

Chapter 6



Supported Monitors and Tests

6.1 Overview

A **monitor** is a process that runs one or more categories of tests with similar functions. Each type of test is identified by the name of the monitor that runs it and the **Test Subtype**, a unique identifier within the monitor.

For example, the Port Monitor can run tests of several subtypes: FTP, HTTP, HTTPS, IMAP, IMAPS, etc. When you create a new FTP test for a device, Helix uses the test's Test Type/Subtype combination (Port/FTP) to look up provisioning information for this category of tests.

Helix provides standard monitors for network, servers and applications. (You can easily add new monitors with the plugin framework described in Chapter 12, "Plugin Monitors"). Efficient and multi-threaded, the standard monitors are designed to minimize the impact of traffic monitoring on your network. The use of Helix tests does not result in a significant increase in resource utilization for the devices being polled because default time intervals are set to provide an accurate picture of device functioning without burdening the system.

Helix is designed to work with SNMP agents such as Empire, UCD, or BMC Patrol, and recognizes MIBs from a variety of standard devices such as Compaq servers and Cisco routers. Note that while information can be gathered from a device's private MIB, some MIBs do not provide enough information to enable the same array of tests that a standard SNMP agent would allow.

Helix's SNMP monitor is an extremely fast, multi-threaded poller with support for 64bit counters where available and also account for the rollover of 32bit counters. Multiple SNMP queries to the same host are sent in the same SNMP packet for speed and optimization. An alternate SNMP port can be queried instead of the default if needed.

In addition to using Helix's standard monitors, you can also use the plugin framework to create new ones very easily as described in Chapter 12, "Plugin Monitors".

6.2 Available Monitors

6.2.1 Network Monitors

Frame Relay

Measure parameters on frame relay such as DLCI status, discards, traffic, FECN, BECN.

ICMP Packet Loss

Verify that the network hosts are available and reachable via the network and also indicate if reachability is degraded. Five packets are sent, and the packet loss is reported as a percentage.

ICMP Round Trip Time

Measure the response time (in milliseconds) of ICMP ping packets to detect network latency. 5 packets are sent in each pass and the average of these five packets is calculated for each test.

Bandwidth Utilization

Measure the traffic (bytes) transmitted between each test interval, and calculate the percentage utilization based on the maximum bandwidth of the interface.

Throughput on Network Interface

Measure the number of packets per second (PPS) sent between each test interval.

Interface Errors

Calculate CRC error rate and discards (per minute) calculated by the delta between sample intervals.

6.2.2 Server Monitors**CPU load**

Report on the percentage of CPU in use (average over past minute) to detect overloaded servers. Note that occasional spikes in CPU load is normal.

Disk space

Report on the percentage of disk space currently in use for each partition.

Physical Memory Usage

Measure percentage of physical memory used. Note that some operating systems use any 'available' physical memory for I/O buffers and hence the percentage of physical memory used will always be high.

Virtual Memory

Report on the number of page swaps per unit time. Paging is a normal phenomenon, but excessive swapping is bad and indicates that the system requires additional physical memory.

6.2.3 Application Monitors

NOTE: the monitors marked with an asterisk are available as a separately licensed feature.

*** Oracle database**

Monitor database status, transaction rate, disk reads & writes, page reads & writes, out of space errors, query rate, committed transactions, aborted transactions, table status, table utilization, datafile reads & writes, replication status, listener status, SID connections.

*** Apache Web Server**

Report on web server traffic, utilization, requests per second, average data bytes per request

*** Microsoft SQL Server**

Measure the status, page reads, TDS packets, threads, page faults, connected users, lock timeouts, deadlocks, cache hit ratio, disk space utilization, transaction rate, log space utilization, replication rate.

*** Microsoft Exchange Server**

Measure traffic, ExDS statistics, Address book Connections, ExDS metrics, MTS, LDAP queries, queue, SMTP connections, failed connections, thread pool usage, failures, disk operations.

*** Microsoft Internet Information Server**

Monitor the traffic, files transferred, active users, active connections, throttled requests, rejected requests, 404 errors, and breakdown on the request types (GET, POST, HEAD, PUT, CGI).

*** DHCP Monitor**

Check if DHCP service on a host is available, whether it has IP addresses available for lease and how long it takes to answer a lease request, request statistics such as discover, release, ack, nak requests.

HTTP

Monitors the availability and response time of HTTP Web servers. Checks for error responses, incomplete pages.

HTTPS

Secure HTTP- This monitor supports all of the features of the HTTP monitor, but also supports SSL encapsulation, in which case the communication is encrypted using SSLv2/SSLv3 protocols for increased security. The monitor will establish the SSL session and then perform HTTP tests to ensure service availability.

SMTP Server

Simple Mail Transport Protocol - Monitors the availability and response time of any mail transport application that supports the SMTP protocol (Microsoft Exchange, Sendmail, Netscape Mail.)

POP3 Server

Monitors the availability and response time of POP3 E-mail services. If legitimate username and password is supplied, will login and validate server response.

IMAP4 Server

Internet Message Access Protocol - Monitors the availability and response time of IMAP4 E-mail services. If legitimate username and password is supplied, will login and validate server response.

IMAPS

Secure IMAP- This monitor supports all of the features of the IMAP monitor, but also supports SSL encapsulation, in which case the communication is encrypted using SSLv2/SSLv3 protocols for increased security. The monitor will establish the SSL session and then perform IMAP tests to ensure service availability.

FTP Server

File Transport Protocol - Monitors the availability and response time of FTP port connection. Connection request sent, receives OK response and then disconnects. If legitimate username and password is supplied, will attempt to login and validate server response.

NNTP News Server

Connects to the NNTP service to check whether or not Internet newsgroups are available, receives OK response and then disconnects.

Generic Port

Monitor the response time for any TCP port, and report a failure if supplied response string is not matched in the server reply.

*** NTP**

Monitors time synchronization service across the network by querying the NTP service on any server and returning the stratum value. If the stratum is below the configured thresholds, an error is reported.*

*** RADIUS**

Remote Authentication Dial-In User Service (RFC 2138 and 2139) - performs a complete authentication test against a RADIUS service, checking the response time for user logon authentication to the ISP platform. Required input: secret, port number, username and password.

*** DNS**

Domain Name Service (RFC 1035) - uses the DNS service to look up the IP addresses of one or more hosts. It monitors the availability of the service by recording the response times and the results of each request.

6.2.4 Custom Monitors

You can extend Helix's monitoring capabilities using the plugin monitor framework. You can write a custom monitor using any programming language and add to Helix. See Chapter 12, "Plugin Monitors"