

AAG
&
NG4i

Nagios Monitoring Solution for IBM i

User manual

V3R0M0

First Version (December 2025)

This edition applies to Version 3 Release 0 Modification Level 0 of the AAG/NG4i product, and to all subsequent releases or modifications until otherwise indicated.

Readers' Comments can be addressed to:

Shield Advanced Solutions Ltd.

75 First Street

Suite #206

Orangeville

Ontario

Canada L9W 5B6

Tel: +1 (1) 519 940 1192

Email to support@shieldadvanced.com

<https://www.shieldadvanced.com>

Table of contents

AAG	1
&	1
NG4i	1
Nagios Monitoring Solution for IBM i	1
User manual	1
V3R0M0	1
Second Version (January 2024)	2
75 First Street	2
Tel: +1 (1) 519 940 1192	2
Email to support@shieldadvanced.com	2
https://www.shieldadvanced.com	2
Table of contents	3
Notices	10
AAG	10
NG4i	10
FT4i	10
IBM	10
Preface	11
What's New this Release:	11
Related Information	11
Internet URL	11
Introduction	12
Product Overview	12
Usage of AAG	12
Installing AAG	13
Installing NG4i	13
Pre-Installation	13
Restoring the Licensed Program	13
Type RSTLICPGM and press PF4	13
Pressing ENTER will restore the licensed program into library NG4I30.	13
RSTLICPGM LICPGM(1NG4ISC)	13
DEV(*SAVF)	13
SAVF(QGPL/NG4I11)	13
License Key Management	14
Hardware and software prerequisites	15

Hardware	15
AAG runs on any Linux capable hardware.....	15
Current supported OS: (Debian, Rasbian, Ubuntu, Centos7&8, Oracle 8)	15
NG4i runs on any Power system running iOS above V7R1	15
Software	15
For all installation of NG4i the following levels of iOS are required	16
Configuring NG4i on the IBM i	17
Starting and stopping NG4i.....	18
Active processes IBM i.....	18
Configuring Nagios with Nconf and AAG commands.....	18
AAG's Web-based Commands Menu.	30
Add System	30
Add Checks	31
Add Services.....	32
About AAG	33
Defaults	34
Using Ansible to take action with AAG.	35
Hosts	39
Services	39
Check commands.....	39
Threshold and Ranges	39
HA4i Check Commands	40
check_HA4i_RATE	40
check_HA4i_APY	40
check_HA4i_RJRN.....	42
check_HA4i_OBJ	43
check_HA4i_SPLF	45
check_HA4i_SYNC.....	46
check_HA4i_RJOBS	47
check_HA4i_SPLFW.....	48
check_HA4i_IJRN	49
check_HA4i_STATUS	50
check_HA4i_ROLESWAP	51
check_HA4i_NEWDEV	52
check_HA4i_NEWLIB	53
check_HA4i_AUDERR	54
check_HA4i_AUDSTS	55
check_HA4i_RSREADY	56

EM4i Check Commands	57
check_EM4i_RESPWAIT.....	57
check_EM4i_MSGMON, check_EM4i_MSGPOL, check_EM4i_SMSMGR	58
Shield General Check Commands	59
check_Shield_KEYEXP	59
check_Shield_SBSSRCH.....	60
check_Shield_JOBSRCH.....	61
check_Shield_RPYW.....	62
check_Shield_DSBPRF	63
check_Shield_SBSJOB	64
check_Shield_JOBQ	64
check_Shield_RCVR	65
check_Shield_CACHEBAT	66
check_Shield_DSBPRF	67
check_Shield_APTUPD.....	68
check_Shield_PTF	69
check_Shield_TOPJOB_CPU	70
check_Shield_TOPJOB_STG.....	71
check_Shield_UPDLVL.....	72
check_Shield_PRDSYNC	73
check_Shield_APTUPD.....	74
check_Shield_JOBSCDE	75
check_Shield_SSLCERT	76
check_Shield_DSKSTS	77
check_Shield_UPTIME.....	78
check_Shield_SYSVAL.....	79
check_Shield_SECUPD.....	80
check_Shield_AUTUPD	81
check_Shield_RCVRBKLG.....	82
check_Shield_OSLVL	83
check_Shield_PING.....	84
check_Shield_ASPSTS	85
check_Shield_ASPAVL.....	86
check_Shield_ASPMIR	87
check_Shield_ASPLIFE.....	88
check_Shield_ASPDSK	89
check_Shield_ASPOVRFLW.....	90
check_Shield_ASPGEOSTS	91

check_Shield_DEVSTS	92
check_Shield_DMGOBJ	95
check_Shield_JOBPCPU	96
check_Shield_JOBSTG.....	98
check_Shield_TOPCPU	100
check_Shield_TOPCPUTIME.....	102
check_Shield_TOPDSKIO.....	104
check_Shield_TOPINTRS	106
check_Shield_TOPINTTRANS.....	108
check_Shield_DQECOUNT.....	110
check_Shield_LIBSIZE.....	111
check_Shield_WRKPRB.....	112
check_Shield_OUTQC.....	114
check_Shield_SSTP	115
check_Shield_IFSCOUNT	116
check_Shield_IFSSIZE	117
check_Shield_LPPSTS.....	118
check_Shield_JOBESTS	119
check_Shield_PORTCONN	120
check_Shield_PGMEXP	121
check_Shield_QHST	122
check_Shield_JOBFUNC.....	123
check_Shield_JOBSBSSTS.....	124
check_Shield_FMWR.....	125
check_Shield_USRCLS.....	126
check_Shield_SPCAUTH.....	127
check_Shield_CPURESET.....	128
HMC Check Commands	153
check_HMC_MSYSYCON	153
check_HMC_MEMSTS	154
check_HMC_SRVEVNT.....	155
check_HMC_SYSLED	155
check_HMC_PARTLED	156
check_HMC_MAINTEXP.....	157
check_HMC_PARTSTS	158
check_HMC_UPD	159
check_HMC_MIGSTS.....	160
check_HMC_LOGINS.....	161

check_HMC_FSSIZE	162
check_HMC_CERT	163
check_HMC_SYSSRC	164
check_HMC_PARTSRC.....	164
BRMS Check Commands	165
check_BRMS_WERR.....	165
check_BRMS_RERR.....	165
check_BRMS_FULL	165
check_BRMS_USED.....	165
check_BRMS_EXPD.....	166
check_BRMS_DUPD.....	166
check_BRMS_EDAT.....	166
check_BRMS_STS	167
FT4i Check Commands	169
check_FT4i_LOG.....	169
VIOS Check Commands <i>*BETA Release*</i>	170
check_VIOS_OSLVL.....	170
Mimix Check Commands	181
check_MMX_DBSND.....	181
check_MMX_SWSTS	182
check_MMX_RJLNK.....	183
check_MMX_OBJAPY	184
check_MMX_FESTS.....	185
check_MMX_ITESTS.....	186
check_MMX_OTESTS.....	187
check_MMX_CFGCHG	188
check_MMX_CNTRSTS	189
check_MMX_APYSTS.....	190
check_MMX_ARSTS.....	191
check_MMX_AGSTS.....	192
check_MMX_SYSSTS	193
check_MMX_JRNSTS	194
IBM i Status Check Commands	195
check_Status_AVLDISK	196
check_Status_TOTDISK.....	196
check_Status_AVLDISKGB.....	197
check_Status_SYSNAME.....	197
check_Status_SYSSTATE	198

check_Status_CPUUSED.....	198
check_Status_NUMJOB	199
check_Status_PADDR	199
check_Status_TADDR.....	200
check_Status_ASP	200
check_Status_STORAGE.....	201
check_Status_UNPSTG	201
check_Status_MAXUNPSTG	202
check_Status_NUMPART	202
check_Status_PARTID	203
check_Status_CPUCAP	203
check_Status_CPUSHARE	204
check_Status_NUMCPU.....	204
check_Status_ACTJOB.....	205
check_Status_ACTTHD.....	205
check_Status_MAXJOB	206
check_Status_TMP256.....	206
check_Status_PRM256	207
check_Status_TMP4GB	207
check_Status_PRM4GB.....	208
check_Status_UCAP	208
check_Status_SPOOL	209
check_Status_MAINMEM.....	209
Job List.....	210
check_Status_PRCTTU	211
check_Status_INTTRN	212
check_Status_DBLCKW.....	213
check_Status_INTLCW	214
check_Status_NDBLCKW	215
check_Status_AUXIOR	216
check_Status_PEAQTS.....	217
check_Status_QTEMPS	218
check_Status_RESPTT	219
check_Status_TSDBLW	220
check_Status_TSINTL.....	221
check_Status_TSNDL	222
check_Status_TMPSTG	223
Secure connections	224

Pushover Acknowledgement Functions	224
Security Bulletins	225
PTF Installation	226
The PTF Objects.....	226
The Cover Letter	226
Update packages IBM i.....	227
Update packages Nagios/Linux.....	228
Support Process	229
Readers' Comments.....	230

Notices

The following terms, used in this publication, are trademarks of Shield Advanced Solutions (Canada) Ltd.

AAG
NG4i
FT4i

The following terms, used in this publication, are trademarks of the IBM Corporation in the United States and/or other countries.

IBM
IBM i

Preface

AAG is a Nagios plugin for Linux with a corresponding IBM i product (1NG4ISC) which is used to return the relevant status for the Nagios requests. The IBM i product provides a constantly running server process that will return status information to the calling program based on the request made. This reduces the overhead seen in other solutions by removing the overhead created by a new job being spawned for each Nagios request.

AAG has been developed with security in mind and provides both a secure and non-secure connection method for transmitting the data between nodes. The installation of SSL certificates will be required for a secure connection, this in turn will require DCM (5770SS1 Option 34) to be installed and configured on the IBM i.

The sign on information required for the IBM i is stored in an encrypted object, each request for information on the IBM i will run under the NG4iUSER profile. The User profile entered will only be used for FTP traffic to the IBM i.

The IBM i LPP 1NG4ISC (NG4i) is needed for status to be pulled back from any IBM i that is to be monitored.

What's New this Release:

The following check commands have been added via updates in the latest version:

*NONE

You can limit the source of any request to a specific IP address to ensure no requests are accepted from any other IP address.

Improved performance by the removal of unnecessary traffic from the communications links. The use of API keys instead of sign on each time a request is received has significantly reduced the overhead and given a 3 – 4 times performance improvement for the checks.

Related Information

Internet URL

Shield Advanced Solutions (Canada) Ltd <https://www.shieldadvanced.com>
IBM <http://www.ibm.com>

IBM i Manuals

DCM <https://www.ibm.com/docs/en/i/7.4?topic=security-digital-certificate-manager>
Security Ref. <https://www.ibm.com/docs/en/i/7.4?topic=security-reference>

Introduction

Product Overview

AAG provides the ability to retrieve the status from an IBM i system through the Nagios Enterprise Monitoring Solution. Both the Linux and IBM i programs are shipped as part of the AAG package. The installation of the Nagios elements is carried out via a batch script and the IBM i objects ship as an IBM LPP (1NG4ISC) which are installed via the RSTLICPGM command.

Having the ability to monitor a range of platforms through a single interface reduces the overhead on the support staff and provides a much simpler solution than having multiple monitoring products for each platform. Nagios can be used to monitor a range of other platforms with many community provided plugins aimed at supplying the required data from those platforms, however the IBM i did not have many and those that existed tended to be outdated and limited in scope. AAG has been developed to address that shortfall and will continue to have new features added as the need arises.

AAG is provided on a SAAS basis which removes the upfront costs associated with many IBM i products provided for the platform today. The Nagios environment can be provided by the customer or it can be built and installed on the customer provided hardware using the scripts that have been developed by Shield Advanced Solutions.

Usage of AAG

AAG is a plug-in component for Nagios plus a LPP that will be installed on the IBM i system(s) that is(are) to be monitored.

The IBM i LPP needs to be installed and a simple configuration to set the secure/non secure flag for the server. Once configured the servers can be started which will then respond to the requests from the Nagios server.

Note:- setting the IBM i as a secure server and configuring the Nagios requests to run over non secure will result in errors being returned. It is important that you configure both sides to use the same communications method.

Once the processes have been started on the IBM i they should not be stopped, if you find that some processes are ending abnormally contact support for assistance to resolve.

The parameters passed to the Nagios plugin determine how the OK, warning, critical flags are issued and are specific to each user's requirements and should be set accordingly.

Installing AAG

AAG is installed on the Nagios server using the binary files provided by Shield Advanced Solutions.

There are Nagios XI wizards available which will reduce the time and effort required to install the hosts and services required for monitoring the IBM i, HMC or VIOS. The Shield Advanced Solutions supplied distribution has a php interface to allow the configuration of hosts and services.

Installing NG4i

NG4i is installed on any IBM i that is to be monitored by AAG.

Pre-Installation

NG4i is installed as an IBM Licensed Program Product (LPP) 1NG4ISC using the RSTLICPGM command. To be able to restore a licensed program you will need to have the relevant authorities to objects on the system.

Restoring the Licensed Program

1. Perform the following after the Save File is on your system.

Type RSTLICPGM and press PF4

The Product ID is 1NG4ISC. This is the licensed program name allocated to NG4i and is used for other activities such as License Management and PTF Management.

The Device is where the product is to be installed from (*SAVF).

The Language for licensed program should be set to *PRIMARY. If you have a primary language other than one of the following you need to have one of the following languages installed as a secondary language. If you have such a situation you will need to change the *PRIMARY to the relevant installed language. All menus, panel groups and text are in English regardless of the language install.

2924 English

Pressing ENTER will restore the licensed program into library NG4I30.

```
RSTLICPGM LICPGM(1NG4ISC)
          DEV(*SAVF)
          SAVF(QGPL/NG4I30)
```

NOTE:

As part of the installation process you will be presented with a license agreement.

F8 will register your agreement to the license agreement and the product will install. You will need to contact Shield for a key to allow the product to run after an initial 30day period. To help provide you with a correct key please run the PRTKEYINF after the product has installed and send the output to Shield Advanced Solutions Ltd. A key will be returned which allows the product to be run for a temporary period.

F9 will stop the installation process and submit a request to remove the licensed program. No license will be installed and elements of the product will not be created, rendering the product unusable. If the product fails to uninstall you can remove the product by issuing a DLTLICPGM by a user with the relevant authority.

License Key Management

NG4i automatically installs a license key which will allow the product to be used for 30 days, after this time a new key will be required which will be supplied by Shield Advanced Solutions Ltd. The key will be generated to match the agreed license period and only issued after receipt of payment.

The 30-day trial period should be used for testing and implementation of the product, no additional temporary keys will be provided.

To install a License Key, take one of the following options:

- Type WRKLICINF on a command line and follow instructions.
- Type ADDLICKEY on a command line and follow instructions.

If you take the WRKLICINF option a screen similar to the following will be shown:

```

                                Work with License Information
                                SAS2
                                02/16/21 11:35:18
System serial number . . . . . : 218FFEW
Processor group . . . . . : P05

Type options, press Enter.
 1=Add license key  2=Change  5=Display detail  6=Print detail
 8=Work with license users ...

Opt  Product   License
     Term     Feature  Description
-----
5770SS1 V7R1M0  5116  HA Switchable Resources
5770SS1 V7R1M0  5117  HA Journal Performance
1DR4IPR V8R1    5001  DR4i Disaster Recovery for the IBM i Version
1FTPCLT V6R1    5001  FTP Client for IBM i
1FTPSEC V7R1    5001  FTP Guard4i FTP Security for the IBM i
1HA4IMN V8R0    5001  HA4i High Availability for IBM i
1NG4ISC V3R0    5001  Nagios monitor for IBM i
                                More...

Parameters or command
====>
F3=Exit          F5=Refresh    F11=Display Usage Information  F12=Cancel
F17=Position to F23=More options

```

Sample Work with Licensed Information

1. Type 1 against the 1NG4ISC entry - Add license key. This will bring up the ADDLICKEY command screen and you need to type in the information that was sent when you purchased the product.

The following information will be automatically entered into the command:

- Product Identifier "1NG4ISC"
- License Term "V3R0"
- Feature "5001"

- System Serial Number *Your IBM i Serial Number*

The following information must be entered before pressing the enter key:

- **The processor group.** This should match the actual processor group of the CPU
- **The License Key.** Supplied by Shield Advanced Solutions Ltd
- **Usage Limit.** *NOMAX
- **Expiration date.** The end date for maintenance and license validity.
- **Vendor Data.** This is the 7-digit code supplied with the license key

The information entered will not be accepted if any of the information is incorrect. The program will check that the system serial number, processor group, license key and vendor data are correct before accepting the data. If you have any problems with the codes other than typing errors please contact your supplier for support.

If you use the ADDLICENSE option, you will be required to fill in all the information as above but the following information will not be entered automatically

- Product Identifier “ING4ISC”
- License Term “V3R0”
- Feature “5001”
- System Serial Number *Your iSeries Serial Number*

Any errors with the license key installation will be logged in your job log. This information will be needed by support to resolve any issues.

A new license auto update processes has been added which will check the current license expiration against the shield website for a later key, if a key is found it will be automatically downloaded and installed. The command LICMAINT is available for this purpose which can be added to a JOBSUDE for regular checking.

Note:

We strongly advise against running the request more than once per week.

Hardware and software prerequisites

To run AAG the following Hardware and Software is required:

Hardware

AAG runs on any Linux capable hardware.

Current supported OS: (Debian, Rasbian, Ubuntu, Centos7&8, Oracle 8)

NG4i runs on any Power system running iOS above V7R2

Software

For the installation of AAG the following software is required

Appropriate Linux version

MySQL database (MariaDB)

Nagios
Open SSL (for secure connectons

For all installation of NG4i the following levels of iOS are required

iOS V7R2M0 or higher

Note: running NG4i on a system which is not running a currently supported i/OS version will negate the ability for fixes to be provided by Shield Advanced Solutions for any problems that originate in the OS or use API's no longer supported at that level.

Configuring NG4i on the IBM i.

The IBM i responders need to be set up to allow the Nagios requests to be handled. The configuration menu can be reached via the NG4i menu or using the command GO NG4ICFG after adding NG4I30 to the library list. Once on the configuration menu take option 1 to show the current NG4i Configuration.

```

Configure NG4i settings
Server Port . . . . . : 49140
Number of jobs . . . . . : 3
Secure Connect . . . . . *NO
HA4i installation library . . . . . *NONE
EM4i installation library . . . . . *NONE
API key . . . . . : K2hFZViPE4v5GGV7PPBw6sJtvURbQguV
FTP Website . . . . . WWW.SHIELDADVANCED.COM

Remote IP Nagios Server . . . . . *ANY

F3=Exit F12=Cancel
(c) Copyright Shield Advanced Solutions (Canada) Ltd. 1997 - 2023
Bottom

```

The following parameters can be set.

Number of jobs	This is the number of jobs launched to respond to the Nagios requests. You will need to adjust depending on the frequency of the requests coming from Nagios.
Secure connect	Determines if the connection between the Nagios Server and the IBM i are to be encrypted. If you use secure you will need to create and deploy the certificates from the IBM i to the Nagios Server as the product uses the certificate for authorization and encryption.
EM4i Library	The installation library of EM4i if installed. This is required if you want to the EM4i specific check commands provided with AAG.
HA4i Library	The installation library of HA4i if installed. This is required if you want to the HA4i specific check commands provided with AAG.
FTP Website	The website where updates will be retrieved from
Remote IP Nagios Server	The IP address from where to accept status requests. Setting to *ANY will allow requests to be accepted from any remote Nagios XI server.

Note: The port setting is updated by the program when enter is pressed to a pre-set port number. These ports must be available for the process to work. 49140 for non secure and 49143 for secure communications. The API key is generated on install or using the GENAPIKEY command.

Starting and stopping NG4i

The processes should be running 24x7 on the IBM i in order to respond to the requests from the Nagios Server.

Starting the NG4i processes can be carried out via the Operations menu (available from the NG4i menu) and using Option 1 or by using the command STRNG4I.

Ending the processes can be carried out via the Operations menu and using Option 2 or by using the command ENDNG4I.

Active processes IBM i

The following is a representation of the active jobs running on a typical system

```
Work with Active Jobs                               SAS1005
                                                    12/01/25 11:14:17 EST
CPU %:   18.3   Elapsed time:  00:00:03   Active jobs:  196

Type options, press Enter.
 2=Change  3=Hold  4=End   5=Work with  6=Release  7=Display message
 8=Work with spooled files 13=Disconnect ...

Current
Opt Subsystem/Job  User      Type  CPU %  Function      Status
-----
   NG4ISBS30      QSYS      SBS   1.0    PGM-NG4I001   DEQW
   NAGRSPCLNT     NG4IUSER  BCI   1.7    PGM-NG4I001   TIMA
   NAGRSPCLNT     NG4IUSER  BCI   1.7    PGM-NG4I001   TIMA
   NAGRSPCLNT     NG4IUSER  BCI   1.7    PGM-NG4I001   TIMA
   NGSVR          NG4IUSER  BCH   1.2    PGM-NG4I000   DEQA

                                                    Bottom

Parameters or command
====>
F3=Exit   F5=Refresh   F7=Find   F10=Restart statistics
F11=Display elapsed data  F12=Cancel  F23=More options  F24=More keys
```

NGSVR Provides control functions for the NGRSPCLNT jobs

NGRSPCLNT Reacts to incoming requests from the remote system.

NG4i Commands

NG4i has a number of commands which allow the automatic management of certain features.

The following commands are provided to assist with product automation/management and take no parameters.

AUTOUPD

Allows the automatic retrieval and apply of the updates available for NG4i

DISHOSTCHK

Disables the host check for this host on the Nagios XI Server.

DISHOSTNTF

Disables notifications for this host on the Nagios XI Server.

DISHOSTSVC

Disables all service checks for this host on the Nagios XI Server.

ENDHOSTCHK

Enables the host check for this host on the Nagios XI Server.

ENBHOSTNTF

Enables notifications for this host on the Nagios XI Server.

ENBHOSTSVC

Enables all service checks for this host on the Nagios XI Server.

GENAPIKEY

Generates a new API key which is used for communications with the remote Nagios Server.

PRTKEYINF

Prints the data required by Shield Advanced Solutions for generating a new key for the product.

The following commands require parameters to be passed.

BLDDBF

Builds the database file required by NG4i.

Parms :

TYPE *ALL/ *CFG All files of just the configuration file.

Note: Do not use this command without the express permission of shield support representative as it may render the product unusable.

CHKMONSVR

Checks that the remote Nagios server is responding to a ping check.

Parms :

MONSVR IP address of the remote server.

DISSVCCHK

Disables a specific service check for this host on the Nagios XI Server.

Parms:

SVC Service name.

ENBSVCCHK

Enables a specific service check for this host on the Nagios XI Server.

Parms:

SVC Service name.

ENDNG4I

Ends the running processes. No requests for status will be returned to the Nagios server.

Parms :

JOBRESTART If the jobs are to be restarted by the NGJOBCHK request.

GETGRPPTF

Determines what group PTFs are required and downloads them.

Parms:

ACT Action required: *SBM submit the requests and download the PTF's. *RPT generate a report for the PTF's that are required.

DEV The device used to hold the downloaded PTF's (*IMGCLG/*SAVF)

IMGCLG Image Catalog Name (DEV = *IMGCLG)

CLGDIR Image Catalog Directory

GETSBPTF

Determines what PTF's are required for CVE's and downloads them.

Parms:

CHKDAT Date to search the online DB for CVE's.

ACT Action required: *SBM submit the requests and download the PTF's. *RPT generate a report for the PTF's that are required.

DEV The device used to hold the downloaded PTF's (*IMGCLG/*SAVF)

IMGCLG Image Catalog Name (DEV = *IMGCLG)

CLGDIR Image Catalog Directory

LICMAINT

Checks the license server for any new license keys available for the product.

Parms:

DAYS Days ahead of the current key expiry to check the server.

MIGRATE

Migrate from previous version.

Parms:

OLDDIR Previous install directory.

NEWDIR New install directory.

NGJOBCHK

Check the status of the NG4i jobs and restart if required.

Parms:

DELAY Delay between resubmission of the JOBSUDE.

JOBNAME Name to use for the JOBSUDE.

RTVLICSTO

Retrieve the license key via the local license store.

Parms:

LICSVR IP address of the local license store.

SNDSVCCHK

Send a passive service check for this host to the Nagios XI Server.

Parms:

SVC Service name.

DTA Data that will be shown for the service status, if you want to pass performance data use the '|' character followed by the performance data.

Note: The service must be able to receive passive checks or the request will not run. The passed in service name must match exactly the service name defined to Nagios XI.

SNDHOSTCHK

Send a passive host check for this host to the Nagios XI Server.

Parms:

DTA Data that will be shown for the service status, if you want to pass performance data use the '|' character followed by the performance data.

Note: The service must be able to receive passive checks or the request will not run. The passed in service name must match exactly the service name defined to Nagios XI.

STRNG4I

Start NG4i processes.

Parms :

JOBRESTART If the jobs are to be restarted by the NGJOBCHK request.

VFYCHKSUM

Verify the checksum for the downloaded save file.

Parms:

FILE Save file name

TYPE Save file type (*UPD=update *LPP=base install)

Configuring Nagios with Nconf and AAG commands.

Note: Since the release of V2R1 Shield provides a web-browser interface to each of the following commands. Find these menus by clicking the “Commands” tab from the main AAG menu. Explanation of the web-browser interface will follow this commands section.

Provided with AAG are several commands to expedite the configuration of an IBM i host. To configure an IBM i system first we must add the host. Using a secure terminal to the Linux partition running our Nagios build (SAS builds can use the Cockpit interface) we can run the following commands:

There are 3 steps to adding the relevant configuration objects to Nagios, each of the commands listed below will generate the required objects and links to allow the various IBM i status to be retrieved.

System definition describes the connection between the Nagios Server and the IBM i, it is represented by the host object under Nagios.

Check commands are the interface to the programs or scripts that will be called to pull back the information from the IBM i.

Services are the wrappers that determine how often the status is requested from the IBM i via the check commands and any attributes that are required to retrieve the data and set the notifications within Nagios. A single check command can be used to pull status back for the IBM i for many objects/jobs.

Note: The commands are located in “/usr/local/nagios/share/sas”. Ensure your path variable is set to include that directory before running the commands.

addSystem Command

Adding a system to the Nagios configuration uses the addSystem command. The following image shows how the process flows when called.

```
chrish@sas-nconf:~$ addSystem
System name: SAS2
Address: SAS2.shield.local
User: CHRISH
Password:
Confirm Password:
Secure Connect[y/n]: y
Add Host to Nagios?[y/n]: y

[ Initializing NConf perl-API (library version 0.3, written by A. Gargiulo) ]
[ Copyright (c) 2006 - 2013 Sunrise Communications AG, Zurich, Switzerland ]

[INFO] Started executing /usr/local/nagios/share/nconf/bin/add_items_from_csv.pl
[INFO] CSV syntax found in file header. Using it.
[INFO] Adding host 'SAS2'
[WARN] Mandatory attribute 'host-preset' missing for host 'SAS2'. Using default value: 'linux-server'.
[INFO] Successfully added host 'SAS2'
[INFO] Finished running /usr/local/nagios/share/nconf/bin/add_items_from_csv.pl
chrish@sas-nconf:~$
```

addSystem Command example

Running the command will prompt the user to enter information required to configure the IBM i host to Nagios. The following information will be collected.

System Name	System identifier (this must match the NConf Hostname)
System Address	The resolvable TCP/IP name assigned to the system or IP address.
Is this a HMC?	If the system you are adding is a HMC (Or a VIOS system), respond with ‘Y’. This sets the HMC flag which is critical to configure an HMC

	host.
User	The user profile that will be used to run the collection requests on the IBM i.
Password	Password for the profile above
Confirm Password	Confirmation password (must match above)
Secure Connect	Is the IBM i running a secure server for NG4i
Add Host to Nagios	Add the host to Nagios
Push NG4i.SAVF to LPAR? [y/n]	Selecting 'Y' will upload the SAVFs required for NG4i install to the host via FTP using inputted username and password.

Notes:

Secure connections will require the installation of certificates that are acceptable by the IBM i. Self-generated certificates are acceptable.

The User Profile entered must have enough authority to extract the status from the IBM i. (we do not suggest using QSECOFR although it can be used).

Setting the Add to Nagios to 'no' will still generate the IBM i connection objects but will not register the host in Nagios.

This command is also used to save passwords and users for Pushover Ack MYSQL login and SSL Certs login.

Once the system has been generated you can view the information set up for the IBM i via the NConf interface, the following screen shows an example of an IBM host configured to Nagios viewed via the NConf interfaces.

Note:

Ensure these values are correct for your IBM i before continuing.

Host will not be added to Nagios until the configuration has been deployed.

Home	Details of host: SAS2																					
Basic Items	<table border="1"> <tr><td>hostname</td><td>SAS2</td></tr> <tr><td>alias</td><td>SAS2</td></tr> <tr><td>address</td><td>SAS2.SHIELD.LOCAL</td></tr> <tr><td>host is collector</td><td>no</td></tr> <tr><td>max check attempts</td><td>5</td></tr> <tr><td>check interval</td><td>10</td></tr> <tr><td>retry interval</td><td>5</td></tr> <tr><td>notification interval</td><td>30</td></tr> <tr><td>notification options</td><td>d,u</td></tr> <tr><td>active checking</td><td>1</td></tr> </table>		hostname	SAS2	alias	SAS2	address	SAS2.SHIELD.LOCAL	host is collector	no	max check attempts	5	check interval	10	retry interval	5	notification interval	30	notification options	d,u	active checking	1
hostname	SAS2																					
alias	SAS2																					
address	SAS2.SHIELD.LOCAL																					
host is collector	no																					
max check attempts	5																					
check interval	10																					
retry interval	5																					
notification interval	30																					
notification options	d,u																					
active checking	1																					
<ul style="list-style-type: none"> › Show History › Show Host parent / child view › Generate Nagios config › Hosts Show / Add › Hostgroups Show / Add › Services Show / Add › Advanced Services Show / Add › Servicegroups Show / Add 	<p>This item is linked to</p> <table border="1"> <tr><td>OS</td><td>IBM i</td></tr> <tr><td>notification period</td><td>24x7</td></tr> <tr><td>monitored by</td><td>Default Nagios</td></tr> <tr><td>host template(s)</td><td>generic-host</td></tr> <tr><td>host preset</td><td>linux-server</td></tr> <tr><td>check period</td><td>24x7</td></tr> </table>		OS	IBM i	notification period	24x7	monitored by	Default Nagios	host template(s)	generic-host	host preset	linux-server	check period	24x7								
OS	IBM i																					
notification period	24x7																					
monitored by	Default Nagios																					
host template(s)	generic-host																					
host preset	linux-server																					
check period	24x7																					
Additional Items	Template inheritance																					
<ul style="list-style-type: none"> › OS Show / Add › Contacts Show / Add › Contactgroups Show / Add › Checkcommands Show / Add › Misccommands Show / Add › Timeperiods Show / Add 	<p>Templates are applied in the following order:</p> <table border="1"> <tr><td>directly linked to host</td><td></td></tr> <tr><td></td><td>generic-host</td></tr> </table>		directly linked to host			generic-host																
directly linked to host																						
	generic-host																					
Advanced Items																						
<ul style="list-style-type: none"> › Host presets Show / Add › Host templates Show / Add › Service templates Show / Add › Host deps. Show / Add › Service deps. Show / Add 																						
Nagios servers																						
<ul style="list-style-type: none"> › Central monitors Show / Add › Distrib. collectors Show / Add 																						
Administration																						
<ul style="list-style-type: none"> › Edit static config files › Attributes Show / Add › Classes Show / Add 																						
Logout																						

Example of IBM i configured within NConf

PushNG4iSAVF Command

Part of configuring a Nagios IBM i host is to install NG4i responder jobs on the LPAR. In order to install NG4i and bring it to the latest updates, several SAVFs need to be pushed to the LPAR. Typically, this requires you to FTP the SAVFs up to the LPAR which can be a hassle and takes a lot of time if you have a large amount of LPARs to add. We have streamlined this process with the PushNG4iSAVF command. Simply enter the system name you wish to use and both the install and update SAVFs will be FTPed to your LPAR. For this command to work, the USER entered when adding the system must have FTP access. It is possible to use *ALL as the system name, this will allow you to walk through all of the systems you have added. You will be asked for each system if you would like to push the SAVFs, simply answer 'Y' or 'N'.

addChecks Command

Adding the check commands to the Nagios configuration uses the addCheck command. The following image shows how the process flows when called.

```
chird@sas-nconf:/usr/local/nagios/share/sas$ ./addChecks
Add Shield General check commands? y
Add IBM i Status check commands? y
Add HA4i check commands? y
Add EM4i check commands? y
Add HMC check commands? y
Add BRMS check commands? y
Add Mimix check commands? y
Add PowerHA check commands? y
Shield General commands successfully added.
IBM i Status commands successfully added.
HA4i commands successfully added.
EM4i commands successfully added.
HMC commands successfully added.
BRMS commands successfully added.
MMX commands successfully added.
PowerHA commands successfully added.
```

addChecks Command example

Running the command will prompt the user for each available group of commands to be installed. The following groups of check commands are available:

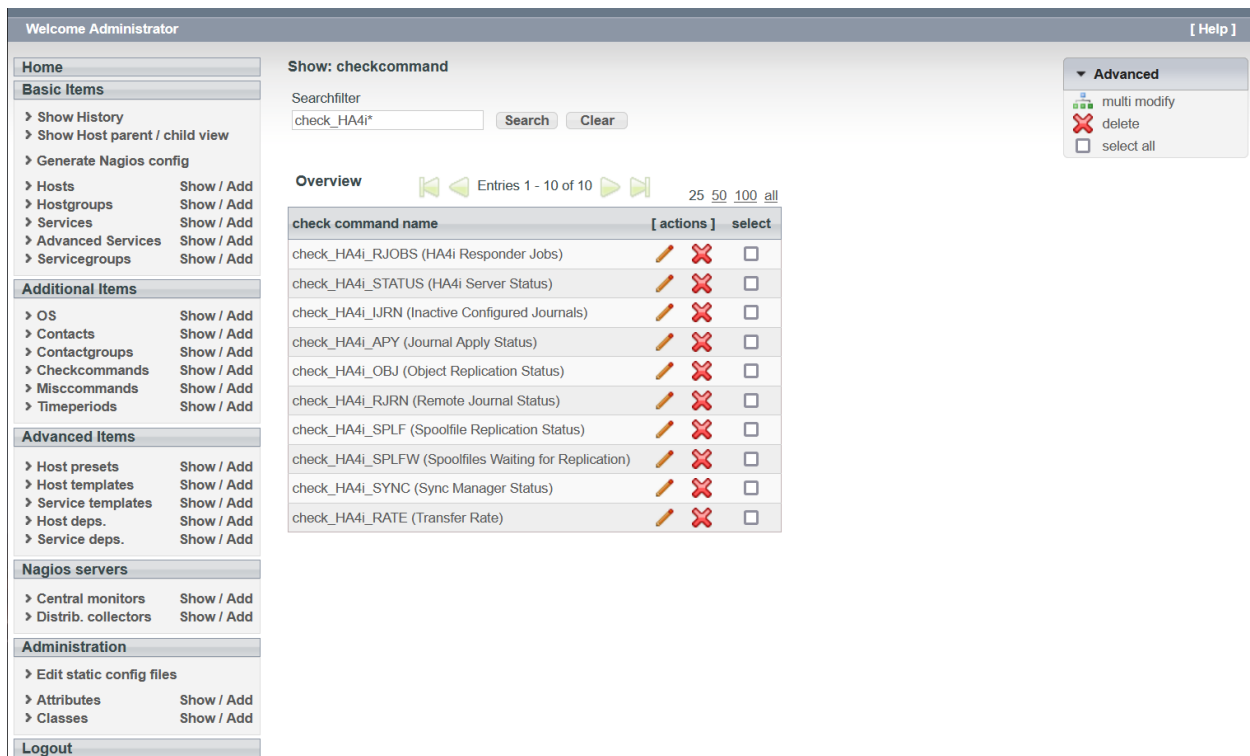
HA4i	Shield’s HA4i product specific checks. HA4i installation is a requirement.
EM4i	Shield’s EM4i message notification specific checks. EM4i installation is required.
Shield	Shield’s general check selection. These checks are not product specific.
Status	IBM i status related checks
HMC	These are check commands to monitor the HMC not an IBM i.
Mimix	Mimix high availability checks
PowerHA	IBM’s PowerHA related checks
BRMS	IBM’s BRMS related checks
VIOS	VIOS related checks

If you do not have the prerequisite applications installed for the Shield applications enter N when prompted to install the check commands. This process can be repeated at a later time should the applications be installed. This process is also repeated after an update to add the latest check commands to your nconf.

