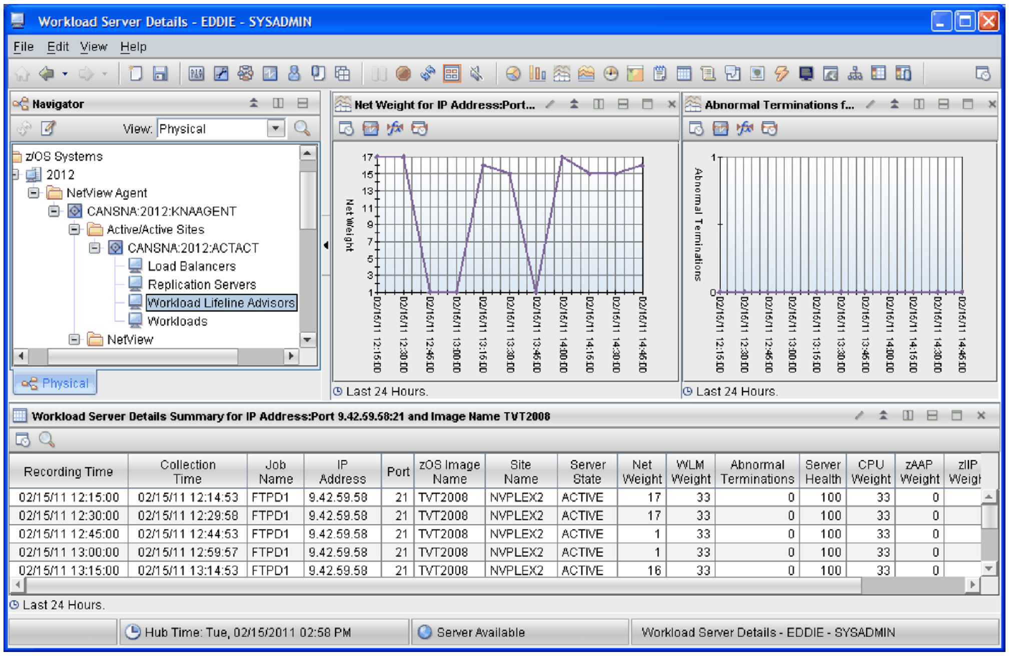
To display this workspace, click the link icon from a row in the Workload Servers and Filtered Workload Servers workspaces, the Workload Servers Summary table. See "Workload Servers Workspace" on page 62.

This workspace provides data that is updated by using sampling.

Historical data is enabled in this workspace.

For information about data collection and data display for this workspace, see *IBM Tivoli NetView for z/OS Installation: Configuring the GDPS Active/Active Continuous Availability Solution*.

This workspace is shown in Figure 35 on page 62.



Workload Server Details Summary for IP Address:Port 9.42.59.58:21 and Image Name TVT2008

Recording Time	Collection Time	Job Name	IP Address	Port	zOS Image Name	Site Name	Server State	Net Weight	WLM Weight	Abnormal Terminations	Server Health	CPU Weight	zAAP Weight	zIIP Weigh
02/15/11 12:15:00	02/15/11 12:14:53	FTPD1	9.42.59.58	21	TVT2008	NVPLEX2	ACTIVE	17	33	0	100	33	0	
02/15/11 12:30:00	02/15/11 12:29:58	FTPD1	9.42.59.58	21	TVT2008	NVPLEX2	ACTIVE	17	33	0	100	33	0	
02/15/11 12:45:00	02/15/11 12:44:53	FTPD1	9.42.59.58	21	TVT2008	NVPLEX2	ACTIVE	1	33	0	100	33	0	
02/15/11 13:00:00	02/15/11 12:59:57	FTPD1	9.42.59.58	21	TVT2008	NVPLEX2	ACTIVE	1	33	0	100	33	0	
02/15/11 13:15:00	02/15/11 13:14:53	FTPD1	9.42.59.58	21	TVT2008	NVPLEX2	ACTIVE	16	33	0	100	33	0	

Figure 35. Workload Server Details Workspace

Workload Servers Workspace

The Workload Servers workspace displays all servers that make up the defined workloads in both active and standby sites.

To display this workspace, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **Active/Active Sites** > *node*:**ACTACT**, select and right-click **Workload Lifeline Advisors**, click **Workspace**, and then click **Workload Servers**.

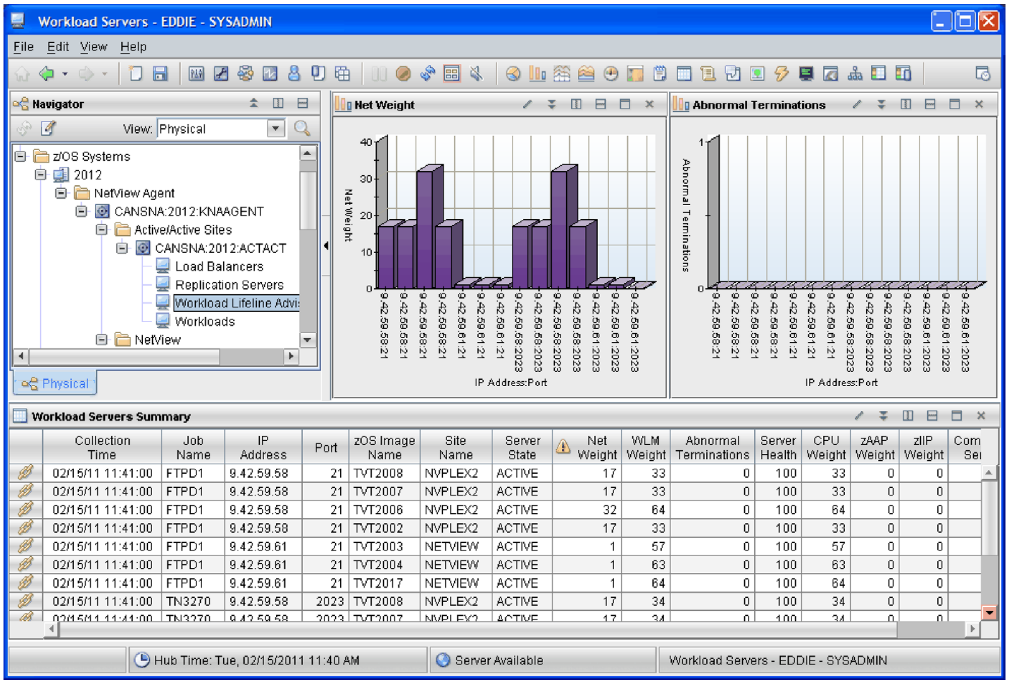
Note: You can also link to this workspace from the Workload Lifeline Advisors workspace.

This workspace provides data that is updated by using sampling.

Historical data is enabled in this workspace.

For information about data collection and data display for this workspace, see *IBM Tivoli NetView for z/OS Installation: Configuring the GDPS Active/Active Continuous Availability Solution*.

This workspace is shown in Figure 36 on page 63.



	Collection Time	Job Name	IP Address	Port	zOS Image Name	Site Name	Server State	⚠ Net Weight	WLM Weight	Abnormal Terminations	Server Health	CPU Weight	zAAP Weight	zIIP Weight	Com Ser
	02/15/11 11:41:00	FTPD1	9.42.59.58	21	TVT2008	NVPLEX2	ACTIVE	17	33	0	100	33	0	0	
	02/15/11 11:41:00	FTPD1	9.42.59.58	21	TVT2007	NVPLEX2	ACTIVE	17	33	0	100	33	0	0	
	02/15/11 11:41:00	FTPD1	9.42.59.58	21	TVT2006	NVPLEX2	ACTIVE	32	64	0	100	64	0	0	
	02/15/11 11:41:00	FTPD1	9.42.59.58	21	TVT2002	NVPLEX2	ACTIVE	17	33	0	100	33	0	0	
	02/15/11 11:41:00	FTPD1	9.42.59.61	21	TVT2003	NETVIEW	ACTIVE	1	57	0	100	57	0	0	
	02/15/11 11:41:00	FTPD1	9.42.59.61	21	TVT2004	NETVIEW	ACTIVE	1	63	0	100	63	0	0	
	02/15/11 11:41:00	FTPD1	9.42.59.61	21	TVT2017	NETVIEW	ACTIVE	1	64	0	100	64	0	0	
	02/15/11 11:41:00	TN3270	9.42.59.58	2023	TVT2008	NVPLEX2	ACTIVE	17	34	0	100	34	0	0	
	02/15/11 11:41:00	TN3270	9.42.59.58	2023	TVT2007	NVPLEX2	ACTIVE	17	34	0	100	34	0	0	

Figure 36. Workload Servers Workspace

Workload Site Details Workspace

The Workload Site Details workspace displays the workload routing weight for a specific site over time.

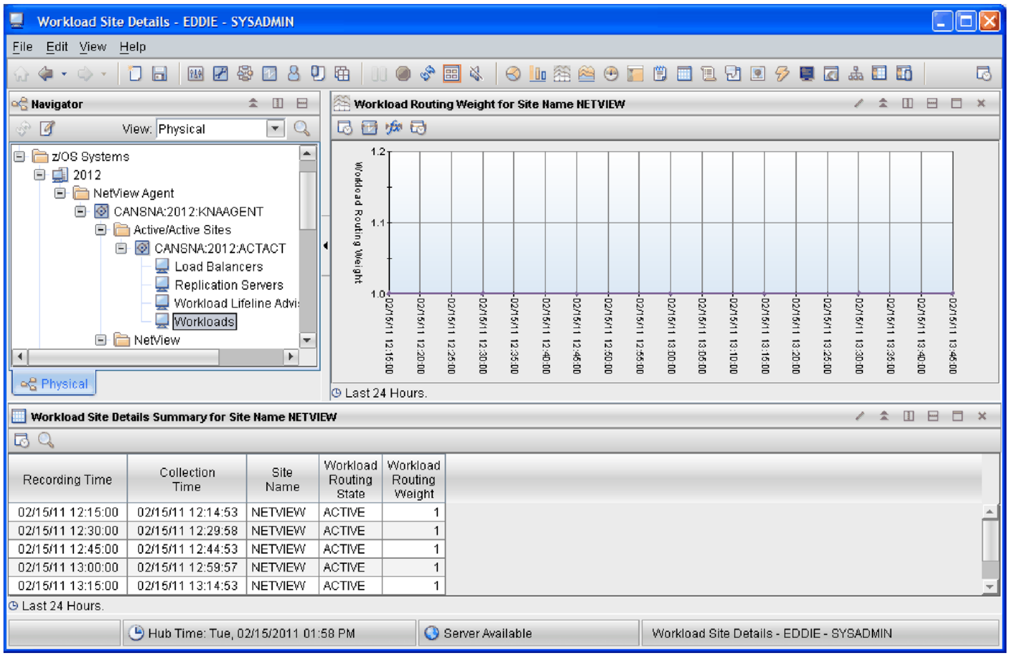
To display this workspace, click the link icon from the Workload Sites workspace, the Workload Sites Summary table. See “Workload Sites Workspace” on page 64.

This workspace provides data that is updated by using sampling.

Historical data is enabled in this workspace.

For information about data collection and data display for this workspace, see *IBM Tivoli NetView for z/OS Installation: Configuring the GDPS Active/Active Continuous Availability Solution*.

This workspace is shown in Figure 37 on page 64.



Recording Time	Collection Time	Site Name	Workload Routing State	Workload Routing Weight
02/15/11 12:15:00	02/15/11 12:14:53	NETVIEW	ACTIVE	1
02/15/11 12:30:00	02/15/11 12:29:58	NETVIEW	ACTIVE	1
02/15/11 12:45:00	02/15/11 12:44:53	NETVIEW	ACTIVE	1
02/15/11 13:00:00	02/15/11 12:59:57	NETVIEW	ACTIVE	1
02/15/11 13:15:00	02/15/11 13:14:53	NETVIEW	ACTIVE	1

Figure 37. Workload Site Details Workspace

Workload Sites Workspace

The Workload Sites workspace displays the sites for the selected workload.

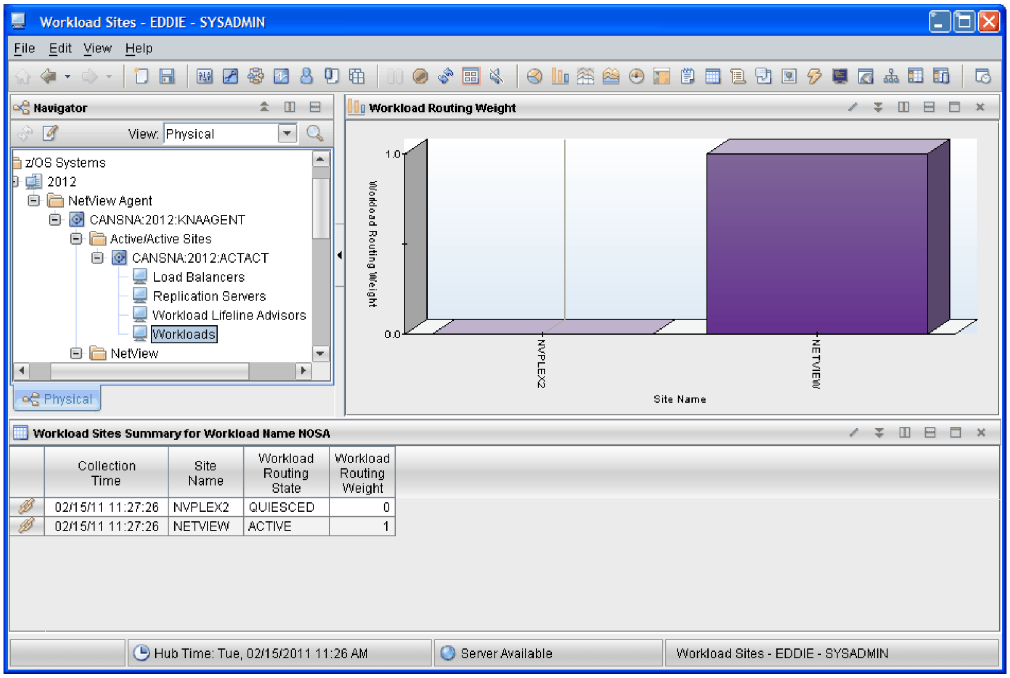
To display this workspace, click the link icon from a row in the Workloads workspace, the Workloads Summary table. See "Workloads Workspace" on page 65.

This workspace provides data that is updated by using sampling.

Historical data is enabled in this workspace.

For information about data collection and data display for this workspace, see *IBM Tivoli NetView for z/OS Installation: Configuring the GDPS Active/Active Continuous Availability Solution*.

This workspace is shown in Figure 38 on page 65.



Workload Sites Summary for Workload Name NOSA

Collection Time	Site Name	Workload Routing State	Workload Routing Weight
02/15/11 11:27:26	NVPLEX2	QUIESCED	0
02/15/11 11:27:26	NETVIEW	ACTIVE	1

Figure 38. Workload Sites Workspace

Workloads Workspace

The Workloads workspace displays all workloads that are defined for the GDPS Active/Active Continuous Availability solution.

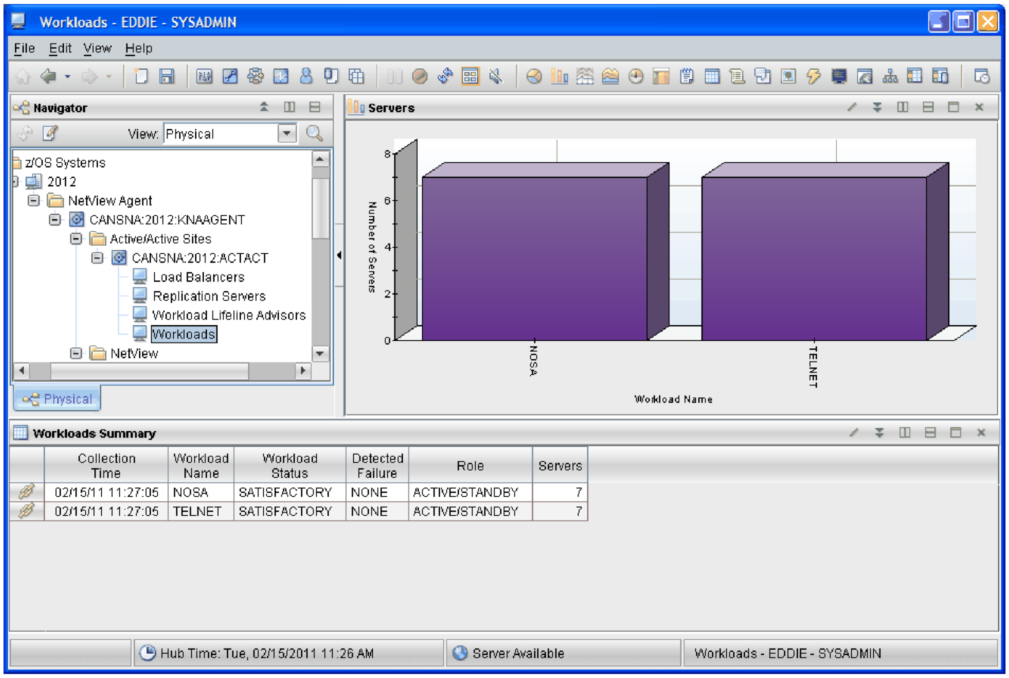
To display this workspace, expand **z/OS Systems** > *system* > **NetView Agent** > *subagent* > **Active/Active Sites** > *node*:**ACTACT**, and then click **Workloads**.

This workspace provides data that is updated by using sampling.

Historical data is not enabled in this workspace.

For information about data collection and data display for this workspace, see *IBM Tivoli NetView for z/OS Installation: Configuring the GDPS Active/Active Continuous Availability Solution*.

This workspace is shown in Figure 39 on page 66.



	Collection Time	Workload Name	Workload Status	Detected Failure	Role	Servers
	02/15/11 11:27:05	NOSA	SATISFACTORY	NONE	ACTIVE/STANDBY	7
	02/15/11 11:27:05	TELNET	SATISFACTORY	NONE	ACTIVE/STANDBY	7

Figure 39. Workload Sites Workspace

Part 3. Appendixes

Appendix A. Situations

The Tivoli Enterprise Portal runs tests called situations on systems where monitoring agents are installed. When the conditions of a situation are met, an event occurs and an event indicator is displayed over the applicable items in the Navigator. You can use situations to raise alerts of certain conditions and to trigger single action commands or automated workflows.

The IBM Tivoli NetView for z/OS Enterprise Management Agent (NetView agent) provides a set of situations that you can use to monitor the systems in your network. These predefined situations serve as models for defining custom situations for your environment.

Open the situation editor to see the definition of situations, to edit situations, or to create new situations using the attributes that are provided by the NetView agent. The left frame of the situation editor is a tree of the situations that are associated with the current Navigator item or, if you opened the editor from the toolbar, the situations for all installed monitoring products. The right frame shows this user assistance until you create or select a situation. In the situation editor tree, NetView situations are displayed under the **NetView** leaf and the GDPS Active/Active Continuous Availability solution situations are displayed under the **Active/Active Sites** leaf. No situations are defined in the situation editor tree under the **NetView Agent** leaf.

The following types of situations are provided with the NetView program:
- "DVIPA Situations"
- "Health Situations" on page 72
- "Stack Situations" on page 76
- "TCP/IP Connection Data Situations" on page 76
- "Telnet Server Situations" on page 77
- "GDPS Active/Active Continuous Availability Solution Situations" on page 77

For more information about using situations and the situation editor, see the *IBM Tivoli Monitoring: Tivoli Enterprise Portal User's Guide*.

DVIPA Situations

The NetView DVIPA situations are described in this section in alphabetical order.

NAS_DVIPA_Abnorm_Trans_Percent

This situation is triggered when the abnormal transaction percent is greater than 25.

By default, this situation does not start automatically and must be manually started to run.

Formula: Abnormal Transaction Percent > 25

NAS_DVIPA_Active_Target_Stacks

This situation is triggered when the number of target stacks that are available to service connection requests is equal to 0.

By default, this situation does not start automatically and must be manually started to run.

Formula: Active Target Stacks == 0

NAS_DVIPA_Bytes_Received

This situation is triggered when the number of bytes received is equal to 0.

By default, this situation does not start automatically and must be manually started to run.

Formula: Bytes Received == 0

NAS_DVIPA_Bytes_Sent

This situation is triggered when the number of bytes sent is equal to 0.

By default, this situation does not start automatically and must be manually started to run.

Formula: Bytes Sent == 0

NAS_DVIPA_Listening_Servers

This situation is triggered when the number of servers ready across all the target stacks to service connection requests is equal to 0.

