CA OPS/MVS® Event Management and Automation

WebCenter Reference Guide

Release 12.1

CA Technologies Product References

This document references the following CA Technologies products:

- CA NetMaster® Network Management for SNA (CA NetMaster NM for SNA)
- CA Network and Systems Management (CA NSM)
- CA OPS/MVS® Event Management and Automation (CA OPS/MVS)
- CA Service Desk (CA Service Desk)
- CA SYSVIEW® Performance Management (CA SYSVIEW)

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Introduction 9

Chapter 2: Administering the Region 11

Chapter 3: Using WebCenter 13

Chapter 4: Alert Monitor 19

Chapter 5: Setting Up the Alert Monitor 21

Chapter 6: Status Monitor 31

Chapter 7: Implementing Status Monitor Filters 33

Chapter 8: Customizing the Status Monitor Display Format 37

Chapter 9: User Profiles 41

Appendix A: Health Checks 45

Chapter 1: Introduction

This section contains the following topics:

General Description

The WebCenter component provides an infrastructure for monitoring z/OS alerts and resource statuses. The interface is hosted completely.

The component provides two user interfaces (UIs):

- A web UI for monitoring

  Note: The uniform resource locator (URL) of the web UI is made available in a CA OPS/MVS global variable named GLOBALW.OPS#.WEBCENTERURL. You display these variables using the CA OPS/MVS OPSVIEW Control option, Global Variables (Option 4.8).

- A 3270 UI for administering the component, and customizing monitor filters and formats

  You access the 3270 UI using the CA OPS/MVS OPSVIEW Control option, WebCenter Control (Option 4.14).

What Does WebCenter Comprise?

WebCenter comprises the following entities:

Knowledge Base (RAMDB)

Is a Virtual Storage Access Method (VSAM) database that maintains the resource information. The information is stored with the following hierarchy: system image definition and resource definitions.

Alert Monitor

Enables you to monitor alerts. You can customize this monitor. You can also configure how alerts are delivered. Monitoring is through the web UI; configuration is through a 3270 UI.

Status Monitor

Enables you to monitor resource statuses. You can customize this monitor. Monitoring is through the web UI; configuration is through a 3270 UI.

Chapter 2: Administering the Region

This section contains the following topics:

Access the Region Using the 3270 Interface

After the WebCenter region has started, users can log in to it using the web interface. These users monitor system resources through the alert and resource monitors. You give them the URL of the web interface for them to access the login page.

The region does not require further configuration. However, you, as a systems programmer, can use the 3270 interface to learn more about the functions available to an administrator. This interface also displays the web interface URL.

Note: The uniform resource locator (URL) of the web UI is made available in a CA OPS/MVS global variable named GLOBALW.OPS#.WEBCENTERURL. You display these variables using the CA OPS/MVS OPSVIEW Control option, Global Variables (Option 4.8).

Follow these steps:

1. Select the CA OPS/MVS OPSVIEW Control, WebCenter Control option (Option 4.14).

   The WebCenter 3270 interface appears.

2. Explore the interface, using the menu options. Press F1 (Help) if you require help on a panel.

Maintain the Region

The Administration and Definition option on the primary menu of the 3270 interface enables you to maintain the region configuration as the system environment changes.

Follow these steps:

1. Enter the **/PARMS** panel shortcut.

   The parameter groups that affect the region configuration are listed. A *parameter group* contains parameters that determine the characteristics of a region. See also Customizer (see page 51).

   Note: For more information about parameter groups, see the online help.

2. Update a group as required.

   For example, to change the port of the web interface:

   a. Enter **U** next to the WEBCENTER parameter group.

      The parameters in the group appear with their current values.

   b. Update the Web Interface Port field, and press F6.

      The port number is changed for the current instance of the region.

   c. Press F3.

      The region saves the changed port number. When the region starts from now on, it uses that port.

   Note: Press F6 to apply a change immediately, and press F3 to save the change permanently.

Important! If the region uses an initialization file at startup, any changes you make manually using the /PARMS panel shortcut are not retained. To keep the changes, regenerate the file using the /CUSTOM.G panel path. For more information about the initialization file, see *WebCenter Installation Guide*.

Chapter 3: Using WebCenter

This section contains the following topics:

WebCenter Features

WebCenter is a web browser interface that lets you access operations functions such as monitoring and history.

When enabled, your systems administrator can get you the URL of WebCenter. The URL is also displayed on the 3270 interface to the corresponding region.

WebCenter is hosted. The WebCenter web server runs in the region.

The problem resolution time is decreased and ease-of-use is increased. Users who are not comfortable accessing mainframe products can diagnose problems with their standard web browser.

Each WebCenter page has a help link in the upper-right corner that you can click for context-sensitive online help.

Set Up Your Web Browser

You can access WebCenter by using Internet Explorer or Firefox.

The WebCenter interface requires the Java Runtime Environment (JRE).

If your organization prevents you from downloading software through the Internet, arrange to have the JRE installed. The JRE is available from http://www.java.com.

The JRE is required to be downloaded once only, not once per WebCenter release.

Note: For software requirements on your PC to support WebCenter, see the *Installation Guide*.

Set Up Internet Explorer

WebCenter requires at least JRE Version 7 Update 21. If you do *not* have the required version of JRE, you receive an error dialog instead. The dialog tells you to download directly from the website.

If your organization permits you to download software from the Internet, you can download and install the Java runtime library. However, this download requires your security settings to permit you to access the website for a once only ActiveX control download.

You can configure the settings through Internet Options from the Tools menu of your browser. On the Security tab, for the web content zone that is associated with access to the website (usually the Internet), click Custom Level. On the Security Setting dialog that appears, the Download signed ActiveX controls option must not be disabled.