Note:

Check commands are paired to a host using Nagios services.

The following image shows the check commands available for a specific group after the command has been run.



HA4i Check commands viewed in NConf

To ensure all check commands were added appropriately, it is recommended to view these checks within the “show - check commands” section of Nconf.

addServices Command

To run checks against each IBM i host, the host and check commands need to be linked in the form of a service. A service determines the parameters passed into the check command and holds the values for interpreting the results for notification via the Nagios interface. The following image shows the process flow for adding services.

```
chrish@sas-nconf:~$ addServices SAS2 SHIELD
Command: /usr/local/nagios/share/nconf/bin/add_items_from_csv.pl -c service -f /usr/share/sas/CSV/SAS2-SHIELD_Services.csv -d ,

[ Initializing NConf perl-API (library version 0.3, written by A. Gargiulo) ]
[ Copyright (c) 2006 - 2013 Sunrise Communications AG, Zurich, Switzerland ]

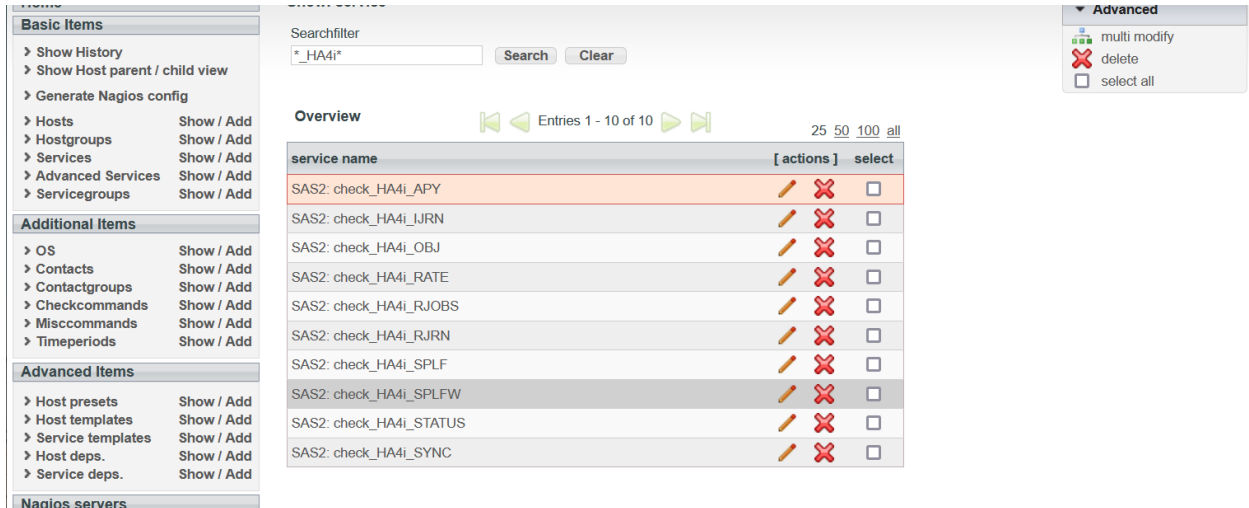
[INFO] Started executing /usr/local/nagios/share/nconf/bin/add_items_from_csv.pl
[INFO] CSV syntax found in file header. Using it.
[INFO] Adding service 'SAS2;;check_Shield_KEYEXP'
[INFO] Successfully added service 'SAS2;;check_Shield_KEYEXP'
[INFO] Adding service 'SAS2;;check_Shield_SBSSRCH'
[INFO] Successfully added service 'SAS2;;check_Shield_SBSSRCH'
[INFO] Adding service 'SAS2;;check_Shield_JOBSRCH'
[INFO] Successfully added service 'SAS2;;check_Shield_JOBSRCH'
[INFO] Adding service 'SAS2;;check_Shield_RPYW'
[INFO] Successfully added service 'SAS2;;check_Shield_RPYW'
[INFO] Adding service 'SAS2;;check_Shield_DSBPRF'
[INFO] Successfully added service 'SAS2;;check_Shield_DSBPRF'
[INFO] Adding service 'SAS2;;check_Shield_SBSJOB'
[INFO] Successfully added service 'SAS2;;check_Shield_SBSJOB'
[INFO] Adding service 'SAS2;;check_Shield_JOBQ'
[INFO] Successfully added service 'SAS2;;check_Shield_JOBQ'
[INFO] Adding service 'SAS2;;check_Shield_RCVR'
[INFO] Successfully added service 'SAS2;;check_Shield_RCVR'
[INFO] Adding service 'SAS2;;check_Shield_CACHEBAT'
[INFO] Successfully added service 'SAS2;;check_Shield_CACHEBAT'
[INFO] Adding service 'SAS2;;check_Shield_TOPJOB_CPU'
[INFO] Successfully added service 'SAS2;;check_Shield_TOPJOB_CPU'
[INFO] Adding service 'SAS2;;check_Shield_TOPJOB_CTG'
[INFO] Successfully added service 'SAS2;;check_Shield_TOPJOB_CTG'
[INFO] Finished running /usr/local/nagios/share/nconf/bin/add_items_from_csv.pl
chrish@sas-nconf:~$
```

addServices command example

The command must be called with the following information. The above image shows adding the SHIELD services to the SAS2 host. The default parameters will be set as the services are added. These parameters can be modified via the PHP commands “Defaults” tab.

Host	The name of the IBM i host created with the addSystem command.
Group	The check command group to be added. -(Shield, Status, EM4i, HA4i, BRMS, PowerHA, MMX, VIOS)

Once the services are added they can be viewed via the NConf Services interface. The following image is an example of the services added by running the above command.

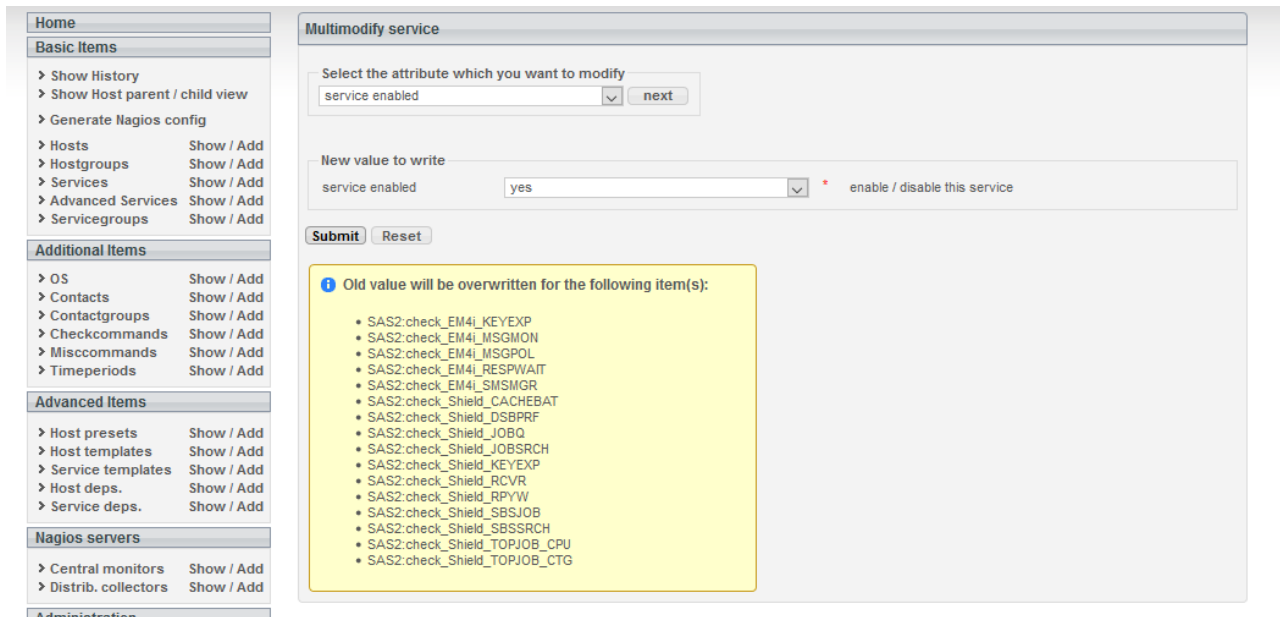


HA4i Add Services viewed in NConf

Note:

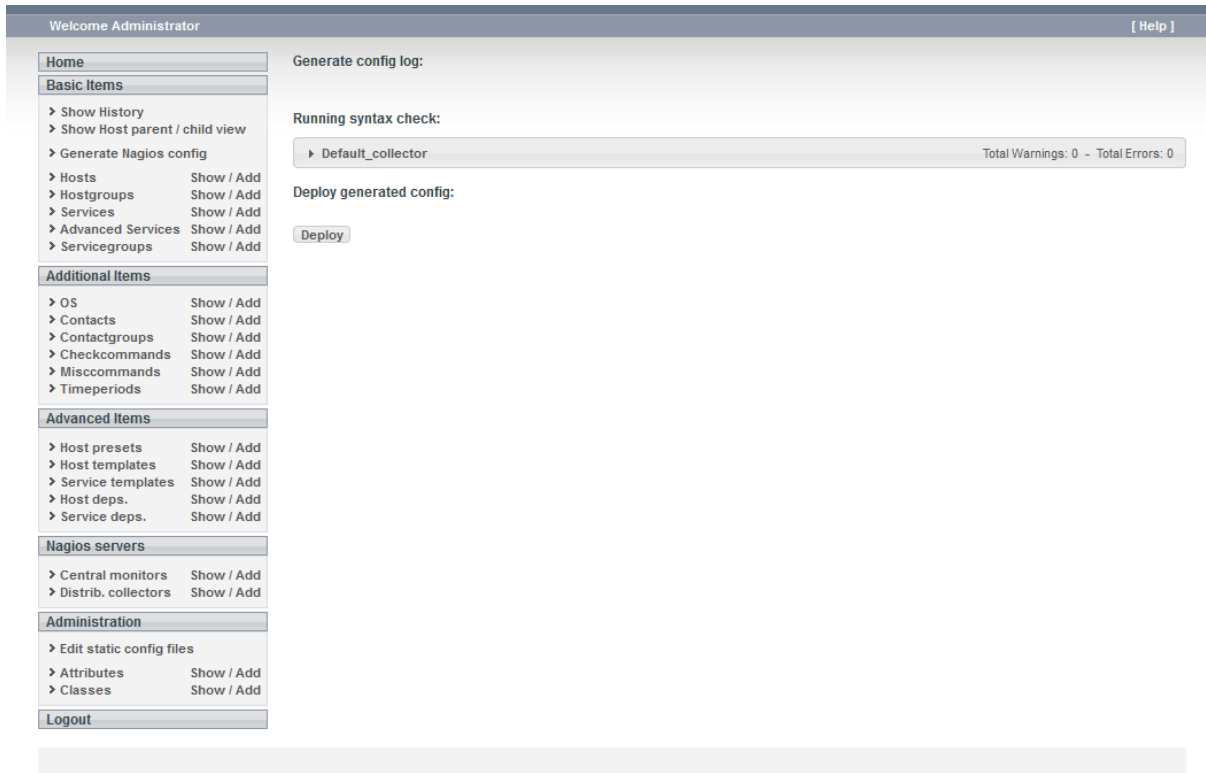
When Services are added to our host they will be disabled by default. Select all of the Services you would like to enable and then at the top right of the window select multi modify from the advanced drop down.

To enable the services after they have been configured you can use NConf to enable them all at once. Select each of the services you want to enable and then click the multi modify link. Then select service enabled from the attribute drop down and click the submit button. The following screen shot shows a sample of services being enabled.



NConf Services enabled example

Once the configurations have been generated you will need to generate and deploy the config for Nagios to start monitoring the services against the host. Click the Generate Nagios Config from the left hand column for the following screen to be displayed.



Generate Config and deploy

Pressing the Deploy button will cause Nagios to implement the services and immediately send out a status request to the IBM i.

Note:

On initial deployment it appears Nagios spawns a thread for each configured services to each of the hosts, this can cause some services to report back that they were unable to connect to the host (timeout). This is expected and can be ignored as over time the requests will be spread out meaning the service requests do not overwhelm the IBM i responder jobs and the status is reported back correctly.

AAG's Web-based Commands Menu.

The previous commands are now able to be called with a menu system that is found under the “Commands” tab on the main AAG page.

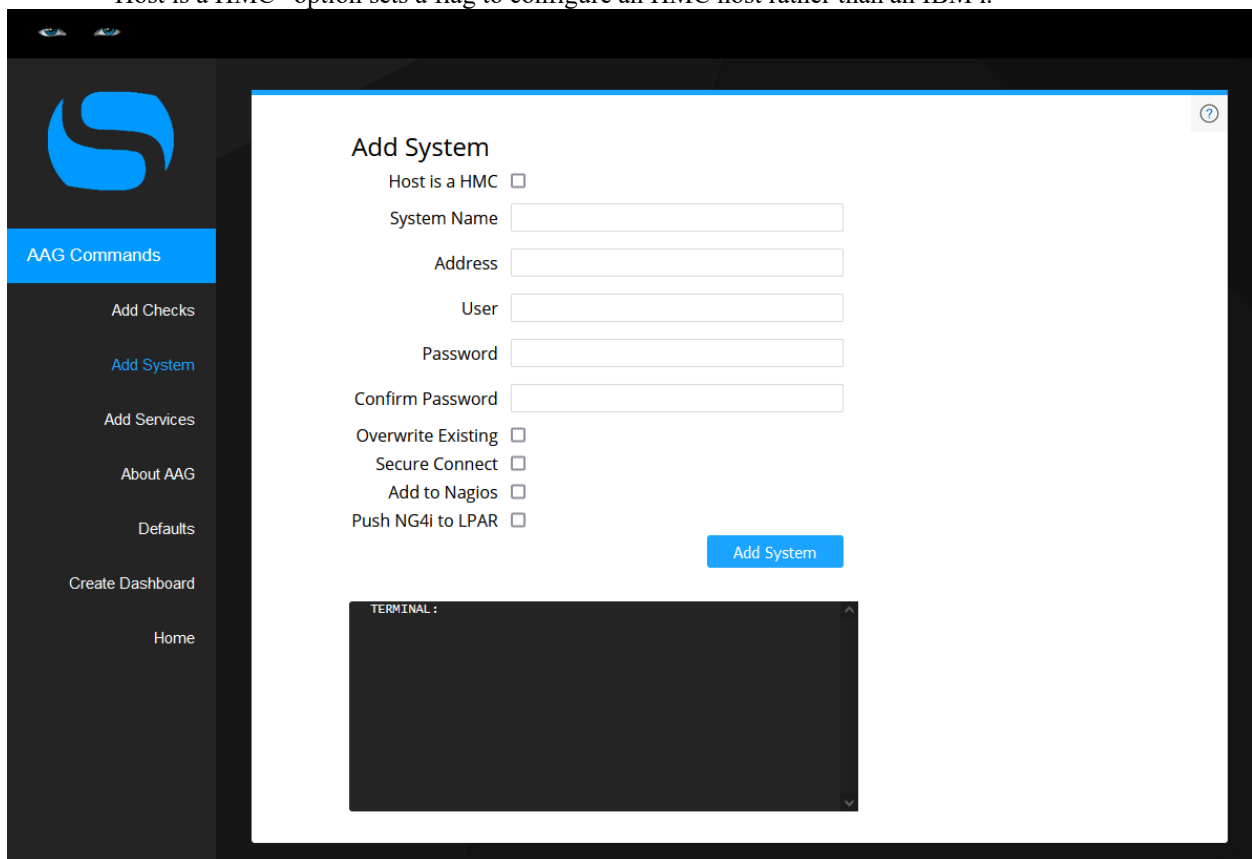
Add System

To add a new system to AAG we can fill in the required input fields in the AddSystem menu. If the system already exists and we are updating the stored information, select the “Overwrite Existing” check box. This will delete the old .BIN file and create a new one.

If this IBM i has been setup to connect via a secure connection we need to select “Secure Connect” to ensure AAG connects on the correct port using the SSL Certificate to authenticate. If the system you are adding is an HMC, using a non-secure connection is not currently supported and this option will be ignored.

Finally, selecting the “Add to Nagios” check box will push this system through to Nagios as a HOST. If we are using this function to simply add the .BIN file for authentication purposes and not adding an IBM i then we do not want to select this option.

“Host is a HMC” option sets a flag to configure an HMC host rather than an IBM i.



The screenshot displays the 'Add System' web form within the AAG interface. On the left is a dark sidebar with a blue 'S' logo and a menu including 'AAG Commands', 'Add Checks', 'Add System', 'Add Services', 'About AAG', 'Defaults', 'Create Dashboard', and 'Home'. The main content area is white and titled 'Add System'. It contains the following fields and options:

- Host is a HMC
- System Name
- Address
- User
- Password
- Confirm Password
- Overwrite Existing
- Secure Connect
- Add to Nagios
- Push NG4i to LPAR

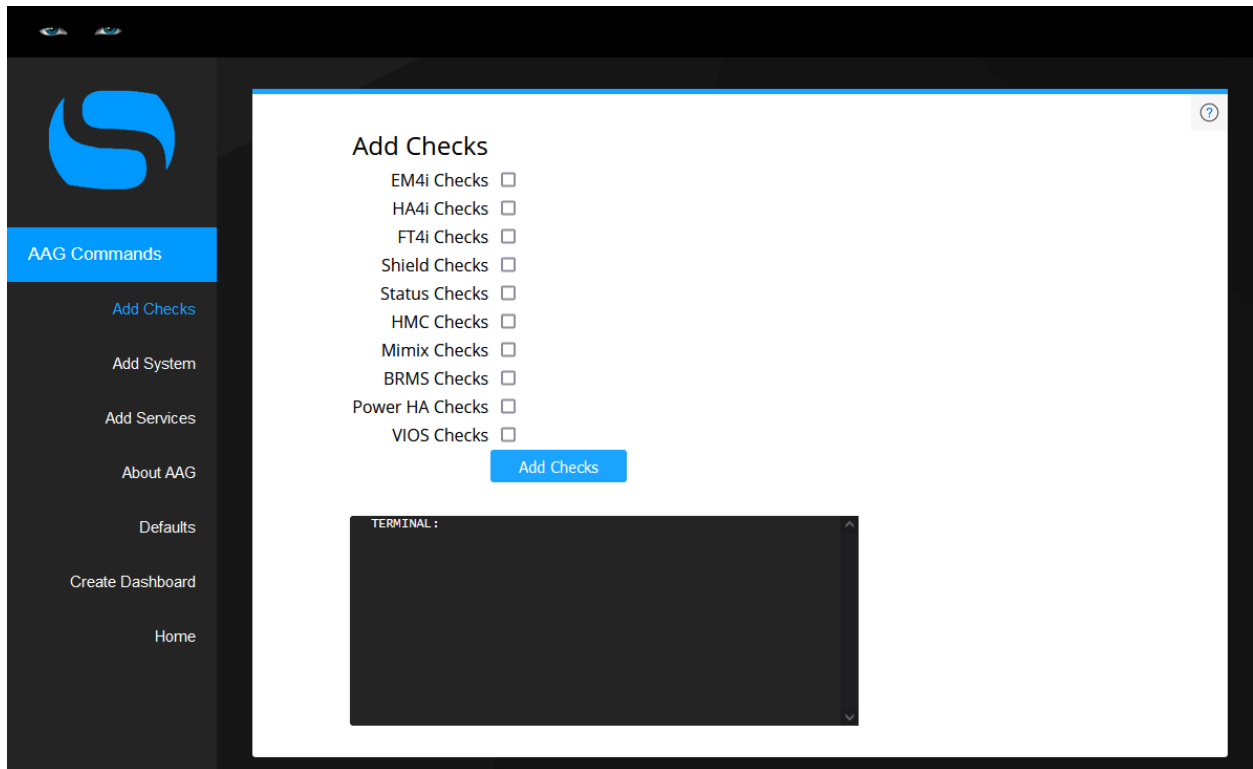
A blue 'Add System' button is positioned to the right of the form fields. Below the form is a terminal window with a black background and white text, labeled 'TERMINAL:' at the top.

Add Checks

Selecting each of the categories of checks will add the AAG checkcommands to Nagios from the list provided by Shield. These are listed in order of their release date so adding new checks after an update will add the latest checkcommands to Nagios without adding the checks that already exist.

**NOTE: If you are running this command after an update or when Shield checks already exist in Nagios you will see an "ERROR" dictating a check already exists. If the check truly already exists, this is normal. Nagios will attempt to add each check sequentially and drop out when a check already exists.*

It is recommended that you only add the checkcommands you will need on your system. However, there are no consequences if check commands are added and never used for a service.



Add Services

Adding Services to a HOST will attach a checkcommand to a specified HOST with timeperiod and notification settings. We can add Services to our Nagios HOSTs with default settings provided by Shield using this command. It is highly recommended that you review the defaults within your new services to ensure the service is running as you expect. If you are to add a run of services to multiple hosts, it is possible to edit the defaults in the “Defaults” tab prior to adding the services.

When Services are added using this method they will be defaulted to “Enabled = no” and will show as a “RED” entry when viewed in NCONF. For these Services to become active simply change the “Enabled” status in NCONF.

This command will act in a similar manner to added checkcommands. If a service already exists for a HOST the auto add feature will stop adding entries. Shields default Services are added sequentially by their release date so that a user may add new services after an update.

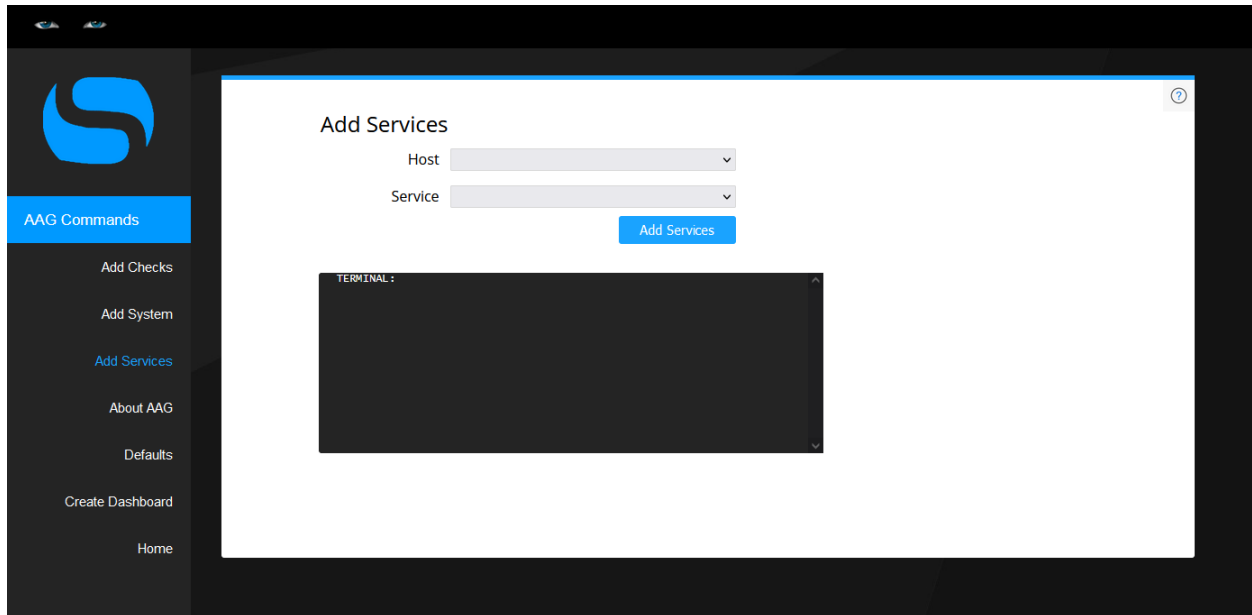
**NOTE: If you have just added a HOST and it is not present in the Host drop down. This is because the list of HOSTs are picked up from the deployed config. Head to Nconf and deploy your config with the newest HOST. Refreshing the commands page, you should find your HOST in the drop down. If you do not, please contact Shield!*

You will notice either (IBM i) or (HMC) listed beside each host in the drop down. Although it is possible to add HMC services to an IBM i and vice versa, these simply will not work.

**NOTE: if you receive the following error:*

```
TERMINAL :  
Failed to open .BIN File. [/usr/local/nagios/share/sas/Storage  
/MYSQL.bin]
```

This is because this function leverages SQL in the background. A host named “MYSQL” must be created containing the username and password for the local MYSQL login. Do not select “Add to Nagios” when creating this host.



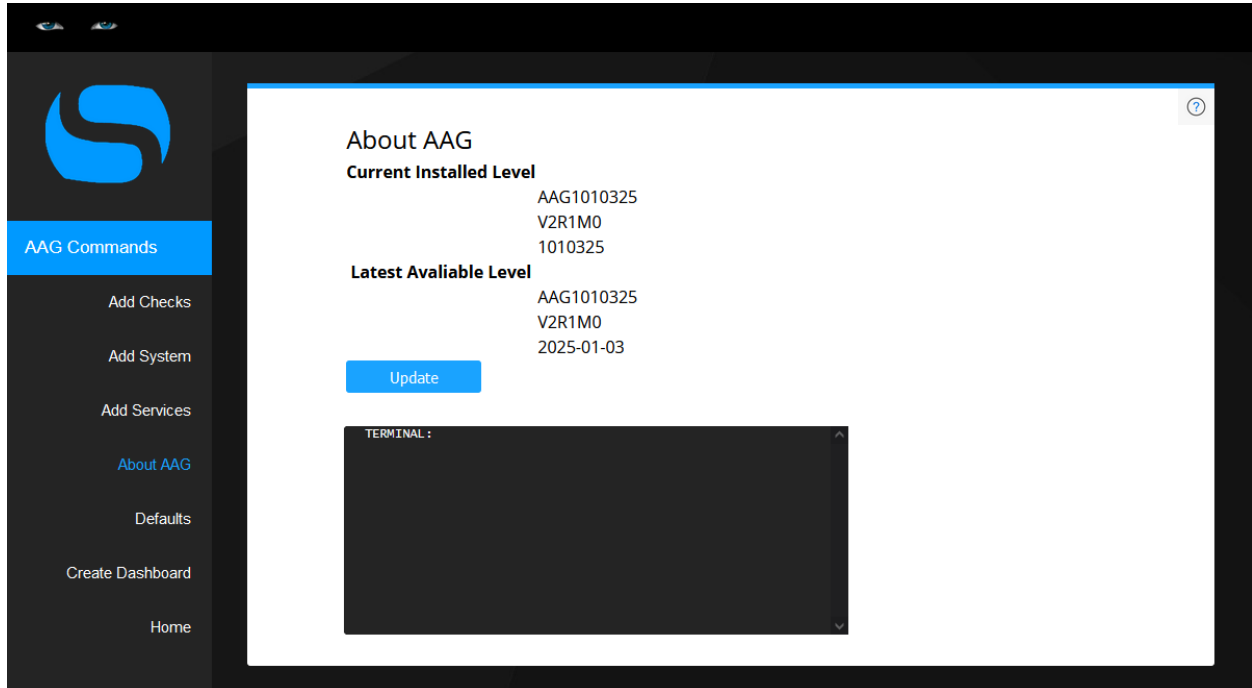
About AAG

Since V1R1M0, it is possible to update AAG via this menu.

This page displays the current installed level of AAG, as well as the latest level available from Shield. Simply click the update button to update the AAG files. If you are looking for the drop down to enter the system type, this has been removed as of V2R0M0 and replaced with an automated feature to pull the OS.

**NOTE: for this to be used several users must be granted permissions to access our update file. Please contact Shield to make this change.*

Review the outputted text in the Terminal window to ensure no errors were present in the update. Should you find errors, please contact Shield and we will make the appropriate changes.



The screenshot displays the 'About AAG' web interface. On the left is a dark sidebar with a blue 'S' logo and a menu including 'AAG Commands', 'Add Checks', 'Add System', 'Add Services', 'About AAG' (highlighted), 'Defaults', 'Create Dashboard', and 'Home'. The main content area has a white background and a blue header. It displays the following information:

- About AAG** (with a help icon)
- Current Installed Level**
 - AAG1010325
 - V2R1M0
 - 1010325
- Latest Available Level**
 - AAG1010325
 - V2R1M0
 - 2025-01-03
- An **Update** button.
- A **TERMINAL :** window at the bottom, which is currently empty.

Defaults

Released in the AAG1112122 update, is the Defaults form. This form will allow users to change the defaults used when adding bulk services to a new host. Previously the only defaults available were those provided by Shield and they were hard coded into the addServices function. This was not beneficial to users adding large amounts of hosts like our MSP clients. We have changed the defaults to be stored in a database rather than hard coded. This will allow users to modify these values to fit the majority of the hosts they are adding. Also added with this change, is the ability to create custom categories to group sets of check commands together which then can be added to a host as a set.

The screenshot shows the 'Change Defaults' form within the AAG/NG4i application. The left sidebar contains navigation options: 'AAG Commands', 'Add Checks', 'Add System', 'Add Services', 'Update AAG', 'Defaults' (highlighted), and 'Home'. The main content area is titled 'Change Defaults' and includes the following fields and controls:

- Category: All (dropdown)
- Default Entry: (dropdown)
- Checkcommand: (dropdown)
- Service Enabled:
- Check Period: (text input)
- Notification Period: (text input)
- Contact Groups: (text input)
- Notes: (text input)
- Event Handler Enabled:
- Max Check Attempts: (text input)
- Check Interval: (text input)
- Retry Interval: (text input)
- First Notification Delay: (text input)
- Notification Interval: (text input)
- Notification Options: (text input)
- Active Checking:
- Passive Checking:
- Notifications Enabled:
- Check Freshness:
- Parameters: (text input)

An 'Apply Changes' button is located at the bottom right of the form. Below the form is a 'TERMINAL' window, which is currently empty.

Using Ansible to take action with AAG.

Since version AAG1021425 AAG is able to run playbooks using Ansible when a service fails. This requires a fair amount of configuration. We will not outline how to install Ansible, but once you have Ansible installed follow the steps below to connect your Ansible playbooks with your AAG monitoring.

First, create a misc command called “RunPlaybook”. Use the following command for the command line:
`/usr/local/nagios/share/sas/runPlaybook $HOSTNAME$ $_SERVICEPLAYBOOK$ $_SERVICEEXTRAVARS$`

Next, we will need to add the “playbook” and “extra variables” fields to our service attributes:

The image shows two side-by-side screenshots of the 'Modify attribute' configuration interface. The left screenshot is for the attribute '_playbook' and the right is for '_extravars'. Both screenshots show the following fields:

- Main:**
 - Nagios-specific attribute name: ? *
 - friendly name (displayed in GUI): ? *
 - description, example or help-text: ?
- Class and datatype:**
 - attribute belongs to class: ? *
 - attribute datatype: ? *
 - item(s) to be assigned: ? *
 - list of possible values separated by ";;": ?
 - pre-defined value(s): ?
 - max. text-field length (chars): ?
- Advanced linking options:**
 - link selected item(s) as children?: ?
 - link selected item(s) bi-directionally?: ?
- Display and output:**
 - attribute is mandatory?: ?
 - attribute is visible?: ? *
 - write attribute to configuration?: ? *
 - ordering: ?
 - naming attribute?: ? *

Ensure to use same spelling including the “_” for the command to work. We ordered these as 23 and 24 in the service layout so they are grouped together

The image shows a screenshot of the service configuration interface. The 'ansible playbook' field is set to 'StartEM4i' and the 'Extra Variables' field is set to 'version=EM4I11'. Below these fields are two lists: 'available items' containing 'services2' and 'selected items' containing 'services1'.

The Ansible playbook input will be the filename of the playbook you wish to run. This playbook must be located in
`/usr/local/nagios/share/sas/playbooks`

Extra Variables are passed into ansible playbooks with the format:
[variable name]=[variable value]

Each additional variable passed must be separated by a space. **If no extra variables are required, input “*NONE” in this field.**

For NagiosXI installs use the Custom variables feature found under the Misc Settings tab in a service.

Manage Custom Variables [Close]

Name	Value	Actions
_playbook	StartEM4i	
_extravars	EM4I11	

Name: Value: [Insert >](#)

[Close](#)

Finally, we need to create a usergroup called “runPlaybook” which includes a contact with the same name:

The screenshot shows the 'Modify contact' configuration page in Nagios XI. The contact name is 'RunPlaybook'. The alias is also 'RunPlaybook'. The host notification period is set to 'none' and the service notification period is '24x7'. The service notification options are set to 'c'. The e-mail address is 'na'. The contact is assigned to the 'RunPlaybook' usergroup. The host notification commands and service notification commands are both set to 'RunPlaybook'. The 'assign contact to contactgroup' section shows 'admins' in the available items and 'runPlaybook' in the selected items.

Field	Value	Notes
contact name	RunPlaybook	*
alias	RunPlaybook	*
host notification period	none	
service notification period	24x7	
host notification options		
service notification options	c	possible values: w,u,c,r,f,[n]
e-mail address	na	*
pager / phone nr.		(country code) + (prefix) + (number)
Pushover User Key		User pushover key
Pushover API Key		API key for pushover
Pushover device		Device notifications sent to
host notification commands	RunPlaybook	
service notification commands	RunPlaybook	
assign contact to contactgroup	runPlaybook	

This user will call the program “runPlaybook” instead of using a notification program when a service fails. For this user I have only used “c” in the “service notification options” so a playbook will only be run if a service is critical. Email address is required but not used. To connect our contact to our misc command we will add the RunPlaybook for both host and service notification commands. Host notification command does not apply here as host notification options were left blank, but is required to generate the nagios config.

Here is an example of calling a playbook to restart EM4i jobs if AAG finds one to be missing:

The service we will be using is check_EM4i_MSGMON

Modify service	
service name	check_EM4i_MSGMON *
service enabled	yes * enable / disable this service
check command	check_Shield_JOBSRCH *
assigned to host	SAS1004 *
check period	24x7 time period to run checks
notification period	24x7 time period to alarm

Should the service fail we want to send a notification to our admin user group and also run the playbook

contact groups	available items	selected items	responsible group
		admins runPlaybook	

We will set the playbook name to StartEM4i and the version to EM4I11

ansible playbook	StartEM4i	Ansible playbook to run on failure
Extra Variables	version=EM4I11	Ansible playbook variables

This is the play book we have created to start the EM4i jobs – StartEM4i.yml

```

chird@sas-nconf: /usr/local/nagios/share/sas/playbooks

GNU nano 3.2

---
- name: Start EM4i Jobs
  hosts: '{{ lpar }}'
  gather_facts: no

  tasks:
  - name: Start EM4i Via CLP
    ibm.power_ibmi.ibm_i_cl_command:
      cmd: 'CALL PGM('{{ version }}/EM4ISTR) PARM('{{ version }})'
  
```

The 'lpar' variable you can see on the third line will be filled in by \$HOSTNAME\$ from Nagios. Your Nagios hostname must match your Ansible host. This playbook then uses the ibmi modules to call a program on the IBM I to start the EM4i jobs. In order to handle the library list we found it better to get ansible to call a CL program on the IBM i.

