

Tru64 UNIX Event Management

DECUS Symposium 2005



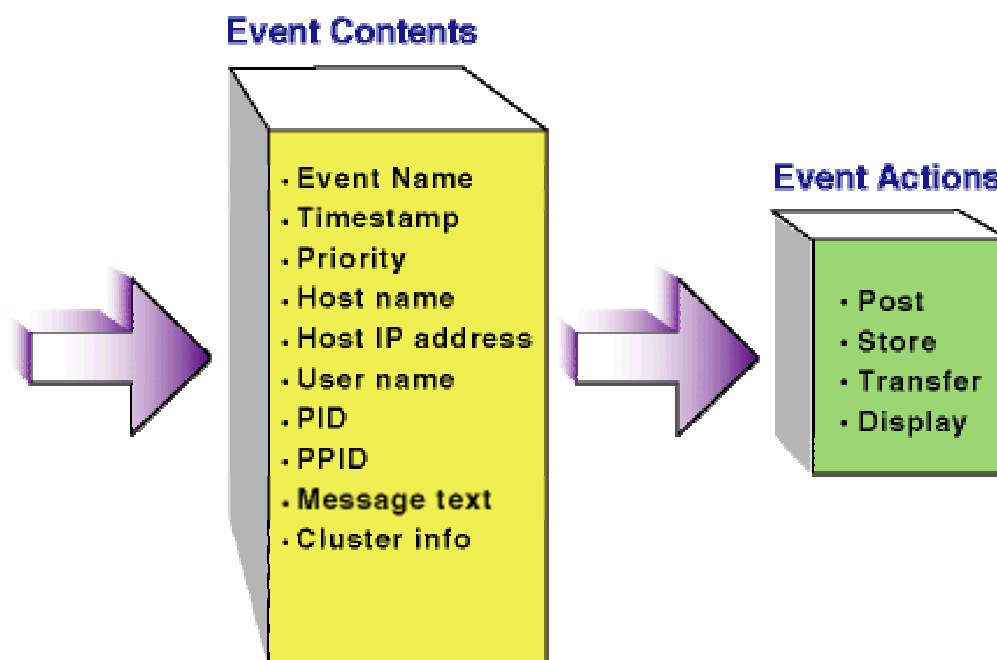
Reinhard Stadler
Technical Consultant

Agenda



- EVM Overview
- Retrieving and Viewing Events
- Configuring EVM
- Filtering and Forwarding

- EVM provides a single point of event information supplementing rather than replacing the traditional UNIX log files
 - Full set of command-line utilities that you can use to post and handle events
 - Integration of a graphical event viewer with the SysMan application suite
 - Events can be selected or filtered
 - Support for all event channels, including syslog and binlog
 - Configurable notification on occurrence of specific events



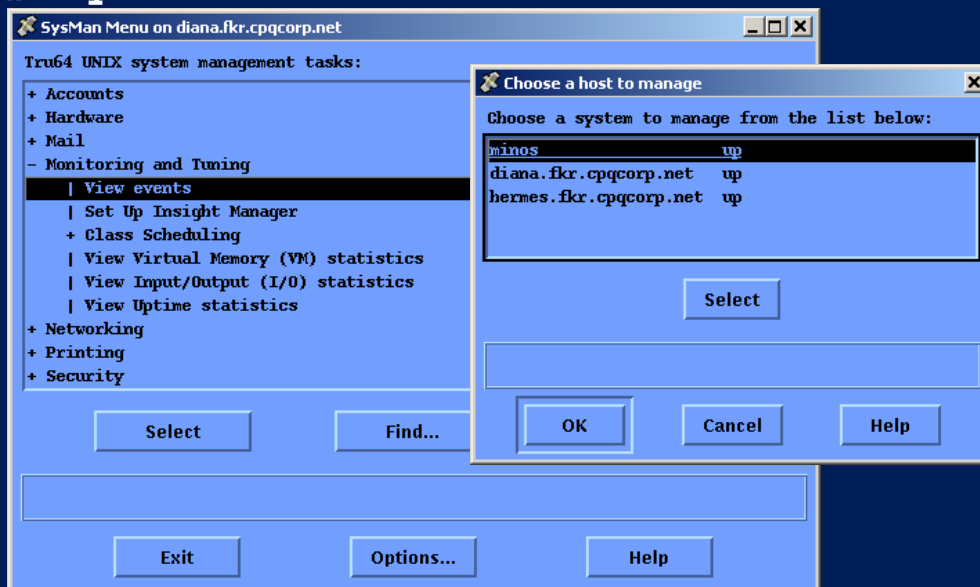
Retrieving and Viewing Events



Using the SysMan Event Viewer



sysman &



Using the SysMan Event Viewer



The screenshot shows the 'View Events on diana.fkr.cpqcorp.net' window with a list of 24679 events. A 'View Events: Customize' dialog box is open, allowing users to select which items to display in the event summaries. The dialog includes checkboxes for 'Eventid (Event Sequence Number)', 'Pri (Event Priority)', 'Timestamp (Posting Timestamp)', 'PID (Posting Process ID)', 'User (Posting User)', 'Host (Posting Host)', 'Cluster (Posting Cluster)', 'Event Name', and 'Summary (Formatted Message)'. The 'Number of events to display' is set to 500. There is also a checkbox to 'Show the Event Sequence Number item in the event summaries'.