For you to access WebCenter correctly, specify the correct options in Internet Explorer.

Note: Depending on your version of the browser, some or all of these options are present and require review.

Follow these steps:

1. Click Tools, Internet Options.

   The Internet Options dialog appears.

2. Click the Security tab.
3. Click the web content zone to which your WebCenter belongs, and then click Custom Level.

   The Security Settings dialog appears.

4. Enable the following options:

   ActiveX controls and plug-ins

   Initialize and script ActiveX controls not marked as safe for scripting

   Run ActiveX controls and plug-ins

   Microsoft VM

   Java permissions: High safety

   Scripting

   Scripting of Java applets

5. Disable the following option:

   Miscellaneous

   Use Pop-up Blocker

   Click OK

6. Click the Privacy Tab, and then click the Sites button.

   The Per Site Privacy Actions dialog appears.

7. Complete the following field:

   Address of website

   Enter the WebCenter URL.

   Click Allow, and then click OK.

8. Click the Advanced Tab.

9. Enable the following option:

   Multimedia

   Show pictures

   If you do *not* require Sun JRE as your default virtual machine, clear the following option:

   Java (Sun)

   Use Java 2 *version_number* for <applet>

   Click OK.

   The options are saved.

Set Up Firefox

If your PC does *not* have JRE installed, the following alert appears when you access WebCenter:

`Java is not enabled in this browser. The Web Interface requires a Java-enabled browser.`

Go to the website to download and install the JRE.

WebCenter requires JRE Version 7 Update 21.

For you to access WebCenter correctly, enable the correct options in Firefox.

Note: Depending on your version of the browser, some or all of these options are present and require review.

Follow these steps:

1. Click Tools, Options.

   The Options dialog appears.

2. Click Content, and review the following options:

   Block pop-up windows

   > Clear the check box, or click Exceptions to add the WebCenter URL to the allowed sites.

   Load images automatically

   > Select the check box.

   Enable JavaScript

   > Select the check box; click Advanced, and select all the check boxes.

   Enable Java

   > Select the check box.

3. Click Privacy, and review the following option:

   Cookies

   > Accept third-party cookies

4. Click OK.

   The options are saved.

Log On to WebCenter

Your WebCenter user ID and password are used to access WebCenter.

Follow these steps:

1. Start your web browser and enter the access URL for WebCenter in the Address text box.

   The WebCenter login page appears.

   Notes:

   - The access URL is defined when your product is installed. You can find the value on the 3270 interface to the mainframe region. For more information, see the *Installation Guide*.

   - To access WebCenter easily and quickly in the future, create a bookmark for the WebCenter web access URL in your web browser.

2. Enter your User ID and Password, and click the Log In button.

   The initial WebCenter page appears, showing a navigational menu on the left pane. Each WebCenter page has a help link in the upper-right corner that you can click for context-sensitive online help.

Chapter 4: Alert Monitor

This section contains the following topics:

General Description

The Alert Monitor provides an integrated, correlated event notification system that indicates to operators that a problem has occurred and that some action is required.

The monitor refreshes your screen each time an alert arrives. The clock in the title line indicates when the screen was refreshed last.

The monitor includes a total indicator, which shows the total number of alerts and the total number of alerts of each severity level. Each severity level appears in a different color.

By default, alerts are sorted in the order of severity, then time. The most severe alerts are listed first, then, in each category of severity, the most recent of the alerts are listed first.

Alerts

Alerts provide the proactive notification of events. An alert is generated, for example, through the ADDRESS ALERTMON host environment. This host environment is used in both OPS/REXX programs and synchronous AOF rules.

From the Alert Monitor, you can update, track, and close alerts.

You can also configure the monitor to forward the alerts automatically to other applications and platforms.

An operator can close an alert manually. When an alert is closed, it is removed from the monitor. However, it is still accessible from Alert History over a defined period (as specified in the ALERTHIST parameter group).

Alerts that were raised before the region was shut down are not displayed on the monitor when the region restarts. These alerts are available from Alert History. The alert history contains information about all alerts.

More Information:

Implement the Alert History Function (see page 28)

Chapter 5: Setting Up the Alert Monitor

This section contains the following topics:

Access Alert Administration

Alert Monitor administration lets you define Alert Monitor filters that apply to all users.

Note: In a multisystem environment, the definitions that are created or customized *after* the regions are connected are synchronized and available across all connected regions.

You perform Alert Monitor administration functions from the Alert Monitor : Administration Menu.

To access Alert Monitor administration functions, enter **/ALADMIN** at the prompt.

The Alert Monitor : Administration Menu appears.

Define Alert Monitor Filters

You can filter the alerts displayed on the Alert Monitor by applying a set of criteria to each of the fields in the alert. The filters that you create can be named and stored for later use, using the FILTER command.

To define an Alert Monitor filter

1. Enter **/ALFILT** at the prompt.

   The Alert Monitor : Filter Definition List panel appears.

2. Press F4 (Add).

   The Alert Filter panel appears.

3. Complete the following fields:

   Name

   Specifies the name of the filter.

   Description

   Describes the filter.

   Filter Expression

   Specifies the Boolean expression that determines what alerts are passed by the filter. For more information about creating Boolean expressions, press F1 (Help).

   Press F3 (File)

   The Alert Monitor filter is saved.

Alert Forwarding

Alerts are displayed on the Alert Monitor; however, you can also forward them to the following platforms:

- EM Console in CA NSM
- UNIX platforms as SNMP traps
- CA NetMaster NM for SNA or Tivoli NetView (TME10) systems, as generic alert NMVTs
- CA Service Desk servers (see page 26), as CA Service Desk requests or incidents

You can apply filter criteria to forward different types of alerts to different platforms.

