

Tru64 UNIX

Best Practice for Viewing High Priority System Events with EVM

November 9, 1999

This best practice describes how to monitor high priority system events for the Tru64™ UNIX® operating system.

Contents

Best Practice for viewing High Priority System Events

Is This Best Practice Right for You?	1
Before You Begin	2
Security Considerations	2
User Authentication	3
User Authorization	3
Remote Access	3
Applying the Best Practice	3
Verifying Success	5
Troubleshooting	6
Alternative Practices	7
Comments and Questions	8
Legal Notice	8

Best Practice for viewing High Priority System Events

The Event Manager (EVM) provides a flexible event posting and notification mechanism, which can be used to notify system administrators when an interesting event happens, and which unifies existing event channels into a single source of event information. Rather than replacing the familiar event channels, such as `syslog` and `binlog`, EVM encapsulates them. These channels remain in place, and continue to handle the same set of events they always did. However, EVM makes the existing channels much more accessible and therefore is the best practice for viewing system events.

The Event Viewer allows you to view events stored in log files. The Event Viewer provides capabilities to select and view events, to refresh the display with new or newly selected events, and optionally to print events or save them in a file. Events may be displayed, printed, or saved in summary or detail format.

You, the System Administrator, can use EVM to monitor high priority systems events, which are of interest to you or unique to your operating environment. EVM can also be configured to perform automatic notification of selected conditions.

Not all best practices apply to all configurations, so you must be sure that, this is appropriate for your system and circumstances. See the *System Administration* Guide for more information.

See the Tru64 UNIX Best Practices Web page for more information about best practices documentation:

<http://www.unix.digital.com/faqs/publications/bp/>

Is This Best Practice Right for You?

Not all best practices apply to all configurations, so you must be sure that, this is appropriate for your system and circumstances. To use this best practice, you must meet the requirements described in the following table.

Requirement	Description
Operating System	Tru64 UNIX Version 5.1
System Configuration	The EVM logger must be configured to log high priority events. If you have changed the configuration, run the <code>evmreload</code> command to ensure that the changes are recognized.
Additional Requirements	Before you attempt to monitor high priority system events, you should be a System Administrator with the appropriate user privileges, and be familiar with the SysMan Menu Application. See the <i>System Administration Guide</i> , <code>sysman(8)</code> and <code>sysman_station(8)</code> reference pages for further information.

If you do not meet the above requirements, see the *System Administration Guide*, and related reference pages for further information. You also may see the Alternative Practices for additional information.

Before You Begin

Before you apply the best practice for viewing high priority system events, you must take the following into consideration:

- Security
- User Authentication
- User Authorization
- Remote Access

Security Considerations

You must be aware that uncontrolled access to certain event information may provide an unauthorized user with sensitive information about system operation. Access is controlled by the `evm.auth` file.

Security is maintained by restricting access to event information to authorized users. EVM also prevents unauthorized users from posting events.

You can administer access control through the authentication file `/etc/evm.auth`, see the `evm.auth(4)` reference page for more information.

User Authentication

The EVM daemon authenticates the identities of all local system users before accepting any connection request. However, in Tru64 UNIX Version 5.1 no authentication is performed on remote users, so remote users are restricted in their authorization.

User Authorization

Access to events is controlled by the EVM authorization file, located in `/etc/evm.auth`. You can authorize users either individually or by group to do any of the following:

- Post selected events
- Access (subscribe to or retrieve from storage) selected events

Remote Access

Remote access allows users on other systems to monitor events on the local system through a network connection.

By default, remote access is disabled in the daemon's configuration file, `/etc/evmdaemon.conf`. You should enable it only if your system is running in a trusted environment.

Applying the Best Practice

Before you monitor system events with EVM, be sure to follow the recommendations in *Before You Begin*.

1. Start the SysMan Menu

```
# sysman -menu &
```
2. Launch the Event Viewer from the View Events leaf of the Monitoring and Tuning branch of the SysMan Menu.
 - a. From the SysMan Menu, select Monitoring and Tuning.
 - b. Then select View Events. The View Events viewer may show all events, unless you have previously set the filter or this is the first time you have used the viewer.
 - c. If you do not see a priority number column displayed in the View Events dialog box, then you will need to select this option. Select

the Customize button, then select Pri (Event Priority) in order to display the priority of events.

3. Set the filter to view priority events as follows:

- a. Select the Filter button.
- b. In the View Events Filter dialog box, select the Priority.
- c. Select a range. Type in a range, usually 500 through 700.
- d. The range is an integer value in the range 0-700, with zero being the least significant priority. The following list describes priorities and their ranges:

Name	Range	Description
Emergency	700	A dangerous situation has been detected and immediate action either is required or has been taken.
Alert	600-699	A dangerous situation is imminent and immediate action either is required or has been taken.
Critical	500-599	A failure has been detected that renders some part of the system inoperable.

- e. Select OK or Apply the priority ranges. The View Events main dialog should now show a list of all events within your selected priority range. See the `EvmEvent(5)` reference page for more information.

4. If you would like to see more detail of a particular event:
 - a. Select an event. The selected event is indicated by a change in background color or a greater than symbol (>) in the first position of the display line, depending on the capabilities of the display in use.
 - b. Select Details... to open the Details of Event dialog box.
Details may give some indication of what to do, for example call Compaq Services if the event indicates a system or hardware problem.
 - c. Select OK to return to the Event Viewer main dialog box when you have finished viewing the event.
5. To change the event for which details are being displayed from the Details of Event dialog box:
 - a. Select Next Event to display the event immediately following the current event.
 - b. Select Previous Event to display the event immediately preceding the current event.
 - c. Select First Event to display the first available event.
 - d. Select Last Event to display the last available event.
 - e. Select OK to close the dialog box, and select another event and select Details... again.
6. If you want to monitor events over a long period without restarting the event viewer, you will need to:
 - a. Select the Refresh button periodically to refresh the event display pool.
 - b. To monitor events as they occur use the `evmwatch` command.
 - c. Refer to the `evmwatch(1)` reference page for further information.

