Dell EMC Events and Alerts for PowerMax and VMAX

Version 9.1

User Guide

REV 1

September 2019

DELLEMC

CONTENTS

Chapter 2 **Asynchronous Events** **41**

Contents

TABLES

Tables

Preface

As part of an effort to improve its product lines, Dell EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your Dell EMC representative if a product does not function properly or does not function as described in this document.

(i) **Note:** This document was accurate at publication time. New versions of this document might be released on Dell EMC Online Support (https://www.dell.com/support/home). Check to ensure that you are using the latest version of this document.

Purpose

This manual lists the alerts and events generated by SYMAPI server daemon, the event daemon, and symcli commands.

Related documentation

The following documents provide information about Solutions Enabler:

Dell EMC Solutions Enabler, VSS Provider, and SMI-S Provider Release Notes

　　Describes new features and any known limitations.

Dell EMC Solutions Enabler Installation and Configuration Guide

　　Provides host-specific installation instructions.

Dell EMC Solutions Enabler CLI Reference Guide

　　Documents the SYMCLI commands, daemons, error codes and option file parameters provided with the Solutions Enabler man pages.

Dell EMC Solutions Enabler Array Controls and Management CLI User Guide

　　Describes how to configure array control, management, and migration operations using SYMCLI commands for arrays running HYPERMAX OS and PowerMaxOS.

Dell EMC Solutions Enabler Array Controls and Management CLI User Guide

　　Describes how to configure array control, management, and migration operations using SYMCLI commands for arrays running Enginuity.

Dell EMC Solutions Enabler SRDF Family CLI User Guide

　　Describes how to configure and manage SRDF environments using SYMCLI commands.

SRDF Interfamily Connectivity Information

　　Defines the versions of PowerMaxOS, HYPERMAX OS and Enginuity that can make up valid SRDF replication and SRDF/Metro configurations, and can participate in Non-Disruptive Migration (NDM).

Dell EMC Solutions Enabler TimeFinder SnapVX CLI User Guide

　　Describes how to configure and manage TimeFinder SnapVX environments using SYMCLI commands.

Dell EMC Solutions Enabler SRM CLI User Guide

Provides Storage Resource Management (SRM) information related to various data objects and data handling facilities.

Dell EMC SRDF/Metro vWitness Configuration Guide

Describes how to install, configure and manage SRDF/Metro using vWitness.

Dell EMC Events and Alerts for PowerMax and VMAX User Guide

Documents the SYMAPI daemon messages, asynchronous errors and message events, SYMCLI return codes, and how to configure event logging.

The following documents provide information about Unisphere:

EMC Unisphere for VMAX Release Notes

Describes new features and any known limitations for Unisphere for VMAX .

EMC Unisphere for VMAX Installation Guide

Provides installation instructions for Unisphere for VMAX.

EMC Unisphere for VMAX Online Help

Describes the Unisphere for VMAX concepts and functions.

EMC Unisphere for VMAX Performance Viewer Online Help

Describes the Unisphere for VMAX Performance Viewer concepts and functions.

EMC Unisphere for VMAX Performance Viewer Installation Guide

Provides installation instructions for Unisphere for VMAX Performance Viewer.

EMC Unisphere for VMAX REST API Concepts and Programmer's Guide

Describes the Unisphere for VMAX REST API concepts and functions.

EMC Unisphere for VMAX Database Storage Analyzer Online Help

Describes the Unisphere for VMAX Database Storage Analyzer concepts and functions.

EMC Unisphere 360 for VMAX Release Notes

Describes new features and any known limitations for Unisphere 360 for VMAX.

EMC Unisphere 360 for VMAX Installation Guide

Provides installation instructions for Unisphere 360 for VMAX.

EMC Unisphere 360 for VMAX Online Help

Describes the Unisphere 360 for VMAX concepts and functions.

The following provide additional information:

EMC VMAX3 Family Product Guide for VMAX 100K, VMAX 200K, VMAX 400K with HYPERMAX OS

Provides product information regarding the purchase of a VMAX3 Family 100K, 200K, 400K.

Dell EMC VMAX3 Family Site Planning Guide for VMAX 100K, VMAX 200K, VMAX 400K with HYPERMAX OS

Provides planning information regarding the purchase and installation of a VMAX3 Family 100K, 200K, 400K.

EMC VMAX All Flash and VMAX3 Family Security Configuration Guide

Describes how to securely deploy a VMAX3 Family (100K, 200K, 400K) or VMAX All Flash (250F, 450F, 850F, 950F) array with HYPERMAX OS.

Dell EMC VMAX All Flash Product Guide for VMAX 250F, 450F, 850F, 950F with HYPERMAX OS

Provides product information regarding the purchase of a VMAX 250F, 450F, 850F, 950F with HYPERMAX OS.

Dell EMC VMAX All Flash Site Planning Guide for VMAX 250F, 450F, 850F, 950F with HYPERMAX OS

Provides planning information regarding the purchase and installation of a VMAX 250F, 450F, 850F, 950F with HYPERMAX OS.

EMC VMAX All Flash and VMAX3 Family Security Configuration Guide

Describes how to securely deploy a VMAX3 Family (100K, 200K, 400K) or VMAX All Flash (250F, 450F, 850F, 950F) array with HYPERMAX OS.

E-Lab™ Interoperability Navigator (ELN)

Provides a web-based interoperability and solution search portal. You can find the ELN at https://elabnavigator.EMC.com.

Special notice conventions used in this document

Dell EMC uses the following conventions for special notices:

⚠ **DANGER** Indicates a hazardous situation which, if not avoided, will result in death or serious injury.

⚠ **WARNING** Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

⚠ **CAUTION** Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

ⓘ **NOTICE** Addresses practices not related to personal injury.

ⓘ **Note:** Presents information that is important, but not hazard-related.

Typographical conventions

Dell EMC uses the following type style conventions in this document:

Table 1 Typographical conventions used in this content

Bold	Used for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)
Italic	Used for full titles of publications referenced in text
Monospace	Used for: • System code • System output, such as an error message or script • Pathnames, filenames, prompts, and syntax • Commands and options
Monospace italic	Used for variables
Monospace bold	Used for user input
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections - the bar means "or"

Table 1 Typographical conventions used in this content (continued)

| { } | Braces enclose content that the user must specify, such as x or y or z |
| ... | Ellipses indicate nonessential information omitted from the example |

Where to get help

Dell EMC support, product, and licensing information can be obtained as follows:

Product information

Dell EMC technical support, documentation, release notes, software updates, or information about Dell EMC products can be obtained at https://www.dell.com/support/home (registration required) or https://www.dellemc.com/en-us/documentation/vmax-all-flash-family.htm.

Product information

For documentation, release notes, software updates, or information about Dell EMC products, go to Dell EMC Online Support at https://www.dell.com/support/home.

Product information

For documentation, release notes, software updates, or information about Dell EMC products, go to Dell EMC Online Support at https://www.dell.com/support/home or the CloudArray portal at https://www.cloudarray.com.

Technical support

To open a service request through the Dell EMC Online Support (https://www.dell.com/support/home) site, you must have a valid support agreement. Contact your Dell EMC sales representative for details about obtaining a valid support agreement or to answer any questions about your account.

Technical support

Dell EMC offers a variety of support options.

- Support by Product — Dell EMC offers consolidated, product-specific information on the Web through the Dell EMC Online Support site.
  The Support by Product web pages (https://www.dell.com/support/home then select **Product Support**) offer quick links to Documentation, White Papers, Advisories (such as frequently used Knowledgebase articles), and Downloads, as well as more dynamic content, such as presentations, discussion, relevant Customer Support Forum entries, and a link to Dell EMC Live Chat.

- Dell EMC Live Chat — Open a Chat or instant message session with an Dell EMC Support Engineer.

Technical support

For technical support, go to Dell EMC Online Support https://www.dell.com/support/home. To open a service request, you must have a valid support agreement. Please contact your Dell EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

eLicensing support

To activate your entitlements and obtain your VMAX license files, visit the Service Center on Dell EMC Online Support (https://www.dell.com/support/home), as directed on your License Authorization Code (LAC) letter emailed to you.

- For help with missing or incorrect entitlements after activation (that is, expected functionality remains unavailable because it is not licensed), contact your Dell EMC Account Representative or Authorized Reseller.

- For help with any errors applying license files through Solutions Enabler, contact the Dell EMC Customer Support Center.

- If you are missing a LAC letter, or require further instructions on activating your licenses through the Online Support site, contact Dell EMC's worldwide Licensing team at licensing@emc.com or call:

  - North America, Latin America, APJK, Australia, New Zealand: SVC4EMC (800-782-4362) and follow the voice prompts.

  - EMEA: +353 (0) 21 4879862 and follow the voice prompts.

SolVe Online and SolVe Desktop

SolVe provides links to customer service documentation and procedures for common tasks. Visit https://solveonline.emc.com/solve/products, or download the SolVe Desktop tool from https://www.dell.com/support/home and search for SolVe Desktop. From SolVe Online or SolVe Desktop, load the *PowerMax and VMAX* procedure generator.

ⓘ **Note:** You need to authenticate (authorize) the SolVe Desktop tool. After it is installed, familiarize yourself with the information under **Help**.

Documentation within the Symmetrix Procedure Generator

The following Dell EMC procedural documentation is available in the Symmetrix Procedure Generator.
The following Dell EMC procedural documentation is available in the Symmetrix Procedure Generator.

For information regarding the Symmetrix Procedure Generator, see: http://www.corkc4.isus.emc.com/wiki/index.php/Symmetrix_Procedure_Generator

- Pre-Hardware Install Checklist

- Post-Hardware Install Checklist

Your comments

Your suggestions help us improve the accuracy, organization, and overall quality of the documentation. Send your comments and feedback to: VMAXContentFeedback@emc.com

Revision history

Provides a description of document changes.

Table 2 Revision history

Revision	Description and/or change
1	Initial revision of the VMAX Management Software Events and Alerts Guide for the V9.1 release.

CHAPTER 1

SYMAPI Server Daemon Messages

This chapter describes the log messages issued by the SYMAPI server daemon (`storsrvd`):

Message format

This section describes messages that are written to the SYMAPI server log and to the system console in z/OS. All messages begin with a message identifier, followed by message text.

The message is in this format:

```
yyyy/mm/dd hh:mm:ss pid thread_name log_category msgid text
```

where:

`yyyy/mm/dd`	Is the date the message was issued.
`hh:mm:ss.xxx`	Is the time the message was issued in hours, minutes, seconds, and milliseconds.
`pid`	Is the process ID of the issuing process.
thread_name	Is the thread name of the issuing thread.
`log_category`	Is the category specified in the `storsrvd:log_filter` statement in the `daemon_options` file, which caused this message to be generated. The valid categories are: SERVER, SESSION, CONTRO, and APIREQ.
`msgid`	Is made up of the following: `ANR` — Indicates the server issued the message. *nnnn* — A numeric identifier for the message. *X* — A one byte severity indicator. Valid values are: • `I` indicates an Informational message • `W` indicates a Warning message • `E` indicates an Error message • `S` indicates a severe condition requiring a message

text	Is the message text.

In this section, each message shows the text of the message with indicators where substitutions are made into the text at runtime. Following the text are four paragraphs giving more information:

- **Set Step Return Code** — In a z/OS environment, some messages will cause the SYMAPI server job step return code to be set to a non-zero value. The following table shows the correlation of message severity to job step return code. Some messages are issued by multiple locations in the code. Not all uses of the message will cause the step return code to be set.

Message identifier	Return codes
I	0
W	4
E	8
S	12

  If multiple messages are issued that cause the step return code to be set, the highest value will be remembered by the server, and returned to the system at job termination.

- The **Destination** of the message — `Log` and/or `Console` is shown. Most messages are written to the server log file. Some messages are written to both the log and console, but not in all cases where the message is generated. Some messages are written to the system console only, particularly those related to operator command processing. The Console destination applies only to z/OS.

- The **Description** paragraph explains the circumstances that cause the message to be issued, and explains each substituted value. This section also describes any action that the Solutions Enabler software will take.

- The **Operator Action** paragraph suggests operator intervention actions where needed.

storsrvd log files

The server writes data to its log files provided by the common daemon infrastructure. These log files are named and handled in a manner consistent with other daemon log files. For example, under the default log management behavior, the files `storsrvd.log0` and `storsrvd.log1` are created in `/var/symapi/log`.

The behavior of the log files is subject to the standard daemon options: `logfile_type`, `logfile_size`, `logfile_perms` and `logfile_retention`. Thus, you can configure the logs as dated files with retention controls instead of the common wrapping pair of log0 and log1. The same rules apply to `storsrvd` as to all other daemons.

Numbered messages issued by storsrvd

The SYMAPI server application-level messages are distinguished from messages issued by the Solutions Enabler common daemon support by the use of a messages identifier.

The following `daemon_options` file keywords affect the appearance of the `storsrvd` messages:

- `log_show_category` displays or suppresses the category (also known as the filter) that applies to a message.

- `log_show_msgid` displays or suppresses the message identifier in the message.

Messages

ANR0000I

text

Destination: Log and console.

Description: This message is a general purpose message to be used for any arbitrary *text*.

Operator Action: None.

ANR0001I

SYMAPI Server for z/OS ready to accept *security_level* connections

Destination: Log and console.

Description: This message is issued when initialization is complete and the server is prepared to field connection requests from remote clients. *security_level* indicates the types of sessions the server will accept. Possible values are:

- ONLY NONSECURE — Indicates that client must expect to negotiate non-SSL sessions with the server.
- ONLY SECURE — Indicates that the server will require clients to negotiate a secure session.
- Both SECURE and NONSECURE — Indicates that the server will accept sessions from clients that cannot negotiate secure and will negotiate secure sessions with clients who can.

Operator Action: None.

ANR0002I

shutdown_type Shutdown requested

Destination: Log and console.

Description: This message indicates that a shutdown request was made. See message ANR0003I for the description of *shutdown_type.*

Operator Action: None.

ANR0003I

shutdown_type Shutdown *progress*. Number of sessions remaining = *number*

Destination: Log and console.

Description: This message is issued at the start of the shutdown process. *shutdown_type* indicates NORMAL, IMMEDIATE, or STOPPED-NORMAL.

In open systems environments, shutdown is requested by the `stordaemon` command.

In Microsoft Windows, you can use the Service Control Manager; in this case the shutdown process will always be IMMEDIATE.

In a z/OS environment, the system operator will request a NORMAL shutdown using the z/OS `STOP` command or the `SHUTDOWN` command.

The number of currently active sessions is shown in *number*. If this value is not 0, the following rules apply:

- If the *shutdown_type* is NORMAL, the server will wait for the active sessions to end. In this case, *progress* indicates *starting* or *in progress*. Each time a session ends, the *in progress* status will be reported.

- If the *shutdown_type* is IMMEDIATE, the server terminates without waiting for active sessions to end. See the description of the SHUTDOWN command for more details on when to use IMMEDIATE shutdown.

Operator Action: None.

ANR0004I

SYMAPI Server running as a started task

Destination: Log.

Description: In a z/OS environment, the server detects when it is running as a started task (running in *STC mode*). This message serves as a visual confirmation that STC mode is active.

Operator Action: None, unless this is not what is intended.

ANR0005E

Normal shutdown failed, attempting immediate shutdown

Set Step Return Code

Destination: Log and console.

Description: The server attempted to perform a normal shutdown, waiting for active sessions to complete. The normal shutdown process failed, and no recovery was possible. An immediate shutdown was attempted, because there is no other possible recovery action to take.

Operator Action: Be aware that the list of connections noted in message ANR0013I on page 21 are terminated before they are able to disconnect.

ANR0006E

Wait returned without connection or console command ready, console ECB contents *value*

Destination: Log.

Description: The server waits for incoming connection requests and instructions from the operator concurrently. If the wait is somehow satisfied but neither of these events occurred, it is considered an error. The server will continue to wait for new events.

Operator Action: This is an abnormal situation and may indicate some error in TCP communications or management of the operator console. If this happens repeatedly, shut the server down and try restarting the server. If the problem persists, examine your system for evidence of other problems in the TCP or console management components of your system.

ANR0008I

Server socket *socket:_event* occurred

Destination: Log.

Description: This message is issued to confirm that connection request has arrived, or that some error condition has been reflected to the TCP socket on which the server is listening. The value of *socket_event* will be *connection request* or *exception condition*.

Operator Action: If the *socket_event* is *connection request* no action is necessary since this is a documentation message, and may aid in problem diagnosis. See the description of message ANR0009E on page 20, if the *socket_event* is *exception condition*.

ANR0009E

Exceeded maximum exceptions on server socket, indicating PORT_EXCEPTION

Set Step Return Code

Destination: Log and console.

Description: This is issued after an exception condition has been raised (which may cause the issuing of ANR0008I). Currently, the maximum exception count is 1, meaning that there is no retry strategy when an exception occurs on the socket on which the server is listening. The server will stop listening and start a NORMAL shutdown when it notices this condition.

Operator Action: If *exception condition* in message ANR0008I on page 19 is indicated, there will be other evidence in your system log showing TCP/IP problems. Refer to documentation from your TCP software provider to resolve the problems you find. When the problems are resolved, you can restart the server.

ANR0010I

SYMAPI Server Shutdown complete

Destination: Log and console.

Description: The server has completed its shutdown process and will return to the operating system.

Operator Action: None. This should serve as a visual confirmation that the server is finished.

ANR0011W

SYMAPI Server not executing from an APF-authorized library, cannot continue

Set Step Return Code

Destination: Log and console.

Description: In a z/OS environment, the SYMAPI server program `storsrvd` must execute from a library authorized by the z/OS Authorized Program Facility, if the base daemon is not in use. The server checks to make sure that this condition is met. This message is issued as a warning , but an error condition may not be reflected until a SYMAPI session requests storage discovery services.

Operator Action: The Solutions Enabler load library can be authorized through APF in several ways. You can use the SETPROG APF command to authorize the library temporarily. In order to make the library authorized at subsequent IPLs, you must edit the PROGxx member of SYS1.PARMLIB. Refer to the IBM documentation for your level of z/OS for exact syntax and editing instructions.

ANR0012I

Accepted *seclevel* session *session_number* from *IP_address* on thread *thread_number*

Destination: Log.

Description: The server successfully handled a connection request for a session, and started a thread to process API requests for the session. The session number is shown in *session_number* and it is being processed on a thread with the number *thread_number*. The session is running from a client program executing on the host at address *IP_address*. *seclevel* indicates the negotiated security level of the session. If *seclevel* is SECURE, transmission is protected using SSL; if *seclevel* is NONSECURE, SSL protection is not in use.

Operator Action: None necessary. This message is documenting the start of a session. You should also see ANR0017I on page 21 at the end of the session.

ANR0013I

Shutdown will wait for client session *session_number* from *IP_address* to terminate itself

Destination: Log and console.

Description: During a normal shutdown, the server will wait for all active sessions to terminate on their own. For each session still active, the server issues this message and will wait for the session(s) to end. The substitution variables are the same as those in message ANR0012I on page 20.

Operator Action: None usually. If sessions are taking an excessive amount of time to complete, you can reissue the shutdown command with the IMMEDIATE operand to terminate the session immediately.

ANR0014W

Terminating client session *session_number* to *IP_address* on Tid *thread_identifier* },

Destination: Log and console.

Description: During an immediate shutdown, the server will report on all active sessions at the time the shutdown process begins. For each session still active, the server issues this message as a note to the operator to indicate which sessions will be terminated end. The substitution variables are the same as those in message ANR0012I on page 20.

Operator Action: None.

ANR0015E

Session broken by dispatcher return value *return_value*, '*message*'.

Destination: Log.

Description: This message is issued when a session is prematurely ended due to an unrecoverable error detected by the server API dispatching layer. When such an error is raised, the SYMAPI client will experience an 'connection aborted' error. The *return_value* and *message* are intended for Dell EMC Customer Service to diagnose the cause of the error.

Operator Action: Collect diagnostic data as directed by Dell EMC Customer Service.

ANR0016I

SYMAPI listener thread is running on thread *thread_number*

Destination: Log.

Description: This message is issued during startup simply to report the thread number (*thread_number*) of the SYMAPI listener thread (the server thread which listens for new connection requests).

Operator Action: None.

ANR0017I

Ending session *session_number,* total requests executed *total_requests*

Destination: Log.

Description: See also message ANR0012I on page 20. This message documents the end of a session. The total number of API requests executed on the session is shown by *total_requests*.

Operator Action: None.

ANR0018E

Rejecting session *session_number* for *user_name@node: reason*

Destination: Log.

Description: A remote client attempted to connect to the running server, but is refused the session for one of the following reasons:

- `The trusted host file disallowed a client server connection` — **the nethost file is allocated to the server, and the combination of the node (either host address or IP address) and the optional user identification (user_name) are not specified in the nethost file. The remote client** `SymInit` **call returns** `SYMAPI_C_HOST_FILE_REJECTION`.

- `The trusted host file could not be read` **or** `The trusted host file has a syntax error` — **the nethost file exists, but could not be read or has a syntax error. The client application will receive either** `SYMAPI_C_HOST_FILE_READ_ERROR` **or** `SYMAPI_C_HOST_FILE_SYNTAX`.

- `The maximum number of network connections has been reached on the server` — **the global limit expressed by the** `max_sessions` **option in the** `daemon_options` **file is exceeded. The application will receive** `SYMAPI_C_MAX_SRVR_CONNECTS_EXCEEDED ()`.

Operator Action: In the case of disallowed connections, the remote client user must ask the server administrator for authorization to use the SYMAPI server. The administrator must add the host (and the optional *user_name*) information to the nethost file to authorize the client application. In the case of host file read or syntax error, make sure that the trusted host file is readable or correct the syntax error in the file. Refer to the *EMC VMAX All Flash and VMAX3 Family Security Configuration Guide* for the syntax of the nethost file. In the case of max connection error, the server administrator may wish to set `max_sessions` to a higher value, or the client application may have to be scheduled when the server is less busy.

ANR0019E

SYMAPI client directed debugging is disabled

Destination: Log and console.

Description: The SYMAPI server initialization process attempts to prepare for client supplied debugging settings when client sessions specify them. Invocation of an internal service failed which prevents the future use of debugging settings from client applications.

This message is preceded by ANR0200E on page 34 which documents the reason for the failure to setup for client debugging.

Operation Action: The output of the preceding message ANR0200E on page 34 gives an indication of the type of failure that is the cause of this situation. Collect and provide documentation as directed by Dell EMC Customer Support.

ANR0020I

SYMAPI server listening on port *port_number* over *protocols*

Destination: Log and console.

Description: This message is issued in conjunction with message ANR0001I on page 18 to inform the system operator about the port (*port_number*) and internet protocols over which the server is communicating. Possible values for *protocols* are:

- IPv4 ONLY — Indicates that the server is listening for connections only using IPv4. Clients that expect an IPv6 connection will fail connecting to the server.

- IPv6 and IPv4 — Indicates that the server is listening explicitly for connections using IPv6 and IPv4.
- IPv6 with IPv4 mapping — Indicates that the IPv6 protocol supports connections from clients who are running either IPv4 or IPv6.

Operator Action: None.

ANR0021I

The current working directory is *directory*

Destination: Log.

Description: This message is issued early in server initialization after the server process attempts to make the SYMAPI database directory the current working directory.

Operator Action: None. This is an informational message.

ANR0022I

SYMAPI server is running on a VMAX Service Processor, forcing port *port*

Destination: Log.

Description: This message is written when the server detects it is running on a VMAX service processor. In this case, the server forces the use of the default port.

Operator Action: None. This is an informational message.

ANR0023I

SYMAPI server Symmwin Pipe Server is initialized

Destination: Log.

Description: This message is written when the special server thread to field requests from the SymmWin component has been started successfully. This will only happen if the server is running on a VMAX service processor.

Operator Action: None. This is an informational message.

ANR0024I

SYMAPI server Enhanced Authentication is ENABLED | DISABLED

Destination: Log and console.

Description: This message is issued during server initialization to indicate Enhanced User Authentication is enabled or disabled.

- ENABLED indicates that if a client sends an authentication message it will be verified.
- DISABLED indicates that if a client sends an authentication message it will not be verified.

Operator Action: On non-Windows hosts, if the authentication mode indicated in the message is not the mode desired, verify that the `/etc/krb5.keytab` file exists, that its permissions indicate that `storsrvd` can access it, and verify that the `klist -k` value in the file shows the correct entry for the host. If the conditions are all correct, turn on high levels of diagnostic logging to look for additional information.

ANR0025E

Rejecting session *session_number* for Host *hostname*: *max_sessions_per_host (limit)* has been reached

Destination: Log.

Description: A remote client attempts to connect to the server, and the server is tracking concurrent sessions per host using the `max_sessions_per_host` configuration option. The current session exceeds the number of concurrent sessions permitted from a specific host. Therefore the session is rejected. `limit` indicates what the current value of `max_sessions_per_host` is and `session_number` is the number of the current session. `hostname` names the host from which the session originates. It may be a simple nodename, a Fully-Qualified Domain Name, or an IP address.

Operator Action: The user of the client application must wait until the number of concurrent sessions from the specific host falls below the limit set by `max_sessions_per_host`, or the server administrator can raise the `max_sessions_per_host` value or disable concurrent user tracking using the stordaemon `setvar storsrvd -name max_sessions_per_host` command. See the *EMC VMAX All Flash and VMAX3 Family Security Configuration Guide* for details on session limits.

ANR0026E

Rejecting session *session_number* for User *user*: *max_sessions_per_user (limit)* has been reached

Destination: Log.

Description: A remote client attempted to connect to the server, and the server is tracking concurrent sessions per user using the `max_sessions_per_user` configuration option. The current session exceeds the number of concurrent sessions permitted from a specific user. Therefore the session is rejected. `limit` indicates the current value of `max_sessions_per_user` and `session_number` is the number of the current session. `user` is the fully-qualified user name as documented in the *EMC VMAX All Flash and VMAX3 Family Security Configuration Guide*.

Operator Action: The user of the client application must wait until the number of concurrent sessions from the specific user falls below the limit set by `max_sessions_per_user`, or the server administrator can raise the `max_sessions_per_user` value or disable concurrent user tracking using the stordaemon `setvar storsrvd -name max_sessions_per_user` command. See the *EMC VMAX All Flash and VMAX3 Family Security Configuration Guide* for details on session limits.