By default, this situation does not start automatically and must be manually started to run.

Formula: Listening Servers == 0

NAS_DVIPA_Number_of_Connections

This situation is triggered when the total number of connections that are distributed to the target stack is equal to 0. This situation is no longer applicable in V5R4 or later because the attribute in the situation formula belongs to a deprecated attribute group. A new situation, NAS_DVIPA_Targ_Active_Conns, provides a similar capability as of V5R4.

By default, this situation does not start automatically and must be manually started to run.

Formula: Number of Connections == 0

NAS_DVIPA_Pct_Seg_Retran

This situation is triggered when the percentage of segments that are retransmitted is greater than or equal to 3.

By default, this situation does not start automatically and must be manually started to run.

Formula: Percent Segments Retransmitted >= 3

NAS_DVIPA_Port_Health_Percent

This situation is triggered when the port health percent is less than 90.

By default, this situation does not start automatically and must be manually started to run.

Formula: Port Health Percent < 90

NAS_DVIPA_Server_Accept_Percent

This situation is triggered when the server acceptance percent is less than 70. This situation is no longer applicable in V5R4 or later because the attribute in the situation formula belongs to a deprecated attribute group. A new situation, NAS_DVIPA_Target_Serv_Resp_Rate, provides a similar capability as of V5R4.

By default, this situation does not start automatically and must be manually started to run.

Formula: Server Acceptance Percent < 70

NAS_DVIPA_Targ_Active_Conns

This situation is triggered when the number of active connections is equal to 0.

By default, this situation does not start automatically and must be manually started to run.

Formula: Active Connections == 0

NAS_DVIPA_Targ_Delta_Conns

This situation is triggered when the number of delta connections is equal to 0.

By default, this situation does not start automatically and must be manually started to run.

Formula: Delta Connections == 0

NAS_DVIPA_Targ_Listening_Srvrs

This situation is triggered when the number of listening servers is equal to 0.

By default, this situation does not start automatically and must be manually started to run.

Formula: Listening Servers == 0

NAS_DVIPA_Target_Serv_Resp_Rate

This situation is triggered when the target server responsiveness value is less than 80.

By default, this situation does not start automatically and must be manually started to run.

Formula: Target Server Responsiveness Rate < 80

NAS_DVIPA_Total_Bytes_Received

This situation is triggered when the number of bytes received over the connection is equal to 0.

By default, this situation does not start automatically and must be manually started to run.

Formula: Total Bytes Received == 0

NAS_DVIPA_Total_Bytes_Sent

This situation is triggered when the number of bytes sent over the connection is equal to 0.

By default, this situation does not start automatically and must be manually started to run.

Formula: Total Bytes Sent == 0

NAS_DVIPA_WLM_Weight

This situation is triggered when the WLM weight is equal to 0.

By default, this situation does not start automatically and must be manually started to run.

Formula: WLM Weight == 0

Health Situations

The NetView health situations are described in this section in alphabetical order.

NAS_NVApp_Status

This situation is triggered when the NetView status is inactive.

By default, this situation does not start automatically and must be manually started to run.

Formula: Status == 'INACTIVE'

NAS_NVApp_Total_CPU

This situation is triggered when the current NetView CPU percentage is greater than or equal to 95.

By default, this situation does not start automatically and must be manually started to run.

Formula: Total CPU >= 95

NAS_NVApp_Total_Storage

This situation is triggered when the current NetView storage utilization is greater than or equal to 52 430.

By default, this situation does not start automatically and must be manually started to run.

Formula: Total Storage >= 52430

NAS_NVTask_CPU_Util_Crit

This situation is triggered when the relative percentage of the CPU utilization for a task is greater than or equal to 90.

By default, this situation does not start automatically and must be manually started to run.

Formula: CPU Utilization >= 90

NAS_NVTask_CPU_Util_Info

This situation is triggered when the relative percentage of the CPU utilization for a task is greater than or equal to 50 and less than 75.

By default, this situation does not start automatically and must be manually started to run.

Formula: CPU Utilization >= 50 AND CPU Utilization < 75

NAS_NVTask_CPU_Util_Warn

This situation is triggered when the relative percentage of the CPU utilization for a task is greater than or equal to 75 and less than 90.

By default, this situation does not start automatically and must be manually started to run.

Formula: CPU Utilization >= 75 AND CPU Utilization < 90

NAS_NVTask_Input_Msg_Rate_Crit

This situation is triggered when the rate of messages coming into a task is greater than or equal to 200 000.

By default, this situation does not start automatically and must be manually started to run.

Formula: Input Message Rate >= 200000

NAS_NVTask_Input_Msg_Rate_Info

This situation is triggered when the rate of messages coming into a task is greater than or equal to 100 000 and less than 150 000.

By default, this situation does not start automatically and must be manually started to run.

Formula: Input Message Rate >= 100000 AND Input Message Rate < 150000

NAS_NVTask_Input_Msg_Rate_Warn

This situation is triggered when the rate of messages coming into a task is greater than or equal to 150 000 and less than 200 000.

By default, this situation does not start automatically and must be manually started to run.

Formula: Input Message Rate >= 150000 AND Input Message Rate < 200000

NAS_NVTask_IO_Rate_Crit

This situation is triggered when the rate of I/O requests for a task is greater than or equal to 200 000.

By default, this situation does not start automatically and must be manually started to run.

Formula: I/O Rate >= 200000

NAS_NVTask_IO_Rate_Info

This situation is triggered when the rate of I/O requests for a task is greater than or equal to 50 000 and less than 100 000.

By default, this situation does not start automatically and must be manually started to run.

Formula: I/O Rate >= 50000 AND I/O Rate < 100000

NAS_NVTask_IO_Rate_Warn

This situation is triggered when the rate of I/O requests for a task is greater than or equal to 100 000 and less than 200 000.

By default, this situation does not start automatically and must be manually started to run.

Formula: I/O Rate >= 100000 AND I/O Rate < 200000

NAS_NVTask_Msg_Queue_Crit

This situation is triggered when the number of buffers that are on the public message queue or queues for a task is greater than or equal to 3 000.

By default, this situation does not start automatically and must be manually started to run.

Formula: Message Queue Count >= 3000

NAS_NVTask_Msg_Queue_Info

This situation is triggered when the number of buffers that are on the public message queue or queues for a task is greater than or equal to 1 000 and less than 2 000.

By default, this situation does not start automatically and must be manually started to run.

Formula: Message Queue Count >= 1000 AND Message Queue Count < 2000

NAS_NVTask_Msg_Queue_Warn

This situation is triggered when the number of buffers that are on the public message queue or queues for a task is greater than or equal to 2 000 and less than 3 000.

By default, this situation does not start automatically and must be manually started to run.

Formula: Message Queue Count >= 2000 AND Message Queue Count < 3000

NAS_NVTask_Output_Msg_Rate_Crit

This situation is triggered when the rate of messages leaving a task is greater than or equal to 200 000.

By default, this situation does not start automatically and must be manually started to run.

Formula: Output Message Rate >= 200000

NAS_NVTask_Output_Msg_Rate_Info

This situation is triggered when the rate of messages leaving a task is greater than or equal to 100 000 and less than 150 000.

By default, this situation does not start automatically and must be manually started to run.

Formula: Output Message Rate >= 100000 AND Output Message Rate < 150000

NAS_NVTask_Output_Msg_Rate_Warn

This situation is triggered when the rate of messages leaving a task is greater than or equal to 150 000 and less than 200 000.

By default, this situation does not start automatically and must be manually started to run.

Formula: Output Message Rate >= 150000 AND Output Message Rate < 200000

NAS_NVTask_Status_Crit

This situation is triggered when the overall indicator of the health of a task reaches a critical value. The formula for this situation (Status=='INACTIVE' and Task Name=='DSIUDST') is provided as a sample. You need to determine the task and status that constitute a critical status for your network.

By default, this situation does not start automatically and must be manually started to run.

Formula: Status == 'INACTIVE' AND Task Name = 'DSIUDST'

NAS_NVTask_Storage_Crit

This situation is triggered when the amount of storage that is currently used by a task is greater than or equal to 200 000.

By default, this situation does not start automatically and must be manually started to run.

Formula: Storage >= 200000

NAS_NVTask_Storage_Info

This situation is triggered when the amount of storage that is currently used by a task is greater than or equal to 100 000 and less than 150 000.

By default, this situation does not start automatically and must be manually started to run.

Formula: Storage >= 100000 AND Storage < 150000

NAS_NVTask_Storage_Warn

This situation is triggered when the amount of storage that is currently used by a task is greater than or equal to 150 000 and less than 200 000.

By default, this situation does not start automatically and must be manually started to run.

Formula: Storage == 150000 AND Storage < 200000

Stack Situations

The NetView stack situations are described in this section.

NAS_Stack_Status

This situation is triggered when the status of the stack is not active.

By default, this situation does not start automatically and must be manually started to run.

Formula: Status != 'ACTIVE'

TCP/IP Connection Data Situations

The NetView TCP/IP connection data situations are described in this section in alphabetical order.

NAS_TCPIPConn_Bytes_Received

This situation is triggered when the number of bytes received over the TCP/IP connection is equal to 0.

By default, this situation does not start automatically and must be manually started to run.

Formula: Bytes Received == 0

NAS_TCPIPConn_Bytes_Sent

This situation is triggered when the number of bytes sent over the TCP/IP connection is equal to 0.

By default, this situation does not start automatically and must be manually started to run.

Formula: Bytes Sent == 0

NAS_TCPIPConn_Pct_Seg_Retran

This situation is triggered when the percent of TCP/IP packets retransmitted is greater than or equal to 3.

By default, this situation does not start automatically and must be manually started to run.

Formula: Percent Segments Retransmitted >= 3

Telnet Server Situations

The NetView Telnet server situations are described in this section in alphabetical order.

NAS_Telnet_Active_Ports

This situation is triggered when the number of active ports that are associated with the Telnet server job is equal to 0.

By default, this situation does not start automatically and must be manually started to run.

Formula: Active Ports == 0

NAS_Telnet_Configured_Ports

This situation is triggered when the number of configured ports that are associated with the Telnet server job is equal to 0.

By default, this situation does not start automatically and must be manually started to run.

Formula: Configured Ports == 0

NAS_Telnet_SP_Port_Status

This situation is triggered when the status of the Telnet server port is not active.

By default, this situation does not start automatically and must be manually started to run.

Formula: Port Status != ACTIVE'

NAS_Telnet_SP_Server_Status

This situation is triggered when the status of the Telnet server is not active.

By default, this situation does not start automatically and must be manually started to run.

Formula: Server Status != 'ACTIVE'

GDPS Active/Active Continuous Availability Solution Situations

The GDPS Active/Active Continuous Availability solution situations are described in this section.

NAS_AA_DB2_QPctFull

This situation is triggered when the queue percent full as determined by the DB2 apply server reaches a warning level.

By default, this situation does not start automatically and must be manually started to run.

Formula: Queue Percent Full >= 80

NAS_AA_IMS_AppQPctFull_Crit

This situation is triggered when the apply queue percent full as determined by the IMS apply server reaches the defined critical value.

By default, this situation does not start automatically and must be manually started to run.

Formula: Apply Queue Percent Full >= 80

NAS_AA_IMS_AppQPctFull_Warn

This situation is triggered when the apply queue percent full as determined by the IMS apply server reaches the defined warning value.

By default, this situation does not start automatically and must be manually started to run.

Formula: Apply Queue Percent Full >= 60 AND Apply Queue Percent Full < 80

NAS_AA_IMS_CapQPctFull_Crit

This situation is triggered when the capture queue percent full as determined by the IMS capture server reaches the defined critical value.

By default, this situation does not start automatically and must be manually started to run.

Formula: Capture Queue Percent Full >= 80

NAS_AA_IMS_CapQPctFull_Warn

This situation is triggered when the capture queue percent full as determined by the IMS capture server reaches the defined warning value.

By default, this situation does not start automatically and must be manually started to run.

Formula: Capture Queue Percent Full >= 60 AND Capture Queue Percent Full < 80

NAS_AA_LB_Status

This situation is triggered when the status of the load balancer is not active.

By default, this situation does not start automatically and must be manually started to run.

Formula: Status != ACTIVE

NAS_AA_RS_AppServerStatus

This situation is triggered when the status of the apply server is inactive. When this situation is triggered, a system command issues the AQN008I message for use in automation by the GDPS Active/Active Continuous Availability solution.

By default, this situation does not start automatically and must be manually started to run.

Formula: Apply Server Status == INACTIVE

NAS_AA_RS_CapServerStatus

This situation is triggered when the status of the capture server is inactive. When this situation is triggered, a system command issues the AQN008I message for use in automation by the GDPS Active/Active Continuous Availability solution.

By default, this situation does not start automatically and must be manually started to run.

Formula: Capture Server Status == INACTIVE

NAS_AA_RS_DB2WorkloadState

This situation is triggered when the state of the workload as determined by the DB2 capture server or DB2 apply server is considered to be unsatisfactory. When this situation is triggered, a system command issues the AQN008I message for use in automation by the GDPS Active/Active Continuous Availability solution.

By default, this situation does not start automatically and must be manually started to run.

Formula: (Workload Type == DB2 AND Capture Workload State == INACTIVE) OR (Workload Type == DB2 AND Apply Workload State == INACTIVE)

NAS_AA_RS_IMSWorkloadState

This situation is triggered when the state of the workload as determined by the IMS capture server is considered to be unsatisfactory. When this situation is triggered, a system command issues the AQN008I message for use in automation by the GDPS Active/Active Continuous Availability solution.

By default, this situation does not start automatically and must be manually started to run.

Formula: Workload Type == IMS AND Capture Workload State != 'REPLICATE CONTINUOUS' AND Capture Workload State != STARTING

NAS_AA_RS_LatencyExceeded

This situation is triggered when the average latency has reached the defined warning value. Latency can also be defined in a System Automation for z/OS policy and should match the latency that is defined in the situation formula. When this situation is triggered, a system command issues the AQN008I message for use in automation by the GDPS Active/Active Continuous Availability solution.

By default, this situation does not start automatically and must be manually started to run.

Formula: Average Latency >= 3000

This situation is associated with the NAP_AA_RS_LatencyReset policy, which resets the latency when the NAS_AA_RS_LatencyExceeded situation is resolved. This predefined policy performs the following actions:

1. Waits until the NAS_AA_RS_LatencyExceeded situation is true.
2. Waits until the NAS_AA_RS_LatencyExceeded situation is false.
3. Issues the NA: AQNE1004 LATENCYRESET take action command.

By default, this policy does not start automatically and must be manually started to run.

For more information about policies, see *IBM Tivoli Monitoring: Tivoli Enterprise Portal User's Guide*.

NAS_AA_WLA_Agents

This situation is triggered when the number of Multi-site Workload Lifeline Agents that are connected to the primary Multi-site Workload Lifeline Advisor is equal to 0.

By default, this situation does not start automatically and must be manually started to run.

Formula: Role == PRIMARY AND Workload Lifeline Agents == 0

NAS_AA_WLA_LBs

This situation is triggered when the number of external and internal (for example, sysplex distributor) load balancers that are registered with the primary Multi-site Workload Lifeline Advisor is equal to 0.

By default, this situation does not start automatically and must be manually started to run.

Formula: Role == PRIMARY AND Registered Load Balancers == 0

NAS_AA_WLA_NetWeight

This situation is triggered when the net weight for this server application relative to other server instances that are defined for this workload on the same site is equal to 0. The net weight is calculated by applying the Communications Server health as a percentage of the WLM weight for this server. It is then normalized against the other server instances (active on this same site) that are defined for this workload.

By default, this situation does not start automatically and must be manually started to run.

Formula: Net Weight == 0

NAS_AA_Workload_Status

This situation is triggered when the overall status of the workload is not satisfactory.

By default, this situation does not start automatically and must be manually started to run.

Formula: Workload Status != SATISFACTORY

Appendix B. Take Action Commands

You can use take action commands to issue certain NetView for z/OS commands from within the Tivoli Enterprise Portal. The arguments that can be specified for the take action commands are the same as the keywords for the NetView for z/OS commands. Required arguments and default values are also the same, unless otherwise specified. The argument values provide assistance when you are issuing the command. If an argument value is not specified, the keyword has no value.

All take action command responses, except for the Browse NetView Logs take action command response, are displayed in the NetView Command Response workspace; see "NetView Command Response Workspace" on page 45.

Take action commands that are used with the GDPS Active/Active Continuous Availability solution are available only from the workspaces that are defined to the **Active/Active Sites** subnode in the Tivoli Enterprise Portal navigator. These commands are not accessible from the workspaces that are defined to the **NetView** subnode in the Tivoli Enterprise Portal navigator. Similarly, the take action commands that are available from the workspaces that are defined to the **NetView** subnode are not available from the workspaces that are defined to the **Active/Active Sites** subnode.

You can issue the following take action commands from the IBM Tivoli NetView for z/OS Enterprise Management Agent. The corresponding NetView for z/OS command is shown in parentheses. For more information about these commands, see the NetView for z/OS online help.

- "Browse NetView Logs (AGTBRW)" on page 82
- "Format Packet Trace (FMTPACKT)" on page 82
- "Issue NetView Commands" on page 83
- "List NetView Task (LIST)" on page 83
- "List Status for All NetView Tasks (LIST)" on page 83
- "Purge Packet Trace (PKTS)" on page 83
- "Quiesce the Telnet Server Port" on page 83
- "Resume the Telnet Server Port" on page 84
- "Start NetView Task (START)" on page 84
- "Stop Force NetView Task (STOP)" on page 84
- "Stop Immed NetView Task (STOP)" on page 84
- "Stop NetView Task (STOP)" on page 84
- "View Application-Instance DVIPA (DVIPSTAT)" on page 84
- "View Data Collection Statistics (NACTL)" on page 84
- "View Data Collection Statistics for Active/Active Sites (ACTVCTL)" on page 84
- "View DB2 Replication Details (ACTVREPL)" on page 85
- "View Distributed DVIPA Connection Routing (DVIPDDCR)" on page 85
- "View Distributed DVIPA Server Health (DVIPHLTH)" on page 85
- "View DVIPA Connections (DVIPCONN)" on page 85
- "View DVIPA Definition and Status (DVIPSTAT)" on page 85
- "View DVIPA Distributor Targets (DVIPTARG)" on page 85
- "View DVIPA Sysplex Distributors (DVIPPLEX)" on page 86
- "View HiperSockets Configuration and Status (HIPERSOC)" on page 86
- "View IMS Replication Details (ACTVREPL)" on page 86
- "View Load Balancer Groups (ACTVLIFE)" on page 86
- "View Load Balancer Workloads (ACTVLIFE)" on page 86
- "View Load Balancers (ACTVLIFE)" on page 86

Browse NetView Logs (AGTBRW)

Use this command to browse the network log from the NetView for z/OS Enterprise Management Agent. See the NetView for z/OS online help for more information about the AGTBRW, BLOG, and BROWSE commands.

Format Packet Trace (FMTPACKT)

Use this command to collect a subset of the packet trace entries (based on the specified QUERY parameters), convert the trace entries into a readable form, and then generate reports based on the specified options.

See the NetView for z/OS online help for more information about the FMTPACKT command and parameters:

- PKTS_QUERYCommandParameters - Retrieve a subset of packet trace entries.
- PIPE_FMTPACKTOptions - Specify report options.

The FMTPACKT command is used differently by the NetView for z/OS Enterprise Management Agent than it is used on the NetView for z/OS command line. This command differs in the NetView for z/OS Enterprise Management Agent in the following ways:

- The following FMTPACKT keywords, which do not require a value when the command is issued from the NetView command line, do require a value if specified on the Format Packet Trace take action command; otherwise, the keyword is ignored:
  - SESSION
  - STATS
  - STREAMS
- FMTPACKT has formatting options that do not fit into the *argument=argument* value format. These options are argument values only on the Format Packet Trace take action command:
  - reportfmt
    SUMMARY
    FULL

SHORT
TALLY

- timefmt

  LOCAL
  GMT

- datafmt

  PORTSEL
  ASCII
  BOTH
  EBCDIC
  HEX

- segment

  SEGMENT
  NOSEGMNT

Issue NetView Commands

Use this command to enter commands that can be issued from a NetView for z/OS command line. Not all NetView for z/OS commands are enabled from the Tivoli Enterprise Portal. Some, including NetView full screen commands (for example, NPDA and NLDM), are not available in the Tivoli Enterprise Portal.

List NetView Task (LIST)

Use this command to display the status of the task. The default command that is issued by this take action command is LIST TASK=*task*. See the NetView for z/OS online help for more information about the LIST command.

