halcyon software

guide to IBM Service Monitoring templates
Copyright

Copyright 2010 - 2014 Halcyon Software Limited. All rights reserved.
This document is intended as a guide to the reports generated by using Halcyon software.
This documentation contains Halcyon proprietary and confidential information and may not be
disclosed, used, or copied without the prior consent of Halcyon Software Limited, or as set forth
in the applicable license agreement. Users are solely responsible for the proper use of the
software and the application of the results obtained.
Although Halcyon Software Limited has tested the software and reviewed the documentation,
the sole warranty for the software may be found in the applicable license agreement between
Halcyon Software Limited and the user.
Publication Revision: November 2014

Overview

Halcyon Templates are designed to provide the same level of monitoring across a number of
similar devices by applying a set of user-defined filters with a single-click. This greatly reduces
set-up time and ensures all systems are covered by at least a basic level of monitoring.
Should you need to make a system-wide change at a later date, a single update covers all
systems using the template.

Halcyon IBM i Templates also are available for the following specialized environments:
• Lawson M3 (Movex)
• Misys
• Misys Midas Plus
• JD Edwards
• Maxava
• Quick/EDD
• SAP
• Infor XA
• Infor System21
If you already use any of Halcyon's Level 1 to 4 software suites then follow these instructions to install templates to a customized environment on the IBM i.

If you do not currently use Halcyon's tools in your IBM environment but wish to have more information, an on-line demonstration or a free trial then please see the list of contacts on the back page of this guide.

### Installation of Customized Environment

Follow these instructions to install templates to a customized environment.

1. Install the Halcyon solution, using the appropriate installation guide.

2. Once successfully installed, log into the environment to which you wish to apply the customized template, for example, HALPROD/HALCYON.

3. From the command line run `ENDMON` and press F4. Follow the prompts to complete the ending of the monitors.

   **Note:** The installation of the customized environment fails if the monitors are not stopped.

4. From the command line type `CSTENV` and press F4.

5. Type the required authorization code for the template you wish to apply and press Enter.
Enter the customization code

Note: Each customized environment requires an authorization code. Please contact technicalservices@halcyonsoftware.com or your local Halcyon office or reseller for details on how to obtain this code.

The Customized environment is now installed.

6 From the main menu of your Halcyon solution, select option 5=Work with Rules. The template rules applicable to the customized environment that you installed can be found in the listed queue and rule groups. Default action schedules are installed and additionally, where appropriate, changes to system defaults may also be made.

In most cases, the templates supplied can be used immediately upon completion of installation, but there may be instances where you need to change rule properties to match those of your own environment. This can be done by taking option 2=Change against the rule and making the required changes. Similarly, should you require multiple rules for different message queues or devices and so on you can use option 3=Copy against the rule and then make the required amendments.
Rule Actions

Unless otherwise specified, all template rules are implemented with a default action schedule which sends an alert message to your local console (option 10=Message Console from the main menu). Should you wish to amend this option, take option 2=Change against the action within the rule and make the amendments as required.

Note: Please refer to the user reference guide for your Halcyon solution for details of actions that may be applied to rules.
IBM Service Monitoring templates allow you to check that all critical IBM i ports, required for the continued running of vital services are open and available. The template also contains a series of performance monitors to keep a constant check to ensure important service jobs are active or inactive as required. The combined set of IBM Service Monitoring templates consists of 231 separate rules to instantly alert you to any issues that may arise.

TCP/IP Rules

SERVICES Check service port listening
This rule group contains 103 IBM Service Monitoring customization rules that can be used to monitor critical IBM i ports.

Tomcat basic servlet & JSP engine Apache Web Server
The IBM i implementation of Apache Software Foundation (ASF) Jakarta Tomcat servlet engine provides a lightweight servlet engine that supports servlets, JavaServer pages (JSPs), and Web application archive (WAR) files. The HTTP Server for IBM i supports a module (mod_jk) that allows communication between the HTTP Server (powered by Apache) and ASF Tomcat.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 8009, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct address parameters for your organization.
BootP DHCP Relay Agent & Svr (port 67/dhcp/bootps)
i5/OS® provides a DHCP/BOOTP relay agent that can be used to forward DHCP packets to a DHCP server on a different network.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 67, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct address parameters for your organization.

BootP DHCP Relay Agent (port 942)
The BootP DHCP Relay Agent forwards Bootstrap Protocol (BootP) and Dynamic Host Configuration Protocols (DHCP) packets from the local system to one or more different DHCP servers.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 942, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

Central Server Agent (port 8470/as-central)
Non-SSL communication with the IBM i central server job. Central server is used when a Client Access license is required, and also for downloading translation tables.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 8470, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

Central Server Agent (port 9470/as-central-s)
Non-SSL communication with the IBM i central server job. Central server is used when a Client Access license is required, and also for downloading translation tables.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 9470, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.
CIM Object Manager (port 5988/wbem-http)
The CIM Object Manager manages CIM objects on a WBEM-enabled system. A CIM object is a representation, or model, of a managed resource, such as a printer, disk drive, or CPU. CIM objects are stored internally as Java classes. CIM Object Manager listens for XML/HTTP connections on HTTP port 5988. This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed. By default, the rule checks Local port number 5988, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

Cluster Resource Services (port 657)
Cluster Resource Services consists of a set of multi-threaded jobs. When clustering is active on an IBM i, the jobs will be run in the QSYSWRK subsystem. The jobs run using the QDFTJOBD job description. This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed. By default, the rule checks Local port number 657, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

Database Server Daemon (port 8471/as-database)
Database server is used for accessing the IBM i database, the daemon running as a background process. This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed. By default, the rule checks Local port number 8471, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

Database Server Daemon (port 8478/as-transfer)
Database server is used for accessing the IBM i database, the transfer process being used to transfer data from one database to another. This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed. By default, the rule checks Local port number 8478, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.
**Database Server Daemon (port 9471/as-database)**
Database server is used for accessing the IBM i database, the daemon running as a background process.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 9471, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**Data Queue Server Daemon (port 8472/as-dtaq)**
A data queue is an object that is used by IBM i application programs for communications. Applications can use data queues to pass data between jobs. Multiple iSeries jobs can send or receive data from a single data queue.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 8472, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**Data Queue Server Daemon (port 9472/as-dtaq-s)**
A data queue is an object that is used by IBM i application programs for communications. Applications can use data queues to pass data between jobs. Multiple iSeries jobs can send or receive data from a single data queue.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port 8472, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**DNS Server (port 53/domain)**
Port 53 is the common port for the Domain Name Service.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port 53, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**Domino Server (port 1532)**
IBM Domino (formerly IBM Lotus Domino) is an IBM server product that provides enterprise-grade e-mail, collaboration capabilities, and a custom application platform.
This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 1532, Remote system *INADDR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**DRDA DDM Server TCP/IP Listener (port 446/drda)**
The DRDA (Distributed database programming) / DDM (Distributed data management server) allows clients access to the functions included with DB2 UDB for IBM i.

The DRDA TCP/IP server listens on port 446 (the well-known DRDA port).

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 446, Remote system *INADDR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**DRDA DDM Server TCP/IP Listener (port 447/ddm)**
The DRDA (Distributed database programming) / DDM (Distributed data management) server allows clients access to the functions included with DB2 UDB for IBM i.

The DDM TCP/IP server listens on port 447 (the well-known DDM port).

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 447, Remote system *INADDR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**DRDA DDM Server TCP/IP Listener (port 448/ddm-ssl)**
The DRDA (Distributed database programming) / DDM (Distributed data management server) allows clients access to the functions included with DB2 UDB for IBM i.

The DDM-SSL TCP/IP server listens on port 448 (the well-known SSL port).