Using AAG

Hosts

AAG is a polling solution that relies on a host configuration to contact the remote system and request the status of a specific service.

The information for each host is collected via batch scripts that can be called on the Nagios server, it will collect the address, username, password and secure setting for the connection and store them securely with encryption of the password. When a connection is initiated the user information will be used to sign on to the remote system and set the user as the profile the job runs under, this means the user must have the authority to run any commands required to extract the status information.

Note:-

If a secure connection is required, you will need to request and install certificates for the remote IBM i system on the Nagios server or the connection requests will fail. Information on generating and installing certificates can be found in the relevant manuals.

For IBM i hosts the remote system will need to have the NG4i product installed as it is required to retrieve the information and convert to ASCII for consumption by the Nagios server.

Services

Nagios services are the pairing of a check command and a host. By adding a service, Nagios will check the data attained by the check command, from the specified host, on a scheduled basis.

Check commands

Nagios uses check commands to query data from a host and then tests this data against user specified ranges. AAG provides a number of check commands specifically related to the IBM i platform and are made available via the NG4i LPP. The following are check commands are provided by NG4i to AAG.

Threshold and Ranges

The following formatting can be used for all ranges:

10	< 0 or > 10, (outside the range of {0 .. 10})
10:	< 10, (outside {10 .. ∞})
~:10	> 10, (outside the range of {-∞ .. 10})
10:20	< 10 or > 20, (outside the range of {10 .. 20})
@10:20	≥ 10 and ≤ 20, (inside the range of {10 .. 20})

Ranges work along the lines of Sets from discrete mathematics.

*NOTE – when using the format starting with ~ ... ensure to surround the range with “ ” as the command line will attempt to replace ~ with the users home directory if no “ ” are present.

HA4i Check Commands

check_HA4i_RATE

Returns the observed transfer rate between the HA4i *MGT and *NET system.

Purpose:

Provides an indication of the bandwidth available to HA4i for transferring objects and data between the *MGT and *NET system..

Service State Information	
Current Status:	CRITICAL (for 0d 0h 0m 9s)
Status Information:	CRITICAL-Connection Speed: 232Mb/s
Performance Data:	
Current Attempt:	1/5 (SOFT state)
Last Check Time:	10-27-2021 13:55:19
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.228 seconds
Next Scheduled Check:	10-27-2021 14:00:19
Last State Change:	10-27-2021 13:55:19
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 13:55:24 (0d 0h 0m 4s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Example of output from *check_HA4i_Rate*

The command can also be used to request a JSON string representing the complete status for HA4i. We do not create a service that pulls this information back as it cannot be used by Nagios for notification determination. This would require *NET /*MGT or *ALL to be entered as the type.

check_HA4i_APY

Returns the apply status from the *NET system. For each of the configured apply processes.

Purpose:

Retrieves the apply status for each of the configure Apply programs, this can be segmented to notify when an apply process reached a certain backlog, or an apply process is not running etc.

Parameters:

Critical Critical range to check Delta between last read and last applied.
Warning Warning range to check Delta between last read and last applied.
B-log Severity Severity level for back log errors. (0, 1, 2, 3)

The information is returned in the following format.

Journal : Local Journal name and library.
Apply Job Name : The job name assigned to the apply process.
Apply Status : The status of the apply job.
 *APPLYING Entries are being applied
 *WAITING Waiting for entries in the Remote Journal

Error : Errors logged [Y/N].
 Applied Entry : Last entry applied by the apply job.
 Last Entry : Last entry available in the Journal.
 Backlog : Entries not applied (this can be entries which are not required).
 Remote Journal : The remote journal name and library.

NOTE:

*This request must be run on the *NET system, running this request on the *MGT system will result in an error being returned.*

The following image provides an example of the information returned when this command is run.

Service State Information

```

Current Status: OK (for 1d 1h 0m 58s)
Status Information: All 5 journals are OK.

Journal : BATCHJRN B_JRN_LIB
Apply Job Name : HA4IDQ0000
Apply Status : *WAITING
Error : N
Applied Entry : 272036
Last Entry : 272036
Difference between last applied and last read: 0
Remote Journal : BATCHJRN BATCHRMT

Journal : BJRN BJRN_TST
Apply Job Name : HA4IDQ0001
Apply Status : *WAITING
Error : N
Applied Entry : 0
Last Entry : 0
Difference between last applied and last read: 0
Remote Journal : BJRN BJRN_TST@R

Journal : JTJRN JTBCHJRN
Apply Job Name : HA4IDQ0004
Apply Status : *WAITING
Error : N
Applied Entry : 197
Last Entry : 197
Difference between last applied and last read: 0
Remote Journal : JTJRN JTBCHJRN@R

Journal : QSQJRN COMMIT
Apply Job Name : HA4IDQ0002
Apply Status : *WAITING
Error : N
Applied Entry : 0
Last Entry : 0
Difference between last applied and last read: 0
Remote Journal : QSQJRN COMMIT@R

Journal : QSQJRN CORPDATA
Apply Job Name : HA4IDQ0003
Apply Status : *WAITING
Error : N
Applied Entry : 0
Last Entry : 0
Difference between last applied and last read: 0
Remote Journal : QSQJRN CORPDATA@R

```

check_HA4i_RJRN

Returns the information for each remote journal that is configured and not in *ACTIVE status. This allows the user to discover any remote journals which are not transmitting data changes to the remote system so the apply process can apply those changes to the remote database.

Purpose:

Provides a view of the remote journal status and provides the ability to send notifications if *INACTIVE remote journals are found.

Note HA4i STATUSCHK can be used for Automated Remote Journal Activation. This check will give early indication of errors which cannot be rectified by the STATUSCHK process.

Service State Information

Current Status:	OK (for 6d 1h 21m 54s)
Status Information:	All 5 remote journals are OK.
	Journal : BATCHJRN B_JRN_LIB Apply Job Name : HA4IDQ0001 Remote Journal : BATCHJRN BATCHRMT Status : *ACTIVE
	Journal : BCHJRN JT_BCHJRN Apply Job Name : HA4IDQ0005 Remote Journal : BCHJRN JT_BCHRMT Status : *ACTIVE
	Journal : BJRN BJRN_TST Apply Job Name : HA4IDQ0008 Remote Journal : BJRN BJRN_TST@R Status : *ACTIVE
	Journal : QSQJRN COMMIT Apply Job Name : HA4IDQ0004 Remote Journal : QSQJRN RMTCOMMIT Status : *ACTIVE
	Journal : QSQJRN CORPDATA Apply Job Name : HA4IDQ0000 Remote Journal : QSQJRN RMTQSQJRN Status : *ACTIVE
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 13:54:36
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.030 seconds
Next Scheduled Check:	10-27-2021 14:04:36
Last State Change:	10-21-2021 12:39:36
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:01:28 (0d 0h 0m 2s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

HA4i Remote Journal Status

Parameters:

No parameters to be passed for this check.

Note: The only parameter set in the config is for the severity attached to the notification. 1 = Warning, 2 = Critical.

The information is returned in the following format.

Journal :	Journal name and library
Apply Name :	Apply job name attached to the remote journal
Remote Journal:	Remote Journal name and library
RJ Status :	Remote Journal status
	- *ACTIVE
	- *INACTIVE

NOTE:

*This request should be run on the *MGT system, running this request on the *NET system will result in information being returned about the remote journals configured from the *NET system back to the *MGT system.*

check_HA4i_OBJ

Returns the Object replication status from the *MGT system.

Purpose:

Allows early notification of backlogs and errors as the Object replication process works through the replication requests.

Note HA4i STATUSCHK can be used for Automated Recovery of Errors. This check will give early indication of errors which have not been rectified by the STATUSCHK process.

Service State Information

Current Status:	OK (for 7d 4h 41m 28s)
Status Information:	All *MGT HA4i servers running OK. 0 Object Errors. 0 Profile Errors. 0 Objects waiting to be sent. Last Entry : 278264 Last Read : 278264 0 is the difference between Last Entry and Last Read.
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:01:44
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.034 seconds
Next Scheduled Check:	10-27-2021 14:11:44
Last State Change:	10-20-2021 09:21:43
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:03:08 (0d 0h 0m 3s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

HA4i Object Status

Parameters:

Wait Critical	Range to check number of objects waiting to be replicated, returns critical code.
Wait Warning	Range to check number of objects waiting to be replicated, returns warning code.
Delta Critical	Range to check delta between last entry and last read, returns critical code.
Delta Warning	Range to check delta between last entry and last read, returns warning code.
Severity	Severity of code to be returned if object/profile errors are present.

The information is returned in the following format.

If all servers are running OK the following is returned:

All *MGT HA4i servers running OK.

If there are any problems, they will be reported in the following format

Journal Scraper : Journal scraper status
Object replication : Object replication status
Retry Manager : Retry Manager status

Number Object Errors : Number of errors reported by Object replication
Number Profile Errors : Number of Profile replication errors
Number Waiting : Number of object replication request to process.
Last Entry : Last journal sequence in QAUDJRN
Last Read : Last Journal sequence read by the journal scraper.
Delta: Delta value between last entry and last read.

NOTE:

*This request must be run on the *MGT system, running this request on the *NET system will result in an error being returned.*

check_HA4i_SPLF

Returns the Spool file replication status from the *MGT system.

Purpose:

Allows early notification of backlogs and errors as the Spool File replication process works through the replication requests.

Note HA4i STATUSCHK can be used for Automated Recovery of Errors. This check will give early indication of errors which have not been rectified by the STATUSCHK process.

Service State Information

Current Status:	OK (for 0d 13h 32m 37s)
Status Information:	All Spool file servers running OK. 0 Spool file errors. 0 Spool files waiting to be sent. Last Entry : 278264 Last Read : 278229 35 is the difference between Last Entry and Last Read.
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:02:56
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.030 seconds
Next Scheduled Check:	10-27-2021 14:12:56
Last State Change:	10-27-2021 00:32:56
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:05:28 (0d 0h 0m 5s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

HA4i Spoolfile replication status

Parameters:

Wait Critical	Range for number of spool files waiting to be replicated, returns critical code.
Wait Warning	Range for number of spool files waiting to be replicated, returns warning code.
Delta Critical	Range for delta between last entry and last read, returns critical code.
Delta Warning	Range for delta between last entry and last read, returns warning code.
Severity	Severity for code returned if errors are present.

The information is returned in the following format.

If all servers are running OK the following is returned:

All Spool file servers running OK.

If there are any problems, they will be reported in the following format

Journal Scraper :	Journal scraper status
Spool replication :	Spoolfile replication status
Number Spoolfile Errors :	Number of errors reported by Object replication
Number Spoolfile Waiting :	Number of object replication request to process.
Last Entry :	Last journal sequence in QAUDJRN
Last Read :	Last Journal sequence read by the journal scraper.
Delta:	Delta value between last entry and last read.

NOTE:

This request must be run on the *MGT system, running this request on the *NET system will result in an error being returned.

check_HA4i_SYNC

Returns the Sync Manager status from the *MGT system. This is the process that resynchronizes journaled objects to the remote system using the journal to manage the save and restore and subsequent apply of entries recorded after the save completed on the source system.

Purpose:

Provide early notification of backlogs in the number of objects that are being processed by the Sync Manager. In normal circumstances there should never be an resync requests in the queue as normal HA4i replication processes should handle any object replication requirements, however there are times when this queue can have a significant number of requests queued which may take a long time to recover due to bandwidth and locking issues.

Service State Information

Current Status:	OK (for 6d 23h 8m 59s)
Status Information:	Sync Manager running OK. Sync queue depth = 0.
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:02:47
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.027 seconds
Next Scheduled Check:	10-27-2021 14:12:47
Last State Change:	10-20-2021 14:57:47
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:06:38 (0d 0h 0m 8s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

HA4i Sync Manager Status

Parameters:

- Critical Range for sync Queue depth, returns critical code.
- Warning Range for sync Queue depth, returns warning code.

The information is returned in the following format.

- Sync Manager : Sync Manager status
- Queue Depth : Number of sync requests waiting to be processed.

NOTE:

This request must be run on the *MGT system, running this request on the *NET system will result in an error being returned.

check_HA4i_RJOBS

Returns the Number of responder jobs running on the system. This request does not require the *MGT or *NET system type to be passed in, it will return the number of responder jobs running by using the system type to extract the job information.

Purpose:

Returns the number of responder jobs that are active on the system, if responder jobs end abnormally it will affect any replication requests between the systems and so it is important that they are always active. Warning notifications can be sent when the number of jobs is less than the required qty or Critical notifications if none are running etc.

Note HA4i STATUSCHK can be used for Automated Restart of the responders. This check will give early indication of errors which have not been rectified by the STATUSCHK process.

Service State Information	
Current Status:	OK (for 7d 1h 49m 34s)
Status Information:	HA4i Responder Jobs running: 3
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:03:18
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.025 seconds
Next Scheduled Check:	10-27-2021 14:13:18
Last State Change:	10-20-2021 12:18:18
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:07:48 (0d 0h 0m 4s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

HA4i Responder job status

Parameters:

- Critical Range for number of HA4i responder jobs running, returns critical code.
- Warning Range for number of HA4i responder jobs running, returns warning code.

The information is returned in the following format.

Number of Jobs : Number of responder jobs running.

check_HA4i_SPLFW

Returns the number of spool files that have been marked for replication but are still waiting to be sent to the remote system.

Purpose:

Allows early notification of problems with the replication process that could affect recovery due to large numbers of spool files waiting to be replicated to the target system.

Note: This does not report any errors that have been logged by the process.

Service State Information

Current Status:	OK (for 6d 23h 21m 25s)
Status Information:	Spool Files waiting to be replicated: 0
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:04:14
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.026 seconds
Next Scheduled Check:	10-27-2021 14:14:14
Last State Change:	10-20-2021 14:49:12
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:10:28 (0d 0h 0m 9s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

HA4i Spoolfiles waiting replication

Parameters:

Critical	Range for number of spool files awaiting replication, returns critical code.
Warning	Range for number of spool files awaiting replication, returns warning code.

The information is returned in the following format.

Number of Spool files : Number of spool files waiting to be replicated.

NOTE:

*This request must be run on the *MGT system, running this request on the *NET system will result in an error being returned.*

check_HA4i_IJRN

Returns the number of journals that have been configured for replication between the *MGT and *NET system which are *INACTIVE (not sending data to the remote system). The details are listed for each of the inactive journals.

Purpose:

Not all remote journals are used for replication by HA4i, this request will only report *INACTIVE remote journals that are currently configured to HA4i. It also reports additional information about each *INACTIVE journal.

Note HA4i STATUSCHK can be used for Automated Restart of the remote journal links. This check will give early indication of errors which have not been rectified by the STATUSCHK process.

Service State Information	
Current Status:	OK (for 7d 4h 50m 13s)
Status Information:	All Configured journals are *ACTIVE. (5/5)
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:08:11
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.029 seconds
Next Scheduled Check:	10-27-2021 14:18:11
Last State Change:	10-20-2021 09:21:25
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:11:28 (0d 0h 0m 10s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

HA4i Configure Remote Journal Status

Parameters:

Critical	Range for the number of journals which are configured and have the status of *INACTIVE, returns critical code.
Warning	Range for the number of journals which are configured and have the status of *INACTIVE, returns warning code.

The information is returned in the following format.

If all configured journals are *ACTIVE the status returns the following data, the number configured and number active are reported inside the brackets.

All Configured journals are *ACTIVE. (5/5)

If there are configured journals with a status that is not *ACTIVE, then this message will be printed:

For each journal that is inactive the following information is also returned in JSON format.

Journal : Journal name and library

Remote Journal : Remote journal name and library
 RDBDE : Relation Database Directory entry used by the RJ.
 Status : Remote journal status
 Backlog : Current backlog to be sent when it becomes active.

NOTE:

Backlog will always report as -1 if the remote journal is inactive.
 This request should be run on the *MGT system, running this request on the *NET system will result in information being returned about the remote journals configured from the *NET system

check_HA4i_STATUS

Returns the server HA4i Server status for each specific server running in the HA4i subsystem.

Purpose:

Let's you know if a specific server is not running on the system and allows notification to allow manual intervention if required. It can also be used to identify trends where the server jobs are inactive but restarted by STATUSCHK.

Note: HA4i STATUSCHK can be used for Automated Restart of the servers. This check will give early indication of errors which have not been rectified by the STATUSCHK process.

Service State Information

Current Status:	OK (for 5d 23h 16m 9s)
Status Information:	All HA4i Servers are running OK. CMDSVR Running OK. EMMGR Running OK. SYNCMGR Running OK. PRFSYNC Running OK.
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:11:24
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.034 seconds
Next Scheduled Check:	10-27-2021 14:21:24
Last State Change:	10-21-2021 14:56:24
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:12:28 (0d 0h 0m 5s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

HA4i Server Status

Parameters:

No parameters are passed to this check command.

The information is returned in JSON string format with the following keys.

- *MGT:
 - CMDSVR: Command server status (launches responder jobs)
 - EMMGR: Email Manager (Returns WARNING when not running)
 - SYNCMGR: Sync Manager (source only)
 - PRFSYNC: Required for profile sync requests

*NET:
 CFGREP : Target only (replicates any configuration changes back to the source)
 APYMGR: Launches and manager the apply processes (target only)

check_HA4i_ROLESWAP

Returns the Role-Swap Status from HA4i.

Purpose:

This check returns the end-state of the last HA4i role-swap that was taken along with the date of the last role-swap.

Service State Information

Current Status:	OK (for 5d 18h 51m 49s)
Status Information:	Role-Swap was successfull. Latest Role-Swap: 2022-01-31 13:59:41
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	03-24-2022 09:25:35
Check Type:	ACTIVE
Check Latency / Duration:	0.737 / 0.035 seconds
Next Scheduled Check:	03-25-2022 09:25:35
Last State Change:	03-18-2022 14:34:02
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	03-24-2022 09:25:49 (0d 0h 0m 2s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

HA4i Role-Swap

Parameters:

Name Name of Data area for HA4i role-swap.
 Library Library where the HA4i role-swap data area is located.
 Severity Return code if the last role-swap was not successful. [0,1,2]

The information is returned in the following format.

Role-Swap Status : Successful / unsuccessful.
 Latest Role-Swap : Date of last role swap.

check_HA4i_NEWDEV

Check command to check if new devices have been added which have not been added to replication.

Note: Ensure new device logging is set in the HA4i configs.

To ignore non-replicated devices a flag needs to be set in the SQL table find information on this on page 98 of the HA4i Manual. This SQL can be called to update that flag:

```
UPDATE HA4i72.DEVLOG SET IGNAAG='Y' WHERE DEVNAM = '[Library name]'
```

Purpose:

This check returns a warning code, if new devices have been added to the system and not replicated.

Service State Information	
Current Status:	OK (for 5d 19h 40m 55s)
Status Information:	There are no new Devices that are not replicated.
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	03-24-2022 09:25:35
Check Type:	ACTIVE
Check Latency / Duration:	0.207 / 0.032 seconds
Next Scheduled Check:	03-24-2022 10:25:35
Last State Change:	03-18-2022 14:34:03
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	03-24-2022 10:14:50 (0d 0h 0m 8s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

HA4i New Devices

Parameters:

There are no parameters passed into this check command.

check_HA4i_NEWLIB

Check command to check if new libraries have been added which have not been configured into replication.

Note: Ensure new library logging is set in the HA4i configs.

To ignore non-replicated libraries a flag needs to be set in the SQL table find information on this on page 96 of the HA4i Manual. This SQL can be called to update that flag:

```
UPDATE HA4i72.LIBLOG SET IGNAAG='Y' WHERE LIBNAM = '[Library name]'
```

Purpose:

This check returns a warning code, if new libraries have been added to the system and not replicated.

Service State Information

Current Status:	OK (for 5d 19h 47m 36s)
Status Information:	There are no new Libraries that are not replicated.
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	03-24-2022 09:25:35
Check Type:	ACTIVE
Check Latency / Duration:	0.122 / 0.033 seconds
Next Scheduled Check:	03-24-2022 10:25:35
Last State Change:	03-18-2022 14:34:03
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	03-24-2022 10:21:30 (0d 0h 0m 9s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

HA4i New Libraries

Parameters:

There are no parameters passed into this check command.

check_HA4i_AUDSTS

This check will return the information related to a specified HA4i Audit. An UNKNOWN status is returned if the audit information is older than 24hours because we do not believe this data is still relevant. It is also possible to set parameters to check if the audit is currently running or has ended. These can be used to ensure an audit is running when it should, and has not overflowed its audit window.

Current Status:	OK (for 0d 0h 0m 14s)
Status Information:	Job Info: AUDCHK CHRISH 011190 Job Status: *ACTIVE Time Start: 2023/11/17 16:07:12 Time End: // : Count: 10 Errors: 0 Resync: *NO Command: AUDLIBF FILE(*ALL) TYPE(*ALL) LIB(B_DTA_LIB) SKPREC(0) CLRAUD(*YES) SPLLL(*FULL) OPFM(*NONE) IGNNONJRN(*NO) IGNECL(*NO) RESYNC(*NO) LOG(*YES) DAYS(0) MAXAUD(-1) GENMAP(*YES)
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	11-17-2023 15:06:44
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.050 seconds
Next Scheduled Check:	11-17-2023 16:06:44
Last State Change:	11-17-2023 15:06:44
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	11-17-2023 15:06:54 (0d 0h 0m 4s ago)

HA4i Audit Status

Parameters:

Type	Range for number of EM4i messages waiting for responses, returns critical code.
Library	Range for number of EM4i messages waiting for responses, returns warning code.
Error Critical	Range for number of errors found by audit, returns critical code.
Error Warning	Range for number of errors found by audit, returns warning code.
Running Severity	Alert severity returned if the audit is still currently running.
Not Running Severity	alert severity returned if the audit is not currently running.

Returns the number of messages waiting and then for each message the following information.

- Job Info: Job name, User, Job number.
- Job Status: Status of Job.
- Time Start: Time the job started.
- Time End: Time the job ended.
- Count: Number of objects audited.
- Errors: Number of errors found by Audit.
- Resync: Option of audit if resync is on or off.
- Command: Command run for audit.

check_HA4i_RSREADY

Check command to check show if the replication pair are ready for Role swap.

Purpose:

This check returns different warning levels for different errors or problems found. The purpose of this check is to show in a single location if your target system is up to date with no issues or errors, ready for a role swap.

Service State Information

Current Status:	OK (for 3d 7h 2m 46s)
Status Information:	Systems are READY for RoleSwap. No apply errors found. No Remote Journal problems found. No Config Replication errors found. No Object Replication errors found. No Spool File Replication errors found. No Profile Replication errors found. No Sync Manager problems found. No Sync Manager problems found. No Email Manager problems found on NET system. No Email Manager problems found on MGT system. No Command Server problems found on NET system. No Command Server problems found on MGT system. No Message Wait problems found on NET system. No Message Wait problems found on MGT system. No Environment problems found.
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	08-07-2024 13:06:58
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.158 seconds
Next Scheduled Check:	08-07-2024 14:06:58
Last State Change:	08-04-2024 06:05:20
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	08-07-2024 13:08:02 (0d 0h 0m 4s ago)

HA4i New Libraries

Parameters:

There are no parameters passed into this check command.

EM4i Check Commands

check_EM4i_RESPWAIT

Returns the number of *INQ messages EM4i is waiting for responses for as well as the time the notifications were received by EM4i.

Service State Information	
Current Status:	OK (for 2d 2h 1m 52s)
Status Information:	0 EM4i Messages waiting for a reply.
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 15:21:32
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.027 seconds
Next Scheduled Check:	10-27-2021 15:31:32
Last State Change:	10-25-2021 13:21:32
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:23:17 (0d 0h 0m 7s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

EM4i messages waiting response

Parameters:

Qty Critical

Range for number of EM4i messages waiting for responses, returns critical code.

Qty Warning

Range for number of EM4i messages waiting for responses, returns warning code.

Wait Critical

Range for time EM4i message has spent waiting, returns critical code.

Wait Warning

Range for time EM4i message has spent waiting, returns warning code.

Returns the number of messages waiting and then for each message the following information.

Message ID

Message ID

Date

Date notification was sent

Time

Time the message notification was sent.

check_EM4i_MSGMON, check_EM4i_MSGPOL, check_EM4i_SMSMGR

These services use the check command `check_Shield_JOBSRCH` to ensure EM4i jobs are running. Check the JOBSRCH item below for more details.

check_EM4i_MSGCFG

Returns message IDs that EM4i has picked up as not being configured. This helps with replacing “*ALL” in message IDs.

Service State Information

Current Status:	OK (for 0d 0h 0m 10s+)
Status Information:	5 messages waiting to be configured. Message Queue: QSYSOPR Library: QSYS Message ID: CPA070199 Message Queue: QSYSOPR Library: QSYS Message ID: CPA702599 Message Queue: QSYSOPR Library: QSYS Message ID: MSG00010 Message Queue: QSYSOPR Library: QSYS Message ID: TCP913840 Message Queue: QSYSOPR Library: QSYS Message ID: TST00050
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	09-23-2025 10:33:01
Check Type:	ACTIVE
Check Latency / Duration:	1.293 / 0.030 seconds
Next Scheduled Check:	09-24-2025 10:33:01
Last State Change:	N/A
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	09-23-2025 10:33:01 (0d 0h 0m 1s ago)

EM4i message IDs which have not been configured

Parameters:

- Critical Count Critical range for number of EM4i message IDs which have not been configured but have been picked up on message queue.
- Warning Count Warning range for number of EM4i message IDs which have not been configured but have been picked up on message queue.

Returns the number of message IDs waiting to be configured. Returns the following for each entry:

- Message Queue Message Queue that message ID was found on.
- Library Library of message queue.
- Message ID Message ID found.

Shield General Check Commands

check_Shield_KEYEXP

Returns the number of days before a license key for the LPP entered will expire. It can be used for any IBM i LPP.

Purpose:

Provide early warning of any license key that is due to expire for any IBM i License Program Product. Shield products all ship as LPP's and some are shipped with limited key periods, this allows you to preempt any product stoppages caused by expired keys.

Note: Most Shield products ship with self-monitoring programs that also capture key expiration.

Service State Information	
Current Status:	OK (for 6d 9h 12m 15s)
Status Information:	Key has no expiry (1HA4ISN).
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:06:17
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.024 seconds
Next Scheduled Check:	10-27-2021 14:16:17
Last State Change:	10-21-2021 05:01:16
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:13:28 (0d 0h 0m 3s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Key Expiry

Parameters:

Product Name	Name of LPP to be checked (7 char).
Product Version	Version of LPP to be checked (6 char).
Product Option	Option of LPP to be checked (4 char).
Days Critical	Range to check number of days until product expiry against, returns critical.
Days Warning	Range to check number of days until product expiry against, returns warning.

Returns the number of days before the key expires.

check_Shield_SBSSRCH

Returns the number of jobs that are running in a specified subsystem, with the status of *MSGW.

Purpose:

Returns the number of jobs running in a subsystem that are sitting *MSGW status.

Service State Information

Current Status:	OK (for 0d 19h 57m 32s)
Status Information:	Jobs in (EM4ISBS10 EM4110) with status of *MSGW: 0
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:09:22
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.013 seconds
Next Scheduled Check:	10-27-2021 14:19:22
Last State Change:	10-26-2021 18:19:22
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:16:48 (0d 0h 0m 6s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

1 Jobs *MSGW status by subsystem

Parameters:

Library	Subsystem library (10 char).
Subsystem	Subsystem to be checked (10 char).
Critical	Range for number of jobs with status of *MSGW, returns critical code.
Warning	Range for number of jobs with status of *MSGW, returns warning code.

Returns the number of jobs that are running in the subsystem with a status of message wait.

check_Shield_JOBSRCH

Returns the number of jobs that are running which match the search criteria.

Purpose:

Provides a count of the jobs that match the entered criteria which can be checked against a number expected to be running. If the number of jobs is less or more than expected notifications can be sent out to allow any problems to be rectified.

Service State Information

Current Status:	OK (for 6d 15h 17m 23s)
Status Information:	Active Jobs matching [BCH*/JT4IUSER*/ALL]: 0
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:16:00
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.026 seconds
Next Scheduled Check:	10-27-2021 14:26:00
Last State Change:	10-20-2021 23:00:58
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:18:18 (0d 0h 0m 3s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Number of Matching jobs in Subsystem.

Parameters:

- Job Name Search for jobs matching job name. (Can be generic)
- Job User Search for jobs matching username. (Can be generic)
- Job Number Search for jobs matching job number. (Can be *ALL)
- Critical Range for number of jobs found matching search criteria, returns critical code.
- Warning Range for number of jobs found matching search criteria, returns warning code.

Returns the number of jobs running which match the job information entered.

Returns the number of messages that are waiting for a reply in a specific message queue.

Purpose:

Provides early notification of messages in specific message queues that require a response from a user, this could be due to an error in a job which is stopping the job from running and therefore needs immediate attention.

Service State Information

Current Status:	OK (for 2d 1h 13m 58s)
Status Information:	0 Messages waiting for a reply.
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:26:46
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.026 seconds
Next Scheduled Check:	10-27-2021 14:36:46
Last State Change:	10-25-2021 13:16:45
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:30:38 (0d 0h 0m 5s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Reply Wait status by *MSGQ

Parameters:

- Message Queue Message Queue Name (10 char).
- Library Message Queue Library (10 char).
- Qty Critical Range for number of messages awaiting a reply, returns critical code.
- Qty Warning Range for number of messages awaiting a reply, returns warning code.
- Wait Critical Range for length of time a message has been awaiting a reply, returns critical code.
- Wait Warning Range for length of time a message has been awaiting a reply, returns warning code.

Returns the number of *RPYW messages in the queue in the following format.

If there are no messages waiting for a reply, this message will be outputted:

0 Messages waiting for a reply.

If there are any messages in the queue that require a response the following information will be returned.

- Number of messages Number of messages in queue with a type of *INQ
- Job Job Name that sent the message
- User Username that sent the message
- Job Number The job number of the sending job
- Message ID Message ID for the message
- Message Message text
- Message Waiting for How long the message has been waiting for a response

check_Shield_DSBPRF

Returns the number of profiles that are in a disabled state.

There are usually a number of profiles that are *DISABLED by choice and they remain static, however if more profiles become disabled it could be an indication of problems building, or simply show when profiles need to be reset.

Service State Information

Current Status:	OK (for 7d 5h 9m 10s)
Status Information:	Disabled Profiles: 6 EM4IUSER :FRED :JT4IUSER :QCLUMGT :QTCM :RE4IUSER :
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:24:23
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.039 seconds
Next Scheduled Check:	10-27-2021 14:34:23
Last State Change:	10-20-2021 09:24:23
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:33:28 (0d 0h 0m 5s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Disabled Profiles count

Parameters:

- Critical Range for number of disabled profiles on a system, returns critical code.
- Warning Range for number of disabled profiles on a system, returns warning code.

Returns number of disabled profiles.

check_Shield_SBSJOB

Returns the number of active jobs for a given subsystem or all subsystems.

Service State Information

Current Status:	OK (for 0d 20h 16m 55s)
Status Information:	Jobs in subsystem (JT4ISBS10) : 0
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:29:09
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.009 seconds
Next Scheduled Check:	10-27-2021 14:39:09
Last State Change:	10-26-2021 18:19:08
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:35:58 (0d 0h 0m 5s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Active Job Count

Parameters:

- Subsystem Subsystem name *ALL
- Library Subsystem library or *ALL
- Critical Range for number of jobs running in specified subsystem/library, returns critical code.
- Warning Range for number of jobs running in specified subsystem/library, returns warning code.

Returns the number of active jobs found

check_Shield_JOBQ

Returns the number of jobs sitting on the job queue entered.

Service State Information

Current Status:	OK (for 6d 7h 26m 59s)
Status Information:	Jobs in JobQ (EM4IJOBQ EM4I10) : 0 JobQ status: RELEASED
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:35:40
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.023 seconds
Next Scheduled Check:	10-27-2021 14:45:40
Last State Change:	10-21-2021 07:10:40
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:37:38 (0d 0h 0m 1s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Job Queue Count

Parameters:

Job Queue	Job Queue name.
Library	Job Queue library.
Critical	Range for number of jobs sitting on specified job queue, returns critical code.
Warning	Range for number of jobs sitting on specified job queue, returns warning code.

Returns the number of jobs waiting to run on the job queue.

check_Shield_RCVR

Returns the quantity and total size of the receivers in Library passed in.

Service State Information

Current Status:	OK (for 6d 19h 43m 0s)
Status Information:	Number of receivers: 2 Size of receivers: 3890.7MB
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 15:19:17
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.025 seconds
Next Scheduled Check:	10-27-2021 15:29:17
Last State Change:	10-20-2021 19:36:34
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:19:27 (0d 0h 0m 7s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Receiver size qty

Parameters:

Library	Receiver Library (10 char).
Qty Critical	Range for number of receivers in library, returns critical code.
Qty Warning	Range for number of receivers in library, returns warning code.
Size Critical	Range for Size of each receiver in library, returns critical code.
Size Warning	Range for Size of each receiver in library, returns warning code.

Returns Library, qty of receivers and the total size of receivers.

check_Shield_CACHEBAT

Returns the state for any cache battery found.

Service State Information

Current Status:	OK (for 7d 5h 58m 17s)
Status Information:	No Cache Batteries installed.
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 15:22:09
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.027 seconds
Next Scheduled Check:	10-27-2021 15:32:09
Last State Change:	10-20-2021 09:24:05
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:22:17 (0d 0h 0m 5s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Check Cache Battery status

Parameters:

No parameters are passed for this check command.

Returns the cache battery state and quantity in the following format

Error State	If the battery is in error
Battery Type	Type of battery installed
Maintainable	If the battery is maintainable
Cache Written	Data Cache written to disk
Days Warn	Days to warning issue
Days Error	Days to error
Power on	Power on Time
Adj Pwr	Adjusted Power on Time

check_Shield_DSBPRF

Returns the number of profiles that are in a disabled state.

There are usually a number of profiles that are *DISABLED by choice and they remain static, however if more profiles become disabled it could be an indication of problems building, or simply show when profiles need to be reset.

Service State Information

Current Status:	OK (for 7d 5h 9m 10s)
Status Information:	Disabled Profiles: 6 EM4IUSER :FRED :JT4IUSER :QCLUMGT :QTCM :RE4IUSER :
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:24:23
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.039 seconds
Next Scheduled Check:	10-27-2021 14:34:23
Last State Change:	10-20-2021 09:24:23
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:33:28 (0d 0h 0m 5s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Disabled Profiles count

Parameters:

Critical Range for number of disabled profiles on a system, returns critical code.
Warning Range for number of disabled profiles on a system, returns warning code.

Returns number of disabled profiles.

check_Shield_APTUPD

Returns the number Linux updates/upgrades available on the Nagios system. This check can now handle APT or YUM depending on the OS.