ANR0027E

Rejecting session *session_number* for Host *hostname*: *max_sessions_per_user* is zero.

Destination: Log.

Description: A remote client attempted to connect to the server, and the server is tracking concurrent sessions. Even though max_sessions_per_host may not prevent this session from being initialized, the server detected that `max_sessions_per_user` is set to zero, in which case the session will be refused when the server checks the concurrent sessions allowed per user. Therefore the server rejects the session based on this early detection. *session_number* is the number of the current session, and *hostname* names the host from which the session originates. It may be a simple nodename, a Fully-Qualified Domain Name, or an IP address.

If `max_sessions_per_user` is not set to zero, the concurrent user check is made later in the process, and the session will either be accepted if the session does not exceed the limit set by `max_sessions_per_user`, or refused if it does, in which case the server returns message .

Operator Action: When any of the session limit options `max_sessions`, `max_sessions_per_host`, or `max_sessions_per_user` is set to 0, all new sessions attempting to connect to the host are refused. The server administrator can alter any of the

options or disable concurrent host and user session tracking using the stordaemon `setvar storsrvd -name max_sessions_XXXX` command. See the *EMC VMAX All Flash and VMAX3 Family Security Configuration Guide* for details on session limits.

ANR0030E

Failed to load configuration for *name*

Set Step Return Code

Destination: Log and console.

Description: This message is issued when an error is detected in the loading of the configuration settings for the SYMAPI server daemon. The instance name is the name of the daemon for which configuration was attempted.

Operator Action: Examine the messages that precede this message. A syntax error in the configuration file section for the daemon instance *name* is the most likely cause. For example, the port definition may have specified an invalid number for the port, or an invalid security level may have been specified for the `symapi_security_level` option in the SYMAPI `options` file.

ANR0031E

The security_level (or -seclevel) keyword requires a security level to be specified

Set Step Return Code

Destination: Log.

Description: This `-seclevel` operand was specified without a value on the `stordaemon setvar` command line.

Operator Action: If you specify a security level, you must specify a valid value for the security level through the `stordaemon setvar` command. The valid values are NONSECURE, ANY, and SECURE. No abbreviations are accepted.

ANR0032E

The -log_filter keyword requires list of log filter types to be specified

Set Step Return Code

Destination: Log.

Description: This `-log_filter` operand was specified without a value on the `storsrvd` command line.

Operator Action: If you specify `-log_filter`, you must specify the desired list of filter types. Use the `stordaemon getvar storsrvd -name log_categories` for the list of appropriate filter types.

ANR0033E

The '-port' or 'storsrvd:port' keyword requires a non-zero decimal number less than 65535

Set Step Return Code

Destination: Log.

Description: An invalid value was specified for the SYMAPI server port. If the `storsrvd` command operand **-port** or the `storsrvd:port` statement is used, the value specified for the port must be a non-zero decimal number less 65535. Many port numbers in the lower ranges must also be avoided since they are used by well known processes (for example, the `inetd` and `ftpd` daemons).

Operator Action: Correct the command line or `daemon_options` file specification, and restart the server.

ANR0034I

The port is not reloaded while the server is running, bypassing any new port definition

Destination: Log.

Description: During execution of the `reload` command, a change to the port specification was detected. This message is issued to alert the administrator to the fact that the port definition cannot be changed during the reload operation.

Operator Action: In order to change the port, you must shut down the `storsrvd` process, make the port change, and restart `storsrvd`.

ANR0104E

Command syntax error: *explanation*

Destination: Log and console.

Description: The operator entered a command with invalid syntax explained by `explanation`.

Operator Action: Examine the syntax description for the command you want to enter, and re-enter it with the proper operands.

ANR0105E

Ambiguous or invalid command token entered: *token_text*

Destination: Log and console.

Description: The operator entered a command but either the command verb or a keyword name in *token_text* was misspelled or its abbreviation was too short to uniquely identify the intent.

Operator Action: Examine the syntax description for the command you want to enter, and re-enter it with the proper operands.

ANR0106I

Environment variable *name* has been set to *value*

Destination: Console.

Description: The operator entered the `SETENV` command, and the environment variable was successfully set.

Operator Action: None. This message provides confirmation that the variable was set as intended.

ANR0107E

option is not a valid runtime option

Destination: Log and console.

Description: The operator entered the `setvar` command, but the name of the runtime option (*option*) was not recognized as a valid option.

Operator Action: Examine the description of the `setvar` command for the supported options. Re-enter the command with the desired option. `setvar` accepts the runtime option names with or without the dash prefix.

ANR0108E

value is not a valid value for runtime option *option*

Destination: Log and console.

Description: The operator entered the `setvar` command with the name of a valid runtime option (*option*), but the value (*value*) specified for *option* was not valid.

Operator Action: Examine the description of the `setvar` command for the proper values corresponding to each supported option. Re-enter the command with the corrected value for the desired option.

ANR0110E

Invalid *option* command option name found following successful parse: decimal value is *code_value*

Destination: Console.

Description: This message indicates a programming or environmental error in command parsing and execution. The parsing of the command was successful, but the secondary scan performed by the execution phase found an invalid token.

Operator Action: Collect and provide documentation as directed by Dell EMC Customer Support.

ANR0111I

option runtime option has been set to *value*

Destination: Log and console.

Description: The operator entered the `setvar` command to change the value of the runtime option *option*. The command text was successfully parsed, and the command was executed successfully. The new value of the variable is *value*.

Operator Action: None.

ANR0112I

command_name command requires additional operands

Destination: Console.

Description: The operator issued command `command_name` without sufficient operands. Default processing could not be established.

Operator Action: Re-enter the command with desired operands, according to the documentation. You can also use the `help` command to determine the required operands.

ANR0113I

option current value: *value*

Destination: Console.

Description: This message is issued by the `DISPLAY` or `SHOW` command for a runtime option. The *option* is the runtime option specified in the `SHOW` command, and its current setting is *value*.

Operator Action: None. The operator may issue this command before changing the value of a runtime option, or may want to confirm its value after setting it (although message ANR0111I on page 27 can be used for the latter purpose).

ANR0114I

environment_variable is currently not set

Destination: Console.

Description: The operator entered the `SHOW -ENV` command to display the value of an environment variable. The variable has not been set.

Operator Action: None.

ANR0115I

environment_variable is set to an empty value

Destination: Console.

Description: The operator entered the `SHOW -ENV` command to display the value of an environment variable. The variable is set in the environment of the server, but the value is the empty string.

Operator Action: None.

ANR0116I

The *option* runtime option may not be changed while the server is running

Destination: Console.

Description: The operator or stordaemon user issued the `stordaemon setvar -name` command to change an option which cannot be changed while the server is running.

Operator Action: To change the desired option on the next run of `storsrvd`, you can use `stordaemon setoption` or edit the `daemon_options` file in the SYMAPI configuration directory. If you use the `setoption` command and then try to use `reload`, additional log messages may be issued indicating that some changed options will not be reloaded.

ANR0120I

SYMAPI Active Session List:

Destination: Console.

Description: The operator issued the `LIST SESSIONS` command and there are active sessions to list. This message is the heading for the list of sessions which follows.

Operator Action: None.

ANR0121I

No active sessions found.

Destination: Console.

Description: The operator issued the `LIST SESSIONS` command or the `SHOW SESSION` command and there are no active sessions to list/show.

Operator Action: None.

ANR0122I

Session *number* is not active

Destination: Console.

Description: The operator issued the `SHOW SESSION` command with the `-NUM` option to display a specific session, and the specified session was not active.

Operator Action: None.

ANR0123I

Show *server* Details:

Destination: Console.

Description: The operator issued the `SHOW -SERVER` command to display the details for the server. This line is written to mark the beginning of the server details output.

Operator Action: None.

ANR0124I

Show Session details for Session *session_number* on Thread *thread_number*:

Destination: Console.

Description: The operator issued the `SHOW SESSION` command to display details of one or more currently active sessions. This line is written at the beginning of the details for each session to be displayed.

Operator Action: None.

ANR0140E

Secure sessions are not supported on this platform. The security level specified is *security_level*

Set Step Return Code

Destination: Log and console.

Description: This message is issued when either the SYMAPI `options` file or `daemon_options` file specified a security level of ANY or SECURE on a platform where secure sessions are not supported. In the case of the `options` file, the `SYMAPI_SERVER_SECURITY_LEVEL=` or the `SYMAPI_SECURITY_LEVEL=` statement specified this value. In the case of the `daemon_options` file, the `storsrvd:security_level` specified ANY or SECURE. The value may have been specified for the `-seclevel` operand of the `storsrvd` command.

> (i) **Note:**
> Starting with Solutions Enabler V7.6, `SYMAPI_SERVER_SECURITY_LEVEL` from the SYMAPI `options` file and `storesrvd:security_level` from the `daemon_options` file are deprecated.

Operator Action: If security level is specified through any configuration statement or `storsrvd` command operand, it must specify NONSECURE on platforms where secure sessions are not supported. It is safer to omit the specification altogether, or to specify the dash character '-'. Refer to the *Dell EMC eLab Navigator* for a list of platforms where secure sessions are supported.

ANR0141E

Could not extract server *file* filename, rc=*returncode*

Destination: Log.

Description: During initialization, the SYMAPI server was not able to determine the name of the file to be used in SSL initialization. The string *file* refers to the SSL type file that the server was about to reference. The failing return code is displayed in *returncode*.

Operator Action: In an Open Systems environment, the server certificate and private key files should have been installed by the normal installation procedure. In z/OS and Microsoft Windows, the location of the Solutions Enabler configuration directory can be adjusted to your configuration needs. Follow the platform specific installation instructions to install the default server certificate files.

ANR0142E

About this task

function establishment failed with rc= *returncode (error_message)*

Destination: Log.

Description: During SSL initialization, the component referred to by *function* failed to be established. If *function* is CERTIFICATE or PRIVATE KEY, then the `symapisrv_cert.pem` file may be damaged or it may not have been successfully copied to the SYMAPI configuration directory.

Operator Action: If server certificate and key files are not installed by default on the platform where the server is running, additional installation steps are necessary. Refer to the platform specific installation instructions to install the files. You can specify NONSECURE for the security level if desired; in which case, the server will not attempt to load the certificate and key files.

ANR0143E

Rejected session *address*: security level mismatch reason: *error_message*

Destination: Log.

Description: A mismatch of security levels occurred when an initiating client session requested a security mode that the server was not able to honor.

address is the IP address of the client and *error_message* contains the error message indicating the actual problem.

Operator Action: If possible, modify the security level of the client to match the security mode that the server is using. If that is not possible, then (unless other clients will be impacted), modify the security level of the server to match the security level the client is requesting.

ANR0144E

Secure Library Init error: rc=*return_code (error_message)*

Destination: Log.

Description: Some component failed during SSL initialization. The *return_code* value corresponds to the message explained in the string *error_message*.

Operator Action: If you are unable to resolve the problem indicated in string *error_message*, contact Dell EMC technical support for assistance with this error.

ANR0145E

The value *value* specified for security level is invalid

Set Step Return Code

Destination: Log.

Description: This message is issued when an attempt is made to set the security level for the SYMAPI server daemon using one of the supported methods, and the value specified is invalid. The methods to set the security level are: the `storsrvd -seclevel` command line option, the `storsrvd:security_level` statement in the `daemon_options` file, or the `stordaemon`

`setvar` command. The valid values are NONSECURE, ANY, or SECURE. Note that a separate message (ANR0148E on page 31) is issued if an invalid value is specified in the SYMAPI options file.

> (i) **Note:**
> Starting with Solutions Enabler V7.6, `storesrvd:security_level` from the `daemon_options` file is deprecated.

Operator Action: Correct the value specified on the command line or in the `daemon_options` file, and restart the server or re-execute the `stordaemon` command.

ANR0146I

Security level has changed from *old_security_level*. New sessions will use *new_security_level*

Destination: Log.

Description: The security level to be used by the server was changed successfully using the `setvar` or `reload` command through the `stordaemon` CLI on the z/OS console. The level was changed from *old_security_level* to *new_security_level*. New sessions will negotiate based on the new security level set, but existing sessions are unaffected by the new level, and will continue to use the security level negotiated when they started.

Operator Action: Confirm that the *new_security_level* is the intended security level. If so, no further action is required. If not, you may want to refer to the server logs or other logs to determine why the security level was changed.

ANR0147I

The SYMAPI options file specified an empty value for `option_name`, changing to platform internal default *security_level*

Destination: Log.

Description: A configuration file statement `option_name` specified an empty value for the server security level. Such a specification is an error, but the server will substitute the default security level value with *security_level* for the platform on which the server is running. The default value is SECURE for platforms that support secure mode and NONSECURE for those platforms that do not support secure mode.

Operator Action: The omission of the security level on an explicit configuration is most likely a mistake. Refer to the SYMAPI `options` file or the `daemon_options` file to correct the omission, if you want to suppress the appearance of ANR0147I on page 31.

> (i) **Note:**
> Starting with Solutions Enabler V7.6, `storesrvd:security_level` from the `daemon_options` file is deprecated.

ANR0148E

The SYMAPI option SYMAPI_SERVER_SERCURITY_LEVEL specified an invalid value

Set Step Return Code

Destination: Log and console.

Description: This message is issued during server initialization when an invalid value is specified in the SYMAPI `options` file statement `SYMAPI_SERVER_SECURITY_LEVEL` or `SYMAPI_SECURITY_LEVEL`. The value for security level can be defined in several places. Here is a list of them and their priorities:

1. Security level defined by the command `stordaemon start storsrvd -args -security_level <security level>`. This takes precedence over everything else.

2. `SYMAPI_SECURITY_LEVEL` defined in the SYMAPI **options** file.

3. `SECURITY_LEVEL` defined in the `daemon_options` file.

4. `SYMAPI_SERVER_SECVRITY_LEVEL` defined in the SYMAPI `options` file.

> (i) **Note:**
> `SECURITY_LEVEL` from the `daemon_options` file and
> `SYMAPI_SERVER_SECURITY_LEVEL` from the SYMAPI `options` file are deprecated.

Note that a separate message (ANR0145E on page 30) is issued if an invalid value is specified in any of the other methods: `storsrvd` command line, `daemon_options` file, or the `stordaemon setvar` command.

Operator Action: Correct the value specified in the SYMAPI `options` file statement `SYMAPI_SERVER_SECURITY_LEVEL` or `SYMAPI_SECURITY_LEVEL`. The valid values are NONSECURE, ANY, or SECURE. The `SYMAPI_SERVER_SECURITY_LEVEL` statement is now deprecated and replaced by `SYMAPI_SECURITY_LEVEL`. The former statement is still accepted for compatibility reasons.

ANR0149D

Security level has been taken from the SYMAPI option *value*

Destination: Log.

Description: This message is issued when the value for the server security level is defined in the SYMAPI `options` file and has not been specified on the `storsrvd` command line. This message is informational only.

value is either `SYMAPI_SECURITY_LEVEL` or `SYMAPI_SERVER_SECURITY_LEVEL`.

ANR0150E

The value *value* specified for client certificate verification is invalid

Destination: Log.

Description: This message is issued during server initialization when the value for the client certificate verification option, as defined in the `daemon_options` file, is invalid. It can also be issued when attempting to change this option with the `stordaemon` command to an invalid value.

Operator Action: Correct the value specified in the `daemon_options` file statement `security_clt_secure_lvl` or as specified on the command line. The valid values are NOVERIFY, VERIFY or MUSTVERIFY.

ANR0151E

Common Name in client certificate not valid: expected *name*, received *common name*

Destination: Log.

Description: This message is issued during setup of secure mode between client/server. The common name in the client certificate does not match the name the server is expecting.

Operator Action: Check the client certificate to verify that the names contained in the certificate are known hostnames to the server. Either generate a client certificate with the hostname that the server is expecting or add the common name in the client certificate to the applicable `/etc/hosts` file on the server.

ANR0152E

Issue detected with server certificate file *filename*

Destination: Log.

Description: This message is issued during initialization of the secure library. A problem with the certificate file has been detected.

Operator Action: Check for the existence of the certificate file on the server. If you have set the `security_alt_cert_file` parameter in the `daemon_options` file, verify that it points to a valid file.

ANR0153E

Issue detected with server PrivateKey file *filename*

Destination: Log.

Description: This message is issued during initialization of the secure library. A problem with the PrivateKey file has been detected.

Operator Action: Check for the existence of the `Privatekey` file on the server. If you have set the `security_alt_key_file` parameter in the `daemon_options` file, verify that it points to a valid file.

ANR0154E

Host name pattern in certificate is not valid: *pattern* for the client *Host Name*

Set Step Return Code

Destination: Log.

Description: This message is issued during setup of secure mode between client/server. It indicates an illegal pattern has been put into the client certificate. *Pattern* shows the pattern in the client certificate, and *HostName* shows the name of the client host which was attempting to connect to the server.

Operator Action: Generate a new client certificate without the illegal host name pattern. The only characters allowed for a host name pattern are letters, numbers, periods (.), colons (:), and hyphens (-).

ANR0155E

Subject Alternative Names in the client certificate not valid: expected *name*, received *list*

Set Step Return Code

Destination: Log.

Description: This message is issued during setup of secure mode between client and server. The list of Subject Alternative Names in the client certificate did not contain a match of the name or IP address that the server is expecting. The name the server expected to find is *name*, but it found the list of Subject Alternative Names in the *list*.

Operator Action: Check the client certificate to verify that the names in the certificate are hostnames or IP addresses known to the server. Either generate a client certificate with the hostname that the server is expecting or add the name(s) in the Subject Alternative Name field(s) in the client certificate to the applicable */etc/hosts* file on the server.

ANR0156E

Federal Information Processing Standard (FIPS) mode has failed to be enabled

Set Step Return Code

Destination: Log.

Description: This message is issued during server initialization if the server is configured to run in secure mode on a platform that supports FIPS mode and the server was unable initialize FIPS mode.

Operator Action: The details about error conditions will be recorded in the `storsrvd` log files. Refer to the log file for signs of why FIPS mode initialization failed. The most likely cause of the error is that the cryptography library failed to load.

ANR0200E

service_name error *return_code: explanation;* from *calling_routine*, line *line_number*

Destination: Log.

Description: Server logic called the routine named by *service_name* and received a failure indicated by *return_code,* where *explanation* is text that corresponds to the *return_code.*The failure was detected at line *line_number* in the routine *calling_routine.* The routine *calling_routine* was not able to continue due to the failure of *service_name.*

Operator Action: None, generally. This message may occur in very rare circumstances during handling of an operator command, and may indicate a syntax error that was not handled properly by parsing logic. Examine the command and reissue it if it was specified incorrectly.

ANR0201E

Unable to allocate *count* bytes for *object_name*

Destination: Log.

Description: The server attempted to allocate *count* number of bytes. *object_name* is a description of what the server was trying to allocate. This message may indicate that the server is over-committed with regard to the number of concurrent sessions, or that there may be a memory leak in the server.

Operator Action: Increase the amount of memory available to the server using the appropriate method for the platform the server is running on. If this does not solve the problem, a memory leak may be indicated by other failure messages. Collect and forward error documentation to Dell EMC Customer Support for analysis.

ANR0202E

Unable to *operation_name*port *port*, error *error_number*indicates *explanation*

Set Step Return Code

Destination: Log and console.

Description: An error occurred operating on the socket on which the server listens for new connections. *operation_name*will indicate an error during bind, listen, initialize, accept, or start new thread. The *error_number*is the decimal value of the system error variable *errno*(in Windows, the value returned from the `GetLastError() call`), and the *explanation*is the text that explains the meaning of *error_number.port* is the TCP/IP port which clients use to connect to the SYMAPI server. The server shuts down after issuing this message.

Operator Action: In most cases, other messages will also be issued giving other details about an error situation. Follow your normal procedures for detecting and correcting problems in your TCP/IP network. Correct the TCP/IP problem and restart the server.

ANR0204E

Unable to decode return value *return_value* from *process*

Set Step Return Code

Destination: Log and console.

Description: The *return_value* from a call to a routine or other logic could not be interpreted. *process* may be the name of the function or may be a general description of processing that resulted in a return value which could not be interpreted.

Operator Action: None. This message will be preceded by other error messages that provide more detail. If your normal processing is unaffected, no action is necessary. Otherwise, you may need to collect and provide documentation as directed by Dell EMC Customer Support.

ANR0205E

action is not currently supported

Destination: Log and console.

Description: An action or feature was requested that is either not yet supported or is no longer supported. The name of the action or feature not supported is *action*.

Operator Action: None. The feature you requested is not available for use in this release. If you receive this message in error, examine the job log for other evidence of a failure which may be related to the action or feature you attempted to use.

ANR0207S

Failed to start *name* thread, error = *code (explanation)*

Set Step Return Code

Destination: Log and console.

Description: This message is issued in two cases:

- During server initialization, the attempt to start the dedicated SYMAPI listener thread failed. In this case, *name* is *SYMAPI Listener*. The server will immediately abort initialization and will stop.

- During handling of the arrival of a SYMAPI session, the attempt to start a dedicated thread for the session failed. In this case, *name* is *SYMAPI session*. The server continues to listen for other sessions, although the ability to start new threads can be limited. Other messages may accompany this one with additional diagnostic detail. The return code and explanation from the thread-start service call are displayed in *code* and *explanation*.

Operator Action: Examine other messages in the log files and other system output. You may be able to determine the cause and corrective action from other messages. In the second case, system resources required to start threads may be exhausted due to the current SYMAPI session count. Your system may be configured to allow a maximum number of threads per process, and this limit may have been exceeded. Complete diagnosis may require assistance of Dell EMC technical support.

ANR0208E

Unable to verify SYMAPI Database directory *db_dir*

Set Step Return Code

Destination: Log and console.

Description: The server attempts to make the SYMAPI database directory the current directory during initialization in order to cause non-default database files to be placed in the database directory if the name is not a fully-qualified pathname. This message is issued during server initialization if the SYMAPI database directory does not exist or is inaccessible. The most common reason is that the database directory does not exist. The name of the directory the server attempted to verify is shown in *db_dir*.

Operator Action: The Solutions Enabler installation process creates the database directory normally. If this operation failed during installation, the installation process would have terminated with an error. You can create the directory using the tool appropriate to your platform. Use the directory name shown in *db_dir* in the message text.

ANR0209I

Authentication service name *service_name* exceeds maximum length

Destination: Log and console.

Description: The `storsrvd` process is attempting to copy *service_name* to an internal structure and is unable to because of its length.

Operator Action: If possible, shorten the name of the host shown in *service_name*. Otherwise, you may need to collect and provide documentation as directed by Dell EMC Customer Support. The server will continue to operate in non-authenticated mode.

ANR0210E

EMCSAI version does not meet minimum version requirement of *nn.nn.nn*

Destination: Log and console.

Description: The version of ResourcePak Base running on the host does not meet the minimum version required by Solutions Enabler.

Operator Action: Ensure that Solutions Enabler is configured to work with ResourcePak Base at the indicated version or later.

ANR0211E

Unable to obtain EMCSAI version, RC=%a (%b) EMCRC=%c, EMCRS=%d

Destination: Log and, in some cases, the console.

Description: This message is issued as a result of an interface error when Solutions Enabler checks the ResourcePak Base version.

Where:

%a is the return code from the call to the ResourcePak Base EMCSAI interface

%b is a text description of the message.

%c is the EMCSAI Return Code (emcrc)

%d is the EMCSAI Reason Code (emcrs)

The most common cause of error is that Solutions Enabler is configured to work with a version of ResourcePak Base which is not running or which does nor exist. Either one of these conditions will result in the following message being issued:

ANR0211E Unable to obtain EMCSAI version, RC=28 (Symmetrix Control Facility is not available) EMCRC=0, EMCRS=0

Operator Action: In all other cases of the message, contact Dell EMC for support.

ANR0212E

Unable to determine peer *identifier*, System call: *callname*, RC: *return_code*

Set Step Return Code

Destination: Log and console.

Description: During session negotiation, the server attempts to look up the name of the client host which has initiated the session. If the name of the host cannot be determined, the server then attempts to look up the IP address of the client host. The *identifier* will be either "*nodename*" or "*address*" depending on which failure occurs.

Where:

callname is the name of the system function called to execute the lookup.

return_code is the failure return code from that function.

Operator Action: The session continues to be initiated, if possible. If the session is SECURE, then it's very likely that the validation of the hostname in the certificate will fail, since it is compared to the identifier obtained from the system. If the system cannot return a hostname, DNS and local host TCP/IP configuration can be changed to configure a hostname properly. In the rare case that the system cannot obtain an IP address, it is an indication of a severe IP configuration problem. Your network system administrator should be consulted to determine the nature of the network configuration problem.

ANR0220I

Thread *thread_number* will execute without condition handling protection

Destination: Log.

Description: In a z/OS environment, the session on thread *thread_number* will be executed without the protection of a condition handler. The `setvar -cond_hdlr OFF` command had been previously issued, causing condition handling suppression. This message is a confirmation that the session will be run without protection. An abend on the thread will cause the operating system to terminate the server address space.

You can associate the thread number with a session number by using the `LIST SESSIONs` command. The second column of the list sessions output is the thread number of the session.

Operator Action: None.

ANR0221E

Unable to set condition handling for thread *thread_number*, msgno=*LE_message_num*, sev=*LE_severity*

Destination: Log and console.

Description: In a z/OS environment, the thread (*thread_number*) handling a session attempted to set condition handling by calling the Language Environment routine CEEHDLR but received a non-zero return value from the call. The Language Environment feedback message number is shown in *LE_message_number* and the severity of the return is shown in *LE_severity.*

Operator Action: None.

ANR0222E

ConditionHandler invoked on thread *thread_number*; writing dump to DD *dump_location*

or

ConditionHandler invoked on thread *thread_number*; writing dump to *file_name* in SYMAPI log directory

Destination: Log and console.

Description: In a z/OS environment, an abnormal condition was raised during the session running on *thread_number*. A dump will be written to the DD name *dump_location.* The general format of the DD name is DMP*nnnnn* where *nnnnn* is the *thread_number.*

If you prefer that the dump be written to a file instead of to the spool, you can use DD SYM$ENV in the server's JCL and add this environment variable:

```
SYMAPI_LE_DUMP_LOGDIR = 1
```

After this variable is set, if an abnormal condition were to arise during the session running on *thread_number*, a file *file_name* will be written to the Solutions Enabler log directory. The general format of the file name is DMP*nnnnn* where *nnnnn* is the *thread_number*.