Alert forwarding does not require manual intervention; it occurs automatically when the alert is created.

Implement Alert Forwarding

You implement alert forwarding by using Customizer parameter groups.

Note: TNGTRAP and SERVICEDESK do not have clear (close) alert events.

Follow these steps:

1. Enter **/PARMS** at the prompt.

   The Customizer : Parameter Groups list appears.

2. Enter **U** in front of the ALERTS parameter group in the Interfaces category.

   The parameter group opens for you to update.

   Note: For information about the fields, press F1 (Help).

3. Complete the following field:

   Dest Type

   Specifies the type of alert forwarding that you want to use.

   Values: NMVT, NONE, SERVICEDESK, SNMPTRAP, and TNGTRAP

   Press Enter.

   The fields dynamically change to match the specified destination type.

4. Review the fields, and update as required.

   (Optional) Press F8 (Forward), and repeat Step 3 for each Definition ID.

   Note: Press F1 (Help) for information about the fields.

5. Press F6 (Action).

   The changes are applied.

6. Press F3 (File).

   The settings are saved.

SNMP Trap Definition

The MIB definition for alerts that are forwarded as SNMP traps is provided in the member, $AMTRAP, supplied in the CC2DSAMP data set. You can download this member to your UNIX system and can compile it.

Note: On some UNIX systems, the $ sign has special meaning. When copying this member to your UNIX system, you can rename it to avoid problems.

The supplied MIB defines two traps with the following object identifiers:

- $AMTRAP = 1.3.6.1.4.1.1126.1.2.1.2 (for an alert)
- $AMTRAPC = 1.3.6.1.4.1.1126.1.2.1.3 (when an alert is cleared)

Forward to Tivoli NetView

To receive alerts in a Tivoli NetView region, the CNMCALRT task must be defined and active. The alerts are formatted as Operator Notification generic alerts.

To forward alerts to Tivoli NetView

1. Check the DSIDMN (or DSIDMNB) member in the DSIPARM PDS. DSIPARM.PDS is allocated by the Tivoli NetView started task.
2. Ensure that the CNMCALRT task is included and is initialized (INIT=Y). For example:

   ```
   TASK MOD=CNMCALRT,TSKID=CNMCALRT,PRI=6,INIT=Y
   ```

   Note: This statement is necessary for the z/OS software alert forwarding function.

Forward to CA NSM

To format the traps sent to a CA NSM management platform, you must load the rules to reformat the alert messages for display on the EM Console.

To forward alerts to the EM Console in CA NSM

1. Use FTP to download the message definition rules in binary mode from the UNIEMMSG member of your CC2DSAMP data set created at installation. For example, using the Windows FTP client from the prompt:

   ```
   >ftp myhost
   Connected to myhost.mycompany.com.
   User (myhost.mycompany.com:(none)): user01
   331 Send password please.
   Password: xxxxxxxx
   230 USER01 is logged on. Working directory is "/u/users/user01".
   ftp>cd "prefix.ppvv.CC2DSAMP"
   250 The working directory "prefix.ppvv.CC2DSAMP" is a partitioned data set
   ftp>binary
   200 Representation type is Image
   ftp> get uniemmsg uniemmsg.txt
   200 Port request OK.
   125 Sending data set prefix.ppvv.CC2DSAMP(UNIEMMSG) FIXrecfm 80
   250 Transfer completed successfully.
   ftp: 3200 bytes received in 0.67Seconds 4.77Kbytes/sec.
   ftp>quit
   ```

2. From a Windows prompt on the destination CA NSM EM Server, load the message definition rules from the downloaded file. Enter the following command at the prompt to define the rules to event management:

   ```
   cautil -f "uniemmsg.txt"
   ```

3. Enter the following command to load the rules:

   ```
   oprcmd opreload
   ```

4. In your region, set the alert forwarding destination to TNGTRAP.

Alert Forwarding to CA Service Desk

Before you can forward alert details to CA Service Desk to create requests, you implement CA Service Desk Integration.

Note: For more information, see the *CA Common Services for z/OS Service Desk Integration Guide.*

Do not forward any alerts to CA Service Desk until integration is completely and correctly implemented; otherwise, all alert forwarding requests to CA Service Desk fail.

Enable State Change Alerts

The region can automatically generate an alert for a resource that changes state. The region closes such an alert automatically when it recognizes that the problem that caused the alert no longer exists. You can enable the alerts for selected state changes. You can also specify the severity levels of the generated state change alerts.

Follow these steps:

1. Enter the **/PARMS** panel shortcut.

   The Parameter Groups panel appears.

2. Enter **F STATECHANGE**.

   The cursor locates the STATECHANGE parameter group.

3. Enter **U** next to the group.

   The group opens for updating.

4. Enter a severity number from 1 through 4 in the fields for the states you want to enable alerting. For example, if you want a Severity 2 alert for state changes to UNKNOWN, enter **2** in the Unknown field.

   Press F6 (Action).

   The region starts generating alerts for those state changes.

5. Press F3 (File).

   The group is updated with the changes.

CA Service Desk Integration

The CA Service Desk Integration feature creates CA Service Desk requests from forwarded alerts.

You can define multiple forwarding destinations to CA Service Desk, with each one pointing to a different CA Service Desk server.

Note: If your CA Service Desk installation is configured with the optional ITIL application, incidents are created instead of requests.

Many CA Technologies mainframe products use this feature to consolidate their problem notification on a specified CA Service Desk server. The feature uses W3C SOAP (Simple Object Access Protocol) to invoke the web services that CA Service Desk provides.