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 448, Remote system *INADDR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.
Extended Dynamic Remote SQL (port 4402/as-edrsql)
The Extended Dynamic Remote SQL server (QXDAEDRSQL) supports remote iSeries SQL access and other database functions. The QXDAEDRSQL server allows clients access to DB2 UDB functions.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 4402, Remote system *INNTENADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

File Server Daemon & Svr (port 8473/as-file)
Port 8473 uses the vp2p protocol for service type vp2p. A malformed request to port 8473 is known to cause denial of service attacks.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 8473, Remote system *INNTENADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

File Server Daemon & Svr (port 8477/as-netdrive)
The server daemon allows client applications to start communications with a host server that is using sockets communications support.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 8477, Remote system *INNTENADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

File Server Daemon & Svr (port 9473/as-file-s)
The server daemon allows client applications to start communications with a host server that is using sockets communications support. Port 9473 is the secure port connection.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 8477, Remote system *INNTENADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.
FTP (port 21/ftp-control)
The FTP server provides enhanced security while sending and receiving files over a untrusted network. FTP server uses Secure Sockets Layer (SSL) to secure passwords and other sensitive data during an information exchange. A client can connect to a non-encrypted TCP port (usually TCP port 21) and then negotiate authentication and encryption options.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 21, Remote system *INETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

FTP (port 990/ftps-control)
Most SSL-enabled applications connect a client to separate TCP ports, one port for "unprotected" sessions and the other for secure sessions. A client can choose a secure FTP port (usually TCP port 990), where connections are assumed to be SSL. The IBM i FTP server provides for both of these options.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 990, Remote system *INETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

Graphical Debug Server - Hub (port 4026/as-debug)
Graphical IBM i debugger can be regarded as the graphical version of traditional the green screen debugger for IBM i.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 4026, Remote system *INETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

HTTP Server (port 80/www-http)
Port 80 is used by the HyperText Transport Protocol (HTTP). HTTP is the protocol websites and web browsers use to communicate with each other.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 80, Remote system *INETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.
HTTP Server (port 2001/as-admin-http)
Port 2001 is used on the IBM i as a non-secure HTTP connection for the IBM Web Administration interface.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 2001, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

HTTP Server (port 2010/as-admin-https)
Port 2010 is used on the IBM i as a secure HTTP connection for the IBM Web Administration interface.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 2010, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

IBM Director (port 14247)
IBM® Systems Director processes require access to a number of ports on managed systems. Managed systems include Common Agent managed systems, Platform Agent managed systems, and Agentless managed systems. Port 14247 is used for inbound interprocess communication (IPC) with IBM Director Agent.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Port 14247, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

IBM Director (port 14248)
IBM® Systems Director processes require access to a number of ports on managed systems. Managed systems include Common Agent managed systems, Platform Agent managed systems, and Agentless managed systems. Port 14248 is used for outbound interprocess communication (IPC) with IBM Director Agent.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 14248, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.
IBM Directory Server (port 389/ldap)
By default, port TCP port 389 is used by IBM Tivoli Directory Server running a Lightweight Directory Access Protocol (LDAP). This port is unsecured.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 389, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

IBM Directory Server (port 636/ldaps)
By default, port TCP port 636 is used by IBM Tivoli Directory Server running a Lightweight Directory Access Protocol (LDAP). This port is secured.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 636, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

InfoPrint Server Font Downloader (port 8251)
IBM Infoprint Server provides essential electronic delivery options for IBM i along with the capabilities to consolidate network printing on the IBM i.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 8251, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

INETD Super Server (port 13/daytime)
The Daytime Protocol is a service in the Internet Protocol Suite, intended for testing and measurement purposes in computer networks.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 13, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.
**INETD Super Server (port 37/time)**

Time is a daemon process that runs for the internal system on port 37 for machine formatted time.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 37, Remote system *INNINETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**Web PDF Server (port 8490/as-iwapdfsrv)**

The Web PDF Server is used when any user needs to transform a spooled file to PDF using InfoPrint Server support.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 8490, Remote system *INNINETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**NetServer Daemon (port 137 TCP/netbios-ns)**

NetBIOS is an API providing various networking services. The NetBIOS Name Service is part of the NetBIOS-over-TCP protocol suite and is a service providing name lookup, registration, and so on.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 137, Remote system *INNINETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**NetServer Daemon (port 139 TCP/netbios-ssn)**

NetBIOS is an API providing various networking services. The NetBIOS Session Service mode lets two computers establish a connection, allows messages to span multiple packets, and provides error detection and recovery.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 139, Remote system *INNINETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.
**NetServer Daemon (port 445 TCP/cifs)**
NetBIOS is an API providing various networking services. Port 445 is used to provide a direct TCP connection to a Common Internet File System (CIFS) which is the standard way that computer users share files across corporate intranets and the Internet.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 445, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**TCP/IP Tape Server (port 3494/IBM3494)**
The 3494 tape library requires a communications line for the Library Manager functions.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 3494, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**Line Printer Daemon (port 515/lpd)**
The Line Printer Daemon protocol/Line Printer Remote protocol (or LPD, LPR) is a network protocol for submitting print jobs to a remote printer. A server for the LPD protocol listens for requests on TCP port 515.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 515, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**Management Central Svr (port 5544/as-mgtcrlj)**
Management Central is a three tier distributed architecture that hosts a set of IBM i Systems Management applications. Management Central encompasses the C++ and Java (TM) based class infrastructures implemented within IBM i Navigator Graphical Clients, IBM i MC Central System Servers and IBM i MC Endpoint System Servers.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 5544, Remote system *INTNETADR, and Remote internet address 0.0.0.0.
The Remote internet address setting will need changing to the correct parameters for your organization.

Management Central Svr (port 5555/as-mgtctrl)
Management Central is a three tier distributed architecture that hosts a set of IBM i Systems Management applications. Management Central encompasses the C++ and Java (TM) based class infrastructures implemented within IBM i Navigator Graphical Clients, IBM i MC Central System Servers and IBM i MC Endpoint System Servers.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 5555, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

Management Central Svr (port 5566/as-mgtctrl-ss)
Management Central is a three tier distributed architecture that hosts a set of IBM i Systems Management applications. Management Central encompasses the C++ and Java (TM) based class infrastructures implemented within IBM i Navigator Graphical Clients, IBM i MC Central System Servers and IBM i MC Endpoint System Servers.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 5566, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

Management Central Svr (port 5577/as-mgtctrl-cs)
Management Central is a three tier distributed architecture that hosts a set of IBM i Systems Management applications. Management Central encompasses the C++ and Java (TM) based class infrastructures implemented within IBM i Navigator Graphical Clients, IBM i MC Central System Servers and IBM i MC Endpoint System Servers.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default the rule checks Local port number 5577, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.
MQ Series Server (port 1414)
The default WebSphere® MQ listener is set up on the port number that you specify when setting up the client-connection channel. By default the listener will listen on port 1414.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 1414, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

Network Print Svr (port 8474/as-netprt)
The Print Server on port 8474 is used internally for Network Printer Services.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 8474, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

Network Print Svr (port 8479/as-vrtprint)
Port 8479 is used as the communication port for a virtual printer.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 8479, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

Network Print Svr (port 9474/as-netprt-s)
Port 9474 is used as the communication port for a secure network printer.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.
By default the rule checks Local port number 9474, Remote system *INNTETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

Network Station Login Daemon (port 256)
The Network Station Manager is a piece of software running on the boot server. It has a web interface and allows you to administrate all your Network Stations from a single point. The Login Daemon should run continuously to handle periodic service requests that it is expected to receive.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 256, Remote system *INNTETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

OnDemand Daemon (port 1445)
The OnDemand Server lets you store large amounts of historical data on a disk, high-capacity optical volumes, or tape. It also provides quick access to stored data by online retrieval. The Login Daemon should run continuously to handle periodic service requests that it is expected to receive.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 1445, Remote system *INNTETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

OnDemand Common Server (port 1450)
OnDemand servers manage control information and index data, store and retrieve documents and resource group files, and process query requests from OnDemand client programs.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 1450, Remote system *INNTETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

OnDemand Server (port 1445)
OnDemand servers manage control information and index data, store and retrieve documents and resource group files, and process query requests from OnDemand client programs.
This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 1445, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**POP (port 110/pop3)**

For POP3 clients to access mail files on the server, you must enable a POP3 port on the server. By default, the IBM® Lotus® Domino® POP3 service uses TCP/IP port 110.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 110, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**QoS RSVP Agent (port 1698)**