Operator Action: Consult Dell EMC Customer Support for directions on completing documentation to provide for analysis and correction.

ANR0223E

Dump to *dump_location* is complete; thread *thread_number* will be terminated

or

Dump to *file_name* in SYMAPI log directory is complete; thread *thread_number* will be terminated

Destination: Log and console.

Description: This message should immediately follow ANR0222E on page 37. It denotes that the dump whose beginning is marked by the previous ANR0222E on page 37 message is now complete. And the dump is written to either *DD name dump_location* or a file named *file_name* in SYMAPI log directory. Furthermore, thread *thread_number* that caused this dump will be terminated.

Operator Action: None.

ANR0224S

Recursive entry to condition handler on thread*thread_number*

Destination: Log and console.

Description: In a z/OS environment, condition handling processing detected a recursive (second) entry into the condition handling routine. This may indicate an abend while attempting to handle an earlier abend.

Operator Action: None.

ANR0225E

Condition handling is not supported on this platform

Destination: Log.

Description: In a z/OS environment, language environment *condition handling* supports capturing abnormal termination of a thread without affecting other threads in the process (job). This message is issued when an attempt is made to set or display the current condition handling setting in a non-z/OS environment, using the `stordaemon getvar` or `setvar` command.

Operator Action: Correct the `setvar` or `getvar` command to specify an option which is supported in the environment where you are using the `stordaemon` command.

ANR0300E

API Request code *SYMAPI_request_code API_name* rejected; it is restricted and disabled

Destination: Log.

Description: A SYMAPI request code that describes a control operation was received. The server checked the *SYMAPI_request_code* (function named in *API_name*) to determine whether execution has been disabled. The API request was found to be disabled. This message will only be issued in the z/OS environment.

Operator Action: None. In a z/OS environment, control operations may have been disabled by using the installation job `#12CNTRL` in the Solutions Enabler RIMLIB dataset.

ANR0301I

API Request code *SYMAPI_request_code API_name* executing

Destination: Log.

Description: The server received a SYMAPI request described by the decimal code *SYMAPI_request_code.*This message is issued when the server begins executing the API request. The name of the SYMAPI function name is *API_name*.

Operator Action: None.

ANR0302I

API Request code *SYMAPI_request_code* complete, processing status *SYMAPI_return_ code* (*explanation*)

Destination: Log.

Description: The API request named in message ANR0301I on page 39 completed executing. The decimal code of *SYMAPI_request_code*corresponds to the API request code. The return value of the API request was *SYMAPI_return_ code,*and the corresponding text is *explanation.*

Operator Action: None.

ANR0303I

Executing SymExit to clean up (client exited without calling SymExit)

Destination: Log.

Description: The client application exited its process before calling SymExit to end the remote session with the SYMAPI server. The server calls SymExit on behalf of the client to free up resources which are still held.

Operator Action: None.

ANR0304I

Cleanup SymExit return: *return_value* (*explanation*)

Destination: Log.

Description: The cleanup call to SymExit completed, and the return value was *return_value*. The *explanation* is the text associated with *return_value*.

Operator Action: None.

ANR0305E

REMOTE_CACHED mode not supported for client node *Host_name* version
client_version_number - connection rejected

Destination: Log.

Description: A client running a version of Solutions Enabler earlier than V7.2 attempted to connect to a SYMAPI server running V7.6 or higher, which is not allowed.

Operator Action: None.

ANR0306E

Connection rejected from client node *HostName* -- its version (*version*) is no longer supported in C/S mode

Destination: Log.

Description: Client connections using SYMAPI versions lower than V7.2 are not supported. *Hostname* is the name of the client host where the connection originated, and *version* is the version of the SYMAPI library with which the client program was built.

Operator Action: The developer of the application must upgrade to a newer version of the SYMAPI library. If the client program is the SymCLI, there may be an incorrect version installed on the client host, or the client may intend to connect to a different server.

ANR0307E

Connection rejected from client node hostname -- its version (*HostName*) is newer than our version

Destination: Log.

Description: The SYMAPI version of the client program is newer than the server's version. Such a connection is not supported. *HostName* is the name of the client host where the connection originated, and *version* is the version of the SYMAPI library with which the client program was built.

Operator Action: Insure the client program is directing its connection request to the correct server.

CHAPTER 2

Asynchronous Events

This chapter lists the possible asynchronous error and message events trapped by the event daemon.

Unisphere for PowerMax alert monitoring recommendations

This section outlines the list of recommended alerts for you to monitor or consider monitoring (depending on your environment) when configuring alert policies using Unisphere for PowerMax.

Note that this relates to storage system running HYPERMAX OS 5977 or higher.

Alert notifications should also be enabled for these alerts.

In addition, notifications should be configured for the default SystemThresholds Alerts set and Notifications set.

It is recommended that you monitor the following:

- Array Component events
- Array Events
- Array - Deferred Service Threshold Alert
- Array - Director Status
- Array - Disk Status
- Array - Environmental Alert
- Array - Hotspare Invoked
- Array - Migration Complete Alert
- Array - Port Link status
- Array - Port status
- Array - RVA Spare Coverage
- Array - SP Alerts
- Array - SRDF Alerts
- Array - SRDF Job Flow Control Change
- Array - SRDF Link Status
- Array - SRDF/A No Cycle Switch Alert
- Array - SRDF/A Session
- Array - SRDF/A Session dropped, transmit idle state timeout
- Array - SRDF/A Session entering transmit idle state
- Array - SRDF/A Session recovered from a transmit idle state
- Array - Target Enginuity Warning

Consider monitoring the following depending on customer environment:

- Array - Device Config Change
- Array - Device Status
- Array - Thin Device Allocation
- Array - Thin Device Usage

Configuring event logging

The `daemon_options` file contains a set of parameters that can be modified to affect event daemon behavior. The file contains editable behavior parameters set to certain optional defaults in the line entries. Commented lines beginning with a pound sign (#) are ignored.

To remove any parameter option, remove the line entry, rename the file, or comment the line by adding a pound sign (#) at the beginning of the line entry.

Configuring event logging involves the following steps:

1. Specify logging targets.
2. Configure an event target.
3. Specify events to log.

The remainder of this section explains `daemon_options` file settings required to complete each of these steps.

(i) **Note:**

Changes made to the `daemon_options` file while the daemon is running will not take effect until you issue a `stordaemon reload` command.

Specify logging targets

To specify a logging mechanism, define the following parameter in the `daemon_options` file:

```
storevntd:log_event_targets = snmp syslog system file
```

(i) **Note:**

You must set this parameter to one or more of the valid values; otherwise, event logging will not occur. When specifying multiple values, separate them with a space.

where:

`snmp` specifies to log events by way of SNMP traps. Solutions Enabler supports SNMP version 3 traps.

(i) **Note:** The z/OS Event Daemon does not support `snmp` as a logging target, only `syslog`, `system`, and `file`.

`syslog` (supported on all platforms) specifies to log events to a Syslog server across the network, bypassing (if on UNIX) the local host's Syslog service and its configuration settings.

`system` does the following depending on the operating system:

- In UNIX, it specifies to log events to local host's Syslog services. The Syslog's configuration settings control where it directs the message.
- In Windows, it specifies to log events to the Windows Event Log.
  `file` specifies to log events to a file on disk.

  For example:

```
storevntd:log_event_targets = snmp system
```

Configure an event target

Configuring SNMP event targets

The event daemon provides the necessary SNMP MIB support and trap generation services required to monitor the status of VMAX storage environments from third-party enterprise management frameworks.

The event daemon includes a loadable SNMP library which, once enabled and configured in the `daemon_options` file, acts as a self contained SNMP agent. It is responsible for maintaining internal Fibre Alliance MIB (V3.0) tables, responding to SNMP browse requests, and generating traps in response to events.

ⓘ **Note:** SNMPv3 is supported only on Windows 64-bit and Linux 64-bit systems.

To configure SNMP or SNMPv3, follow the steps below:

1. For an application to receive SNMP trap information from the event daemon, you must specify it as a trap target by defining the following parameter in the `daemon_options` file:

```
storevntd:snmp_trap_client_registration = IP,Port,Filter,State,Version
```

where:

IP is the application's IP address.

Port is the port on which the application will be listening for the trap. The default port is 162.

Filter is the trap filtering severity level as defined in the FC-management MIB. The application will only receive traps of the specified severity level (or lesser). The default value is 10 (Mark), which means that all events are delivered.

State is the start up row state in the `trap_client_registration` table in the FC-management MIB. Possible values are ACTIVE and INACTIVE.

Version is the trap generation version. This can be *v1* or *v3*. If no version is specified, then *v1* is considered as a default value.

Table 3 on page 46 maps the event daemon severity level to the SNMP severity levels, as specified in the FC-management MIB.

Multiple entries can be on the same line, separated by a blank space. In addition, they can be on their own line, delineated with a backslash (\) character on the preceding line.

```
storevntd:SNMP_TRAP_CLIENT_REGISTRATION =  \
                                11.22.33.44,162,10,ACTIVE,v3
 \


                                55.66.77.88,162,10,ACTIVE
```

For example, the following registration file specifies that the daemon will only send SNMP traps to the indicated clients when it detects an event of a severity level less than or equal to 5 (that is, Error, Critical, Emergency). The daemon will ignore events with a severity level greater than 5:

```
storevntd:snmp_trap_client_registration = 10.2.12.30,162,5,ACTIVE, v3 \
                                12.250.130.200,162,5,ACTIVE, v1
```

SNMP targets can also be dynamically configured with SNMP versions as shown in the below example:

```
stordaemon setvar storevntd –name

snmp_host='11.22.33.44:162:10:v3,55.66.77.88:162:10:v1'
```

For SNMPv1, this is the end of the configuration procedure. For SNMPv3, continue with the steps below.

2. Create a username with a password (for authentication) and privacy key (for encryption) for the registered SNMPv3 target. IP (or host) and port of the target is the key in this case as shown below:

```
symcfg authorization add -snmp -host 11.22.33.44
         -username testuser -password
testpassword
         -port 162 -key testprivkey
```

3. To create user credentials use the `symcfg authorization add` CLI command. API users can use the SymPwdDbEntryAdd() API.

   (i) **Note:** If the user configures more than two SNMPv3 targets on the same host but using different ports, then user credentials have to be created separately for each SNMP target. Creation of user credentials for different listeners running on the same host can be created using namespace offered by the CLI.

```
Example 1: IP - 11.22.33.44 and port 162
        symcfg authorization add -snmp -host 11.22.33.44
          -username testuser -password testpassword -namespace
             IP_11_22_33_44_162 -port 162 -key testprivkey

        Example 2: IP - 11.22.33.44 and port 1162
        symcfg authorization add -snmp -host 11.22.33.44
          -username testuser1 -password testpassword1 -namespace
             IP_11_22_33_44_1162 -port 1162 -key testprivkey1
```

4. To delete user credentials use the `symcfg authorization delete` CLI command.

```
symcfg authorization delete -host 11.22.33.44 -snmp
```

To delete user credentials that was created using namespace, namespace name has to be mentioned.

```
symcfg authorization delete -host 11.22.33.44 -snmp
                  -namespace IP_11_22_33_44_162
```

API users can use the SymPwdDbEntryRemove() API.

5. If the user credentials are added using SymPwdDbEntryAdd() or deleted using SymPwdDbEntryRemove() APIs, each API invoked has to be followed by the SymPwdDbCommit() API execution to permanently reflect the changes in the DB file.

6. Obtain the unique engine ID for the storevntd from which events are expected to be received by the SNMPv3 target using the `stordaemon getvar` command. For example:

```
stordaemon getvar storevntd -name snmp_v3_engineid
storevntd
snmp_v3_engineid=0x8001f888067458b6ba12a815a0000
```

7. Traps received by the SNMP manager are validated with the engine ID, username, password (using SHA authentication), passphrase (for AES encryption). For example, if the SNMP target is a Net-SNMP trap receiver with the following data:

```
Engined ID of the storevntd - 0x8001f888067458b6ba12a815a0000 (Auto
generated value)
UserName registered of the storevntd with the above engine ID - "traptest"
Password registered of the storevntd with the above engine ID -
```

```
"mypassword"
Passphrase registered of the storevntd with the above engine ID -
"mynewpassword"
```

The configuration file of the snmptrapd would look as follows:

```
"createUser -e 0x8001f888067458b6ba12a815a0000 traptest SHA mypassword
AES mypassword
authuser log traptest"
```

8. During the delivery of SNMPv3 traps to the SNMPv3 target, the event daemon retrieves the user name and other credentials registered for the destination host (IP and port as the key) using the SymPwdDbEntryList2() API and fills in those details into the SNMPv3 packets. When the packet reaches the destination, the trap receiver authenticates and decrypts the packet using the same credentials.

(i) Note: If SNMPv3 is specified as target during the SNMP target registration and no user credentials are configured for the SNMP target host, then the SNMP trap will not be sent.

Table 3 Event daemon severity level/SNMP severity level mappings

Event daemon severity	SNMP trap severity
	1 (Unknown)
fatal	2 (Emergency)
	3 (Alert)
critical	4 (Critical)
major	5 (Error)
minor	5 (Error)
warning	6 (Warning)
info	8 (Info)
normal	8 (Info)
	9 (Debug)
--	10 (Mark)

Object IDs
Object Identifiers (OIDs) are entries in the Management Information Base (MIB). OIDs containing the number 1139 are considered vendor extension OIDs.

Table 4 Object details

Object name	Object identifier	Description
connUnitEventId	1.3.6.1.3.94.1.11.1.3	This is the event index, mainly for internal use.
connUnitEventSeverity	1.3.6.1.3.94.1.11.1.6	The SNMP trap severity. The values are listed in Table 3 on page 46.

Table 4 Object details (continued)

Object name	Object identifier	Description
connUnitEventType	1.3.6.1.3.94.1.11.1.7	This is the event type. Possible values are: • UNKNOWN: 1 • OTHER: 2 • STATUS: 3 • CONFIGURATION: 4 • TOPOLOGY: 5
connUnitEventObject	1.3.6.1.3.94.1.11.1.8	This field is always NULL.
connUnitEventDescr	1.3.6.1.3.94.1.11.1.9	This is the description of the event. See sections Array Events: Event IDs 1050 - 1199 on page 56 and Array Events: Event IDs 1200-1999 on page 89 for detail.
connUnitName	1.3.6.1.3.94.1.6.1.20	This is the array ID.
connUnitType	1.3.6.1.3.94.1.6.1.3	This is the array type. Possible values are: • OTHER: 2 • STORAGE_SUBSYSTEM : 11
emcAsyncEventSource	1.3.6.1.4.1.1139.3.8888.1.0	The source of the events: • Symmetrix: 2 • CLARiiON: 3
emcAsyncEventCode	1.3.6.1.4.1.1139.3.8888.2.0	This OID has been defined in gateway.mib. This is the event ID. See sections Array Events: Event IDs 1050 - 1199 on page 56 and Array Events: Event IDs 1200-1999 on page 89 for detail.
emcAsyncEventComponentType	1.3.6.1.4.1.1139.3.8888.3.0	This is the component type, for example FastSRP.
emcAsyncEventComponentName	1.3.6.1.4.1.1139.3.8888.4.0	The component name, for example SRP on which the event was generated.

Example

The following example shows an SNMP trap to monitor a SRP capacity change event. For detailed explanations of the OIDs, see table 3.

This is a unique string that is specific to the
array/configuration the event occurred on.

This is the Event Index. The last octet (79 in this example) is used
as the last octet for all the other OIDs for this event
(except for OIDs 1.3.6.1.3.94.1.6.1.20 and 1.3.6.1.3.94.1.6.1.3).

\n[1] .**1.3.6.1.3.94.1.11.1.3** 80.6.4.130.222.183.80.64.0.0.0.0.0.0.0.0.79 (Integer): 79

\n[2] .**1.3.6.1.3.94.1.11.1.7**.80.6.4.130.222.183.80.64.0.0.0.0.0.0.0.0.79 (Integer): 2 ← This is the Event Type. In this example, it is 2 that means Other.

\n[3] .**1.3.6.1.3.94.1.11.1.8**.80.6.4.130.222.183.80.64.0.0.0.0.0.0.0.0.79 (ObjectIdentifier): .0.0 ← This is the Event Object. This value is always NULL.

\n[4] .**1.3.6.1.3.94.1.11.1.9**.80.6.4.130.222.183.80.64.0.0.0.0.0.0.0.0.79 (OctetString): Symmetrix 000192601409 FastSRP SRP_1 : The Effective used capacity
for SRP has changed to 100 percent. ← This is the Event Description, corresponding to the Event ID (1512 in this example).

\n[5] .**1.3.6.1.3.94.1.11.1.6**.80.6.4.130.222.183.80.64.0.0.0.0.0.0.0.0.79 (Integer): 6 ← This is the Event Severity.

\n[6] .**1.3.6.1.3.94.1.6.1.20**.80.6.4.130.222.183.80.64.0.0.0.0.0.0.0.0 (OctetString): 000192601409 ← This is the Array ID

\n[7] .**1.3.6.1.3.94.1.6.1.3**.80.6.4.130.222.183.80.64.0.0.0.0.0.0.0.0 (Integer): 11 ← This is array type. This is 11 that means Storage Subsystem for these traps.

\n[8] .**1.3.6.1.4.1.1139.3.8888.1.0** (Integer): 2 ← This is the Event Source (2 represents Symmetrix)

\n[9] .**1.3.6.1.4.1.1139.3.8888.2.0** (Integer): 1512 ← This is the Event ID

\n[10] .**1.3.6.1.4.1.1139.3.8888.3.0** (Integer): 1054 ← This is the Component Type (1054 represents FastSRP)

\n[11] .**1.3.6.1.4.1.1139.3.8888.4.0** (OctetString): SRP_1 ← This is the Component Name on which the event was generated (SRP in this example).

Configuring a log file

The `daemon_options` file contains parameters (Table 5 on page 48) that allow you to configure the log file.

The target log file is not actually opened (or created, if necessary) until the event daemon actually has an event to log. Depending on the events it is monitoring, this may not be until long after it starts.

Table 5 Event log file configuration options

Parameter	= <OptValue | defaultvalue>	Description
storevntd:log_event_file_name	*LogEventFileName* | events	Specifies the base name of the event log files, which can also include the full pathname. This file is created in the standard Solutions Enabler log directory. For UNIX, the directory is: `/var/symapi/log` For Windows, the directory is: `c:\Program Files\EMC\SYMAPI\log`
storevntd:log_event_file_type	dated | wrap	Specifies the type of file to use. `dated` specifies that a new event log file should be created each day, with the name *xxxx-YYYYMMDD*`.log`. Where *xxxx* is the *LogEventFileName*. `wrap` specifies that event logging will

Table 5 Event log file configuration options (continued)

Parameter	= <OptValue | defaultvalue>	Description
		alternate between two files (`xxxx.log0` and `xxxx.log1`) - switching from one to the other when it reaches its maximum size, as specified in the `log_event_file_size` parameter. By default, a single file will be used.
storevntd:log_event_file_size	> 0 - *nn* | 1	When used with the `log_event_file_type` parameter set to wrap, this parameter specifies the maximum file size (in KB) allowed before wrapping to the alternate file. This value should be a decimal number greater than zero. Note: The maximum value for the `log_event_file_size` is 2097152 KB.
storevntd:log_event_file_retention	> 0 - *nn* | 3	When used with the `log_event_file_type` parameter set to dated, this parameter specifies the number of days to retain the log files. This value should be a decimal number greater than zero.
storevntd:log_event_file_perms	rw, n | r	Specifies the permissions for the event log files. `rw` specifies that anyone can read or write to the files.

Table 5 Event log file configuration options (continued)

Parameter	= <OptValue | defaultvalue>	Description
		r specifies that anyone can read the files, but only the root/administrator (or whatever identity the event daemon is running as) can write to the files.
		n specifies that only the root/ administrator (or whatever identity the event daemon is running as) can read and write to the files.

Configuring a Syslog target

The daemon_options file contains parameters (Table 6 on page 50) that allow you to configure a Syslog target.

Table 6 Event log file configuration options

Parameter	= <OptValue | defaultvalue>	Description
storevntd:log_event_ syslog_host	*SyslogHostName*	Specifies the name of the host on which the Syslog server is running. This value must be supplied.
storevntd:log_event_ syslog_port	*nnn* | 514	Specifies the port on which the server is listening.

Specifying events to log

Solutions Enabler provides the ability to capture both array events and non-array events from certain application to log files. This is accomplished by building event lists, which is a mechanism for specifying the types of events for which to generate traps. These event lists are defined in the daemon_options file.

Array events

To build an array event list, define the following parameter in the daemon_options file:

ⓘ Note:

Many array events are organized into categories. These categories are hierarchical in that a category can contain individual events, as well as other categories.

```
storevntd:log_symmetrix_events = [sid=SymmID,] UID|Category ... [,sev=SEV]
[,tgt=TGT] [,comp=COMP] [,comp_type=CPMP_TYPE] [thresh_critical=Percent,
thresh_maj=Percent, thresh_warn=Percent, thresh_info=Percent, thresh=Percent]
[,ignore]
```

where:

sid— Specifies the 12-digit ID of the VMAX array to which the record applies. You must specify the full SID (12 digits). If this field is missing, the registration applies to all local and remote VMAX arrays.

UID — The numerical event UID value.

Category — One or more of the following event categories, separated with a comma:

For events in the 1150 - 1199 range:

- events (all events in this category)

- array subsystem

- checksum

- diagnostic

- environmental

- device pool

- service processor

- srdf system

- srdf link

- srdf session

- srdf consistency group

- director

- device

- disk

For events in the 1200 - 1999 range:

- status (general component state change)

- optimizer (Optimizer/FAST related)

- groups (Group (DG/CG) related)

(i) Note:
Each of the event categories may contain numerous individual events, as described in the *Dell EMC Events and Alerts for PowerMax and VMAX User Guide*.

sev— Specifies the minimum severity level for which events should be logged. All events with a severity level at or above the specified severity will be logged. Take care when setting this option. Possible values are:

- normal

- info

- warning

- minor

- major

- critical

- fatal

tgt — Specifies the target to which the daemon should log the events. Possible values are: snmp, syslog, system, and file.

The value you specify for *TGT* must match one of the values you specified in the `log_event_targets` parameter; otherwise, the daemon will not log events for this record.

The target you specify here will override the global `log_event_targets` setting described in

comp — Specifies the specific sub-component for which you want to log events. For example, a particular device, disk, pool, etc. When you specify a value for this field, the event daemon will only log events for the specified component. You can either specify a single component or a comma separated list of components. If the latter, you must enclose the list with double quotes.

For example:

`comp=0100`	a single device
`"comp=0100,0200,030"`	multiple devices
`"comp=finance,sales"`	multiple pools

cmpnt_type — Specifies a type of component. When present, only events for the specified component type are delivered. If omitted, events for any component type are delivered. This is most useful for events that can be delivered against multiple types of components.

An example is the Pool Status events, which can be generated for DSE, Thin or Snap Pools. Possible values are: `device`, `disk`, `director`, `port`, `dsepool`, `tpdatapool`, `snappool`, `dg`, `cg`, `sg`, `srdf-grp` and `migrsess`.

`thresh_critical=`*Percent* `thresh_maj=`*Percent* `thresh_warn=`*Percent* `thresh_inf=`*Percent* `thresh=`*Percent*	Specifies the threshold level at which the daemon delivers an event and at what severity it is delivered. This setting overrides the default threshold levels for an event. These parameters are only used when specifying threshold type events. Only a subset of the full threshold functionality is supported. The MINOR and FATAL severities cannot be specified and a >= comparison is assumed. The `thresh=`*nnn* setting is an alias for `thresh_maj`.

ignore — Indicates that events matched by this record are not to be delivered, even if they are matched by some other record. The order of records doesn't matter. If an event is matched by any record with the ignore parameter, it will be ignored.

Only a single `log_symmetrix_events` option can be present. Since this can become quite long, it can be spread across multiple lines in the file via the use of '\' continuation characters at the end of a line.

> (i) **Note:**
> The comment character (#) has no effect if it follows a line with the continuation character (\).

Non-array events

To build a non-array event list, define the following parameter in the `daemon_options` file:

```
storevntd:log_app_events = [appid=appid,] CAT[category,] [comp=COMP,]
[comp_type=COMP_TYPE,] [,tgt=TGT]
```

where:

appid— Specifies an application id. By default, all application events will be monitored.

CAT — Specifies event(s) to be monitored. This can be either the name of an event category or a numerical event ID. This is the only field that is required. One or more values (comma separated) may be present. The Supported categories are: SMC and SPA.

comp — Certain events apply to specific sub-components within the application. This field specifies that only events for the specified component (or components) should be delivered. If more than one component is present, the entire field must be enclosed in double quotes.

For example:

`comp=name`	a single component
`"comp=name1,name2,name3"`	multiple components

comp_type — Specifies events to be monitored. This must be one or more of the predefined types. The supported component types are: `univmax`, `univspa`, `univspv`, `jboss`, and `dbms`.

tgt — Specifies the target to which the daemon should log the events. Possible values are: `snmp`, `syslog`, `system`, and `file`.

The value you specify for *TGT* must match one of the values you specified in the `log_event_targets` parameter; otherwise, the daemon will not log events for this record.

The target you specify here will override the global `log_event_targets` setting described in

An example with 4 records or separate registrations is as follows:

```
storevntd:log_event_targets = syslog file
storevntd:log_symmetrix_events = \
  sid=000192600356, 1200,1201,1202 ;\
  sid=000192600357, "comp=0001,0002,0003",1204,1205 ;\
  1212,1213, thresh_major=60, thresh_warning=50, thresh_info=30 ;\
  tgt=file, sid=000194900123, status
```

Array event codes

The descriptions in this chapter are focused on running the event daemon in a logging mode - where events are automatically forwarded to a file on disk, syslog, SNMP, or the Windows Event Service.