Verifying Success

After you apply the best practice for Viewing High Priority System Events with EVM, you know that you were successful when the event viewer display only shows events in the selected range.

If the best practice was not successful, see *Troubleshooting* for information about identifying and solving problems.

Troubleshooting

If you determine that the best practice was not successful, as described in *Verifying Success*, use the following table to identify and solve problems.

If you suspect that EVM is not operating correctly, the first step should be to check the message files in `/var/evm/adm/logfiles`. Messages in these files are also displayed through the EVM viewer and `evmget`, also, check that `evmd`, and `evmllogger` are running. The following list describes some common problems and the initial steps you should take in trying to resolve such problems:

Problem	Possible Solutions
No events listed in Viewer.	Do you have the authorization required to see all events? If you are not logged in as root on the local system you will not be authorized to see everything. Either log in as root and try again, or update the authorization file. See the <code>evm.auth(4)</code> reference page for further information.
Expected events are not being logged.	Only events with a priority of 200 or higher are logged by the EVM logger. You can alter the logger's configuration to change this. Check what events are being filtered by the <code>evmlog</code> section of the configuration file. See the <code>evmllogger(4)</code> reference page for further information.
Expected <code>syslog</code> or <code>binlog</code> events are not visible through EVM.	You must either be logged in as root or belong to the <code>adm</code> group in order to access <code>syslog</code> and <code>binlog</code> events. You can change this behavior by changing the <code>evm.auth</code> file.

Problem	Possible Solutions
High priority <code>binlog</code> events are not showing up.	By default, only one week of <code>binlog</code> events are displayed. Change the channel configuration file (<code>evmchannel.conf</code>), where the <code>binlog</code> file line that says <code>-r d8</code> , where 8 is the number of days worth of events (e.g. change 8 to 31, or remove the <code>-d8</code>).
Event retrieval through the event viewer is slow.	Check the sizes of all log files, particularly the <code>evmlog</code> files (<code>/var/evm/evmlog</code>), the binary error log (<code>/var/adm/binary.errlog</code>) and the SysMan Station daemon log files (<code>/var/adm/sysman/smsd*.log*</code>). If the files are big, refer to <i>System Administration Guide</i> for log file management procedures.

Refer to the *System Administration Guide* for more troubleshooting information.

Alternative Practices

Although this best practice is the recommended method for viewing High Priority System Events, if your system does not meet the requirements described in *Is This Best Practice Right for You?*, you can use an alternative method:

1. Do not filter events, but sort events into descending priority order. To sort events do the following:
 - a. Select the Sort... button.
 - b. In the Sort Event Summaries dialog box, select sort order, Descending.
 - c. Select Apply to view events in descending order, with the highest priority events listed first.
 - d. Select OK to close the Sort Event Summaries dialog box.
2. If you prefer to view events by using the command line utilities rather than the graphical event viewer, you might find these examples helpful:
 - a. The following example retrieves all events with a priority of 600 or greater, sorts them into descending order of priority (most urgent first) and then ascending order of time (oldest first), and displays them.

```
# evmget -f "[priority >= 600]" | evmsort -s @timestamp- |  
evmshow -t "@timestamp [priority]@"
```

Refer to the `evmget(1)` and `evmsort(1)` reference page for further information.

- b. In the following example, all available events are retrieved and piped to `evmshow` for formatting. The show template causes the events to be displayed as timestamp value, followed by the event's priority enclosed in brackets, followed by the formatted event string.

```
# evmget | evmshow -t "@timestamp [priority] @" | more
```

Refer to the `evmshow(1)` reference page for further information.

- c. The following example watches for all events with a priority of at least 600, and displays them on `stdout`.

```
# evmwatch -f '[priority >= 600]' | evmshow -t "@timestamp [priority]@"
```

Refer to the `evmwatch(8)` reference page for further information.

3. Use the following EVM Administrative Utilities:

- a. `evmreload(8)` - if the logger configuration is changed.
- b. `evmstart(8)` - only if the EVM daemon (`evmd`) is not running.

See the *System Administration* Guide for more information about viewing system events.

Comments and Questions

We value your comments and questions on the information in this document. Please mail your comments to us at this address:

`readers_comment@zk3.dec.com`

Legal Notice

COMPAQ and the Compaq logo are registered in the U.S. Patent and Trademark Office.

Confidential computer software. Valid license from Compaq required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendors standard commercial license.

Compaq shall not be liable for technical or editorial errors or omissions contained herein. The information in this publication is subject to change without notice and is provided "as is" without warranty of any kind. The entire risk arising out of the use of this information remains with recipient. In no event shall Compaq be liable for any direct, consequential, incidental, special, punitive, or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption or loss of business information), even if Compaq has been advised of the possibility of such damages. The foregoing shall apply regardless of the negligence or other fault of either party and regardless of whether such liability sounds in contract, negligence, tort, or any other theory of legal liability, and notwithstanding any failure of essential purpose of any limited remedy.

The limited warranties for Compaq products are exclusively set forth in the documentation accompanying such products. Nothing herein should be construed as constituting a further or additional warranty.