RSVP is a receiver-oriented signaling protocol that enables applications to request Quality of Service on an IP network.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 1698, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**Remote Command Svr Daemon (port 8475/as-rmtcm)**

The remote command and distributed program call server support allows users and applications to issue IBM i CL commands and call programs. This support allows the user to run multiple commands in the same job.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 8475, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**Remote Command Svr Daemon (port 9475/as-rmtcm)**

The remote command and distributed program call server support allows users and applications to issue IBM i CL commands and call programs. This support allows the user to run multiple commands in the same job. Port 9475 is used as a secure connection for this daemon.
This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 9475, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**Remote Execution (port 512/exec)**
Remote Execution allows you to execute shell commands on a remote computer.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 512, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**RouteD (port 520/routed)**
The Routing Information Protocol (RIP) is a distance-vector routing protocol, which employs the hop count as a routing metric. RIP uses the User Datagram Protocol (UDP) as its transport protocol, and is assigned the reserved port number 520.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 520, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**Remote Procedure Call (port 111/sunrpc)**
SunRPC (Sun Remote Procedure Call) is a common Unix protocol used to implement many services including NFS.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 111, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**Secure Shell Daemon (port 22/ssh)**
Secure Shell (SSH) is a cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services between two networked computers that connects, via a secure channel over an insecure network, a server and a client (running SSH server and SSH client programs, respectively).
This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 22, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**Server Port Mapper (port 449/as-svrmap)**
The server mapper daemon is a batch job that runs in the QSYSWRK subsystem. It provides a method for client applications to determine the port number associated with a particular server. This job listens on a well-known port for a connection request from a client. The well-known port number for TCP/IP is 449.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 449, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**Signon Server Daemon (port 8476/as-signon)**
Sign-on server is used for every Client Access connection to authenticate users and to change passwords.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 8476, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**Signon Server Daemon (port 9476/as-signon-s)**
Sign-on server is used for every Client Access connection to authenticate users and to change passwords. Port 9476 is the secure port for this daemon service.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 9476, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**Simple Network Time Protocol (port 123/ntp)**
Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks and uses Port 123.
This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 123, Remote system *INFINETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**SMTP Server Daemon (port 25/smtp)**

SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. The daemon run continuously in the background to ensure that the STMP server is always available on Port 25.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 25, Remote system *INFINETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**SNMP Agent (port 161/snmp)**


This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 161, Remote system *INFINETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**SNMP Trap Manager (port 162/snmp-trap)**

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. The manager receives notifications (Traps and InformRequests) on Port 162.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 162, Remote system *INFINETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**TCP/IP L2TP Server (port 1701)**

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. L2TP uses Port 1701.
This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 1701, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**Telnet Server (port 23/telnet)**

Telnet is a client-server protocol, based on a reliable connection-oriented transport. Typically, this protocol is used to establish a connection to Transmission Control Protocol (TCP) port number 23, where a Telnet server application (telnetd) is listening.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 23, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**Telnet Server (port 992/telnet-ssl)**

This rule is essentially the same as the previous rule except that the port uses Secure Sockets Layer (SSL) technology.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 992, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**Triggered Cache Manager (port 7049)**

The Triggered Cache Manager (TCM) function provides a means to manage cached copies of static and dynamically produced Web pages including those generated by CGI programs, Net.Data®, or Java™ servlets. The TCP port value must be greater than 0 and less than 65536. The default port value is 7049.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 7049, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.
**Trivial FTP (port 69/tftp)**
Trivial File Transfer Protocol (TFTP) is a file transfer protocol notable for its simplicity. It is generally used for automated transfer of configuration or boot files between machines in a local environment. Data transfer is initiated on Port 69.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 69, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**WebFacing Server (port 4004/as-WebFacing)**
The WebFacing server acts as a gateway between WebSphere Application Server and your original iSeries application. When the WebFacing runtime server is started, if it does not see a WebFacing port definition as-WebFacing in WRKSRVTBLE, then the default port 4004 is used.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 4004, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**WebSphere Application Server V4 AE Admin Server (port 900)**
WebSphere Application Server (WAS) is a software product that performs the role of a web application server. More specifically, it is a software framework and middleware that hosts Java based web applications. By default the administrative console connects to the administrative server via port 900.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 900, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**WebSphere Application Server V4 AE Admin Server (port 9000)**
WebSphere Application Server (WAS) is a software product that performs the role of a web application server. More specifically, it is a software framework and middleware that hosts Java based web applications. By default the Location Service Daemon (LSD) runs on port 9000.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.
By default, the rule checks Local port number 9000, Remote system *
*INETADR, and Remote internet address 0.0.0.0. The Remote internet
address setting will need changing to the correct parameters for your
organization.

WebSphere Application Server V4 AE App Server (port 9080)
WebSphere Application Server (WAS) is a software product that performs the
role of a web application server. More specifically, it is a software framework
and middleware that hosts Java based web applications. By default the HTTP
Transport Port is 9080.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated
if the status changes since the last check was completed.

By default, the rule checks Local port number 9080, Remote system *
*INETADR, and Remote internet address 0.0.0.0. The Remote internet
address setting will need changing to the correct parameters for your
organization.

WebSphere Application Server V5 App Svr/Deploy Mgr (port 9090)
This is the TCP/IP port on which the Web container listens for requests for the
administrative application. You can specify this port with the administrative
console or with the CHGWASSVR script. By default the HTTP Administrative
console port (HTTP_TRANSPORT_ADMIN) is Port 9090.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated
if the status changes since the last check was completed.

By default, the rule checks Local port number 9080, Remote system *
*INETADR, and Remote internet address 0.0.0.0. The Remote internet
address setting will need changing to the correct parameters for your
organization.

WebSphere AS V5 Application Sever/Deploy Mgr (port 9043)
This is the secure TCP/IP port on which the Web container listens for secure
requests for the administrative application. You can specify this port with the
administrative console or with the chgwassvr script.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated
if the status changes since the last check was completed.

By default, the rule checks Local port number 9043, Remote system *
*INETADR, and Remote internet address 0.0.0.0. The Remote internet
address setting will need changing to the correct parameters for your
organization.

WebSphere AS V5 Application Server (port 2809)
In WebSphere Application Server V5 the administrative console connects to the
administrative server via port 2809. (This is a change from Port 900 in V4).

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated
if the status changes since the last check was completed.
By default, the rule checks Local port number 2809, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**WebSphere Application Server V5 App Server (port 8880)**
Simple Object Access Protocol (SOAP) port is used for communication between the development environment and the server. These ports are used for making Java™ Management Extensions (JMX) connections with the server. The default setting of the SOAP port is port 8880 and selected when working with a remote server.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 8880, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**WebSphere Application Server V5 App Server (port 9080)**
In WebSphere Application Server V5 the port on which the application server listens defaults to Port 9080.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 9080, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**WebSphere Application Server V5 App Server (port 7873)**
In WebSphere Application Server V5, the Data Replication Service (DRS) client address defaults to Port 7873.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 7873, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**WebSphere Application Server V5 App Server (port 5557)**
In WebSphere Application Server v5, the Java Messaging Service (JMS) server security port defaults to Port 5557.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.
By default, the rule checks Local port number 5557, Remote system "*INTERNETADR", and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**WebSphere Application Server V5 App Server (port 5558)**
WebSphere MQ Real-time Transport is a lightweight protocol optimized for use with nonpersistent messaging. It is used exclusively by Java Message Service (JMS) clients, and provides high levels of scalability and message throughput.