Events below are described in the following format:

<Event-ID>	<Event-Name>
Category	<Event-Category>
Component	<Event-Component>
Severity	<Event-Severity>
Message	<Event-Message>

Where:

<Event-ID>	The event ID - from the SYMAPI_AEVENT2_UID_T enumeration in symapi.h
<Event-Name>	The internal name for this event.
<Event-Category>	The category that this event belongs to, if any. Registering against a category has the effect of registering for all events that belong to that category.
<Event-Component>	The component, if one is known, that the event is delivered with. For Event Logging (to file, Syslog, SNMP, Windows Events), the component will only be present if a specific component (for example: a specific device, disk, pool, ...) is known.[a]
<Event-Severity>	The severity that the event is delivered with: Fatal, Critical, Major, Minor, Warning, Info or Normal.
<Event-Message>	The message that the event is delivered with.

    a. The system ignores leading zero(es) when matching device numbers in event registrations against those in delivered events. That means if you register for events on device 01234 or 001234, events for device 1234 will be received.

Unless all events are delivered with an Entity-Name set to the Symmetrix ID that relates to the event.

Classes of Events

There are 3 general types of events:

- Event daemon events: Event IDs 0-199 on page 55 — Events in this range (there are only a handful) are generated by the event daemon itself - and reflect conditions within it.

- [Array Events: Event IDs 1050 - 1199](#) on page 56 — Events in this range correspond to entries retrieved from the 'Error' log on a storage array. Some of these are informational in nature; others correspond to actual errors.

- [Array Events: Event IDs 1200-1999](#) on page 89 — Events in this range are manufactured by the event daemon itself based on its regular polling of conditions on a storage array.

- [Event daemon events: Event IDs 5000-5200](#) on page 136 — Events in this range are generated by external producers.

Severity Calculation for status/state events

For a number of the array status events, an event severity is calculated dynamically from the status of the component in question (or overall array). In most cases, the mapping to severity is as follows:

Severity	Meaning
Normal	The component is now (back) in a normal state of operation.
Info	The component is no longer present (during certain operations).
Warning	The component is in a degraded sate of operation. The storage array is no longer present (during certain operations). The component is in an unknown state. The component is (where possible) in a write-disabled state.
Major	The component is offline.
Fatal	The component is in a dead or failed state.

Event daemon events: Event IDs 0-199

Events in this range are generated by the event daemon - and reflect its internal state.

They are automatically delivered to any registered applications as needed. There is no need to explicitly register for them.

1

1	SYMAPI_AEVENT2_UID_EVT_RESTARTED
Category	Event
Component	
Severity	Warning

1	SYMAPI_AEVENT2_UID_EVT_RESTARTED
Message	event daemon restarted; events may have been lost.

Notes

Generated when the event daemon is restarted after a crash.

2

2	SYMAPI_AEVENT2_UID_EVT_EVENTS_LOST
Category	Event
Component	
Severity	Warning
Message	event daemon communications problem; events may have been lost.
Unisphere policy name	**Event Lost Alert**
Action type	Alert

Notes

Generated when the event daemon encounters a communication problem attempting to send events back to a client.

3

3	SYMAPI_AEVENT2_UID_EVT_EVENTS_OVERFLOW
Category	Event
Component	
Severity	Warning
Message	Event Queue overflow; events may have been lost.
Unisphere policy name	**Event Overflow Alert**
Action type	Alert

Notes

Generated when one of the internal Event Queues (within a client process or event daemon) overflows and events are discarded.

Array Events: Event IDs 1050 - 1199

Events in this range correspond to entries retrieved from the Error log on a storage array. Some of these are informational in nature; others correspond to actual errors.

These correspond to events returned by the `symevent` SYMCLI command.

There are a number of categories that can be used to register for a related subset of these events.

- array subsystem

- db checksum
- diagnostic
- environmental
- device pool
- service processor
- srdf system
- srdf link
- srdfa session
- srdf consistency group
- director
- device
- disk

1050

1050	SYMAPI_AEVENT2_UID_MOD_DIAG_TRACE_TRIG
Category	diagnostic
Component	Diag [not present in logged events]
Severity	Info
Message	Diagnostic event trace triggered.

1051

1051	SYMAPI_AEVENT2_UID_MOD_DIAG_TRACE_TRIG_REM
Category	diagnostic
Component	Diagnostic [not present in logged events]
Severity	Info
Message	Remote (SRDF) diagnostic event trace triggered.

1052

1052	SYMAPI_AEVENT2_UID_MOD_ADAPT_CPY_WRT_PEND
Category	srdf system
Component	Director (for example, Director=SA-03C)
Severity	Warning
Message	Too many suspend/halt chains encountered, switching to Adaptive Copy Write Pending Mode.

Note

- System, Mainframe

- Set mode of operation

1053

1053	SYMAPI_AEVENT2_UID_MOD_DIR_MEM_ERR
Category	array subsystem
Component	Cache [not present in logged events]
Severity	Warning
Message	Memory bank(s) automatically disabled due to cache error.

1054

1054	SYMAPI_AEVENT2_UID_MOD_DISKDRV_SPARE_INVK
Category	disk
Component	Disk [not present in logged events]
Severity	Warning
Message	Spare invoked against a disk.

Unisphere policy name	**Hotspare Invoked**
Action type	Alert
Solutions Enabler mapping	This alert is registered as a result of registering for SYMAPI_AEVENT2_UID_ALERT_HOTSPARE_CHANGE

Notes

The following identifies the Symmetrix errors:

- 0x0006 — Spare invoked on a failing device.
- 0x0052 — Spare invoked (mirror mask changed).

1055

1055	SYMAPI_AEVENT2_UID_MOD_M2_RESYNC_M1
Category	device
Component	Device (For example, Device=1234)
Severity	Info
Message	M2 mirror resynchronizing with its M1 mirror.

Notes

Drive replacements/BCV activity. There is no action required because the drives are in a synchronized state.

1056

1056	SYMAPI_AEVENT2_UID_MOD_M1_RESYNC_M2
Category	device
Component	Device (For example, Device=1234)
Severity	Info
Message	M1 mirror resynchronizing with its M2 mirror.

Notes

Drive replacements/BCV activity. There is no action required because the drives are in a synchronized state.

1057

1057	SYMAPI_AEVENT2_UID_MOD_DSKSPS_NOT_RESP
Category	Director
Component	Director ID (For example, Director=SA-03C)
Severity	Fatal
Message	Disk director not responding.

Notes

Disk adapter may have failed; additional action may be required.

1058

1058	SYMAPI_AEVENT2_UID_MOD_JOB_DEV_MIGRATE_COMPLETE
Category	device
Component	Device (For example, Device=1234)
Severity	Info
Message	Data migration completed on all migration devices.

1059

1059	SYMAPI_AEVENT2_UID_MOD_RESYNC_STARTED
Category	device
Component	Device ID (For example, Device=1234)
Severity	Info
Message	Device resynchronization process started.

Notes

Drive replacements/BCV activity.

1060

1060	SYMAPI_AEVENT2_UID_MOD_RDF_HOTSPARE_INVK
Category	disk
Component	Disk [not present in logged events]
Severity	Warning
Message	Spare invoked against a remote R2 mirror disk.

Unisphere policy name	**Hotspare Invoked**
Action type	Alert
Solutions Enabler mapping	This alert is registered as a result of registering for SYMAPI_AEVENT2_UID_ALERT_HOTSPARE_CHANGE

Notes

Drive replacement required in remote RDF array; additional action may be required.

1061

1061	SYMAPI_AEVENT2_UID_MOD_RDF_SIM_MSG
Category	srdf system
Component	SRDF [not present in logged events]
Severity	Info
Message	SIM message initiated to a remote SRDF attached array.

Unisphere policy name	**SRDF Alerts**
Action type	Alert
Solutions Enabler mapping	This alert is registered as a result of registering for the event category SYMAPI_AEVENT2_CODE_CAT_SYMM_SRDF_SYS. This event category consists of all events with the category "srdf system".

Notes

Error is logged in a remote box and we are unsure what the error is.

1062

1062	SYMAPI_AEVENT2_UID_MOD_RDF_ERR
Category	srdf system
Component	SRDF [not present in logged events]
Severity	Major
Message	SRDF error occurred.

Unisphere policy name	SRDF Alerts
Action type	Alert
Solutions Enabler mapping	This alert is registered as a result of registering for the event category SYMAPI_AEVENT2_CODE_CAT_SYMM_SRDF_SYS. This event category consists of all events with the category "srdf system".

1063

1063	SYMAPI_AEVENT2_UID_MOD_FCPORT_FAIL
Category	director
Component	Director (For example, Director=SA-03C)
Severity	Major
Message	Fibre Channel front-end has failed or is inoperable.

Unisphere policy name	Port Link Status
Action type	Alert

1064

1064	SYMAPI_AEVENT2_UID_MOD_RDF_LINKS_DOWN
Category	srdf link
Component	SRDFA Gr (For example, SRDF-grp=1)
Severity	Minor
Message	No SRDF links in an RDF group are operational.

Unisphere policy name	SRDF Link Status
Action type	Alert/Refresh OM
Solutions Enabler mapping	This alert is registered as a result of registering for the event category SYMAPI_AEVENT2_CODE_CAT_SYMM_SRDF_LINK. This event category consists of all events with the category "srdf link".

Notes

This message indicates that all RDF links for a particular RDF group have become unavailable. Your R1 is up, but replication across the link is not occurring.

1065

1065	SYMAPI_AEVENT2_UID_MOD_RDF_LINKS_UP
Category	srdf link

1065	SYMAPI_AEVENT2_UID_MOD_RDF_LINKS_UP
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Info
Message	All SRDF links in an RDF group are operational.

Unisphere policy name	**SRDF Link Status**
Action type	Alert/Refresh OM
Solutions Enabler mapping	This alert is registered as a result of registering for the event category SYMAPI_AEVENT2_CODE_CAT_SYMM_SRDF_LINK. This event category consists of all events with the category "srdf link".

Notes

This message indicates that all RDF links for an RDF group are now operational.

1066

1066	SYMAPI_AEVENT2_UID_MOD_BUS_ARBITER_ERR
Category	array subsystem
Component	
Severity	Info
Message	Bus Arbiter problem.

1067

1067	SYMAPI_AEVENT2_UID_MOD_TEMP_OUT_OF_LIMIT
Category	environmental
Component	Env [not present in logged events]
Severity	Major or Critical
Message	Internal temperature too high.

Unisphere policy name	**Environmental Alert**
Action type	Alert
Solutions Enabler mapping	This alert is registered as a result of registering for the event category SYMAPI_AEVENT2_CODE_CAT_SYMM_ENV. This event category consists of all events with the category "Environmental".

Notes

Environmental errors can vary in severity. Contact Dell EMC immediately.

1068

1068	SYMAPI_AEVENT2_UID_MOD_ALARM_SIGNAL_ERR
Category	environmental
Component	Diag [not present in logged events]
Severity	Warning
Message	Alarm signal was set, but no alarm found.

1069

1069	SYMAPI_AEVENT2_UID_MOD_PWR_ALARM_SIGNAL
Category	environmental
Component	Power [not present in logged events]
Severity	Warning
Message	Power subsystem alarm or fault has occurred.

1070

1070	SYMAPI_AEVENT2_UID_MOD_DEV_MIR_NR
Category	device
Component	Device (For example, Device=1234)
Severity	Warning
Message	Device mirror not ready.

Notes

This message indicates that one of the mirrored devices is Not Ready. This may be due to BCV or Optimizer activity or a drive failure. A not ready device can indicate a potential problem. Please contact Dell EMC if you are unsure of how to proceed.

1071

1071	SYMAPI_AEVENT2_UID_MOD_DEV_MIR_WD
Category	device
Component	Device (For example, Device=1234)
Severity	Warning
Message	Device mirror write disabled.

Notes

A write disabled device can indicate a potential problem. Please contact Dell EMC if you are unsure of how to proceed.

1072

1072	SYMAPI_AEVENT2_UID_MOD_DEV_RDF_MIR_NR
Category	device
Component	Device (For example, Device=1234)
Severity	Warning
Message	SRDF R2 device not ready.

Notes

This message indicates that an R1 device has gone Not Ready on the RDF link without user intervention. The device is still physically Ready to the local hosts, but it is logically Not Ready to the R2 side. Therefore, remote replication is suspended. This can indicate a potential problem. Please contact Dell EMC if you are unsure of how to proceed.

1073

1073	SYMAPI_AEVENT2_UID_MOD_SP_NOT_RESP
Category	service processor
Component	
Severity	Major
Message	Service Processor down or not communicating with array.

Notes

This error occurs when we cannot communicate with the array to determine if any errors exist. Contact Dell EMC immediately.

1074

1074	SYMAPI_AEVENT2_UID_MOD_PHONEHOME_FAIL
Category	service processor
Component	Comm [not present in logged events
Severity	Warning
Message	Service Processor could not complete a call for service.

Notes

This error occurs when the array fails to dial home. If you have other errors on the array, this can be significant. Contact Dell EMC immediately.

1075

1075	SYMAPI_AEVENT2_UID_MOD_SENSOR_12V_ON
Category	environmental
Component	Power [not present in logged events]

1075	SYMAPI_AEVENT2_UID_MOD_SENSOR_12V_ON
Severity	Warning
Message	Abnormal DC voltage (perhaps 12 Volts) situation exists.

1076

1076	SYMAPI_AEVENT2_UID_MOD_PWR_CABLE_MISSING
Category	environmental
Component	Power [not present in logged events]
Severity	Warning
Message	Power subsystem environmental sense cable missing.

1077

1077	SYMAPI_AEVENT2_UID_MOD_COOL_AC_LINE_ERR
Category	environmental
Component	Power [not present in logged events]
Severity	Warning
Message	Power system AC line interruption detected.

1078

1078	SYMAPI_AEVENT2_UID_MOD_BATT_STATUS
Category	environmental
Component	Power [not present in logged events]
Severity	Warning
Message	Battery system not fully charged.

1079

1079	SYMAPI_AEVENT2_UID_MOD_PWR_LATCHED_ALARM
Category	environmental
Component	Power [not present in logged events]
Severity	Warning
Message	Latched alarms discovered for the power subsystem.

1080

1080	SYMAPI_AEVENT2_UID_MOD_RDF_1LINK_DOWN
Category	srdf link

1080	SYMAPI_AEVENT2_UID_MOD_RDF_1LINK_DOWN
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Warning
Message	Single SRDF link in an RDF group is not operational.
Unisphere policy name	**SRDF Link Status**
Action type	Alert/Refresh OM
Solutions Enabler mapping	This alert is registered as a result of registering for the event category SYMAPI_AEVENT2_CODE_CAT_SYMM_SRDF_LINK. This event category consists of all events with the category "srdf link".

Notes

This message indicates that one RDF link for a particular RDF group has become unavailable and data is no longer replicating across the link. Please contact Dell EMC if you are unsure about how to proceed.

1081

1081	SYMAPI_AEVENT2_UID_MOD_RDF_1LINK_UP
Category	srdf link
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Info
Message	Single SRDF link in an RDF group is now operational.
Unisphere policy name	**SRDF Link Status**
Action type	Alert/Refresh OM
Solutions Enabler mapping	This alert is registered as a result of registering for the event category SYMAPI_AEVENT2_CODE_CAT_SYMM_SRDF_LINK. This event category consists of all events with the category "srdf link".

1082

1082	SYMAPI_AEVENT2_UID_MOD_PHONEHOME_SUCCESS
Category	service processor
Component	Comm [not present in logged events]
Severity	Info
Message	Service Processor successfully completed a call for service.

1083

1083	SYMAPI_AEVENT2_UID_MOD_SP_SET_REG_ERR
Category	array subsystem
Component	
Severity	Warning
Message	Subsystem unable to set a shared register.

1084

1084	SYMAPI_AEVENT2_UID_MOD_MEM_DISABLED
Category	array subsystem
Component	Cache [not present in logged events]
Severity	Warning
Message	Disabled Memory Bank error reported to a host.

1085

1085	SYMAPI_AEVENT2_UID_MOD_DIAG_BIT_VLDTY_ERR
Category	environmental
Component	Diag [not present in logged events]
Severity	Warning
Message	Validity problem detected during environmental test.

1086

1086	SYMAPI_AEVENT2_UID_MOD_ENABLE_DIAG_ENV_TEST
Category	environmental
Component	Diag [not present in logged events]
Severity	Info
Message	Environmental testing enabled in diagnostic mode.

1087

1087	SYMAPI_AEVENT2_UID_MOD_SP_COMM_BRD_MISMATCH
Category	environmental
Component	Comm [not present in logged events]
Severity	Critical

1087	SYMAPI_AEVENT2_UID_MOD_SP_COMM_BRD_MISMATCH
Message	Communication board data does not match expected value.

1088

1088	SYMAPI_AEVENT2_UID_MOD_DIR_BRD_MISMATCH
Category	environmental
Component	Comm [not present in logged events]
Severity	Critical
Message	Communication board information mismtach.

1089

1089	SYMAPI_AEVENT2_UID_MOD_THRMLDET_TEST_FAIL
Category	environmental
Component	Env [not present in logged events]
Severity	Major
Message	Failure detected during thermal test.

1090

1090	SYMAPI_AEVENT2_UID_ALRM_PWR_TIME_TEST_FAIL
Category	environmental
Component	
Severity	Major
Message	Power-on-Time inconsistencies detected.

1091

1091	SYMAPI_AEVENT2_UID_MOD_SP_CONNECT_TIME_NOT_FOUND
Category	service processor
Component	Comm [not present in logged events]
Severity	Major
Message	No records found for the last Service Processor connection time.

1092

1092	SYMAPI_AEVENT2_UID_MOD_SP_COMM_VIA_SERIAL
Category	service processor
Component	Comm [not present in logged events]
Severity	Info
Message	Service Processor communicating via a serial line.

1093

1093	SYMAPI_AEVENT2_UID_MOD_REMMGMT_CONNECT
Category	service processor
Component	Comm [not present in logged events]
Severity	Info
Message	Remote session to the Service Processor connected.

1094

1094	SYMAPI_AEVENT2_UID_MOD_REMMGMT_REJECT
Category	service processor
Component	Comm [not present in logged events]
Severity	Info
Message	Remote session to the Service Processor denied access.

1095

1095	SYMAPI_AEVENT2_UID_MOD_REMMGMT_DISCONNECT
Category	service processor
Component	Comm [not present in logged events]
Severity	Info
Message	Remote session to the Service Processor disconnected.
service processor	

1096

1096	SYMAPI_AEVENT2_UID_ALRM_MEMERR_SP_MEM_ABOVE_LIMIT
Category	service processor
Component	SP [not present in logged events]

1096	SYMAPI_AEVENT2_UID_ALRM_MEMERR_SP_MEM_ABOVE_LIMIT
Severity	Warning
Message	Service Processor detected excessive memory usage.

Notes

Symmwin is using excessive memory on the service processor.

1097

1097	SYMAPI_AEVENT2_UID_MOD_BATT_TST_FAIL
Category	environmental
Component	Power [not present in logged events]
Severity	Warning
Message	Battery test detected a failure.

1098

1098	SYMAPI_AEVENT2_UID_MOD_SP_DIR_COMM_ERR
Category	service processor
Component	SP [not present in logged events]
Severity	Warning
Message	Service Processor could not communicate with a director.

1099

1099	SYMAPI_AEVENT2_UID_MOD_SP_DIR_QRY_ERR
Category	service processor
Component	SP [not present in logged events]
Severity	Warning
Message	Service Processor could not query a director.

1100

1100	SYMAPI_AEVENT2_UID_MOD_SP_COMM_VIA_DIR
Category	service processor
Component	SP [not present in logged events]
Severity	Info
Message	Service Processor is communicating via local director.

1101

1101	SYMAPI_AEVENT2_UID_MOD_SENSOR_READ_ERR
Category	service processor
Component	Env [not present in logged events]
Severity	Minor
Message	Service Processor unable to read an environmental sensor.

1102

1102	SYMAPI_AEVENT2_UID_MOD_SP_CARD_ERR
Category	service processor
Component	Comm [not present in logged events]
Severity	Minor
Message	Service Processor detected a failed or unrecognized communications card.

1103

1103	SYMAPI_AEVENT2_UID_MOD_ENV_READING_ABOVE_LIMIT
Category	environmental
Component	Env [not present in logged events]
Severity	Minor
Message	Service Processor is communicating via local director.

1104

1104	SYMAPI_AEVENT2_UID_MOD_SP_DISK_FULL
Category	service processor
Component	SP [not present in logged events]
Severity	Minor
Message	Service Processor disk is full.

1105

1105	SYMAPI_AEVENT2_UID_MOD_SMOKE_DET_MALF
Category	environmental
Component	Env [not present in logged events]
Severity	Minor

1105	SYMAPI_AEVENT2_UID_MOD_SMOKE_DET_MALF
Message	Service Processor detected a smoke detector malfunction.

1106

1106	SYMAPI_AEVENT2_UID_MOD_ALARM_SMOKE_DETECTED
Category	environmental
Component	Env [not present in logged events]
Severity	Minor
Message	Service Processor detected a smoke detector alert.

1107

1107	SYMAPI_AEVENT2_UID_MOD_PHONEHOME_TRIG
Category	service processor
Component	Comm [not present in logged events]
Severity	Info
Message	Service Processor triggered a call home for service.

Notes

Indicates that the service processor has called home for service. Please contact Dell EMC if you are unsure about how to proceed.

1108

1108	SYMAPI_AEVENT2_UID_MOD_DEV_CHKSUM
Category	checksum
Component	Device (For example: Device=1234)
Severity	Info
Message	Database Double Checksum event triggered.

1109

1109	SYMAPI_AEVENT2_UID_MOD_RDF_CG_TRIG
Category	srdf consistency group
Component	SRDF [not present in logged events]
Severity	Info
Message	RDF CG trip event triggered.

1110

1110	SYMAPI_AEVENT2_UID_MOD_SP_REBOOTED
Category	service processor
Component	SP [not present in logged events]
Severity	Info
Message	Service Processor successfully rebooted.

1111

1111	SYMAPI_AEVENT2_UID_MOD_SAVEDEVS_FULL
Category	device pool
Component	SnapPool, DSEPool or TPDataPool [not present in logged events]
Severity	Critical
Message	Save or data device pool is full.

Notes

The following defines what the Symmetrix errors mean:

- 0x0046 — SNAP device pool is full
- 0x0083 — DSE pool full
- 0x0085 — Unknown 6F1C error. Catchall
- 0x0086 — Thin pool is full

1112

1112	SYMAPI_AEVENT2_UID_MOD_RDFA_INACTIVE
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Warning
Message	RDF/A session inactive.

Unisphere policy name	**SRDF/A Session**
Action type	Alert
Solutions Enabler mapping	This alert is registered as a result of registering for the event category SYMAPI_AEVENT2_CODE_CAT_SYMM_SRDFA_SESS. This event category consists of all events with the category "srdfa session".

Notes

A full device pool may indicate a problem with replication. Please contact Dell EMC if you are unsure about how to proceed.

1113

1113	SYMAPI_AEVENT2_UID_MOD_RDFA_ACTIVE
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Info
Message	SRDF/A session active.

Unisphere policy name	SRDF/A Session
Action type	Alert
Solutions Enabler mapping	This alert is registered as a result of registering for the event category SYMAPI_AEVENT2_CODE_CAT_SYMM_SRDFA_SESS. This event category consists of all events with the category "srdfa session".

1114

1114	SYMAPI_AEVENT2_UID_MOD_DEV_NR
Category	device
Component	Device (For example, Device=1234)
Severity	Warning
Message	Volume (device) not ready.

Notes

A Not Ready device may indicate a problem with a specific device. Please contact Dell EMC if you are unsure about how to proceed.

1115

1115	SYMAPI_AEVENT2_UID_MOD_SAVEDEVS_NEAR_FULL
Category	device pool
Component	SnapPool, DSEPool or TPDataPool [not present in logged events]
Severity	Warning
Message	Save or data device pool is almost full.

Notes

The following defines what the Symmetrix errors mean:

- 0x0047 — DSE pool is at 90% capacity

- 0x0081 — Spillover pool at 90% capacity

- 0x0082 — Thin pool at 90% capacity

- 0x0084 — Unknown 0471 error (all other errors)

1116

1116	SYMAPI_AEVENT2_UID_MOD_DEV_SAVEDEV_NR
Category	device pool
Component	SnapPool, DSEPool or TPDataPool [not present in logged events]
Severity	Major
Message	Active Data device or Save device in a pool is not ready.

Notes

Indicates a device has become Not Ready in one of the device pools. Please contact Dell EMC if you are unsure about how to proceed.

1117

1117	SYMAPI_AEVENT2_UID_MOD_DIR_NOT_RESP
Category	director
Component	Director (For example, Director=SA-03C)
Severity	Fatal
Message	Director not responding.

Notes

Indicates a director has stop responding. This may be a serious problem. Please contact Dell EMC if you are unsure about how to proceed.

1118

1118	SYMAPI_AEVENT2_UID_MOD_TIMEOUT_R2_WP_LIMIT
Category	srdf system
Component	SRDF [not present in logged events]
Severity	Major
Message	Timeout writing to an R2 device; writes pending limit reached.

1119

1119	SYMAPI_AEVENT2_UID_MOD_SESS_DROP_WPL_DSBL
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)

1119	SYMAPI_AEVENT2_UID_MOD_SESS_DROP_WPL_DSBL
Severity	Major
Message	SRDF/A session dropped: write pending limit reached. Host throttling is disabled.

1120

1120	SYMAPI_AEVENT2_UID_MOD_SESS_DROP_WPL_ENBL
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Major
Message	SRDF/A session dropped: write pending limit reached. Host throttling is enabled.

1121

1121	SYMAPI_AEVENT2_UID_MOD_SESS_DROP_DEV_NR_OFF
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Major
Message	SRDF/A session dropped: device not ready. Tolerance mode is off.

1122

1122	SYMAPI_AEVENT2_UID_MOD_SESS_DROP_DEV_NR_CG
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Major
Message	SRDF/A session dropped: device not ready through consistency group.

1123

1123	SYMAPI_AEVENT2_UID_MOD_SESS_DROP_NO_RDF_LNK
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Major
Message	SRDF/A session dropped: no SRDF links operational.

Unisphere policy name	**SRDF/A Session**
Action type	Alert
Solutions Enabler mapping	This alert is registered as a result of registering for the event category SYMAPI_AEVENT2_CODE_CAT_SYMM_SRDFA_SESS. This event category consists of all events with the category "srdfa session".

Notes

Indicates that the SRDF links may no longer be operational. Please contact Dell EMC if you are unsure how to proceed.

1124

1124	**SYMAPI_AEVENT2_UID_MOD_SESS_DROP_TIMEOUT_MSC**
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Major
Message	SRDF/A session dropped: timeout in MSC mode.