Software Requirements

CA Service Desk Integration has the following software requirements:

- CA Service Desk
- CA Common Services for z/OS, specifically the CAICCI and CAISDI/soap components

How Requests Are Created

To create a CA Service Desk request from an alert, the following internal steps are performed:

1. The CA Common Services for z/OS CAICCI component is used to pass the request to the CA Common Services for z/OSCAISDI soap component. CAISDI/soap is a z/OS-hosted SOAP client.
2. CAISDI/soap sets up an IP connection with the CA Service Desk server, then uses HTTP/HTTPS requests to invoke the necessary web services on the CA Service Desk server to create the new request or incident.
3. The request or incident number is returned and annotated in the alert.

Request Assignment

By default, CA Service Desk requests created by your region appear as *assigned* requests, with an assignee and an end user of System_NetMaster_User.

Your CA Service Desk administrator can customize the product templates to change these assignments to suit your organization.

Request Updating

A CA Service Desk request created from an alert is static. It reflects the alert details that were current at the time it was created.

Note: A CA Service Desk request is not subsequently updated with any changes to the alert, nor closed when the corresponding alert is closed.

Requests are intended for initial problem notification to a wider and more general data center audience. CA Service Desk Integration complements the functions of the Alert Monitor; it does not replace the Alert Monitor.

Every request (if HTML format is used) contains hyperlinks to various WebCenter pages, including the Alert Monitor. You should use the Alert Monitor for real-time dynamic alerting functions.

For recurring alerts, a request is created for the first occurrence only.

Request Description Format

By default, your region generates CA Service Desk request description content in HTML format.

By default, CA Service Desk does *not* render embedded HTML directives in the request description field. To support this rendering, customize your CA Service Desk server. This task involves customizing the detail_cr.htmpl form to add KEEPTAGS and KEEPLINKS support.

Note: For more information, see the *CA Service Desk Manager Implementation Guide*.

Implement the Alert History Function

The Alert Monitor retains data in an alert history file. You can define the time period that alerts are retained.

To specify the time period that alerts are retained

1. Enter **/PARMS** at the prompt.

   The Parameter Groups list appears.

2. Enter **U** in front of the $NM ALERTHIST parameter group in the Files category.

   The ALERTHIST - Alert History File Specification panel appears.

3. Complete the following fields:

   Days to Retain Alerts

   Specifies the number of days that you want to retain alerts in the history file.

   Limits: 999 days

   Default: 7 days

   Time of Day for Alert Purge

   Specifies the time of day (in the format *hh.mm*) at which alerts older than the value in the Days to Retain Alerts field are deleted.

   Press F6 (Action).

   The changes are applied.

4. Press F3 (File).

   The settings are saved.

Reorganize Files and Monitor Space Usage

Over time, the alert history file can become fragmented. You can reorganize the file to improve its efficiency.

To reorganize the Alert History database for optimum space usage

1. Copy (REPRO) the alert history file to a backup file.
2. Delete and redefine the original file.

Use the same attributes that were used when the file was defined at region setup. See the generated S01LCALC member in your INSTALL.JCL data set; this member has the original VSAM definition JCL for the file.

Monitor the amount of disk space used by the data set to estimate the optimal file size and optimal frequency of reorganization.

Example: Back Up Alert History File

This example backs up an alert history file.

```
//BKALERTH EXEC PGM=IDCAMS
//SYSPRINT DD   SYSOUT=*
//IN       DD   DSN=?prefix.ALERTH,DISP=SHR
//OUT      DD   SN=?prefix.ALERTH.BACKUP.SEQ,DISP=OLD
//SYSIN    DD   *
 REPRO INFILE(IN) OUTFILE(OUT)
/*
```

The sequential backup file has the following format:

```
DSORG=PS,RECFM=VB,LRECL=32756,BLKSIZE=32760
```

Extract Alert Data for Reporting

You can extract alert data from the Alert History database in a character separated values (CSV) format for processing by external reporting and analysis tools. The default field separator character is comma (,). You can change it in the ALERTHIST parameter group.

To extract alert data for reporting and analysis

1. Allocate a sequential data set with the following attributes:
   - LRECL is greater than or equal to 300 bytes.
   - RECFM is VB.
2. Enter **/ALHIST**.

   The History Menu appears.
3. Type **EX** at the prompt, and specify the data set name that you have allocated in the Extract DSN field.

   (Optional) If you want to limit the extracted data, select an Alert Monitor filter (see page 22) through the Filter Name field.

   Press Enter.

   The data is extracted to the specified data set.
4. Transfer the data set to your personal computer (PC) in ASCII format, and save it with an appropriate extension. (For example, if you plan to use Microsoft Excel to process the data, use the .csv extension.)

   The extracted data is saved in a text file.
5. Open the text file by using your preferred PC application.

   The extracted data is presented in your preferred format for analysis.
6. Analyze your data by applying facilities such as graphs and charts, tables, and macros.

Chapter 6: Status Monitor

This section contains the following topics:

General Description

The status monitor (or resource monitor) enables you to monitor at the resource level in your environment in real time. The monitor displays resources line by line, and uses color and highlighting to notify you of changes in their states.

From the monitor, you can enter commands against resources.

Authorized users can define filters that enable the viewing of information about specific resources.

Resources

The resources are discovered automatically and defined in the knowledge base. *Resources* are defined to a region as part of a system image. The information is derived from the resource data that is held in the active CA OPS/MVS Relational Data Framework (RDF) resource tables.

Chapter 7: Implementing Status Monitor Filters

This section contains the following topics:

Implement the Status Monitor Filters

You use filters to customize a Status Monitor panel. For example, you can define a filter that displays only those resources with a problem state, enabling you to monitor by exception. (A NOTOK filter is supplied for this purpose.)