List Status for All NetView Tasks (LIST)

Use this command to list the status for all NetView tasks. The default command that is issued by this take action command is LIST STATUS=TASK. See the NetView for z/OS online help for more information about the LIST STATUS command.

Purge Packet Trace (PKTS)

Use this command to purge packet data records matching the input criteria. If the purge is successful, the BNH774I message is returned. The default command that is issued by this take action command is PKTS PURGE LADDR=*laddr* LPORT=*lport* RADDR=*raddr* RPORT=*rport* INTFNAME=*intfname* TIME=*time* TCPNAME=*tcpname* PROTOCOL=*protocol*. See the NetView for z/OS online help for more information about the PKTS PURGE command.

Quiesce the Telnet Server Port

Use this command to quiesce the specified Telnet server port. The default MVS command issued by this take action command is MVS VARY TCPIP,,TELNET,QUIESCE,PORT=*port*. For information about the VARY TCPIP command, see *z/OS Communications Server IP System Administrator's Commands*.

Resume the Telnet Server Port

Use this command to resume the Telnet server port. The default MVS command issued by this take action command is MVS VARY TCPIP,,TELNET,RESUME,PORT=*port*. For information about the VARY TCPIP command, see *z/OS Communications Server IP System Administrator's Commands*.

Start NetView Task (START)

Use this command to start the specified optional NetView task. The default command that is issued by this take action command is START TASK=*task*. See the NetView for z/OS online help for more information about the START command.

Stop Force NetView Task (STOP)

Use this command to stop a task that cannot process normally. The default command that is issued by this take action command is STOP FORCE=*task*. See the NetView for z/OS online help for more information about the STOP command.

Stop Immed NetView Task (STOP)

Use this command to stop the specified NetView task immediately. The default command that is issued by this take action command is STOP IMMED=*task*. See the NetView for z/OS online help for more information about the STOP command.

Stop NetView Task (STOP)

Use this command to cause a task to end normally. The default command that is issued by this take action command is STOP TASK=*task*. See the NetView for z/OS online help for more information about the STOP command.

View Application-Instance DVIPA (DVIPSTAT)

Use this command to view the application-instance dynamic virtual IP address (DVIPA). This command issues the CNMSDVIP sample, which issues the DVIPSTAT command. The CNMSDVIP sample and the DVIPSTAT command have the same operands. See the NetView for z/OS online help for more information about the DVIPSTAT command.

View Data Collection Statistics (NACTL)

Use this command to view data collection statistics. The default command that is issued by this take action command is NACTL LISTINFO. See the NetView for z/OS online help for more information about the NACTL LISTINFO command.

View Data Collection Statistics for Active/Active Sites (ACTVCTL)

Note: This command is used with the GDPS Active/Active Continuous Availability solution.

Use this command to view data collection statistics for the GDPS Active/Active Continuous Availability solution. The default command that is issued by this take action command is ACTVCTL. See the NetView for z/OS online help for more information about the ACTVCTL command.

View DB2 Replication Details (ACTVREPL)

Note: This command is used with the GDPS Active/Active Continuous Availability solution.

Use this command to view DB2 replication details. The default command that is issued by this take action command is ACTVREPL. See the NetView for z/OS online help for more information about the ACTVREPL command.

View Distributed DVIPA Connection Routing (DVIPDDCR)

Use this command to view the distributed dynamic virtual IP address (DVIPA) connection routing. This command issues the CNMSDDCR sample, which issues the DVIPDDCR command. The CNMSDDCR sample and the DVIPDDCR command have the same operands. See the NetView for z/OS online help for more information about the DVIPDDCR command.

View Distributed DVIPA Server Health (DVIPHLTH)

Use this command to view the distributed dynamic virtual IP address (DVIPA) server health. This command issues the CNMSDVPH sample, which issues the DVIPHLTH command. The CNMSDVPH sample and the DVIPHLTH command have the same operands. See the NetView for z/OS online help for more information about the DVIPHLTH command.

View DVIPA Connections (DVIPCONN)

Use this command to view the dynamic virtual IP address (DVIPA) connections. This command issues the CNMSDVPC sample, which issues the DVIPCONN command. The CNMSDVPC sample and the DVIPCONN command have the same operands. See the NetView for z/OS online help for more information about the DVIPCONN command.

View DVIPA Definition and Status (DVIPSTAT)

Use this command to view the status of the dynamic virtual IP addresses (DVIPAs). This command issues the CNMSDVIP sample, which issues the DVIPSTAT command. The CNMSDVIP sample and the DVIPSTAT command have the same operands. See the NetView for z/OS online help for more information about the DVIPSTAT command.

View DVIPA Distributor Targets (DVIPTARG)

Use this command to view information about the distributed dynamic virtual IP address (DVIPA) targets. This command issues the CNMSTARG sample, which issues the DVIPTARG command. The CNMSTARG sample and the DVIPTARG command have the same operands. See the NetView for z/OS online help for more information about the DVIPTARG command.

View DVIPA Sysplex Distributors (DVIPPLEX)

Use this command to view information about distributed dynamic virtual IP address (DVIPA) sysplex distributors. This command issues the CNMSPLEX sample, which issues the DVIPPLEX command. The CNMSPLEX sample and DVIPPLEX command have the same operands. See the NetView for z/OS online help for more information about the DVIPPLEX command.

View HiperSockets Configuration and Status (HIPERSOC)

Use this command to view the HiperSockets configuration and status. This command issues the CNMSHIPR sample, which issues the HIPERSOC command. The CNMSHIPR sample and the HIPERSOC command have the same operands. See the NetView for z/OS online help for more information about the HIPERSOC command.

View IMS Replication Details (ACTVREPL)

Note: This command is used with the GDPS Active/Active Continuous Availability solution.

Use this command to view IMS replication details. The default command that is issued by this take action command is ACTVREPL. See the NetView for z/OS online help for more information about the ACTVREPL command.

View Load Balancer Groups (ACTVLIFE)

Note: This command is used with the GDPS Active/Active Continuous Availability solution.

Use this command to view load balancer groups. The default command that is issued by this take action command is ACTVLIFE. See the NetView for z/OS online help for more information about the ACTVLIFE command.

View Load Balancer Workloads (ACTVLIFE)

Note: This command is used with the GDPS Active/Active Continuous Availability solution.

Use this command to view load balancer workloads. The default command that is issued by this take action command is ACTVLIFE. See the NetView for z/OS online help for more information about the ACTVLIFE command.

View Load Balancers (ACTVLIFE)

Note: This command is used with the GDPS Active/Active Continuous Availability solution.

Use this command to view load balancers. The default command that is issued by this take action command is ACTVLIFE. See the NetView for z/OS online help for more information about the ACTVLIFE command.

View NetView Applications (NVSTAT)

Use this command to view NetView applications. This command issues the CNMSNVST sample, which issues the NVSTAT command. The CNMSNVST sample and the NVSTAT command have the same operands. See the NetView for z/OS online help for more information about the NVSTAT command.

View NetView Resource Utilization (RESOURCE)

Use this command to view NetView resource utilization. See the NetView for z/OS online help for more information about the RESOURCE command.

View OSA Channels and Ports (OSAPORT)

Use this command to view the OSA channels and ports. This command issues the CNMSOSAP sample, which issues the OSAPORT command. The CNMSOSAP sample and the OSAPORT command have the same operands. See the NetView for z/OS online help for more information about the OSAPORT command.

View Replication Servers (ACTVREPL)

Note: This command is used with the GDPS Active/Active Continuous Availability solution.

Use this command to view replication servers. The default command that is issued by this take action command is ACTVREPL. See the NetView for z/OS online help for more information about the ACTVREPL command.

View Session Configuration Data (SESSC)

Use this command to display session monitor configuration data. See the NetView for z/OS online help for more information about the SESSC command.

View Session Data (AGTSESMG)

Use this command to display SNA sessions collected by the session monitor. See the NetView for z/OS online help for more information about the SESMGET and SESS commands.

View Stack Configuration and Status (STACSTAT)

Use this command to view stack configuration and status. This command issues the CNMSSTAC sample, which issues the STACSTAT command. The CNMSSTAC sample and the STACSTAT command have the same operands. See the NetView for z/OS online help for more information about the STACSTAT command.

View Stack-Defined DVIPA (DVIPSTAT)

Use this command to view the stack-defined dynamic virtual IP address (DVIPA). This command issues the CNMSDVIP sample, which issues the DVIPSTAT command. The CNMSDVIP sample and the DVIPSTAT command have the same operands. See the NetView for z/OS online help for more information about the DVIPSTAT command.

View TASKMON Data by Task (TASKMON)

Use this command to monitor NetView tasks. The output under each group is sorted by the severity index. See the NetView for z/OS online help for more information about the TASKMON command.

View TASKMON Data for All Tasks (TASKMON)

Use this command to monitor all NetView tasks. The default command that is issued by this take action command is TASKMON ALL. See the NetView for z/OS online help for more information about the TASKMON command.

View TASKUTIL Data by Task (TASKUTIL)

Use this command to display CPU utilization and storage use for NetView tasks. See the NetView for z/OS online help for more information about the TASKUTIL command.

Note: If the task name on the selected row is MAINTASK, the command is converted to the proper syntax; that is, you see TASKUTIL MAINTASK, but the command that gets processed is TASKUTIL TYPE=MNT.

View TASKUTIL Data for All Tasks (TASKUTIL)

Use this command to display CPU utilization and storage use for all NetView tasks. The default command that is issued by this take action command is TASKUTIL TYPE=ALL. See the NetView for z/OS online help for more information about the TASKUTIL command.

View TCP/IP Connections (AGTTCPC)

Use this command to view TCP/IP connection data. This command issues the CNMSTCPC sample, which displays TCP/IP connection data collected by NetView TCPCONN services. See the NetView for z/OS online help for more information about the AGTTCPC and TCPCONN commands.

View Telnet Server Configuration and Status (TELNSTAT)

Use this command to view Telnet server configuration and status. This command issues the CNMSTNST sample, which issues the TELNSTAT command. The CNMSTNST sample and the TELNSTAT command have the same operands. See the NetView for z/OS online help for more information about the TELNSTAT command.

View Telnet Server Port Configuration and Status (TNPTSTAT)

Use this command to view Telnet server port configuration and status. This command issues the CNMSTPST sample, which issues the TNPTSTAT command. The CNMSTPST sample and the TNPTSTAT command have the same operands. See the NetView for z/OS online help for more information about the TNPTSTAT command.

View VIPA Routes (VIPAROUT)

Use this command to view virtual IP address (VIPA) routes. This command issues the CNMSVPRT sample, which samples the output of the VIPAROUT command. See the NetView for z/OS online help for more information about the VIPAROUT command.

View Workload Lifeline Advisors (ACTVLIFE)

Note: This command is used with the GDPS Active/Active Continuous Availability solution.

Use this command to view Workload Lifeline Advisors. The default command that is issued by this take action command is ACTVLIFE. See the NetView for z/OS online help for more information about the ACTVLIFE command.

View Workload Lifeline Agents (ACTVLIFE)

Note: This command is used with the GDPS Active/Active Continuous Availability solution.

Use this command to view Workload Lifeline Agents. The default command that is issued by this take action command is ACTVLIFE. See the NetView for z/OS online help for more information about the ACTVLIFE command.

View Workload Servers (ACTVLIFE)

Note: This command is used with the GDPS Active/Active Continuous Availability solution.

Use this command to view workload servers. The default command that is issued by this take action command is ACTVLIFE. See the NetView for z/OS online help for more information about the ACTVLIFE command.

View Workload Sites (ACTVLIFE)

Note: This command is used with the GDPS Active/Active Continuous Availability solution.

Use this command to view workload sites. The default command that is issued by this take action command is ACTVLIFE. See the NetView for z/OS online help for more information about the ACTVLIFE command.

View Workloads (ACTVLIFE)

Note: This command is used with the GDPS Active/Active Continuous Availability solution.

Use this command to view workloads. The default command that is issued by this take action command is ACTVLIFE. See the NetView for z/OS online help for more information about the ACTVLIFE command.

Appendix C. Attributes

Use the Tivoli NetView for z/OS Enterprise Management Agent attributes to build views that display the availability of your network.

A direct relationship exists between the attributes and the table views. An attribute group corresponds to a table view. Each attribute group has one or more attribute items. The attribute items correspond to the columns in a table view. For information about an attribute group and the attributes in the group, click the group name in the Contents pane. For a list of the attribute groups that are associated with the predefined workspaces, see Appendix D, "Workspaces and Attribute Groups," on page 149.

Attributes That Require z/OS V1R11 Communications Server or Later

The following table shows the attributes or specific attribute values that require z/OS V1R11 Communications Server or later.

Table 6. Attributes That Require z/OS V1R11 Communications Server or Later

Attribute Group	Attributes or Attribute Values That Require z/OS V1R11 Communications Server or Later
Distributed DVIPA Connection Routing	All attributes
Distributed DVIPA Server Health	DESTIP Weight Proportional CP Weight Proportional zAAP Weight Proportional zIIP Weight Raw Composite Weight Raw CP Weight Raw zAAP Weight Raw zIIP Weight
Distributed DVIPA Targets	Active Connections Distribution Port Function (distTargetControlled value)
DVIPA Definition and Status	Application Server Name Time Activated
DVIPA Sysplex Distributors	Configured Target Stacks DESTIP ALL Distribution Method (targetControlled value) PROCTYPE CP PROCTYPE ZAAP PROCTYPE ZIIP PROCXCOST ZAAP PROCXCOST ZIIP ILWEIGHTING
Stack Configuration and Status	Segmentation Offload Enabled Sysplex WLM Polling Interval TCP Stack Source VIPA Enabled TCP Stack Source VIPAV6 Enabled zIIP IP Security Enabled
HiperSockets Configuration and Status	All attributes
VIPA Routes	All attributes

Attributes That Require z/OS V1R12 Communications Server or Later

The following table shows the attributes or specific attribute values that require z/OS V1R12 Communications Server or later.

Table 7. Attributes That Require z/OS V1R12 Communications Server or Later

Attribute Group	**Attributes or Attribute Values That Require z/OS V1R12 Communications Server or Later**
DVIPA Sysplex Distributors	Auto Switch Back Distribution Method (hotStandby value) Health Switch Hot Standby Rank
Distributed DVIPA Targets	Hot Standby Rank Hot Standby Server Status Hot Standby Server Type
OSA Ports	Channel Type (osaIntraensembleData and osaIntraensembleManage values)

Active DVIPA Connection Count Attributes

Use these attributes to view active dynamic virtual IP address (DVIPA) connection counts.

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Origin Node The parent node of the workspace.

Total Active DVIPA Connections The total number of active DVIPA connections.

Active Session Count Attributes

Use these attributes to view active session counts.

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Origin Node The parent node of the workspace.

Total Active Sessions The total number of active sessions.

Active TCPIP Connection Count Attributes

Use these attributes to view active TCP/IP connection counts.

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Origin Node The parent node of the workspace.

Total Active Connections The total number of active connections.

DB2 Replication Apply Server Attributes

Use these attributes to view detailed server data for the DB2 apply replication server.

Note: This attribute group is used with the GDPS Active/Active Continuous Availability solution.

Active Subscriptions The total count of active subscriptions across all active queues.

Apply Image Name The image name of the apply server.

Apply Server Name The job name of the apply server.

Apply Server Status The status of the NetView connection to the apply server. The following values are valid:
- ACTIVE
- INACTIVE

Apply Site Name The name of the apply site.

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

DB2 Apply Server The DB2 subsystem or the DB2 group attach name.

Origin Node The parent node of the workspace.

Start Time A time stamp that represents when the Q Apply task was started.

DB2 Replication Apply Workload Attributes

Use these attributes to view detailed workload data for the DB2 apply replication server.

Note: This attribute group is used with the GDPS Active/Active Continuous Availability solution.

Agents The number of Q Apply agents.

Apply Image Name The image name of the apply server.

Apply Server Name The job name of the apply server.

Apply Site Name The name of the apply site.

Apply Sleep Time The number of milliseconds that Q Apply agents for this receive queue were idle while waiting for work.

Apply Workload State The state of the workload as determined by the apply server. The following values are valid:
- INACTIVE

- REPLICATE CONTINUOUS

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Current Memory The amount of memory in bytes that the Q Apply browser thread used for reading transactions from this queue.

DB2 Apply Server The DB2 subsystem or the DB2 group attach name.

Deadlock Retries The number of times that the Q Apply program reapplied row changes because of lock timeouts and deadlocks.

Heartbeat Latency The average elapsed milliseconds between the time that heartbeat messages were sent by the Q Capture program and the time that they were received by the Q Apply program.

Job Dependencies The number of transactions that are delayed because of job name dependencies.

Key Dependencies The total number of replication key constraints that were detected, forcing transactions to be serialized.

Memory Full Time The number of seconds that the Q Apply program was unable to build transactions from this receive queue because its agents were using all the available memory to apply transactions.

Monster Transactions The number of transactions that exceeded the memory limit for the receive queue that was set in the IBMDB2_RECVQUEUES table.

MQ Bytes Read The number of bytes that were read from this receive queue.

OKSQLSTATE Errors The number of row changes that caused an SQL error that is defined as acceptable in the OKSQLSTATES field of the IBMQREP_TARGETS table. The Q Apply program ignores these errors.

Oldest Commit LSN The commit log sequence number (LSN) from the source recovery log that corresponds to the oldest transaction that was applied.

Oldest Commit Sequence An internal log marker that corresponds to the oldest transaction that was applied.

Oldest In-flight Transactions A time stamp that represents the source commit time of the oldest currently in-flight transaction. An in-flight transaction has not been fully applied and committed at the target.

Origin Node The parent node of the workspace.

Queue Depth The number of messages on the queue.

Queue Percent Full The fullness of the queue as a percentage.

Queue Start Time The time stamp at the Q Apply server when the receive queue was started.

Receive Queue Name The name of the receive queue.

RI Dependencies The total number of referential integrity (RI) conflicts that were detected, forcing transactions to be serialized.

RI Retries The number of times that the Q Apply program had to reapply row changes because of referential integrity (RI) conflicts when the transactions that they were part of were executed in parallel.

Rows Applied The number of insert, update, and delete operations from this receive queue that the Q Apply program applied to the target.

Rows Not Applied The number of rows that were unable to be applied and were entered in the IBMDB2_EXCEPTIONS table.

Rows Processed The number of rows that were applied but might not yet be committed to the target.

Rows Read The number of rows that were read from this receive queue.

Spilled Rows The number of rows that the Q Apply program sent to temporary spill queues while targets were being loaded or while Q subscriptions were placed into a spill state by the spillsub parameter of the MODIFY or asnqacmd command.

Spilled Rows Applied The number of spilled rows that were applied to the target.

Transactions Applied The number of transactions from this receive queue that the Q Apply program committed to the target.

Transactions Read The number of transactions that were read from this receive queue.

Transactions Serialized The number of transactions that conflicted with another transaction, because of either a row conflict or a referential integrity conflict. In these cases, the Q Apply program suspends parallel processing and applies the row changes within the transaction in the order that they were committed at the source.

Unique Dependencies The total number of unique index constraints that were detected, forcing transactions to be serialized.

Unique Retries The number of times that the Q Apply program tried to reapply rows that were not applied in parallel because of unique index constraints.

Workload Name The name of the workload.

DB2 Replication Capture Server Attributes

Use these attributes to view detailed server data for the DB2 capture replication server.

Note: This attribute group is used with the GDPS Active/Active Continuous Availability solution.

Capture Image Name The image name of the capture server.

Capture Server Name The job name of the capture server.

Capture Server Status The status of the NetView connection to the capture server. The following values are valid:
- ACTIVE
- INACTIVE

Capture Site Name The name of the capture site.

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Current Log Sequence The most recent logical log sequence number in the recovery log that the Q Capture program read.

Current Log Time The time stamp at the Q Capture server of the latest database commit that was seen by the Q Capture log reader.

DB2 Capture Server The DB2 subsystem or the DB2 group attach name.

End of Log Time The time stamp at the Q Capture control server when the Q Capture program reached the end of the log.

End of Logs The number of times that the Q Capture program reached the end of the log.

Log Read API Time The number of milliseconds that the Q Capture program spent using the DB2 log read application program interface (API) to retrieve log records.

Log Read Calls The number of log read API calls that the Q Capture program made.

Log Reader Sleep Time The number of seconds that the Q Capture log reader thread slept because there were no changes to capture or because the Q Capture program is operating at its memory limit.

Maximum Transaction Size The largest transaction, in bytes, that the Q Capture program processed.

Origin Node The parent node of the workspace.