1125

1125	**SYMAPI_AEVENT2_UID_MOD_SESS_DROP_TIMEOUT_HA**
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Major
Message	SRDF/A session dropped: timeout on Host Adapter.

1126

1126	**SYMAPI_AEVENT2_UID_MOD_SESS_DROP_TIMEOUT_RA**
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Major
Message	SRDF/A session dropped: timeout on RA.

1127

1127	**SYMAPI_AEVENT2_UID_MOD_GEN_CHKSUM**
Category	checksum

1127	SYMAPI_AEVENT2_UID_MOD_GEN_CHKSUM
Component	Device (For example, Device=1234)
Severity	Info
Message	Generic Double Checksum event triggered.

1128

1128	SYMAPI_AEVENT2_UID_MOD_POW_ZONE_COUNTDOWN_STARTED
Category	environmental
Component	Power [not present in logged events]
Severity	Minor
Message	One of the Power Zones is down - shutdown will occur in 20 hours.

1129

1129	SYMAPI_AEVENT2_UID_MOD_POW_ZONE_5HOURS_TO_GO
Category	environmental
Component	Power [not present in logged events]
Severity	Major
Message	One of the Power Zones is down - shutdown will occur in 5 hours.

1130

1130	SYMAPI_AEVENT2_UID_MOD_SRDFA_DROP_FROM_HOST
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Major
Message	SRDF/A session drop requested [host software initiated].

Unisphere policy name	SRDF/A Session
Action type	Alert
Solutions Enabler mapping	This alert is registered as a result of registering for the event category SYMAPI_AEVENT2_CODE_CAT_SYMM_SRDFA_SESS. This event category consists of all events with the category "srdfa session".

1131

1131	SYMAPI_AEVENT2_UID_MOD_SRDFA_DROP_PEND_FROM_HOST
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Major
Message	SRDF/A session drop at cycle boundary requested [host software initiated].
Unisphere policy name	**SRDF/A Session**
Action type	Alert
Solutions Enabler mapping	This alert is registered as a result of registering for the event category SYMAPI_AEVENT2_CODE_CAT_SYMM_SRDFA_SESS. This event category consists of all events with the category "srdfa session".

1132

1132	SYMAPI_AEVENT2_UID_MOD_SRDFA_DEACTIV_FROM_HOST
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Major
Message	SRDF/A session transition out of Asynchronous mode requested [host software initiated].
Unisphere policy name	**SRDF/A Session**
Action type	Alert
Solutions Enabler mapping	This alert is registered as a result of registering for the event category SYMAPI_AEVENT2_CODE_CAT_SYMM_SRDFA_SESS. This event category consists of all events with the category "srdfa session".

1133

1133	SYMAPI_AEVENT2_UID_MOD_SRDFA_CONS_DEACTIV_FROM_HOST
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Major

1133	SYMAPI_AEVENT2_UID_MOD_SRDFA_CONS_DEACTIV_FROM_HOST
Message	SRDF/A session transition from Asynchronous to Synchronous mode requested [host software initiated].

Unisphere policy name	SRDF/A Session
Action type	Alert
Solutions Enabler mapping	This alert is registered as a result of registering for the event category SYMAPI_AEVENT2_CODE_CAT_SYMM_SRDFA_SESS. This event category consists of all events with the category "srdfa session".

1134

1134	SYMAPI_AEVENT2_UID_MOD_SRDFA_DROP
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Major
Message	SRDF/A session drop requested.

Unisphere policy name	SRDF/A Session
Action type	Alert
Solutions Enabler mapping	This alert is registered as a result of registering for the event category SYMAPI_AEVENT2_CODE_CAT_SYMM_SRDFA_SESS. This event category consists of all events with the category "srdfa session".

1135

1135	SYMAPI_AEVENT2_UID_MOD_SRDFA_DROP_PEND
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Major
Message	SRDF/A session drop at cycle boundary requested.

Unisphere policy name	SRDF/A Session
Action type	Alert
Solutions Enabler mapping	This alert is registered as a result of registering for the event category SYMAPI_AEVENT2_CODE_CAT_SYMM_SRDFA_SESS. This

1136

1136	SYMAPI_AEVENT2_UID_MOD_SRDFA_DEACTIV
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Major
Message	SRDF/A session transition out of Asynchronous mode requested.

1137

1137	SYMAPI_AEVENT2_UID_MOD_SRDFA_CONS_DEACTIV
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Major
Message	SRDF/A session transition from Asynchronous to Synchronous mode requested.

Notes

- ...

1138

1138	SYMAPI_AEVENT2_UID_MOD_SRDFA_SE_TRANS_IDLE,
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Info
Message	SRDF/A Session entering transmit idle state.
Unisphere policy name	**SRDF/A Session entering transmit idle state**
Action type	Alert

1139

1139	SYMAPI_AEVENT2_UID_MOD_SRDFA_SR_TRANS_IDLE,
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Info

1139	SYMAPI_AEVENT2_UID_MOD_SRDFA_SR_TRANS_IDLE,
Message	SRDF/A Session recovered from a transmit idle state.
Unisphere policy name	**SRDF/A Session recovered from a transmit idle state**
Action type	Alert

1140

1140	SYMAPI_AEVENT2_UID_MOD_SRDFA_TO_TRANS_IDLE
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Major
Message	SRDF/A Session dropped, transmit idle state timeout.
Unisphere policy name	**SRDF/A Session dropped, transit idle state timeout**
Action type	Alert

1141

1141	SYMAPI_AEVENT2_UID_MOD_SRDFA_SD_NO_ONL_RA
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Major
Message	SRDF/A Session dropped, no online RAs.

1142

1142	SYMAPI_AEVENT2_UID_MOD_PSA_M_FAN_FAULT
Category	environmental
Component	Fan [not present in logged events]
Severity	Major
Message	Power Supply A multiple Fan fault.

1143

1143	SYMAPI_AEVENT2_UID_MOD_PSA_S_FAN_FAULT
Category	environmental
Component	Fan [not present in logged events]
Severity	Major
Message	Power Supply A single Fan fault.

1144

1144	SYMAPI_AEVENT2_UID_MOD_PSA_FAULTED
Category	environmental
Component	Power [not present in logged events]
Severity	Major
Message	Power Supply A faulted.

1145

1145	SYMAPI_AEVENT2_UID_MOD_PSA_SHUTDOWN
Category	environmental
Component	Power [not present in logged events]
Severity	Major
Message	Power Supply A shutdown.

1146

1146	SYMAPI_AEVENT2_UID_MOD_PSB_M_FAN_FAULT
Category	environmental
Component	Fan [not present in logged events]
Severity	Major
Message	Power Supply B multiple fan fault.

1147

1147	SYMAPI_AEVENT2_UID_MOD_PSB_S_FAN_FAULT
Category	environmental
Component	Fan [not present in logged events]
Severity	Major
Message	Power Supply B single fan fault.

1148

1148	SYMAPI_AEVENT2_UID_MOD_PSB_FAULTED
Category	environmental
Component	Power [not present in logged events]
Severity	Major
Message	Power Supply B single fan fault.

1149

1149	SYMAPI_AEVENT2_UID_MOD_PSB_SHUTDOWN
Category	environmental
Component	Power [not present in logged events]
Severity	Major
Message	Power Supply B shutdown.

1150

1150	SYMAPI_AEVENT2_UID_MOD_LCC_A_TEMP_HIGH
Category	environmental
Component	LCC [not present in logged events]
Severity	Major
Message	Link Card Controller A temperature high.

Unisphere policy name	**Environmental Alert**
Action type	Alert
Solutions Enabler mapping	This alert is registered as a result of registering for the event category SYMAPI_AEVENT2_CODE_CAT_SYMM_ENV. This event category consists of all events with the category "Environmental".

1151

1151	SYMAPI_AEVENT2_UID_MOD_LCC_B_TEMP_HIGH
Category	environmental
Component	LCC [not present in logged events]
Severity	Major
Message	Link Card Controller B temperature high.

Unisphere policy name	**Environmental Alert**
Action type	Alert
Solutions Enabler mapping	This alert is registered as a result of registering for the event category SYMAPI_AEVENT2_CODE_CAT_SYMM_ENV. This event category consists of all events with the category "Environmental".

1152

1152	SYMAPI_AEVENT2_UID_MOD_SPS_INTRN_FAULT
Category	environmental
Component	Power [not present in logged events]
Severity	Major
Message	Supplemental Power Supply internal fault.

1153

1153	SYMAPI_AEVENT2_UID_MOD_SPS_BAT_ENDLINE
Category	environmental
Component	Power [not present in logged events]
Severity	Major
Message	Supplemental Power Supply battery end of line.

1154

1154	SYMAPI_AEVENT2_UID_MOD_SPS_LOW_VOLTAGE
Category	environmental
Component	Power [not present in logged events]
Severity	Major
Message	Supplemental Power Supply low input AC Voltage.

1155

1155	SYMAPI_AEVENT2_UID_MOD_AUDIT_HIGH_ACTIVITY
Category	array subsystem
Component	
Severity	Warning
Message	Entries are being written to the audit log at an unusually high rate.

1156

1156	SYMAPI_AEVENT2_UID_MOD_AUDIT_SFS_MIRR_OFF
Category	array subsystem
Component	
Severity	Major

1156	SYMAPI_AEVENT2_UID_MOD_AUDIT_SFS_MIRR_OFF
Message	Audit log has lost its redundancy due to an SFS mirror being offline.

1157

1157	SYMAPI_AEVENT2_UID_MOD_AUDIT_LOG_WRAPPED
Category	array subsystem
Component	
Severity	Warning
Message	Audit log entries have been overwritten in an unusually short time period.

1158

1158	SYMAPI_AEVENT2_UID_MOD_SRDFA_DROP_WPL_CP
Category	srdfa session
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Major
Message	SRDF/A Session dropped, write pending limit reached on a cache partition.

Unisphere policy name	SRDF/A Session
Action type	Alert
Solutions Enabler mapping	This alert is registered as a result of registering for the event category SYMAPI_AEVENT2_CODE_CAT_SYMM_SRDFA_SESS. This event category consists of all events with the category "srdfa session".

Notes

The following identifies what each Symmetrix error means:

- 0x0079 — SNOW dropped due to WP limit being reached in cache partion 0
- 0x007A — SNOW dropped due to WP limit being reached in cache partion 1
- 0x007B — SNOW dropped due to WP limit being reached in cache partion 2
- 0x007C — SNOW dropped due to WP limit being reached in cache partion 3
- 0x007D — SNOW dropped due to WP limit being reached in cache partion 4
- 0x007E — SNOW dropped due to WP limit being reached in cache partion 5
- 0x007F — SNOW dropped due to WP limit being reached in cache partion 6
- 0x0080 — SNOW dropped due to WP limit being reached in cache partion 7

1159

1159	SYMAPI_AEVENT2_UID_ALERT_SRDFA_NO_CYCLE_SWITCH
Category	srdf system
Component	SRDF [not present in logged events]
Severity	Warning
Message	There has been no SRDF/A cycle switching within the past hour.

Unisphere policy name	**SRDF/A No Cycle Switch Alert**
Action type	Alert

1160

1160	SYMAPI_AEVENT2_UID_ALERT_SRDF_JFC_STATE_CHANGE,
Category	srdf link
Component	SRDFA Grp (For example, SRDF-grp=1)
Severity	Warning
Message	The job flow control setting has changed on RDF group.

Unisphere policy name	**SRDF Job Flow Control Change**
Action type	Alert

1161

1161	SYMAPI_AEVENT2_UID_ALERT_SRP_SNAP_CAP_EXCEEDED
Category	device pool
Component	SnapPool, DSEPool or TPDataPool [not present in logged events]
Severity	WARNING
Message	The maximum SRP snapshot/RDFA DSE capacity has been exceeded.

1162

1162	SYMAPI_AEVENT2_UID_ALERT_EDISK_FULL
Category	disk
Component	Disk [not present in logged events]

1162	SYMAPI_AEVENT2_UID_ALERT_EDISK_FULL
Severity	Warning
Message	External disk group is fully allocated.

Unisphere policy name	**External disk group fully allocated**
Action type	Alert

1163

1163	SYMAPI_AEVENT2_UID_MOD_RDF_1PATH_DOWN
Category	srdf link
Component	SRDF
Severity	Warning
Message	Sinlge SRDF Path is not operational.

Unisphere policy name	**Sinlge SRDF Path is not operational**
Action type	Alert

Note: This event is only supported from HYPERMAX OS 5977.

1164

1164	SYMAPI_AEVENT2_UID_MOD_DIR_PSA_OVER_TEMP
Category	environmental
Component	Director
Severity	Warning
Message	Director Power Supply A Over temperature.

Note: This event is only supported from PowerMaxOS 5978.

1165

1165	SYMAPI_AEVENT2_UID_MOD_DIR_PSB_OVER_TEMP
Category	environmental
Component	Directory
Severity	Warning
Message	Director Power Supply B Over temperature.

Note: This event is only supported from PowerMaxOS 5978.

1166

1166	SYMAPI_AEVENT2_UID_MOD_DIR_OVER_TEMP
Category	environmental
Component	Director
Severity	Warning
Message	Director Power Supply Over temperature.

Note: This event is only supported from PowerMaxOS 5978.

1167

1167	SYMAPI_AEVENT2_UID_MOD_RDF_1PATH_UP
Category	srdf link
Component	SRDF
Severity	Warning
Message	Sinlge SRDF Path in an RDF group is now operational.
Unisphere policy name	**Sinlge SRDF Path is now operational**
Action type	Alert

Note: This event is only supported from HYPERMAX OS 5977.

Array Events: Event IDs 1200-1999

Events in this range are manufactured by the event daemon itself based on its regular polling of conditions on a storage array.

There are two categories that can be used to register for a related of these events:

- status
- optimizer

1200

1200	SYMAPI_AEVENT2_UID_ALERT_DEV_STATUS
Category	status
Component	Device number Device =1234
Severity	If Online: Normal If Online Degraded: Warning If Offline: Major If Not Present: Info

1200	SYMAPI_AEVENT2_UID_ALERT_DEV_STATUS
Message	Device state has changed to [Not Present | Unknown | Online | Write Disabled | Offline | Failed].
Unisphere policy name	**Device Status**
Action type	Alert

Notes

- 'Not Present' means that the device could not be seen by Solutions Enabler.
- 'Online' means that the device service state is normal.
- 'Failed' means that there was a problem communicating with the array.

1201

1201	SYMAPI_AEVENT2_UID_ALERT_ARRAY_STATUS
Category	status
Component	
Severity	If Online: Normal If Online Degraded: Warning If Offline: Major If Not Present: Warning or Major (depending on situation) If Unknown: Warning or Major (depending on situation)
Message	Array state has changed to [Not Present | Unknown | Online | Write Disabled | Offline | Failed].

Notes

- This event reflects the overall state of the array - including its Disks, Directors, Ports.
- 'Not Present' means that the array couldn't be seen by Solutions Enabler.
- 'Online' means that the array is operational.
- 'Unknown' means that:
  - One or more Ports are in an Offline or Write-Disabled state.
  - One or more Directors are in an Offline or Dead state.
  - Device events [1200] events are also enabled and one or more device is in a Not-Ready state.
  - Array sub-component events [1404] are also enabled and one or more are in a failed (Offline) state (Fans, Power Supplies, LCCs, MIBEs, Enclosures, etc.).
- 'Failed' means that there was a problem communicating with the array.

1202

1202	SYMAPI_AEVENT2_UID_ALERT_DIRECTOR_STATUS
Category	status
Component	Director identifier For example: Director=SA-03C
Severity	If Online: Normal If Online Degraded: Warning If Offline: Major If Failed: Fatal If Not Present: Info
Message	Director state has changed to [Not Present | Unknown | Online | Write Disabled | Offline | Failed].

Unisphere policy name	**Director Status**
Action type	Alert

Notes

- 'Not Present' means the director was not seen by Solutions Enabler.
- 'Online' means that the director status is Online.
- 'Online [Degraded]' means that one or more of the director's ports were in an Offline or Write-Disabled state.
- 'Offline' means that the director status is Offline.
- 'Failed' means that the director status is Dead.

1203

1203	SYMAPI_AEVENT2_UID_ALERT_PORT_STATUS
Category	status
Component	Port identifier For example: Port=SA-03C:2 (for Port 2 on Director SA-03C)
Severity	If Online: Normal If Offline: Major If Write Disabled: Warning If Unknown: Warning

1203	SYMAPI_AEVENT2_UID_ALERT_PORT_STATUS
	If Not Present: Info
Message	Port state has changed to Not Present | Unknown | Online | Write Disabled | Offline | Failed

Unisphere policy name	**Port Status**
Action type	Alert

Indicates that the status for some Director Port has changed.

Notes

- 'Not Present' means the port was not seen.
- 'Online' means a port status of On.
- 'Offline' means a port status of Off.
- 'Write Disabled' means a port status of Write-Disabled.

1204

1204	SYMAPI_AEVENT2_UID_ALERT_DISK_STATUS
Category	status
Component	Spindle ID (Disk identifier is supported for internal disks only) For example: Disk=123 or Disk=16B:C2 (for Director 16B, DA Interface C, SCSI ID/Target 2) (internal disks only)
Severity	If Online: Normal If Online Spare: Normal If Online Degraded: Warning If Offline: Warning If Offline Spare: Warning If Not Present: Info
Message	Disk state is now <State> Where State can be: Online Offline

1204	SYMAPI_AEVENT2_UID_ALERT_DISK_STATUS
	Online Spare Offline Spare Online Degraded Not Present

Unisphere policy name	**Disk status**
Action type	Alert

Notes

- 'Not Present' means that the disk could not be seen by Solutions Enabler.
- 'Online' means that one or more of the disk's Hypers are in a Ready state.
- 'Online Spare' means that the disk is a Spare and one or more of the disk's Hypers are in a Ready state.
- 'Online [Degraded]' means that the disk can only be reached via a single array DS controller. This disk state is for external disk only and supported with Enginuity 5876 and later.
- 'Offline' means that all of the disk's Hypers are in a Not-Ready state.
- 'Offline Spare' means that the disk is a Spare and all of the disk's Hypers are in a Not-Ready state

1205

1205	SYMAPI_AEVENT2_UID_ALERT_DEV_CONFIG_CHANGE
Category	status
Component	Device number For example: Device=1234
Severity	Info
Message	Device configuration has changed.

Unisphere policy name	**Device Config Change**
Action type	Alert/Refresh OM

Indicates that the configuration of some device has changed.

Notes

- The following aspects of a device's configuration is considered by this event:
  - The base device configuration.
  - The meta configuration of the device (META_HEAD, META_MEMBER).

- The bound-vs-bound state of a TDEV (bound vs unbound).
- Whether a dynamic spare disk is invoked for the device.
- The RDF mode of the device (of either leg for Concurrent SRDF).
- The data pool bound to by a TDEV changes. This reflects a device being bound, unbound or re-bound to a different pool, and is also triggered when the name of the pool changes.

1206

1206	SYMAPI_AEVENT2_UID_ALERT_POOL_STATUS
Category	status
Component	Pool name For example: SnapPool=Sales, DSEPool=Finance, TPDataPool=Eng
Severity	If Online: Normal If Online Degraded: Warning If Offline: Major If Not Present: Info
Message	Snap Savedev Pool state has changed to Not Present | Unknown | Online | Write Disabled | Offline | Failed SRDF/A DSE Pool state has changed to Not Present | Unknown | Online | Write Disabled | Offline | Failed Data Pool state has changed to Not Present | Unknown | Online | Write Disabled | Offline | Failed

Unisphere policy name	**Device Pool Status**
Action type	Alert

Indicates that the status of a Snap, SRDF/A DSE or ThinData Pool has changed.

Notes

- 'Not Present' means that the pool no longer exists.
- 'Online' means that the pool is in an enabled.'
- 'Online [Degraded]' means that the pool is in a mixed state.

- 'Offline' means that the pool is in a disabled state.

1207

1207	SYMAPI_AEVENT2_UID_ALERT_POOL_CONFIG_CHANGE
Category	status
Component	Pool name For example: SnapPool=Sales, DSEPool=Finance, TPDataPool=Eng
Severity	Info
Message	Snap Savedev Pool configuration has changed. SRDF/A DSE Pool configuration has changed. Data Pool configuration has changed.

Unisphere policy name	**Device Pool Config Change**
Action type	Alert

Indicates that the configuration of a Snap, SRDF/A DSE or ThinData Pool has changed.

Notes

- A pool's configuration changes if:
  - The set of Enabled devices in the pool changes.
  - The total size (free + used) of all the Enabled devices in the pool changes.

1208

1208	SYMAPI_AEVENT2_UID_THRESH_POOL_FREESPACE
Category	status
Component	Pool name For example: SnapPool=Sales, DSEPool=Finance, TPDataPool=Eng
Severity	Determined by Threshold values. See below.
Message	Snap Savedev Pool utilization is now <NN> percent. SRDF/A DSE Pool utilization is now <NN> percent.

1208	SYMAPI_AEVENT2_UID_TH RESH_POOL_FREESPACE
	Data Pool utilization is now <NN> percent.

Unisphere policy name	**Device Pool Free Space**
Action type	Alert

This is a Threshold event that reflects the amount (as a percentage) of used space within a pool.

Unless threshold values are supplied with the registration, the following defaults are used to derive an event severity:

If value is 100% — Fatal

If value is >= 80% — Critical

If value is >= 70% — Major

If value is >= 65% — Minor

If value is >= 60% — Warning

Otherwise — Normal

Notes

- Used space size is determined by calls to SymPoolShow().

- Events are only delivered at multiples of 5% ... for <NN> equal to 5%, 10%, 15%, ... , 75%, 80%, 85%, 90%, 95% and 100%.

- Threshold events are only delivered when the severity, as determined by threshold values, changes.

1209

1209	SYMAPI_AEVENT2_UID_AL ERT_SEL_CHANGE
Category	status
Component	Symmetrix Lock Number For example: SEL=15
Severity	Info
Message	Symmetrix External Lock has been acquired. Symmetrix External Lock has been released.

Indicates that the state (released vs acquired) of one of the monitored Symmetrix External Locks (SELs) has changed.

Note

At this time, only SEL #15 (used by Config Change) is monitored.

1210

1210	SYMAPI_AEVENT2_UID_ALERT_HOTSPARE_CHANGE
Category	status
Component	Disk identifier of the Spare For example: Disk=16B:C2 (for Director 16B, DA InterfaceC, SCSI ID/Target 2)
Severity	For 5x74 and newer arrays: Normal For older arrays: If invoked: Warning If no longer invoked: Normal
Message	For 5x74 and newer arrays: Disk is lo longer a Spare. Disk is now a Spare. Disk is now an invoked Spare. For older arrays: Spare has been invoked against a failed disk. Spare is no longer invoked against a failed disk.

Unisphere policy name	**Hotspare Invoked**
Action type	Alert
Solutions Enabler mapping	This alert is registered as a result of registering for SYMAPI_AEVENT2_UID_ALERT_HOTSPARE_CHANGE

Indicates that a disk has started or stopped acting as a spare.

Note

With Permanent Sparing on newer arrays, a failing disk and a spare will exchange roles. The failed disk will end up as a failed spare, and the spare will end up as a normal disk. The "Disk is now an invoked Spare" event will rarely if ever be delivered.

1211

1211	SYMAPI_AEVENT2_UID_ALERT_NUM_HOTSPARES_T
Category	status
Component	

1211	SYMAPI_AEVENT2_UID_AL ERT_NUM_HOTSPARES_T
Severity	Determined by Threshold values. See below.
Message	Number of available disk spares is <NN>.

This is a Threshold event that reflects the number of available Spare Disks on the storage array.

Unless threshold values are supplied with the registration, the following defaults are used to derive an event severity:

If value is 0 — Critical

If value is 1 — Major

If value is 2 — Warning

Otherwise — Info

Note

Threshold events are only delivered when the severity, as determined by threshold values, changes.

1212

1212	SYMAPI_AEVENT2_UID_TH RESH_TDEV_ALLOCATED
Category	status
Component	Device number For example: Device=1234
Severity	Determined by Threshold values. See below.
Message	Thin Device is now <NN> percent allocated.

Unisphere policy name	**Thin Device Allocation**
Action type	Alert

This is a Threshold event that reflects the amount (as a percentage) of a Thin Device that is backed by space in a Data Pool.

Unless threshold values are supplied with the registration, the following defaults are used to derive an event severity:

If value is 100% — Fatal

If value is >= 80% — Critical

If value is >= 70% — Major

If value is >= 65% — Minor

If value is >= 60% — Warning

Otherwise — Normal

Notes

- Events are only delivered at multiples of 5% ... for <NN> equal to 5%, 10%, 15%, ... , 75%, 80%, 85%, 90%, 95% and 100%.

- Threshold events are only delivered when the severity, as determined by threshold values, changes.

1213

1213	SYMAPI_AEVENT2_UID_THRESH_TDEV_USED
Category	status
Component	Device number For example: Device=1234
Severity	Determined by Threshold values. See below.
Message	Thin Device is now <NN> percent used.

Unisphere policy name	**Thin Device Usage**
Action type	Alert

This is a Threshold event that reflects the amount (as a percentage) of a Thin Device that has been written to.

Unless threshold values are supplied with the registration, the following defaults are used to derive an event severity:

If value is 100% — Fatal

If value is >= 80% — Critical

If value is >= 70% — Major

If value is >= 65% — Minor

If value is >= 60% — Warning

Otherwise — Normal

Notes

- Events are only delivered at multiples of 5% ... for <NN> equal to 5%, 10%, 15%, ... , 75%, 80%, 85%, 90%, 95% and 100%.

- Threshold events are only delivered when the severity, as determined by threshold values, changes.

1214

1214	SYMAPI_AEVENT2_UID_ALERT_DIRECTOR_CONFIG_CHANGE
Category	status

1214	SYMAPI_AEVENT2_UID_ALERT_DIRECTOR_CONFIG_CHANGE
Component	Director
Severity	Info
Message	Director configuration has changed.

Indicates that the configuration changed for a Director.

1215

1215	SYMAPI_AEVENT2_UID_ALERT_PORT_CONFIG_CHANGE
Category	status
Component	Port For example: Port=SA-03C:2 (for Port 2 on Director SA-03C)
Severity	Info
Message	Port configuration has changed.

Indicates that the configuration changed for a Port on a Front End (FE) Director.