Service State Information	
Current Status:	OK (for 5d 19h 52m 50s)
Status Information:	Linux OS is up to date.
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	03-23-2022 09:25:36
Check Type:	ACTIVE
Check Latency / Duration:	4.869 / 0.511 seconds
Next Scheduled Check:	03-26-2022 09:25:36
Last State Change:	03-18-2022 14:34:04
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	03-24-2022 10:26:50 (0d 0h 0m 4s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Linux Updates

Parameters:

Severity Severity of the code to be returned if updates/upgrades are available.
OS OS of the local machine. [debian/centos]

Returns the number of updates/upgrades available or a message stating the Linux OS is up to date.

check_Shield_PTF

Lists the PTF levels installed on system and latest PTF levels available if *ALL is passed in as the first parameter. Otherwise, this check will return information on a specific PTF passed in. Returns severity code passed in as parameter if not all PTFs listed are up to date.

Service State Information

Current Status: OK (for 1d 1h 37m 40s)

Status Information: Installed PTF levels:

OS Level: V7R2M0
PTF GRP ID: SF99223
Installed level: 1
WARNING-PTF update available:1/6

OS Level: V7R2M0
PTF GRP ID: SF99251
Installed level: 2
WARNING-PTF update available:2/15

OS Level: V7R2M0
PTF GRP ID: SF99480
Installed level: 6
WARNING-PTF update available:6/9

OS Level: V7R2M0
PTF GRP ID: SF99481
Installed level: 7
WARNING-PTF update available:7/21

OS Level: V7R2M0
PTF GRP ID: SF99481
Installed level: 8
WARNING-PTF update available:8/21

OS Level: V7R2M0
PTF GRP ID: SF99658
Installed level: 3
WARNING-PTF update available:3/6

OS Level: V7R2M0
PTF GRP ID: SF99658
Installed level: 6
Latest release:6

OS Level: V7R2M0
PTF GRP ID: SF99702
Installed level: 24
WARNING-PTF update available:24/27

OS Level: V7R2M0
PTF GRP ID: SF99702
Installed level: 26
WARNING-PTF update available:26/27

OS Level: V7R2M0
PTF GRP ID: SF99713
Installed level: 16
WARNING-PTF update available:16/50

OS Level: V7R2M0
PTF GRP ID: SF99713
Installed level: 39
WARNING-PTF update available:39/50

OS Level: V7R2M0
PTF GRP ID: SF99759
Installed level: 6
WARNING-PTF update available:6/40

OS Level: V7R2M0
PTF GRP ID: SF99759
Installed level: 7
WARNING-PTF update available:7/40

OS Level: V7R2M0
PTF GRP ID: SF99766
Installed level: 3
Latest release:3

OS Level: V7R2M0
PTF GRP ID: SF99767
Installed level: 3
WARNING-PTF update available:3/11

OS Level: V7R2M0
PTF GRP ID: SF99767
Installed level: 8
WARNING-PTF update available:8/11

OS Level: V7R2M0
PTF GRP ID: SF99769
Installed level: 1
Latest release:1

OS Level: V7R2M0
PTF GRP ID: SF99775
Installed level: 34
WARNING-PTF update available:34/35

OS Level: V7R2M0
PTF GRP ID: SF99775
Installed level: 35
Latest release:35

OS Level: V7R2M0
PTF GRP ID: SF99776
Installed level: 3
WARNING-PTF update available:3/19

OS Level: V7R2M0
PTF GRP ID: SF99776
Installed level: 5
WARNING-PTF update available:5/19

Performance Data:

Current Attempt: 1/2 (HARD state)

Last Check Time: 03-24-2022 09:25:41

Check Type: ACTIVE

Check Latency / Duration: 0.737 / 2.459 seconds

Next Scheduled Check: 03-25-2022 09:25:41

Last State Change: 03-23-2022 09:25:34

Last Notification: N/A (notification 0)

Is This Service Flapping? NO (11.71% state change)

In Scheduled Downtime? NO

Last Update: 03-24-2022 11:03:10 (0d 0h 0m 4s ago)

IBM i PTF Updates

Parameters:

PTF Group
Severity

Specific PTF group to be checked or user can pass in *ALL.
Severity of the code to be returned if PTFs are not all at the latest level.

Lists out the OS level, PTF group ID, installed level and latest available level. If the installed level is less than the latest level, then a warning is printed instead of the latest level with installed/latest levels listed.

check_Shield_TOPJOB_CPU

****This check has been deprecated. Use check_Shield_JOB_CPU instead.**

Returns the information about jobs that match the entered parameters specific to the CPU used and the runtime.

Service State Information

Current Status:	CRITICAL (for 0d 0h 3m 51s)
Status Information:	CRITICAL - (Job:645950) Runtime: 190290 CRITICAL - (Job:645951) Runtime: 190290 CRITICAL - (Job:645952) Processor Used: 331 CRITICAL - (Job:645952) Runtime: 190290
	Job: SMSMGR Job User: EM4IUSER Job Number: 645950 Processor Used: 29 CRITICAL - Runtime: 190290
	Job: MSGMON Job User: EM4IUSER Job Number: 645951 Processor Used: 7 CRITICAL - Runtime: 190290
	Job: MSGPOL Job User: EM4IUSER Job Number: 645952 CRITICAL - Processor Used: 331 CRITICAL - Runtime: 190290
Performance Data:	
Current Attempt:	2/5 (SOFT state)
Last Check Time:	10-27-2021 16:00:24
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.026 seconds
Next Scheduled Check:	10-27-2021 16:05:24
Last State Change:	10-27-2021 15:58:49
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 16:02:38 (0d 0h 0m 2s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Active Job Status (CPU /runtime)

Parameters:

- Job Name Filter job list by Name (Can be a full name or generic).
- Username Filter job list by Username (can be generic).
- Job Number Filter job list by job number (can be generic).
- CPU Critical Range for processor used by job, returns critical code.
- CPU Warning Range for processor used by job, returns warning code.
- Runtime Critical Range for job runtime, returns critical code.
- Runtime Warning Range for job runtime, returns warning code.

Returns the following information for each job that matches the job criteria entered.

JobName Job Name given to the active job.

JobUser	User Profile the job is running under.
JobNumber	Job Number assigned by the system
prused	Total Processor used by the job (milliseconds)
runtime	How long the job has been running (seconds)

[check_Shield_TOPJOB_STG](#)

****This check has been deprecated. Use check_Shield_JOBSTG instead.**

Returns the information about jobs that match the entered parameters specific to the QTEMP size and the temporary storage used.

Service State Information

Current Status:	CRITICAL (for 0d 0h 5m 45s)
Status Information:	CRITICAL - (Job:645950) QTEMP: 4263936 CRITICAL - (Job:645951) QTEMP: 65536 CRITICAL - (Job:645952) QTEMP: 4263936
	Job: SMSMGR Job User: EM4IUSER Job Number: 645950 CRITICAL - QTEMP: 4263936 STG: 5
	Job: MSGMON Job User: EM4IUSER Job Number: 645951 CRITICAL - QTEMP: 65536 STG: 4
	Job: MSGPOL Job User: EM4IUSER Job Number: 645952 CRITICAL - QTEMP: 4263936 STG: 4
Performance Data:	
Current Attempt:	3/5 (SOFT state)
Last Check Time:	10-27-2021 16:04:16
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.026 seconds
Next Scheduled Check:	10-27-2021 16:09:16
Last State Change:	10-27-2021 15:58:49
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 16:04:31 (0d 0h 0m 3s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Active Job Status (QTEM / temp storage)

Parameters:

Job Name	Filter job list by Name (Can be a full name or generic).
Username	Filter job list by Username (can be generic).
Job Number	Filter job list by job number (can be generic).
QTEMP Critical	Range for job QTEMP size, returns critical code.
QTEMP Warning	Range for job QTEMP size, returns warning code.
Storage Critical	Range for job Storage, returns critical code.

Storage Warning Range for job Storage, returns warning code.

Returns the following information for each job that matches the job criteria entered.

JobName	Job Name given to the active job.
JobUser	User Profile the job is running under.
JobNumber	Job Number assigned by the system
qtemp	Size of the QTEMP library for the job (bytes)
stg	Temporary storage assigned to the job (MB)

check_Shield_UPDLVL

Returns the update information for shield products. Checks if the product is currently in maintenance and checks latest vs installed PTFs and updates.

Service State Information

Current Status:	OK (for 12d 20h 48m 41s)
Status Information:	Maintenance expiry date: 2022-10-01 Latest PTF: 1NG1100 Current PTF: 1NG1100 Lastest Update: NG4I061322 Current Update: NG4I061322
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	07-04-2022 15:04:11
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.246 seconds
Next Scheduled Check:	07-05-2022 15:04:11
Last State Change:	06-22-2022 15:04:11
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (8.95% state change)
In Scheduled Downtime?	NO
Last Update:	07-05-2022 11:52:48 (0d 0h 0m 4s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Update status for NG4i

Parameters:

Product ID	Product ID for Shield product.
Product Version	Product Version for Shield product.
Critical Days	Range for days until maintenance expires, returns critical code.
Warning Days	Range for days until maintenance expires, returns warning code.

Returns the following information:

Maintenance Expiry Date	Date that product maintenance expires.
Latest PTF	Latest PTF level released by Shield.
Current PTF	Current PTF level installed on system.
Latest Update	Latest update released by Shield.
Current Update	Current update level installed on system.

check_Shield_PRDSYNC

Compares update levels between AAG and NG4i to ensure they are in sync. These two must be in sync to ensure communication between the responder server and Nagios is flawless.

Service State Information

Current Status:	OK (for 20d 22h 32m 58s)
Status Information:	AAG current update level: AAG1061322 NG4i current level: NG4I061322
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	07-05-2022 11:33:16
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.092 seconds
Next Scheduled Check:	07-05-2022 12:33:16
Last State Change:	06-14-2022 13:28:16
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	07-05-2022 12:01:08 (0d 0h 0m 6s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Product Sync between AAG and NG4i

Parameters:

Error Severity Returned severity level if products are not synced.

Returns the following information:

AAG current update level
NG4i current level

AAG update level installed on system.
NG4i update level installed on system.

check_Shield_APTUPD

Checks Linux is up to date using APT update. This service is designed to run against the local host of Nagios, on either a Debian, RPi or any other OS that uses APT.

Service State Information

Current Status:	OK (for 41d 19h 35m 24s)
Status Information:	Linux OS is up to date.
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	07-02-2022 16:30:20
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 1.557 seconds
Next Scheduled Check:	07-05-2022 16:30:20
Last State Change:	05-24-2022 16:30:20
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	07-05-2022 12:05:38 (0d 0h 0m 6s ago)

Active Checks:	ENABLED
Passive Checks:	DISABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Linux OS is up to date

Parameters:

Severity Returned severity level if there are updates available.

Returns the following information:

CRITICAL - There are 10 package(s) to be upgraded.

OR

WARNING - There are 10 package(s) to be upgraded.

OR

There are 10 package(s) to be upgraded.

OR

Linux OS is up to date.

check_Shield_JOBSCDE

Returns information on a job schedule entry.

Service State Information

Current Status:	OK (for 41d 19h 38m 42s)
Status Information:	Job successfully submitted. Name: NASBACKUP Status: SCD Next submission: 04/07/22 23:55:00 Last submission: 01/07/22 23:55:00
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	07-04-2022 16:33:24
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.117 seconds
Next Scheduled Check:	07-05-2022 16:33:24
Last State Change:	05-24-2022 16:33:24
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	07-05-2022 12:11:58 (0d 0h 0m 8s ago)

Active Checks:	ENABLED
Passive Checks:	DISABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Details of NASBACKUP job schedule entry

Parameters:

Job schedule entry name Name of Job schedule entry to check.

Returns the following information:

Job submitted status	Lists if last scheduled job was submitted successfully or not.
Name	Name of job schedule entry.
Status	Status of job schedule entry.
Next submission	Date and time of next scheduled job entry
Last submission	Date and time of last scheduled job entry

check_Shield_SSLCERT

Returns Number of SSL Certificates expiring within the next X days. Certificate information will be printed out for each certificate found to be expiring.

Note: Use addSystem to add an encrypted file to store the login information for the Certificate store. Use the format '[HOSTNAME]-[TYPE]' hostname must match the hostname originally set when the host was added to Nagios. If you are using NagiosXI be sure to addSystem via the command line.

Type is the type of SSL Certificate store. Current types supported:

- 0 = *SYSTEM
- 1 = *OBJECTSIGNING
- 2 = *SIGNATUREVERIFICATION

Service State Information

Current Status:	OK (for 7d 0h 35m 28s)
Status Information:	No SSL Certificates expiring in the next 30 days.
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	07-05-2022 11:48:31
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 2.876 seconds
Next Scheduled Check:	07-06-2022 11:48:31
Last State Change:	06-28-2022 11:43:28
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	07-05-2022 12:18:48 (0d 0h 0m 8s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

SSL Certs expiring in the next 30 days

Parameters:

Type	Type of certificate store to be checked.
Days	Number of days in the future to be checked for expiring certificates.
Qty Critical	Range for number of certificates expiring within the date set, returns critical code.
Qty Warning	Range for number of certificates expiring within the date set, returns warning code.

Returns the following information:

No SSL Certificates expiring in the next 30 days.

OR

CRITICAL-10 SSL Certificates will expire within the next 30 day(s).

Certificate Label Certificate label of cert expiring.

Certificate Name Certificate name of cert expiring

Certificate Expiry Date cert will expire.

[check_Shield_DSKSTS](#)

Returns disk errors reported by the system and number of disks reported by system.

Service State Information

Current Status:	OK (for 21d 20h 43m 33s)
Status Information:	0 Disk errors reported. All 9 disks reported out of 9 configured.
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	07-04-2022 15:48:10
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.121 seconds
Next Scheduled Check:	07-05-2022 15:48:10
Last State Change:	06-13-2022 15:48:10
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	07-05-2022 12:31:43 (0d 0h 0m 0s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Disk status for IBM i

Parameters:

ASP Number ASP reference number.

Qty of Configured Disks Number of disks that should be reported by system. (comparison value)

Disk Error Severity Severity of alert if disk errors are found.

Returns the following information:

0 Disk errors reported.

All 4 disks reported out of 4 configured.

check_Shield_UPTIME

Returns number of minutes since last IPL.

Service State Information

Current Status:	OK (for 0d 2h 6m 37s)
Status Information:	System uptime: 26054min.
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	07-29-2022 11:34:31
Check Type:	ACTIVE
Check Latency / Duration:	0.741 / 0.000 seconds
Next Scheduled Check:	07-29-2022 11:44:31
Last State Change:	07-29-2022 09:31:37
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	07-29-2022 11:38:04 (0d 0h 0m 10s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	DISABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

System uptime

Parameters:

Critical Uptime Range for number of min. since last IPL, returns critical code.
Warning Uptime Range for number of min. since last IPL, returns warning code.

Returns the following information:

System Uptime Number of min since last IPL.

check_Shield_SYSVAL

Checks system value compared to a comparison parameter to return a status which is either OK or the Severity parameter passed in.

Service State Information

Current Status:	OK (for 0d 1h 59m 32s)
Status Information:	System value matches passed parameter. (0->0)
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	07-29-2022 11:24:35
Check Type:	ACTIVE
Check Latency / Duration:	0.180 / 0.000 seconds
Next Scheduled Check:	07-29-2022 11:44:35
Last State Change:	07-29-2022 09:44:31
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (11.05% state change)
In Scheduled Downtime?	NO
Last Update:	07-29-2022 11:43:54 (0d 0h 0m 9s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	DISABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

System Value check

Parameters:

System Value	System Value to be checked.
Comparison Value	Value to compare returned system value to. If there is a mismatch, then an error is returned.
Severity	Severity to level to return if system value does not match comparison value.

Returns the following information:

System value matches passed parameter. ([System Value]->[Comparison Value])

OR

WARNING-System value does not match passed parameter. ([System Value]->[Comparison Value])

check_Shield_SECUPD

Returns security bulletins posted since date passed into first parameter.

Service State Information

Current Status:	CRITICAL (for 0d 0h 37m 8s)
Status Information:	CRITICAL-There are outstanding security bulletins.
	Date: 2022-06-13 CVEID: CVE-2022-22720 CVSSBS: 7.3 LPP: 5770DG1 PTF: SI79640
	Date: 2022-06-13 CVEID: CVE-2022-22721 CVSSBS: 7.3 LPP: 5770DG1 PTF: SI79640
	Date: 2022-06-15 CVEID: CVE-2022-22475 CVSSBS: 5.3 LPP: 5770SS1 PTF: SI79991
	Date: 2022-06-15 CVEID: CVE-2022-22393 CVSSBS: 3.1 LPP: 5770SS1 PTF: SI79991
	Date: 2022-06-15 CVEID: CVE-2022-0396 CVSSBS: 5.3 LPP: 5770SS1 PTF: SI79976

System Value check

Parameters:

Date	Date to filter bulletins, suggested to enter the date of the last time updates were installed.
Severity	Severity to level to return if there are outstanding security bulletins.

Returns the following information for each bulletin:

Date	Date the security bulletin was posted.
CVEID	Bulletin ID number.
CVSSBS	Severity level of bulletin.
LPP	IBM LPP effected.
PTF	PTF containing Fix.

check_Shield_AUTUPD

This check reaches out to the Shield website to check for the latest AAG update level. If it is found that AAG is not at the latest level then either a notification will be sent out to the users stating there is an update available OR this check can be configured to automatically update AAG.

It is recommended this service is run against the localhost as no communication with another system is necessary.

**NOTE: to use this function special permissions need to be set within Nagios. Please contact Shield to allow us to make the appropriate changes.*

Service State Information	Service State Information
Current Status: OK (for 0d 1h 27m 54s) Status Information: Current AAG level:AAG1090222 Latest AAG level:AAG1090222 Performance Data: Current Attempt: 1/1 (HARD state) Last Check Time: 09-06-2022 11:18:19 Check Type: ACTIVE Check Latency / Duration: 0.000 / 0.384 seconds Next Scheduled Check: 09-07-2022 11:18:19 Last State Change: 09-06-2022 11:18:19 Last Notification: N/A (notification 0) Is This Service Flapping? NO (18.36% state change) In Scheduled Downtime? NO Last Update: 09-06-2022 12:46:03 (0d 0h 0m 10s ago)	Current Status: CRITICAL (for 0d 0h 0m 10s) Status Information: There is an update available for AAG! Update not downloaded as AUTO-UPDATE is turned off. Current AAG level:AAG1090221 Latest AAG level:AAG1090222 Performance Data: Current Attempt: 1/1 (HARD state) Last Check Time: 09-06-2022 12:47:43 Check Type: ACTIVE Check Latency / Duration: 0.000 / 0.597 seconds Next Scheduled Check: 09-07-2022 12:47:43 Last State Change: 09-06-2022 12:47:43 Last Notification: N/A (notification 0) Is This Service Flapping? YES (24.21% state change) In Scheduled Downtime? NO Last Update: 09-06-2022 12:47:53 (0d 0h 0m 0s ago)
Service State Information	
Current Status: WARNING (for 0d 0h 0m 5s) Status Information: AAG successfully updated to the latest level. AAG1090221 -> AAG1090222 Performance Data: Current Attempt: 1/1 (HARD state) Last Check Time: 09-06-2022 12:48:25 Check Type: ACTIVE Check Latency / Duration: 0.000 / 1.784 seconds Next Scheduled Check: 09-07-2022 12:48:26 Last State Change: 09-06-2022 12:48:25 Last Notification: N/A (notification 0) Is This Service Flapping? YES (29.93% state change) In Scheduled Downtime? NO Last Update: 09-06-2022 12:48:29 (0d 0h 0m 1s ago)	

AAG Auto update

After an auto update has been ran, this check will be set to a WARNING value until the next check to alert the user of the update.

Parameters:

Auto Update [0/1] This flag sets whether AAG should automatically update or simply notify the user there are update available.

NOTE: the following parameters are only important if auto update is set to 1

Build[NAGIOS/NAGIOSXI/GEARMAN] The Nagios build type AAG is running on.

Update file(updateAAG.sh) This is only used in special cases. If you do not require a specialized update script, please use "updateAAG.sh".

Severity Notification severity if AAG has found updates are available and Auto update is set to 0.

check_Shield_RCVRBKLG

Returns journal receiver backlog and time to clear.

Service State Information

Current Status:	OK (for 0d 0h 0m 2s)
Status Information:	Current Backlog for BATCHJRN BATCHRMT : 0 Minutes to clear backlog: 0
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	11-23-2022 13:00:24
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.047 seconds
Next Scheduled Check:	11-23-2022 13:10:24
Last State Change:	11-23-2022 13:00:24
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (11.84% state change)
In Scheduled Downtime?	NO
Last Update:	11-23-2022 13:00:26 (0d 0h 0m 0s ago)

Active Checks:	ENABLED
Passive Checks:	DISABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Receiver Backlog

Parameters:

Remote DB Dir.	Remote database entry directory.
Remote Journal	Remote journal name.
Remote Library	Remote journal library.
Local Journal	Local journal name
Local Library	Local journal library.
Backlog Critical	Critical range for size of backlog.
Backlog Warning	Warning range for size of backlog.
Catch-up Critical	Critical range for number of minutes for the journal receiver to catch up.
Catch-up Warning	Warning range for number of minutes for the journal receiver to catch up.

Returns the following information:

Current Backlog	Size of current backlog.
Min. to clear backlog	Number of minutes to clear receiver backlog.

check_Shield_OSLVL

Returns installed OS release level.

Service State Information

Current Status:	OK (for 14d 23h 6m 0s)
Status Information:	OS Level: V7R2M0
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	02-14-2023 10:43:28
Check Type:	ACTIVE
Check Latency / Duration:	0.181 / 0.026 seconds
Next Scheduled Check:	02-15-2023 10:43:28
Last State Change:	01-31-2023 10:40:51
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	02-15-2023 09:46:43 (0d 0h 0m 8s ago)

Active Checks:	ENABLED
Passive Checks:	DISABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

OS Level

Parameters:

There are no parameters for this check.

Returns the OS level in the following format:

OS Level: VXRXXM

check_Shield_PING

Returns response time from pinging an address.

Service State Information

Current Status:	OK (for 0d 2h 45m 7s)
Status Information:	AVG time to ping www.shieldadvanced.com: 4ms Success rate of packets: 100% (5/5) MAX time to ping: 5ms MIN time to ping: 4ms
Performance Data:	Success=100;Min=4;Avg=4;Max=5
Current Attempt:	1/2 (HARD state)
Last Check Time:	02-15-2023 13:13:18
Check Type:	ACTIVE
Check Latency / Duration:	1.636 / 0.056 seconds
Next Scheduled Check:	02-15-2023 14:13:18
Last State Change:	02-15-2023 10:28:26
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	02-15-2023 13:13:31 (0d 0h 0m 2s ago)

Active Checks:	ENABLED
Passive Checks:	DISABLED
Obsessing:	ENABLED
Notifications:	DISABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

PING response

Parameters:

Address	IP Address or DNS entry to attempt to ping.
PING Critical	Critical range for AVERAGE response time(ms).
PING Warning	Warning range for AVERAGE response time(ms).

Returns the following information:

Success rate	Success rate of packets sent including (received/sent).
AVG response time	Average response time returned over 5 packets sent.
MAX response time	Longest response time returned from 5 packets sent.
MIN response time	Shortest response time returned from 5 packets sent.

check_Shield_ASPSTS

Returns status of queried ASP.

Service State Information

Current Status:	OK (for 0d 1h 14m 41s)
Status Information:	ASP01 is Available.
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	02-17-2023 11:45:45
Check Type:	ACTIVE
Check Latency / Duration:	0.134 / 0.065 seconds
Next Scheduled Check:	02-17-2023 12:45:45
Last State Change:	02-17-2023 10:45:38
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	02-17-2023 12:00:15 (0d 0h 0m 4s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	DISABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

ASP Status

Parameters:

Device ASP device to be queried.
Severity Severity of return value if status is not Active or Available

The ASP status will return one of the following:

Available
Active
Varied ON
Varied OFF

check_Shield_ASPAVL

Returns MB of available disk space.

Service State Information

Current Status:	OK (for 0d 1h 26m 27s)
Status Information:	ASP01 available disk space: 47369MB.
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	02-17-2023 11:45:45
Check Type:	ACTIVE
Check Latency / Duration:	0.292 / 0.000 seconds
Next Scheduled Check:	02-17-2023 12:45:45
Last State Change:	02-17-2023 10:45:39
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	02-17-2023 12:12:06 (0d 0h 0m 0s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	DISABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

ASP Available Disk Space

Parameters:

Device	ASP device to be queried.
Critical Range	Critical range for available space.
Warning Range	Warning range for available space.

check_Shield_ASPMIR

Returns Mirror status of ASP.

Service State Information

Current Status:	CRITICAL (for 0d 1h 34m 59s)
Status Information:	CRITICAL-Mirror is not configured.
Performance Data:	
Current Attempt:	2/2 (HARD state)
Last Check Time:	02-17-2023 12:20:25
Check Type:	ACTIVE
Check Latency / Duration:	1.131 / 0.064 seconds
Next Scheduled Check:	02-17-2023 13:20:25
Last State Change:	02-17-2023 10:45:38
Last Notification:	N/A (notification 1)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	02-17-2023 12:20:36 (0d 0h 0m 1s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	DISABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

ASP Mirror Status

Parameters:

Device ASP device to be queried.
Severity Severity of notification to be sent if status is not ACTIVE

The ASP Mirror status will return one of the following:

This mirrored unit of a mirrored pair is ACTIVE
This mirrored unit is being SYNCHRONIZED
This mirrored unit is SUSPENDED
Mirror is not configured

check_Shield_ASPLIFE

Returns percentage of remaining life for ASP NVMe drives.

Service State Information

Current Status:	UNKNOWN (for 0d 4h 57m 20s) (Has been acknowledged)
Status Information:	ERROR:No devices found matching ASP01.
Performance Data:	
Current Attempt:	2/2 (HARD state)
Last Check Time:	02-17-2023 10:45:38
Check Type:	ACTIVE
Check Latency / Duration:	0.815 / 0.063 seconds
Next Scheduled Check:	02-18-2023 10:45:38
Last State Change:	02-17-2023 10:43:00
Last Notification:	02-17-2023 10:43:00 (notification 1)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	02-17-2023 15:40:15 (0d 0h 0m 5s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	DISABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

ASP NVMe Life Remaining

Parameters:

Device ASP device to be queried.
Critical Range Critical range for remaining life.
Warning Range Warning range for remaining life.

Note: check will return "ERROR:No devices found matching [ASP]" if ASP drives are not NVMe.

check_Shield_ASPDSK

Returns Disk status for ASP.

Service State Information

Current Status:	OK (for 0d 5h 6m 19s)
Status Information:	ASP01 has 47369MB of available disk space remaining. 1 Disks reported with 1 configured. ASP01 has 47722MB of total disk space.
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	02-17-2023 15:45:45
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.361 seconds
Next Scheduled Check:	02-17-2023 16:45:45
Last State Change:	02-17-2023 10:45:38
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	02-17-2023 15:51:55 (0d 0h 0m 2s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	DISABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

ASP Disk Status

Parameters:

Device	ASP device to be queried.
Configured Disks	Number of configured disks to be compared to the number of disks returned from check.
Critical Range	Critical range for available disk space.
Warning Range	Warning range for available disk space.

check_Shield_ASPOVRFLW

Returns overflow storage status for ASP.

Service State Information

Current Status:	OK (for 0d 5h 8m 18s)
Status Information:	ASP01-Overflow storage: 0MB
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	02-17-2023 15:45:45
Check Type:	ACTIVE
Check Latency / Duration:	0.133 / 0.061 seconds
Next Scheduled Check:	02-17-2023 16:45:45
Last State Change:	02-17-2023 10:45:38
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	02-17-2023 15:53:55 (0d 0h 0m 1s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	DISABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

ASP Overflow Storage

Parameters:

Device	ASP device to be queried.
Critical Range	Critical range for MB of overflow storage.
Warning Range	Warning range MB of overflow storage.

check_Shield_ASPGEOSTS

Returns geographic mirror data status.

Service State Information

Current Status:	CRITICAL (for 0d 3h 23m 46s)
Status Information:	ASP01-Geographic mirroring is not configured.
Performance Data:	
Current Attempt:	2/2 (HARD state)
Last Check Time:	02-17-2023 15:46:45
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.528 seconds
Next Scheduled Check:	02-17-2023 16:46:45
Last State Change:	02-17-2023 12:46:45
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	02-17-2023 16:10:25 (0d 0h 0m 6s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	DISABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

ASP Geo Mirror Status

Parameters:

Device ASP device to be queried.
Severity Severity of notification to be returned.

The ASP Geographic Mirror status will return one of the following:

- Geographic mirroring is not configured.
- The remote copy is absolutely in sync with the production copy.
- The remote copy contains usable data. A detached mirror copy always has this state.
- There is incoherent data in the mirror copy and the data cannot be used.

check_Shield_DEVSTS

Returns device status of passed in device.

Service State Information

Current Status:	OK (for 0d 0h 4m 2s+)
Status Information:	Device status: ACTIVE
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	06-28-2023 16:13:41
Check Type:	ACTIVE
Check Latency / Duration:	1.669 / 0.030 seconds
Next Scheduled Check:	06-28-2023 17:13:41
Last State Change:	N/A
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	06-28-2023 16:17:30 (0d 0h 0m 3s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Device Status

Parameters:

Device Type	Type of device to check.
Device Name	Name of device to be checked.
Status List	This is a list of statuses to compare against returned device status. If a match is not found an alert will be sent. Values separated by “:”
Severity	Alert severity if returned status does not match comparison value. [0,1,2,3]

The Device status will return one of the following values:

0	VARIED OFF
1	OPERATIONAL
2	AS/36 DISABLED
5	DEALLOCATED
6	UNPROTECTED
7	ALLOCATED
8	STAND-ALONE
10	VARY OFF PENDING

20 VARY ON PENDING
21 VARY ON PENDING/DETACHED
22 VARY ON PENDING/ALLOCATE
30 VARIED ON
31 VARIED ON/ALLOCATE
32 VARYON/CNNPENDING
33 AS/36 ENABLED
40 CONNECT PENDING
50 SIGNON DISPLAY
51 ACTIVE/CNN PENDING
60 ACTIVE
61 ACTIVE/DETACHED
62 ACTIVE/SOURCE
63 ACTIVE READER
64 ACTIVE/TARGET
65 ACTIVE/ALLOCATE
66 ACTIVE WRITER
67 AVAILABLE
68 UNAVAILABLE
70 HELD
71 HELD/DETACHED
72 HELD/SOURCE
73 HELD/TARGET
74 HELD/ALLOCATE
75 POWERED OFF
80 RCYPND
81 RCYPND/DETACHED
82 RCYPND/SOURCE
83 RCYPND/TARGET
84 RCYPND/ALLOCATE
90 RCYCNL

91	RCYCNL/DETACHED
92	RCYCNL/SOURCE
93	RCYCNL/TARGET
94	RCYCNL/ALLOCATE
95	SYSTEM REQUEST
96	REBUILD
100	FAILED
101	FAILED/DETACHED
102	FAILED/SOURCE
103	FAILED READER
104	FAILED/TARGET
105	FAILED/ALLOCATE
106	FAILED WRITER
107	SHUTDOWN
110	DIAGNOSTIC MODE
111	*DAMAGED
112	*LOCKED
113	*UNKNOWN
114	DEGRADED
200	INVALID STATUS

check_Shield_DMGOBJ

Returns number of damaged objects found in a library. It is possible to input *ALLUSR in the library, but not *ALL. This is to reduce the load this check will take on the system.

Service State Information

Current Status:	OK (for 0d 0h 59m 41s)
Status Information:	There are 0 damaged objects in NG4I11.
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	06-28-2023 16:43:50
Check Type:	ACTIVE
Check Latency / Duration:	1.535 / 0.029 seconds
Next Scheduled Check:	06-29-2023 16:43:50
Last State Change:	06-28-2023 15:44:17
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	06-28-2023 16:43:51 (0d 0h 0m 7s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Damaged Objects

Parameters:

Library	Library to be searched for damaged objects.
Critical Range	Critical alert range for the number of damaged objects returned.
Warning Range	Warning alert range for the number of damaged objects returned.

The Damaged Object status will return:

There are 0 damaged objects in LIBRARY.

OR

CRITICAL-There are 2 damaged objects in LIBRARY.

Object OBJ1 : LIBRARY is Damaged

Object OBJ2 : LIBRARY is Partially Damaged

check_Shield_JOB_CPU

This check REPLACES check_Shield_TOPJOB_CPU which has been deprecated. Returns the Job processor time and runtime for all jobs matching the inputted search criteria, these are not organized to show top jobs.

Service State Information

Current Status:	OK (for 1d 19h 9m 59s)
Status Information:	All jobs within set ranges.
	Job: NGSVR Job User: NG4IUSER Job Number: 708424 Processor Time Used: 8(ms) Runtime: 152882(ms)
	Job: NAGRSPCLNT Job User: NG4IUSER Job Number: 708425 Processor Time Used: 9120(ms) Runtime: 152882(ms)
	Job: NAGRSPCLNT Job User: NG4IUSER Job Number: 708426 Processor Time Used: 18535(ms) Runtime: 152882(ms)
	Job: NAGRSPCLNT Job User: NG4IUSER Job Number: 708427 Processor Time Used: 18594(ms) Runtime: 152882(ms)
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	06-30-2023 10:11:13
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.179 seconds
Next Scheduled Check:	06-30-2023 10:21:13
Last State Change:	06-28-2023 15:07:30
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	06-30-2023 10:17:21 (0d 0h 0m 8s ago)

Job CPU

Parameters:

Job Name	Job name search parameter.
Job User	Job user search parameter.
Job Number	Job number search parameter.
Critical CPU	Critical alert range for the processor time used.
Warning CPU	Warning alert range for the processor time used.
Critical CPU	Critical alert range for the runtime returned.
Warning CPU	Warning alert range for the runtime returned.

For each job matching the search criteria the following will be returned:

Job: NGSVR
Job User: NG4IUSER
Job Number: 708424
Processor Time Used: 8(ms)
Runtime: 152882(ms)

check_Shield_JOBSTG

This check REPLACES check_Shield_TOPJOB_STG which has been deprecated. Returns the Job QTEMP size and Temporary Storage for all jobs matching the inputted search criteria, these are not organized to show top jobs.

Service State Information

Current Status:	OK (for 1d 19h 11m 32s)
Status Information:	All jobs within set ranges.
	Job: NGSVR Job User: NG4IUSER Job Number: 708424 QTEMP: 65536(bytes) Temp Storage: 4(MB)
	Job: NAGRSPCLNT Job User: NG4IUSER Job Number: 708425 QTEMP: 108204032(bytes) Temp Storage: 11(MB)
	Job: NAGRSPCLNT Job User: NG4IUSER Job Number: 708426 QTEMP: 109256704(bytes) Temp Storage: 11(MB)
	Job: NAGRSPCLNT Job User: NG4IUSER Job Number: 708427 QTEMP: 120791040(bytes) Temp Storage: 11(MB)
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	06-30-2023 10:14:28
Check Type:	ACTIVE
Check Latency / Duration:	0.130 / 0.030 seconds
Next Scheduled Check:	06-30-2023 10:24:28
Last State Change:	06-28-2023 15:07:30
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	06-30-2023 10:19:01 (0d 0h 0m 1s ago)

Damaged Objects

Parameters:

- Job Name Job name search parameter.
- Job User Job user search parameter.
- Job Number Job number search parameter.
- Critical QTEMP Critical alert range for the QTEMP size.
- Warning QTEMP Warning alert range for the QTEMP size.
- Critical Temp Storage Critical alert range for the temporary storage used.

Warning Temp Storage Warning alert range for the temporary storage used.