In WebSphere Application Server v5, the MQ Real-time Transport port defaults to Port 5558.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 5558, Remote system "*INTERNETADR", and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**WebSphere AS V5 App Server (port 5559)**
In WebSphere Application Server v5, the Java Messaging Service (JMS) server direct access defaults to Port 5559.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 5559, Remote system "*INTERNETADR", and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**WebSphere Application Server V5 App Server (port 9501)**
In WebSphere Application Server v5, the WebSphere Application Server secure association service defaults to Port 9501. This is the TCP/IP port on which the Secure Association Services (SAS) listen for inbound authentication requests.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 9501, Remote system "*INTERNETADR", and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**WebSphere Application Server V5 App Server (port 9502)**
In WebSphere Application Server v5, the WebSphere Application Server common secure port defaults to Port 9502. This is the TCP/IP port on which the Common Secure Interoperability Version 2 (CSIV2) Service listens for inbound client authentication requests.
This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 9502, Remote system *INETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**WebSphere Application Server V5 App Server (port 9503)**

In WebSphere Application Server v5, the WebSphere Application Server common secure port defaults to Port 9503. This is the TCP/IP port on which the Common Secure Interoperability Version 2 (CSIV2) Service listens for inbound server authentication requests.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 9503, Remote system *INETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**WebSphere Application Server V5 NDE App Server (port 9810)**

The WebSphere Application Server v5 Network Deployment Edition (NDE) uses Port 9810 as the Remote Method Invocation (RMI) Connector Port.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 9810, Remote system *INETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**WebSphere Application Server V5 NDE App Server (port 7873)**

The WebSphere Application Server v5 Network Deployment Edition (NDE) uses Port 7873 for the Data Replication Service (DRS) client address.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 9810, Remote system *INETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**WebSphere Application Server V5 NDE App Server (port 9501)**

The WebSphere Application Server v5, Network Deployment Edition (NDE) secure association service defaults to Port 9501. This is the TCP/IP port on which the Secure Association Services (SAS) listen for inbound authentication requests.
This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 9501, Remote system *INETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**WebSphere Application Server V5 NDE App Server (port 9502)**

In WebSphere Application Server v5, Network Deployment Edition (NDE) the common secure port defaults to Port 9502. This is the TCP/IP port on which the Common Secure Interoperability Version 2 (CSIV2) Service listens for inbound client authentication requests.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 9502, Remote system *INETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**WebSphere Application Server V5 NDE App Server (port 9503)**

In WebSphere Application Server v5, Network Deployment Edition (NDE) the common secure port defaults to Port 9503. This is the TCP/IP port on which the Common Secure Interoperability Version 2 (CSIV2) Service listens for inbound server authentication requests.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 9503, Remote system *INETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

**WebSphere Application Server V5 Deploy Manager (port 9809)**

The Deployment Manager is a process (a special WebSphere instance) responsible for managing the installation and maintenance of Applications and other resources related to a J2EE environment. It also maintains user repositories for authentication and authorization for WebSphere and other applications running in the environment. You can use RMI to connect wsadmin to the Deployment Manager. In this case, the default port is 9809.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 9809, Remote system *INETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.
WebSphere Application Server V5 Deploy Manager (port 8879)
Within WebSphere Application Server V5 Deployment Manager, the default connection type for the wsadmin client is Simple Object Access Protocol (SOAP) on Port 8879.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 8879, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

WebSphere Application Server V5 Deploy Manager (port 7989)
Within WebSphere Application Server V5 Deployment Manager, the default connection type for the Data Replication Service (DRS) client address is Port 7989.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 7989, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

WebSphere Application Server V5 Deploy Manager (port 9401)
Within WebSphere Application Server V5 Deployment Manager, the default SAS server authentication listener port is on Port 9401.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 9401, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

WebSphere Application Server V5 Deploy Manager (port 9402)
In WebSphere Application Server v5 Deployment Manager, the common secure port defaults to Port 9402. This is the TCP/IP port on which the Common Secure Interoperability Version 2 (CSIV2) Service listens for inbound client authentication requests.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 9402, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.
WebSphere Application Server V5 Deploy Manager (port 9403)
In WebSphere Application Server v5 Deployment Manager, the common secure port defaults to Port 9403. This is the TCP/IP port on which the Common Secure Interoperability Version 2 (CSIV2) Service listens for inbound server authentication requests.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 9403, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

WebSphere Application Server V5 Deploy Manager (port 9100)
The Object Request Broker (ORB) listener port is used for communication between catalog services in a catalog service domain, and for communication between catalog services and container servers and clients. In WebSphere Application Server v5 Deployment Manager the ORB listener port defaults to Port 9100.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 9100, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

WebSphere Application Server V5 Deploy Manager (port 7277)
In WebSphere Application Server v5 Deployment Manager, Port 7277 is used by the deployment manager to discover the NodeAgent.

This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 7277, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.

WebSphere Host On-Demand Mgr (port 8999)
WebSphere Host On-Demand provides secure access to your host applications and data from a Java™-enabled Web browser. IBM recommends using Port 8999 for this purpose. This TCP/IP rule runs every 5 minutes on a 24/7 basis and an alert is generated if the status changes since the last check was completed.

By default, the rule checks Local port number 8999, Remote system *INTNETADR, and Remote internet address 0.0.0.0. The Remote internet address setting will need changing to the correct parameters for your organization.
Performance Rules

SERVICES IBM Service Monitoring
This rule group contains 128 IBM Service Monitoring customization rules that can be used to monitor the performance activity of critical IBM subsystems and jobs.

Check subsystem QSYSWRK active
The QSYSWRK subsystem is the system subsystem which runs jobs needed by various system functions.

This *SUBSYSTEM Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of the subsystem being found in a status of *INACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if Block I/O Daemon job active
The mounts of remote directories and the initiation of the appropriate numbers of Network File System (NFS) block I/O daemons (biod daemon) to handle remote access are performed during client system boot.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QNFSBIO in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if BootP DHCP Relay Agent job active
The DHCP Relay Agent handles the forwarding the DHCP and BOOTP client broadcast packets off of the local network and on to a set of servers.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTODDHCP in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if BootP Server job active
Bootstrap Protocol (BOOTP) provides a dynamic method for associating workstations with servers and assigning workstation IP addresses and initial program load (IPL) sources.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTBOOTP in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.
A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if CCServer Agent job active**
The i5/OS system receiving change control client requests transfers and does not process the requests sent to the Change Control (CC) Server Agent. The CC Server agent processes the activities.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QCQNCMPMS in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Central Server job active**
The IBM Central Server provides services such as license management and other iSeries Access for Windows client management functions.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QZSCSRVS in subsystem QUSRWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Central Server Daemon job active**
The Central Server daemon ensures that the Central Server is always available. The central server daemon job is QZSCSRVSD.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QZSCSRVD in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if CIM Object Manager job active**
A CIM object manager (CIMOM) is a program that is installed on storage subsystems so that management application appliances, such as IBM System Storage™ Productivity Center, can perform operations on that storage subsystem.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QYCMCIMOM in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.
Check if Cluster Resource Services jobs active
Cluster Resource Services consists of a set of multi-threaded jobs. All Cluster Resource Services jobs automatically provide a joblog to aid in problem determination.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QCSTSRCD in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if Cluster QCSTCTSRCD job active
Job QCSTCTSRCD is the Cluster Resource Services daemon which ensures the Cluster Resource Services are always available.

This *JOB Performance rule is used to check that the QCSTCTSRCD is active and if so, releases the dependent jobs QCSTCTRMCMD and QCSTCTCASD.

This rule runs on a 24/7 basis and the on the first occurrence of job QCSTCTSRCD in subsystem QSYSWRK being found in an *ACTIVE status in any given 24 hour period, this rule is held and the two subsequent rules are released. Rule 70 - Check if Central Server Daemon Job is active, is also released.

Check if Cluster QCSTCTSRCD job inactive
Job QCSTCTSRCD is the Cluster Resource Services daemon which ensures the Cluster Resource Services are always available.

This *JOB Performance rule is used to check if QCSTCTSRCD is inactive and if so, holds the dependent jobs QCSTCTRMCMD and QCSTCTCASD.

This rule runs on a 24/7 basis and the on the first occurrence of job QCSTCTSRCD in subsystem QSYSWRK being found in an *INACTIVE status in any given 24 hour period, this rule and the subsequent rule are held and the previous rule is released. Rule 70 - Check if Central Server Daemon Job is active, is also held.