Restart Log Sequence The logical log sequence number in the recovery log at which the Q Capture program starts during a warm restart. This value represents the earliest log sequence number that the Q Capture program found for which a commit or abort record has not yet been found.

Rows Processed The number of rows (individual insert, update, or delete operations) that the Q Capture program read from the log.

Transaction Memory Used The memory that the Q Capture program used to construct transactions from the log.

Transactions Processed The number of transactions that the Q Capture program processed.

Transactions Skipped The number of transactions (containing changed rows) that were not put on queues because the changes were to columns that are not part of a Q subscription or publication, for example, the ALL_CHANGED_ROWS parameter in the IBMDB2_SUBS table was set to No.

Transactions Spilled The number of transactions that the Q Capture program spilled to a file after exceeding the MEMORY_LIMIT threshold.

DB2 Replication Capture Workload Attributes

Use these attributes to view detailed workload data for the DB2 capture replication server.

Note: This attribute group is used with the GDPS Active/Active Continuous Availability solution.

Capture Image Name The image name of the capture server.

Capture Server Name The job name of the capture server.

Capture Site Name The name of the capture site.

Capture Workload State The state of the workload as determined by the capture server. The following values are valid:
- INACTIVE
- REPLICATE CONTINUOUS

Changed Rows Skipped The number of changed rows that were not put on this send queue because the changes were to columns that are not part of a Q subscription or publication. The ALL_CHANGED_ROWS parameter in the IBMDB2_SUBS table was set to the default value of No.

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM/DD/YY hh:mm:ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Current Log Sequence The most recent logical log sequence number in the recovery log that the Q Capture program read for this send queue. The Q Capture program updates this column if the send queue is active.

DB2 Capture Server The DB2 subsystem or the DB2 group attach name.

Delete Row Operations Suppressed The number of delete row operations that were not put on this send queue because the Q subscription or publication was created with the option to suppress replication of delete operations.

MQ Bytes Sent The number of bytes that were put on the send queue during the collection interval, including data from the source table and the message header.

MQ Messages Sent The number of messages that were put on the send queue during the collection interval.

Origin Node The parent node of the workspace.

Queue Full Error Count The number of times that the Q Capture program retried putting messages (MQPUT) on this send queue.

Restart Log Sequence The logical log sequence number from which the Q Capture program starts putting messages on this send queue during a warm restart. This value represents the earliest log sequence number that the Q Capture program found that did not have a commit or abort record. The Q Capture program updates this column if the send queue is active.

Rows Published The number of rows (individual insert, update, or delete operations) that the Q Capture program put on this send queue.

Rows Skipped The number of rows that the Q Capture program did not transmit to this send queue because they did not meet the search condition that is defined in the Q subscription or publication.

Send Queue Name The name of the send queue.

Transactions Published The number of transactions that the Q Capture program put on this send queue.

Workload Name The name of the workload.

Distributed DVIPA Connection Routing Attributes

Use these attributes to view information about distributed DVIPA connection routing.

Configured Timed Affinity The affinity value that is defined in the TIMEDAFFINITY parameter on the VIPADISTRIBUTE TCP/IP profile statement. The TIMEDAFFINITY parameter indicates to the sysplex distributor that connections to a particular distributed DVIPA from the same client, as identified by the IP address, need to be routed to the same server instance, even when multiple server instances are on a single target stack.

Destination IP Address The destination IP address for this connection.

Destination Port The destination port for this connection.

Destination Port String The destination port for this connection, formatted as a string.

Destination XCF IP Address The dynamic XCF IP address of the stack that is processing this connection.

Established Connections The number of currently established connections associated with the Configured Time Affinity attribute.

Gateway IP Address The gateway that is used to send packets to the target stack. If the value is equal to 0.0.0.0 for an IPv4 entry or :: for an IPv6 entry, the destination can be reached without going through a gateway.

Interface Name The name of the interface for the route being used to distribute packets to the target stack.

Origin Node The parent node of the workspace.

Source IP Address The source IP address for this connection.

Source IP Address Source Port For NetView product internal use. This attribute is the concatenation of the Source IP Address and Source Port attribute values, which is used to depict the x-axis in the bar chart view. The format of the concatenated values is *ip*:*port*, where *ip* is the Source IP Address value and *port* is the Source Port value.

Source Port The source port for this connection.

Source Port String The source port for this connection, formatted as a string.

System ID The SMF system ID.

Timed Affinity Time Left The number of seconds left before the affinity between the client IP address and the dynamic VIPA destination IP address and port is removed. After the last established connection is closed, the affinity remains for the number of seconds that is indicated in the Configuration Timed Affinity attribute.

Update Time The date and time that the data was last updated.

VIPA Route Flag An indication of whether the VIPAROUTE parameter is being used to route packets to the target stack for this connection. The value is a 1-byte hexadecimal number where bit 0 is the leftmost bit and the bits have the following values:

- Bit 0 (Yes): Indicates that the best available route, based on the VIPAROUTE parameters, is being used to distribute packets to the target stack.
- Bit 1 (No): Indicates that the dynamic XCF interface is being used to distribute packets to the target stack.
- Bit 2 (Unavailable): Indicates that the TCP/IP stack attempted to use the route based on the VIPAROUTE parameters but, because an error was detected during VIPAROUTE statement validation, the dynamic XCF interface is being used to distribute packets to the target stack.
- Bits 4 - 7: Reserved.

Distributed DVIPA Server Health Attributes

Use these attributes to view health statistics for all application servers that reside on distributed dynamic virtual IP address (DVIPA) targets.

Abnormal Transaction Percent The percent of abnormal transaction completions for the server application on the target port or the average of the individual values for all the server applications sharing the port.

Application Server Name The job name of the application server.

Connection Establishment Rate A measure of the percentage of the connection setup requests received at the target that achieve completion with the client, that is, arrive at the connection established state. It is displayed as a percentage.

DESTIP Weight The weight that is used by the distributor, when the distribution method for incoming connection requests is weightedActive, to determine the proportion of active connections on this target.

DVIPA The dynamic virtual IP address.

DVIPA DVIPA Port For NetView product internal use. This attribute is the concatenation of the DVIPA and DVIPA Port attribute values. The format of the concatenated values is *dvipa*:*dvipa_port*, where *dvipa* is the DVIPA value and *dvipa_port* is the DVIPA Port value.

DVIPA Port The DVIPA port.

DVIPA Port String The DVIPA port, formatted as a string.

Dynamic XCF IP Address The dynamic XCF IP address of the target TCP/IP stack.

Origin Node The parent node of the workspace.

Port Health Percent The health indicator of the server application on the target port. If several server applications share the port, this is the average of the individual values for all the server applications sharing the port. A value of less than 100 percent indicates that one or more of the servers has problems.

Proportional CP Weight An indication of the general CP utilization proportion.

- When the distribution method is BASEWLM, the value is the raw value modified by the expected general CP utilization proportion that is configured on the VIPADISTRIBUTE PROCTYPE statement for this application.
- When the distribution method is SERVERWLM, the value is the raw value modified by the proportion of general CP capacity that is currently being consumed by the workload of this application as compared to the other processors (zAAP and zIIP).

Proportional zAAP Weight An indication of the zAAP utilization proportion.

- When the distribution method is BASEWLM, the value is the raw value modified by the expected zAAP utilization proportion that is configured on the VIPADISTRIBUTE PROCTYPE statement for this application.
- When the distribution method is SERVERWLM, the value is the raw value modified by the proportion of zAAP capacity that is currently being consumed by the workload of this application as compared to the other processors (general CPU and zIIP).

Proportional zIIP Weight An indication of the zIIP utilization proportion.

- When the distribution method is BASEWLM, the value is the raw value modified by the expected zIIP utilization proportion that is configured on the VIPADISTRIBUTE PROCTYPE statement for this application.
- When the distribution method is SERVERWLM, the value is the raw value modified by the proportion of zIIP capacity that is currently being consumed by the workload of this application as compared to the other processors (general CPU and zAAP).

Raw Composite Weight The raw composite weight for this server. The composite weight is based on the general CPU, zAAP, and zIIP processor utilization of the application.

Raw CP Weight An indication of the WLM general CP weight recommendation.

- When the distribution method is BASEWLM, the value is the WLM system general CP weight recommendation, which is based on the amount of displaceable general CPU capacity on this system as compared to the other target systems.
- When the distribution method is SERVERWLM, the value is the WLM server-specific general CP recommendation, which is the amount of displaceable general CPU capacity based on the importance of the application workload (as defined by the WLM policy) as compared to the other target systems.

Raw zAAP Weight An indication of the WLM zAAP weight recommendation.

- When the distribution method is BASEWLM, the value is the WLM system zAAP weight recommendation, which is based on the amount of displaceable zAAP capacity on this system as compared to the other target systems.
- When the distribution method is SERVERWLM, the value is the WLM server-specific zAAP recommendation, which is the amount of displaceable zAAP capacity based on the importance of the application workload (as defined by the WLM policy) as compared to the other target systems.

Raw zIIP Weight An indication of the WLM zIIP weight recommendation.

- When the distribution method is BASEWLM, the value is the WLM system zIIP weight recommendation, which is based on the amount of displaceable zIIP capacity on this system as compared to the other target systems.
- When the distribution method is SERVERWLM, the value is the WLM server-specific zIIP recommendation, which is the amount of displaceable zIIP capacity based on the importance of the application workload (as defined by the WLM policy) as compared to the other target systems.

Server Accept Efficiency Fraction A measure, calculated at intervals of approximately one minute, that indicates the efficiency of the server application in accepting new connection requests and managing the backlog queue. This value is displayed as a percentage.

Sysplex Name The name of the sysplex.

System ID The SMF system ID.

Target Connectivity Success Rate A measure of the percentage of connection setup requests routed from the distributor that are successfully received by the target for this server. It is displayed as a percentage.

Target Server Responsiveness Rate The responsiveness value for the target server. The sysplex distributor monitors the ability of a target server to process new connections. At each interval of approximately one minute, the sysplex distributor generates a target server responsiveness fraction percentage to indicate how well the server is accepting new TCP connection setup requests. This value is not a measure of how well the server is servicing the connections.

TCPIP Job Name The TCP/IP job name.

Update Time The date and time that the data was last updated. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

WLM Weight The Workload Manager (WLM) weight value for either the z/OS images on which the target TCP/IP stack is located or the specific server on the target stack.

zOS Image Name The name of the z/OS operating system on which the target stack resides.

Distributed DVIPA Targets Attributes

Use these attributes to view information about the distributed dynamic virtual IP address (DVIPA) targets.

Active Connections The current number of active connections for the DVIPA and port that were distributed to the target stack.

Address Space ID The MVS address space ID of the address space that opened the socket. This is a 4-digit hexadecimal number.

Application Server Name The job name of the application server.

Delta Connections The number of connections for the DVIPA and port that were distributed to the target stack during the most recent time interval.

Distribution Port Function An indication of certain attributes of the distribution function for the DVIPA and port. This is a 1-byte hexadecimal number, where the bits have the following values and bit 0 is the leftmost bit.

- Bit 0 (distBaseWlm): Corresponds to the DISTMETHOD BASEWLM parameter on the VIPADISTRIBUTE TCP/IP profile statement.
- Bit 1 (distRoundRobin): Corresponds to the DISTMETHOD ROUNDROBIN parameter on the VIPADISTRIBUTE TCP/IP profile statement.
- Bit 2 (targetpathInactive): Indicates that the distributor cannot send data packets to the target stack because no path to the target stack exists.
- Bit 3 (distServerWlm): Corresponds to the DISTMETHOD SERVERWLM parameter on the VIPADISTRIBUTE TCP/IP profile statement.
- Bit 4 (local): Indicates that the local target stack is used for outbound connections unless the local target stack cannot process the connection.
- Bit 5 (distWeightedActive): Corresponds to the DISTMETHOD WEIGHTEDACTIVE parameter on the VIPADISTRIBUTE TCP/IP profile statement.
- Bit 6 (distTargetControlled): Corresponds to the DISTMETHOD TARGCONTROLLED parameter on the VIPADISTRIBUTE TCP/IP profile statement. This distribution method can be used only with tier 1 targets, such as DataPower® appliances, that are not z/OS tier 1 targets and is available with z/OS V1R11 Communications Server or later.

For example, the hexadecimal value X'A0', which is the same as the binary value B'10100000', indicates that the 0 (distBaseWlm) and 2 (targetpathInactive) bits are set.

DVIPA The dynamic virtual IP address.

DVIPA Port The DVIPA port.

DVIPA Port String The DVIPA port, formatted as a string.

DVIPA DVIPA Port For NetView product internal use. This attribute is the concatenation of the DVIPA and DVIPA Port attribute values, which is used to depict the x-axis in the bar chart view. The format of the concatenated values is *dvipa*:*dvipa_port*, where *dvipa* is the DVIPA value and *dvipa_port* is the DVIPA Port value.

Dynamic XCF IP Address The dynamic XCF IP address of the target TCP/IP stack.

Dynamically Added Port An indication of whether the target port was dynamically added to distribution or explicitly specified. The following values are valid:

- Yes: The port was dynamically added.
- No: The port was explicitly specified.

Hot Standby Rank When the distribution method is HOTSTANDBY, an indication of the backup target that is selected if the preferred target becomes unavailable. The backup target with the highest rank is used. Valid values are in the range 1–254; the default value is 1. This data is available with z/OS V1R12 Communications Server or later.

Hot Standby Server Status The server status when the distribution method is HOTSTANDBY. This data is available with z/OS V1R12 Communications Server or later. The following values are valid:

- Backup (0): Specifies that this is currently a backup (hot-standby) server.
- Active (1): Specifies that this is currently the active server.

Hot Standby Server Type The server type when the distribution method is HOTSTANDBY. This data is available with z/OS V1R12 Communications Server or later. The following values are valid:

- Backup (2): Specifies that this server is a backup target. A backup target is initially a hot-standby target. Connections are not distributed to hot-standby targets. If the active target becomes unavailable, the distributor switches targets and one of the hot-standby targets becomes the active target.
- Preferred (1): Specifies that this server is the preferred target. If AUTOSWITCHBACK is configured, the preferred target is the active target if it is available and has had no health problems. If the active target becomes unavailable, the distributor switches to a hot-standby target, the active target becomes a hot-standby target, and the selected hot-standby target becomes the active target.

Listening Servers The number of servers at the port on the target system that are ready to service connection requests.

Origin Node The parent node of the workspace.

Sysplex Name The name of the sysplex.

System ID The SMF system ID.

TCPIP Host Name The short TCP/IP host name of the target stack.

TCPIP Job Name The TCP/IP job name of the target stack.

Total Connections The number of connections for the DVIPA and port that were distributed to the target stack.

Update Time The date and time that the data was last updated. By default, this value is displayed as *MM/DD/YY hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

XCF Group Name The XCF name that is used by this TCP/IP stack when joining the sysplex.

zOS Image Name The name of the z/OS operating system on which the target stack resides.

DVIPA Connections Attributes

Use these attributes to view the dynamic virtual IP address (DVIPA) connections.

Address Space ID The MVS address space ID of the address space that opened the socket. This is a 4-digit hexadecimal number.

AT-TLS Cipher The negotiated cipher that is used by the secure connection. This value, which is shown as a hexadecimal code, applies only if AT-TLS Connection Status has a value of Secure.

AT-TLS Connection Status The current application transparent transport layer security (AT-TLS) policy status for the connection. The following values are valid:

- Not_Secure (1): The SSL handshake has not completed successfully. A connection can have this status for several reasons, and AT-TLS Policy Status should be examined. If AT-TLS Policy Status is No_TTLS, No_Policy, or Not_Enabled, the handshake does not occur. If AT-TLS Policy Status is Enabled, Appl_Cntl, or Not_Known, the SSL handshake might occur.
- In_Progress (2): The SSL handshake for the connection is in progress.
- Secure (3): The connection is secure. The SSL handshake completed successfully.

AT-TLS Partner Userid The user ID that is associated with the certificate of the partner. This value is applicable only if AT-TLS Connection Status has a value of Secure and a user ID is associated with the certificate of the partner.

AT-TLS Policy Status The AT-TLS status for the connection. The following values are valid:

- Not_Known (0): The TCP/IP stack has not examined the AT-TLS configuration for the connection because the connection has not progressed to a state where the stack is ready to process this information.
- No_TTLS (1): NOTTLS was specified or was the default in the TCP/IP configuration profile when the AT-TLS configuration was examined for the connection. AT-TLS processing is not performed for the connection.
- No_Policy (2): No AT-TLS policy is defined for the connection. AT-TLS processing is not performed for the connection.
- Not_Enabled (3): An AT-TLS policy is configured for this connection, but the TTLSEnabled parameter is set to OFF. AT-TLS processing is not performed for this connection.
- Enabled (4): An AT-TLS policy is configured for this connection, and the TTLSEnabled parameter is set to ON. AT-TLS processing is performed for this connection.

- Appl_Cntrl (5): An AT-TLS policy is configured for the connection, and the ApplicationControlled parameter is set to ON. The application that owns the connection is to tell the TCP/IP stack when to perform the secure handshake.

AT-TLS Security Type The type of system SSL secure session defined in the AT-TLS policy that is used by the connection. The following values are valid:

- N/A (0): Not applicable because AT-TLS Policy Status has a value other than Enabled or Appl Cntrl.
- Client (1): The SSL handshake is performed as a client.
- Server (2): The SSL handshake is performed as a server.
- SRVCAPASS (3): The SSL handshake is performed as a server requiring client authentication, but the client certificate validation is bypassed.
- SRVCAFULL (4): The SSL handshake is performed as a server requiring client authentication, and, if the client presents a certificate, client certificate validation is performed.
- SRVCAREQD (5): The SSL handshake is performed as a server requiring client authentication, and the client must present a certificate so that client certificate validation can be performed.
- SRVCASAFCHK (6): The SSL handshake is performed as a server requiring client authentication; the client must present a certificate so that client certificate validation can be performed, and the client certificate must have an associated user ID defined to the security product.

AT-TLS SSL Protocol The negotiated SSL protocol in use by the connection. The following values are valid:

- SSL_V2: SSL Version 2
- SSL_V3: SSL Version 3
- TLS_V1: TLS Version 1
- N/A: Not applicable

Byte Rate The number of bytes that were sent or received per minute during the most recent time interval.

Bytes Received The number of bytes that were received during the most recent time interval.

Bytes Received String The number of bytes that were received during the most recent time interval, formatted as a string.

Bytes Sent The number of bytes that were sent during the most recent time interval.

Bytes Sent or Received The number of bytes that were sent or received during the most recent time interval.

Bytes Sent or Received String The number of bytes that were sent or received during the most recent time interval, formatted as a string.

Bytes Sent String The number of bytes that were sent during the most recent time interval, formatted as a string.

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Connection ID The hexadecimal representation of the connection number.

Connection Start Time The date and time that the connection started. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Connection State The state of the connection. The following values are valid:

- CLOSED (1): The connection has ended and no longer exists.
- LISTENING (2): The connection is waiting for a connection request from any remote TCP and port.
- SYN_SENT (3): The connection is waiting for a matching connection request after sending a connection request. If a connection is in this state for two successive sample intervals, an exception is generated.
- SYN_RECEIVED (4): The connection is waiting for a confirming connection request acknowledgment after receiving and sending a connection request.
- ESTABLISHED (5): The connection is established.
- FIN_WAIT_1 (6): The connection is waiting for a connection stop request from the remote TCP or an acknowledgment of the connection stop request.
- FIN_WAIT_2 (7): The connection is waiting for a connection stop request from the remote TCP.
- CLOSE_WAIT (8): The connection is waiting for a connection stop request from the local port.
- LAST_ACK (9): The connection is waiting for an acknowledgment of the connection stop request that it sent to the remote TCP.
- CLOSING (10): The connection is waiting for a connection stop request acknowledgment from the remote TCP.
- TIME_WAIT (11): The host is waiting to ensure that a remote TCP has received a connection stop request. When the wait time is over, the socket pair that defines the connection is available for reuse.
- DELETE_TCB (12): The TCP connection has closed, and the resources that represent the connection are waiting to be cleaned up.

Current Send Window Size The current size of the send window.

DDVIPA For NetView product internal use. This attribute indicates a distributed DVIPA if the value is 1.

DVIPA The dynamic virtual IP address.

DVIPA Port The DVIPA port.

DVIPA Port String The DVIPA port, formatted as a string.

Interface Name The name of the interface.