Notes

- The only aspects of a port's configuration that are considered the following flags from the FA port flags:
- The _VCM_ENABLED flag.
- The _VOL_SET_ADDR (VSA) flag.

1216

1216	SYMAPI_AEVENT2_UID_ALERT_POOL_DEV_STATE_CHANGE
Category	status
Component	Pool name For example: SnapPool=Sales , DSEPool=Finance , TPDataPool=Eng
Severity	Info

1216	SYMAPI_AEVENT2_UID_ALERT_POOL_DEV_STATE_CHANGE
Message	Snap Savedev Pool device state has changed. SRDF/A DSE Pool device state has changed. Data Pool device state has changed.

Indicates that the state of a device in a Snap, SRDF/A DSE or ThinData Pool has changed.

1217

1217	SYMAPI_AEVENT2_UID_DFR_SVC_STATE
Category	status
Component	
Severity	If the replacement threshold has been exceeded : Warning Otherwise: Info
Message	The deferred services replacement threshold has been exceeded - service is required. The deferred services replacement threshold is no longer exceeded.

Unisphere policy name	**Deferred Service Threshold Alert**
Action type	Alert

Indicates that the Deferred Service replacement threshold indicator for a storage array has changed. This change can be in either direction - from not-exceeded to exceeded ... or from exceeded to not-exceeded.

Note

- This event will only be generated if Deferred Service is enabled for the storage array.

1218

1218	SYMAPI_AEVENT2_UID_DEV_CFG_CHKSUM
Category	status
Component	Device number For example: Device=1234

1218	SYMAPI_AEVENT2_UID_DEV_CFG_CHKSUM
Severity	Info
Message	The device configuration checksum has changed.

Indicates that the configuration of a device has changed. The implementation makes use of a checksum maintained by the event daemonover a device's core configuration data. An event is generated when this checksum changes.

1219

1219	SYMAPI_AEVENT2_UID_MIGRATE_COMPLETE
Category	status
Component	Migrate Session name For example: MigrSess=jones17
Severity	If success: Info If terminated: Info If timed out: Warning If failed: Major
Message	The migrate operation is complete: success. The migrate operation is complete: timed out. The migrate operation is complete: terminated. The migrate operation is complete: failed.

Unisphere policy name	**Migration Complete Alert**
Action type	Alert

Indicates that a VLUN migration has completed or failed.

Note

- This is only generated for explicitly initiated VLUN migrations - not movements being performed by FAST.

1220

1220	SYMAPI_AEVENT2_UID_POOL_REBAL_COMPLETE
Category	status

1220	SYMAPI_AEVENT2_UID_POOL_REBAL_COMPLETE
Component	The Data Pool name. For example: TPDataPool=Eng
Severity	If success: Info If terminated: Info If timed out: Warning If failed: Major
Message	Thin Pool rebalancing operation is complete: success. Thin Pool rebalancing operation is complete: timed out. Thin Pool rebalancing operation is complete: terminated. Thin Pool rebalancing operation is complete: failed.

Unisphere policy name	Thin Pool Rebalancing Complete Alert
Action type	Alert

Indicates that a Thin Pool rebalancing activity has completed.

Note

This event is only supported for Symmetrix arrays running Enginuity 5875.

1221

1221	SYMAPI_AEVENT2_UID_ALERT_SPINDLE_STATUS
Category	status
Component	Device number; for example: Device=1234
Severity	Determined by status.
Message	Disk state is now [Online | Offline | Online Degraded | Online Spare | Offline Spare].

Note

The following values are used to derive an event severity:

- If Online — Normal

- If Offline — Warning
- If Degraded — Warning

1222

1222	SYMAPI_AEVENT2_UID_ALERT_LREP_CACHEUSE_PCT_CHG
Category	status
Component	Local Replication cache usage
Severity	Threshold severity
Message	Local replication resource usage has changed to <NN> percent.

Unisphere policy name	**Local Replication Utilization**
Action type	Alert

1223

1223	SYMAPI_AEVENT2_UID_ALERT_SYS_METADATAUSE_PCT_CHG
Category	status
Component	System Meta Data Utilization
Severity	Threshold severity
Message	Array metadata usage has changed to <NN> percent.

Unisphere policy name	**System Meta Data Utilization**
Action type	Alert

1224

1224	SYMAPI_AEVENT2_UID_ALERT_FE_METADATAUSE_PCT_CHG
Category	status
Component	Front-End Meta Data Utilization
Severity	Threshold severity
Message	Front-End metadata usage has changed to <NN> percent.

Unisphere policy name	**Front-End Meta Data Utilization**
Action type	Alert

Note: This event is only supported from PowerMaxOS 5978.

1225

1225	SYMAPI_AEVENT2_UID_ALERT_BE_METADATAUSE_PCT_CHG
Category	status
Component	Back-End Meta Data Utilization
Severity	Threshold severity
Message	Back-End metadata usage has changed to <NN> percent.

Unisphere policy name	**Back-End Meta Data Utilization**
Action type	Alert

Note: This event is only supported from PowerMaxOS 5978.

1230

1230	SYMAPI_AEVENT2_UID_ALERT_ARRAY_CONFIG_CHANGE
Category	status
Component	
Severity	Info
Message	Array configuration has changed.

Indicates that some change has been made to the configuration of the storage array.

Note

This event is derived from one of the QuickConfig indication maintained on the storage array.

1231

1231	SYMAPI_AEVENT2_UID_ALERT_MASKING_CHANGE
Category	status
Component	
Severity	Info
Message	Device Masking database has changed.

Indicates that some change have been made to the device masking database on the storage array.

Note

This event is derived from one of the QuickConfig indication maintained on the storage array.

1232

1232	SYMAPI_AEVENT2_UID_ALERT_ACCESS_CONTROL_CHANGE
Category	status
Component	
Severity	Info
Message	Access Control definitions have changed.

Indicates that some change has been made to the Access Control [symacl] database on the storage array.

Note

This is derived from one of the QuickConfig indication maintained on the storage array.

1233

1233	SYMAPI_AEVENT2_UID_ALERT_DYNAMIC_RDF_CONFIG
Category	status
Component	
Severity	Info
Message	Dynamic RDF operation performed on device.

Indicates that a dynamic RDF operation has been performed on some device.

Note

This is derived from one of the QuickConfig indication maintained on the storage array.

1234

1234	SYMAPI_AEVENT2_UID_ALERT_SNAP_CLONE_CONFIG
Category	status
Component	
Severity	Info
Message	Snap session created, activated or deleted.

Indicates that a snap / clone session has been created, activated or deleted.

Note

This is derived from one of the QuickConfig indication maintained on the storage array.

1235

1235	SYMAPI_AEVENT2_UID_AL ERT_BCV_CONTROL_CON FIG
Category	status
Component	
Severity	Info
Message	BCV device pairing has changed.

Indicates that the BCV pairing for some device has changed.

Note

This is derived from one of the QuickConfig indication maintained on the storage array.

1236

1236	SYMAPI_AEVENT2_UID_AL ERT_DEV_NAME_HP_ID_C ONFIG
Category	status
Component	
Severity	Info
Message	HPUX device identifier has changed.

Indicates that the HPUX device identifier for some device has been changed.

Note

This is derived from one of the QuickConfig indication maintained on the storage array.

1237

1237	SYMAPI_AEVENT2_UID_AL ERT_DEV_NAME_CONFIG
Category	status
Component	
Severity	Info
Message	Device Name has changed.

Indicates that the device name for some device has been changed.

Note

This is derived from one of the QuickConfig indication maintained on the storage array.

1238

1238	SYMAPI_AEVENT2_UID_AL ERT_DEV_NICE_NAME_CO NFIG
Category	status
Component	
Severity	Info
Message	Device Nice Name has changed.

Indicates that the device nice name for some device has been changed.

Note

This is derived from one of the QuickConfig indication maintained on the storage array.

1239

1239	SYMAPI_AEVENT2_UID_AL ERT_DEV_NAME_VMS_ID_ CONFIG
Category	status
Component	
Severity	Info
Message	OpenVMS device identifier has changed.

Indicates that the OpenVMS device identifier for some device has been changed.

Note

This is derived from one of the QuickConfig indication maintained on the storage array.

1240

1240	SYMAPI_AEVENT2_UID_DE VICE_RESV_CHANGE
Category	status
Component	
Severity	Info
Message	Device Reservations data has changed.

Indicates that the Device Reservation state for some device on the storage array has changed.

Note

This event requires checking for modifications to file(s) within SFS.

1241

1241	SYMAPI_AEVENT2_UID_SRDFA_CYCLE_TIME_T
Category	status
Component	The SRDF Group. For example: SRDF-grp=13
Severity	Determined by Threshold values. See below.
Message	Time since last SRDFA cycle switch exceeds minimum cycle time by <NN> seconds.

This is a Threshold event that indicates the amount (in seconds) by which an SRDFA Group's Cycle Time exceeds the minimum that is configured.

Unless threshold values are supplied with the registration (in the daemon_options file), the following defaults are used to derive an event severity:

If value is >= 5 — Warning

Otherwise — Normal

Notes

This is determined by calling SymReplicationGet() and examining the time_since_last_switch and duration_of_last_cycle quantities for Active, R1, non-MSC sessions.

The event value corresponds to the number of seconds that the larger of these two is beyond the configured min_cycle_time. If the time(s) are less than min_cycle_time (everything normal), the event value is 0. To protect against rounding problems, the test is actually against min_cycle_time +1. If the times are less than min_cycle_time+1, the event value will be 0. Therefore, possible event values are: 0, 2, 3, 4, 5, etc.

For example, assuming a min_cycle_time of 10:

time_since_last_switch	event value
9	0
10	0
11	0
13	3

1242

1242	SYMAPI_AEVENT2_UID_SRDFA_WP_CACHEUSE_T
Category	status

1242	SYMAPI_AEVENT2_UID_SRDFA_WP_CACHEUSE_T
Component	
Severity	Determined by Threshold values. See below.
Message	SRDFA cycles now using <NN> percent of the cache available for it.

This is a Threshold event that indicates the percentage of cache that is available for SRDFA use that is actually holding SRDFA Write Pending data.

Unless threshold values are supplied with the registration, the following defaults are used to derive an event severity:

If value is >= 90% — Warning

Otherwise — Info

Notes

- This is determined by calling SymReplicationGet() and summing the active_cycle_size and inactive_cycle_size values for all active R1 or R2 sessions. The maximum available cache is computed in the usual manner:

```
if      ((max_host_throttle == 0) and
        (rdfa_max_cache_usage > 0) and
        (rdfa_max_cache_usage < 100))
    max_avail = (max_wr_pend_slots * rdfa_max_cache_usage) / 100
else
    max_avail = max_wr_pend_slots
```

The event value is the sun of the active and inactive cycle sizes expressed as a percentage of this max avail cache size.

- warning: Exercise caution when assigning significance to this event. The fact that an amount of cache is available for SRDFA to use (max_avail above) doesn't mean that it is guaranteed to be available for its use. There are other sources of Write Pending data that can use up this space as well - leaving it unavailable for SRDFA's use.

1243

1243	SYMAPI_AEVENT2_UID_WP_CACHEUSE_T
Category	status
Component	
Severity	Determined by Threshold values. See below.
Message	Write Pending data is now using <NN> percent of the cache.

Notes

This is a Threshold event that indicates the percentage of Symmetrix Cache that is holding Write Pending data.

Unless threshold values are supplied with the registration, the following defaults are used to derive an event severity:

If value is >= 90% — Warning

Otherwise — Info

1244

1244	SYMAPI_AEVENT2_UID_ALERT_ARR_COMP_STATUS
Category	status
Component	Power=xxx Fan=xxx LCC=xxx Enclosure=xxx MM=xxx IOMC=xxx Dir=xxx
Severity	If Online: Normal If Online Degraded: Warning If Offline: Major If Unknown: Warning
Message	Component state has changed to [Not Present	Unknown	Online	Write Disabled	Offline	Failed]

Unisphere policy name	**Array Component Events**
Action type	Alert

- Online — means that the component is a Normal or Degraded state.
- Online [Degraded] — means that the component is in a degraded state.
- Offline — means that the component is in a Failed state.

The format of the specific component name (*xxx* above) may differ depending on the VMAX model. Some examples you might encounter are:

SB-1/Fan-A	Fan in System Bay
SB-1/ENC-1	Enclosure within System Bay
SB-1/ENC-1/Fan-A	Fan in Enclosure-Slot within System Bay

SB-1/MIBE-L-2A	MIBE within System Bay
SB-1/MIBE-L-2A/PS-A	Power Supply in MIBE within System Bay

Notes

Indicates a change in environmental status for one of the following types of sub-components within the VMAX array:

Fans:	[Fan]
Power Supplies:	[Power]
Link Control Cards:	[LCC]
Management Modules	[MM]
IO Module Carriers	[IOMC]
Directors (for environmental alerts):	[Dir]
Enclosures or Matrix Interface Board Enclosures	[Enclosure]

1245

1245	**SYMAPI_AEVENT2_UID_DSE_SPILL_TIME_T**
Category	status
Component	The SRDF Group. For example: SRDF-grp=13
Severity	Determined by Threshold values. See below.
Message	DSE Spillover has been occurring on the RDF group for <N> minutes.

This is a Threshold event that indicates the amount of time (in minutes) that SRDF DSE Spillover has been occurring for.

Unless threshold values are supplied with the registration, the following defaults are used to derive an event severity:

If value is >= 30 (minutes) — Warning

Otherwise — Normal

Note

Threshold events are only delivered when the severity, as determined by threshold values, changes.

1246

1246	SYMAPI_AEVENT2_UID_ALERT_DISK_GRP_CHG
Category	status
Component	The Symmetrix Disk group number (decimal). For example: DiskGrp=2
Severity	INFO
Message	Disk Group has changed. or Disk Group has been deleted or Disk Group has been created

Note

This event is only supported on VMAX arrays running Enginuity 5876 and HYPERMAX OS 5977.

1247

1247	SYMAPI_AEVENT2_UID_ALERT_DISK_SPARE_CVG
Category	status
Component	Disk identifier For example: Disk=16B:C2 (for Director 16B, DA InterfaceC, SCSI ID/Target 2)
Severity	INFO
Message	Disk has spare coverage. or Disk no longer has spare coverage.

Unisphere policy name	RVA Spare Coverage
Action type	Alert

Note

This event is only supported on VMAX arrays running Enginuity 5876 and HYPERMAX OS 5977.

1248

1248	SYMAPI_AEVENT2_UID_ALERT_DISK_SPARE_PCT_CHNG
Category	status
Component	The Symmetrix Disk group number (decimal). For example: DiskGrp=2
Severity	INFO
Message	The spare capacity for diskgroup on engine [0..9]+ has changed to [0..100] percent.

Note

This event is only supported on VMAX arrays running HYPERMAX OS 5977.

1249

1249	SYMAPI_AEVENT2_UID_ALERT_SPINDLE_SPARE_CVG
Category	status
Component	Disk identifier For example: Disk=16B:C2 (for Director 16B, DA InterfaceC, SCSI ID/Target 2)
Severity	Info
Message	Disk has spare coverage. OR Disk no longer has spare coverage.

1252

1252	SYMAPI_AEVENT2_UID_BASED_THRESH_GK_UTIL_AVG
Category	
Component	
Severity	User specified threshold severity.

1252	SYMAPI_AEVENT2_UID_BASED_THRESH_GK_UTIL_AVG
Message	Gatekeeper utilization has now reached [0..100] percent.

Unisphere policy name	**GK Utilization**
Action type	Alert

Note

If there is no threshold specified, the event will not be posted. If there is a threshold specified for the event, the event severity will be set accordingly. After the first event, every subsequent event with the same severity as the first event will be ignored.

1253

1253	SYMAPI_AEVENT2_UID_BASED_GK_TIMEOUT
Category	
Component	
Severity	Warning
Message	Number of gatekeeper timeouts that have occurred within the past minute is [0-9]+.

Unisphere policy name	**GK Timeout**
Action type	Alert

1280

1280	SYMAPI_AEVENT2_UID_ALERT_CACHE_PART_CHANGE
Category	status
Component	
Severity	Info
Message	Cache Partitioning configuration has changed.

Indicates that the Cache Partitioning data on the array has been changed.

Note

This is derived from one of the QuickConfig indication maintained on the VMAX array.

1281

1281	SYMAPI_AEVENT2_UID_ALERT_DYNAMIC_MAPPING_CHANGE
Category	status
Component	
Severity	Info
Message	Dynamic Mapping configuration for a device has changed.

Indicates that the Dynamic Mapping info for some device has been changed on the VMAX array.

Note

This is derived from one of the QuickConfig indications maintained on the VMAX array.

1282

1282	SYMAPI_AEVENT2_UID_ALERT_META_CONFIG_CHANGE
Category	status
Component	
Severity	Info
Message	Meta configuration for a device has changed.

Indicates that the Meta configuration for some device has been changed on the VMAX array.

Note

This is derived from one of the QuickConfig indications maintained on the VMAX array.

1283

1283	SYMAPI_AEVENT2_UID_ALERT_INITIATOR_GRP_CHANGE
Category	status
Component	
Severity	Info
Message	Initiator Group has changed.

Indicates that some Initiator Group on the array has been changed.

Note

This is derived from one of the QuickConfig indication maintained on the VMAX array.

1284

1284	SYMAPI_AEVENT2_UID_ALERT_STORAGE_GRP_CHANGE
Category	status
Component	
Severity	Info
Message	Storage Group has changed.

Indicates that some Storage Group on the array has been changed.

Note

This is derived from one of the QuickConfig indication maintained on the VMAX array.

1285

1285	SYMAPI_AEVENT2_UID_ALERT_DIR_PORT_GRP_CHANGE
Category	status
Component	
Severity	Info
Message	Director Port Group has changed.

Indicates that some Director Port Group on the array has been changed.

Note

This is derived from one of the QuickConfig indication maintained on the VMAX array.

1286

1286	SYMAPI_AEVENT2_UID_ALERT_MASKING_VIEW_CHANGE
Category	status
Component	
Severity	Info
Message	Masking View has changed.

Indicates that some Masking View on the array has been changed.

Note

This is derived from one of the QuickConfig indication maintained on the VMAX array.

1287

1287	SYMAPI_AEVENT2_UID_ALERT_FEAT_REG_CHANGE
Category	status
Component	
Severity	Info
Message	Feature Registration DB has changed.

Indicates that a change has been made to the Feature Registration DataBase on the VMAX array.

Note

This is derived from one of the QuickConfig indication maintained on the VMAX array.

1288

1288	SYMAPI_AEVENT2_UID_ALERT_APP_REG_CHANGE
Category	status
Component	
Severity	Info
Message	Application Registration DB has changed.

Indicates that a change has been made to the Application Registration DataBase on the VMAX array.

Note

This is derived from one of the QuickConfig indication maintained on the VMAX array.

1289

1289	SYMAPI_AEVENT2_UID_ALERT_TIERS_CHANGE
Category	optimizer
Component	
Severity	Info
Message	FAST tiers have changed.

Indicates that a change has been made to the FAST (Fully Automated Storage Tiering) Tiers on the VMAX array.

Note

This is derived from one of the QuickConfig indication maintained on the VMAX array.

1290

1290	SYMAPI_AEVENT2_UID_ALERT_FAST_POLICY_CHANGE
Category	optimizer
Component	
Severity	Info
Message	FAST policies have changed.

Indicates that a change has been made to the FAST (Fully Automated Storage Tiering) Policies on the VMAX array.

Note

This is derived from one of the QuickConfig indication maintained on the VMAX array.

1291

1291	SYMAPI_AEVENT2_UID_ALERT_FAST_ASSOCS_CHANGE
Category	optimizer
Component	
Severity	Info
Message	FAST associations have changed.

Indicates that a change has been made to the FAST (Fully Automated Storage Tiering) Associations on the VMAX array.

Note

This is derived from one of the QuickConfig indication maintained on the VMAX array.

1292

1292	SYMAPI_AEVENT2_UID_ALERT_FAST_TIME_WDS_CHANGE
Category	optimizer
Component	
Severity	Info

1292	SYMAPI_AEVENT2_UID_ALERT_FAST_TIME_WDS_CHANGE
Message	Optimizer/FAST time windows have changed.

Indicates that a change has been made to the FAST (Fully Automated Storage Tiering) time windows on the VMAX array.

Note

This is derived from one of the QuickConfig indication maintained on the VMAX array.

1293

1293	SYMAPI_AEVENT2_UID_ALERT_FAST_CTL_PARMS_CHANGE
Category	optimizer
Component	
Severity	Info
Message	Optimizer/FAST control parameters have changed.

Indicates that a change has been made to the FAST (Fully Automated Storage Tiering) control parameters on the VMAX array.

Note

This is derived from one of the QuickConfig indication maintained on the VMAX array.

1294

1294	SYMAPI_AEVENT2_UID_ALERT_SG_CONFIG_CHANGE
Category	status
Component	
Severity	Info
Message	Storage group configuration has changed

Indicates that a change has been made to a storage group on the VMAX array.

Note

This is derived from one of the QuickConfig indication maintained on the VMAX array.

This event is only supported with HYPERMAX OS 5977.

1295

1295	SYMAPI_AEVENT2_UID_ALERT_IG_CONFIG_CHANGE
Category	status
Component	
Severity	Info
Message	Initiator group configuration has changed

Indicates that a change has been made to an initiator group on the VMAX array.

Note

This is derived from one of the QuickConfig indication maintained on the VMAX array.

This event is only supported with HYPERMAX OS 5977.

1296

1296	SYMAPI_AEVENT2_UID_ALERT_PG_CONFIG_CHANGE
Category	status
Component	
Severity	Info
Message	Port group configuration has changed

Indicates that a change has been made to a port group on the VMAX array.

Note

This is derived from one of the QuickConfig indication maintained on the VMAX array.

This event is only supported with HYPERMAX OS 5977.

1297

1297	SYMAPI_AEVENT2_UID_ALERT_MV_CONFIG_CHANGE
Category	status
Component	
Severity	Info
Message	Masking view configuration has changed

Indicates that a change has been made to a masking view configuration on the VMAX array.

Note

This is derived from one of the QuickConfig indication maintained on the VMAX array.

This event is only supported with HYPERMAX OS 5977.

1298

1298	SYMAPI_AEVENT2_UID_ALERT_SG_SCOPE_CHANGE
Category	status
Component	
Severity	Info
Message	Storage group scope has changed

Indicates that a change has been made to a storage group scope on the VMAX array.

Note

This is derived from one of the QuickConfig indication maintained on the VMAX array.

This event is only supported with HYPERMAX OS 5977.

1299

1299	SYMAPI_AEVENT2_UID_ALERT_IG_SCOPE_CHANGE
Category	status
Component	
Severity	Info
Message	Initiator group scope has changed

Indicates that a change has been made to an initiator group scope on the VMAX array.

Note

This is derived from one of the QuickConfig indication maintained on the VMAX array.

This event is only supported with HYPERMAX OS 5977.

1300

1300	SYMAPI_AEVENT2_UID_ALERT_MV_SCOPE_CHANGE
Category	status
Component	
Severity	Info

1300	SYMAPI_AEVENT2_UID_ALERT_MV_SCOPE_CHANGE
Message	Masking view scope has changed

Indicates that a change has been made to a masking view scope on the VMAX array.

Note

This is derived from one of the QuickConfig indication maintained on the VMAX array.

This event is only supported with HYPERMAX OS 5977.

1320

1320	SYMAPI_AEVENT2_UID_ALERT_MF_SPLIT_CHANGE
Category	status
Component	
Severity	Info
Message	A Mainframe Split has been [created | changed | deleted].

Indicates that a change to the list of Mainframe Splits has been detected on a VMAX3 array.

Note

This event is only supported with HYPERMAX OS 5977 Q1 16.

1321

1321	SYMAPI_AEVENT2_UID_ALERT_CU_IMAGE_CHANGE
Category	status
Component	
Severity	Info
Message	A Control Unit Image has been [created | changed | deleted].

Indicates that a change to the list of Mainframe Splits has been detected on a VMAX3 array.

Note

This event is only supported with HYPERMAX OS 5977 Q1 16.

1330

1330	SYMAPI_AEVENT2_UID_ALERT_RDF_STATUS_CHANGE
Category	status

1330	SYMAPI_AEVENT2_UID_ALERT_RDF_STATUS_CHANGE
Component	SRDF [not present in logged events]
Severity	Info
Message	RDF status has changed to [online | offline | transmit idle] state.

1335

1335	SYMAPI_AEVENT2_UID_ALERT_VWITNESS_STATUS_CHANGE
Category	status
Component	SRDF [not present in logged events]
Severity	Info
Message	Virutal Witness has changed state.

1400

1400	SYMAPI_AEVENT2_UID_AUTHZ_RULES_CHANGED
Category	
Component	
Severity	Info
Message	User Authorization rules have changed.

Indicates that a change has been made to the User Authorization [symauth] database on the VMAX array.

Note

This is determined by checking for modifications to the User Authorization file stored in SFS.

1401

1401	SYMAPI_AEVENT2_UID_AUDIT_LOG_SIZE_T
Category	
Component	

1401	SYMAPI_AEVENT2_UID_AUDIT_LOG_SIZE_T
Severity	Determined by Threshold values. See below.
Message	Audit log is at <NN> percent of capacity (before wrapping).

This is a threshold event that tracks as a percentage the amount of data in an array Audit Log - how close the log is to its *wrapping* point where existing entries begin to be over-written.

Unless threshold values are supplied with the registration, the following defaults are used to derive an event severity:

If value is >= 80% — Warning

Otherwise — Nornal

Notes

- What is actually reported is the position of the write pointer within the Audit Log as a percentage: 0% for the beginning, 100% for the end.
- This event is intended to be used as an indication that a backup of the Audit Log is needed - if appropriate.

1402

1402	SYMAPI_AEVENT2_UID_ALERT_SEC_AUDIT
Category	
Component	
Severity	Info
Message	<< The actual message from the Audit Record >>

Indicates that a security-related record was written to the array Audit Log.

Notes

- This event is delivered when audit records with an Audit Class of SECURITY are detected in the Audit Log.
- The audit message is a free-form string that may span multiple lines (containing multiple new line characters).

1403

1403	SYMAPI_AEVENT2_UID_ALERT_SEC_FAIL_AUDIT
Category	
Component	

1403	SYMAPI_AEVENT2_UID_ALERT_SEC_FAIL_AUDIT
Severity	Info
Message	<< The actual message from the Audit Record >>

Indicates that a Security alert was written to the array Audit Log.