A Status Monitor filter uses a Boolean expression to determine what to display on the monitor. You restrict the display by using the resource attributes such as name and status.

Note: In a multisystem environment, the definitions that are created or customized *after* the regions are connected are synchronized and available across all connected regions.

Access Status Monitor Filter Definitions

The status Monitor filters let you configure your view of monitored resources to suit your requirements. You can selectively view different groups of resources by swapping filters.

To access Status Monitor filter definitions, enter **/FILTERS** at the prompt.

The Status Monitor Filter List appears.

The panel displays the list of filter definitions in the knowledge base. You can add a definition, or can browse, update, copy or delete an existing definition. A number of filters are predefined as working examples.

Add a Status Monitor Filter

To add a Status Monitor filter definition

1. Access the Status Monitor Filter List.
2. Press F4 (Add).

   The Status Monitor Filter panel appears.

   Note: If you change your mind and do not want to add the filter, press F12 (Cancel) to cancel the operation any time before Step 5.
3. Complete the Name and Description fields in the Filter Definition window to identify the new filter.

   Note: Press F1 (Help) for a description of the fields.
4. Specify a Boolean expression (see page 36) in the Filter Expression window to define the filter.
5. Press F3 (File).

   The new definition is saved.

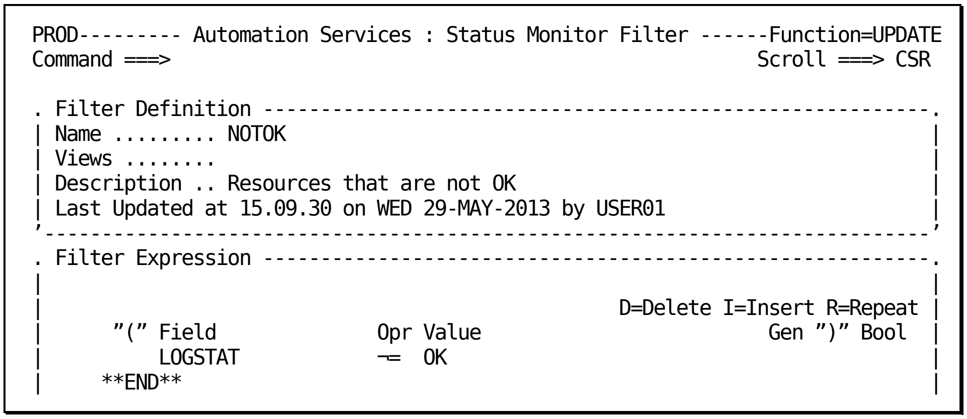
Status Monitor Filter Panel

The Status Monitor Filter panel specifies the details of a Status Monitor filter. The operation that you are performing is displayed at the top right of the panel, for example, Function=UPDATE.

The panel contains two windows. The Filter Definition window identifies the filter by name and description, and the Filter Expression window specifies the Boolean expression that defines the filter.

Example: Define a Status Monitor Filter

This example defines a filter named NOTOK. The filter enables an operator to monitor resources that have a logical state other than OK. The following panel shows the completed filter:



```
PROD--------- Automation Services : Status Monitor Filter ------Function=UPDATE
Command ===>                                                     Scroll ===> CSR

. Filter Definition -----------------------------------------------------------.
| Name ......... NOTOK                                                         |
| Views ........                                                               |
| Description .. Resources that are not OK                                     |
| Last Updated at 15.09.30 on WED 29-MAY-2013 by USER01                        |
'------------------------------------------------------------------------------'
. Filter Expression -----------------------------------------------------------.
|                                                                              |
|                                                 D=Delete I=Insert R=Repeat  |
|      "(" Field              Opr Value                         Gen ")" Bool  |
|          LOGSTAT            ¬=  OK                                          |
|     **END**                                                                 |
```

The filter expression causes a Status Monitor to display only resources that have a logical state that is not OK.

How You Define the Status Monitor Filter Expression

Use the Filter Expression window on the Status Monitor Filter panel to specify the Boolean expression that defines the filter. The expression uses resource attributes as criteria to determine what to display on the Status Monitor.

To display the list of valid values for a field, enter a question mark (?) in the field.

The following action codes helps you enter the expression:

D

Deletes the selected line.

I

Inserts a blank line after the selected line.

R

Repeats a selected line.

Maintenance of Status Monitor Filter Definitions

You can browse, update, copy, and delete filter definitions from the Status Monitor Filter List panel.

If the Filter Expression window does not fully display the Boolean expression while you are browsing a definition, press F12 (Max) to expand the window.

Chapter 8: Customizing the Status Monitor Display Format

This section contains the following topics:

Status Monitor Display Formats

A status monitor display format determines what information is displayed on the status monitor.

Default formats are supplied. You can modify the default formats or can set up other formats to suit your requirements.

From a web browser, users can select a defined format through Options when viewing the status monitor.

Note: In a multisystem environment, the definitions that are created or customized *after* the regions are connected are synchronized and available across all connected regions.

Create a Status Monitor Display Format

You can create format definitions to customize what information is displayed on the status monitor.

Follow these steps:

1. Enter **/FORMATS** at the prompt.

   A list of the status monitor formats appears.

2. Press F4 (Add).

   The List Description panel appears.

   Note: You can also use the C action code to open a copy of an existing display format definition that you can modify.

3. Complete the fields as required.
4. Press F8 (Forward).

   The List Format panel appears. The panel provides a text editor window.

5. By using the text editor, enter column headings and variables to specify the information to display on the status monitor.
6. Press F3 (File).

   The format is created.

Specify the Status Monitor Display Format

Specify the status monitor display format on the List Format panel.

For each type of information you want to display on the status monitor, specify a static heading and a variable that contains the required information.