Last Activity Remote Timestamp The most recent time stamp value, in milliseconds, that is received from the remote side of the connection. If the TCP time stamp header option is not used, the value of this field is zero. If the TCP time stamp header option is used, this field contains bits 10 - 41 of a related time stamp that is provided by z/OS Communications Server. The related time stamp is in store clock (STCK) format, which approximately indicates units of seconds. To convert this field into a STCK value and then into a date and time, follow these steps:

1. Determine the current STCK value by using the following NetView command:
   ```
   PIPE EDIT IFRAUGMT C2X|CONS
   ```
2. Prefix bits 0 - 9 of the current STCK value to the field; if that conversion yields a time in the future, then subtract 1 from bits 0 - 9 of the current STCK value and prefix that value to the field instead.
3. To convert the resulting STCK value (the field with the prefix added) to a date and time, run the following NetView command:
   ```
   PIPE EDIT 'resulting_STCK_value'X ZDT 1|CONS
   ```

Last Activity Timestamp The date and time of the last activity on this connection. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Last Timestamp Age The time, in milliseconds, when the most recent time stamp from the partner was updated. If the TCP time stamp header option is not used, the value of this field is zero. If the TCP time stamp header option is used, this field contains bits 10 - 41 of a related time stamp that is provided by z/OS Communications Server. The related time stamp is in store clock (STCK) format, which approximately indicates units of seconds. To convert this field into a STCK value and then into a date and time, follow these steps:

1. Determine the current STCK value by using the following NetView command:
   ```
   PIPE EDIT IFRAUGMT C2X|CONS
   ```
2. Prefix bits 0 - 9 of the current STCK value to the field; if that conversion yields a time in the future, then subtract 1 from bits 0 - 9 of the current STCK value and prefix that value to the field instead.
3. To convert the resulting STCK value (the field with the prefix added) to a date and time, run the following NetView command:
   ```
   PIPE EDIT 'resulting_STCK_value'X ZDT 1|CONS
   ```

LU Name For connections for TN3270 sessions, the SNA logical unit (LU) name.

Max Send Window Size The maximum size of the send window.

Number of Duplicate ACKS The number of duplicate acknowledgements that are received by this connection.

Origin Node The parent node of the workspace.

Passive or Active Open The type of open that is performed. The following values are valid:
- 0: Passive open; the remote end initiated the connection.
- 1: Active open; the local end initiated the connection.

Percent Segments Retransmitted The percent of TCP segments that were retransmitted over this connection since the connection started.

Remote IP Address The remote IP address for the connection.

Remote Port The port associated with the remote IP address that initiated the connection.

Remote Port String The port associated with the remote IP address that initiated the connection, formatted as a string.

Resource Name The text identification for the resource. It represents the user who opened the socket.

Segments Received The number of segments that were received over this connection during the most recent time interval.

Segments Retransmitted The number of segments that were retransmitted over this connection during the most recent time interval.

Segments Sent The number of segments that were sent over this connection during the most recent time interval.

Segments Sent or Received The number of segments that were sent or received over this connection during the most recent time interval.

SNA Application Name For connections for TN3270 sessions, the SNA application name.

Sysplex Name The name of the sysplex.

System ID The SMF system ID.

TCB Address The address of the TCB in the address space that opened the socket.

TCPIP Host Name The short TCP/IP host name that was discovered for the TCP/IP job.

TCPIP Job Name The TCP/IP job name for which a connection endpoint is found.

Telnet Logmode The VTAM logmode if the TCP connection is for a TN3270 or TN3270E session.

Telnet Protocol The Telnet mode. Valid values are TN3270, TN3270E, LINEMODE, and N/A.

Telnet User Client Name The user ID of the client if the TCP connection is for a TN3270 or TN3270E session.

Total Bytes The sum of the bytes that were sent and bytes that were received over the connection since the connected started.

Total Bytes Received The number of bytes that were received over the connection since the connection started.

Total Bytes Received String The number of bytes that were received over the connection since the connection started, formatted as a string.

Total Bytes Sent The number of bytes that were sent over the connection since the connection started.

Total Bytes Sent String The number of bytes that were sent over the connection since the connection started, formatted as a string.

Total Bytes String The sum of the bytes that were sent and bytes that were received over the connection since the connected started, formatted as a string.

Total Segments The total number of segments that were sent and received for this connection since the connection started.

Total Segments Received The total number of segments that were received from IP for this connection since the connection started.

Total Segments Retransmitted The total number of segments that were retransmitted over this connection since the connection started.

Total Segments Sent The total number of segments that were sent to IP for this connection since the connection started.

zOS Image Name The name of the z/OS operating system for which DVIPA connection information is requested.

zOS Release Level The release level of the z/OS operating system.

DVIPA Definition and Status Attributes

Use these attributes to view the status of the dynamic virtual IP addresses (DVIPAs).

Application Server Name The job name of the application server. This attribute contains a value only for application-instance DVIPA.

Distributor Status The status of the DVIPA on the given TCP/IP stack in relation to the sysplex distributor function. The following values are valid:

- none (1): The DVIPA is not participating in a sysplex distributor function.
- distributor (2): The stack is a sysplex distributor for the DVIPA.
- target (3): The stack is a target stack for the DVIPA.
- distributorAndTarget (4): The stack is both a sysplex distributor and a target stack for the DVIPA.

DVIPA The dynamic virtual IP address.

Interface Name The name of the IPv4 or IPv6 interface associated with the IP address.

LPAR Name The name of the LPAR.

Mobility An indication of how a DVIPA can be moved to another TCP/IP stack. The following values are valid:

- none (1): Moveable status does not apply to the DVIPA. This value is used for entries where backup is specified for the Origin and Status fields.
- immediate (2): This DVIPA can be moved to another stack as soon as the other stack requests ownership.
- whenIdle (3): This DVIPA can be moved to another stack when it has no connections on the current stack.
- nonDisruptive (4): This DVIPA can be moved to another stack as soon as the other stack requests ownership. Existing connections are maintained by the new stack until they are closed, and new connection requests are directed to the new stack.
- disruptive (5): This DVIPA cannot be moved nondisruptively if it is within the defined range on the stack. This value is not supported for IPv6.

Origin An indication of how the DVIPA was configured to the TCP/IP stack. The following values are valid:

- unknown (1): An error occurred.
- backup (2): The VIPADYNAMIC VIPABACKUP TCP/IP profile statement was used to configure the given TCP/IP stack as a backup for the DVIPA.
- define (3): The VIPADYNAMIC VIPADEFINE TCP/IP profile statement was used to configure the given TCP/IP stack as the owner of the DVIPA.
- rangeBind (4): The DVIPA was dynamically defined when an application issued a BIND function call.
- rangeIoctl (5): The DVIPA was dynamically defined when an application issued the SIOCSVIPA IOCTL function call.
- target (6): The DVIPA was dynamically defined on the stack because this stack is a target stack for the sysplex distributor function.

Origin Node The parent node of the workspace.

Rank The rank of this stack in the chain of backup stacks for a given DVIPA. For entries that do not have an Origin value of backup or define, this value does not apply and is set to N/A.

Reporting NetView Domain The NetView domain that reported the DVIPA.

Service Manager An indication of whether the DVIPA is participating in the Service Manager function on the given TCP/IP stack. The following values are valid:

- Yes: The DVIPA is participating in the Service Manager function.
- No: The DVIPA is not participating in the Service Manager function.

Status The status of the DVIPA on the given TCP/IP stack. The following values are valid:

- unknown (1): An error occurred.
- active (2): The DVIPA is active.
- backup (3): The given TCP/IP stack is currently a backup owner for the DVIPA.
- moving (4): The DVIPA was active for the TCP/IP stack but the ownership transferred to another TCP/IP stack (for example, because of a takeover).
- quiescing (5): The DVIPA is no longer a target but still has connections. When all existing connections are closed, the status changes to deactivated.
- deactivated (6): The VARY,,TCPIP,SYSPLEX,DEACTIVATE command was run for this DVIPA. The DVIPA remains deactivated until a VARY,,TCPIP,SYSPLEX,REACTIVATE command is run for this DVIPA.
- deactLeavegroup (7): The VARY,,TCPIP,SYSPLEX,DEACTIVATE command was run for this DVIPA, and the VARY,,TCPIP,SYSPLEX,LEAVEGROUP command was run for this stack. If the stack rejoins the sysplex group before a VARY,,TCPIP,SYSPLEX,REACTIVATE command is run for this DVIPA, this DVIPA remains deactivated and the DVIPA status changes to deactivated.
- deactAutonomics (8): The VARY,,TCPIP,SYSPLEX,DEACTIVATE command was run for this DVIPA and the stack left the sysplex group because of an error condition detected by the sysplex autonomics function. If the stack rejoins the sysplex group before a VARY,,TCPIP,SYSPLEX,REACTIVATE command is run for this DVIPA, this DVIPA remains deactivated and the DVIPA status changes to deactivated.

- inactLeavegroup (9): The VARY,,TCPIP,SYSPLEX,LEAVEGROUP command was run for this stack, and the DVIPA is currently inactive. The DVIPA is reactivated if a VARY,,TCPIP,SYSPLEX,JOINGROUP command is run for this stack.
- inactAutonomics (10): The stack left the sysplex group because of an error condition detected by the sysplex autonomics function.

Sysplex Name The name of the sysplex.

System ID The SMF system ID.

TCPIP Host Name The short TCP/IP host name.

TCPIP Job Name The TCP/IP job name.

Time Activated The date and time that the DVIPA was activated. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Update Time The date and time that the data was last updated. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

XCF Group Name The XCF name used by this TCP/IP stack when joining the sysplex. If the stack has not joined the sysplex group, this value is a zero-length string.

zOS Image Name The name of the z/OS operating system.

DVIPA Sysplex Distributors Attributes

Use these attributes to view information about the distributed dynamic virtual IP address (DVIPA) sysplex distributors.

Active Target Stacks The number of target TCP/IP stacks that are available to service connection requests.

Auto Switch Back An indication of whether the AUTOSWITCHBACK or NOAUTOSWITCHBACK option for the HOTSTANDBY distribution method is specified on the VIPADISTRIBUTE statement. This indication is available with z/OS V1R12 Communications Server or later. The following values are valid:

- No (0): Specifies that the distributor does not switch back to the preferred target when it becomes available.
- Yes (1): Specifies that the distributor automatically switches distribution back to the preferred target when the preferred target becomes available.

Configured Target Stacks The number of configured target TCP/IP stacks. For distributors with DESTIP=ALL defined, this value does not apply and is set to N/A.

DESTIP ALL An indication of whether the DESTIP ALL parameter is specified on the VIPADISTRIBUTE statement. The following values are valid:

- 0: No
- 1: Yes

Distribution Method The method of distribution used for incoming connection requests. The following values are valid:

- baseWlm (1): Workload Manager (WLM) and policy information are used to determine the distribution.
- roundRobin (2): WLM and policy information are ignored and requests are distributed in a round-robin fashion among the existing server instances.
- serverWlm (3): Server-specific WLM and policy information is used to determine distribution.
- weightedActive (4): WLM and policy information are not used to determine how to route future incoming connection requests for this distributed DVIPA. Instead, distribution of incoming TCP connection requests is balanced across the targets such that the number of active connections on each target is proportionally equivalent to a configured active connection weight for each target (specified on the DESTIP parameter of each target).
- targetControlled (5): Incoming connection requests are distributed using weights provided by the Tier 1 targets. This distribution method can be used only with tier 1 targets, such as DataPower appliances, that are not z/OS tier 1 targets.
- hotStandby(6): One preferred target and at least one hot-standby target are configured. This distribution method is available with z/OS V1R12 Communications Server or later.

DVIPA The dynamic virtual IP address.

DVIPA Port The DVIPA port.

DVIPA Port String The DVIPA port, formatted as a string.

Dynamic XCF IP Address The dynamic XCF IP address of the target TCP/IP stack.

Health Switch An indication of whether the HEALTHSWITCH or NOHEALTHSWITCH option for the HOTSTANDBY distribution method is specified on the VIPADISTRIBUTE statement. This indication is available with z/OS V1R12 Communications Server or later. The following values are valid:

- No (0): Specifies that the distributor ignores health metrics and switches from the active target only if the target is not ready or if the distributor does not have an active route to the target.
- Yes (1): Specifies that the distributor automatically switches from the active target if the target is not healthy.

ILWEIGHTING When the value of the Distribution Method attribute is serverWlm, an indication of the weighting factor that WLM uses when comparing displaceable capacity at different importance levels (ILs) as it determines a SERVERWLM recommendation for each system.

Interface Name The name of the IPv4 or IPv6 interface associated with the IP address.

Listening Servers The number of servers across all the target stacks that are ready to service connection requests.

LPAR Name The name of the LPAR.

Mobility An indication of how a DVIPA can be moved to another TCP/IP stack. The following values are valid:

- none (1): Moveable status does not apply to the DVIPA. This value is used for entries where backup is specified for the Origin and Status fields.
- immediate (2): This DVIPA can be moved to another stack as soon as the other stack requests ownership.
- whenIdle (3): This DVIPA can be moved to another stack when it has no connections on the current stack.
- nonDisruptive (4): This DVIPA can be moved to another stack as soon as the other stack requests ownership. Existing connections are maintained by the new stack until they are closed, and new connection requests are directed to the new stack.
- disruptive (5): This DVIPA cannot be moved nondisruptively if it is within the defined range on the stack. This value is not supported for IPv6.

Opt Local An indication of whether TCP/IP target stacks should bypass sending connection requests for the DVIPA to the sysplex distributor stack when a server application is available on the target stack. The following values are valid:

- -1: The target stack should send the connection request to the sysplex distributor stack. This value corresponds to the NOOPTLOCAL parameter on the VIPADISTRIBUTE TCP/IP profile statement.
- 0: The connections originating from a target stack within the sysplex always are to bypass sending the connection request to the sysplex distributor.
- 1: The connections originating from a target stack within the sysplex are to bypass sending the connection request to the sysplex distributor as long as the WLM weight for the server on the local stack is not 0. This is the default value if OPTLOCAL is specified without a value.
- 2 - 16: The value is used as a multiplier against the raw WLM weight of the local target stack to cause it to be favored over other target stacks. The higher the value, the more the local stack is favored over other target stacks.

Origin Node The parent node of the workspace.

PROCTYPE CP When the value of the Distribution Method attribute is baseWlm, an indication of the proportion of the workload that is expected to use conventional processors.

PROCTYPE zAAP When the value of the Distribution Method attribute is baseWlm, an indication of the proportion of the workload that is expected to use zAAP processors.

PROCTYPE zIIP When the value of the Distribution Method attribute is baseWlm, an indication of the proportion of the workload that is expected to use zIIP processors.

PROCXCOST zAAP When the value of the Distribution Method attribute is serverWlm, an indication of the crossover cost of running the targeted zAAP workload on a conventional processor instead of on the zAAP processor.

PROCXCOST zIIP When the value of the Distribution Method attribute is serverWlm, an indication of the crossover cost of running the targeted zIIP workload on a conventional processor instead of on the zIIP processor.

Rank The rank of this stack in the chain of backup stacks for a given DVIPA. For entries that do not have an Origin value of backup or define, this value does not apply and is set to N/A.

Status The status of the DVIPA on the given TCP/IP stack. The following values are valid:

- unknown (1): An error occurred.
- active (2): The DVIPA is active.
- backup (3): The given TCP/IP stack is currently a backup owner for the DVIPA.
- moving (4): The DVIPA was active for the TCP/IP stack but the ownership transferred to another TCP/IP stack (for example, because of a takeover).
- quiescing (5): The DVIPA is no longer a target but still has connections. When all existing connections are closed, the status changes to deactivated.
- deactivated (6): The VARY,,TCPIP,SYSPLEX,DEACTIVATE command was run for this DVIPA. The DVIPA remains deactivated until a VARY,,TCPIP,SYSPLEX,REACTIVATE command is run for this DVIPA.
- deactLeavegroup (7): The VARY,,TCPIP,SYSPLEX,DEACTIVATE command was run for this DVIPA, and the VARY,,TCPIP,SYSPLEX,LEAVEGROUP command was run for this stack. If the stack rejoins the sysplex group before a VARY,,TCPIP,SYSPLEX,REACTIVATE command is run for this DVIPA, this DVIPA remains deactivated and the DVIPA status changes to deactivated.
- deactAutonomics (8): The VARY,,TCPIP,SYSPLEX,DEACTIVATE command was run for this DVIPA and the stack left the sysplex group because of an error condition detected by the sysplex autonomics function. If the stack rejoins the sysplex group before a VARY,,TCPIP,SYSPLEX,REACTIVATE command is run for this DVIPA, this DVIPA remains deactivated and the DVIPA status changes to deactivated.
- inactLeavegroup (9): The VARY,,TCPIP,SYSPLEX,LEAVEGROUP command was run for this stack, and the DVIPA is currently inactive. The DVIPA is reactivated if a VARY,,TCPIP,SYSPLEX,JOINGROUP command is run for this stack.
- inactAutonomics (10): The stack left the sysplex group because of an error condition detected by the sysplex autonomics function.

Sysplex Name The name of the sysplex.

Sysplex Port Enabled An indication of whether the sysplex-wide ephemeral port assignment is enabled. The following values are valid:

- Yes: The function is enabled.
- No: The function is not enabled.

System ID The SMF system ID.

TCPIP Host Name The short TCP/IP host name.

TCPIP Job Name The TCP/IP job name.

Timed Affinity The duration, in seconds, that the sysplex distributor function maintains an affinity between connections from a specific client and a server instance on a target stack. A value of 0 indicates that no connection affinity is maintained. A non-zero value indicates that, as long as the number of seconds specified have not elapsed since the close of the previous connection, a subsequent connection for a client is routed to the same server as the previous connection.

Update Time The date and time that the data was last updated. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

XCF Group Name The XCF name used by this TCP/IP stack when joining the sysplex. If the stack has not joined the sysplex group, this value is a zero-length string.

zOS Image Name The name of the z/OS operating system.

zOS Release Level The release level of the z/OS operating system.

HiperSockets Configuration and Status Attributes

Use these attributes to view information about HiperSockets configuration and status.

Channel Number The HiperSockets channel path identifier (CHPID).

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

CPC Name The name of the central processor complex (CPC) on which the HiperSockets interface resides.

Interface Administration Status The desired state of the interface. This value is stored as an integer but displayed as a string. The following values are valid:
- 1: up
- 2: down
- 3: testing

Interface Name The textual name of the interface.

Interface Operational Status The current operational state of the interface. This value is stored as an integer but displayed as a string. The following values are valid:
- 1: up
- 2: down
- 3: testing
- 4: unknown
- 5: dormant
- 6: notPresent
- 7: lowerLayerDown

IQDIO Routing Enabled An indication of whether the IQDIOROUTING parameter is specified in the IPCONFIG TCP/IP profile statement. When this routing function is enabled, inbound packets that are to be forwarded by this TCP/IP stack are eligible to be routed directly between a HiperSockets device and an OSA-Express device in QDIO mode without needing to be sent to this TCP/IP stack for forwarding. This type of routing over a HiperSockets device (iQDIO) is called HiperSockets Accelerator.

IQD Network ID An internal system-generated identifier that represents the internal logical network. The IQD (Internal QDIO) network ID is associated with the IQD channel path ID (CHPID) and can span the entire central processor complex (CPC), based on the system configuration of the IQD CHPID. Operating systems running on this CPC that are connected to the same IQD Network ID use the same internal logical network and therefore have network connectivity. The ID can change during system initial machine load (IML) or with dynamic I/O updates for the IQD CHPID.

Multiple Write Enabled An indication that the IQDMULTIWRITE parameter is specified in the GLOBALCONFIG TCP/IP profile statement. When multiple write is enabled, HiperSockets interfaces are configured to use HiperSockets multiple write support when this function is supported by the IBM System z® environment.

Origin Node The parent node of the workspace.

Protocol The IPv4 or IPv6 protocol for the interface.

QDIO Accelerator Enabled An indication of whether the QDIOACCELERATOR parameter, which enables the QDIO accelerator function, is specified in the IPCONFIG TCP/IP profile statement.

QDIO Priority An indication of which QDIO outbound priority level is to be used. For traffic that is routed using HiperSockets Accelerator and that is received over a HiperSockets device and routed to an OSA-Express in QDIO mode, the data is sent using the priority level, which can be 1 - 4 with a default value of 1. For information about OSA-Express, see the *z/OS Communications Server: SNA Network Implementation Guide*. The IQDIO Routing and QDIO Accelerator functions are mutually exclusive. You can specify a QDIO priority value with whichever function you specify. If neither function is specified, the QDIO priority field is 0.

System ID The SMF system ID.

TCPIP Job Name The TCP/IP job name.