For each job matching the search criteria the following will be returned:

Job: NAGRSPCLNT
Job User: NG4IUSER
Job Number: 708427
QTEMP: 120791040(bytes)
Temp Storage: 11(MB)

check_Shield_TOPCPU

Returns the top x jobs which are organized by CPU percentage over a period of time. It is possible to set the max number of jobs and the minimum value returned.

Service State Information

Current Status:	OK (for 1d 19h 25m 57s)
Status Information:	All jobs are below set ranges.
	Elapsed Time 0:0:0 Job: NAGRSPCLNT/NG4IUSER/708426 CPU: 41.60%
	Elapsed Time 0:0:0 Job: NAGRSPCLNT/NG4IUSER/708425 CPU: 37.50%
	Elapsed Time 0:0:0 Job: SCPF/QSYS/000000 CPU: 0.00%
	Elapsed Time 0:0:0 Job: QSYSARB3/QSYS/706463 CPU: 0.00%
	Elapsed Time 0:0:0 Job: QDBSRV01/QSYS/706469 CPU: 0.00%
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	06-30-2023 10:31:12
Check Type:	ACTIVE
Check Latency / Duration:	0.176 / 0.040 seconds
Next Scheduled Check:	06-30-2023 10:51:12
Last State Change:	06-28-2023 15:11:11
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	06-30-2023 10:37:01 (0d 0h 0m 7s ago)

Top 5 Jobs by CPU(%)

Parameters:

Max Count	Maximum number of jobs returned.
Min Value	Minimum CPU % to be returned.
Reset	Reset flag, see information below on the reset.
Critical CPU	Critical alert range for the CPU percentage returned.
Warning CPU	Warning alert range for the CPU percentage returned.

Reset Flag:

Resetting the elapsed time is carried out after the data has been retrieved. This provides the ability to see the usage stats over a set period of time ie: request is run with reset=1, the data returned on this request reflects the stats using the elapsed time since the last reset. Another request for the same data in 5 minutes time would have an elapsed time period of 5 minutes. This reset will affect the following requests so be aware of how each request is run.

For each job matching the search criteria the following will be returned:

Elapsed Time 0:0:0
Job: QDBSRV01/QSYS/706469
CPU: 0.00%

check_Shield_TOPCPU

Returns the top x jobs which are organized by CPU time (ms) over a period of time. It is possible to set the max number of jobs and the minimum value returned.

Service State Information

Current Status:	OK (for 5d 5h 11m 46s)
Status Information:	All jobs are below set ranges.
	Elapsed Time 0:13:33 Job: ADMIN2/QLWISVR/001759 CPU: 0:0:0ms
	Elapsed Time 0:13:33 Job: QFILESYS1/QSYS/001610 CPU: 0:0:0ms
	Elapsed Time 0:13:33 Job: QTSMTPCLT/QTCP/002410 CPU: 0:0:0ms
	Elapsed Time 0:13:33 Job: ADMIN1/QWEBADMIN/001758 CPU: 0:0:0ms
	Elapsed Time 0:13:33 Job: ADMIN5/QLWISVR/001756 CPU: 0:0:0ms
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	09-01-2023 12:03:26
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.091 seconds
Next Scheduled Check:	09-01-2023 12:23:26
Last State Change:	08-27-2023 07:00:56
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	09-01-2023 12:12:35 (0d 0h 0m 7s ago)

Top 5 Jobs by CPU(ms)

Parameters:

Max Count	Maximum number of jobs returned.
Min Value	Minimum CPU time to be returned.
Reset	Reset flag, see information below on the reset.
Critical CPU (ms)	Critical alert range for the CPU time returned.
Warning CPU (ms)	Warning alert range for the CPU time returned.

Reset Flag:

Resetting the elapsed time is carried out after the data has been retrieved. This provides the ability to see the usage stats over a set period of time ie: request is run with reset=1, the data returned on this request reflects the stats using the elapsed time since the last reset. Another request for the same data in 5 minutes time would have an elapsed time period of 5 minutes. This reset will affect the following requests so be aware of how each request is run.

NOTE: The reset is based on the responder job where the request is run, therefore a reset in one responder job does not affect the others, this means if a request hits a different responder job the elapsed time may not reflect the time of the reset request in the other responder job.

For each job matching the search criteria the following will be returned:

Elapsed Time 0:13:33

Job: ADMIN5/QLWISVR/001756

CPU: 0:0:0ms

check_Shield_TOPDSKIO

Returns the top x jobs which are organized by Disk I/O over a period of time. It is possible to set the max number of jobs and the minimum value returned.

Service State Information

Current Status:	OK (for 0d 4h 37m 8s)
Status Information:	All jobs are below set ranges.
	Elapsed Time 0:18:0 Job: SCPF/QSYS/000000 DISK IO: 0
	Elapsed Time 0:18:0 Job: QSYSARB3/QSYS/001114 DISK IO: 0
	Elapsed Time 0:18:0 Job: QDBSRV01/QSYS/001120 DISK IO: 0
	Elapsed Time 0:18:0 Job: QDBSRV02/QSYS/001121 DISK IO: 0
	Elapsed Time 0:18:0 Job: QDBSRV03/QSYS/001122 DISK IO: 0
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	09-01-2023 12:00:42
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.073 seconds
Next Scheduled Check:	09-01-2023 12:20:42
Last State Change:	09-01-2023 07:40:42
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	09-01-2023 12:17:45 (0d 0h 0m 5s ago)

Top 5 Jobs by Disk I/O

Parameters:

Max Count	Maximum number of jobs returned.
Min Value	Minimum Disk I/O to be returned.
Reset	Reset flag, see information below on the reset.
Critical DISK IO	Critical alert range for the Disk I/O returned.
Warning DISK IO	Warning alert range for the Disk I/O time returned.

Reset Flag:

Resetting the elapsed time is carried out after the data has been retrieved. This provides the ability to see the usage stats over a set period of time ie: request is run with reset=1, the data returned on this request reflects the stats using the elapsed time since the last reset. Another request for the same data in 5 minutes time would have an elapsed time period of 5 minutes. This reset will affect the following requests so be aware of how each request is run.

NOTE: The reset is based on the responder job where the request is run, therefore a reset in one responder job does not affect the others, this means if a request hits a different responder job the elapsed time may not reflect the time of the reset request in the other responder job.

For each job matching the search criteria the following will be returned:

Elapsed Time 0:18:0
Job: QDBSRV03/QSYS/001122
DISK IO: 0

check_Shield_TOPINTRS

Returns the top x jobs which are organized by interactive response time over a period of time. It is possible to set the max number of jobs and the minimum value returned.

Service State Information

Current Status:	OK (for 0d 21h 43m 14s)
Status Information:	All jobs are below set ranges.
	Elapsed Time 1:0:0 Job: SCPF/QSYS/000000 Interactive Response time: 0.00s
	Elapsed Time 1:0:0 Job: QSYSARB3/QSYS/001114 Interactive Response time: 0.00s
	Elapsed Time 1:0:0 Job: QDBSRV01/QSYS/001120 Interactive Response time: 0.00s
	Elapsed Time 1:0:0 Job: QDBSRV02/QSYS/001121 Interactive Response time: 0.00s
	Elapsed Time 1:0:0 Job: QDBSRV03/QSYS/001122 Interactive Response time: 0.00s
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	09-01-2023 12:22:42
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.053 seconds
Next Scheduled Check:	09-01-2023 12:42:42
Last State Change:	08-31-2023 14:42:37
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	09-01-2023 12:25:45 (0d 0h 0m 6s ago)

Top 5 Jobs by Interactive Response Time

Parameters:

- Max Count Maximum number of jobs returned.
- Min Value Minimum Disk I/O to be returned.
- Reset Reset flag, see information below on the reset.
- Critical Response Time Critical alert range for the Response Time returned.
- Warning Response Time Warning alert range for the Response Time returned.

Reset Flag:

Resetting the elapsed time is carried out after the data has been retrieved. This provides the ability to see the usage stats over a set period of time ie: request is run with reset=1, the data returned on this request reflects the stats using the elapsed time since the last reset. Another request for the same data in 5 minutes time would have an elapsed time period of 5 minutes. This reset will affect the following requests so be aware of how each request is run.

NOTE: The reset is based on the responder job where the request is run, therefore a reset in one responder job does not affect the others, this means if a request hits a different responder job the elapsed time may not reflect the time of the reset request in the other responder job.

For each job matching the search criteria the following will be returned:

Elapsed Time 1:0:0
Job: QDBSRV03/QSYS/001122
Interactive Response time: 0.00s

check_Shield_TOPINTTRANS

Returns the top x jobs which are organized by interactive transactions over a period of time. It is possible to set the max number of jobs and the minimum value returned.

Service State Information

Current Status:	OK (for 0d 21h 50m 23s)
Status Information:	All jobs are below set ranges.
	Elapsed Time 0:0:29 Job: SCPF/QSYS/000000 Interactive Transactions: 0
	Elapsed Time 0:0:29 Job: QSYSARB3/QSYS/001114 Interactive Transactions: 0
	Elapsed Time 0:0:29 Job: QDBSRV01/QSYS/001120 Interactive Transactions: 0
	Elapsed Time 0:0:29 Job: QDBSRV02/QSYS/001121 Interactive Transactions: 0
	Elapsed Time 0:0:29 Job: QDBSRV03/QSYS/001122 Interactive Transactions: 0
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	09-01-2023 12:41:12
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.084 seconds
Next Scheduled Check:	09-01-2023 13:01:12
Last State Change:	08-31-2023 15:01:11
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	09-01-2023 12:51:25 (0d 0h 0m 9s ago)

Top 5 Jobs by Interactive Transactions

Parameters:

Max Count	Maximum number of jobs returned.
Min Value	Minimum Disk I/O to be returned.
Reset	Reset flag, see information below on the reset.
Critical Transactions	Critical alert range for the Transactions returned.
Warning Transactions	Warning alert range for the Transactions returned.

Reset Flag:

Resetting the elapsed time is carried out after the data has been retrieved. This provides the ability to see the usage stats over a set period of time ie: request is run with reset=1, the data returned on this request reflects the stats using the elapsed time since the last reset. Another request for the same data in 5 minutes time would have an elapsed time period of 5 minutes. This reset will affect the following requests so be aware of how each request is run.

NOTE: The reset is based on the responder job where the request is run, therefore a reset in one responder job does not affect the others, this means if a request hits a different responder job the elapsed time may not reflect the time of the reset request in the other responder job.

For each job matching the search criteria the following will be returned:

Elapsed Time 0:0:29
Job: QDBSRV03/QSYS/001122
Interactive Transactions: 0

check_Shield_DQECOUNT

Returns the data queue entry count for passed DQ.

Service State Information

Current Status:	OK (for 0d 21h 55m 40s)
Status Information:	Data Queue Entries:0 (QSYSDTAQ QSYS 0:116496) Max Data Queue Entries:116496
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	09-01-2023 11:59:54
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.081 seconds
Next Scheduled Check:	09-01-2023 12:59:54
Last State Change:	08-31-2023 14:59:54
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	09-01-2023 12:55:25 (0d 0h 0m 9s ago)

DQ Entry Count for QSYSDTAQ

Parameters:

Data Queue	Name of Data Queue.
Library	Library for Data Queue.
Critical Entries	Critical alert range for the number of DQ entries returned.
Warning Entries	Warning alert range for the number of DQ entries returned.

The following will be returned:

Data Queue Entries	Number of entries on Data Queue.
Max Data Queue Entries	Maximum number of entries possible on Data Queue

check_Shield_LIBSIZE

Returns size and number of objects in a Library.

Service State Information	
Current Status:	OK (for 0d 22h 13m 23s)
Status Information:	Library Size (NG4I20): 7041024 bytes Number of objects in NG4I20: 89
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	09-01-2023 13:00:12
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.080 seconds
Next Scheduled Check:	09-01-2023 14:00:12
Last State Change:	08-31-2023 15:00:11
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	09-01-2023 13:13:25 (0d 0h 0m 9s ago)

Library size of NG4I20

Parameters:

Library	Library for to be monitored.
Critical Size	Critical alert range for the size(bytes) returned.
Warning Size	Warning alert range for the size(bytes returned).
Critical Object Count	Critical alert range for the number of objects in library returned.
Warning Object Count	Warning alert range for the number of objects in library returned.

The following will be returned:

Data Queue Entries	Number of entries on Data Queue.
Max Data Queue Entries	Maximum number of entries possible on Data Queue

check_Shield_WRKPRB

Returns problems logged on IBM i with WRKPRB.

Service State Information	
Current Status:	OK (for 0d 23h 7m 56s)
Status Information:	There are no problems logged on the system.
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	09-01-2023 13:42:37
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.037 seconds
Next Scheduled Check:	09-01-2023 14:42:37
Last State Change:	08-31-2023 14:42:37
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	09-01-2023 13:50:25 (0d 0h 0m 8s ago)

WRKPRB problems

Parameters:

Critical Problem Count Critical alert range for the number of problems listed on the system.
Warning Problem Count Warning alert range for the number of problems listed on the system.
Whitelist List of problem statuses to be included towards counted problem count.
Separated by ',' [C,O,R,S,A,P,V]

C – Closed
O – Opened
R – Ready
S – Sent
A – Answered
P – Prepared
V – Verified

The following will be returned:

There are no problems logged on the system.

OR

WARNING-Open problem count:1

Problem ID:2326440613

Date:20230921114946

Problem Type:3

Problem Status:ANSWERED

Problem ID:2325800012

Date:20230915000004

Problem Type:1

Problem Status:READY

check_Shield_OUTQC

Returns number of spoolfiles on an OutQ.

Service State Information

Current Status:	OK (for 0d 23h 48m 33s)
Status Information:	Spoolfile count on QPRINT: 10
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	09-01-2023 14:32:37
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.088 seconds
Next Scheduled Check:	09-01-2023 14:42:37
Last State Change:	08-31-2023 14:52:37
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	09-01-2023 14:41:05 (0d 0h 0m 5s ago)

Spoolfile count on QPRINT

Parameters:

- Out Queue Out queue to be monitored.
- Library Library for out queue.
- Critical Spoolfile Count Critical alert range for the number of spoolfiles on the out queue.
- Warning Spoolfile Count Warning alert range for the number of spoolfiles on the out queue.

The following will be returned:

Spoolfile count on [Out Queue]: 1

check_Shield_SSTP

Returns SST Profile Status

Service State Information

Current Status:	OK (for 0d 0h 1m 9s)
Status Information:	SST profile status (QSECOFR): SST profile QSECOFR is ENABLED.
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	09-28-2023 13:28:29
Check Type:	ACTIVE
Check Latency / Duration:	1.239 / 0.022 seconds
Next Scheduled Check:	09-28-2023 14:28:29
Last State Change:	09-28-2023 13:27:27
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	09-28-2023 13:28:35 (0d 0h 0m 1s ago)

SST Profile Status

Parameters:

User SST user profile to be checked. *ALL is a viable option.
Type Type of status to be returned [STATUS/EXPDAT/PWDEXP]. Profile status, expiry date, password expiry.
Severity Critical alert range for the number of spoolfiles on the out queue.

The following will be returned:

Spoolfile count on [Out Queue]: 10

check_Shield_IFSCOUNT

Returns IFS directory count.

Service State Information

Current Status:	OK (for 0d 0h 0m 18s+)
Status Information:	Number of Objects in '/home/ng4i/log' Streamfiles: 6 Directories: 1 Symbolic Links: 0 Inaccessible Objects: 0
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	12-20-2023 09:20:10
Check Type:	ACTIVE
Check Latency / Duration:	1.408 / 0.024 seconds
Next Scheduled Check:	12-22-2023 09:20:10
Last State Change:	N/A
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	12-20-2023 09:20:12 (0d 0h 0m 8s ago)

Object count in IFS directory

Parameters:

Path	Path to IFS directory.
File System Type	Type of file system, ie LOCAL/QNTC.
Critical Streamfile	Critical alert range for the number of Streamfiles in the directory.
Warning Streamfile	Warning alert range for the number of Streamfiles in the directory.
Critical Directories	Critical alert range for the number of Sub directories in the directory.
Warning Directories	Warning alert range for the number of Sub directories in the directory.
Critical Symbolic Links	Critical alert range for the number of Symbolic Links in the directory.
Warning Symbolic Links	Warning alert range for the number of Symbolic Links in the directory.
Critical Inaccessible Obj	Critical alert range for the number of Inaccessible Objects in the directory.
Warning Inaccessible Obj	Critical alert range for the number of accessible Objects in the directory.

The following will be returned:

Number of Objects in '[PATH]'
Streamfiles: [Streamfile Count]
Directories: [Directory Count]
Symbolic links: [Symbolic Link Count]
Inaccessible Objects: [Inaccessible Objects Count]

check_Shield_IFSSIZE

Returns IFS directory size.

Service State Information

Current Status:	OK (for 0d 0h 19m 49s+)
Status Information:	Size of '/home/ng4i/log': 4.1MB Objects in '/home/ng4i/log': 6 Directories in '/home/ng4i/log': 1
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	12-20-2023 09:20:13
Check Type:	ACTIVE
Check Latency / Duration:	1.739 / 0.023 seconds
Next Scheduled Check:	12-21-2023 09:20:13
Last State Change:	N/A
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	12-20-2023 09:39:42 (0d 0h 0m 9s ago)

IFS directory size.

Parameters:

Path	Path to IFS directory
Critical Size	Critical alert range for the Size of the directory.
Warning Size	Warning alert range for the Size of the directory.
Critical Objects	Critical alert range for the number of Objects in the directory.
Warning Objects	Warning alert range for the number of Objects in the directory.
Critical Directories	Critical alert range for the number of Sub directories in the directory.
Warning Directories	Warning alert range for the number of Sub directories in the directory.

The following will be returned:

Size of '[PATH]': [Size in MB]
Objects in '[PAT]': [Object Count]
Directories in '[PATH]': [Directory Count]

check_Shield_LPPSTS

Returns Status of IBM i LPP.

Service State Information

Current Status:	OK (for 0d 0h 49m 15s)
Status Information:	LPP Load State: *INSTALLED 1NG4INV Error Status: *NONE
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	12-20-2023 10:09:27
Check Type:	ACTIVE
Check Latency / Duration:	1.570 / 0.026 seconds
Next Scheduled Check:	12-21-2023 10:09:27
Last State Change:	12-20-2023 09:20:17
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	12-20-2023 10:09:27 (0d 0h 0m 5s ago)

Status of NG4i LPP.

Parameters:

LPP	LPP Name
Option	LPP Option.
Version	LPP Version.
LoadID	LPP Load ID.
Severity	Severity if LPP has the status of *DAMAGED or is in ERROR.

The following will be returned:

LPP Load Status: [*DEFINED, *PACKAGED, *CREATED, *DAMAGED, *INSTALLED, *LOADED]

[LPP] Error Status : [*NONE/*ERROR]

check_Shield_JOBESTS

Returns End Status jobs matching search criteria.

Service State Information

Current Status:	OK (for 0d 1h 42m 28s)
Status Information:	Job: NGSVR NG4USER 025810 Job Status: Job has not ended.
	Job: NAGRSPCLNT NG4USER 025811 Job Status: Job has not ended.
	Job: NAGRSPCLNT NG4USER 025812 Job Status: Job has not ended.
	Job: NAGRSPCLNT NG4USER 025813 Job Status: Job has not ended.
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	03-18-2024 12:52:44
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.070 seconds
Next Scheduled Check:	03-18-2024 13:02:44
Last State Change:	03-18-2024 11:12:44
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	03-18-2024 12:55:06 (0d 0h 0m 6s ago)

End status of NG4User jobs.

Parameters:

Job Name	Search field for job Name. Can use *ALL.
Job User	Search field for job User. Can use *ALL.
Job Number	Search field for job Number. Can use *ALL.
Job Run Type	Search field for job Run Type. *ACTIVE,*JOBQ,*OUTQ,*ALL
Job Type	Search field for job Type. “*” - This value lists all job types. *NOTE: quotation marks required. A - The job is an autostart job. B - The job is a batch job. I - The job is an interactive job. M - The job is a subsystem monitor job. R - The job is a spooled reader job. S - The job is a system job. W - The job is a spooled writer job. X - The job is the start-control-program-function (SCPF) system job

The following will be returned for EACH job matching search criteria:

Job: [Job Name] [Job User] [Job Number]
Job Status: [Job Status].

check_Shield_PORTCONN

Returns current connections on a specified port.

Service State Information

Current Status:	OK (for 0d 0h 0m 33s+)
Status Information:	Current Connections[Port:49140]: 4
	Remote IP: 10.10.10.65 Remote Port: 50592 Bytes In: 110 Bytes Out: 33 User Profile: NG4IUSER
	Remote IP: 10.10.10.143 Remote Port: 44414 Bytes In: 130 Bytes Out: 279 User Profile: NG4IUSER
	Remote IP: 10.10.10.143 Remote Port: 50736 Bytes In: 130 Bytes Out: 279 User Profile: NG4IUSER
	Remote IP: 10.10.10.143 Remote Port: 53034 Bytes In: 118 Bytes Out: 214 User Profile: NG4IUSER
Performance Data:	Connections=4
Current Attempt:	1/2 (HARD state)
Last Check Time:	04-23-2024 11:31:11
Check Type:	ACTIVE
Check Latency / Duration:	1.401 / 0.062 seconds
Next Scheduled Check:	04-23-2024 12:31:11
Last State Change:	N/A
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	04-23-2024 11:31:34 (0d 0h 0m 4s ago)

Connections on Port 49140.

Parameters:

Port	Port to check for connections.
Address Type	IP Address type [IPV4/IPV6].
Critical Range	Critical range for number of connections.
Warning Range	Warning range for number of connections.

The following will be returned for EACH connection:

Remote IP: [Remote system IP address]
Remote Port: [Port used by remote system].
Bytes In: [bytes in]
Bytes Out: [bytes out]
User Profile: [Related user profile]

check_Shield_PGMEXP

Returns state of requested Exit point for given program.

Service State Information	
Current Status:	OK (for 0d 0h 5m 6s+)
Status Information:	Exit Point: Registered (QIBM_QTMF_SVR_LOGON / FT4I012 / FT4I10)
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	05-14-2024 12:20:10
Check Type:	ACTIVE
Check Latency / Duration:	1.244 / 0.025 seconds
Next Scheduled Check:	05-14-2024 13:20:10
Last State Change:	N/A
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	05-14-2024 12:26:29 (0d 0h 0m 7s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	DISABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Exit point for FT4I012.

Parameters:

Exit Point	Exit Point to check.
Exit Point Format	Format of Exit Point.
Program	Program to be checked.
Program Library	Library of requested program.
Severity	Severity of alert to be sent if Exit Point is not “Registered”.

The following will be returned:

Exit Point: Registered ([Exit Point] / [Program] / [Library])

OR

Exit Point not found. ([Exit Point] / [Program] / [Library])

check_Shield_QHST

Returns messages found on QHST that match the requested message IDs.

Service State Information

Current Status:	OK (for 0d 0h 0m 13s+)
Status Information:	Number of Messages found: 0 Message ids requested: CPA7025,CPC3703
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	01-27-2025 14:02:35
Check Type:	ACTIVE
Check Latency / Duration:	3.315 / 0.000 seconds
Next Scheduled Check:	01-27-2025 14:12:35
Last State Change:	N/A
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	01-27-2025 14:02:39 (0d 0h 0m 4s ago)

QHST search for CPA7025 and CPC3703

Parameters:

Message ID	List of message IDs to search for. This is delimited by “;”
Minutes	Number of Min to check back.
Critical Message Count	Critical alert range for number of messages found.
Warning Message Count	Warning alert range for number of messages found.

The following will be returned:

Number of Messages found: 1

Message ids requested: CPA7025,CPC3703

For each Message found the following will be returned:

Severity, Message ID, Message Type, Date Sent and Time Sent.

check_Shield_JOBFUNC

Returns list of jobs running requested function as requested user.

Service State Information

Current Status:	OK (for 0d 0h 4m 54s)
Status Information:	Number of Jobs running with User NG4IUSER and Function NG4I001: 3
	Job: NAGRSPCLNT User: NG4IUSER Job Number: 040193
	Job: NAGRSPCLNT User: NG4IUSER Job Number: 040194
	Job: NAGRSPCLNT User: NG4IUSER Job Number: 040195
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	05-30-2024 12:38:46
Check Type:	ACTIVE
Check Latency / Duration:	1.440 / 0.023 seconds
Next Scheduled Check:	05-31-2024 12:38:51
Last State Change:	05-30-2024 12:38:46
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	05-30-2024 12:43:31 (0d 0h 0m 9s ago)

Jobs running NG4I001 as NG4IUSER.

Parameters:

Job Name	Search criteria for Job Name.
User	Search criteria for User.
Function	Search criteria for Function.
Critical Job Count	Critical range for count of jobs returned.
Warning Job Count	Warning range for count of jobs returned.

The following will be returned:

Number of Jobs running with User [USER] and Function [FUNCTION]: [COUNT]

For each job returned:

Job: NAGRSPCLNT

User: NG4IUSER

Job Number: 040193

check_Shield_JOBSBSSTS

Returns list of jobs in requested SubSystem with a specified Status.

Service State Information

Current Status:	OK (for 0d 0h 13m 51s)
Status Information:	Number of Jobs in NG4ISBS21 with status TIMW: 2
	Job: NAGRSPCLNT User: NG4IUSER Job Number: 040194
	Job: NAGRSPCLNT User: NG4IUSER Job Number: 040195
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	05-30-2024 12:38:50
Check Type:	ACTIVE
Check Latency / Duration:	1.920 / 0.053 seconds
Next Scheduled Check:	05-31-2024 12:38:51
Last State Change:	05-30-2024 12:38:50
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	05-30-2024 12:52:31 (0d 0h 0m 10s ago)

Jobs in NG4ISBS21 with Status TIMW.

Parameters:

Sub System	Search criteria for Subsystem.
Status	Search criteria for Status.
Critical Job Count	Critical range for count of jobs returned.
Warning Job Count	Warning range for count of jobs returned.

The following will be returned:

Number of Jobs in [Sub System] with status [Status]: [Count]

For each job returned:

Job: NAGRSPCLNT
User: NG4IUSER
Job Number: 040195

check_Shield_USRCLS

Returns User profiles with specified User Class.

Service State Information

Current Status:	OK (for 0d 0h 9m 12s)
Status Information:	Number of User Profiles with class - *SECOFR: 2 User Profiles: QSECOFR QSYS
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	03-31-2025 17:08:23
Check Type:	ACTIVE
Check Latency / Duration:	0.895 / 0.116 seconds
Next Scheduled Check:	04-01-2025 17:08:25
Last State Change:	03-31-2025 17:08:23
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	03-31-2025 17:17:31 (0d 0h 0m 4s ago)

Users with *SECOFR authority.

Parameters:

User Class	User class to search for.
Critical Count	Critical range for alert on number returned.
Warning Count	Warning range for alert on number returned.

The following will be returned:

List of User profiles matching the user class requested.

check_Shield_SPCAUTH

Returns User profiles with specified Special Authority.

Service State Information

Current Status:	OK (for 0d 0h 6m 10s)
Status Information:	Number of User Profiles with special authority - *ALLOBJ: 4 QLPAUTO QLPINSTALL QSECOFR QSYS
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	03-31-2025 17:08:21
Check Type:	ACTIVE
Check Latency / Duration:	1.317 / 0.026 seconds
Next Scheduled Check:	04-01-2025 17:08:25
Last State Change:	03-31-2025 17:08:21
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	03-31-2025 17:14:31 (0d 0h 0m 0s ago)

Users with *ALLOBJ authority.

Parameters:

Special Authority	Special Authority to search for.
Critical Count	Critical range for alert on number returned.
Warning Count	Warning range for alert on number returned.

The following will be returned:

List of User profiles matching the special authority requested.

check_Shield_CPURESET

Returns CPU percentage used with a Reset flag.

NOTE: the value is rounded up to the closest round number before being checked against ranges.

Service State Information

Current Status:	OK (for 0d 0h 15m 9s)
Status Information:	CPU Usage: 1.200000% (This value has been rounded before checked against ranges...)
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	03-31-2025 17:06:07
Check Type:	ACTIVE
Check Latency / Duration:	1.734 / 0.017 seconds
Next Scheduled Check:	03-31-2025 17:26:07
Last State Change:	03-31-2025 17:04:51
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	03-31-2025 17:19:50 (0d 0h 0m 10s ago)

CPU % used

Parameters:

- Critical CPU Usage Critical range for alert on percent returned.
- Warning CPU Usage Warning range for alert on percent returned.

The following will be returned:

CPU usage value as a %

Note: This call will reset the stats for the CPU usage after retrieving the actual CPU usage at the specific time of the call. This means the CPU stats reflect the same values as those presented when F10 is pressed on the WRKACTJOB.

check_Shield_STLUSR

Returns User Profiles who have not logged on in a given number of days.

*NOTE: these users must have a password and be *ENABLED*

Service State Information

Current Status:	OK (for 0d 0h 9m 28s)
Status Information:	2 Stale Users on system. Users who have not logged on in 30 days: NGUSER TESTUSR
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	04-09-2025 15:07:55
Check Type:	ACTIVE
Check Latency / Duration:	1.308 / 0.029 seconds
Next Scheduled Check:	04-10-2025 15:07:55
Last State Change:	04-09-2025 15:03:31
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	04-09-2025 15:12:58 (0d 0h 0m 1s ago)

Stale Users

Parameters:

Days	Number of days to look back for login.
Critical Count	Critical range for number of User profiles found.
Warning Count	Warning range for number of User profiles found.

The following will be returned:

No stale users found on system.

OR

[Count] Stale users on system.

Users who have not logged on in [Days] days:

[List of user profiles]

check_Shield_UPFFL

Returns count of Failed Logins for a requested User Profile. The count is reset when a user signs in successfully.

Service State Information

Current Status:	OK (for 0d 0h 17m 17s)
Status Information:	Failed Logins for TESTUSR: 0
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	04-09-2025 15:08:04
Check Type:	ACTIVE
Check Latency / Duration:	1.713 / 0.016 seconds
Next Scheduled Check:	04-10-2025 15:08:04
Last State Change:	04-09-2025 15:03:49
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	04-09-2025 15:20:59 (0d 0h 0m 7s ago)

Failed logins for TESTUSR

Parameters:

Profile	Profile to check.
Critical Failed Logins	Critical range for number of Failed Logins
Warning Failed Logins	Warning range for number of Failed Logins.

The following will be returned:

Failed Logins for [User]: [Count]

check_Shield_UPFSTS

Returns Status for requested User Profile.

Service State Information

Current Status:	OK (for 0d 0h 20m 11s)
Status Information:	TESTUSR Status: *ENABLED
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	04-09-2025 15:08:16
Check Type:	ACTIVE
Check Latency / Duration:	0.891 / 0.161 seconds
Next Scheduled Check:	04-09-2025 16:08:16
Last State Change:	04-09-2025 15:04:06
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	04-09-2025 15:24:09 (0d 0h 0m 8s ago)

Status for TESTUSR

Parameters:

Profile Profile to check.
Severity Severity of alert returned if user is not *ENABLED.

The following will be returned:
[User] Status: [Status]

check_Shield_UPFPWDE

Returns number of days until a requested user's password expires.

Service State Information

Current Status:	OK (for 0d 0h 23m 17s)
Status Information:	Password for TESTUSR does not expire.
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	04-09-2025 15:08:07
Check Type:	ACTIVE
Check Latency / Duration:	1.474 / 0.023 seconds
Next Scheduled Check:	04-10-2025 15:08:07
Last State Change:	04-09-2025 15:03:55
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	04-09-2025 15:27:09 (0d 0h 0m 3s ago)

Password Expiry for TESTUSR

Parameters:

Profile Profile to check.
Critical Days Critical range for number of days until expiry
Warning Days Warning range for number of days until expiry.

The following will be returned:

Password for [User] does not expire.

OR

Days until [User] password expiry: [Days until expiry]

check_Shield_UPFCLS

Compares User profiles user class against a comparison value. Alert sent if comparison does not match.

Service State Information

Current Status:	CRITICAL (for 0d 0h 23m 21s) (Has been acknowledged)
Status Information:	CRITICAL-TESTUSR Status: *USER Comparison Value: *SECOFR
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	04-09-2025 15:07:59
Check Type:	ACTIVE
Check Latency / Duration:	2.179 / 0.017 seconds
Next Scheduled Check:	04-10-2025 15:08:09
Last State Change:	04-09-2025 15:07:59
Last Notification:	04-09-2025 15:08:09 (notification 1)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	04-09-2025 15:31:19 (0d 0h 0m 1s ago)

User Class TESTUSR

Parameters:

Profile	Profile to check.
Comparison Value	Value to compare User class against
Severity	Severity of Alert if comparison does not match.

The following will be returned:

[User] User Class: [User Class]
Comparison Value: [User Class]

check_Shield_UPFSA

Compares User profiles Special Authorities against a comparison value. Alert sent if comparison does not match.

Note: Comparison string needs to be a string of 8 characters either 'Y' or 'N' such as "YYYYYYYY" or "NYYYYYNY". The positions relate to the following:

- [0] *ALLOBJ
- [1] *SECADM
- [2] *JOBCTL
- [3] *SPLCTL
- [4] *SAVSYS
- [5] *SERVICE
- [6] *AUDIT
- [7] *IOSYSCFG

Service State Information

Current Status:	OK (for 0d 0h 35m 21s)
Status Information:	CRITICAL-TESTUSR Special Authorities: *ALLOBJ *AUDIT
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	04-09-2025 15:08:10
Check Type:	ACTIVE
Check Latency / Duration:	1.287 / 0.022 seconds
Next Scheduled Check:	04-10-2025 15:08:10
Last State Change:	04-09-2025 15:04:01
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	04-09-2025 15:39:18 (0d 0h 0m 4s ago)

Special Authorities of TESTUSR
- Compared against "YYYYYYYY"

Parameters:

- Profile Profile to check.
- Comparison Value Value to compare Special Authorities against
- Severity Severity of Alert if comparison does not match.

The following will be returned:

- [User] Special Authorities:
- [List of Special Authorities]

check_Shield_UPFSTG

Returns total storage used by the requested user profile. This is the size of all objects owned by the User Profile.

Service State Information

Current Status:	OK (for 0d 0h 40m 59s)
Status Information:	TESTUSR Storage Used: 0MB
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	04-09-2025 15:08:12
Check Type:	ACTIVE
Check Latency / Duration:	0.952 / 0.017 seconds
Next Scheduled Check:	04-10-2025 15:08:12
Last State Change:	04-09-2025 15:04:34
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	04-09-2025 15:45:28 (0d 0h 0m 5s ago)

TESTUSR Storage used

Parameters:

Profile	Profile to check.
Critical Storage	Critical range for storage used by User
Warning Storage	Warning range for storage used by User.
Unit	Unit to be used for storage value. (KB/MB/GB/TB)

The following will be returned:

[User] Storage Used: [Storage used][Unit]

check_Shield_UPFEXP

Returns number of days until user profile expires.

Service State Information

Current Status:	OK (for 0d 0h 46m 16s)
Status Information:	TESTUSR does not expire.
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	04-09-2025 15:08:02
Check Type:	ACTIVE
Check Latency / Duration:	1.862 / 0.171 seconds
Next Scheduled Check:	04-10-2025 15:08:02
Last State Change:	04-09-2025 15:03:43
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	04-09-2025 15:49:58 (0d 0h 0m 1s ago)

TESTUSR Expiry Date

Parameters:

Profile	Profile to check.
Critical Storage	Critical range for number of days until user expires.
Warning Storage	Warning range for number of days until user expires.

The following will be returned:

[User] does not expire.

[User] expires in [Days] days.

check_Shield_MSGSEV

Returns messages of a requested severity or higher within the last X minutes found on requested message queue.