Notes

- This event is delivered when audit records corresponding to one of the following are detected in the Audit Log:
- Access Control failures (host based access control, symacl).
- User Authorization failures (user based access control, symauth).
- SymmWin / SSC Logon failures.
- SymmWin Logins
- iSCSI authorization failures
- The audit message is a free-form string that may span multiple lines (containing multiple new line characters).

1404

1404	SYMAPI_AEVENT2_UID_ALERT_ALL_AUDIT
Category	
Component	
Severity	Info
Message	<< The actual message from the Audit Record >>.

Indicates some (any) record written to the array Audit Log.

Note

The audit message is a free-form string that may span multiple lines (containing multiple new line characters).

1500

1500	SYMAPI_AEVENT2_UID_ALERT_OPTMZ_SWAP_ACT
Category	Optimizer
Component	
Severity	Info
Message	Optimizer Swap activity (from Audit Log).

Indicates some Optimizer Swap activity.

Note

This is derived by detecting a record written by the Optimizer to the array Audit Log.

1501

1501	SYMAPI_AEVENT2_UID_ALERT_OPTMZ_MOVE_ACT
Category	Optimizer
Component	
Severity	Info
Message	Optimizer Move activity (from Audit Log).

Indicates some Optimizer Move activity.

Note

This is derived by detecting a record written by the Optimizer to the array Audit Log.

1502

1502	SYMAPI_AEVENT2_UID_ALERT_OPTMZ_SCHEDULE
Category	Optimizer
Component	
Severity	Info
Message	Optimizer configuration change (from Audit Log).

Indicates some Optimizer configuration change.

Note

This is derived by detecting a record written by the Optimizer to the array Audit Log.

1503

1503	SYMAPI_AEVENT2_UID_ALERT_FAST_SWAP_ACT
Category	Optimizer
Component	
Severity	Info
Message	FAST Controller Swap activity (from Audit Log).

Indicates some FAST Controller activity.

Note

This is derived by detecting a record written by the Optimizer to the array Audit Log.

1504

1504	SYMAPI_AEVENT2_UID_ALERT_FAST_MOVE_ACT
Category	Optimizer
Component	
Severity	Info
Message	FAST Controller Move activity (from Audit Log).

Indicates some FAST Controller Move activity.

Note

This is derived by detecting a record written by the Optimizer to the array Audit Log.

1505

1505	SYMAPI_AEVENT2_UID_ALERT_FAST_SCHEDULE
Category	Optimizer
Component	
Severity	Info
Message	FAST Controller configuration change (from Audit Log).

Indicates some FAST Controller configuration change.

Note

This is derived by detecting a record written by the Optimizer to the array Audit Log.

1506

1506	SYMAPI_AEVENT2_UID_ALERT_OPTMZ_RB_ACT
Category	Optimizer
Component	
Severity	Info
Message	Optimizer Rollback activity (from Audit Log).

Note

This is derived by detecting a record written by the Optimizer to the array Audit Log.

1507

1507	SYMAPI_AEVENT2_UID_ALERT_OPTMZ_APPRVL_NEEDED
Category	status
Component	
Severity	Info
Message	User approval is required for a Config Change plan generated by the Optimizer/FAST Controller.

Unisphere policy name	**User approval required for Optimizer/FAST Config Change**
Action type	Alert

Note

Indicates that user approval of the a swap state is required and user approval is required.

1508

1508	SYMAPI_AEVENT2_UID_ALERT_FAST_STATE_SWITCH
Category	Optimizer
Component	
Severity	Info
Message	The FAST (DP or VP) controller has switched to a different state.

Unisphere policy name	**FAST Controller switched state**
Action type	Alert

Note

Indicates that the FAST controller state has changed. The possible states are:

- Disabled
- Enabled
- Disable in progress
- Enable in progress
- Disable with error

- Degraded

1509

1509	SYMAPI_AEVENT2_UID_ALERT_OPTMZ_MODE_SWITCH
Category	Optimizer
Component	
Severity	Info
Message	The Optimizer has switched to a different mode.

Unisphere policy name	**Optimizer switched mode**
Action type	Alert

Note

Indicates that the Optimizer status state has changed.

1510

1510	SYMAPI_AEVENT2_UID_ALERT_FAST_ALLOC_CHANGE
Category	Optimizer
Component	<policy_name>
Severity	Info
Message	[Policy name] FAST policy allocated capacity is now [0..100] percent.

Note

This event checks for allocated capacity change of all associated pools under the same FAST VP policy. And as such, if FAST VP policy is accidentally used, this event will never be generated.

1511

1511	SYMAPI_AEVENT2_UID_ALERT_FAST_TIER_PERF_CHANGE
Category	Optimizer
Component	<tier_name>
Severity	Info

1511	SYMAPI_AEVENT2_UID_ALERT_FAST_TIER_PERF_CHANGE
Message	The FAST Tier <name> performance has changed.

Unisphere policy name	**FAST FTS Performance**
Action type	Alert

Note

This event is only supported with Enginuity 5876 Q42012 SR and above.

1512

1512	SYMAPI_AEVENT2_UID_ALERT_FAST_SRP_ALLOC_CHANGE
Category	Status
Component	Fast SRP <SRP_Name>
Severity	Threshold severity
Message	The Effective used capacity for SRP has changed to <NN> percent

Unisphere policy name	**Storage Resource Pool Free Space**
Action type	Alert

Unless threshold values are supplied with the registration, the following defaults are used to derive an event severity:

If value is 100% — Fatal

If value is >= 80% — Critical

If value is >= 70% — Major

If value is >= 65% — Minor

If value is >= 60% — Warning

Otherwise — Normal

(i) Note:

- Events are only delivered at multiples of 5% ... for <NN> equal to 5%, 10%, 15%, ... , 75%, 80%, 85%, 90%, 95% and 100%.

- Threshold events are only delivered when the severity, as determined by threshold values, changes.

- This event is only supported with HYPERMAX OS 5977.

1513

1513	SYMAPI_AEVENT2_ UID_ALERT_FAST_S RP_FREE_CAP_CHA NGE
Category	status
Component	Fast SRP <SRP_Name>
Severity	Threshold severity
Message	The Snapshot capacity for SRP has changed to <NN> percent.

1514

1514	SYMAPI_AEVENT2_UI D_ALERT_FAST_SRP_ CONFIG_CHANGE
Category	status
Component	Fast SRP <SRP_Name>
Severity	Info
Message	The SRP configuration has changed.

1515

1515	SYMAPI_AEVENT2_ UID_ALERT_FAST_S RP_MAX_CAP_CHA NGE
Category	status
Component	Fast SRP <SRP_Name>
Severity	Info
Message	The SRP maximum capacity has changed to [0..9]+ GB.

Note

This event is only supported with Enginuity 5876 Q42012 SR and above.

1520

1520	SYMAPI_AEVENT2_UID _ALERT_FAST_SLO_NA ME_CHANGE
Category	status
Component	Fast SLO
Severity	Info
Message	Service Level name has changed to <SL name>.

1540

1540	SYMAPI_AEVENT2_UI D_ALERT_STOR_CON T_CONFIG_CHANGE
Category	status
Component	Storage Container
Severity	Info
Message	Storage container has been [added | modified | deleted].

1541

1541	SYMAPI_AEVENT2_U ID_ALERT_STOR_CO NT_SUBSCR_CAP_C HANGE
Category	status
Component	Storage Container
Severity	Threshold Severity
Message	Storage container subscribed capacity has changed to [0..100] percent.

1550

1550	SYMAPI_AEVENT2_UID_AL ERT_ISCSI_IP_IF_CHANGE
Category	status

1550	**SYMAPI_AEVENT2_UID_ALERT_ISCSI_IP_IF_CHANGE**
Component	iSCSI IP Interface <IpInterface_value>
Severity	Info
Message	iSCSI IP interface configuration has been [added | deleted | modified].

1551

1551	**SYMAPI_AEVENT2_UID_ALERT_ISCSI_IP_ROUTE_CHANGE**
Category	status
Component	iSCSI Route <IpRoute_value>
Severity	Info
Message	iSCSI IP route has been [added | removed].

1552

1552	**SYMAPI_AEVENT2_UID_ALERT_ISCSI_TGT_CHANGE**
Category	status
Component	iSCSI Target <iSCSITarget_Name>
Severity	Info
Message	iSCSI Target has been [added | deleted | modified].

1600

1600	**SYMAPI_AEVENT2_UID_GROUP_CONFIG**
Category	
Entity	Not set -- set to NULL.
Component	DG or CG group. For example: DG=prod17 or CG=prod18
Severity	Info

1600	SYMAPI_AEVENT2_UID_GROUP_CONFIG
Message	Group has changed.

Indicates that the composition of a device group (DG) or composite group (CG) has changed.

Notes

- The Entity name and type (normally a Symmetrix ID) are not provided for this event. When registering to receive the event, there is no need to supply an ID (symid=000194900123) - if one is supplied, it will be ignored.

- If GNS is not enabled, this event indicates that a group definition in the Solutions Enabler DB file on this host has changed.

- If GNS is enabled, this event indicates that a global group definition stored within GNS (on storage arrays) has changed.

1601

1601	SYMAPI_AEVENT2_UID_THRESH_GNS_SPACE
Category	GNS
Component	
Severity	Threshold severity
Message	GNS is now using [0..100] percent of the available group space

1602

1602	SYMAPI_AEVENT2_UID_THRESH_GNS_RECS
Category	GNS
Component	
Severity	Threshold severity
Message	GNS is now using [0..100] percent of the available group directory entries.

1650

1650	SYMAPI_AEVENT2_UID_POLL_CYCLE_COMPLETE
Category	
Component	
Severity	Info

1650	SYMAPI_AEVENT2_UID_POLL_CYCLE_COMPLETE
Message	The polling cycle is complete.

Event daemon events: Event IDs 5000-5200

Events in this range are generated by an external producer.

5000

5000	
Category	Event
Component	SMC
Severity	
Message	

Events generated by the SMC will have the appropriate OID information to a given event (such as a "device configuration change"), but the Event Code (OID 1.3.6.1.4.1.1139.3.8888.2.0) will display a value of 5000 instead of the corresponding Event Code generated by the Event Daemon (for example 1205 in the case of a "device configuration change").

5200

5200	
Category	Event
Component	SPA
Severity	
Message	

Events generated by the SPA will have the appropriate OID information to a given event (such as a "device configuration change"), but the Event Code (OID 1.3.6.1.4.1.1139.3.8888.2.0) will display a value of 5200 instead of the corresponding Event Code generated by the Event Daemon (for example 1205 in the case of a "device configuration change").

Unisphere policy name - Alert ID mapping

The following table presents an overview of Unisphere policy names and their corresponding Solutions Enabler Alert/Event IDs. For details on the events, use the hyperlinks.

Table 7 Unisphere policy name - Alert ID mapping

Unisphere policy name	Alert/ Event ID	Solutions Enabler event definition
Hotspare Invoked	1054	SYMAPI_AEVENT2_UID_MOD_DISKDRV_SPARE_INVK
	1060	SYMAPI_AEVENT2_UID_MOD_RDF_HOTSPARE_INVK

Table 7 Unisphere policy name - Alert ID mapping (continued)

Unisphere policy name	Alert/ Event ID	Solutions Enabler event definition
	1210	SYMAPI_AEVENT2_UID_ALERT_HOTSPARE_CHANGE
Port Link Status	1063	SYMAPI_AEVENT2_UID_MOD_FCPORT_FAIL
Environmental Alert	1067	SYMAPI_AEVENT2_UID_MOD_TEMP_OUT_OF_LIMIT
	1150	SYMAPI_AEVENT2_UID_MOD_LCC_A_TEMP_HIGH
	1151	SYMAPI_AEVENT2_UID_MOD_LCC_B_TEMP_HIGH
SRDF/A Session entering transmit idle state	1138	SYMAPI_AEVENT2_UID_MOD_SRDFA_SE_TRANS_IDLE
SRDF/A Session recovered from a transmit idle state	1139	SYMAPI_AEVENT2_UID_MOD_SRDFA_SR_TRANS_IDLE
SRDF/A Session dropped, transit idle state timeout	1140	SYMAPI_AEVENT2_UID_MOD_SRDFA_TO_TRANS_IDLE
SRDF/A No Cycle Switch Alert	1159	SYMAPI_AEVENT2_UID_ALERT_SRDFA_NO_CYCLE_SWITCH
SRDF Job Flow Control Change	1160	SYMAPI_AEVENT2_UID_ALERT_SRDF_JFC_STATE_CHANGE
External disk group fully allocated	1162	SYMAPI_AEVENT2_UID_ALERT_EDISK_FULL
Device Status	1200	SYMAPI_AEVENT2_UID_ALERT_DEV_STATUS
Director Status	1202	SYMAPI_AEVENT2_UID_ALERT_DIRECTOR_STATUS
Port Status	1203	SYMAPI_AEVENT2_UID_ALERT_PORT_STATUS
Disk status	1204	SYMAPI_AEVENT2_UID_ALERT_DISK_STATUS
Device Pool Status	1206	SYMAPI_AEVENT2_UID_ALERT_POOL_STATUS
Device Pool Config Change	1207	SYMAPI_AEVENT2_UID_ALERT_POOL_CONFIG_CHANGE
Device Pool Free Space	1208	SYMAPI_AEVENT2_UID_THRESH_POOL_FREESPACE
Thin Device Allocation	1212	SYMAPI_AEVENT2_UID_THRESH_TDEV_ALLOCATED
Thin Device Usage	1213	SYMAPI_AEVENT2_UID_THRESH_TDEV_USED
Deferred Service Threshold Alert	1217	SYMAPI_AEVENT2_UID_ALERT_DFR_SVC_STATE
Migration Complete Alert	1219	SYMAPI_AEVENT2_UID_ALERT_MIGRATE_COMPLETE

Table 7 Unisphere policy name - Alert ID mapping (continued)

Unisphere policy name	Alert/ Event ID	Solutions Enabler event definition
Thin Pool Rebalancing Complete Alert	1220	SYMAPI_AEVENT2_UID_ALERT_POOL_REBAL_COMPLETE
Array Component Events	1244	SYMAPI_AEVENT2_UID_ALERT_ARR_COMP_STATUS
RVA Spare Coverage	1247	SYMAPI_AEVENT2_UID_ALERT_DISK_SPARE_CVG
GK Utilization	1252	SYMAPI_AEVENT2_UID_BASED_THRESH_GK_UTIL_AVG
GK Timeout	1253	SYMAPI_AEVENT2_UID_BASED_GK_TIMEOUT
User approval required for Optimizer/FAST Config Change	1507	SYMAPI_AEVENT2_UID_ALERT_OPTMZ_APPRVL_NEEDED
FAST Controller switched state	1508	SYMAPI_AEVENT2_UID_ALERT_FAST_STATE_SWITCH
Optimizer switched mode	1509	SYMAPI_AEVENT2_UID_ALERT_OPTMZ_MODE_SWITCH
FAST FTS Performance	1511	SYMAPI_AEVENT2_UID_ALERT_FAST_TIER_PERF_CHANGE
Storage Resource Pool Free Space	1512	SYMAPI_AEVENT2_UID_ALERT_FAST_SRP_ALLOC_CHANGE
Device Config Change	1205	SYMAPI_AEVENT2_UID_ALERT_DEV_CONFIG_CHANGE
Event Lost Alert	2	SYMAPI_AEVENT2_UID_EVT_EVENTS_LOST
Event Overflow Alert	3	SYMAPI_AEVENT2_UID_EVT_EVENTS_OVERFLOW
SRDF Alerts	1061	SYMAPI_AEVENT2_UID_MOD_RDF_SIM_MSG
	1062	SYMAPI_AEVENT2_UID_MOD_RDF_ERR
SRDF/A Session	1112	SYMAPI_AEVENT2_UID_MOD_RDFA_INACTIVE
	1113	SYMAPI_AEVENT2_UID_MOD_RDFA_ACTIVE
	1123	SYMAPI_AEVENT2_UID_MOD_SESS_DROP_NO_RDF_LNK
	1130	SYMAPI_AEVENT2_UID_MOD_SRDFA_DROP_FROM_HOST
	1131	SYMAPI_AEVENT2_UID_MOD_SRDFA_DROP_PEND_FROM_HOST
	1132	SYMAPI_AEVENT2_UID_MOD_SRDFA_DEACTIV_FROM_HOST

Table 7 Unisphere policy name - Alert ID mapping (continued)

Unisphere policy name	Alert/ Event ID	Solutions Enabler event definition
	1133	SYMAPI_AEVENT2_UID_MOD_SRDFA_CONS_DEACTIV_FROM_HOST
	1134	SYMAPI_AEVENT2_UID_MOD_SRDFA_DROP
	1135	SYMAPI_AEVENT2_UID_MOD_SRDFA_DROP_PEND
	1158	SYMAPI_AEVENT2_UID_MOD_SRDFA_DROP_WPL_CP
SRDF Link Status	1064	SYMAPI_AEVENT2_UID_MOD_RDF_LINKS_DOWN
	1065	SYMAPI_AEVENT2_UID_MOD_RDF_LINKS_UP
	1080	SYMAPI_AEVENT2_UID_MOD_RDF_1LINK_DOWN
	1081	SYMAPI_AEVENT2_UID_MOD_RDF_1LINK_UP

CHAPTER 3

SYMCLI Return Codes

This chapter describes the SYMCLI Return Codes for Open VMS, Windows, and Unix.

SYMCLI Return Codes for OpenVMS

Return code handling for OpenVMS

A set of return codes for the various conditions possible with each SYMCLI command are provided for UNIX and Windows platforms. However, for the OpenVMS platforms, discernible return codes are not yet available and, therefore, require interpolation or special processing of the returned hexadecimal value (resulting from a $STATUS query). This is because the format of the OpenVMS return value also includes a severity level field in the three least significant bits (00-02). The return code is described in the next field (03-15). The table belows describes the set of possible return hex values and their associated meaning with SYMCLI on OpenVMS.

For OpenVMS, use write sys$output $status to view a return code. The following special DCL program can automatically convert these OpenVMS values to the proper SYMCLI return codes:

```
[SAMPLE-DCL]
    $ ! Example: Convert SYMCLI return codes.
    $ !
    $ a = ( %x0000ffff .and. 'p1)  ! Mask off bits 16-31.
    $ a = ( a/8 ) ! Shift 3-15 right.
    $ write sys$output 'a;        ! Print return code
    $                             ! without severity
    $                             ! level.    $ !
```

The following table lists the status or error codes that can be returned by the various SYMCLI commands on OpenVMS platforms.

Table 8 Return code handling for OpenVMS

Returned hex value	SYMCLI code	OpenVMS severity level	SYMCLI name
%X1FFF0001	00	1 (S)	SUCCESS
%X1FFF000C	01	4 (F)	FAIL
%X1FFF0012	02	2 (E)	DB_FILE_IS LOCKED
%X1FFF001A	03	2 (E)	SYM_IS_LOCKED
%X1FFF0023	04	3 (I)	NOT_ALL_SYNCHRONIZED
%X1FFF002B	05	3 (I)	NONE_SYNCHRONIZED
%X1FFF0033	06	3 (I)	NOT_ALL_UPDATED
%X1FFF003B	07	3 (I)	NONE_UPDATED
%X1FFF0043	08	3 (I)	NOT_ALL_PINGED
%X1FFF004B	09	3 (I)	NONE_PINGED
%X1FFF0053	10	3 (I)	NOT_ALL_SYNCHED
%X1FFF005B	11	3 (I)	NONE_SYNCHED
%X1FFF0063	12	3 (I)	NOT_ALL_RESTORED

Table 8 Return code handling for OpenVMS (continued)

Returned hex value	SYMCLI code	OpenVMS severity level	SYMCLI name
%X1FFF006B	13	3 (I)	NONE_RESTORED
%X1FFF0073	14	3 (I)	NOT_ALL_VALID
%X1FFF007B	15	3 (I)	NONE_VALID
%X1FFF0083	16	3 (I)	SYM_NOT_ALL_LOCKED
%X1FFF008B	17	3 (I)	SYM_NONE_LOCKED
%X1FFF0093	18	3 (I)	ALREADY_IN_STATE
%X1FFF009A	19	2 (E)	GK_IS_LOCKED
%X1FFF00A2	20	2 (E)	WP_TRACKS_IN_CACHE
%X1FFF00AA	21	2 (E)	NEED_MERGE_TO_RESUME
%X1FFF00B2	22	2 (E)	NEED_FORCE_TO_PROCEED
%X1FFF00BA	23	2 (E)	NEED_SYMFORCE_TO_PROCEED
%X1FFF00C3	24	3 (I)	NOT_IN_SYNC
%X1FFF00CB	25	3 (I)	NOT_ALL_SPLIT
%X1FFF00D3	26	3 (I)	NONE_SPLIT
%X1FFF00DB	27	3 (I)	NOT_ALL_SYNCINPROG
%X1FFF00E3	28	3 (I)	NONE_SYNCINPROG
%X1FFF00EB	29	3 (I)	NOT_ALL_RESTINPROG
%X1FFF00F3	30	3 (I)	NONE_RESTINPROG
%X1FFF00FB	31	3 (I)	NOT_ALL_SUSPENDED
%X1FFF0103	32	3 (I)	NONE_SUSPENDED
%X1FFF010B	33	3 (I)	NOT_ALL_FAILED_OVER
%X1FFF0113	34	3 (I)	NONE_FAILED_OVER
%X1FFF011B	35	3 (I)	NOT_ALL_UPDATEINPROG

Table 8 Return code handling for OpenVMS (continued)

Returned hex value	SYMCLI code	OpenVMS severity level	SYMCLI name
%X1FFF0123	36	3 (I)	NONE_UPDATEINPROG
%X1FFF012B	37	3 (I)	NOT_ALL_PARTITIONED
%X1FFF0133	38	3 (I)	NONE_PARTITIONED
%X1FFF013B	39	3 (I)	NOT_ALL_ENABLED
%X1FFF0143	40	3 (I)	NONE_ENABLED
%X1FFF014B	41	3 (I)	NOT_ALL_SYNCHRONIZED_AND_ENABLED
%X1FFF0153	42	3 (I)	NONE_SYNCHRONIZED_AND_ENABLED
%X1FFF015B	43	3 (I)	NOT_ALL_SUSP_AND_ENABLED
%X1FFF0163	44	3 (I)	NONE_SUSP_AND_ENABLED
%X1FFF016B	45	3 (I)	NOT_ALL_SUSP_AND_OFFLINE
%X1FFF0173	46	3 (I)	NONE_SUSP_AND_OFFLINE
%X1FFF017A	47	2 (E)	WONT_REVERSE_SPLIT
%X1FFF0182	48	2 (E)	CONFIG_LOCKED
%X1FFF018A	49	2 (E)	DEVS_ARE_LOCKED
%X1FFF0192	50	2 (E)	MUST_SPLIT_PROTECT
%X1FFF019A	51	2 (E)	PAIRED_WITH_A_DRV
%X1FFF01A2	52	2 (E)	PAIRED_WITH_A_SPARE
%X1FFF01AB	53	3 (I)	NOT_ALL_COPYINPROG
%X1FFF01B3	54	3 (I)	NONE_COPYINPROG
%X1FFF01BB	55	3 (I)	NOT_ALL_COPIED
%X1FFF01C3	56	3 (I)	NONE_COPIED

Table 8 Return code handling for OpenVMS (continued)

Returned hex value	SYMCLI code	OpenVMS severity level	SYMCLI name
%X1FFF01CB	57	3 (I)	NOT_ALL_COPYONA CCESS
%X1FFF01D3	58	3 (I)	NONE_COPYONACC ESS
%X1FFF01DA	59	2 (E)	CANT_RESTORE_PR OTECT
%X1FFF01E3	60	3 (I)	NOT_ALL_CREATED
%X1FFF01EB	61	3 (I)	NONE_CREATED
%X1FFF01F3	62	3 (I)	NOT_ALL_READY
%X1FFF01FB	63	3 (I)	NONE_READY
%X1FFF0202	64	2 (E)	SYM_IS_LOCKED
%X1FFF020A	65	2 (E)	SPLIT_IN_PROG
%X1FFF0213	66	3 (I)	NOT_ALL_COPYON WRITE
%X1FFF021B	67	3 (I)	NONE_COPYONWRI TE
%X1FFF0223	68	3 (I)	Reserved for future use.
%X1FFF022B	69	3 (I)	Reserved for future use.
%X1FFF0233	70	3 (I)	NOT_ALL_CONSIST ENT
%X1FFF023B	71	3 (I)	NONE_CONSISTENT
%X1FFF0242	72	2 (E)	MAX_SESSIONS_EX CEEDED
%X1FFF024B	73	3(I)	NOT_ALL_PRECOPY
%X1FFF0253	74	3(I)	NONE_PRECOPY
%X1FFF025B	75	3(I)	NOT_ALL_PRECOPY _CYCLED
%X1FFF0263	76	3(I)	NONE_PRECOPY_C YCLED
%X1FFF026A	77	2(E)	CONSISTENCY_TIM EOUT
%X1FFF0273	78	3(I)	NOT_ALL_FAILED
%X1FFF027B	79	3(I)	NONE_FAILED
%X1FFF0283	80	3(I)	CG_NOT_CONSISTE NT

Table 8 Return code handling for OpenVMS (continued)

Returned hex value	SYMCLI code	OpenVMS severity level	SYMCLI name
%X1FFF028B	81	3(I)	NOT_ALL_CREATEIN PROG
%X1FFF0293	82	3(I)	NONE_CREATEINPR OG
%X1FFF029B	83	3(I)	NOT_ALL_RECREAT EINPROG
%X1FFF02A3	84	3(I)	NONE_RECREATEIN PROG
%X1FFF02AB	85	3(I)	NOT_ALL_TERMINP ROG
%X1FFF02B3	86	3(I)	NONE_TERMINPRO G
%X1FFF02BB	87	3(I)	NOT_ALL_VERIFYIN PROG
%X1FFF02C3	88	3(I)	NONE_VERIFYINPRO G
%X1FFF02CB	89	3(I)	NOT_ALL_VERIFIED
%X1FFF02D3	90	3(I)	NONE_VERIFIED
%X1FFF02DA	91	2(E)	RDFG_TRANSMIT_ID LE
%X1FFF02E2	92	2(E)	NOT_ALL_MIGRATE D
%X1FFF02EA	93	2(E)	NONE_MIGRATED
%X1FFF02F2	94	2(E)	NOT_ALL_MIGRATEI NPROG
%X1FFF02FA	95	2(E)	NONE_MIGRATEINP ROG
%X1FFF0302	96	2(E)	NOT_ALL_INVALID
%X1FFF030A	97	2(E)	NONE_INVALID
%X1FFF04C2	98	2(E)	EMPTY_BACKUP
%X1FFF04CA	99	2(E)	NOT_ALL_BOUND
%X1FFF0802	100	2(E)	NONE_BOUND
%X1FFF080A	101	2(E)	NOT_ALL_BINDING
%X1FFF0812	102	2(E)	NONE_BINDING
%X1FFF081A	103	2(E)	NOT_ALL_ALLOCATI NG
%X1FFF0822	104	2(E)	NONE_ALLOCATING