VLAN ID A decimal number that indicates the virtual LAN identifier that is to be assigned to an interface.

zIIP Multiple Write Enabled An indication that the IQDIOMULTIWRITE subparameter for the ZIIP parameter is specified in the GLOBALCONFIG TCP/IP profile statement. When zIIP multiple write is enabled, the stack is configured to displace CPU cycles for HiperSockets multiple write workload onto a zIIP.

zOS Image Name The name of the z/OS operating system.

IMS Replication Apply Details Attributes

Use these attributes to view detailed IMS replication apply information.

Note: This attribute group is used with the GDPS Active/Active Continuous Availability solution.

Apply Queue Percent Full The percentage of the target (apply) cache in use (queue depth), computed as (Current Cache Size/Maximum Cache Size)*100 and rounded down to the nearest whole integer.

Apply Server Name The job name of the apply server.

Apply Workload State The state of the workload as determined by the apply server. The following values are valid:
- DESCRIBE
- ENDING CONTROLLED
- ENDING IMMEDIATELY
- ERROR
- INACTIVE
- REPLICATE CONTINUOUS
- STARTING

Bytes Applied The cumulative total number of bytes that were applied.

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Commits Applied The cumulative total number of commit messages that were applied. The number of commits reflects the number of transactions.

Current Cache Size The current number of bytes that are in use in the target (apply) cache.

Deletes Applied The cumulative total number of delete messages that were applied.

IMS Source System Identifier A unique identifier that is used to correlate a target subscription to the corresponding source subscription.

IMS Target URL The target universal resource locator (URL), which, along with the source system identifier, is used to correlate a target subscription to the corresponding source subscription.

Inserts Applied The cumulative total number of insert messages that were applied.

Maximum Cache Size The maximum size of the target (apply) cache in bytes.

Origin Node The parent node of the workspace.

Rollbacks Processed The cumulative total number of rollbacks that were processed.

Rows Applied The cumulative total number of rows that were applied.

State Error Code For an Apply Workload State attribute value of ERROR, the error identification, shown as a hexadecimal code. Otherwise, the value does not apply and is set to N/A.

For information about the error codes, see the information about system messages in the IMS product library.

State Last Changed A time stamp that represents when the value of the Apply Workload State attribute was last changed.

Updates Applied The cumulative total number of update messages that were applied.

Workload Name The name of the workload.

IMS Replication Capture Details Attributes

Use these attributes to view detailed IMS replication capture information.

Note: This attribute group is used with the GDPS Active/Active Continuous Availability solution.

Bytes Received The cumulative total number of bytes that were received by the source server.

Capture Queue Percent Full The percentage of the source (capture) cache that is in use (queue depth), computed as (Current Cache Size/Maximum Cache Size)*100 and rounded down to the nearest whole integer.

Capture Server Name The job name of the capture server.

Capture Workload State The state of the workload as determined by the capture server. The following values are valid:
- DESCRIBE
- ENDING CONTROLLED
- ENDING IMMEDIATELY
- ERROR
- INACTIVE
- REPLICATE CONTINUOUS
- STARTING

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Commits Received The cumulative total number of commit messages that were received by the source server. The number of commits reflects the number of transactions.

Current Cache Size The current number of bytes that are in use in the source (capture) cache.

Deletes Sent The cumulative total number of delete messages that were sent to the target server.

IMS Source System Identifier A unique identifier that is used to correlate a target subscription to the corresponding source subscription.

IMS Target URL The target universal resource locator (URL), which, along with the source system identifier, is used to correlate a target subscription to the corresponding source subscription.

Inserts Sent The cumulative total number of insert messages that were sent to the target server.

Maximum Cache Size The maximum size of the source (capture) cache in bytes.

Origin Node The parent node of the workspace.

Rollbacks Processed The cumulative number of rollbacks that were processed.

Rows Received The cumulative total number of rows that were received by the source server.

State Error Code For a Capture Workload State attribute value of ERROR, the error identification, shown as a hexadecimal code. Otherwise, the value does not apply and is set to N/A.

For information about the error codes, see the information about system messages in the IMS product library.

State Last Changed A time stamp that represents when the value of the Capture Workload State attribute was last changed.

Updates Sent The cumulative total number of update messages that were sent to the target server.

Workload Name The name of the workload.

Inactive TCPIP Connection Count Attributes

Use these attributes to view inactive TCP/IP connection counts.

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Kept Inactive Connections The number of inactive connections stored in the data space.

Origin Node The parent node of the workspace.

Inactive TCPIP Connection Data Attributes

Use these attributes to view inactive TCP/IP connections.

AT-TLS Connection Status The current application transparent transport layer security (AT-TLS) policy status for the connection. The following values are valid:

- Not_Secure (1): The SSL handshake has not completed successfully. A connection can have this status for several reasons, and AT-TLS Policy Status should be examined. If AT-TLS Policy Status is No_TTLS, No_Policy, or Not_Enabled, the handshake does not occur. If AT-TLS Policy Status is Enabled, Appl_Cntl, or Not_Known, the SSL handshake might occur.
- In_Progress (2): The SSL handshake for the connection is in progress.
- Secure (3): The connection is secure. The SSL handshake completed successfully.

AT-TLS Policy Status The AT-TLS status for the connection. The following values are valid:

- Not_Known (0): The TCP/IP stack has not examined the AT-TLS configuration for the connection because the connection has not progressed to a state where the stack is ready to process this information.
- No_TTLS (1): NOTTLS was specified or was the default in the TCP/IP configuration profile when the AT-TLS configuration was examined for the connection. AT-TLS processing is not performed for the connection.

- No_ Policy (2): No AT-TLS policy is defined for the connection. AT-TLS processing is not performed for the connection.
- Not_Enabled (3): An AT-TLS policy is configured for this connection, but the TTLSEnabled parameter is set to OFF. AT-TLS processing is not performed for this connection.
- Enabled (4): An AT-TLS policy is configured for this connection, and the TTLSEnabled parameter is set to ON. AT-TLS processing is performed for this connection.
- Appl_Cntrl (5): An AT-TLS policy is configured for the connection, and the ApplicationControlled parameter is set to ON. The application that owns the connection is to tell the TCP/IP stack when to perform the secure handshake.

Byte Rate The number of bytes that were sent or received per minute for this connection for the entire duration of the connection.

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Connection End Time The date and time that the connection ended. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Connection ID The hexadecimal representation of the connection number.

Connection Start Time The date and time that the connection started. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Local IP Address The local IP address for this TCP connection. IPv4 and IPv6 addresses can be displayed.

Local Port The local port for this TCP connection.

Local Port String The local port for this TCP connection, formatted as a string.

Max Send Window Size The maximum size of the send window for this connection.

Origin Node The parent node of the workspace.

Passive or Active Open The type of open that is performed. The following values are valid:
- 0: Passive open; the remote end initiated the connection.
- 1: Active open; the local end initiated the connection.

Remote IP Address The remote IP address for this TCP connection. IPv4 and IPv6 addresses can be displayed.

Remote Port The remote port for this TCP connection.

Remote Port String The remote port for this TCP connection, formatted as a string.

Reserved For NetView product internal use.

Resource Name The text identification of the resource. This value represents the user who opened the socket. It is updated during bind processing.

Sysplex Name The name of the sysplex.

System ID The SMF system ID.

TCB Address The address of the TCB in the address space that opened the connection.

TCPIP Job Name The TCP/IP job name.

Telnet APPL Name The target VTAM application name if the TCP connection is for a TN3270 or TN3270E session.

Telnet Logmode The VTAM logmode if the TCP connection is for a TN3270 or TN3270E session.

Telnet LU Name The VTAM LU name if the TCP connection is for a TN3270 or TN3270E session.

Telnet Protocol The Telnet mode. Valid values are TN3270, TN3270E, LINEMODE, and N/A.

Termination Reason Code The reason that the connection was stopped. The following values are valid:

- SendErr_FRCA(AFPA) (x'11'): An error occurred during a send using FRCA(AFPA), possibly because the stack is stopping.
- FIN_FRCA(AFPA) (x'12'): A persistent socket used by FRCA(AFPA) is closed by a FIN.
- Stack_Terminating (x'21'): The connection is stopping because the stack is stopping.
- Last_DVIPA_Term (x'22'): The last stack that can own the dynamic VIPA bound to the socket is stopping.
- Intrusion_Detect (x’31’): Intrusion detection found the connection to be malicious and closed the connection.
- NetAccess_Denied (x’32’): The connection is denied because of a NetAccess rule.
- ACK_In_LAST_ACK (x'33'): The acknowledgment that was received is in the lastack state.
- Admin_Action (x'41'): The connection is stopped because of an administrator action (for example, using Netstat DRop/-D command or the NMI API).
- App_Laddr_Deleted (x'42'): The connection is stopped because the local IP address bound by the application was deleted from the stack.
- App_Close_NoAccept (x'51'): The connection from a client is stopped because the application closed the socket before performing an accept().
- App_Closed (x'52'): The application using the socket closed the connection using a close().
- OrderlyPascalClose (x'53'): A pascal routine issued an orderly close request.
- Pascal_Disconnect (x'54'): A pascal routine issued a disconnect request.
- Pascal_AcceptError (x'55'): An error occurred during a pascal accept.
- Client_Sent_Reset (x'61'): The connection is stopped because the client sent a reset.

- Excessive_Retrans (x'71'): The connection is closed because the same packet is being retransmitted multiple times.
- Window_To_Zero (x'72'): The connection is closed because the TCP window is reduced to zero and multiple window probes were not acknowledged.
- Keepalive_Not_Ackn (x'73'): The connection is closed because multiple keepalive probes were not acknowledged.
- Finwait2_Timeout (x'74'): The connection is stopped because the stack timed out waiting for a fin in the finwait-2 state.

Total Bytes The total number of bytes that were sent and received for this connection for the entire duration of the connection.

Total Bytes Received The total number of bytes that were received from IP for this connection for the entire duration of the connection.

Total Bytes Received String The total number of bytes that were received from IP for this connection for the entire duration of the connection, formatted as a string.

Total Bytes Sent The total number of bytes that were sent to IP for this connection for the entire duration of the connection.

Total Bytes Sent String The total number of bytes that were sent to IP for this connection for the entire duration of the connection, formatted as a string.

Total Bytes String The total number of bytes that were sent and received for this connection for the entire duration of the connection, formatted as a string.

Total Segments Retransmitted The total number of segments that were retransmitted over this connection for the entire duration of the connection.

Type of Service Type of Service (ToS) used by this connection.

Load Balancer Groups Attributes

Use these attributes to view group configuration information for an external load balancer.

Note: This attribute group is used with the GDPS Active/Active Continuous Availability solution.

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Group Correlator For NetView product internal use.

Group Name The name of the group that is registered to the load balancer. For internal load balancers (sysplex distributors), this attribute does not apply. By default, this attribute is not displayed in the Load Balancer Workloads workspace.

IP Address The IP address for a server application that is registered for the group.

Load Balancer Correlator For NetView product internal use.

Origin Node The parent node of the workspace.

Port The port number for a server application that is registered for the group.

Workload Availability An indication of whether the server applications on the active site are available and if these server applications are able to handle additional requests for this workload. The following values are valid:

- Yes (1): The server applications for this workload are available and able to handle new workload requests.
- No (2): The server applications for this workload are either not available or not able to handle new workload requests.

By default, this attribute is not displayed in the Load Balancer Groups workspace.

Workload Correlator For NetView product internal use.

Workload Name The name of the workload. By default, this attribute is not displayed in the Load Balancer Groups workspace.

Load Balancers Attributes

Use these attributes to view the external load balancers and sysplex distributors that are defined to load balance a specific workload.

Note: This attribute group is used with the GDPS Active/Active Continuous Availability solution.

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

IP Address The IP address of the load balancer.

Load Balancer Correlator For NetView product internal use.

Origin Node The parent node of the workspace.

Registered Load Balancer Groups The number of groups that are registered by the load balancer. For internal load balancers (sysplex distributors), this attribute does not apply.

Role The role of the load balancer. The following values are valid:

- 1st TIER (1)
- 2nd TIER (2)
- UNKNOWN (3)

Note: The 1st TIER and 2nd TIER values do not pertain to the TIER1 and TIER2 keywords that are provided by the z/OS Communications Server VIPADYNAMIC statement.

Status The status of the load balancer. The following values are valid:

- ACTIVE (1)
- INACTIVE (2)

Type The type of load balancer. The following values are valid:

- EXTERNAL (0)
- SYSPLEX DISTRIBUTOR (1)

NetView Applications Attributes

Use these attributes to view information about NetView applications.

Domain Name The NetView domain name.

NetView Version The NetView version.

Network ID The VTAM network ID.

Origin Node The parent node of the workspace.

RMTCMD IP Address The IPv4 or IPv6 address that is used for the RMTCMD command. The address might be a DVIPA.

RMTCMD Port The port number that is used for the RMTCMD command. A value of 0 indicates that the RMTCMD command is not active for IP.

RMTCMD Port String The port number that is used for the RMTCMD command, formatted as a string.

Role The role of this NetView program. Valid values are NETWORK, SA, GDPS, or a user-defined description.

Status The status of this NetView program. The following values are valid:
- ACTIVE: The NetView program is running.
- INACTIVE: The NetView program is not running.
- LEAVING: The z/OS system on which the NetView program is running is leaving the sysplex.
- UNKNOWN: The NetView program is no longer an active member of the XCF sysplex group of which it is a member.

Sysplex Name The name of the sysplex.

Sysplex Rank The sysplex rank for this NetView program. The following values are valid:
- -1: Not participating in the sysplex group
- 0: Basic NetView program
- 1 - 249: Master-capable NetView program
- 250: Master NetView program

Sysplex Role The sysplex role for this NetView program. The following values are valid:
- BASIC: Basic NetView program.
- EBASIC: Basic NetView program in a sysplex with an enterprise master NetView program.
- EMASTER: Enterprise master NetView program.
- EMCAP: Master-capable NetView program in a sysplex with an enterprise master NetView program.
- MASTER: Master NetView program.
- MCAP: Master-capable NetView program.
- RBASIC: Basic NetView program outside the sysplex that is forwarding data to the enterprise master program.
- RMASTER: Master NetView program outside the sysplex that is forwarding data to the enterprise master program.

- RMCAP: Master-capable NetView program outside the sysplex that is forwarding data to the enterprise master program.

System ID The SMF system ID.

Total CPU The current NetView CPU percentage.

Total Storage The current NetView storage utilization in kilobytes.

Update Time The date and time that the data was last updated. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

XCF Group List A list of XCF groups of which this NetView program is a member. A maximum of 3 groups can be displayed.

zOS Image Name The name of the z/OS operating system.

NetView Audit Log Attributes

Use these attributes to display NetView audit log records.

Date The date that the message was sent.

Message Log Audit trail messages for take action commands. The following messages are written in this field:
- Audit trail messages BNH806I and BNH807I that are issued for take action commands using the NetView for z/OS Enterprise Management Agent or the APSERV command receiver, or only message BNH806I that is issued for take action commands processed by the APSERV command receiver.
- Error messages that are issued for the Browse NetView Logs take action command.

Message Time The date and time that the message was sent.

Origin Node The parent node of the workspace.

Time The time that the message was sent.

NetView Command Response Attributes

Use these attributes to view NetView command responses. Although the NetView Command Response Summary view is not a table view, you can view the attributes with the query editor.

Command Output The command or command response.

INOUT For NetView product internal use. This attribute indicates whether the data is the input or output of a command.

More For NetView product internal use. This attribute indicates whether the data is a continuation of previous command output.

Origin Node The parent node of the workspace.

Timestamp The time and date that the command was processed.

Userid For NetView product internal use. This attribute indicates the operator that issued the command.

NetView Log Attributes

Use these attributes to display network log records.

DateTime Label For NetView product internal use. This attribute is the concatenation of the Date and Time attribute values, which is used to depict the x-axis in the bar chart view.

First Record Date The date of the first record retrieved.

HDRMTYPE The message type (HDRMTYPE) of the record.

Network Log The network log from which the records are retrieved.

Message The message text.

Message Domain The NetView domain ID or record originator.

Message Time The time that the message was logged.

Operator ID The operator ID of the record originator.

Origin Node The parent node of the workspace.

Record Count For NetView product internal use. This attribute is needed to generate the bar chart view.

Routing Code The routing code for the message.

Sequence Number The sequence number for the VSAM key.

NetView Tasks Attributes

Use these attributes to view information about NetView tasks for the specified NetView domain.

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

CPU Utilization Processor utilization statistics.

Critical CPU Util Indicator For NetView product internal use. This attribute is set to 1 if the current CPU utilization is greater than or equal to the Critical CPU Util Threshold value.

Critical CPU Util Threshold The critical CPU utilization threshold value. If the current CPU utilization is greater than or equal to this value, the CPU utilization is flagged as being at a critical value. For information about how the NetView OVERRIDE and DEFAULTS commands work with this attribute, see the *IBM Tivoli NetView for z/OS User's Guide: NetView*.

Critical Storage Indicator For NetView product internal use. This attribute is set to 1 if the current storage is greater than or equal to the Critical Storage Threshold value.

Critical Storage Threshold The critical storage threshold value. If the current storage is greater than or equal to this value, the storage is flagged as being at a critical value. For information about how the NetView OVERRIDE and DEFAULTS commands work with this attribute, see the See the *IBM Tivoli NetView for z/OS User's Guide*.

Domain Name The NetView domain name.

Input Message Rate The rate of messages coming into a task. The count consists of only the message queued to tasks using the NetView DQIMQS services, and only the buffers accounted for by DSIMQS.

I/O Rate The rate of I/O requests for this task.

Message Queue Count The number of buffers on the public message queue or queues of the task.

Origin Node The parent node of the workspace.

Output Message Rate The rate of messages leaving a task. The count consists of only the message queued to tasks using the NetView DQIMQS services, and only the buffers accounted for by DSIMQS.

Status The status of this task.

Storage The task storage used by this task, in kilobytes.

Task Name The name of this task.

OSA Channels and Ports Attributes

Use these attributes to view information about OSA channels and ports.

Active MAC Address A 6-byte octet string that contains the current MAC address in use on the OSA. The values are in canonical format. The format is a 12-digit hexadecimal string.

Active Speed Mode The actual speed and mode in which the OSA is running. This value is stored as an integer but is displayed as a string. The valid values are based on the type of OSA, and a value of 1 indicates a different active speed mode depending on the type of OSA.

- For the OSA-Express 10 Gigabit Ethernet feature, the following values are valid:
  - 1: unknown
  - 8: tenGigabitFullDuplex
- For OSA-Express3, the following values are valid:
  - 0: unknown
  - 1: tenMegabits
  - 2: tenMbFullDuplex
  - 3: oneHundredMbHalfDuplex
  - 4: oneHundredMbFullDuplex
  - 6: oneThousandMbFullDuplex

  - 8: tenGigabitFullDuplex
- For OSA-Express, the following values are valid:
  - 0: unknown
  - 1: tenMbHalfDuplex
  - 2: tenMbFullDuplex
  - 3: oneHundredMbHalfDuplex
  - 4: oneHundredMbFullDuplex
  - 6: oneThousandMbFullDuplex

Burned-In MAC Address A 6-byte octet string that contains the burned-in MAC address on the OSA. The values are in canonical format. The format is a 12-digit hexadecimal string.

Channel Hardware Level The hardware model of the channel. This value is stored as an integer but is displayed as a string. The following values are valid:

- unavailable (0): The hardware level is unavailable.
- unknown (1): The hardware level is unknown.
- osaExp150 (2): The hardware level is 1.50, which indicates the OSA-Express feature.
- osaExp175 (3): The hardware level is 1.75, which indicates the OSA-Express feature.
- osaExp300 (4): The hardware level is 3.00, which indicates the OSA-Express2 feature.
- osaExp400 (5): The hardware level is 4.00, which indicates the OSA-Express3 feature.

Channel Number The channel path identifier (CHPID) corresponding to this device.

Channel Type The type of channel. The following values are valid:

- osaExpress (16)
- osaDirectExpress (17)
- osaIntraensembleData (48): This value is available with z/OS V1R12 Communications Server or later.
- osaIntraensembleManage (49): This value is available with z/OS V1R12 Communications Server or later.

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Configuration Speed Mode The configured port speed. This attribute indicates the speed that was configured by the user for the OSA-Express Fast Ethernet feature. This value is stored as an integer and is displayed as a string. For OSA-Express Gigabit or 10 Gigabit Ethernet features, it is not used and returns -1. The following values are valid:

- -1: notValidGigabit
- 0: autoNegotiate
- 1: tenMbHalfDuplex
- 2: tenMbFullDuplex
- 3: oneHundredMbHalfDuplex
- 4: oneHundredMbFullDuplex
- 6: oneThousandMbFullDuplex

- 8: tenGigabitFullDuplex

CPC Name The name of the central processor complex (CPC) on which the OSA resides.