Check if Cluster QCSTCTSRCD dependent jobs active
Checks to see if jobs QCSTCTRMCMD, which monitors resources by communicating with the Resources Managers and QCSTCTCASD, which acts as the authentication server for RMC are active. Both jobs are dependent on the Cluster Resource Services Daemon QCSTCTSRCD.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of jobs QCSTCTRMCMD and QCSTCTCASD in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.
Check if Cluster QCSTCTRMCD job active
Checks to see if the QCSTCTRMCD job, which monitors resources by communicating with the Resources Managers, is active.

This *JOB Performance rule is used to check that the QCSTCTRMCD is active and if so, releases the dependent jobs QSVRMSERMD, QCSTHRMD, QYUSCMCRMD and QYUSALRMD.

This rule runs on a 24/7 basis and the on the first occurrence of job QCSTCTRMCD in subsystem QSYSWRK being found in an *ACTIVE status in any given 24 hour period, this rule is held and the two subsequent rules are released.

Check if Cluster QCSTCTRMCD job inactive
Job QCSTCTRMCD is the Cluster Resource Services daemon which ensures the Cluster Resource Services are always available.

This *JOB Performance rule is used to check that the QCSTCTRMCD is inactive and if so, holds the dependent jobs QSVRMSERMD, QCSTHRMD, QYUSCMCRMD and QYUSALRMD.

This rule runs on a 24/7 basis and the on the first occurrence of job QCSTCTRMCD in subsystem QSYSWRK being found in an *INACTIVE status in any given 24 hour period, this rule and the subsequent rule are held and the previous rule is released.

Check if Cluster QCSTCTSMCD dependent jobs active
This rule checks to see if jobs:
- QSVRMSERMD: Manages problem information and prepares it for delivery to the HMC.
- QCSTHRMD: Provides resource classes to represent an individual machine.
- QYUSCMCRMD: Provides resource classes to represent the Management Server, which is the HMC
- QYUSALRMD: Provides a facility for recording information about the system's operation.

which are dependent on Cluster QCSTCTSMCD are active.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of jobs QSVRMSERMD, QCSTHRMD, QYUSCMCRMD and QYUSALRMD in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

Check if Cluster CMD/API dependent jobs active
Cluster resource services consists of a set of multi-threaded jobs. When clustering is active on a system, the following jobs run as system jobs:
- Cluster control job consists of one job that is named QCSTCTL.
- Cluster resource group manager consists of one job that is named QCSTCRGM.
The QCSTCTL and QCSTCRGM jobs are cluster critical jobs. That is, the jobs must be running in order for the node to be active in the cluster.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of jobs QCSTCTL, QCSTCRGM, QCSTCRGRM, QCSTSAM and QCSTCTCFRM in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Clustered Hash Table job active**

The Clustered Hash Table server enables sharing and replicating data between cluster nodes using the Clustered Hash Table APIs. The data is stored within the clustered hash table server in non-persistent storage.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job CHTSVR1 in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check collection job active (QPMWKCOL dependent)**

The Work with Collector (QPMWKCOL) API starts, ends, or changes the collection of performance data for a particular resource on your system.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QPMASERV in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period. QPMASERV acts as a server, communicating between the APIs (QPMWKCOL and QPMLPFRD) and the QPMACLCT job, which does the actual data collection.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Collection job QYPSPFRCOL active**

Performance data collection is conducted by the Collection Services server job QYPSPFRCOL. QYPSPFRCOL creates a management collection object (*MGTCOL) to store performance data.

This *JOB Performance rule is used to check that the QYPSPRFCOL is active and if so, releases the dependent job CRTPFRDT.

This rule runs on a 24/7 basis and the on the first occurrence of job QYPSPFRCOL in subsystem QSYSWRK being found in an *ACTIVE status in any given 24 hour period, this rule is held and the two subsequent rules are released.

**Check if Collection job QYPSPFRCOL inactive**

Performance data collection is conducted by the Collection Services server job QYPSPFRCOL. QYPSPFRCOL creates a management collection object (*MGTCOL) to store performance data.
This *JOB Performance rule is used to check that the QYPSPFRCOL is inactive and if so, holds the dependent job CRTPFRDT.

This rule runs on a 24/7 basis and the on the first occurrence of job QYPSPFRCOL in subsystem QSYSWRK being found in an *INACTIVE status in any given 24 hour period, this rule and the subsequent rule are held and the previous rule is released.

**Check if QYPSPFRCOL dependent job active**
Performance data collection is conducted by the Collection Services server job QYPSPFRCOL. QYPSPFRCOL creates a management collection object (*MGTCOL) to store performance data.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of QYPSPFRCOL dependent job CRTPFRDT in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Collection job QPMASERV active**
The QPMASERV collection job acts as a server, communicating between the APIs (QPMWKCOL and QPMLPFRD).

This *JOB Performance rule is used to check that the QPMASERV is active and if so, releases the dependent job QPMACLCT.

This rule runs on a 24/7 basis and the on the first occurrence of job QPMASERV in subsystem QSYSWRK being found in an *ACTIVE status in any given 24 hour period, this rule is held and the two subsequent rules are released.

**Check if Collection job QPMASERV inactive**
The QPMASERV collection job acts as a server, communicating between the APIs (QPMWKCOL and QPMLPFRD).

This *JOB Performance rule is used to check that the QPMASERV is inactive and if so, holds the dependent job QPMACLCT.

This rule runs on a 24/7 basis and the on the first occurrence of job QPMASERV in subsystem QSYSWRK being found in an *INACTIVE status in any given 24 hour period, this rule and the subsequent rule are held and the previous rule is released.

**Check if QPMASERV dependent job active**
The QPMASERV collection job acts as a server, communicating between the APIs (QPMWKCOL and QPMLPFRD).

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of QPMASERV dependent job QPMACLCT in subsystem QSYSWRK being found in any status other than *INACTIVE in any given 24 hour period. The QPMACLCT job performs the actual data collection.
A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if Connect FlowManager jobs active
The flow manager is a flexible framework that accepts requests from the delivery gateway, invokes a multi-step business process flow to implement the request and generate a response, and passes the response back to the delivery gateway.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of jobs QBEFMNTR and QBEFSRVR in subsystem QCONNECT being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if Controlled End TCP/IP job active
The job QTCPEND is used to end the TCP/IP job in a controlled manner.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTCPEND in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if Database Server job active
QZDASOINIT is the prestart job for the database host server that is being called by a Web application.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QZDASOINIT in subsystem QUSRWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if Database Server Daemon job active
QZDASRVSD is the program that controls host database server daemon activation.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QZDASRVSD in subsystem QSERVER being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.
Check if Database SSL Server job active
QZDASOINIT job is used when the connection is from ODBC or type 4 JDBC. When the type 4 JDBC is configured to use SSL, QZDASSINIT job is used instead of QZDASOINIT.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QZDASSINIT in subsystem QUSRWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if Datalink File Manager jobs active
The DataLink File Manager (DLFM) is the component that maintains the link status for the files on a server and keeps track of metadata for each file. This code handles linking, unlinking, and commitment control issues.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of DLFM jobs QZDFMCOD, QZDFMCPD, QZDFMDGD, QZDFMGCD, QZDFMRTD, QZDFMSVR, QZDFMUPD in subsystem QSYSWRK being found in any status other then *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if Data Queue Server job active
The Data Queue Server provides access to iSeries data queues. A data queue is an object that is used by iSeries application programs for communications. Applications can use data queues to pass data between jobs. Multiple iSeries jobs can send or receive data from a single data queue.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QZHQSSRV in subsystem QUSRWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if Data Queue Server Daemon job active
The Data Queue Server provides access to iSeries data queues. A data queue is an object that is used by iSeries application programs for communications. Applications can use data queues to pass data between jobs. Multiple iSeries jobs can send or receive data from a single data queue.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of daemon job QZHQSRVD in subsystem QSYSSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.
Check if DB2 Text Extender Admin Server job active
DB2 Text Extender enables programmers to include SQL queries for text documents in their applications.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job DESSRVGB in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if DB2 Text Extender Daemon job active
DB2 Text Extender enables programmers to include SQL queries for text documents in their applications.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of daemon job DESDEM in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if DB2 Text Extender Update Index Server job active
The automatic indexing feature of DB2 Text Extender uses executable job DESXCTL.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of executable job DESXCTL in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if DHCP Server job active
The Dynamic Host Configuration Protocol (DHCP) provides configuration parameters to TCP/IP hosts. It is a client/server protocol that centrally controls and delivers TCP/IP configuration parameters to dynamically configured clients.
This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of DHCP Server job QTODDHCPS in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if DNS Server job active**
The Domain Name System (DNS) is a distributed database. This allows local control of the segments of the entire database, and data in each segment are also available across the entire network through a client/server scheme.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of DNS Server job QTOBDNS in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if DRDA/DDM Server TCP/IP job active**
The same server software is used for both DDM and DRDA TCP/IP access to DB2 UDB for IBM i. The DDM server consists of two or more jobs, one of which is the DDM listener (see below). The other job or jobs, as initially configured, are prestart jobs which service requests from the DRDA or DDM client after the initial connection is made. The set of all associated jobs, the listener and the server jobs, are collectively referred to as the DDM server.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of DRDA/DDM Server job QRWTSRVR in subsystem QUSRWRK being found in any status other than *ACTIVE in any given 24 hour period. QRWTSRVR is a prestart job that services IBM DRDA requests running over TCP/IP.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if DRDA DDM TCP/IP Listener job active**
The DRDA "listener" server job is QRWTLSTN.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of DRDA/DDM listener job QRWTLSTN in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.
Check if Extended Dynamic Remote SQL job active
The Extended Dynamic Remote SQL server allows clients access to the
functions included with DB2(R) UDB for IBM i. This server provides support for
remote SQL access, access to data through the XDA interface and database
functions (such as creating and deleting files and adding and removing file
members).