Service State Information

Current Status:	OK (for 0d 0h 0m 20s+)
Status Information:	No messages with severity 0 or above found in last 15 min.
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	04-28-2025 16:28:40
Check Type:	ACTIVE
Check Latency / Duration:	1.948 / 0.156 seconds
Next Scheduled Check:	04-28-2025 16:43:40
Last State Change:	N/A
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	04-28-2025 16:28:50 (0d 0h 0m 1s ago)

Message severity 0 in last 15 minutes

Parameters:

Message Queue	Message Queue to search.
Library	Message Queue library.
Message Severity	Minimum message severity to return.
Minutes	Number of minutes to look back.
Alert Severity	Alert level to return if messages are found.

The following will be returned:

No messages with severity %d or above found in last %d min.

OR

[Number of messages] message(s) with severity [Requested Severity] or above found in last [Requested minutes] min.

Message ID: [Message ID]

Message Severity: [Message Severity]

Message Date: [DD/MM/YY]

Message Time: [HH:MM:SS]

check_Shield_JOBSCDE2

Returns details on a requested job schedule entry.

Service State Information

Current Status:	OK (for 0d 0h 0m 24s)
Status Information:	AUDCHK Status: The entry is Scheduled Submit Status: Job successfully submitted. Job Details: AUDCHK CHRISH 102347 Completion Status: The job completed normally. Active Date: 25/09/23 11:15:00 End Date: 25/09/23 11:15:26 End Severity: 30 End Reason: Job ending in normal manner.
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	09-23-2025 11:25:26
Check Type:	ACTIVE
Check Latency / Duration:	2.154 / 0.020 seconds
Next Scheduled Check:	09-23-2025 11:55:30
Last State Change:	09-23-2025 11:25:26
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	09-23-2025 11:25:41 (0d 0h 0m 9s ago)

Job schedule entry details

Parameters:

JOBSCDE Job schedule entry.
End Severity Comparison Comparison value for job end severity
Severity Severity of alert returned if an issue is found with the JOBSCDE.

The following will be returned:

AUDCHK Status:
Submit Status:
Job Details:
Completion Status:
Active Date:
End Date:
End Severity:
End Reason:

check_Shield_IFSSTR

Returns search results of looking for a substring within an IFS file.

Service State Information

Current Status:	OK (for 0d 0h 0m 36s+)
Status Information:	Substring "Bytes received" found in /home/ng4i/log/NG4i108_debug.dta
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	09-23-2025 11:58:52
Check Type:	ACTIVE
Check Latency / Duration:	1.238 / 0.041 seconds
Next Scheduled Check:	09-24-2025 11:58:52
Last State Change:	N/A
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	09-23-2025 11:59:15 (0d 0h 0m 6s ago)

Searching for "Bytes received" in an IFS file

Parameters:

Filename	IFS file to search in, this includes the full path to the object.
Substring	Substring to search for. This parameter must be surrounded by ' '. ie. 'Bytes received'
Flag	Alert flag. This allows the user to either search for the substring with "1" or ensure the substring is not present with "0".
Severity	Severity of alert returned if flag is not satisfied.

The following will be returned:

Substring [Substring] found in [Filename]

OR

[Severity] Substring [Substring] not found in [Filename]

check_Shield_DTAATR

Returns search results of looking for a substring within a Data Area.

Service State Information

Current Status:	OK (for 0d 0h 2m 51s+)
Status Information:	Substring "NG4I072225" found in UPDATELVL
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	09-23-2025 12:10:27
Check Type:	ACTIVE
Check Latency / Duration:	1.518 / 0.022 seconds
Next Scheduled Check:	09-24-2025 12:10:27
Last State Change:	N/A
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	09-23-2025 12:10:27 (0d 0h 0m 2s ago)

Searching for "NG4I072225" in UPDATELVL

Parameters:

Filename	Data Area to search in.
Substring	Substring to search for. This parameter must be surrounded by ' '. ie. 'NG4I072225'
Flag	Alert flag. This allows the user to either search for the substring with "1" or ensure the substring is not present with "0".
Severity	Severity of alert returned if flag is not satisfied.

The following will be returned:

Substring [Substring] found in [Filename]

OR

[Severity] Substring [Substring] not found in [Filename]

check_Shield_DSKCHG

Returns change in disk usage over a set time period. The way to use this check is to utilize the Nagios check period to set the interval you wish to monitor disk usage over. AAG will then compare the disk usage when it runs to the disk usage from the last time the check was run to determine the change over time.

Service State Information

Current Status:	OK (for 1d 1h 59m 23s)
Status Information:	0% change in used disk space since last check.
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	09-23-2025 12:05:44
Check Type:	ACTIVE
Check Latency / Duration:	0.840 / 0.030 seconds
Next Scheduled Check:	09-23-2025 12:15:44
Last State Change:	09-22-2025 10:15:44
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	09-23-2025 12:14:57 (0d 0h 0m 10s ago)

% of disk change over time

Parameters:

Data Area	Data Area the user has created to store the latest disk usage. Creating multiple data areas will allow to monitor change over multiple time periods.
Critical %	Critical range for % of change.
Warning %	Warning range for % of change.

The following will be returned:

[Disk usage change %] change in used disk space since last check.

check_Shield_JOBRUNTIME

Returns jobs which have been running longer than the minimum run time value.

Service State Information

Current Status:	OK (for 0d 0h 0m 10s+)
Status Information:	4 jobs above minimum time. Job: NGSVR/NG4IUSER/102056 Runtime: 1611 min. Job: NAGRSPCLNT/NG4IUSER/102066 Runtime: 1611 min. Job: NAGRSPCLNT/NG4IUSER/102078 Runtime: 1611 min. Job: NAGRSPCLNT/NG4IUSER/102091 Runtime: 1611 min.
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	09-23-2025 13:03:04
Check Type:	ACTIVE
Check Latency / Duration:	2.308 / 0.022 seconds
Next Scheduled Check:	09-23-2025 14:03:04
Last State Change:	N/A
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	09-23-2025 13:03:05 (0d 0h 0m 1s ago)

Jobs found above min runtime.

Parameters:

Subsystem	Subsystem of jobs requested.
Minimum RunTime	Min value returned for runtime of jobs.
Job Type	Filter for job type. Job types available are: A – Autostart job B – Batch job I – Interactive job M – Subsystem monitor job R – Spooled reader job S – System job W – Spooled writer job X – start-control-program-function system job
Critical Qty	Critical range for the number of jobs returned.
Warning Qty	Warning range for the number of jobs returned.
Critical RunTime	Critical range for the runtime of each job returned.
Warning RunTime	Warning range for the runtime of each job returned.

The following will be returned:

No messages with severity %d or above found in last %d min.

Security Check Commands

check_Security_ADMUSRS

Returns all user profiles with *SECADM/*ALLOBJ/*AUDIT authorities.

Service State Information

Current Status:	WARNING (for 0d 0h 11m 35s)
Status Information:	WARNING-9 profiles found with *SECADM,*ALLOBJ,*AUDIT: [REDACTED] QSECOFR QSYS [REDACTED]
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	11-11-2025 09:11:03
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.026 seconds
Next Scheduled Check:	11-12-2025 09:11:03
Last State Change:	11-11-2025 09:07:16
Last Notification:	11-11-2025 09:07:16 (notification 1)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	11-11-2025 09:18:41 (0d 0h 0m 10s ago)

Admin user profiles

Parameters:

Critical Count

Critical range for the number of Admin Users found.

Warning Count

Warning range for the number of Admin Users found.

The following is returned:

[State]-[Count] profiles found with *SECADM,*ALLOBJ,*AUDIT:
[List of users returned]

check_Security_IDSSTS

Returns current status of Intrusion Detection System monitoring.

Service State Information

Current Status:	OK (for 0d 0h 20m 25s)
Status Information:	IDS Status: Active
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	11-11-2025 09:11:39
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.019 seconds
Next Scheduled Check:	11-11-2025 10:11:39
Last State Change:	11-11-2025 09:09:05
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	11-11-2025 09:29:21 (0d 0h 0m 9s ago)

Admin user profiles

Parameters:

Comparison Value Value to compare current status against.
Severity Severity of notification if comparison does not match.

The following is returned:
IDS Status: [Status]

check_Security_AUDJEAF

Returns Authority Failure journal entries found in last (n)min.

Service State Information

Current Status:	OK (for 0d 0h 22m 51s)
Status Information:	No Authority Failure entries found in last 45min.
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	11-11-2025 09:11:12
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.021 seconds
Next Scheduled Check:	11-11-2025 09:41:12
Last State Change:	11-11-2025 09:07:35
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	11-11-2025 09:30:22 (0d 0h 0m 4s ago)

Authority Failure Entries

Parameters:

Minutes	Number of Minutes to look back for journal entries.
Critical Count	Critical range for the number of AF journal entries found.
Warning Count	Warning range for the number of AF journal entries found.

The following is returned:

No Authority Failure entries found in last [Minutes]min.

OR

[Count] Authority Failure entries found in last [Minutes]min:

Sequence Number:

Violation Type:

Object Name:

Job Name:

Job Number:

Program Name:

{Repeated for each AF Journal Entry found.}

check_Security_AUDJEAD

Returns Auditing Change entries found in last (n)min.

Service State Information

Current Status:	WARNING (for 0d 0h 18m 56s)
Status Information:	WARNING-8 Auditing Change entries found in last 45min: Sequence Number: 47257 Violation Type: O Audit Value: *NONE Object Name: ADDEPNT1 CHLIB *PGM Sequence Number: 47258 Violation Type: O Audit Value: *CHANGE Object Name: ADDEPNT1 CHLIB *PGM Sequence Number: 47259 Violation Type: O Audit Value: *NONE Object Name: ADDEPNT2 CHLIB *PGM Sequence Number: 47260 Violation Type: O Audit Value: *CHANGE Object Name: ADDEPNT2 CHLIB *PGM Sequence Number: 47261 Violation Type: O Audit Value: *NONE Object Name: ADDJQNTNP CHLIB *PGM Sequence Number: 47262 Violation Type: O Audit Value: *CHANGE Object Name: ADDJQNTNP CHLIB *PGM Sequence Number: 47263 Violation Type: O Audit Value: *CHANGE IFS Path: /home/iftstest Sequence Number: 47264/iftstest Violation Type: O Audit Value: *NONE IFS Path: /home/iftstest

Auditing Change Entries

Parameters:

Minutes	Number of Minutes to look back for journal entries.
Critical Count	Critical range for the number of AD journal entries found.
Warning Count	Warning range for the number of AD journal entries found.

The following is returned:

No Auditing Change entries found in last [Minutes]min.

OR

[Count] Auditing Change entries found in last [Minutes]min:

Sequence Number:

Violation Type:

Audit Value:

Depending on DLO / IFS / OBJ

DLO Name:

Folder Path:

OR

IFS Path:

OR

Object Name:

{Repeated for each AD Journal Entry found}

check_Security_AUDJECA

Returns Authority Change entries found in last (n)min.

Service State Information

Current Status:	CRITICAL (for 0d 0h 20m 34s)
Status Information:	CRITICAL-12 Authority Change entries found in last 45min: Sequence Number: 47265 Entry Type: A Command Type: RPL User Name: *PUBLIC Object Authorities: Y Y Y Auth List Name: Object Name: OBJ Sequence Number: 47266 Entry Type: A Command Type: RPL User Name: *PUBLIC Object Authorities: Y Y Y Auth List Name: Object Name: OBJ Sequence Number: 47267 Entry Type: A Command Type: RPL User Name: *PUBLIC Object Authorities: Y Y Y Auth List Name: Object Name: OBJ Sequence Number: 47268 Entry Type: A Command Type: RPL User Name: *PUBLIC Object Authorities: Y Auth List Name: Object Name: OBJ

Authority Change Entries

Parameters:

Minutes	Number of Minutes to look back for journal entries.
Critical Count	Critical range for the number of CA journal entries found.
Warning Count	Warning range for the number of CA journal entries found.

The following is returned:

No Authority Change entries found in last [Minutes]min.

OR

[Count] Authority Change entries found in last [Minutes]min:

Sequence Number:

Entry Type:

Command Type:

Username:

Object Authorities:

Auth List Name:

Depending on DLO / IFS / OBJ

DLO Name:

Folder Path:

OR

IFS Path:

OR

Object Name:

{Repeated for each CA Journal Entry found}

check_Security_AUDJECF

Returns Profile Change entries found in last (n)min.

Service State Information

Current Status:	WARNING (for 0d 0h 21m 1s)
Status Information:	WARNING-8 Profile Change entries found in last 45min: Sequence Numer: 47277 Entry Type: A User Profile: TESTUSR Password Changed: Password Expired: User Class: Profile Status: *DISABLED Initial Program: Initial Menu: All Object: Previous All Object: Sequence Numer: 47279 Entry Type: A User Profile: TESTUSR Password Changed: Password Expired: User Class: Profile Status: *ENABLED Initial Program: Initial Menu: All Object: Previous All Object: Sequence Numer: 47281 Entry Type: A User Profile: TESTUSR Password Changed: Password Expired: User Class: *SYSOPR Profile Status: Initial Program: Initial Menu: All Object: Previous All Object:

Profile Change Entries

Parameters:

Minutes	Number of Minutes to look back for journal entries.
Critical Count	Critical range for the number of CP journal entries found.
Warning Count	Warning range for the number of CP journal entries found.

The following is returned:

No Profile Change entries found in last [Minutes]min.

OR

[Count] Profile Change entries found in last [Minutes]min:

Sequence Numer:
Entry Type:
User Profile:
Password Changed:
Password Expired:
User Class:
Profile Status:
Initial Program:
Initial Menu:
All Object:
Previous All Object:
{Repeated for each CP Journal Entry found}

check_Security_AUDJEM

Returns Intrusion Monitor entries found in last (n)min.

Service State Information

Current Status:	OK (for 0d 0h 24m 24s)
Status Information:	No Intrusion Monitor entries found in last 45min.
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	11-11-2025 09:11:23
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.021 seconds
Next Scheduled Check:	11-11-2025 09:41:23
Last State Change:	11-11-2025 09:08:06
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	11-11-2025 09:32:21 (0d 0h 0m 9s ago)

IM Journal Entries

Parameters:

Minutes	Number of Minutes to look back for journal entries.
Critical Count	Critical range for the number of IM journal entries found.
Warning Count	Warning range for the number of IM journal entries found.

The following is returned:

No Intrusion Monitor entries found in last [Minutes]min.

OR

[Count] Intrusion Monitor entries found in last [Minutes]min:

Sequence Numer:

Entry Type:

Time Stamp:

Detection Point ID:

Probe Type:

Local IP Address:

Local Port:

Remote IP Address:

Remote Port:

{Repeated for each IM Journal Entry found}

check_Security_AUDJEPW

Returns Password entries found in last (n)min.

Service State Information

Current Status:	WARNING (for 0d 0h 21m 7s)
Status Information:	WARNING-1 Password entries found in last 45min: Sequence Numer: 47295 Violation Entry Type: C Username: CHIRD Device Name: QPADEV0003
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	11-11-2025 09:11:27
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.021 seconds
Next Scheduled Check:	11-11-2025 09:41:27
Last State Change:	11-11-2025 09:11:27
Last Notification:	11-11-2025 09:11:27 (notification 1)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	11-11-2025 09:32:31 (0d 0h 0m 3s ago)

Password Entries Found

Parameters:

Minutes Number of Minutes to look back for journal entries.
Critical Count Critical range for the number of PW journal entries found.
Warning Count Warning range for the number of PW journal entries found.

The following is returned:

No Password entries found in last [Minutes]min.

OR

[Count] Password entries found in last [Minutes]min:

Sequence Numer:

Violation Entry Type:

Username:

Device Name:

{Repeated for each PW Journal Entry found}

check_Security_AUDJVP

Returns Network entries found in last (n)min.

Service State Information

Current Status:	OK (for 0d 0h 23m 52s)
Status Information:	No Network entries found in last 45min.
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	11-11-2025 09:11:30
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.017 seconds
Next Scheduled Check:	11-11-2025 09:41:30
Last State Change:	11-11-2025 09:08:36
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	11-11-2025 09:32:21 (0d 0h 0m 7s ago)

Network Journal Entries

Parameters:

Minutes	Number of Minutes to look back for journal entries.
Critical Count	Critical range for the number of VP journal entries found.
Warning Count	Warning range for the number of VP journal entries found.

The following is returned:

No Network entries found in last [Minutes]min.

OR

[Count] Network entries found in last [Minutes]min:

Sequence Numer:

Error Type:

Server Name:

Server Date:

Server Time:

Long Computer Name:

Username:

{Repeated for each VP Journal Entry found}

check_Security_AUDJEX0

Returns Network Authentication entries found in last (n)min.

Service State Information

Current Status:	OK (for 0d 0h 25m 15s)
Status Information:	No Network Authentication entries found in last 45min.
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	11-11-2025 09:11:35
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.020 seconds
Next Scheduled Check:	11-11-2025 09:41:35
Last State Change:	11-11-2025 09:08:48
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	11-11-2025 09:34:01 (0d 0h 0m 2s ago)

Network Authentication Entries

Parameters:

Minutes	Number of Minutes to look back for journal entries.
Critical Count	Critical range for the number of X0 journal entries found.
Warning Count	Warning range for the number of X0 journal entries found.

The following is returned:

No Network Authentication entries found in last [Minutes]min.

OR

[Count] Network Authentication entries found in last [Minutes]min:

Sequence Number:

Entry Type:

Local IP Address:

Remote IP Address:

{Repeated for each X0 Journal Entry found}

HMC Check Commands

check_HMC_MSYSICON

Retrieves Managed systems connection status.

Service State Information

Current Status:	OK (for 1d 0h 38m 48s)
Status Information:	8286-41A*218FFEW: Connected 9009-41A*78AC2B0: Connected 9105-41B*78713D1: Connected
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	11-15-2023 16:34:02
Check Type:	ACTIVE
Check Latency / Duration:	0.557 / 0.000 seconds
Next Scheduled Check:	11-15-2023 17:34:02
Last State Change:	11-14-2023 16:12:21
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	11-15-2023 16:51:02 (0d 0h 0m 7s ago)

Managed system connection status'

Parameters:

Severity

Severity of alert to be returned if managed system is not connected.

For each of the managed systems the connection status is returned.

check_HMC_MEMSTS

Retrieves HMC memory status.

Service State Information

Current Status:	OK (for 1d 0h 54m 11s)
Status Information:	Memory usage: 0% Memory total: 32918780KiB Memory free: 11377540KiB Memory used: 7798136KiB Memory buff/cache: 13743104KiB
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	11-15-2023 17:04:04
Check Type:	ACTIVE
Check Latency / Duration:	0.217 / 0.224 seconds
Next Scheduled Check:	11-15-2023 17:19:04
Last State Change:	11-14-2023 16:12:21
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	11-15-2023 17:06:23 (0d 0h 0m 9s ago)

HMC Memory Status

Parameters:

Usage Critical Range Range for memory usage percentage which will return a critical alert.
Usage Warning Range Range for memory usage percentage which will return a warning alert.

The Following will be returned:

Memory usage Percentage of memory used.
Memory Total Total amount of memory .
Memory Free Amount of Free memory returned in KiB.
Memory Used Amount of Used memory returned in KiB.
Memory buff/cache Memory buffer/cache returned in KiB.

check_HMC_SRVEVNT

Retrieves Service events logged for a Managed System.

Service State Information	
Current Status:	OK (for 0d 0h 5m 38s)
Status Information:	9009-41A*78AC2B0 Service Events: No results were found.
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	11-17-2023 13:24:21
Check Type:	ACTIVE
Check Latency / Duration:	1.377 / 0.287 seconds
Next Scheduled Check:	11-18-2023 13:24:27
Last State Change:	11-17-2023 13:24:21
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	11-17-2023 13:29:56 (0d 0h 0m 3s ago)

Service Events

Parameters:

Managed System	Managed System to check.
Status[Open/Closed]	Status of Service events to return.
Days to look back	Number of days to look back for service events.

The Following will be returned:

System name: No results were found.

OR

Individual read out for each service event.

check_HMC_SYSLED

Retrieves LED status of a Managed System.

Service State Information	
Current Status:	OK (for 0d 0h 16m 12s)
Status Information:	9009-41A*78AC2B0 LED Status: off
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	11-17-2023 13:39:27
Check Type:	ACTIVE
Check Latency / Duration:	0.386 / 0.000 seconds
Next Scheduled Check:	11-17-2023 13:54:27
Last State Change:	11-17-2023 13:24:21
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	11-17-2023 13:40:26 (0d 0h 0m 7s ago)

Managed System LED Status

Parameters:

Managed System	Managed System to check.
Severity	Severity if the LED is on.

The Following will be returned:

System name: "LED status".

`check_HMC_PARTLED`

Retrieves LED status of a Partition under a Managed System.

Service State Information

Current Status:	OK (for 0d 0h 16m 12s)
Status Information:	9009-41A*78AC2B0 LED Status: off
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	11-17-2023 13:39:27
Check Type:	ACTIVE
Check Latency / Duration:	0.386 / 0.000 seconds
Next Scheduled Check:	11-17-2023 13:54:27
Last State Change:	11-17-2023 13:24:21
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	11-17-2023 13:40:26 (0d 0h 0m 7s ago)

Partition LED Status

Parameters:

Managed System Managed System where the partition exists.
Partition Partition to check.
Severity Severity if the LED is on.

**NOTE: “*ALL” may be passed as the Partition parameter. This will check all LPARs on the system for the LED status ‘on’.*

The Following will be returned:

Partition name: “LED status”.

check_HMC_MAINTEXP

Retrieves hardware maintenance expiry date for a Managed System.

Service State Information	
Current Status:	CRITICAL (for 0d 0h 20m 37s)
Status Information:	CRITICAL-9009-41A*78AC2B0 Hardware maintenance has expired. Expiry date: 08/09/2023
Performance Data:	
Current Attempt:	2/2 (HARD state)
Last Check Time:	11-17-2023 13:24:22
Check Type:	ACTIVE
Check Latency / Duration:	2.462 / 1.055 seconds
Next Scheduled Check:	11-18-2023 13:24:26
Last State Change:	11-17-2023 13:24:22
Last Notification:	11-17-2023 13:24:26 (notification 2)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	11-17-2023 13:44:56 (0d 0h 0m 3s ago)

Hardware Expiry Date

Parameters:

Managed System	Managed System to be checked.
Date Format	Date format of HMC [DMY/MDY]
Critical Days	Range for number of days until expiry, returns critical alert.
Warning Days	Range for number of days until expiry, returns warning alert.

The Following will be returned:

System name: Maintenance has expired.
OR
System name: days until maintenance expiry: [days]
Expiry Date

check_HMC_PARTSTS

Retrieves running status of Partition and the OS.

Service State Information

Current Status:	OK (for 0d 0h 26m 20s)
Status Information:	SAS902 State: Running OS: os400
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	11-17-2023 13:39:26
Check Type:	ACTIVE
Check Latency / Duration:	0.807 / 0.000 seconds
Next Scheduled Check:	11-17-2023 13:54:26
Last State Change:	11-17-2023 13:24:21
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	11-17-2023 13:50:37 (0d 0h 0m 4s ago)

Partition Status

Parameters:

Managed System Managed System where the partition exists.
Partition Partition to check.

The Following will be returned:

Partition name: partition status.
OS: partition operating system.

check_HMC_UPD

Retrieves updates available for HMC.

Service State Information

Current Status:	WARNING (for 0d 0h 37m 50s)
Status Information:	WARNING-There are updates available. PTF: vMF71298 Type: ifix Date: 2023/9/28 PTF: vMF71190 Type: sp Date: 2023/8/16 PTF: vMF71106 Type: ifix Date: 2023/6/15
Performance Data:	
Current Attempt:	2/2 (HARD state)
Last Check Time:	11-17-2023 13:24:20
Check Type:	ACTIVE
Check Latency / Duration:	0.735 / 2.699 seconds
Next Scheduled Check:	11-18-2023 13:24:20
Last State Change:	11-17-2023 13:17:30
Last Notification:	11-17-2023 13:17:40 (notification 1)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	11-17-2023 13:55:16 (0d 0h 0m 4s ago)

Partition Status

Parameters:

Severity Severity of alert if updates are available.

The Following will be returned for each available update:

- PTF: Available PTF.
- Type: Type of PTF.
- Date: PTF release date.

check_HMC_MIGSTS

Returns Migration status of a partition.

Service State Information

Current Status:	OK (for 0d 0h 36m 34s)
Status Information:	SAS902 Migration Status: Not Migrating
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	11-17-2023 13:24:22
Check Type:	ACTIVE
Check Latency / Duration:	2.187 / 0.275 seconds
Next Scheduled Check:	11-17-2023 14:24:26
Last State Change:	11-17-2023 13:24:22
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	11-17-2023 14:00:46 (0d 0h 0m 10s ago)

Migration Status

Parameters:

Managed System Managed System where the partition exists.
Partition Partition to check.

The Following will be returned:

Partition name Migration Status: migration status.

check_HMC_LOGINS

Returns Number of HMC login sessions and details for each login.

Service State Information

Current Status:	CRITICAL (for 0d 0h 50m 34s)
Status Information:	CRITICAL-Current webui logins: 20 Username: chird Session ID: 119797 Logon Time: 10/27/2023 17:20:37 Logon Mode: Enhanced+
	Username: chris Session ID: 120014 Logon Time: 10/27/2023 18:47:21 Logon Mode: Rest API
	Username: chris Session ID: 120020 Logon Time: 10/27/2023 18:51:56 Logon Mode: Rest API
	Username: chris Session ID: 120047 Logon Time: 10/27/2023 18:57:00 Logon Mode: Rest API

HMC Logins

Parameters:

Type [ssh/webui]	Type of Logins to return. Either SSH or WEBUI.
Critical Count	Critical range for the number of logins returned.
Warning Count	Warning range for the number of logins returned.

The Following will be returned for each login session:

- Username: Username of session.
- Session ID: Session ID of session
- Logon Time: Time user logged in.
- Logon Mode: Mode of session.

check_HMC_FSSIZE

Returns File System size and percentage of available space.

Service State Information

Current Status:	OK (for 0d 1h 2m 54s)
Status Information:	File System Sizes: File System: /var Available space: 82% Total space: 5829 Free space: 4757 File System: /var/hsc/log WARNING-Available space: 15% Total space: 5959 Free space: 913 File System: /dump Available space: 87% Total space: 30065 Free space: 26015 File System: /extra Available space: 50% Total space: 19986 Free space: 9959 File System: /data Available space: 70% Total space: 40141 Free space: 28047 File System: / Available space: 49% Total space: 15645 Free space: 7638
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	11-17-2023 13:24:22
Check Type:	ACTIVE
Check Latency / Duration:	2.832 / 0.542 seconds
Next Scheduled Check:	11-17-2023 15:24:22
Last State Change:	11-17-2023 13:15:24
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	11-17-2023 14:18:16 (0d 0h 0m 2s ago)

HMC Logins

Parameters:

Critical Available Space Critical range for the percentage of available space.

Warning Available Space Warning range for the percentage of available space.

The Following will be returned for each File System:

File System: File System path

Available space: Returned in %

Total space: Total space of file system.

Free space: Total free space of file system.

check_HMC_CERT

Returns information on the HMC Certificate.

Service State Information

Current Status:	OK (for 0d 1h 24m 37s)
Status Information:	Cert Expires in: 888 days. Cert Type: self-signed Date Created: May 27, 2019, 3:41:08 PM Expiry Date: Apr 23, 2026, 3:41:08 PM
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	11-17-2023 13:24:23
Check Type:	ACTIVE
Check Latency / Duration:	3.431 / 0.000 seconds
Next Scheduled Check:	11-18-2023 13:24:23
Last State Change:	11-17-2023 13:15:24
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	11-17-2023 14:39:56 (0d 0h 0m 5s ago)

HMC Certificate Expiry

Parameters:

Critical Days

Critical range for the number of days until Certificate expiry.

Warning Days

Warning range for the number of days until Certificate expiry.

The Following will be returned:

Cert Expires in: Number of days until Certificate expiry.

Cert Type: Certificate Type.

Date Created: Date Certificate was created.

Expiry Date: Date Certificate expires.

check_HMC_SYSSRC

Returns Managed System SRC code.

Service State Information

Current Status:	OK (for 0d 1h 21m 37s)
Status Information:	9009-41A*78AC2B0 SRC code: 00000000
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	11-17-2023 14:39:27
Check Type:	ACTIVE
Check Latency / Duration:	0.964 / 0.000 seconds
Next Scheduled Check:	11-17-2023 14:54:27
Last State Change:	11-17-2023 13:24:20
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	11-17-2023 14:45:56 (0d 0h 0m 1s ago)

Managed System SRC Code

Parameters:

Managed System	Managed system to be checked.
Severity	Severity of alert if SRC code is not '00000000'.

The Following will be returned:
Managed System SRC code: SRC code.

check_HMC_PARTSRC

Returns Partition SRC code.

Service State Information

Current Status:	OK (for 0d 1h 26m 57s)
Status Information:	SAS902 SRC code: 00000000
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	11-17-2023 14:39:26
Check Type:	ACTIVE
Check Latency / Duration:	0.283 / 0.004 seconds
Next Scheduled Check:	11-17-2023 14:54:26
Last State Change:	11-17-2023 13:24:21
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	11-17-2023 14:51:16 (0d 0h 0m 2s ago)

Partition SRC Code

Parameters:

Managed System	Managed system where the Partition exists.
Partition	Partition to be checked.
Comparison	Comparison value to check against SRC code.
Severity	Severity of alert if SRC code does not match comparison value.

The Following will be returned:
Partition SRC code: SRC code.

BRMS Check Commands

check_BRMS_WERR

Returns number of Write errors from BRMS.

Parameters:

Serial	The volume serial which BRMS uses to identify the volume.
Critical Errors	Critical alert range for the number of Write Errors.
Warning Errors	Warning alert range for the number of Write Errors.

The following will be returned:

Write errors: 5

check_BRMS_RERR

Returns number of Read errors from BRMS.

Parameters:

Serial	The volume serial which BRMS uses to identify the volume.
Critical Errors	Critical alert range for the number of Read Errors.
Warning Errors	Warning alert range for the number of Read Errors.

The following will be returned:

Read errors: 5

check_BRMS_FULL

Returns details on if a volume is full.

Parameters:

Serial	The volume serial which BRMS uses to identify the volume.
Severity	Severity of alert to return if volume is full.

The following will be returned:

CRITICAL- Volume is FULL.

OR

Volume is not FULL.

check_BRMS_USED

Returns number of times a volume is used.

Parameters:

Serial	The volume serial which BRMS uses to identify the volume.
Critical Times Used	Critical alert range for the number of times a volume is used.
Warning Times Used	Warning alert range for the number of times a volume is used.

The following will be returned:

Number times volume used: 5

check_BRMS_EXPD

Returns status of expiry date set for volume.

Parameters:

Serial The volume serial which BRMS uses to identify the volume.

The following will be returned:

Volume's expiry date has been set.

OR

Volume has permanent retention status.

OR

Volume is using version expiration.

OR

Volume expiry status is unknown.

check_BRMS_DUPD

Returns duplication status for media.

Parameters:

Serial The volume serial which BRMS uses to identify the volume.

The following will be returned:

No duplication status is set.

OR

Media has been duplicated and is also marked for duplication.

OR

Media has been duplicated.

OR

Media is marked for duplication.

OR

Duplication status is unknown:

check_BRMS_EDAT

Returns days until volume expires.

Parameters:

Serial The volume serial which BRMS uses to identify the volume.

Critical Days to Expiry Critical alert range for the number of days until volume expires.

Warning Days to Expiry Warning alert range for the number of days until volume expires.

The following will be returned:

Volume has expired:

OR

Volume expires in: 10 days

check_BRMS_STS

Returns BRMS backup status for control group.

Parameters:

Control Group	The name of the Control Group that was backed up.
Date	Date of the Backup.
System	The name of the system where the backup was performed.
Critical Objects Not Saved	Critical alert range for the number of objects not saved.
Warning Objects Not Saved	Warning alert range for the number of objects not saved.

The following will be returned:

BRMS Status for: [Control group]

Job:

Save Status:

Backup Min:

Objects Saved:

Objects Not Saved:

FT4i Check Commands

check_FT4i_LOG

Retrieves records from FT4i FTP log, matching passed in ALWFLAG and number of min.

Service State Information	
Current Status:	OK (for 0d 0h 0m 10s)
Status Information:	FT4i Record(s) found: 3-Password Error
Performance Data:	
Current Attempt:	1/2 (HARD state)
Last Check Time:	05-14-2024 13:55:58
Check Type:	ACTIVE
Check Latency / Duration:	1.539 / 0.022 seconds
Next Scheduled Check:	05-14-2024 14:56:04
Last State Change:	05-14-2024 13:55:58
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	05-14-2024 13:56:04 (0d 0h 0m 4s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	DISABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

FTP log entries matching 11 ALWFLAG (Password errors)

Parameters:

ALWFLAG	Allow flag to be searched for in FT4i log.
Minutes	Number of min to search back from current time.
Critical Records	Critical range for number of records returned.
Warning Records	Warning range for number of records returned.

Returns the following information.

FT4i Records found: [Records] Number of records found with ALWFLAG.

Accepted ALWFLAGs:

-1	Check Messages Log
0	Config setting
1	Accepted
2	Reject * No Accept Match
3	Matched Reject Entry
4	No Accept or Reject Match
5	Matched Accept and Reject
6	No Profile match found
7	Profile not allowed to start session
8	Outside of allowed time band
9	Profile IP mismatch
10	Analysis only
11	Password Error
12	Profile Disabled

VIOS Check Commands **BETA Release**

`check_VIOS_OSLVL`

Retrieves the VIOS OS level.

Service State Information	
Current Status:	OK (for 0d 0h 26m 24s+)
Status Information:	VIOS OS Level: 3.1.4.50
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	01-06-2025 13:27:52
Check Type:	ACTIVE
Check Latency / Duration:	1.973 / 0.359 seconds
Next Scheduled Check:	01-13-2025 12:06:52
Last State Change:	N/A
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	01-06-2025 13:51:15 (0d 0h 0m 5s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Current VIOS OS level

Returns the following information.

VIOS OS Level: [Current level]

check_VIOS_SEASTAT

Retrieves status of a Shared Ethernet Adapter. This check is still in development... It currently only returns an error message if accounting is disabled on an SEA device.

Service State Information

Current Status:	CRITICAL (for 0d 0h 53m 50s) (Has been acknowledged)
Status Information:	SEA Error: Device ent5 has accounting disabled
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	01-06-2025 13:58:03
Check Type:	ACTIVE
Check Latency / Duration:	4.724 / 0.447 seconds
Next Scheduled Check:	01-06-2025 14:58:09
Last State Change:	01-06-2025 13:58:03
Last Notification:	01-06-2025 13:58:09 (notification 1)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	01-06-2025 14:51:45 (0d 0h 0m 8s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

ENT5 SEA Status

Parameters:

SEA Device Shared Ethernet Adapter device name.
Severity Severity if Error is returned.

Returns the following information.

SEA Status: [Current Status]

check_VIOS_USRSTS

Retrieves status of a requested VIOS username, including the roles assigned to a user, the numbers of failed logins and if the user is currently locked.

Service State Information

Current Status:	OK (for 0d 19h 27m 56s+)
Status Information:	padmin Roles: PAdmin,CacheAdm padmin is not locked. padmin login retries: 0
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	01-06-2025 13:28:14
Check Type:	ACTIVE
Check Latency / Duration:	1.663 / 0.284 seconds
Next Scheduled Check:	01-07-2025 13:28:14
Last State Change:	N/A
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	01-07-2025 09:31:25 (0d 0h 0m 7s ago)

User padmin Status

Parameters:

Username	User account to be retrieved.
Critical Retries	Critical range for number of failed logins.
Warning Retries	Warning range for number of failed logins.
Severity	Severity the user account is locked.