Disabled Status A more detailed explanation for the disabled state when the value of the LAN Traffic State attribute is 5 (disabled). When the value of ibmOsaExp10GigEthLanTrafficState is not disabled (the LAN Traffic State attribute has a value other than 5), the value is stored as zero and displayed as zeros. This value is stored as a hexadecimal integer and displayed as a 4-digit hexadecimal number mapped by the following bit settings. The value can be a combination of the bits. For more information about these values, see the *System z10, System z9 and eServer zSeries Open Systems Adapter-Express Customer's Guide and Reference*.
- 0: reserved0
- 1: internalPortFailure
- 2: reserved2
- 3: reserved3
- 4: reserved4
- 5: reserved5
- 6: portTemporarilyDisabled
- 7: reserved7
- 8: reserved8
- 9: serviceProcessorRequest
- 10: networkRequest
- 11: osasfRequest
- 12: configurationChange
- 13: linkFailureThresholdExceeded
- 14: reserved14
- 15: reserved15

LAN Traffic State The LAN state, expressed as a value of 0 - 8. A value of disabled (5) is further explained in the Disabled Status attribute. This value is stored as an integer but is displayed as a string. The following values are valid. For more information about these values, see the *System z10, System z9 and eServer zSeries Open Systems Adapter-Express Customer's Guide and Reference*.
- 0: undefined
- 1: unavailable
- 2: enabling
- 3: disabling
- 4: enabled
- 5: disabled
- 6: linkMonitor
- 7: definitionError
- 8: configuredOffline

Origin Node The parent node of the workspace.

Port Name The name of the port as specified by the VTAM Transport Resource List Entry (TRLE).

Port Number The physical port number for this port.

Port Type The physical port type. This value is stored as an integer but is displayed as a string. The following values are valid:
- 65: gigabitEthernet
- 81: fastEthernet

- 97: oneThousandBaseTEthernet
- 145: tenGigabitEthernet
- 161: osaexp3gigabitEthernet
- 177: osaexp3oneThousandBaseTEthernet
- 193: osaexp3tenGigabitEthernet

Service Mode An indicator of whether the processor is in service mode. The following values are valid:
- 0: No
- 1: Yes

Subtype The type of OSA feature present. This value is stored as an integer but is displayed as a string. The following values are valid:
- 1: unknown
- 65: gigabitEthernet
- 81: fastEthernet
- 97: oneThousandBaseTEthernet
- 145: tenGigabitEthernet
- 161: osaexp3gigabitEthernet
- 177: osaexp3oneThousandBaseTEthernet
- 193: osaexp3tenGigabitEthernet

System ID The SMF system ID.

Replication Servers Attributes

Use these attributes to view information for all replication servers (DB2 and IMS).

Note: This attribute group is used with the GDPS Active/Active Continuous Availability solution.

Apply Image Name The image name of the apply server.

Apply Server ASID The address space ID of the apply server. This is a 4-digit hexadecimal number.

Apply Server Name The job name of the apply server.

When the value of Workload Type is DB2, the DB2 Apply Server attribute in the DB2 Replication Details workspace indicates the DB2 subsystem or the DB2 group attach name.

Apply Server Status The status of the NetView connection to the apply server. The following values are valid:
- ACTIVE
- INACTIVE

Apply Site Name The name of the apply site.

Apply Workload Collection Time The date and time that the NetView program received the data from the apply server for this workload.

Apply Workload State The state of the workload as determined by the apply server.

When the value of Workload Type is DB2, the following values are valid:

- INACTIVE
- REPLICATE CONTINUOUS

When the value of Workload Type is IMS, the following values are valid:

- DESCRIBE
- ENDING CONTROLLED
- ENDING IMMEDIATELY
- ERROR
- INACTIVE
- REPLICATE CONTINUOUS
- STARTING

Average Apply Latency The average elapsed time in milliseconds between the time that transactions were received by the target server and the time that transactions were committed to the target data source. This average includes only the transactions that were processed during the last polling interval.

When the value of Workload Type is DB2, average apply latency is the average elapsed time in milliseconds between the time that the Q Apply program read transactions from the receive queue and the time that they were committed to the target.

When the value of Workload Type is IMS, average apply latency is the average elapsed time in milliseconds between the time that a transaction was received by the target server and the time that the processing of the transaction was completed by the database management system (DBMS).

Average Capture Latency The average elapsed time in milliseconds between the time that transactions were committed to the source table or database and the time that transactions were sent to the target server. This average includes only the transactions that were processed during the last polling interval.

When the value of Workload Type is DB2, average capture latency is the average elapsed time in milliseconds between the time that transactions were committed to the source table and the time that the Q Capture program puts the last message for the transactions on the send queue.

When the value of Workload Type is IMS, average capture latency is the average elapsed time in milliseconds between the time that a transaction was committed to the source database and the time that the transaction was sent to the target server.

Average Latency The average elapsed time in milliseconds between the time that transactions were committed to the source table or database and the time that transactions were committed to the target table or database. This average includes only the transactions that were processed during the last polling interval.

Average Network Latency The average elapsed time in milliseconds between the time that transactions were sent to the target server and the time that the target server received them. This average includes only the transactions that were processed during the last polling interval.

When the value of Workload Type is DB2, average network latency is the average elapsed time in milliseconds between the time that the Q Capture program put messages on the send queue and the time that the Q Apply program got them from the receive queue.

When the value of Workload Type is IMS, average network latency is the average elapsed time in milliseconds between the time that a transaction was sent to the target server and the time that the transaction was received by the target server.

Bytes Received The cumulative total number of bytes that were received by the target server.

Bytes Sent The cumulative total number of bytes that were sent to the target server.

Capture Image Name The image name of the capture server.

Capture Server ASID The address space ID of the capture server. This is a 4-digit hexadecimal number.

Capture Server Name The job name of the capture server.

When the value of Workload Type is DB2, the DB2 Capture Server attribute in the DB2 Replication Details workspace indicates the DB2 subsystem or the DB2 group attach name.

Capture Server Status The status of the NetView connection to the capture server. The following values are valid:
- ACTIVE
- INACTIVE

Capture Site Name The name of the capture site.

Capture Workload Collection Time The date and time that the NetView program received the data from the capture server for this workload.

Capture Workload State The state of the workload as determined by the capture server.

When the value of Workload Type is DB2, the following values are valid:
- INACTIVE
- REPLICATE CONTINUOUS

When the value of Workload Type is IMS, the following values are valid:
- DESCRIBE
- ENDING CONTROLLED
- ENDING IMMEDIATELY
- ERROR
- INACTIVE
- REPLICATE CONTINUOUS
- STARTING

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

DB2 Apply Server For a Workload Type of DB2, the DB2 subsystem or the DB2 group attach name. Otherwise, the value is set to N/A.

DB2 Capture Server For a Workload Type of DB2, the DB2 subsystem or the DB2 group attach name. Otherwise, the value is set to N/A.

DB2 Receive Queue For a Workload Type of DB2, the name of the receive queue. Otherwise, the value is set to N/A.

DB2 Send Queue For a Workload Type of DB2, the name of the send queue. Otherwise, the value is set to N/A.

IMS Source System Identifier For a Workload Type of IMS, a unique identifier that is used to correlate a target subscription to the corresponding source subscription. Otherwise, the value is set to N/A.

IMS Target URL For a Workload Type of IMS, the universal resource locator (URL), which, along with the source system identifier, is used to correlate a target subscription to the corresponding source subscription. Otherwise, the value is set to N/A.

Origin Node The parent node of the workspace.

Point in Time Consistency A time stamp that represents the point in time at which all transactions have been applied to the target without gaps that might result from parallel apply.

Rows Received The cumulative total number of rows that were received by the target server.

Rows Sent The cumulative total number of rows that were sent to the target server.

Transactions Received The cumulative total number of transactions that were received by the target server.

Transactions Sent The cumulative total number of transactions that were sent to the target server.

Workload Name The name of the workload.

Workload Type The type of workload. The following values are valid:
- DB2
- IMS

Session Data Attributes

Use these attributes to view session data.

Application Recovery The application LU recovery status. The following values are valid:
- P: The application LU recovery is pending.
- I: The application LU recovery is in progress.
- C: The application LU recovery is complete.

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

DateTime Label Deprecated attribute.

DLUS DLUR An indication that this session traverses a DLUS-DLUR pipe. For more information, enter HELP NLDM 'DLUS-DLUR PIPE' from a NetView for z/OS host session.

Endpoint Change The endpoint change notification. The following values are valid:

- PRI: The control point (CP) at the primary endpoint changed since the session started.
- SEC: The CP at the secondary endpoint changed since the session started.
- P/S: The CPs at both the primary and the secondary endpoints changed since the session started.

Origin Node The parent node of the workspace.

PCID The fully-qualified procedure correlation identifier (PCID) of the session.

Primary Domain The NetView domain associated with the primary endpoint. Other valid values include X-NET, NNNA, C-C, N/A or blanks. For more information, enter HELP NLDM 'DOM' from a NetView for z/OS host session.

Primary Name The network-qualified name of the primary endpoint.

Primary Takeover Giveback The status of the takeover, giveback, or both for the primary resource. The following values are valid:

- TOV: The resource is taken over.
- GTK: The resource was previously given back and is now taken over.
- GBK: The resource is given back.
- TGV: The resource was previously taken over and is now given back.

Primary Type The type of the primary endpoint.

RecordCount Deprecated attribute.

Secondary Domain The NetView domain associated with the secondary endpoint. Other valid values include X-NET, NNNA, C-C, N/A, or blanks. For more information, enter HELP NLDM 'DOM' from a NetView for z/OS host session.

Secondary Name The network-qualified name of the secondary endpoint.

Secondary Takeover Giveback The status of the takeover, giveback, or both, for the secondary resource. The following values are valid:

- TOV: The resource is taken over.
- GTK: The resource was previously given back and is now taken over.
- GBK: The resource is given back.
- TGV: The resource was previously taken over and is now given back.

Secondary Type The type of the secondary endpoint.

SenseCount Deprecated attribute.

Start Time The date and time that the session started. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

System ID The SMF system ID.

XRF Type The extended recovery facility session type. For more information, enter HELP NLDM 'XRF' from a NetView for z/OS host session.

Stack Configuration and Status Attributes

Use these attributes to view the stack configuration and status information.

AT-TLS Enabled An indication that the stack can have a policy defined and active for the application transparent transport layer security (AT-TLS) protocol.

IP Address The IPv4 or IPv6 address for this TCP/IP stack.

IPSec Enabled An indication that the stack can have an IP security policy defined and active.

IPSecV6 Enabled An indication that the stack can have an IPv6 security policy defined and active.

IPv6 Enabled An indication that the stack is IPv6 enabled.

LPAR Name The name of the LPAR.

Origin Node The parent node of the workspace.

Primary Interface The link name that is designated as the default local host for use by the GETHOSTID() function. This value applies only to IPv4 links.

Segmentation Offload Enabled An indication that SEGMENTATIONOFFLOAD support is enabled. When this support is enabled, the stack offloads TCP segmentation to OSA-Express features.

Source VIPA Enabled An indication that SOURCEVIPA support is enabled. When this support is enabled, TCP/IP uses the TCPSTACKSOURCEVIPA address (if specified) or the corresponding virtual IP address in the HOME list as the source IP address for outbound data grams that do not have an explicit source address.

Source VIPAV6 Enabled An indication that SOURCEVIPA support is enabled for IPv6.

Status The status of the stack. Valid values are ACTIVE, INACTIVE, TERMINATION, STARTING, and STOP_CMD.

Status Count For NetView product internal use. This attribute is needed to generate the bar chart view.

Sysplex Name The name of the sysplex.

Sysplex WLM Polling Interval The amount of time, in seconds, that determines how quickly the sysplex distributor and the target servers of the sysplex distributor poll WLM for new weight values. A non-zero value indicates that SYSPLEXWLMPOLL support is enabled. A short time results in quicker reactions to target status changes. A valid value is 1 - 180 seconds. The default value is 60 seconds.

System ID The SMF system ID.

TCPIP Host Name The short TCP/IP host name.

TCPIP Job Name The TCP/IP job name.

TCP Stack Source VIPA Enabled An indication that TCPSTACKSOURCEVIPA support is enabled. When this support is enabled, and if SOURCEVIPA was enabled, the IPv4 address is used as the source IP address for outbound TCP connections. The value of the IPv4 address must be a static VIPA or an active dynamic VIPA (DVIPA).

TCP Stack Source VIPAV6 Enabled An indication that TCPSTACKSOURCEVIPA support is enabled for IPv6.

Update Time The date and time that the data was last updated. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

VTAM XCF Group The XCF group name that is used to partition VTAM nodes within a sysplex.

XCF Group Name The XCF name used by this TCP/IP stack when joining the sysplex. If the stack has not joined the sysplex group, this value is a zero-length string.

zIIP IP Security Enabled An indication that ZIIP IPSECURITY support is enabled. When this support is enabled, CPU cycles for IPSec workload to a zIIP should be displaced when possible.

zOS Image Name The name of the z/OS operating system.

zOS Release Level The release level of the z/OS operating system.

TCPIP Connection Data Attributes

Use these attributes to view TCP/IP connections.

Address Space ID The MVS address space ID of the address space that opened the socket. This is a 4-digit hexadecimal number.

AT-TLS Cipher The negotiated cipher that is used by the secure connection. This value, which is shown as a hexadecimal code, applies only if AT-TLS Connection Status has a value of Secure. For valid values, see information about the TTLSCipherParms statement in the *z/OS Communications Server: IP Configuration Reference*.

AT-TLS Connection Status The current application transparent transport layer security (AT-TLS) policy status for the connection. The following values are valid:

- Not_Secure (1): The SSL handshake has not completed successfully. A connection can have this status for several reasons, and AT-TLS Policy Status should be examined. If AT-TLS Policy Status is No_TTLS, No_Policy, or Not_Enabled, the handshake does not occur. If AT-TLS Policy Status is Enabled, Appl_Cntl, or Not_Known, the SSL handshake might occur.
- In_Progress (2): The SSL handshake for the connection is in progress.
- Secure (3): The connection is secure. The SSL handshake completed successfully.

AT-TLS Partner Userid The user ID associated with the certificate of the partner. This value is applicable only if AT-TLS Connection Status has a value of Secure and a user ID is associated with the certificate of the partner.

AT-TLS Policy Status The AT-TLS status for the connection. The following values are valid:

- Not_Known (0): The TCP/IP stack has not examined the AT-TLS configuration for the connection because the connection has not progressed to a state where the stack is ready to process this information.
- No_TTLS (1): NOTTLS was specified or was the default in the TCP/IP configuration profile when the AT-TLS configuration was examined for the connection. AT-TLS processing is not performed for the connection.
- No_ Policy (2): No AT-TLS policy is defined for the connection. AT-TLS processing is not performed for the connection.
- Not_Enabled (3): An AT-TLS policy is configured for this connection, but the TTLSEnabled parameter is set to OFF. AT-TLS processing is not performed for this connection.
- Enabled (4): An AT-TLS policy is configured for this connection, and the TTLSEnabled parameter is set to ON. AT-TLS processing is performed for this connection.
- Appl_Cntrl (5): An AT-TLS policy is configured for the connection, and the ApplicationControlled parameter is set to ON. The application that owns the connection is to tell the TCP/IP stack when to perform the secure handshake.

AT-TLS Security Type The type of system SSL secure session defined in the AT-TLS policy that is used by the connection. The following values are valid:

- N/A (0): Not applicable because AT-TLS Policy Status has a value other than Enabled or Appl Cntrl.
- Client (1): The SSL handshake is performed as a client.
- Server (2): The SSL handshake is performed as a server.
- SRVCAPASS (3): The SSL handshake is performed as a server requiring client authentication, but the client certificate validation is bypassed.
- SRVCAFULL (4): The SSL handshake is performed as a server requiring client authentication, and, if the client presents a certificate, client certificate validation is performed.
- SRVCAREQD (5): The SSL handshake is performed as a server requiring client authentication, and the client must present a certificate so that client certificate validation can be performed.
- SRVCASAFCHK (6): The SSL handshake is performed as a server requiring client authentication; the client must present a certificate so that client certificate validation can be performed, and the client certificate must have an associated user ID defined to the security product.

AT-TLS SSL Protocol The negotiated SSL protocol in use by the connection. The following values are valid:

- SSL_V2: SSL Version 2
- SSL_V3: SSL Version 3
- TLS_V1: TLS Version 1
- N/A: Not applicable

Byte Rate The number of bytes that were sent or received per minute during the most recent time interval.

Bytes Received The number of bytes that were received during the most recent time interval.

Bytes Received String The number of bytes that were received during the most recent time interval, formatted as a string.

Bytes Sent The number of bytes that were sent during the most recent time interval.

Bytes Sent or Received The number of bytes that were sent or received during the most recent time interval.

Bytes Sent or Received String The number of bytes that were sent or received during the most recent time interval, formatted as a string.

Bytes Sent String The number of bytes that were sent during the most recent time interval, formatted as a string.

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Connection ID The hexadecimal representation of the connection number.

Connection Start Time The date and time that the connection started. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Connection State The state of the connection. The following values are valid:

- CLOSED (1): The connection has ended and no longer exists.
- LISTENING (2): The connection is waiting for a connection request from any remote TCP and port.
- SYN_SENT (3): The connection is waiting for a matching connection request after sending a connection request. If a connection is in this state for two successive sample intervals, an exception is generated.
- SYN_RECEIVED (4): The connection is waiting for a confirming connection request acknowledgment after receiving and sending a connection request.
- ESTABLISHED (5): The connection is established.
- FIN_WAIT_1 (6): The connection is waiting for a connection stop request from the remote TCP or an acknowledgment of the connection stop request.
- FIN_WAIT_2 (7): The connection is waiting for a connection stop request from the remote TCP.
- CLOSE_WAIT (8): The connection is waiting for a connection stop request from the local port.
- LAST_ACK (9): The connection is waiting for an acknowledgment of the connection stop request that it sent to the remote TCP.
- CLOSING (10): The connection is waiting for a connection stop request acknowledgment from the remote TCP.
- TIME_WAIT (11): The host is waiting to ensure that a remote TCP has received a connection stop request. When the wait time is over, the socket pair that defines the connection is available for reuse.
- DELETE_TCB (12): The TCP connection has closed, and the resources that represent the connection are waiting to be cleaned up.

Current Send Window Size The current size of the send window.

Interface Name The name of the interface.

Last Activity Remote Timestamp The most recent time stamp value, in milliseconds, received from the remote side of the connection. If the TCP time stamp header option is not used, the value of this field is zero. If the TCP time stamp header option is used, this field contains bits 10 - 41 of a related time stamp that is provided by z/OS Communications Server. The related time stamp is in store clock (STCK) format, which approximately indicates units of seconds. To convert this field into a STCK value and then into a date and time, follow these steps:

1. Determine the current STCK value by using the following NetView command:
   `PIPE EDIT IFRAUGMT C2X|CONS`
2. Prefix bits 0 - 9 of the current STCK value to the field; if that conversion yields a time in the future, then subtract 1 from bits 0 - 9 of the current STCK value and prefix that value to the field instead.
3. To convert the resulting STCK value (the field with the prefix added) to a date and time, run the following NetView command:
   `PIPE EDIT 'resulting_STCK_value'X ZDT 1|CONS`

Last Activity Timestamp The date and time of the last activity on this connection. By default, this value is displayed as *MM/DD/YY hh:mm:ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Last Timestamp Age The time, in milliseconds, when the most recent time stamp from the partner was updated. If the TCP time stamp header option is not used, the value of this field is zero. If the TCP time stamp header option is used, this field contains bits 10 - 41 of a related time stamp that is provided by z/OS Communications Server. The related time stamp is in store clock (STCK) format, which approximately indicates units of seconds. To convert this field into a STCK value and then into a date and time, follow these steps:

1. Determine the current STCK value by using the following NetView command:
   `PIPE EDIT IFRAUGMT C2X|CONS`
2. Prefix bits 0 - 9 of the current STCK value to the field; if that conversion yields a time in the future, then subtract 1 from bits 0 - 9 of the current STCK value and prefix that value to the field instead.
3. To convert the resulting STCK value (the field with the prefix added) to a date and time, run the following NetView command:
   `PIPE EDIT 'resulting_STCK_value'X ZDT 1|CONS`

Local IP Address The local IP address for this TCP connection. IPv4 and IPv6 addresses can be displayed.

Local Port The local port for this TCP connection.