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on
the first occurrence job QXDAEDRSQL in subsystem QSYSWRK being found
in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before
the alert is re-issued.

Check if E-Z Setup Servers job active
EZ-Setup simplifies the process of establishing a relationship with a server
when using a graphical interface by providing task-based interfaces that assist
you with your server setup. The communication path used by EZ-Setup requires
three jobs, QNEOSOEM, to be running in the QSYSWRK subsystem.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on
the first occurrence job QNEOSOEM in subsystem QSYSWRK being found
in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before
the alert is re-issued.

Check if File Server Daemon & Server job active
File server jobs and the database host server daemon job (QZDASRVSD) run
in the QSERVER subsystem. The file server daemon job is QPWFSERVSD.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on
the first occurrence job QPWFSERVSD in subsystem QSERVER being found in
any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before
the alert is re-issued.

Check if File Server S2 job active
QPWFSERVVS2 is a server prestart job associated with the QWPFSERVSD
daemon job.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on
the first occurrence job QPWFSERVVS2 in subsystem QSERVER being found in
any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before
the alert is re-issued.
Check if File Server SO job active
QPWFSERVSO is a server prestart job associated with the QWPFSERVSD daemon job.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence job QPWFSERVSO in subsystem QSERVER being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if File Server SSL job active
QPWFSERVSS is a server prestart job associated with the QWPFSERVSD daemon job.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence job QPWFSERVSS in subsystem QSERVER being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if FTP jobs active
The FTP server jobs are started when the Start TCP/IP (STRTCP) command is run and with the FTP AUTOSTART parameter is set to *YES, or when the Start TCP/IP Server (STRTCPSVR) command is run with a SERVER parameter value of *FTP or *ALL.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated if no jobs beginning with QTFTP* are found to be running in subsystem QSYSWRK.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if QTESDBGHUB job active
The Debug Hub (QTESDBGHUB) is a job that runs on the IBM i server. It's the central point of contact for the graphical system debugger. The Debug Hub is responsible for remembering who's currently registered for debug and starting Debug Server jobs.

This *JOB Performance rule is used to check that the QTESDBGHUB is active and if so, releases the dependent job QTESDBGSVR.

This rule runs on a 24/7 basis and the on the first occurrence of job QPMASERV in subsystem QSYSWRK being found in an *ACTIVE status in any given 24 hour period, this rule is held and the two subsequent rules are released. Rule 240 - Check if QMAPSRV dependent job active is also released.
Check if QTESDBGHUB job inactive
The Debug Hub (QTESDBGHUB) is a job that runs on the IBM i server. It’s the central point of contact for the graphical system debugger. The Debug Hub is responsible for remembering who’s currently registered for debug and starting Debug Server jobs.

This *JOB Performance rule is used to check if QTESDBGHUB is inactive and if so, holds the dependent job QTESDBGSVR.

This rule runs on a 24/7 basis and the on the first occurrence of job QTESDBGHUB in subsystem QSYSWRK being found in an *INACTIVE status in any given 24 hour period, this rule and the subsequent rule are held and the previous rule is released. Rule 240 - Check if QMAPSRV dependent job is active, is also held.

Check if QTESDBGHUB dependent job active
The Debug Server runs in its own job (QTESDBGSVR), which uses the STRSRVJOB command to service another job to be debugged.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QPWFSERVSS in subsystem QUSRWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if Help Server job active
The IBM Help Server is an interface for the Infocenter. It also provides a framework (using Eclipse) that allows applications to write to it. This framework then is responsible for serving help text for these applications.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QIBMHELP in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if HTTP Server jobs active
IBM HTTP Server (IHS) is a web server based on the Apache Software Foundation's Apache HTTP Server that runs on AIX, HP-UX, Linux, Solaris, Windows NT, IBM i and z/OS.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated if no job is found to be running in subsystem QHTTPSVR.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.
Check if IBM Director jobs active
IBM Director is an integrated suite of tools that provide comprehensive system-management capabilities to maximize system availability. It supports the management of a variety of hardware and operating systems, including most Intel® microprocessor-based systems and certain IBM System i™, System p™, System x™, and System z™ servers.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of jobs QCPMGTACT and QCPMGTSVR in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if IBM Directory Server jobs active
IBM Directory Server for IBM i (also referred to as Directory Services) provides Lightweight Directory Access Protocol (LDAP). LDAP runs over Transmission Control Protocol/Internet Protocol (TCP/IP), and is popular as a directory service for both Internet and non-Internet applications.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QDIRSRVR in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if InfoPrint Font Downloader job active
Listens on a TCP/IP port for InfoPrint Manager Double-Byte Character Set (DBCS) Font Downloader connections. After connecting, new or refreshed PostScript fonts can be sent to the system for use with InfoPrint server. The font downloader job receives and installs these fonts.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QXTFRNTDWN in subsystem QUSRWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if InfoPrint Server Transform jobs active
InfoPrint Server for iSeries Transform jobs convert Adobe® PDF 1.3 and PS Level 3 data streams to IBM Advanced Function Presentation (AFP) data stream. This transform is indirectly called through the Image Print Transform function of i5/OS.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of jobs QADBDAEMON and QXIODAEMON in subsystem QUSRWRK being found in any status other than *ACTIVE in any given 24 hour period.
A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if InfoPrint Server Transform Manager jobs active**
InfoPrint Server for iSeries Transform Manager manages heavyweight data stream transform jobs for InfoPrint Server/400-provided transforms.
This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QXTRTFMMGR in subsystem QUSRWRK being found in any status other than *ACTIVE in any given 24 hour period.
A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if INETD Super Server job active**
Internet Daemon (INETD) Super Server listens for client requests for many different programs. Using INETD saves system resources by not requiring processes to be started and listing on ports for services that are not used often. When a client request is received, INETD generates a process to run the configured program to handle the request.
This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTOGINTD in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.
A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if PTF Delivery Server job active**
Internet PTF Delivery Server allows you to order and download PTFs using the Internet.
This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QESISRV in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.
A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Web PDF Server jobs active**
IBM i Access for Web PDF Server starts by the printer servlet support of IBM i Access for Web when any user needs to transform a spooled file to PDF using InfoPrint Server support.
This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of jobs QIWAPDFSRV and QJVMACMDSRV in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.
A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.
Check if NetServer Daemon job active
QZLSSERVER is the NetServer Daemon job that runs in the background to ensure the availability of the IBM NetServer.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QZLSSERVER in subsystem QSERVER being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if NetServer job active
i5/OS NetServer enables Microsoft® Windows® and Linux® Samba clients to access shared directory paths and shared output queues on the system. Clients on a network use the file and print-sharing functions for their operating systems.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QZLSFILE in subsystem QSERVER being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if Joblog Server job active
The Joblog Server generates spooled job logs in the background.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QJOBLOGSVR in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if LDAP Publishing Agent job active
LDAP Publishing Agent publishes or stores information in a Directory Services (LDAP) server. Multiple jobs of this type can be running on a given system, each publishing a different type of information.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QGLDPUBA in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if LDAP Publishing Engine job active
LDAP Publishing Engine asynchronously processes LDAP publishing requests made with the QgldPubDirObj API.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QGLDPUBE in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.
A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Line Printer Daemon jobs active**
Line Printer Daemon receives files sent by the Line Printer Request (LPR). You can use the LPD server to receive spooled files from another system, or you can use the LPD server to receive print output from another system.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated if no jobs beginning with QTLPD* are found to be running in subsystem QSYSWRK. A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Managed System Agent jobs active**
Managed System Agent monitors scheduled jobs and the control language (CL) input streams that are run as a result of activities received from the central site system.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of jobs QCQEPMON in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period. A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Management Central Agent jobs active**
Management Central Agent performs work for the Management Central server.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of jobs QYPSAPI, QYPSPTF, QYPSRTMTCMD, QYPSGETINV, QYPSRPTC, QYPSUSRADM and QYPSBDTSVR in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Management Central Server job active**
Management Central Server manages multiple systems from a single system in the TCP/IP network. This central system manages the other systems (called endpoint systems) in your network.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QYPSJSRV in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.
Check if Mount Server job active
Mount Server is a Remote Procedure Call (RPC) registered Network File System (NFS) service that handles mount and unmount requests for NFS clients.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QNFSMNTSD in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if MQ Series Server job active
MQ Series Server provides the infrastructure for mission-critical communication between applications, either within an organization or business to business.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job RUNMQLSR in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if Network Lock Manager job active
Network Lock Manager is a RPC-registered NFS service that provides byte-range locking for NFS files.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QNFSNLMD in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if Network Print Server job active
The network print server provides client access to i5/OS print objects and resources.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QNPSERVS in subsystem QUSRWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if Network Print Server Daemon job active
The network print server provides client access to i5/OS print objects and resources. The daemon job runs in the background to ensure availability of the network print server.
This "JOB" Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QNPSERVSD in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Network Station Login Daemon job active**
The Network Station Login Daemon allows IBM Network Stations and other applications that use remote authentication protocol (RAP) to authenticate on the i5/OS operating system.