Follow these steps:

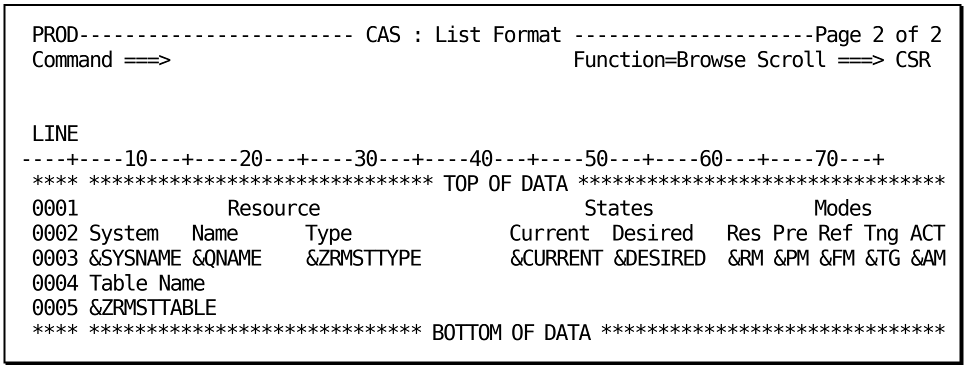
1. From the List Format panel, specify the headings. A heading can be up to ten lines. These lines are known as heading lines.
2. Specify the corresponding variables beneath the heading lines. Specify the variables in a single line, which is known as an entry line.

   If the name of a variable is longer than the data to be displayed, create a shorter alias for the name.

Note: Each line has a limit of 75 characters. If you require more characters, you can extend the heading-entry combination over subsequent lines. You can have up to ten such heading-entry line combinations.

Example: Definition for a Display Format

This example contains two heading-entry line combinations.



```
 PROD------------------------ CAS : List Format ---------------------Page 2 of 2
 Command ===>                                   Function=Browse Scroll ===> CSR


 LINE
----+----10---+----20---+----30---+----40---+----50---+----60---+----70---+
 **** ****************************** TOP OF DATA ********************************
 0001             Resource                       States              Modes
 0002 System   Name      Type              Current  Desired   Res Pre Ref Tng ACT
 0003 &SYSNAME &QNAME    &ZRMSTTYPE        &CURRENT &DESIRED  &RM &PM &FM &TG &AM
 0004 Table Name
 0005 &ZRMSTTABLE
 **** ***************************** BOTTOM OF DATA ******************************
```

Status Monitor Headings

A heading describes the information being displayed under it. Type the headings as you would like them to appear on the status monitor. A heading can contain up to 10 lines of text.

Status Monitor Variables

The variable contains the information that you want to display. You can use the following variables: &ZRMST*rdf_column*.

rdf_column

Is the name of a column in Relational Data Framework that CA OPS/MVS provides.

Note: For other variables, press F1 (Help) on the List Format panel.

Create Shorter Aliases for Variable Names

The name of a variable can sometimes be longer than the displayed data. You can enter a shorter name and then make that shorter name an alias of the actual name.

To create aliases to variable names

1. From the List Format panel, press F5 (Fields).

   The List Entry Line Fields panel appears.

2. The Entry Line Field column contains the variable name you specified in the display format. Type the corresponding real variable name under the Real Field heading.

3. After you have created the aliases, you can perform one of the following actions:

   - If you want to save the format and exit the format definition panels, press F3 (File).
   - If you want to save the format and remain on the List Entry Line Fields panel, press F4 (Save).
   - If you want to return to the List Format panel, press F5 (Format).

Chapter 9: User Profiles

This section contains the following topics:

General Description

The user profiles set user preferences and tailoring options. The profiles set the working environment for a user.

- At one level, user profiles contain default settings for the operational environment. Users can update their own profiles, and the system administrator can update any user profile.
- At the next level, the defaults that are set in the user profile record determine the specific environments that a user sees. A user can, however, change those defaults for a work session.

Note: In a multisystem environment, the definitions that are created or customized *after* the regions are connected are synchronized and available across all connected regions.

Define User Profiles

The user profile controls what information a user sees on monitors.

Follow these steps:

1. Enter the **/SSADMIN** panel shortcut.

   The Automation Services : Administration Menu appears.

2. Select the option, **UP** - User Profiles.

   The User Profile List appears.

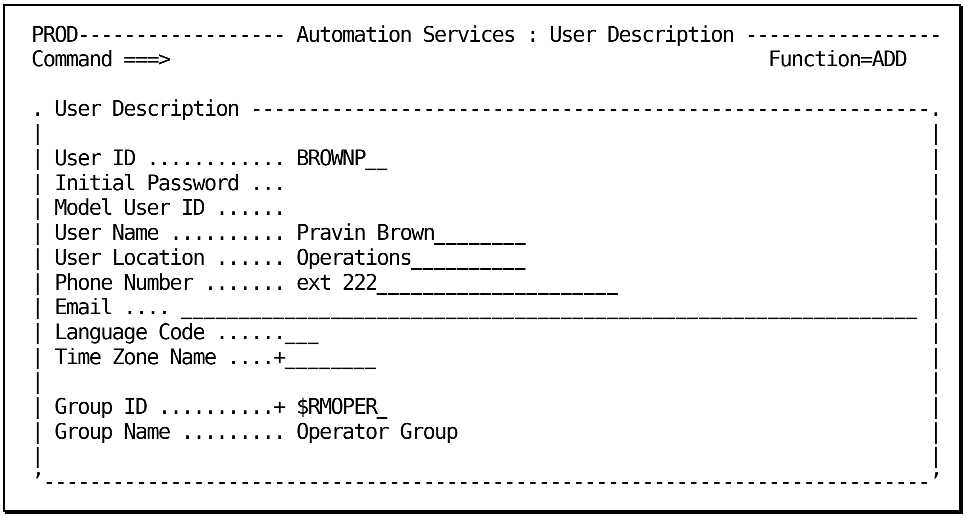
3. Press F4 (Add) to add a user profile. The action presents you with the first panel in the user profile definition. The following sections describe some of the panels. Use F8 (Forward) to scroll to each new panel.