Table 8 Return code handling for OpenVMS (continued)

Returned hex value	SYMCLI code	OpenVMS severity level	SYMCLI name
%X1FFF082A	105	2(E)	NOT_ALL_DEALLOC ATING
%X1FFF0832	106	2(E)	NONE_DEALLOCATI NG
%X1FFF083A	107	2(E)	NOT_ALL_DRAINING
%X1FFF0842	108	2(E)	NONE_DRAINING
%X1FFF084A	109	2(E)	NOT_ALL_UNBOUN D
%X1FFF0882	110	2(E)	NONE_UNBOUND
%X1FFF088A	111	2(E)	NOT_ALL_NONPOO LED
%X1FFF0892	112	2(E)	NONE_NONPOOLED
%X1FFF0892	113	2(E)	NOT_ALL_DRAINWAI T
%X1FFF089A	114	2(E)	NONE_DRAINWAIT
%X1FFF08AA	115	2(E)	NOT_ALL_DISABLED
%X1FFF08B2	116	2(E)	NONE_DISABLED
%X1FFF08BA	117	2(E)	NOT_ALL_DEACTIVA TED
%X1FFF08C2	118	2(E)	NONE_DEACTIVATE D
%X1FFF08CA	119	2(E)	NOT_ALL_UNBINDIN G
%X1FFF902	120	2(E)	NONE_UNBINDING
%X1FFF090A	121	2(E)	NOT_ALL_RECLAIMI NG
%X1FFF0912	122	2(E)	NONE_RECLAIMING
%X1FFF091A	123	2(E)	NOT_ALL_BALANCI NG
%X1FFF0922	124	2(E)	NONE_BALANCING
%X1FFF092A	125	2(E)	DEVMASK_VALDTE_ FAILED
%X1FFF0932	126	2(E)	DEVMASK_FREQNT_ CHANGES
%X11FF093A	127	2(E)	STAR_INV_STATE
%X11FFF0942	128	2(E)	STAR_ALLOWED_FR OM_WKLD

Table 8 Return code handling for OpenVMS (continued)

Returned hex value	SYMCLI code	OpenVMS severity level	SYMCLI name
%X1FFF094A	129	2(E)	STAR_INV_DEF_FILE_FMT
%X1FFF0982	130	2(E)	STAR_ACTN_FILE_ERROR
%X1FFF098A	131	2(E)	STAR_DEF_FILE_ERROR
%X1FFF0992	132	2(E)	STAR_SETUP_REQD
%X1FFF0992	133	2(E)	STAR_SETUP_INV_OPMODE
%X1FFF09A2	134	2(E)	STAR_OPMODE_REQD
%X1FFF09AA	135	2(E)	STAR_CTL_SITE_REQD
%X1FFF09B2	136	2(E)	STAR_WKLD_SITE_REQD
%X1FFF09BA	137	2(E)	STAR_WKLD_OP_REQD
%X1FFF09C2	138	2(E)	STAR_CREATE_GROUP_FAIL
%X1FFF09CA	139	2(E)	STAR_FULL_COPY_REQD
%X1FFF0A02	140	2(E)	STAR_INV_ACTION_WOF
%X1FFF0A0A	141	2(E)	STAR_BUILDCG_REQD
%X1FFF0A13	142	3(I)	NOT_ALL_FAILEDBACK
%X1FFF0A1B	143	3(I)	NONE_FAILEDBACK
%X1FFF0A23	144	3(I)	NOT_ALL_STOPPED
%X1FFF0A2B	145	3(I)	NONE_STOPPED
%X1FFF0A33	146	3(I)	NOT_ALL_CONSISTENT_NOINVALIDS
%X1FFF0A3B	147	3(I)	NONE_CONSISTENT_NOINVALIDS
%X1FFF0A43	148	3(I)	NOT_ALL_SYNCHRONOUS
%X1FFF0A4B	149	3(I)	NONE_SYNCHRONOUS

Table 8 Return code handling for OpenVMS (continued)

Returned hex value	SYMCLI code	OpenVMS severity level	SYMCLI name
%X1FFF0A83	150	3(I)	NOT_ALL_SEMISYNCHRONOUS
%X1FFF0A8B	151	3(I)	NONE_SEMISYNCHRONOUS
%X1FFF0A93	152	3(I)	NOT_ALL_ASYNCHRONOUS
%X1FFF0A9B	153	3(I)	NONE_ASYNCHRONOUS
%X1FFF0AA3	154	3(I)	NOT_ALL_ACP_WP
%X1FFF0AAB	155	3(I)	NONE_ACP_WP
%X1FFF0AB4	156	3(I)	NOT_ALL_ACP_DISK
%X1FFF0ABB	157	3(I)	NONE_ACP_DISK
%X1FFF0AC3	158	3(I)	NOT_ALL_COMPRESSING
%X1FFF0ACB	159	3(I)	NONE_COMPRESSING
%X1FFF0AC3	160	3(I)	NOT_ALL_UNCOMPRESSING
%X1FFF0B0B	161	3(I)	NONE_UNCOMPRESSING
%X1FFF0B13	162	3(I)	NOT_ALL_ESTABLISHED
%X1FFF0B1B	163	3(I)	NONE_ESTABLISHED
%X1FFF0B23	164	3(I)	NOT_ALL_ESTINPROG
%X1FFF0B2B	165	3(I)	NONE_ESTINPROG
%X1FFF0B33	166	3(I)	NOT_ALL_LINKED
%X1FFF0B3B	167	3(I)	NONE_LINKED
%X1FFF0B43	168	3(I)	NOT_ALL_DEFINED
%X1FFF0B4B	169	3(I)	NONE_DEFINED
%X1FFF0B83	170	3(I)	NOT_ALL_CIPLINKED
%X1FFF0B8B	171	3(I)	NONE_CIPLINKED
%X1FFF0B93	172	3(I)	NOT_ALL_COPIEDLINKED

Table 8 Return code handling for OpenVMS (continued)

Returned hex value	SYMCLI code	OpenVMS severity level	SYMCLI name
%X1FFF0B9B	173	3(I)	NONE_COPIEDLINKED
%X1FFF0BA3	174	3(I)	NOT_ALL_DESTAGED
%X1FFF0BAB	175	3(I)	NONE_DESTAGED
%X1FFF0BB3	176	3(I)	NOT_ALL_FREEING_ALL
%X1FFF0BBB	177	3(I)	NONE_FREEING_ALL
%X1FFF0BC3	178	3(I)	NOT_ALL_ACTIVE
%X1FFF0BCB	179	3(I)	NONE_ACTIVE
%X1FFF0C03	180	3(I)	NOT_ALL_DRAINED
%X1FFF0C0B	181	3(I)	NONE_DRAINED
%X1FFF0C13	182	3(I)	NOT_ALL_ACTIVEACTIVE
%X1FFF0C1B	183	3(I)	NONE_ACTIVEACTIVE
%X1FFF0C23	184	3(I)	NOT_ALL_ACTIVEBIAS
%X1FFF0C2B	185	3(I)	NONE_ACTIVEBIAS

SYMCLI Return Codes for Windows and Unix

The following table lists the status or error codes that can be returned by the various SYMCLI commands on a Windows and UNIX (for example, in a UNIX C shell, returned using echo $status).

Table 9 Return code handling for Windows and UNIX

Code	Code symbol	Description
0	SUCCESS	CLI call completed successfully.
1	FAIL	CLI call failed.
2	DB_FILE_IS_LOCKED	Another process has an exclusive lock on the Host database file.
3	SYM_IS_LOCKED	Another process has an exclusive lock on the Symmetrix.

Table 9 Return code handling for Windows and UNIX (continued)

Code	Code symbol	Description
4	NOT_ALL_SYNCHRONIZED	NOT all of the mirrored pairs are in the 'Synchronized' state.
5	NONE_SYNCHRONIZED	NONE of the mirrored pairs are in the 'Synchronized' state.
6	NOT_ALL_UPDATED	NOT all of the mirrored pairs are in the 'Updated' state.
7	NONE_UPDATED	NONE of the mirrored pairs are in the 'Updated' state.
8	NOT_ALL_PINGED	NOT all of the remote Symmetrix units can be pinged.
9	NONE_PINGED	NONE of the remote Symmetrix units can be pinged.
10	NOT_ALL_SYNCHED	NOT all of the mirrored pairs are in the 'Synchronized' state.
11	NONE_SYNCHED	NONE of the mirrored pairs are in the 'Synchronized' state.
12	NOT_ALL_RESTORED	NOT all of the pairs are in the 'Restored' state.
13	NONE_RESTORED	NONE of the pairs are in the 'Restored' state.
14	NOT_ALL_VALID	NOT all of the mirrored pairs are in a valid state.
15	NONE_VALID	NONE of the mirrored pairs are in a valid state.
16	SYM_NOT_ALL_LOCKED	NOT all of the specified Symmetrix units have an exclusive Symmetrix lock.
17	SYM_NONE_LOCKED	NONE of the specified Symmetrix units have an exclusive Symmetrix lock.
18	ALREADY_IN_STATE	The Device(s) is (are) already in the desired state or mode.
19	GK_IS_LOCKED	All GateKeeper devices to the Symmetrix unit are currently locked.

Table 9 Return code handling for Windows and UNIX (continued)

Code	Code symbol	Description
20	WP_TRACKS_IN_CACHE	Operation cannot proceed because the target device has Write Pending I/O in the cache.
21	NEED_MERGE_TO_RESUME	Operation cannot proceed without first performing a merge of the RDF Track Tables.
22	NEED_FORCE_TO_PROCEED	Operation cannot proceed in the current state except if you specify a force flag.
23	NEED_SYMFORCE_TO_PROCEED	Operation cannot proceed in the current state except if you specify a symforce flag.
24	NOT_IN_SYNC	The Symmetrix configuration and the database file are NOT in sync.
25	NOT_ALL_SPLIT	NOT all of the mirrored pairs are in the 'Split' state.
26	NONE_SPLIT	NONE of the mirrored pairs are in the 'Split' state.
27	NOT_ALL_SYNCINPROG	NOT all of the mirrored pairs are in the 'SyncInProg' state.
28	NONE_SYNCINPROG	NONE of the mirrored pairs are in the 'SyncInProg' state.
29	NOT_ALL_RESTINPROG	NOT all of the pairs are in the 'RestInProg' state.
30	NONE_RESTINPROG	NONE of the pairs are in the 'RestInProg' state.
31	NOT_ALL_SUSPENDED	NOT all of the mirrored pairs are in the 'Suspended' state.
32	NONE_SUSPENDED	NONE of the mirrored pairs are in the 'Suspended' state.
33	NOT_ALL_FAILED_OVER	NOT all of the mirrored pairs are in the 'Failed Over' state.
34	NONE_FAILED_OVER	NONE of the mirrored pairs are in the 'Failed Over' state.
35	NOT_ALL_UPDATEINPROG	NOT all of the mirrored pairs are in the 'R1 UpdInProg' state.

Table 9 Return code handling for Windows and UNIX (continued)

Code	Code symbol	Description
36	NONE_UPDATEINPROG	NONE of the mirrored pairs are in the 'R1 UpdInProg' state.
37	NOT_ALL_PARTITIONED	NOT all of the mirrored pairs are in the 'Partitioned' state.
38	NONE_PARTITIONED	NONE of the mirrored pairs are in the 'Partitioned' state.
39	NOT_ALL_ENABLED	NOT all of the mirrored pairs are in the 'Enabled' consistency state.
40	NONE_ENABLED	NONE of the mirrored pairs are in the 'Enabled' consistency state.
41	NOT_ALL_SYNCHRONIZED_AND_ENABLED	NOT all of the mirrored pairs are in the 'Synchronized' rdf state and the 'Enabled' consistency state.
42	NONE_SYNCHRONIZED_AND_ENABLED	NONE of the mirrored pairs are in the 'Synchronized' rdf state and in the 'Enabled' consistency state.
43	NOT_ALL_SUSP_AND_ENABLED	NOT all of the mirrored pairs are in the 'Suspended' rdf state and 'Enabled' consistency state.
44	NONE_SUSP_AND_ENABLED	NONE of the mirrored pairs are in the 'Suspended' rdf state and the 'Enabled' consistency state.
45	NOT_ALL_SUSP_AND_OFFLINE	NOT all of the mirrored pairs are in the 'Suspended' rdf state and 'Offline' link suspend state.
46	NONE_SUSP_AND_OFFLINE	NONE of the mirrored pairs are in the 'Suspended' rdf state and the 'Offline' link suspend state.
47	WONT_REVERSE_SPLIT	Performing this operation at this time will not allow you to perform the next BCV split as a reverse split.
48	CONFIG_LOCKED	Access to the configuration server is locked.

Table 9 Return code handling for Windows and UNIX (continued)

Code	Code symbol	Description
49	DEVS_ARE_LOCKED	One or more devices are locked.
50	MUST_SPLIT_PROTECT	If a device was restored with the protect option, it must be split with the protect option.
51	PAIRED_WITH_A_DRV	The function can not be performed since the STD device is already paired with a DRV device.
52	PAIRED_WITH_A_SPARE	NOT all of the Snap pairs are in the 'Copy in progress' state.
53	NOT_ALL_COPYINPROG	NOT all of the pairs are in the 'CopyInProgress' state.
54	NONE_COPYINPROG	NONE of the pairs are in the 'CopyInProgress' state.
55	NOT_ALL_COPIED	NOT all of the pairs are in the 'Copied' state.
56	NONE_COPIED	NONE of the pairs are in the 'Copied' state.
57	NOT_ALL_COPYONACCESS	NOT all of the pairs are in the 'CopyonAccess' state.
58	NONE_COPYONACCESS	NONE of the pairs are in the 'CopyonAccess' state.
59	CANT_RESTORE_PROTECT	The protected restore operation can not be completed because there are write pendings or the BCV mirrors are not synchronized.
60	NOT_ALL_CREATED	NOT all of the pairs are in the 'Created' state.
61	NONE_CREATED	NONE of the pairs are in the 'Created' state.
62	NOT_ALL_READY	NOT all of the BCVs local mirrors are in the 'Ready' state.
63	NONE_READY	NONE of the BCVs local mirrors are in the 'Ready' state.
64	STD_BKGRND_SPLIT_IN_PROG	The operation cannot proceed because the STD Device is splitting in the Background.

Table 9 Return code handling for Windows and UNIX (continued)

Code	Code symbol	Description
65	SPLIT_IN_PROG	The operation cannot proceed because the pair is splitting.
66	NOT_ALL_COPYONWRITE	NOT all of the pairs are in the 'CopyOnWrite' state.
67	NONE_COPYONWRITE	NONE of the pairs are in the 'CopyOnWrite' state.
68	NOT_ALL_RECREATED	Not all devices are in the 'Recreated' state.
69	NONE_RECREATED	No devices are in the 'Recreated' state.
70	NOT_ALL_CONSISTENT	NOT all of the mirrored pairs are in the 'Consistent' state.
71	NONE_CONSISTENT	NONE of the mirrored pairs are in the 'Consistent' state.
72	MAX_SESSIONS_EXCEEDED	The maximum number of sessions has been exceeded for the specified device.
73	NOT_ALL_PRECOPY	Not all source devices are in the 'Precopy' state.
74	NONE_PRECOPY	No source devices are in the 'Precopy' state.
75	NOT_ALL_PRECOPY_CYCLED	Not all source devices have completed one precopy cycle.
76	NONE_PRECOPY_CYCLED	No source devices have completed one precopy cycle.
77	CONSISTENCY_TIMEOUT	The operation failed because of a Consistency window timeout.
78	NOT_ALL_FAILED	NOT all of the pairs are in the 'Failed' state.
79	NONE_FAILED	NONE of the pairs are in the 'Failed' state.
80	CG_NOT_CONSISTENT	CG is NOT RDF-consistent.
81	NOT_ALL_CREATEINPROG	NOT all of the pairs are in the 'CreateInProg' state.
82	NONE_CREATEINPROG	None of the pairs are in the 'CreateInProg' state.
83	NOT_ALL_RECREATEINPROG	NOT all of the pairs are in the 'RecreateInProg' state.

Table 9 Return code handling for Windows and UNIX (continued)

Code	Code symbol	Description
84	NONE_RECREATEINPROG	None of the pairs are in the 'RecreateInProg' state.
85	NOT_ALL_TERMINPROG	NOT all of the pairs are in the 'TerminateInProg' state.
86	NONE_TERMINPROG	None of the pairs are in the 'TerminateInProg' state.
87	NOT_ALL_VERIFYINPROG	NOT all of the pairs are in the 'VerifyInProg' state.
88	NONE_VERIFYINPROG	None of the pairs are in the 'VerifyInProg' state.
89	NOT_ALL_VERIFIED	NOT all of the pairs are in the requested states.
90	NONE_VERIFIED	NONE of the pairs are in the requested states Note: This message is returned when multiple states are verified at once.
91	RDFG_TRANSMIT_IDLE	RDF group is operating in SRDF/A Transmit Idle.
92	NOT_ALL_MIGRATED	Not all devices are in the ' Migrated' state.
93	NONE_MIGRATED	None of devices are in the 'Migrated' state.
94	NOT_ALL_MIGRATEINPROG	Not all devices are in the 'MigrateInProg' state.
95	NONE_MIGRATEINPROG	None of devices are in the 'MigrateInProg' state.
96	NOT_ALL_INVALID	Not all devices are in the 'Invalid' state.
97	NONE_INVALID	None of devices are in the 'Invalid' state.
98	EMPTY_BACKUP	Cannot create an empty backup file.
99	NOT_ALL_BOUND	Not all devices are in the 'Bound' state.
100	NONE_BOUND	None of the devices are in the 'Bound' state
101	NOT_ALL_BINDING	Not all devices are in the 'Binding' state.
102	NONE_BINDING	None of the devices are in the 'Binding' state.

Table 9 Return code handling for Windows and UNIX (continued)

Code	Code symbol	Description
103	NOT_ALL_ALLOCATING	Not all devices are in the 'Allocating' state.
104	NONE_ALLOCATING	None of the devices are in the 'Allocating' state
105	NOT_ALL_DEALLOCATING	Not all devices are in the 'Deallocating' state.
106	NONE_DEALLOCATING	None of the devices are in the 'Deallocating' state.
107	NOT_ALL_DRAINING	Not all devices are in the 'Draining' state.
108	NONE_DRAINING	None of the devices are in the 'Draining' state.
109	NOT_ALL_UNBOUND	Not all devices are in the 'Unbound' state.
110	NONE_UNBOUND	None of the devices are in the 'Unbound' state.
111	NOT_ALL_NONPOOLED	Not all devices are in the 'Nonpooled' state.
112	NONE_NONPOOLED	None of the devices are in the 'Nonpooled' state.
113	NOT_ALL_DRAINWAIT	Not all devices are in the 'Drainwait' state.
114	NONE_DRAINWAIT	None of the devices are in the 'Drainwait' state.
115	NOT_ALL_DISABLED	Not all devices are in the 'Disabled' state.
116	NONE_DISABLED	None of the devices are in the 'Disabled' state.
117	NOT_ALL_DEACTIVATED	Not all devices are in the 'Deactivated' state.
118	NONE_DEACTIVATED	None of the devices are in the 'Deactivated' state.
119	NOT_ALL_UNBINDING	Not all devices are in the 'Unbinding' state.
120	NONE_UNBINDING	None of the devices are in the 'Unbinding' state.
121	NOT_ALL_RECLAIMING	Not all devices are in the 'Reclaiming' state.
122	NONE_RECLAIMING	None of the devices are in the 'Reclaiming' state.

Table 9 Return code handling for Windows and UNIX (continued)

Code	Code symbol	Description
123	NOT_ALL_BALANCING	Not all devices are in the 'Balancing' state.
124	NONE_BALANCING	None of the devices are in the 'Balancing' state.
125	DEVMASK_VALDTE_FAILED	The device masking data contains inconsistencies.
126	DEVMASK_FREQNT_CHANGES	The device masking data is continuously changing. Please try again.
127	STAR_INV_STATE	The operation is not allowed in the current Star state.
128	STAR_ALLOWED_FROM_WKLD	The operation is allowed from workload site only.
129	STAR_INV_DEF_FILE_FMT	The Star definition file format is not valid.
130	STAR_ACTN_FILE_ERROR	An error occured while accessing the Star action file.
131	STAR_DEF_FILE_ERROR	An error occured while accessing the Star definition file.
132	STAR_SETUP_REQD	The Star Setup action is required.
133	STAR_SETUP_INV_OPMODE	The specified Star mode of operation is not valid.
134	STAR_OPMODE_REQD	The Star mode of operation is required for this operation.
135	STAR_CTL_SITE_REQD	The Star control site name is required for this operation.
136	STAR_WKLD_SITE_REQD	The Star workload site name is required for this operation.
137	STAR_WKLD_OP_REQD	The Star workload site name and Star mode of operation is required for this operation.
138	STAR_CREATE_GROUP_FAIL	An error occured while creating Star group.
139	STAR_FULL_COPY_REQD	Star differential resync is not available. The FULL_COPY flag is required.
140	STAR_INV_ACTION_WOF	Operation can not be performed except if force flag is used.

Table 9 Return code handling for Windows and UNIX (continued)

Code	Code symbol	Description
141	STAR_BUILDCG_REQD	The Star Buildcg action is required.
142	NOT_ALL_FAILEDBACK	Not all devices are in the 'Failedback' state.
143	NONE_FAILEDBACK	None of the devices are in the 'Failedback' state.
144	NOT_ALL_STOPPED	Not all devices are in the 'Stopped' state.
145	NONE_STOPPED	None of the devices are in the 'Stopped' state.
146	NOT_ALL_CONSISTENT_NOINVALIDS	Not all devices are in the 'Consistent with no invalid tracks' state.
147	NONE_CONSISTENT_NOINVALIDS	None of the devices are in the 'Consistent with no invalid tracks' state
148	NOT_ALL_SYNCHRONOUS	Not all devices are in the 'Synchronous RDF' mode.
149	NONE_SYNCHRONOUS	None of the devices are in the 'Synchronous RDF' mode.
150	NOT_ALL_SEMISYNCHRONOUS	Not all devices are in the 'Semi-Synchronous RDF' mode.
151	NONE_SEMISYNCHRONOUS	None of the devices are in the 'Semi-Synchronous RDF' mode.
152	NOT_ALL_ASYNCHRONOUS	Not all devices are in the 'Asynchronous RDF' mode.
153	NONE_ASYNCHRONOUS	None of the devices are in the 'Asynchronous RDF' mode.
154	NOT_ALL_ACP_WP	Not all devices are in the 'Adaptive Copy Write Pending RDF' mode.
155	NONE_ACP_WP	None of the devices are in the 'Adaptive Copy Write Pending RDF' mode.
156	NOT_ALL_ACP_DISK	Not all devices are in the 'Adaptive Copy Disk RDF' mode.
157	NONE_ACP_DISK	None of the devices are in the 'Adaptive Copy Disk RDF' mode.

Table 9 Return code handling for Windows and UNIX (continued)

Code	Code symbol	Description
158	NOT_ALL_COMPRESSING	Not all devices are in the 'Compressing' state.
159	NONE_COMPRESSING	None of the devices are in the 'Compressing' state.
160	NOT_ALL_UNCOMPRESSING	Not all devices are in the 'Uncompressing' state.
161	NONE_UNCOMPRESSING	Not all devices are in the 'Established' state.
162	NOT_ALL_ESTABLISHED	Not all devices are in the 'Established' state.
163	NONE_ESTABLISHED	None of the devices are in the 'Established' state.
164	NOT_ALL_ESTINPROG	Not all devices are in the 'Estinprog' state.
165	NONE_ESTINPROG	None of the devices are in the 'Estinprog' state.
166	NOT_ALL_LINKED	Not all devices are in the 'Linked' state.
167	NONE_LINKED	None of the devices are in the 'Linked' state.
168	NOT_ALL_DEFINED	Not all devices are in the 'Defined' state.
169	NONE_DEFINED	None of the devices are in the 'Defined' state.
170	NOT_ALL_CIPLINKED	Not all linked devices are in the 'Copyinprog' state.
171	NONE_CIPLINKED	None of the linked devices are in the 'Copyinprog' state.
172	NOT_ALL_COPIEDLINKED	Not all linked devices are in the 'Copied' state.
173	NONE_COPIEDLINKED	None of the linked devices are in the 'Copied' state.
174	NOT_ALL_DESTAGED	Not all devices are in the 'Destaged' state.
175	NONE_DESTAGED	None of the devices are in the 'Destaged' state.
176	NOT_ALL_FREEING_ALL	Not all devices are in the 'FreeingAll' state.
177	NONE_FREEING_ALL	None of the devices are in the 'FreeingAll' state.

Table 9 Return code handling for Windows and UNIX (continued)

Code	Code symbol	Description
178	NOT_ALL_ACTIVE	Not all devices are in the 'Active' state.
179	NONE_ACTIVE	"None of the devices are in the 'Active' state.
180	NOT_ALL_DRAINED	Not all devices are in the 'Drained' state.
181	NONE_DRAINED	None of the devices are in the 'Drained' state.
182	NOT_ALL_ACTIVEACTIVE	Not all devices are in the 'ActiveActive' state.
183	NONE_ACTIVEACTIVE	None of the devices are in the 'ActiveActive' state.
184	NOT_ALL_ACTIVEBIAS	Not all devices are in the 'ActiveBias' state.
185	NONE_ACTIVEBIAS	None of the devices are in the 'ActiveBias' state.

INDEX