This "JOB" Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QYTCNSLD in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Network Status Monitor job active**
Network Status Monitor (NSM) provides applications with information about the status of network hosts. The Network Lock Manager (NLM) daemon uses the NSM to track network hosts that have locks.

This "JOB" Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QNFSNSMD in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if NFS Server jobs active**
Network File System (NFS) Server stores files on a system and allows clients in the network to access and use the single set of files. NFS is typically used to share files among UNIX-type systems.

This "JOB" Performance rule runs on a 24/7 basis and an alert is generated if no jobs beginning with QNFSNSD* are found to be running in subsystem QSYSWRK.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if OnDemand Daemon job active**
The OnDemand Server lets you store large amounts of historical data on a disk, high-capacity optical volumes, or tape. It also provides quick access to stored data by online retrieval. The OnDemand Daemon job ensures that the OnDemand server is always available.

This "JOB" Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QRLGMGR in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.
A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if OnDemand Server job active**
The OnDemand Server lets you store large amounts of historical data on a disk, high-capacity optical volumes, or tape. It also provides quick access to stored data by online retrieval.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QRLGSRV in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if POP jobs active**
Post Office Protocol (POP) allows the system to store e-mail for clients who use POP for their e-mail. E-mail is stored on the server until clients request it, at which time the mail is forwarded to the client and deleted from the server.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated if no jobs beginning with QTPOP* are found to be running in subsystem QSYSWRK.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if QoS Policy Agent job active**
Quality of Service (QoS) Policy Agent provides Network Quality of Service functions for the system. These services include: Differentiated Services that allow a user to specify special handling for TCP/IP connections and Integrated Services that allow applications using the RSVP internet protocol to request special handling for TCP/IP connections.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTOQSRVR in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if QoS RSVP Agent job active**
RSVP is a receiver-oriented signaling protocol that enables applications to request Quality of Service(QoS) on an IP network. The RSVP agent uses the RSVP protocol to propagate the QoS request through the routers along the paths for the data flow.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTOQRAGENT in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.
Check if Remote Command Agent job active
Remote Command Agent accepts the remote commands from central site systems. From any location in your network, you can send commands to run on distributed systems that have Managed System Services installed.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QVARRCV in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if Remote Command Server job active
QZRCSRVVS jobs are i5/OS TCP Remote Command Server jobs that the Management Central Java™ server uses for calling commands and APIs.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QZRCSRVVS in subsystem QUSRWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if Remote Command Server Daemon job active
The Remote Command Server daemon (QZRCSRVSD) runs in the background and ensures that the Remote Command Server is always available.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QZRCSRVSD in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if Remote Execution (RExec) job active
Remote Execution (RExec) allows a client user to send system commands to a remote system for processing. When RExec receives a client request, it first validates the user profile and password and then runs the requested command. The results are returned to the client.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated if no jobs beginning with QTRXC* are found to be running in subsystem QSYSWRK.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if RouteD jobs active
RouteD provides dynamic routing. Dynamic routing deals with the ability to determine how to route traffic based upon a changing network topology.
This *JOB Performance rule runs on a 24/7 basis and an alert is generated if no jobs beginning with QTRTD* are found to be running in subsystem QSYSWRK. A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Remote Procedure Call job active**
Remote Procedure Call (RPC) runs Network File System daemons and other commands.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QNFSRPCD in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Server Port Mapper job active**
Server Port Mapper allows the client to find the port of the particular service. The client sends in a request with the service name, and the port mapper looks up the service in the service table and returns the port number to the client.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QZSOSMAPD in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Hardware Problem Reporting jobs active**
Hardware Problem Reporting predicts and prevents hardware errors by early detection of potential problems, downloads fixes, and automatically calls IBM Service when necessary.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of jobs QS9PROBMON and QS9PALMON in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Inventory Transmission job active**
Job QS9SACOL tells Management Central to collect the inventory. The inventory collections may be a collection of the entire inventory (including areas such as PTFs, products, hardware, and contact information) or only those areas that have changes since the last inventory collection. When the inventory collection is done, the QYPSJSVR job submits the QYIVRIPS job. The QYIVRIPS job initiates the inventory send and passes the function off to the communications.
This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QYIVRIPS in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Signon Server Daemon job active**
The Signon server provides security for clients. This security function prevents access to the system by users with expired passwords, validates user profile passwords and returns user profile security information for use with password caching and IBM i Navigator Application Administration. The Daemon job runs in the background and ensures that the Signon Server is always available.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QZSOSGND in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Signon Server job active**
The Signon server provides security for clients. This security function prevents access to the system by users with expired passwords, validates user profile passwords and returns user profile security information for use with password caching and IBM i Navigator Application Administration.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QZSOSIGN in subsystem QUSRWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Simple Network Time Protocol job active**
The Simple Network Time Protocol Service provides time synchronization services to other systems.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTOTNTP in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if SMTP Bridge Client job active**
The Simple Mail Transfer Protocol (SMTP) Bridge Client converts Systems Network Architecture distribution services (SNADS) outbound mail to simple SMTP mail for an SMTP client to send.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTSMTMPBRCL in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.
A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if SMTP Bridge Server job active**
SMTP Bridge Server creates an mail server framework (MSF) message and stream file from the inbound mail received from the SMTP server.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTSMTPBRSR in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if SMTP Client Daemon job active**
The SMTP Client allows end-to-end delivery of mail from one mail server to another. A direct connection exists between the SMTP sender and the destination SMTP receiver. The client keeps the mail at the sender until it transmits and copies it. This daemon runs in the background and ensures that the STMP Client is always available.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTSMTPCLTD in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if SMTP Client job active**
The SMTP Client allows end-to-end delivery of mail from one mail server to another. A direct connection exists between the SMTP sender and the destination SMTP receiver. The client keeps the mail at the sender until it transmits and copies it.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTSMTPCLTP in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if SMTP Mail Scheduler job active**
The SMTP Mail Scheduler sets the time intervals that you want the system to connect to your Internet service provider (ISP) and send your e-mail.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTSMTOPSCH in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.
Check if SMTP Server Daemon job active
The SMTP Server allows end-to-end delivery of mail from one mail server to another. A direct connection exists between the SMTP sender and the destination SMTP receiver. The client keeps the mail at the sender until it transmits and copies it. This daemon runs in the background and ensures that the SMTP Server is always available.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTSMTPSRVD in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if SMTP Server job active
The SMTP Server allows end-to-end delivery of mail from one mail server to another. A direct connection exists between the SMTP sender and the destination SMTP receiver. The client keeps the mail at the sender until it transmits and copies it.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTSMTPSRVP in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if SNMP Trap Manager jobs active