Returns the following information.

- [user] Roles: [Roles assigned to user]
- [user] is locked / not locked.
- [user] login retries: [Number of failed logins]

check_VIOS_ERRLOG

Retrieves number of errors logged in the last X hours. This can be filtered down to a single device or use *ALL to return errors across all devices.

Service State Information

Current Status:	OK (for 0d 20h 31m 7s)
Status Information:	No Errors Logged in last 60 hours.
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	01-07-2025 09:57:09
Check Type:	ACTIVE
Check Latency / Duration:	0.270 / 0.000 seconds
Next Scheduled Check:	01-07-2025 10:12:09
Last State Change:	01-06-2025 13:27:07
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	01-07-2025 09:58:06 (0d 0h 0m 8s ago)

Number of errors logged in last 60 hours

Parameters:

Hours	Number of hours to search back through log.
Device	Device filter, use *ALL to retrieve all.
Critical Count	Critical range for number of errors logged within window.
Warning Count	Warning range for number of errors logged within window.

Returns the following information.

Error Count: [Number of errors logged within window]

Log Entries: [List of errors logged]

check_VIOS_ENTSTATUS

Retrieves a comparison value for requested ENT device. This check allows you to check individual statuses on a given ENT device by comparing to the value you pass in.

Service State Information

Current Status:	OK (for 0d 20h 6m 20s)
Status Information:	ent5 High Availability Mode: Auto Comparison: 'Auto' / 'Auto'
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	01-07-2025 10:03:56
Check Type:	ACTIVE
Check Latency / Duration:	0.921 / 0.000 seconds
Next Scheduled Check:	01-07-2025 11:03:56
Last State Change:	01-06-2025 14:03:48
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	01-07-2025 10:10:06 (0d 0h 0m 2s ago)

High Availability Mode for ent5

Parameters:

ENT Device	ENT device name.
Filter	Status detail to check against.
Comparison	Comparison value to check against filter.
Severity	Severity of alert to be returned if returned value does not match the comparison value.

Returns the following information.

[Device] [Filter]: [Returned value]
Comparison: '[Comparison]' / '[Returned Value]'

check_VIOS_DEVSTATUS

Retrieves device status for given device.

Service State Information

Current Status:	OK (for 0d 21h 28m 31s)
Status Information:	Device: ent4 Status: Available Description: Virtual I/O Ethernet Adapter (I-Han)
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	01-07-2025 10:25:06
Check Type:	ACTIVE
Check Latency / Duration:	0.977 / 0.000 seconds
Next Scheduled Check:	01-07-2025 11:25:06
Last State Change:	01-06-2025 13:25:05
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	01-07-2025 10:53:35 (0d 0h 0m 1s ago)

Ent4 Device Status

Parameters:

ENT Device ENT device name.
Severity Severity of alert to be returned if Status != Available or Defined

Returns the following information.

Device: [Device Name]
Status: [Status of device]
Description: [Device Description]

check_VIOS_PVSIZE

Retrieves physical volume size for VIOS partition.

Service State Information

Current Status:	OK (for 0d 20h 56m 12s+)
Status Information:	Physical Volume: hdisk1 PVID: 00c713d13c8a7d98 SIZE(MB): 102400
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	01-06-2025 13:28:01
Check Type:	ACTIVE
Check Latency / Duration:	1.517 / 0.442 seconds
Next Scheduled Check:	01-07-2025 13:28:01
Last State Change:	N/A
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	01-07-2025 10:59:45 (0d 0h 0m 3s ago)

Physical Volume Size

Parameters:

No Parameters for this check.

Returns the following information.

Physical Volume: [Volume Name]

PVID: [Volume ID]

SIZE(MB): [Volume Size]

check_VIOS_FLOGINS

Retrieves the number of failed logins logged on system.

Current Status:	WARNING (for 0d 21h 59m 47s) (Has been acknowledged)
Status Information:	User: root Date: Tue Jul 11 15:08:57 CDT 2023
	User: UNKNOWN_ Date: Tue Jul 11 15:11:02 CDT 2023
	User: root Date: Fri Dec 6 09:36:31 CST 2024
	User: UNKNOWN_ Date: Wed Dec 11 12:46:36 CST 2024
	User: UNKNOWN_ Date: Wed Dec 11 12:46:50 CST 2024
	User: UNKNOWN_ Date: Wed Dec 11 12:46:58 CST 2024
	WARNING-Number of Failed Logins: 6
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	01-07-2025 10:27:26
Check Type:	ACTIVE
Check Latency / Duration:	0.977 / 0.000 seconds
Next Scheduled Check:	01-07-2025 11:27:26
Last State Change:	01-06-2025 13:27:15
Last Notification:	01-06-2025 13:27:26 (notification 1)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	01-07-2025 11:26:55 (0d 0h 0m 7s ago)

Failed logins for VIOS partition

Parameters:

- Critical Failed Logins Critical range for number of failed logins.
- Warning Failed Logins Warning range for number of failed logins.

Returns the following information.

[Alert Value]-Number of Failed Logins: [Count of failed logins]

User & Date of each failed login.

check_VIOS_VMSTATUS

Retrieves Memory and CPU status for the VIOS partition. This check is still in development, currently there are no alerts or ranges processed by the check.

Service State Information

Current Status:	OK (for 0d 22h 8m 35s)
Status Information:	Logical CPU: 16 Memory: 4096MB Allocated CPU: 0.50 Available Memory: 531986 Free Memory: 421733
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	01-07-2025 11:28:22
Check Type:	ACTIVE
Check Latency / Duration:	0.155 / 0.199 seconds
Next Scheduled Check:	01-07-2025 12:28:22
Last State Change:	01-06-2025 13:28:21
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	01-07-2025 11:36:55 (0d 0h 0m 1s ago)

VM stats for VIOS

Parameters:

There are no Parameters for this check.

Returns the following information.

Logical CPU: [CPU count]
Memory: [Memory in MB]
Allocated CPU: [Allocated CPU]
Available Memory: [Available memory in bytes]
Free Memory: [Free memory in bytes]

check_VIOS_FMWRLVL

Retrieves microcode and firmware levels of the system, adapters, and devices.

Service State Information

Current Status:	OK (for 0d 21h 39m 21s+)
Status Information:	sys0 Firmware: ML1030_060 (t) ML1030_060 (p) ML1030_060 (t)
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	01-06-2025 13:27:28
Check Type:	ACTIVE
Check Latency / Duration:	1.550 / 0.793 seconds
Next Scheduled Check:	01-13-2025 12:06:28
Last State Change:	N/A
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	01-07-2025 11:42:56 (0d 0h 0m 1s ago)

sys0 Firmware Level

Parameters:

Device Device, system or adapter name to be checked.

Returns the following information.

[Device] Firmware: [Firmware level]

check_VIOS_LPARINFO

Retrieves LPAR ID and Name for VIOS partition.

Service State Information

Current Status:	OK (for 0d 21h 42m 42s+)
Status Information:	LPAR ID: 1 LPAR Name: VIOS_p10_1
Performance Data:	
Current Attempt:	1/1 (HARD state)
Last Check Time:	01-06-2025 13:27:43
Check Type:	ACTIVE
Check Latency / Duration:	1.812 / 0.315 seconds
Next Scheduled Check:	01-13-2025 12:06:43
Last State Change:	N/A
Last Notification:	N/A (notification 0)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	01-07-2025 11:46:15 (0d 0h 0m 3s ago)

VIOS LPAR Info

Parameters:

No parameters for this check.

Returns the following information.

LPAR ID: [LPAR number]

LPAR Name: [VIOS LPAR name]

Mimix Check Commands

`check_MMX_DBSND`

Retrieves elements of the old DB send processes that were used prior to the remote journaling capability that has been added to MiMiX.

Service State Information

Current Status:	OK (for 1d 22h 15m 0s)
Status Information:	Data Group State:*ENABLED Database Apply Threads:*NONE Transfer Definition Status:*ACTIVE Database Apply Process:1 Database Reader Process:*ACTIVE Database Send Backlog:0
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	07-26-2022 13:06:35
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 1.956 seconds
Next Scheduled Check:	07-27-2022 13:06:35
Last State Change:	07-25-2022 13:01:33
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	07-27-2022 11:16:26 (0d 0h 0m 7s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

DBSND returned info

Parameters:

Mimix Library	Mimix install library.
Datagroup Name	Name of the data group configured in Mimix.
System 1	System number 1.
System 2	System number 2.

Returns the following information.

Data Group State Message	The status of the data group definition.
Database Apply Threads	Threaded apply status.
Transfer Definition Status	Transfer definition status.
Database Apply Process	Number of active apply processes.
Database Reader Process	Status of the DB reader process.
Database Send Backlog	Size of the DB send backlog.

check_MMx_SWSTS

Returns the switch status for the requested Data Group definition.

Service State Information

Current Status:	OK (for 1d 22h 50m 24s)
Status Information:	Data Group State:*ENABLED Data Source:*SYS1 Switch Status Sys1:*NONE Switch Status Sys2:*NONE Virtual Roleswap Status:*NONE
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	07-26-2022 13:06:35
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 2.128 seconds
Next Scheduled Check:	07-27-2022 13:06:35
Last State Change:	07-25-2022 13:01:33
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	07-27-2022 11:51:56 (0d 0h 0m 1s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

SWSTS returned info

Parameters:

Mimix Library	Mimix install library.
Datagroup Name	Name of the data group configured in Mimix.
System 1	System number 1.
System 2	System number 2.

Returns the following information.

Data Group State	The status of the data group definition.
Data Source	System that is configured to be the production system.
Switch Status Sys1	Status of the switch on System 1.
Switch Status Sys2	Status of the switch on system 2.
Virtual Roleswap Status	Virtual roleswap status.

check_MMx_RJLNK

Returns the status of the remote journal link.

Service State Information

Current Status:	OK (for 1d 23h 10m 11s)
Status Information:	Data Group State:*ENABLED Transfer Definition Status:*ACTIVE Remote Journal Link Status:*ACTIVE
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	07-26-2022 13:06:35
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 1.435 seconds
Next Scheduled Check:	07-27-2022 13:06:35
Last State Change:	07-25-2022 13:01:33
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	07-27-2022 12:11:36 (0d 0h 0m 8s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

RJLNK returned info

Parameters:

Mimix Library	Mimix install library.
Datagroup Name	Name of the data group configured in Mimix.
System 1	System number 1.
System 2	System number 2.

Returns the following information.

Data Group State	The status of the data group definition.
Transfer Definition Status	System that is configured to be the production system.
Remote Journal Link Status	Status of the switch on System 1.

check_MMx_OBJAPY

Returns the status for the object replication processes.

Service State Information

Current Status:	CRITICAL (for 1d 23h 17m 30s)
Status Information:	Data Group State:*ENABLED CRITICAL-Object Send Process:*INACTIVE Object Retrieve Backlog:0 CRITICAL-Object Send Backlog:495678 Object Apply Backlog:0
Performance Data:	
Current Attempt:	5/5 (HARD state)
Last Check Time:	07-27-2022 12:53:51
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.144 seconds
Next Scheduled Check:	07-28-2022 12:53:51
Last State Change:	07-25-2022 13:36:29
Last Notification:	07-27-2022 12:53:51 (notification 3)
Is This Service Flapping?	NO (5.99% state change)
In Scheduled Downtime?	NO
Last Update:	07-27-2022 12:53:56 (0d 0h 0m 3s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

OBJAPY returned info

Parameters:

Mimix Library	Mimix install library.
Datagroup Name	Name of the data group configured in Mimix.
System 1	System number 1.
System 2	System number 2.
Retrieve Backlog Critical	Critical range for the retrieve backlog.
Retrieve Backlog Warning	Warning range for the retrieve backlog.
Send Backlog Critical	Critical range for the send backlog.
Send Backlog Warning	Warning range for the send backlog.
Apply Backlog Critical	Critical range for the apply backlog.
Apply Backlog Warning	Warning range for the apply backlog.

Returns the following information.

Data Group State	The status of the data group definition.
Object Send Process	Status of the object send process.
Object Retrieve Backlog	Object Retrieve backlog.
Object Send Backlog	Object Send backlog.
Object Apply Backlog	Object Apply backlog.

Returns information about the File Tracking entries.

Service State Information

Current Status:	OK (for 1d 23h 56m 26s)
Status Information:	File tracking entries held, due to errors:0 File tracking entries held, not due to errors:0 Inactive file tracking entries:0 File tracking entries not journalled on source:0 File tracking entries not journalled on target:0 File tracking entries under compare repair state:0
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	07-26-2022 13:08:59
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.120 seconds
Next Scheduled Check:	07-27-2022 13:08:59
Last State Change:	07-25-2022 13:08:59
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	07-27-2022 13:05:16 (0d 0h 0m 9s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

FESTS returned info

Parameters:

Mimix Library	Mimix install library.
Datagroup Name	Name of the data group configured in Mimix.
System 1	System number 1.
System 2	System number 2.
Held due to Error	Range for number of file tracking entries held for error.
Held not due to Error	Range for number of file tracking entries that are held not due to error.
Not Active	Range for number of inactive file tracking entries
Not Journalled	Range for number of file tracking entries not journalled on the source.
Not Journalled on Target	Range for number of file tracking entries not journalled on the target.
Compare Repair State	Range for number of file tracking entries under compare repair state.

Returns the following information.

Data Group State	The status of the data group definition.
Object Send Process	Status of the object send process.
Object Retrieve Backlog	Object Retrieve backlog.
Object Send Backlog	Object Send backlog.
Object Apply Backlog	Object Apply backlog.

check_MMx_ITESTS

Returns information about the IFS tracking entries.

Service State Information

Current Status:	OK (for 2d 0h 50m 53s)
Status Information:	IFS Tracking entries held, due to errors:0 IFS Tracking entries held, not due to errors:0 Inactive IFS tracking entries:0 IFS Tracking entries not journalled on source:0 IFS Tracking entries not journalled on target:0
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	07-27-2022 13:31:29
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.132 seconds
Next Scheduled Check:	07-28-2022 13:31:29
Last State Change:	07-25-2022 13:26:29
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	07-27-2022 14:17:16 (0d 0h 0m 6s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

ITESTS returned info

Parameters:

Mimix Library	Mimix install library.
Datagroup Name	Name of the data group configured in Mimix.
System 1	System number 1.
System 2	System number 2.
Held due to Error	Range for number of IFS tracking entries held for error.
Held not due to Error	Range for number of IFS tracking entries that are held not due to error.
Not Active	Range for number of inactive IFS tracking entries
Not Journalled	Range for number of IFS tracking entries not journalled on the source.
Not Journalled on Target	Range for number of IFS tracking entries not journalled on the target.

Returns the following information.

IFS Tracking entries held, due to errors	Number of IFS Tracking entries held, due to errors.
IFS Tracking entries held, not due to errors	Number of IFS Tracking entries held, not due to errors.
Inactive IFS tracking entries	Number of inactive IFS Tracking entries.
IFS Tracking entries not journalled on source	Number of IFS Tracking entries that are not journalled on the source.
IFS Tracking entries not journalled on target	Number of IFS Tracking entries that are not journalled on the target.

Returns information about the Object tracking entries.

Service State Information

Current Status:	OK (for 1d 1h 27m 55s)
Status Information:	Object Tracking entries held, due to errors:0 Object Tracking entries held, not due to errors:0 Inactive Object tracking entries:0 Object Tracking entries not journalled on source:0 Object Tracking entries not journalled on target:0
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	07-27-2022 13:09:49
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.150 seconds
Next Scheduled Check:	07-28-2022 13:09:49
Last State Change:	07-26-2022 13:09:49
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (12.11% state change)
In Scheduled Downtime?	NO
Last Update:	07-27-2022 14:37:36 (0d 0h 0m 8s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

OTESTS returned info

Parameters:

Mimix Library	Mimix install library.
Datagroup Name	Name of the data group configured in Mimix.
System 1	System number 1.
System 2	System number 2.
Held due to Error	Range for number of object tracking entries held for error.
Held not due to Error	Range for number of object tracking entries that are held not due to error.
Not Active	Range for number of inactive object tracking entries
Not Journalled	Range for number of object tracking entries not journalled on the source.
Not Journalled on Target	Range for number of object tracking entries not journalled on the target.

Returns the following information.

Object Tracking entries held, due to errors	Number of Object Tracking entries held, due to errors.
Object Tracking entries held, not due to errors	Number of Object Tracking entries held, not due to errors.
Inactive Object tracking entries	Number of inactive Object Tracking entries.
Object Tracking entries not journalled on source	Number of Object Tracking entries that are not journalled on the source.
Object Tracking entries not journalled on target	Number of Object Tracking entries that are not journalled on the target.

check_MMx_CFGCHG

Returns information about the number of configuration changes that have occurred since the last start.

Service State Information

Current Status:	OK (for 2d 1h 39m 48s)
Status Information:	DLO config changes:*NO IFS config changes:*NO Object config changes:*NO
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	07-27-2022 13:01:29
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.152 seconds
Next Scheduled Check:	07-28-2022 13:01:29
Last State Change:	07-25-2022 13:01:29
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	07-27-2022 14:41:16 (0d 0h 0m 1s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

CFGCHG returned info

Parameters:

Mimix Library	Mimix install library.
Datagroup Name	Name of the data group configured in Mimix.
System 1	System number 1.
System 2	System number 2.

Returns the following information.

DLO config changes	Number of DLO config changes.
IFS config changes	Number of IFS config changes.
Object config changes	Number of Object config changes.

check_MMX_CNTRSTS

Returns information about the container replication status.

Service State Information

Current Status:	OK (for 2d 20h 40m 50s)
Status Information:	Size of the backlog:0 Container send process:0 Last sent sequence number:00000000000000000000
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	07-27-2022 13:03:59
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.146 seconds
Next Scheduled Check:	07-28-2022 13:03:59
Last State Change:	07-25-2022 13:03:59
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	07-28-2022 09:44:46 (0d 0h 0m 3s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

CNTRSTS returned info

Parameters:

Mimix Library	Mimix install library.
Datagroup Name	Name of the data group configured in Mimix.
System 1	System number 1.
System 2	System number 2.
Backlog Warning	Warning Range for backlog.

Returns the following information.

Size of the backlog	Size of the backlog.
Container send process	Number Active send processes.
Last sent sequence number	Last sent sequence number.

check_MMx_APYSTS

Returns the Apply status information for a particular apply session.

Service State Information

Current Status:	CRITICAL (for 0d 0h 1m 37s)
Status Information:	CRITICAL-Apply process:*INACTIVE Apply backlog:0
Performance Data:	
Current Attempt:	1/5 (SOFT state)
Last Check Time:	07-28-2022 11:00:39
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 14.362 seconds
Next Scheduled Check:	07-29-2022 11:00:39
Last State Change:	07-28-2022 11:00:39
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (17.57% state change)
In Scheduled Downtime?	NO
Last Update:	07-28-2022 11:02:07 (0d 0h 0m 9s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

APYSTS returned info

Parameters:

Mimix Library	Mimix install library.
Datagroup Name	Name of the data group configured in Mimix.
System 1	System number 1.
System 2	System number 2.
SSN	Apply session number.
Backlog Critical	Critical range for backlog.
Backlog Warning	Warning range for backlog.

Returns the following information.

Apply process	Status of the apply process.
Apply backlog	Size of the apply backlog.

check_MMx_ARSTS

Returns the receiver information for a particular apply session.

Service State Information

Current Status:	OK (for 0d 0h 16m 40s)
Status Information:	Last sequence number in log space: Date for last entry in the log space:072722 Time for last entry in the log space:010036 Last applied sequence number:0000000000000000211 Last applied entry date:072722 Last applied entry time:010036
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	07-28-2022 11:17:14
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.019 seconds
Next Scheduled Check:	07-29-2022 11:17:14
Last State Change:	07-28-2022 11:00:39
Last Notification:	N/A (notification 0)
Is This Service Flapping?	YES (22.89% state change)
In Scheduled Downtime?	NO
Last Update:	07-28-2022 11:17:16 (0d 0h 0m 3s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

ARSTS returned info

Parameters:

Mimix Library	Mimix install library.
Datagroup Name	Name of the data group configured in Mimix.
System 1	System number 1.
System 2	System number 2.
SSN	Apply session number.

Returns the following information.

- Last sequence number in log space
- Date for last entry in the log space
- Time for last entry in the log space
- Last applied sequence number
- Last applied entry date
- Last applied entry time

check_MMX_AGSTS

Returns the application group status.

Service State Information

Current Status:	OK (for 0d 0h 19m 44s)
Status Information:	Application group status: Application Node status:*INACTIVE Data Cluster Group status: Data Node status: Data Replication status:*ATTN Procedure status:*NONE
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	07-28-2022 11:00:39
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 16.751 seconds
Next Scheduled Check:	07-29-2022 11:00:39
Last State Change:	07-28-2022 11:00:39
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (12.24% state change)
In Scheduled Downtime?	NO
Last Update:	07-28-2022 11:20:16 (0d 0h 0m 7s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

AGSTS returned info

Parameters:

Mimix Library	Mimix install library.
Datagroup Name	Name of the data group configured in Mimix.
System 1	System number 1.
System 2	System number 2.

Returns the following information.

Application group status

(*ACTIVE/*ADDNODPND/*CHGPND/*CRTPND/*DLTCMDPND/*DLTPND/
*ENDCRGPND/*INACTIVE/*INDOUBT/*NONE/*NOTAVAIL/*RESTORED/
*RMVNODPND/*STRCRGPND/*SWTPND/*UNKNOWN)

Application Node status

(*ACTIVE/*INACTIVE/*NONE/*NOTAVAIL/*PARTMGR/*PARTIAL/
*UNKNOWN)

Data Cluster Group status

(blank/*ACTIVE/*ADDNODPND/*ATTN/*CHGPND/*CRTPND/*DLTCMDPND/
*DLTPND/*ENDCRGPND/*INACTIVE/*INDOUBT/*NONE/*NOTAVAIL/
*NOTIFY/*PARTIAL/*RESTORED/*RMVNODPND/*STRCRGPND/*SWTPND/
*UNKNOWN)

Data Node status

(blank/*ACTIVE/*ATTN/*NONE/*NOTAVAIL/*PARTIAL/*UNKNOWN)

Data Replication status

(*ACTIVE/*ATTN/*ATTN_PPRC/*AUTHORITY/*INACTIVE/*NONE/
*NOTAVAIL/*STGMGTSVR/*SUSPENDED/*UNKNOWN/*VRTSWTRCY/
*VRTSWTSTR/*VRTSWTST)

Procedure status

(*ACTIVE/*ATTN/*COMP/*NONE)

check_MMX_SYSSTS

Returns the status associated with a system, top view of all activities.

Service State Information

Current Status:	OK (for 0d 0h 24m 38s)
Status Information:	Returned system definition:BACKTST Journal manager process status:*ACTIVE Journal inspector status:*NOTTGT Collection server status:*ACTIVE Cluster server status:*NONE Procedure status:*COMP
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	07-28-2022 11:00:39
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 14.799 seconds
Next Scheduled Check:	07-29-2022 11:00:39
Last State Change:	07-28-2022 11:00:39
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (12.24% state change)
In Scheduled Downtime?	NO
Last Update:	07-28-2022 11:25:16 (0d 0h 0m 1s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

SYSSTS returned info

Parameters:

Mimix Library Mimix install library.
System System name.

Returns the following information.

Returned system definition

Journal manager process status

(*ACTIVE/*ACTREQ/*INACTIVE/*INACTASP/*JRNRCVCNT/*NONE/
*RCYASP/*UNKNOWN)

Journal inspector status

(*INACTIVE/*PARTIAL/*ACTIVE/*UNKNOWN/*NEWDG/*NONE/
*NOTCFG/*NOTTGT)

Collection server status

Cluster server status (*ACTIVE/*INACTIVE/*UNKNOWN)
 Procedure status (*ACTIVE/*ACTPEND/*FAILED/*INACTIVE/*INACTPEND/*NEW/*NONE/*NOTAVAIL/*PARTITION/*RMVPEND/*UNKNOWN)
 (*ACTIVE/*ATTN/*COMP/*NONE/*UNKNOWN)

check_MMX_JRNSTS

Returns the journal status for specified journal.

Service State Information

Current Status:	OK (for 0d 0h 0m 9s)
Status Information:	Journal name:TEST2DG Journal Library:#MXJRN Last entry in the attached receiver:TEST2D0054 Date of last entry in the receiver:#MXJRN Time of the last entry in the receiver:00000000000000000215
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	07-28-2022 12:16:41
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.335 seconds
Next Scheduled Check:	07-29-2022 12:16:41
Last State Change:	07-28-2022 12:16:41
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (12.11% state change)
In Scheduled Downtime?	NO
Last Update:	07-28-2022 12:16:46 (0d 0h 0m 4s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

ARSTS returned info

Parameters:
 Mimix Library Mimix install library.
 Journal Name Name of the journal configured in Mimix.
 System System name.

Returns the following information.

Journal name
 Journal Library
 Last entry in the attached receiver
 Date of last entry in the receiver
 Time of the last entry in the receiver

IBM i Status Check Commands

Returns the status for type passed in.

Parameters:

Type	The Type of status to return (see below)
Type	Returns
DSKPCT	% of Available disk space
DSKTOT	Total amount of disk space on the system
DSKAVL	Amount of disk available
SYSNAM	Current system name
SSTATE	System State restricted (*RSTD, *NRSTD)
PCTPRC	% Processor used
JOBRUN	Number of jobs running
PERMAD	% Permanent addresses used
TEMPAD	% Temp addresses used
SYSASP	Size of System ASP
STGTOT	Total Storage size
UPTSTG	Unprotected storage
MUPSTG	Maximum unprotected storage
NBPART	Number of partitions
PARTID	Partition ID
PRCCAP	Processor Capacity
PRCSHR	Processor sharing (*NONE, *CAPPED, *UNCAPPED)
NBRPRC	Number of processors
ACTJNB	Number of *ACTIVE jobs
ACTTHD	Number *ACTIVE threads
MAXJOB	Maximum number of jobs in system
TMP256	%Temporary 256MB segments
PRM256	%Permanent 256MB segments
TMP4GB	%Temporary 4GB segments
PRM4GB	%Permanent 4GB segments
UCPCPU	% Uncapped CPU
SHRPRU	% Shared Processor pool used
MEMSTG	Main Memory amount

check_Status_AVLDISK

Returns available disk as a percentage.

Service State Information

Current Status:	OK (for 7d 5h 14m 3s)
Status Information:	Available disk space : 56%
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:39:09
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.048 seconds
Next Scheduled Check:	10-27-2021 14:49:09
Last State Change:	10-20-2021 09:28:14
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:42:07 (0d 0h 0m 10s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Available disk space %

Parameters:

% Critical

Range for Percentage of disk available, returns critical code.

% Warning

Range for Percentage of disk available, returns warning code.

Available disk space : 56%

check_Status_TOTDISK

Returns total disk in GB.

Service State Information

Current Status:	OK (for 6d 2h 10m 2s)
Status Information:	Total disk space : 102GB
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:38:30
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.027 seconds
Next Scheduled Check:	10-27-2021 14:48:30
Last State Change:	10-21-2021 12:33:29
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:43:27 (0d 0h 0m 4s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Total Disk space GB

Parameters:

% Critical

Range for total disk available, returns critical code.

% Warning

Range for total disk available, returns warning code.

Total disk space : 150GB

check_Status_AVLDISKGB

Returns available disk in GB.

Service State Information

Current Status:	OK (for 7d 1h 39m 22s)
Status Information:	Available disk space : 57GB
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:40:32
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.026 seconds
Next Scheduled Check:	10-27-2021 14:50:32
Last State Change:	10-20-2021 13:05:32
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:44:47 (0d 0h 0m 7s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Available Disk space GB

Parameters:

Critical

Range for amount of disk available, returns critical code.

Warning

Range for amount of disk available, returns warning code.

Available disk space : 85GB

check_Status_SYSNAME

Returns system name.

Service State Information

Current Status:	OK (for 6d 23h 14m 6s)
Status Information:	System Name: SAS2
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:36:43
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.026 seconds
Next Scheduled Check:	10-27-2021 14:46:43
Last State Change:	10-20-2021 15:31:43
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:45:47 (0d 0h 0m 2s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

System Name

check_Status_SYSSTATE

Returns system state.

Service State Information	
Current Status:	OK (for 6d 18h 15m 9s)
Status Information:	System State: *NRSTD
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:47:02
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.026 seconds
Next Scheduled Check:	10-27-2021 14:57:02
Last State Change:	10-20-2021 20:32:00
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:47:07 (0d 0h 0m 2s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

System State

Parameters:

Severity

Sets severity of code returned when state is *RSTD.

check_Status_CPUUSED

Returns the percentage of processor used.

Service State Information	
Current Status:	OK (for 7d 5h 18m 39s)
Status Information:	Processor Used: 0%
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:39:23
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.025 seconds
Next Scheduled Check:	10-27-2021 14:49:23
Last State Change:	10-20-2021 09:29:21
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:47:57 (0d 0h 0m 3s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Processor Used %

Parameters:

Critical

Range for percentage of processor used, returns critical code.

Warning

Range for percentage of processor used, returns warning code.

check_Status_NUMJOB

Returns number of jobs running on system.

Service State Information

Current Status:	OK (for 6d 3h 58m 2s)
Status Information:	Jobs running on system : 1108
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:47:11
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.026 seconds
Next Scheduled Check:	10-27-2021 14:57:11
Last State Change:	10-21-2021 10:52:10
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:50:07 (0d 0h 0m 5s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Number of Jobs

Parameters:

Critical
Warning

Range for number of jobs running on system, returns critical code.
Range for number of jobs running on system, returns warning code.

check_Status_PADDR

Returns percentage of permanent addresses used.

Service State Information

Current Status:	OK (for 6d 23h 52m 38s)
Status Information:	Permanent addresses used : 0%
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:43:45
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.049 seconds
Next Scheduled Check:	10-27-2021 14:53:45
Last State Change:	10-20-2021 14:58:45
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:51:17 (0d 0h 0m 6s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Perm Addresses used %

Parameters:

Critical
Warning

Range for percentage of permanent addresses used, returns critical code.
Range for percentage of permanent addresses used, returns warning code.

check_Status_TADDR

Returns percentage of temporary addresses used.

Service State Information	
Current Status:	OK (for 6d 2h 10m 0s)
Status Information:	Temporary addresses used : 0%
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:47:18
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.026 seconds
Next Scheduled Check:	10-27-2021 14:57:18
Last State Change:	10-21-2021 12:42:18
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:52:17 (0d 0h 0m 1s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Temp Addresses Used %

Parameters:

Critical

Range for percentage of temporary addresses used, returns critical code.

Warning

Range for percentage of temporary addresses used, returns warning code.

check_Status_ASP

Returns size of system ASP in GB.

Service State Information	
Current Status:	OK (for 6d 2h 9m 21s)
Status Information:	Size of System ASP : 102GB
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:48:38
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.026 seconds
Next Scheduled Check:	10-27-2021 14:58:38
Last State Change:	10-21-2021 12:43:38
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:52:57 (0d 0h 0m 2s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

System ASP size GB

Parameters:

Critical

Range for size of system ASP, returns critical code.

Warning

Range for size of system ASP, returns warning code.

check_Status_STORAGE

Returns total storage size in GB.

Service State Information	
Current Status:	OK (for 6d 5h 11m 22s)
Status Information:	Total Storage size : 102GB
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:47:26
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.026 seconds
Next Scheduled Check:	10-27-2021 14:57:26
Last State Change:	10-21-2021 09:42:25
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:53:37 (0d 0h 0m 10s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Total Storage GB

Parameters:

Critical

Range for total storage size, returns critical code.

Warning

Range for total storage size, returns warning code.

check_Status_UNPSTG

Returns size of unprotected storage in MB.

Service State Information	
Current Status:	WARNING (for 2d 4h 5m 19s)
Status Information:	WARNING - Unprotected storage : 6196MB
Performance Data:	
Current Attempt:	5/5 (HARD state)
Last Check Time:	10-27-2021 14:49:59
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.026 seconds
Next Scheduled Check:	10-27-2021 14:59:59
Last State Change:	10-25-2021 10:49:58
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:55:07 (0d 0h 0m 10s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Unprotected Storage size GB

Parameters:

Critical

Range for size of unprotected storage, returns critical code.

Warning

Range for size of unprotected storage, returns warning code.

check_Status_MAXUNPSTG

Returns max size of unprotected storage in MB.

Service State Information	
Current Status:	WARNING (for 2d 14h 32m 41s)
Status Information:	WARNING - Maximum unprotected storage : 6220MB
Performance Data:	
Current Attempt:	5/5 (HARD state)
Last Check Time:	10-27-2021 14:53:17
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.026 seconds
Next Scheduled Check:	10-27-2021 15:03:17
Last State Change:	10-25-2021 00:23:17
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:55:57 (0d 0h 0m 1s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Maximum unprotected storage MB

Parameters:

Critical

Range for max size of unprotected storage, returns critical code.

Warning

Range for max size of unprotected storage, returns warning code.

check_Status_NUMPART

Returns number of partitions on system.

Service State Information	
Current Status:	OK (for 6d 15h 17m 19s)
Status Information:	Number of partitions : 6
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:54:27
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.025 seconds
Next Scheduled Check:	10-27-2021 15:04:27
Last State Change:	10-20-2021 23:39:27
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:56:37 (0d 0h 0m 9s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Number of partitions

Parameters:

Critical

Range for number of partitions on system, returns critical code.

Warning

Range for number of partitions on system, returns warning code.

check_Status_PARTID

Returns partition ID for host.

Service State Information	
Current Status:	OK (for 6d 2h 18m 29s)
Status Information:	Partition ID : 2
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:54:04
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.026 seconds
Next Scheduled Check:	10-27-2021 15:04:04
Last State Change:	10-21-2021 12:39:03
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:57:27 (0d 0h 0m 5s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Partition ID

Parameters:

There are no parameters for this check command

check_Status_CPUCAP

Returns processor capacity as a percentage.

Service State Information	
Current Status:	OK (for 7d 5h 29m 30s)
Status Information:	Processor Capacity : 0%
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:48:49
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.026 seconds
Next Scheduled Check:	10-27-2021 14:58:49
Last State Change:	10-20-2021 09:28:49
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:58:17 (0d 0h 0m 2s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

CPU Capacity %

Parameters:

Critical
Warning

Range for percentage of processor capacity, returns critical code.
Range for percentage of processor capacity, returns warning code.

check_Status_CPUSHARE

Returns processor sharing status.

Service State Information	
Current Status:	OK (for 7d 5h 29m 51s)
Status Information:	Processor sharing : *UNCAPPED
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:49:09
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.030 seconds
Next Scheduled Check:	10-27-2021 14:59:09
Last State Change:	10-20-2021 09:29:07
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:58:57 (0d 0h 0m 1s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Processor sharing type

Parameters:

There are no parameters for this check command.

check_Status_NUMCPU

Returns number of processors that are licensed.

Service State Information	
Current Status:	OK (for 6d 11h 2m 4s)
Status Information:	Number of processors : 2
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:52:54
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.028 seconds
Next Scheduled Check:	10-27-2021 15:02:54
Last State Change:	10-21-2021 03:57:53
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 14:59:47 (0d 0h 0m 10s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Number of licensed processors

Parameters:

Critical

Warning

Range for number of processors, returns critical code.

Range for number of processors, returns warning code.

check_Status_ACTJOB

Returns number of *ACTIVE jobs running on system.