Local Port String The local port for this TCP connection, formatted as a string.

Max Send Window Size The maximum size of the send window.

Number of Duplicate ACKS The number of duplicate acknowledgments that are received by this connection.

Origin Node The parent node of the workspace.

Passive or Active Open The type of open performed. The following values are valid:
- 0: Passive open; the remote end initiated the connection.
- 1: Active open; the local end initiated the connection.

Percent Segments Retransmitted The percent of TCP segments that were retransmitted over this connection since the connection started.

Remote IP Address The remote IP address for this TCP connection. IPv4 and IPv6 addresses can be displayed.

Remote Port The remote port for this TCP connection.

Remote Port String The remote port for this TCP connection, formatted as a string.

Resource Name The text identification of the resource. This value represents the user who opened the socket. It is updated during bind processing.

Segments Received The number of segments that were received over this connection during the most recent time interval.

Segments Retransmitted The number of segments that were retransmitted over this connection during the most recent time interval.

Segments Sent The number of segments that were sent over this connection during the most recent time interval.

Segments Sent or Received The number of segments that were sent or received over this connection during the most recent time interval.

Sysplex Name The name of the sysplex.

System ID The SMF system ID.

TCB Address The address of the TCB in the address space that opened the socket.

TCPIP Host Name The short TCP/IP host name that was discovered for the TCP/IP job name.

TCPIP Job Name The TCP/IP job name for which a connection endpoint is found.

Telnet APPL Name The target VTAM application name if the TCP connection is for a TN3270 or TN3270E session.

Telnet Logmode The VTAM logmode if the TCP connection is for a TN3270 or TN3270E session.

Telnet LU Name The VTAM LU name if the TCP connection is for a TN3270 or TN3270E session.

Telnet Protocol The Telnet mode. Valid values are TN3270, TN3270E, LINEMODE, and N/A.

Telnet User Client Name The user ID of the client if the TCP connection is for a TN3270 or TN3270E session.

Total Bytes The total number of bytes that were sent and received for this connection since the connection started.

Total Bytes Received The total number of bytes that were received from IP for this connection since the connection started.

Total Bytes Received String The total number of bytes that were received from IP for this connection since the connection started, formatted as a string.

Total Bytes Sent The total number of bytes that were sent to IP for this connection since the connection started.

Total Bytes Sent String The total number of bytes that were sent to IP for this connection since the connection started, formatted as a string.

Total Bytes String The total number of bytes that were sent and received for this connection since the connection started, formatted as a string.

Total Segments The total number of segments that were sent and received for this connection since the connection started.

Total Segments Received The total number of segments that were received from IP for this connection since the connection started.

Total Segments Retransmitted The total number of segments that were retransmitted over this connection since the connection started.

Total Segments Sent The total number of segments that were sent to IP for this connection since the connection started.

zOS Image Name The name of the z/OS operating system for which TCP/IP connection information is requested.

Telnet Server Attributes

Use these attributes to view information about Telnet servers.

Active Ports The number of active ports that are associated with the Telnet server job.

Address Space ID The MVS address space ID of the address space that opened the socket. This is a 4-digit hexadecimal number.

Configured Ports The number of configured ports that are associated with the Telnet server job.

Origin Node The parent node of the workspace.

Server Status The status of the Telnet server.

Telnet Server Job Name The Telnet server job name.

Update Time The date and time that the data was last updated. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

zOS Image Name The name of the z/OS operating system.

Telnet Server Port Attributes

Use these attributes to view information about Telnet server ports.

Active Connections The current number of connections. When the port is quiesced, this value is 0, even if connections are active. When the port is resumed, only new connections on this port are displayed. This information is retrieved from the z/OS Communications Server network management interface by using an active TCP listeners request. To see all the connections for this port, issue the z/OS Communications Server DISPLAY TCPIP,tnproc,TELNET command. For more information, see *z/OS Communications Server IP System Administrator's Commands*.

Address Space ID The MVS address space ID of the address space that opened the socket. This is a 4-digit hexadecimal number.

Dropped Connections The total number of connections that are dropped by this listener because the backlog was exceeded. This attribute applies only to listener entries.

LPAR Name The name of the LPAR.

Origin Node The parent node of the workspace.

Port The Telnet server port.

Port String The Telnet server port, formatted as a string.

Port Status The status of the Telnet server port.

Resource Name The text identification of the resource. This value represents the user who opened the socket. It is updated during bind processing.

Server Status The status of the Telnet server.

Sysplex Name The name of the sysplex.

System ID The SMF system ID.

TCB Address The address of the TCB in the address space that opened the connection. If the port status is QUIESCED, this attribute has no value.

TCPIP Job Name The name of the TCP/IP job to which this Telnet server port is connected.

TCPIP Stack Affinity The name of the TCP/IP stack job with which this Telnet server has an affinity.

Telnet Server Job Name The Telnet server job name.

Update Time The date and time that the data was last updated. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

zOS Image Name The name of the z/OS operating system.

zOS Release Level The release level of the z/OS operating system.

VIPA Routes Attributes

Use these attributes to view information about the virtual IP address (VIPA) routes.

Destination XCF IP Address The dynamic XCF IP address of the target stack that is receiving connections.

Origin Node The parent node of the workspace.

Status The VIPAROUTE status.
- 1: Defined
- 2: Unavailable
- 3: Active
- 4: Inactive

Status Count For NetView product internal use. This attribute is needed to generate the bar chart view.

System ID The SMF system ID of the system where the DVIPA is configured.

Target Stack IP Address The IP address of the target TCP/IP stack.

Update Time The date and time that the data was last updated. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Workload Lifeline Advisors Attributes

Use these attributes to view the primary and secondary Multi-site Workload Lifeline Advisors.

Note: This attribute group is used with the GDPS Active/Active Continuous Availability solution.

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

IPv4 Address The IPv4 address of the Multi-site Workload Lifeline Advisor.

IPv6 Address The IPv6 address of the Multi-site Workload Lifeline Advisor.

Load Balancers The number of active load balancers and sysplex distributors that are registered with the Multi-site Workload Lifeline Advisor. This attribute is not applicable for secondary Multi-site Workload Lifeline Advisors.

Origin Node The parent node of the workspace.

Role The role of the Multi-site Workload Lifeline Advisor. The following values are valid:
- PRIMARY (1)
- SECONDARY (2)

Workload Lifeline Advisor Correlator For NetView product internal use.

Workload Lifeline Agents The number of Multi-site Workload Lifeline Agents that are connected to the Multi-site Workload Lifeline Advisor. This attribute is not applicable for secondary Multi-site Workload Lifeline Advisors.

zOS Image Name The name of the z/OS operating system where the Multi-site Workload Lifeline Advisor resides.

Workload Lifeline Agents Attributes

Use these attributes to view all Multi-site Workload Lifeline Agents in both the active and standby sites that are gathering server capacity and health information for registered servers and reporting back to the primary Multi-site Workload Lifeline Advisor.

Note: This attribute group is used with the GDPS Active/Active Continuous Availability solution.

Agent State The state of the Multi-site Workload Lifeline Agent. The following values are valid:
- ACTIVE (1)
- INACTIVE (2)

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

IP Address The IP address of the Multi-site Workload Lifeline Agent.

Monitored Servers The number of server applications that are being monitored by this Multi-site Workload Lifeline Agent.

Origin Node The parent node of the workspace.

Site Name The name of the site (for example, the sysplex name) where the Multi-site Workload Lifeline Agent resides.

Workload Lifeline Advisor Correlator For NetView product internal use.

Workload Lifeline Agent Correlator For NetView product internal use.

zOS Image Name The name of the z/OS operating system where the Multi-site Workload Lifeline Agent resides.

Workload Servers Attributes

Use these attributes to view all servers that make up the defined workloads in both active and standby sites.

Note: This attribute group is used with the GDPS Active/Active Continuous Availability solution.

Abnormal Terminations The rate of abnormal transaction completions per 1000 transactions for this server application. This value is optionally supplied by server applications to the Workload Manager, which uses it to adjust the reported WLM weight.

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Communications Server Health The health of the server application as determined by TCP/IP. The value is calculated based on how well the server keeps up with new connection requests on the backlog of the server, how well the server establishes new connections, and whether the server drops connections. This value is treated as a percentage and is used to adjust the net weight.

CPU Weight The CPU factor in the WLM weight. This is the amount of displaceable general CPU capacity based on the importance of the server application as compared to other server instances (active on the same site) that are defined for this workload and modified by the proportion of general CPU capacity that is used by this server, as compared to zAAP and zIIP processors.

IP Address The IPv4 or IPv6 address of a server application that is defined for the workload.

IP Address Port For NetView product internal use. This attribute is the concatenation of the IP Address and Port attribute values and is used to depict the x-axis in the bar chart view. The format of the concatenated values is *ip*:*port*, where *ip* is the IP Address value and *port* is the Port value.

Job Name The MVS job name of the server application.

Net Weight The net weight for this server application relative to other server instances that are defined for this workload on the same site. This value is calculated by applying the Communications Server health as a percentage of the WLM weight for this server. It is then normalized against the other server instances (active on this same site) that are defined for this workload.

Origin Node The parent node of the workspace.

Port The number of the port on which the server application listens.

Server Correlator For NetView product internal use.

Server Health The health indicator of the server application. This indicator is available only for servers that provide this information to Workload Manager. For servers that are healthy or are not reporting this information, a value of 100 is returned. This value is treated as a percentage and is used to adjust the reported WLM weight.

Server State The state of the server application. The following values are valid:
- ACTIVE (1)
- INACTIVE (2)

Site Name The name of the site (for example, the sysplex name) where the server application resides.

WLM Weight The Workload Manager (WLM) weight value for the server application. This value is a measure of how well the server application is meeting the WLM policies of the server application. It represents the amount of displaceable processor capacity based on the importance of the server application as compared to other server instances (active on this same site) that are defined for this workload. The WLM weight is a composite weight and includes the sum of the CP, zAAP, and zIIP weights.

Workload Correlator For NetView product internal use.

Workload Lifeline Advisor Correlator For NetView product internal use.

ZAAP Weight The zAAP factor in the WLM weight. This is the amount of displaceable zAAP capacity based on the importance of the server application as compared to other server instances (active on this same site) that are defined for this workload and modified by the proportion of zAAP capacity that is used by this server, as compared to general CPU and zIIP processors.

ZIIP Weight The zIIP factor in the WLM weight. This is the amount of displaceable zIIP capacity based on the importance of the server application as compared to other server instances (active on this same site) that are defined for this workload and modified by the proportion of zIIP capacity that is used by this server, as compared to general CPU and zAAP processors.

zOS Image Name The name of the z/OS operating system where the server application resides.

Workload Sites Attributes

Use these attributes to view all the sites for the selected workload.

Note: This attribute group is used with the GDPS Active/Active Continuous Availability solution.

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Origin Node The parent node of the workspace.

Site Correlator For NetView product internal use.

Site Name The name of the site where the workload might be active.

Workload Correlator For NetView product internal use.

Workload Routing State The routing state of the workload on this site. The following values are valid:

- ACTIVE (1): If the workload is active on this site, this is the active site.
- QUIESCED (2): If the workload is quiesced on this site, this is the standby site.

  Note: If the workload is quiesced on both sites, the workload on the active site might not be activated yet.

Workload Routing Weight The routing weight of the workload on this site.

Workloads Attributes

Use these attributes to view all workloads that are defined for the GDPS Active/Active Continuous Availability solution.

Note: This attribute group is used with the GDPS Active/Active Continuous Availability solution.

Collection Time The date and time of the data sampling. By default, this value is displayed as *MM*/*DD*/*YY* *hh*:*mm*:*ss*, where *MM* is the month, *DD* is the day, *YY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second.

Detected Failure The monitoring component that detected a failure when the Workload Status attribute value is UNSATISFACTORY. The following values are valid:
- BOTH
- NONE
- REPLICATION
- ROUTING

Load Balancer Correlator For NetView product internal use.

Origin Node The parent node of the workspace.

Role The role of the workload. The following value is valid:
- ACTIVE/STANDBY (1)

Servers The number of servers that make up the workload.

Workload Correlator For NetView product internal use.

Workload Name The name of the workload.

Workload Status The overall status of the workload. This value is calculated from the workload status that is reported by the Multi-site Workload Lifeline product and the workload status that is reported by the replication server that is associated with the workload. The following values are valid:
- SATISFACTORY (1): Both statuses are satisfactory.
- UNSATISFACTORY (2): At least one of the statuses is unsatisfactory.

Appendix D. Workspaces and Attribute Groups

The NetView for z/OS Enterprise Management Agent provides workspaces that display attribute groups that can be altered or replaced to meet your needs. The attribute group is used for situation and query editing and, if applicable, for configuring historical data.

For the NetView for z/OS Enterprise Management Agent workspaces that are accessed from the Navigator view, Table 8 shows the attribute group descriptions, the attribute groups, and the attribute group table identifiers.

Table 8. Navigator Workspaces Mapped to Attribute Groups

Workspace	Attribute Group Description	Attribute Group Name	Attribute Group Table Identifier
Application-Instance DVIPA	DVIPA Definition and Status	NA DVIPA Definition and Status	KNADDS
Distributed DVIPA Server Health	Distributed DVIPA Server Health	NA DDVIPA Server Health	KNADSH
Distributed DVIPA Targets	Distributed DVIPA Targets	NA DDVIPA Targets	KNADTA
Distributed DVIPA Unhealthy Servers	Distributed DVIPA Server Health	NA DDVIPA Server Health	KNADSH
DVIPA Connections	Active DVIPA Connection Count	NA DVIPA Connection Count	KNADCA
	DVIPA Connections	NA DVIPA Connections	KNADCO
DVIPA Definition and Status	DVIPA Definition and Status	NA DVIPA Definition and Status	KNADDS
DVIPA Sysplex Distributors	DVIPA Sysplex Distributors	NA DVIPA Sysplex Distributors	KNADSD
HiperSockets Configuration and Status	HiperSockets Configuration and Status	NA HiperSockets Config and Status	KNAHIP
Inactive TCPIP Connection Data	Inactive TCPIP Connection Count	NA Inactive TCPIP Connection Count	KNATCJ
	Inactive TCPIP Connection Data	NA Inactive TCPIP Connection Data	KNATCI
* Load Balancers	Load Balancers	NA Load Balancers	KNAWL5
NetView Applications	NetView Applications	NA NetView Applications	KNAAPP
NetView Audit Log	NetView Audit Log	NA NetView Audit Log	KNANAL
NetView Command Response	NetView Command Response	NA NetView Command Response	KNACMR
NetView Log	NetView Log	NA NetView Log	KNANLG
NetView Tasks	NetView Tasks	NA NetView Tasks	KNAHEA
OSA Channels and Ports	OSA Channels and Ports	NA OSA Channels and Ports	KNAOSP
* Replication Servers	Replication Servers	NA Replication Servers	KNARSC
Session Data	Active Session Count	NA Session Count	KNASEA
	Session Data	NA Session Data	KNASED
Stack Configuration and Status	Stack Configuration and Status	NA Stack Configuration and Status	KNASCS
Stack-Defined DVIPA	DVIPA Definition and Status	NA DVIPA Definition and Status	KNADDS

Table 8. Navigator Workspaces Mapped to Attribute Groups (continued)

Workspace	Attribute Group Description	Attribute Group Name	Attribute Group Table Identifier
TCPIP Connection Data	Active TCPIP Connection Count	NA TCPIP Connection Count	KNATCA
	TCPIP Connection Data	NA TCPIP Connection Data	KNATCO
Telnet Server Configuration and Status	Telnet Server	NA Telnet Server	KNATAS
	Telnet Server Port	NA Telnet Server Port	KNATCS
* Workload Lifeline Advisors	Workload Lifeline Advisors	NA Workload Lifeline Advisors	KNAWL1
* Workload Lifeline Agents	Workload Lifeline Agents	NA Workload Lifeline Agents	KNAWL4
* Workload Servers	Workload Servers	NA Workload Servers	KNAWL7
* Workloads	Workloads	NA Workloads	KNAWL2
Note: An asterisk (*) in front of the workspace name indicates a workspace for the GDPS Active/Active Continuous Availability solution, for example, * Load Balancers.			

For the NetView for z/OS Enterprise Management Agent workspaces that are accessed only by linking from other workspaces, Table 9 shows the attribute group descriptions, the attribute groups, and the attribute group table identifiers.

Table 9. Linked Workspaces Mapped to Attribute Groups

Workspace	Attribute Group Description	Attribute Group	Attribute Group Table Identifier
* DB2 Replication Details	DB2 Replication Apply Server	NA DB2 Replication Apply Server	KNARD3
	DB2 Replication Apply Workload	NA DB2 Replication Apply Workload	KNARD4
	DB2 Replication Capture Server	NA DB2 Replication Capture Server	KNARD1
	DB2 Replication Capture Workload	NA DB2 Replication Capture Workload	KNARD2
Distributed DVIPA Connection Routing	Distributed DVIPA Connection Routing	NA DDVIPA Connection Routing	KNADCR
Distributed DVIPA Server Health Details	Distributed DVIPA Server Health	NA DDVIPA Server Health	KNADSH
DVIPA Stack Summary	DVIPA Definition and Status	NA DVIPA Definition and Status	KNADDS
	DVIPA Sysplex Distributors	NA DVIPA Sysplex Distributors	KNADSD
	Distributed DVIPA Targets	NA DDVIPA Targets	KNADTA
DVIPA Workload	Distributed DVIPA Targets	NA DDVIPA Targets	KNADTA
Filtered Distributed DVIPA Server Health	Distributed DVIPA Server Health	NA DDVIPA Server Health	KNADSH
Filtered Distributed DVIPA Targets	Distributed DVIPA Targets	NA DDVIPA Targets	KNADTA
Filtered Distributed DVIPA Unhealthy Servers	Distributed DVIPA Server Health	NA DDVIPA Server Health	KNADSH
Filtered DVIPA Connections	Active DVIPA Connection Count	NA DVIPA Connection Count	KNADCA
	DVIPA Connections	NA DVIPA Connections	KNADCO

Table 9. Linked Workspaces Mapped to Attribute Groups (continued)

Workspace	Attribute Group Description	Attribute Group	Attribute Group Table Identifier
Filtered DVIPA Definition and Status	DVIPA Definition and Status	NA DVIPA Definition and Status	KNADDS
Filtered DVIPA Sysplex Distributors	DVIPA Sysplex Distributors	NA DVIPA Sysplex Distributors	KNADSD
Filtered Inactive TCPIP Connection Data	Inactive TCPIP Connection Count	NA Inactive TCPIP Connection Count	KNATCJ
	Inactive TCPIP Connection Data	NA Inactive TCPIP Connection Data	KNATCI
* Filtered Replication Servers	Replication Servers	NA Replication Servers	KNARSC
Filtered Session Data	Active Session Count	NA Session Count	KNASEA
	Session Data	NA Session Data	KNASED
Filtered TCPIP Connection Data	Active TCPIP Connection Count	NA TCPIP Connection Count	KNATCA
	TCPIP Connection Data	NA TCPIP Connection Data	KNATCO
Filtered Telnet Server Configuration and Status	Telnet Server	NA Telnet Server	KNATAS
	Telnet Server Port	NA Telnet Server Port	KNATCS
* Filtered Workload Servers	Workload Servers	NA Workload Servers	KNAWL7
* Filtered Workloads	Workloads	NA Workloads	KNAWL2
* IMS Replication Details	IMS Replication Apply Details	NA IMS Replication Apply Details	KNARI2
	IMS Replication Capture Details	NA IMS Replication Capture Details	KNARI1
* Load Balancer Groups	Load Balancer Groups	NA Load Balancer Groups	KNAWL6
* Load Balancer Workloads	Load Balancer Groups	NA Load Balancer Groups	KNAWL6
NetView Task Details	NetView Tasks	NA NetView Tasks	KNAHEA
Session Data by Name	Session Data	NA Session Data	KNASED
VIPA Routes	VIPA Routes	NA DVIPA Routes	KNADRT
* Workload Server Details	Workload Servers	NA Workload Servers	KNAWL7
* Workload Site Details	Workload Sites	NA Workload Sites	KNAWL3
* Workload Sites	Workload Sites	NA Workload Sites	KNAWL3
Note: An asterisk (*) in front of the workspace name indicates a workspace for the GDPS Active/Active Continuous Availability solution, for example, * DB2 Replication Details.			

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Programming Interfaces

This publication documents information that is NOT intended to be used as Programming Interfaces of Tivoli NetView for z/OS.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml .

Adobe is a trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of IBM or other companies.

Index

Product Number: 5697-NV6

Printed in USA

SC27-2876-00