Use the SNMP Trap Manager to notify other systems running an SNMP console of all SNMP traps that occur on the enclosures connected to a management station.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of jobs QTRPMGR and QTRPRCV in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if SNMP Agent jobs active
The Simple Network Management Protocol (SNMP) Agent supports the exchange of network management messages and information among hosts.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of jobs QSNMPSA, QTMSNMPRCV and QTMSNMP in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.
Check if SQL job active
The SQL Server processes SQL statements from an application that is running SQL in server mode. In server mode, each SQL connection is processed by a separate job.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QSQSRVR in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if System Manager job active
The System Manager receives PTF requests, service requests, and test requests from service requesters.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QECS in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if TCP/IP Event Manager job active
TCP/IP Event Monitor runs whenever TCP/IP is running and provides an internal mechanism to communicate data and events among TCP/IP services and processes.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTCPMONITR in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if TCP/IP Interface Daemon job active
The TCP/IP Interface Daemon starts or ends TCP/IP interfaces. When starting a TCP/IP interface, this daemon also attempts to vary on the line, controller, and device used by that TCP/IP interface.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTCPIP in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if TCP/IP L2TP Server job active
The TCP/IP L2TP Server manages Layer Two Tunneling Protocol (L2TP) connections.
This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTPPL2TP in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if TCP/IP PPP Server job active**
The TCP/IP PPP Server manages Point-to-Point Protocol (PPP) connections.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTPPCTL in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if TCP/IP SLIP Server job active**
The TCP/IP SLIP Server manages Serial Line Internet Protocol (SLIP) connections.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated if no jobs beginning with QTPPDIAL* or QTPPANS* are found to be running in subsystem QSYSWRK.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of jobs QTPPDIAL* and QTPPANS* in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Telnet Device Manager job active**
The TELNET Device Manager manages device descriptions when clients start and end Telnet sessions. The Telnet Device Manager stores the client's IP address and port in the device description.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTVDEVICE in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Telnet Server job active**
The TELNET Server signs on to an interactive job on the system from another system in a TCP/IP network with a Telnet client.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTVTELNET in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.
A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Text Search Engine BG Process job active**
The Text Search Engine Background Process updates or reorganizes a text search index.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job IMOSMBCK in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Text Search Engine Daemon job active**
The Text Search Engine Daemon controls access and processing tasks for indexes belonging to the text search engine instance.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job IMOSMDEM in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Transfer Server TCP/IP job active**
The Transfer Function Server TCP/IP transfers data between the i5/OS operating system and a personal computer.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTFPJTCP in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Trivial FTP jobs active**
Trivial FTP provides basic file transfer functions with no user authentication.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of any job commencing QTTFT* in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if Virtual Print Server job active**
Virtual Print Server TCP/IP prints data from PC application programs on printers connected to the system enabling you to use a printer that is attached to the host system as though the printer were directly attached to your personal computer.
This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QIVWPPJT in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if VPN Connection Manager job active**
Virtual Private Networking (VPN) Connection Manager performs Internet Key Exchange (IKE) protocol processing and manages all VPN connections. VPN allows you to securely extend your private intranet over a public network, such as the Internet.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTVOMAN in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if VPN Key Manager job active**
The VPN key manager is IBM's implementation of the Internet Key Exchange (IKE) protocol. The key manager supports the automatic negotiation of security associations (SAs), as well as the automatic generation and refresh of cryptographic keys.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTOKVPNKE in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if WebFacing Server job active**
The WebFacing Server gives a Web-based application access to application data from interactive programs running on the system.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QQFWFSRV in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if WebSphere V4 AE Admin Server job active**
WebSphere Application Server V4 Advanced Edition, Administration Server allows a WebSphere user to connect a WebSphere Administrative Console to the system to administer the WebSphere configuration.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QEJBADMIN in subsystem QEJBADV4 being found in any status other than *ACTIVE in any given 24 hour period.
A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if WebSphere V4 AE App Server job active**
WebSphere Application Server V4 Advanced Edition, Application Server allows you to implement and manage server-side Java™ components, enterprise beans, Java Server Pages, and JSP files.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job DEFAULT_SE in subsystem QEJBAES4 being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if WebSphere V4 ASSE App Server job active**
WebSphere™ Application Server, Advanced Single Server Edition for Multi-platforms V4.0 is a lower total cost solution for Java-based Web application serving within a dynamic e-business environment.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job DEFAULT_SE in subsystem QEJBADV4 being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if WebSphere V5 App Server job active**
WebSphere v5 is a set of Java-based tools from IBM that allows customers to create and manage sophisticated business Web sites. The central WebSphere tool is the WebSphere Application Server (WAS), an application server that a customer can use to connect Web site users with Java applications or servlets.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job SERVER1 in subsystem QEJBAS5 being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

**Check if WebSphere V5 NDE Deploy Manager job active**
IBM® WebSphere® Application Server Network Deployment provides an advanced, flexible runtime environment for large-scale application deployments. It offers near-continuous availability with advanced performance and management capabilities for mission-critical applications.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job DMGR in subsystem QEJBASND5 being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.
Check if WebSphere V5 NDE Node Agent job active

Each computer in a WebSphere V5 cell is known as a node. The node agent is a server process running several administrative applications. The first is a NodeSync component. This component exchanges information with the deployment manager, and creates a local copy of all the configuration files that the deployment manager sends it.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job NODEAGENT in subsystem QEJBAS5 being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if WebSphere Host On-Demand Manager job active

IBM WebSphere Host On-Demand provides secure browser-based and non-browser-based host access to users in intranet-based and extranet-based environments. Host On-Demand is installed on a Web server, simplifying administrative management and deployment, and the Host On-Demand applet or application is downloaded to the client browser or workstation, providing user connectivity to critical host applications and data.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QHODSVM in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if Workload Management Server job active

Workload Manager (WLM) is designed to provide the system administrator with increased control over how the scheduler virtual memory manager (VMM) and the disk I/O subsystem allocate resources to processes.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QWLMSVR in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.

Check if OMPROUTED Server job active

On a System i® platform, the OMPROUTED TCP/IP server provides support for the RIPng protocol, and for old RIPv1 and RIPv2 protocols that are also supported by the Route Daemon (RouteD) server.

This *JOB Performance rule runs on a 24/7 basis and an alert is generated on the first occurrence of job QTOOROUTE in subsystem QSYSWRK being found in any status other than *ACTIVE in any given 24 hour period.

A ten minute grace period is utilized to enable you to resolve the issue before the alert is re-issued.
Learn More

For white papers, online product tours, datasheets, technical tips and manuals, please visit: http://www.helpsystems.com/halcyon

Contact

www.helpsystems.com
US: +1 952-933-0609
Outside the U.S.: +44 (0) 1252 618 030

Trademarks

IBM®, iSeries®, Power/System i®, IBM i®, i5/OS® and AIX® are registered trademarks of International Business Machines Corporation in the United States and in other countries,

INFOR XA® is a registered trademark of Infor

All other trademarks are respective of their own companies.