4. File or save the new record.

Note: When you have defined one user profile, you can use the **C** (Copy) action to duplicate an existing user profile. You can then change the values for another user in the copied record as required.

User Details

You can specify the user details by using the User Description panel. These details are the same as those details in the user ID definition.



```
PROD----------------- Automation Services : User Description -----------------
Command ===>                                                   Function=ADD

. User Description ----------------------------------------------------------.
|                                                                            |
| User ID ............ BROWNP__                                              |
| Initial Password ...                                                       |
| Model User ID ......                                                       |
| User Name .......... Pravin Brown________                                  |
| User Location ...... Operations__________                                  |
| Phone Number ....... ext 222_____________________                          |
| Email .... _______________________________________________________________ |
| Language Code ......___                                                    |
| Time Zone Name ....+________                                               |
|                                                                            |
| Group ID ..........+ $RMOPER_                                              |
| Group Name ......... Operator Group                                        |
|                                                                            |
'----------------------------------------------------------------------------'
```

Primary Menu Format Control

You can customize the Primary Menu for a user by using the Primary Menu Format Control panel.

The panel enables you to specify defaults for the format of the Primary Menu.

Alert Monitor Display

You can customize the default Alert Monitor display for a user by using the Alert Monitor Profile panel.

The panel enables you to specify the following defaults:

- Alert Monitor filter that restricts the displayed alerts (You can define the filters at the Filter Definition List panel. To access the list, enter **/ALFILT**.)
- Alert sort criteria to be applied when the user accesses the Alert Monitor

Resource Monitor Display

You can customize the resource monitor display for a user by using the Resource Monitor Profile panel.

The following information affects the monitor:

- Resource monitor filter
- Display format
- Sort criteria

User Profile Maintenance

User profile records are maintained by applying actions to items on the User Profile list. You can update, copy, or delete listed profile records.

Update User Profiles

From Administration Menu, you can update a user profile.

Follow these steps:

1. Enter the **/SSADMIN.UP** panel path.

   The defined user profiles are listed.

2. Apply the **U** (Update) action to the item you want to update.

   The Panel Display List panel is displayed.

3. Select the panel that you want to update.

4. Update the fields on this panel as required. If you want to update further fields on other user profile panels, use the following function keys:

   - F7 (Backward) and F8 (Forward) to move between panels
   - F11 (Menu) to return to the Panel Display List

5. File (F3) the updated definition.

Note: You can customize parts of your own user profile from certain associated panels. For example, you can customize your resource monitor profile from the status monitor by using the PROFILE command.

Users can overwrite their profiles.

Delete a User Profile Definition

To delete a user profile record *and* its associated security record, apply the **D** (Delete) action to that item on the User Profile list.

To delete the user profile record while retaining the security record, apply the **DP** (Delete Profile) action.

Appendix A: Health Checks

This section contains the following topics:

CA Health Checker

The CA Health Checker provides a simple and consistent method for CA Technologies products to create health checks to run under the IBM Health Checker for z/OS. The IBM Health Checker helps you identify potential problems in your z/OS environment by checking system or product parameters and system status against recommended settings. WebCenter health checks are automatically activated on the target system when the product is started on a system with IBM Health Checker installed and configured.

The CHECK_OWNER for all WebCenter health checks is CA_OPSMVS.

Use either CA SYSVIEW or SDSF Health Checker displays to list and view the checks. View health check messages in the MVS System Log.

OPSMVS_WEB_ACB

Description

This WebCenter health check checks that the primary ACB of the region is open. This check runs every 5 minutes.

Best Practice

VTAM is required to access the 3270 interface. If you primarily use the WebCenter web interface to access you region, you can lower the priority of this health check.

Parameters accepted

None.

Debug Support

No.

Verbose Support

No.

Reference

None.

Non-exception Messages

The following messages can appear in the health checker:

- This region's primary ACB, *acbname*, is open.
- The region is shutting down. Check is not relevant at this time.

Exception Messages

If an exception occurs, the following messages are issued as WTOs and written to the SYSLOG:

- CAH0001E The check timed out while waiting for a response to a command.
- NMH0106E This region's primary ACB, *acbname*, is not open.

OPSMVS_WEB_INITIALIZE

Description

This WebCenter health check checks region initialization. The check runs once at region startup. If an exception occurs, the check repeats every 5 minutes.

Best Practice

To set up your region, follow the Install Utility procedures in the *Installation Guide* and ensure that the parameters are specified correctly.

Parameters Accepted

None.

Debug Support

No.

Verbose Support

No.

Reference

See the online help for region parameter groups.

Non-exception Messages

The following messages can appear in the health checker:

- The region has initialized successfully.
- The region is initializing. Check is not relevant at this time.
- The region is shutting down. Check is not relevant at this time

Exception Messages

If an exception occurs, the following messages are issued as WTOs and written to the SYSLOG:

- CAH0001E The check timed out while waiting for a response to a command.
- NMH0104E Initialization errors have occurred in region *regionname*.

OPSMVS_WEB_SOCKETS

Description

This WebCenter health check checks that the sockets are available to support the IP connections. The check runs every 15 minutes.

Best Practice

To ensure the IP connections, the port number for the connection must be specified and not in use by another task.

Parameters Accepted

None.