Service State Information	
Current Status:	OK (for 6d 21h 17m 39s)
Status Information:	*ACTIVE jobs : 236
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:58:04
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.025 seconds
Next Scheduled Check:	10-27-2021 15:08:04
Last State Change:	10-20-2021 17:43:03
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:00:37 (0d 0h 0m 5s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Running active jobs

Parameters:

Critical

Range for number of active jobs on system, returns critical code.

Warning

Range for number of active jobs on system, returns warning code.

check_Status_ACTTHD

Returns number of *ACTIVE threads on system.

Service State Information	
Current Status:	OK (for 7d 5h 34m 30s)
Status Information:	*ACTIVE threads : 885
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:57:20
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.026 seconds
Next Scheduled Check:	10-27-2021 15:07:20
Last State Change:	10-20-2021 09:27:20
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:01:47 (0d 0h 0m 3s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Active threads

Parameters:

Critical

Range for number of active threads on system, returns critical code.

Warning

Range for number of active threads on system, returns warning code.

check_Status_MAXJOB

Returns maximum number of jobs on system.

Service State Information

Current Status:	OK (for 7d 0h 15m 47s)
Status Information:	Maximum number of jobs in system : 163520
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 15:02:01
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.026 seconds
Next Scheduled Check:	10-27-2021 15:12:01
Last State Change:	10-20-2021 14:46:58
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:02:37 (0d 0h 0m 8s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Maximum Active jobs

Parameters:

Critical

Range for max number of jobs on system, returns critical code.

Warning

Range for max number of jobs on system, returns warning code.

check_Status_TMP256

Returns % of temporary 256MB segments used.

Service State Information

Current Status:	OK (for 7d 5h 37m 55s)
Status Information:	Temporary 256MB segments : 0%
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 14:56:37
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.026 seconds
Next Scheduled Check:	10-27-2021 15:06:37
Last State Change:	10-20-2021 09:26:36
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:04:27 (0d 0h 0m 4s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

256MB segments used %

Parameters:

Critical

Range for percentage of temp 256MB segments used, returns critical code.

Warning

Range for percentage of temp 256MB segments used, returns warning code.

check_Status_PRM256

Returns % of permanent 256MB segments used.

Service State Information	
Current Status:	OK (for 7d 5h 41m 35s)
Status Information:	Permanent 256MB segments : 0%
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 15:03:57
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.051 seconds
Next Scheduled Check:	10-27-2021 15:13:57
Last State Change:	10-20-2021 09:23:56
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:05:27 (0d 0h 0m 4s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Perm 256MB segments used %

Parameters:

Critical

Warning

Range for percentage of permanent 256MB segments used, returns critical code.
Range for percentage of permanent 256MB segments used, returns warning code.

check_Status_TMP4GB

Returns % of temporary 4GB segments used.

Service State Information	
Current Status:	OK (for 7d 5h 46m 25s)
Status Information:	Temporary 4GB segments : 0%
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 15:06:55
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.025 seconds
Next Scheduled Check:	10-27-2021 15:16:55
Last State Change:	10-20-2021 09:26:54
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:13:17 (0d 0h 0m 2s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Temp 4GB segments used %

Parameters:

Critical

Warning

Range for percentage of temp 4GB segments used, returns critical code.
Range for percentage of temp 4GB segments used, returns warning code.

check_Status_PRM4GB

Returns % of permanent 4GB segments used.

Service State Information

Current Status:	OK (for 7d 5h 49m 41s)
Status Information:	Permanent 4GB segments : 0%
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 15:04:14
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.027 seconds
Next Scheduled Check:	10-27-2021 15:14:14
Last State Change:	10-20-2021 09:24:14
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:13:47 (0d 0h 0m 8s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Perm 4GB segments used %

Parameters:

Critical
Warning

Range for percentage of permanent 4GB segments used, returns critical code.
Range for percentage of permanent 4GB segments used, returns warning code.

check_Status_UCAP

Returns % of uncapped CPU used.

Service State Information

Current Status:	OK (for 7d 5h 45m 53s)
Status Information:	Processor Capacity : 0%
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 15:08:49
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.026 seconds
Next Scheduled Check:	10-27-2021 15:18:49
Last State Change:	10-20-2021 09:28:49
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:14:37 (0d 0h 0m 5s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Uncapped CPU used %

Parameters:

Critical
Warning

Range for percentage of uncapped CPU used, returns critical code.
Range for percentage of uncapped CPU used, returns warning code.

check_Status_SPOOL

Returns % of shared processor pool used.

Service State Information	
Current Status:	OK (for 7d 3h 14m 29s)
Status Information:	Shared Processor pool used : 0%
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 15:06:08
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.025 seconds
Next Scheduled Check:	10-27-2021 15:16:08
Last State Change:	10-20-2021 12:01:07
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:15:27 (0d 0h 0m 9s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Shared processor pool used %

Parameters:

Critical

Range for percentage shared processor pool used, returns critical code.

Warning

Range for percentage of shared processor pool used, returns warning code.

check_Status_MAINMEM

Returns amount of main memory in GB.

Service State Information	
Current Status:	OK (for 6d 8h 6m 40s)
Status Information:	Main Memory amount : 3GB
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 15:14:41
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.026 seconds
Next Scheduled Check:	10-27-2021 15:24:41
Last State Change:	10-21-2021 07:09:40
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:16:17 (0d 0h 0m 3s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Main memory GB

Parameters:

Critical

Range for main memory amount, returns critical code.

Warning

Range for main memory amount, returns warning code.

Job List

Returns a list of jobs which exceed the parameters passed in.

Parameters:

Type	The Type of status to return (see below)
Max	Maximum number of jobs to list in the output
Min	Minimum value before adding to returned list (dependent on the check)
Critical	Critical Range to be checked against.
Warning	Warning Range to be checked against.

Request	Returns
PRCTTU	Processing unit time used - total for the job (milliseconds)
INTTRN	Number of interactive transactions
DBLCKW	Number of database lock waits
INTLCW	Number of internal machine lock waits
NDBLCW	Number of nondatabase lock waits
AUXIOR	Number of auxiliary I/O requests
PEAKTS	Peak temporary storage used (megabytes)
QTEMPS	QTEMP library size, in bytes
RESPTT	Response time total (milliseconds)
TSDBLW	Time spent on database lock waits (milliseconds)
TSINTL	Time spent on internal machine lock waits (milliseconds)
TSNDBL	Time spent on nondatabase lock waits (milliseconds)
TMPSTG	Temporary storage used (megabytes)

check_Status_PRCTTU

Returns amount of processor unit time used in ms for each job.

Service State Information

Current Status:	OK (for 6d 7h 25m 23s)
Status Information:	All jobs within set processor unit time ranges.
	Job: ADMIN2 Job User: QLWISVR Job Number: 641333 Processor Used: 1440203
	Job: ADMIN5 Job User: QLWISVR Job Number: 641331 Processor Used: 260976
	Job: QSLPSVR Job User: QSYS Job Number: 641365 Processor Used: 168016
	Job: QINAVMNSRV Job User: QLWISVR Job Number: 641396 Processor Used: 138815
	Job: QSCWCHMS Job User: QUSER Job Number: 641391 Processor Used: 104633
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 15:25:39
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.034 seconds
Next Scheduled Check:	10-27-2021 15:35:39
Last State Change:	10-21-2021 08:00:38
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:25:57 (0d 0h 0m 4s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Jobs processor used

Parameters:

Max Count	Maximum number of jobs to return.
Min Value	Minimum value of processor unit time to be listed.
Critical	Range for ms of processor unit time used, returns critical code.
Warning	Range for ms of processor unit time used, returns warning code.

check_Status_INTRN

Returns number of interactive transactions per job listed.

Service State Information	
Current Status:	OK (for 1d 0h 27m 13s)
Status Information:	There are currently 0 interactive transactions.
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 15:21:26
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.032 seconds
Next Scheduled Check:	10-27-2021 15:31:26
Last State Change:	10-26-2021 15:01:26
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:28:37 (0d 0h 0m 2s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Jobs Interactive transaction range

Parameters:

Max Count

Maximum number of jobs to return.

Min Value

Minimum number of interactive transactions to be listed.

Critical

Range for number of interactive transactions, returns critical code.

Warning

Range for number of interactive transactions, returns warning code.

check_Status_DBLCKW

Returns amount of database lock waits per job listed.

Service State Information	
Current Status:	OK (for 1d 0h 32m 42s)
Status Information:	There are currently 0 Database Lock Waits.
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 15:29:47
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.033 seconds
Next Scheduled Check:	10-27-2021 15:39:47
Last State Change:	10-26-2021 14:59:47
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:32:27 (0d 0h 0m 2s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Jobs DB Lockwait Range

Parameters:

- Max Count Maximum number of jobs to return.
- Min Value Minimum number of lock waits to be listed.
- Critical Range for number of database lock waits, returns critical code.
- Warning Range for number of database lock waits, returns warning code.

check_Status_INTLCW

Returns amount of internal machine lock waits per job listed.

Service State Information

Current Status:	OK (for 6d 5h 18m 4s)
Status Information:	All jobs within set internal machine lock wait ranges.
	Job: ADMIN5 Job User: QLWISVR Job Number: 641331 Internal Machine Lock Waits: 751
	Job: ADMIN1 Job User: QLWISVR Job Number: 641332 Internal Machine Lock Waits: 720
	Job: ADMIN4 Job User: QWEBADMIN Job Number: 641330 Internal Machine Lock Waits: 705
	Job: QSPPF00001 Job User: QSYS Job Number: 641208 Internal Machine Lock Waits: 281
	Job: QSQSRVR Job User: QUSER Job Number: 642880 Internal Machine Lock Waits: 208
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 15:31:05
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.033 seconds
Next Scheduled Check:	10-27-2021 15:41:05
Last State Change:	10-21-2021 10:16:05
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:34:07 (0d 0h 0m 2s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Jobs internal lockwait range

Parameters:

Max Count	Maximum number of jobs to return.
Min Value	Minimum number of lock waits to be listed.
Critical	Range for number of internal machine lock waits, returns critical code.
Warning	Range for number of internal machine lock waits, returns warning code.

check_Status_NDBLCKW

Returns amount of non-database lock waits per job listed.

Service State Information

Current Status:	CRITICAL (for 4d 7h 44m 16s)
Status Information:	CRITICAL - (Job:645510) Non-Database Lock Waits: 5932 CRITICAL - (Job:645507) Non-Database Lock Waits: 5660 CRITICAL - (Job:645506) Non-Database Lock Waits: 5153
	Job: NAGRSPCLNT Job User: NA4IUSER Job Number: 645510 CRITICAL - Non-Database Lock Waits: 5932
	Job: NAGRSPCLNT Job User: NA4IUSER Job Number: 645507 CRITICAL - Non-Database Lock Waits: 5660
	Job: NAGRSPCLNT Job User: NA4IUSER Job Number: 645506 CRITICAL - Non-Database Lock Waits: 5153
	Job: QYSPFRCOL Job User: QSYS Job Number: 641276 Non-Database Lock Waits: 66
	Job: QDBSRV01 Job User: QSYS Job Number: 641178 Non-Database Lock Waits: 54
Performance Data:	
Current Attempt:	5/5 (HARD state)
Last Check Time:	10-27-2021 15:31:35
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.033 seconds
Next Scheduled Check:	10-27-2021 15:41:35
Last State Change:	10-23-2021 07:51:35
Last Notification:	10-27-2021 15:31:35 (notification 206)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:35:47 (0d 0h 0m 4s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Jobs Database Lockwait range

Parameters:

- Max Count Maximum number of jobs to return.
- Min Value Minimum number of lock waits to be listed.
- Critical Range for number of non-database lock waits, returns critical code.
- Warning Range for number of non-database lock waits, returns warning code.

check_Status_AUXIOR

Returns amount of auxiliary I/O requests per job listed.

Service State Information

Current Status:	CRITICAL (for 4d 7h 43m 56s)
Status Information:	CRITICAL - (Job:645510) Auxiliary I/O Requests: 5944 CRITICAL - (Job:645507) Auxiliary I/O Requests: 5663 CRITICAL - (Job:645506) Auxiliary I/O Requests: 5153
	Job: NAGRSPCLNT Job User: NA4IUSER Job Number: 645510 CRITICAL - Auxiliary I/O Requests: 5944
	Job: NAGRSPCLNT Job User: NA4IUSER Job Number: 645507 CRITICAL - Auxiliary I/O Requests: 5663
	Job: NAGRSPCLNT Job User: NA4IUSER Job Number: 645506 CRITICAL - Auxiliary I/O Requests: 5153
	Job: QYSPFRCOL Job User: QSYS Job Number: 641276 Auxiliary I/O Requests: 66
	Job: QDBSRV01 Job User: QSYS Job Number: 641178 Auxiliary I/O Requests: 54
	Job: QSPLMAINT Job User: QSYS Job Number: 641187 Auxiliary I/O Requests: 53
	Job: SCPF Job User: QSYS Job Number: 000000 Auxiliary I/O Requests: 33
	Job: QDBSRV03 Job User: QSYS Job Number: 641180 Auxiliary I/O Requests: 31
	Job: QDBSRV02 Job User: QSYS Job Number: 641179 Auxiliary I/O Requests: 30
	Job: QJOBLOGSVR Job User: QSYS Job Number: 641239 Auxiliary I/O Requests: 9
Performance Data:	
Current Attempt:	5/5 (HARD state)
Last Check Time:	10-27-2021 15:32:58
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.033 seconds
Next Scheduled Check:	10-27-2021 15:42:58

Jobs Aux I/O requests range

Parameters:

Max Count	Maximum number of jobs to return.
Min Value	Minimum number of auxiliary I/O requests to be listed.
Critical	Range for number of auxiliary I/O requests, returns critical code.
Warning	Range for number of auxiliary I/O requests, returns warning code.

check_Status_PEAKTS

Returns amount of peak temporary storage per job listed.

Service State Information

Current Status:	OK (for 7d 3h 58m 44s)
Status Information:	All jobs within set peak storage ranges.
	Job: ADMIN2 Job User: QLWISVR Job Number: 641333 Peak Temporary Storage: 798
	Job: ADMIN5 Job User: QLWISVR Job Number: 641331 Peak Temporary Storage: 281
	Job: ADMIN4 Job User: QWEBADMIN Job Number: 641330 Peak Temporary Storage: 266
	Job: ADMIN1 Job User: QLWISVR Job Number: 641332 Peak Temporary Storage: 233
	Job: QTCPWRK Job User: QSYS Job Number: 641211 Peak Temporary Storage: 150
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 15:34:20
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.057 seconds
Next Scheduled Check:	10-27-2021 15:44:20
Last State Change:	10-20-2021 11:39:20
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:37:57 (0d 0h 0m 7s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Jobs peak temp storage range

Parameters:

Max Count

Maximum number of jobs to return.

Min Value

Minimum amount of peak temp storage to be listed.

Critical

Range for amount of peak temp storage, returns critical code.

Warning

Range for amount of peak temp storage, returns warning code.

check_Status_QTEMPS

Returns size of QTEMP library in MB per job listed.

Service State Information

Current Status:	OK (for 6d 5h 18m 14s)
Status Information:	All jobs within set QTEMP library size ranges.
	Job: NAGRSPCLNT Job User: NA4IUSER Job Number: 645507 QTEMP Library Size: 82108(MB)
	Job: NAGRSPCLNT Job User: NA4IUSER Job Number: 645510 QTEMP Library Size: 79028(MB)
	Job: NAGRSPCLNT Job User: NA4IUSER Job Number: 645506 QTEMP Library Size: 66752(MB)
	Job: HA4IURNSCR Job User: HA4IUSER Job Number: 644480 QTEMP Library Size: 42068(MB)
	Job: HA4ISPLRDR Job User: HA4IUSER Job Number: 644487 QTEMP Library Size: 38988(MB)
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 15:35:32
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.056 seconds
Next Scheduled Check:	10-27-2021 15:45:32
Last State Change:	10-21-2021 10:20:32
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:38:37 (0d 0h 0m 9s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Jobs QTEMP Library MB range

Parameters:

Max Count	Maximum number of jobs to return.
Min Value	Minimum size of QTEMP library to be listed.
Critical	Range for size of QTEMP library, returns critical code.
Warning	Range for size of QTEMP library, returns warning code.

check_Status_RESPTT

Returns total response time in seconds per job listed.

Service State Information

Current Status:	OK (for 0d 20h 44m 40s)
Status Information:	Total response time is currently 0s.
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 15:34:49
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.032 seconds
Next Scheduled Check:	10-27-2021 15:44:49
Last State Change:	10-26-2021 18:54:49
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:39:27 (0d 0h 0m 2s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Jobs Response time range

Parameters:

Max Count
Min Value
Critical
Warning

Maximum number of jobs to return.
Minimum total response time to be listed.
Range for total response time, returns critical code.
Range for total response time, returns warning code.

check_Status_TSDBLW

Returns total seconds spent in database lock wait, per job listed.

Service State Information	
Current Status:	OK (for 1d 0h 41m 52s)
Status Information:	0 time has been spent in database lock wait.
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 15:38:47
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.033 seconds
Next Scheduled Check:	10-27-2021 15:48:47
Last State Change:	10-26-2021 14:58:47
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:40:37 (0d 0h 0m 2s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Jobs DB Lockwait range

Parameters:

Max Count
Min Value
Critical
Warning

Maximum number of jobs to return.
Minimum time spent in database lock wait to be listed.
Range for time spent in database lock wait, returns critical code.
Range for time spent in database lock wait, returns warning code.

check_Status_TSINTL

Returns total seconds spent in internal lock wait, per job listed.

Service State Information

Current Status:	OK (for 7d 6h 13m 24s)
Status Information:	All jobs within set internal lock wait ranges.
	Job: QJOBLOGSVR Job User: QSYS Job Number: 641237 Time Spent Internal Lock Wait: 533(s)
	Job: ADMIN5 Job User: QLWISVR Job Number: 641331 Time Spent Internal Lock Wait: 350(s)
	Job: ADMIN2 Job User: QLWISVR Job Number: 641333 Time Spent Internal Lock Wait: 339(s)
	Job: ADMIN4 Job User: QWEBADMIN Job Number: 641330 Time Spent Internal Lock Wait: 304(s)
	Job: QJOBLOGSVR Job User: QSYS Job Number: 641239 Time Spent Internal Lock Wait: 281(s)
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 15:38:05
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.033 seconds
Next Scheduled Check:	10-27-2021 15:48:05
Last State Change:	10-20-2021 09:28:05
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:41:27 (0d 0h 0m 2s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

74 Jobs Internal Lockwait range

Parameters:

- Max Count Maximum number of jobs to return.
- Min Value Minimum time spent in internal lock wait to be listed.
- Critical Range for time spent in internal lock wait, returns critical code.
- Warning Range for time spent in internal lock wait, returns warning code.

check_Status_TSNDDBL

Returns total seconds spent in non-database lock wait, per job listed.

Service State Information

Current Status:	CRITICAL (for 3d 22h 33m 59s)
Status Information:	CRITICAL - (Job:645507) Time Spent Non-Database Lock Wait: 12061(s) CRITICAL - (Job:645510) Time Spent Non-Database Lock Wait: 10488(s) CRITICAL - (Job:645506) Time Spent Non-Database Lock Wait: 7866(s)
	Job: NAGRSPCLNT Job User: NA4IUSER Job Number: 645507 CRITICAL - Time Spent Non-Database Lock Wait: 12061(s)
	Job: NAGRSPCLNT Job User: NA4IUSER Job Number: 645510 CRITICAL - Time Spent Non-Database Lock Wait: 10488(s)
	Job: NAGRSPCLNT Job User: NA4IUSER Job Number: 645506 CRITICAL - Time Spent Non-Database Lock Wait: 7866(s)
	Job: QYSPFRCOL Job User: QSYS Job Number: 641276 Time Spent Non-Database Lock Wait: 1573(s)
	Job: PRT02 Job User: QSPLJOB Job Number: 641280 Time Spent Non-Database Lock Wait: 1573(s)
Performance Data:	
Current Attempt:	5/5 (HARD state)
Last Check Time:	10-27-2021 15:38:24
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.034 seconds
Next Scheduled Check:	10-27-2021 15:48:24
Last State Change:	10-23-2021 17:08:24
Last Notification:	10-27-2021 15:38:24 (notification 188)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:42:17 (0d 0h 0m 6s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Jobs non DB Lockwait range

Parameters:

- Max Count Maximum number of jobs to return.
- Min Value Minimum time spent in non-database lock wait to be listed.
- Critical Range for time spent in non-database lock wait, returns critical code.
- Warning Range for time spent in non-database lock wait, returns warning code.

check_Status_TMPSTG

Returns temporary storage used in MB, per job listed.

Service State Information

Current Status:	OK (for 6d 14h 7m 24s)
Status Information:	All jobs within set temp storage ranges.
	Job: ADMIN2 Job User: QLWISVR Job Number: 641333 Temp Storage Used: 626(MB)
	Job: ADMIN4 Job User: QWEBADMIN Job Number: 641330 Temp Storage Used: 174(MB)
	Job: QTCPWRK Job User: QSYS Job Number: 641211 Temp Storage Used: 150(MB)
	Job: ADMIN1 Job User: QLWISVR Job Number: 641332 Temp Storage Used: 148(MB)
	Job: ADMIN5 Job User: QLWISVR Job Number: 641331 Temp Storage Used: 147(MB)
Performance Data:	
Current Attempt:	1/5 (HARD state)
Last Check Time:	10-27-2021 15:41:13
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.034 seconds
Next Scheduled Check:	10-27-2021 15:51:13
Last State Change:	10-21-2021 01:36:12
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-27-2021 15:43:27 (0d 0h 0m 9s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Jobs temporary storage range

Parameters:

- Max Count Maximum number of jobs to return.
- Min Value Minimum temporary storage used to be listed.
- Critical Range for temporary storage used, returns critical code.
- Warning Range for temporary storage used, returns warning code.

Secure connections

AAG has the ability to connect to remote IBM i systems using secure sockets, however this requires the relevant certificate is generated on the IBM i system using Digital Certificate Manager (5770SS1 option 34) and installed on the Nagios Server.

The set up and management of the certificates is beyond the scope of this manual, we have provided links in the related information section that can be used to set up the certificates. Shield Advanced Solutions can provide services to set up the secure connection if required.

Pushover Acknowledgement Functions

Pushover offers the ability to acknowledge emergency notifications. We have added functions to be able to pull these acknowledgments and apply them against the Nagios problem, to which they relate. This allows a user to stop multiple notifications from being sent out, awaiting a response from a user. It also prevents the user from having to log into their local network to be able to acknowledge a problem being pushed out by AAG, while not exposing AAG to the outside world.

This functionality is controlled by the “-r retry” “-e expire” and “-k” parameters pushed to notify-host-by-pushover or notify-service-by-pushover. “-r” is the number of minutes between retry notifications being pushed out and “-e” is how long to keep attempting to notify the user before expiring. You can read much more about these values within the pushover documentation under “Emergency Priority (2)”. It is required to use emergency priority for all messages if you wish to use this functionality. “-k” is the flag which will tell Nagios if this function is to be used. Pass “1” to use this function and “0” to keep the default settings.

If you are upgrading from a version older than AAG1040122 then the misc-commands for notify by pushover for both services and hosts need to be changed. Also, there are updates required for the database and a crontab needs to be added.

Change the Misc. commands for notify-host-by-pushover and notify-service-by-pushover to the following:

```
/usr/local/nagios/share/sas/notify_host_by_pushover.sh -u
"$CONTACTPUSHOVER_USER_KEYS" -a "$CONTACTPUSHOVER_API_KEYS" -s
"spacealarm" -t "$HOSTNAME$ is $HOSTSTATE$" -m "Status: $HOSTOUTPUT$" -d
"\n$LONGHOSTOUTPUT$" -p "$HOSTSTATEID$" -h "$HOSTNAME$" -r "1800" -e "3600" -k
"1"
```

```
/usr/local/nagios/share/sas/notify_service_by_pushover.sh -u
"$CONTACTPUSHOVER_USER_KEYS" -a "$CONTACTPUSHOVER_API_KEYS" -s
"spacealarm" -t "$SERVICEDESC$ on $HOSTNAME$ is $SERVICESTATE$" -m
"$SERVICEOUTPUT$" -d "\n$LONGSERVICEOUTPUT$" -p "$SERVICESTATEID$" -h
"$HOSTNAME$" -v "$SERVICEDESC$" -r "1800" -e "3600" -k "1"
```

To create the DB required for the PO ack:

```
sudo mysql -u root -p

CREATE DATABASE pushover;

Use pushover
```

```
CREATE TABLE receipts( receipt VARCHAR(30) NOT NULL, typ VARCHAR(2) NOT
NULL, host VARCHAR(25) NOT NULL, service VARCHAR(25) NOT NULL, PRIMARY
KEY(receipt));
```

```
exit;
```

Add the cron job:

```
sudo crontab -u nagios -e
```

```
*/* * * * * /usr/local/nagios/share/sas/pocheck
```

Create encrypted file for MYSQL login:

```
addSystem
```

```
System Name: MYSQL
```

```
Username: [mysql login username]
```

```
Password: [mysql login password]
```

Other entries don't matter, respond with 'N' to add host to nagios.

Install JQ:

```
sudo apt install jq
```

Ensure user has privileges to access DB table:

```
GRANT ALL PRIVILEGES ON pushover.* TO '[USER]'@'localhost' IDENTIFIED BY
'[PASSWORD]';
```

Security Bulletins

AAG provides the ability to identify any exposures on your IBM i related to the Security Bulletins provided by IBM. The PTF's that fix the exposure are listed in a Database provided by Shield Advanced Solutions Ltd and can be downloaded from our website in JSON format. In addition to this AAG can review this content against the installed LPPs and PTFs to identify the individual fixes that are available.

A new command GETSBPTF has been provided that will carry out the same review of the Security Bulletins and download any related PTFs to an Image Catalog ready for installation. Once they have been downloaded they can be installed using the PTF options on the PTF menu.

GETSBPTF

IMGCLG	Image Catalog to use, must exist prior to running the command and be free of any content.
CLGDIR	The directory in the IFS that will be used to store the binary files, this directory must exist prior to running the request.
CHKDAT	The date to use as the earliest date Security Bulletins should be reviewed from. Using '20220101' will search the DB for all Security Bulletins

issued since the 1st January 2022. The date format has to be the same as above or the request may fail.

When the command is run a check against the installed LPPs and PTFs is carried out, if any PTFs are required they will be downloaded automatically to the Image Catalog. The images can then be verified and mounted and the IMAGE Catalog loaded to a Virtual Optical device before using the PTF menu to install the PTFs.

PTF Installation

From time to time it may be necessary to provide fixes to problems identified with the NG4i product or provide additional functionality to the product. The method used for shipping the changed or additional objects is the IBM iSeries PTF function. Save File will be shipped by various methods depending on the size of the files to be shipped. Below is a description of how to restore a ZIP file onto your system and then load and apply the PTF.

The ZIP file will have a number of objects embedded within the file. The Save Files which have to be copied to the IBM i will be in the following format.

The PTF Objects

Q1XXnnnn.sav where XX is the product Id such as NG for NG4i, nnnn will be the Version and Release level of the product (10 for this release) and the PTF number 01 – 99. The sav extension is only for reference and should be left off when the file is copied to the IBM i.

Note:-

The PTF process requires separate PTF's to be generated for different features of the same product, as NLV objects (language specific) are packaged separately we now ship separate PTF's for each supported NLV language. The PTF numbering process for NLV objects will be Q1XXaann.savf where XX is NG for NG4i, aa represents the last 2 digits of the NLV code (24 for English) and nn for the PTF number. Only installed features can be updated but the PTF for the base and NLV language must be installed together with the NLV PTF being installed after the base PTF. For an English based system you would install 1NG1001 and then 1NG2401. Failure to install the NLV PTF will cause some programs and features to end abnormally or display incorrect information.

The Cover Letter

XXFnnnncvr.sav where XX is the product Id such as NG for NG4i, F stands for fix, nnnn will be the Version and Release level of the product (10 for this version) and the PTF number 01 – 99. The sav extension is only for reference and should be left off when the file is copied to the iSeries.

A further object is embedded in the file, which is a PC text file, which contains the installation instructions as well as a copy of the cover letter text. This will have the same format as the Cover Letter file but will have an extension of txt.

The ZIP file can be received in a variety of ways, if it is received attached to an Email message on your PC perform the following actions.

1. Save the attachment (ZIP file) to a directory on your PC.
2. Unzip the file into the same directory.
3. Transfer the required unzipped files to the iSeries into a Save File of the same name .

Note:-

For FTP ensure the method of transfer is Binary and that an object of type *SAVF of the same name of the unzipped file without the extension (.SAV) exists in the library.

4. Issue the command LODPTF with LICPGM(1NG4ISC) DEV(*SAVF) and the SAVF parameter is the name and library of the Save File you have just created.

5. Issue an APYPTF command with the product ID as 1NG4ISC.

If the PTF is received by any other method, consult the relevant manuals on how to restore the Save File to your system before issuing the LODPTF and APYPTF commands.

It is intended that all PTFs, which have been tested and found to be stable, will be loaded onto the website for download.

Update packages IBM i

As part of the ongoing update process we provide updates via a save file. These save files will follow a naming convention of NG4IMMDDYY which MMDDYY reflects the data the update was packaged for distribution. Each save file will always contain all updates created since the last PTF was issued. The updates therefore require the latest PTF to be installed prior to installing any updates.

The updates will be available to any user who is active on maintenance via a download option in the maintenance panel group. The panel group will show the latest PTF/Update available plus what is installed on the system currently.

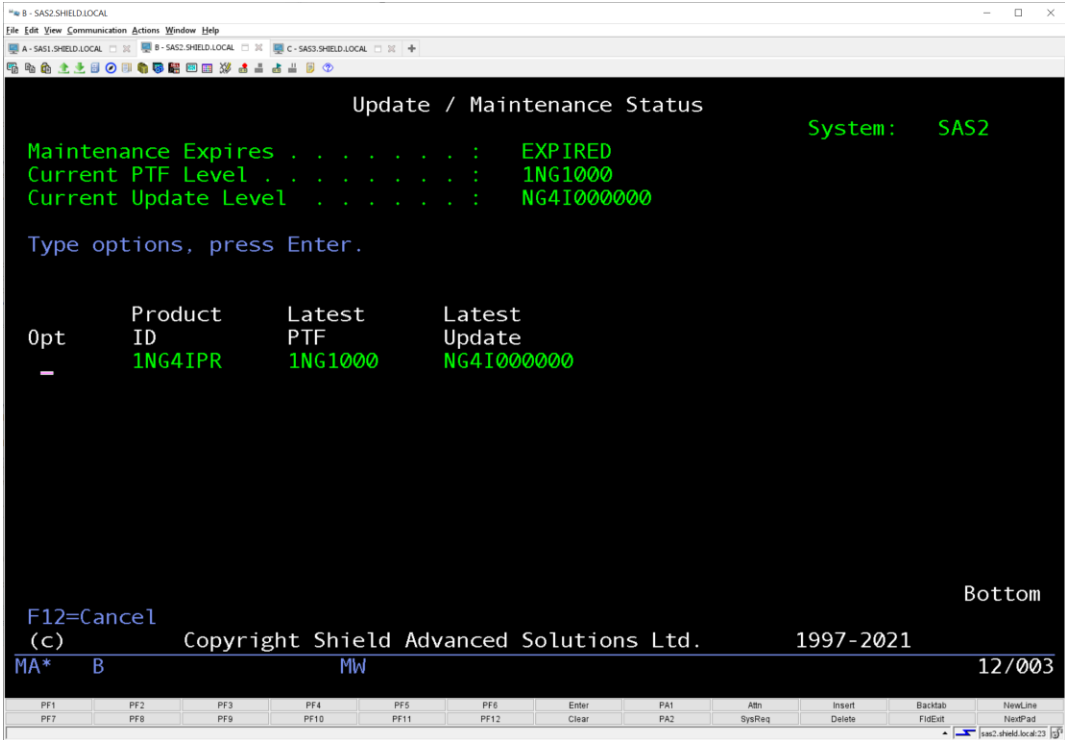


Figure 2 Maintenance screen

The following options will be shown if maintenance is current on the product:

- Option 1 : Retrieve the update and store in QGPL
- Option 2 : Retrieve the PTF and store in QGPL
- Option 3 : Retrieve the update and install
- Option 6 : Retrieve the update documentation and display

The above screen shows the system is at the same level as the latest available.

A new command (AUTOUPD) has been added that will allow an automated check for updates against the shield website, if there is a later update available the program will automatically download and install the update. The system must be current on maintenance and be fully licensed before the command will work. We also suggest that NG4i is restarted after the update has been applied.

Note:

We strongly advance against running the request more than once per week. When the display status request is run NG4i will now check for a license key replacement for the product, if a license key is found that expires later than the currently installed key it will be downloaded and installed replacing the existing key.

If you wish to build your own CLP to carry out the installation of the save file after it has been downloaded to the system (via the AAG distribution method) you can use something similar to the following to install the update:

```

PGM
/* before this program can be compiled need to create the file in QGPL */
/* eg: DSPOBJD OBJ(QGPL/NG4I*) OBJTYPE(*FILE) OUTPUT(*OUTFILE) OUTFILE(QGPL/NG4ISAVFS) */
DCL      VAR(&INSTLIB) TYPE(*CHAR) LEN(10) VALUE(NG4I21)
DCL      VAR(&UPDLVL) TYPE(*CHAR) LEN(10)
DCL      VAR(&MSGDTA) TYPE(*CHAR) LEN(300)
DCLF     FILE(QGPL/NG4ISAVFS) RCDfmt(*ALL)

ADDLIB   LIB(&INSTLIB)
MONMSG   MSGID(CPF2103)
/* get the latest update that has been installed */
RTVDTAARA DTAARA(&INSTLIB/UPDATELVL (11 10)) RTNVAR(&UPDLVL)
READ:    RCVF
MONMSG   MSGID(CPF0864) EXEC(GOTO CMDLBL(END))
CHGVAR   VAR(&MSGDTA) VALUE('Found :' *BCAT &ODOBNM)
SNDMSG   MSG(&MSGDTA) TOUSR(*REQUESTER)
IF       COND(%SST(&ODOBNM 1 10) *GT &UPDLVL) THEN(DO)
    ENDNG4I
    LODRUN   DEV(*SAVF) SAVF(QGPL/&UPDLVL)
    STRNG4I
    GOTO     CMDLBL(END)
ENDDO
GOTO     CMDLBL(READ)
END:
ENDPGM

```

Update packages Nagios/Linux

Updates for the Nagios side of AAG will be passed along as a .ZIP file. Within this .ZIP file AAG's core structure and file system will be appropriately arranged, allowing for the user to simply unzip the file into the AAG folder on their Nagios box. The folder location for AAG is “/usr/local/nagios/share/sas”. Alternatively, the user can call “/usr/local/nagios/share/sas/updateAAG.sh [system type]” which will automatically download the

.ZIP folder, unzip, and distribute the files into their appropriate folders. This is recommended as the new versions of AAG require objects to be placed in several locations across the system. If you are using Mod-Gearman workers, then it is mandatory that you edit the update script to match your installation.

Support Process

To allow us to better control the support of our clients we have introduced a new support process using OSTicket. This process is to be used to log all support requests plus any new feature requests that you may have. It also provides a Knowledgebase which can be viewed by the members to show some of the common questions we are asked and what information we have provided in response to those requests. It is recommended that you register to use the process at your earliest convenience.

The following URL can be used to register for access and sign in once registered.

<https://www.shieldadvanced.com/osticket/>