Debug Support

No.

Verbose Support

No.

Reference

None.

Non-exception Messages

The following messages can appear in the health checker:

- Sockets are configured and active. HTTP port is *nnnn* URL is http://*nnn.nnn.nnn.nnn:nnnn*
- The region is initializing. Check is not relevant at this time.
- The region is shutting down. Check is not relevant at this time

Exception Messages

If an exception occurs, the following messages are issued as WTOs and written to the SYSLOG:

- CAH0001E The check timed out while waiting for a response to a command.
- NMH0110E TCP/IP interface is not active, status is *cccccccc*.
- NMH0111E No port number has been specified for this region.

OPSMVS_WEB_SSI

Description

This WebCenter health check checks that the SOLVE SSI SSID is defined and connected. The check runs every 15 minutes.

Best Practice

Ensure that the following conditions are met:

- The SSI started task is active.
- The SSI SSID value for the region matches the SSID= parameter for the SSI started task.

Parameters Accepted

None.

Debug Support

No.

Verbose Support

No.

Reference

None.

Non-exception Messages

The following messages can appear in the health checker:

- SOLVE SSI SSID correctly defined and connected. SSID is *ssidname*.
- The region is initializing. Check is not relevant at this time.
- The region is shutting down. Check is not relevant at this time.

Exception Messages

If an exception occurs, the following messages are issued as WTOs and written to the SYSLOG:

- CAH0001E The check timed out while waiting for a response to a command.
- NMH0108E SSID error, no SSID specified.
- NMH0108E SSID error, *ssidname* is not connected.
- NMH0108E SSID error, SSID matches AOM SSID(*ssidname*).

OPSMVS_WEB_WEB_PORT

Description

This WebCenter health check checks that the WebCenter web interface is available. This check runs every 15 minutes.

Best Practice

Set up the region parameter groups by following the *Installation Guide*. During the process, specify the web interface port.

Parameters Accepted

None.

Debug Support

No.

Verbose Support

No.

Reference

None.

Non-exception Messages

The following messages can appear in the health checker:

- The region is initializing. Check is not relevant at this time.
- The region is shutting down. Check is not relevant at this time.
- The WebCenter interface is active. HTTP port is *nnnn* URL is http://*nnn.nnn.nnn.nnn:nnnn*

Exception Messages

If an exception occurs, the following messages are issued as WTOs and written to the SYSLOG:

- CAH0001E The check timed out while waiting for a response to a command.
- NMH0113E The WebCenter interface is not [active | configured].

Glossary

activity log

The *activity log* is a VSAM repository for recording messages. It is a data set that contains information about region activities, such as error message details, event processing details, process activities, and compiler messages. It can be either online or in hardcopy format, and is controlled by the LOGFILES parameter group.

alert

Alerts provide the proactive notification of events.

Customizer

Customizer is a facility that helps you set up your region parameters using parameter groups.

Customizer parameter group

A *Customizer parameter group* is a group of parameters that are set through a panel sequence to define a subcomponent of region configuration.

domain ID

A *domain ID* is a 1- to 4-character mnemonic used as a unique region identifier.

generic name

Name in which an asterisk (*) is used to stand for any character.

health checker

The health checker runs under the IBM Health Checker for z/OS. The health checks identify potential problems by checking system parameters, product parameters, and system status against recommended settings.

Inter-Network Management Connection (INMC)

Inter-Network Management Connection (INMC) is a facility that provides general-purpose data transfer between regions.

knowledge base

The *knowledge base* is a database used to store the policies and procedures that govern the operation of your region. It is also known as RAMDB.

link

A term used to describe a logical connection between two peer communications systems.

LMP key

The *LMP key* is used by the CA License Management Program for CA product license authorization.

NMINIT

The NCL procedure automatically executed after system initialization has completed. It cannot contain commands that require VTAM facilities as it is executed before the primary ACB is opened. The procedure name can be changed by the installation.

NMREADY

The NCL procedure automatically executed once system initialization has completed. It can contain commands that require VTAM facilities as it is executed after the primary ACB is opened. Procedure name can be changed by the installation.

panel skip

The ability to chain menu selection requests together without having to display intermediate selection panels.

parameter group

A *parameter group* contains parameters that determine the characteristics of a region. See also Customizer (see page 51).

Primary Menu

The first menu of an application.

PSM (Print Services Manager)

PSM is a facility that simplifies the control of the physical printing of reports on JES or network printers.

resource

Resources are defined to a region as part of a system image. The information is derived from the resource data that is held in the active CA OPS/MVS Relational Data Framework (RDF) resource tables.

shortcut

A *shortcut* is a direct jump to a panel . A shortcut is entered from the prompt as:

- */shortcut-name* to retain the current panel on return.
- =/*shortcut-name* to close the current panel and return to the primary menu on exit.

SOLVE SSI

SOLVE SSI is an implementation of IBM's Subsystem Interface (SSI) that allows product regions to communicate with other software on a system.

status monitor

The status monitor lets you monitor and control individual resources. The monitor displays resource statuses in line-by-line mode. These statuses are color-coded to alert an operator to changes in resource status. Changes in color are governed by changes to the logical state of a resource.

status monitor filter

A Boolean expression that determines which resources are to be displayed on the status monitor. For example, an operator may use a filter that only displays the printers in a system image.

variable

A variable is used to store data that can change. A variable is represented by a word that starts with an ampersand (&), followed by the name of the variable. For example, &A is a variable where A is the name. When &A is processed, it is replaced by the stored value.

VFS (Virtual File System)

The VSAM data set used as a database to configure a region.

wildcard

The term used to describe the character used (usually an asterisk) when defining resources generically-no specific matching character is required in the wildcard character position.

Index