Event ID	Priority	Date	Time	User	Message
205532	200	31-Mar-2003	13:35:30	diana	syslog: NetWorker med
205675	200	31-Mar-2003	13:35:30	diana	syslog: NetWorker med
205668	500	31-Mar-2003	13:35:22	diana	vmunix: NFS server: u
205665	200	31-Mar-2003	13:33:13	diana	syslog: NetWorker med
205664	600	31-Mar-2003	13:32:37	diana	CAAD[1049279]: An err
205663	600	31-Mar-2003	13:32:37	diana	CAAD[1049279]: RTD #0
205656	200	31-Mar-2003	13:27:36	diana	syslog: NetWorker med
616608	400	31-Mar-2003	13:21:05	hermes	syslog: yp_all - TCP
205645	500	31-Mar-2003	13:20:18	diana	vmunix: NFS3 RFS3_GET
205643	200	31-Mar-2003	13:20:07	diana	syslog: NetWorker med
205638	200	31-Mar-2003	13:20:07	diana	[4 times] syslog: Net
205636	200	31-Mar-2003	13:20:06	diana	svslog: NetWorker med

Using the SysMan Event Viewer



The screenshot shows the 'View Events on diana.fkr.cpqcorp.net' window with a list of 24679 events. A 'View Events: Filter' dialog box is open, allowing users to filter events based on various criteria. The dialog includes checkboxes for 'Event Name', 'Posting Host', 'Priority', 'Before', 'Since', and 'Age'. The 'Event Name' filter is set to 'equal to sys.unix.*'. The 'Priority' filter is set to 'equal to' with a range of 600 to 700. The 'Before' and 'Since' filters are set to 'Day: 12', 'Month: Jan', and 'Year: 2001'. The 'Age' filter is set to 'less than 30 days'. There is also a checkbox to 'Displays only events this year or later'.

Event ID	Priority	Date	Time	User	Message
205532	200	31-Mar-2003	13:35:30	diana	syslog: NetWorker med
205675	200	31-Mar-2003	13:35:30	diana	syslog: NetWorker med
205668	500	31-Mar-2003	13:35:22	diana	vmunix: NFS server: u
205665	200	31-Mar-2003	13:33:13	diana	syslog: NetWorker med
205664	600	31-Mar-2003	13:32:37	diana	CAAD[1049279]: An err
205663	600	31-Mar-2003	13:32:37	diana	CAAD[1049279]: RTD #0
205656	200	31-Mar-2003	13:27:36	diana	syslog: NetWorker med
616608	400	31-Mar-2003	13:21:05	hermes	syslog: yp_all - TCP
205645	500	31-Mar-2003	13:20:18	diana	vmunix: NFS3 RFS3_GET
205643	200	31-Mar-2003	13:20:07	diana	syslog: NetWorker med
205638	200	31-Mar-2003	13:20:07	diana	[4 times] syslog: Net
205636	200	31-Mar-2003	13:20:06	diana	svslog: NetWorker med

Using the SysMan Event Viewer



View Events on diana.fkr.cpqcorp.net

Event summaries from minos
24679 events matched specified filter. 500 event summaries displayed.

205532	200	31-Mar-2003 13:35:20	...
205675	200	31-Mar-2003 13:35:20	...
205668	500	31-Mar-2003 13:35:20	...
205665	200	31-Mar-2003 13:33:20	...
205664	600	31-Mar-2003 13:32:20	...
205663	600	31-Mar-2003 13:32:20	...
205656	200	31-Mar-2003 13:27:20	...
616608	400	31-Mar-2003 13:21:20	...
205645	500	31-Mar-2003 13:20:20	...
205643	200	31-Mar-2003 13:20:20	...
205638	200	31-Mar-2003 13:20:20	...
205636	200	31-Mar-2003 13:20:20	...

View Events: Sort Event Summaries

Sort Key

- EventId (Event Sequence Number)
- Pri (Event Priority)
- Timestamp (Posting Timestamp)
- Host (Posting Host)
- Summary (Formatted Message)

Sort Order

- Ascending
- Descending

Select an item to serve as the sort key.

Buttons: OK, Apply, Cancel, Help

Using the SysMan Event Viewer



View Events on diana.fkr.cpqcorp.net

Event summaries from minos
24679 events matched specified filter. 500 event summaries displayed.

View Events: Details of Event with Id = 205663

==== Syslog event =====
EVM event name: sys.unix.syslog.daemon

Syslog daemon events are posted by system daemons to alert the administrator to an unusual condition. The user name field usually indicates which daemon posted the event. The text of the message indicates the reason for the event.

Formatted Message:
CAAD[1049279]: RTD #0: Action Script
/var/cluster/caa/script/networker.scr(check) timed out! (timeout=600)

Event Data Items:
Event Name : sys.unix.syslog.daemon
Priority : 600
PID : 1049152
PPID : 1048577

Buttons: Next Event, Previous Event, First Event, Last Event, OK, Save..., Print..., Help

- `evmget` Retrieves stored events
 - `evmshow` Accepts one or more EVM events and outputs them in the requested format
 - `evmsort` Reads a stream of events and sorts them according to supplied criteria
 - `evmwatch` Outputs specified events as they arrive
 - `evmpost` Accepts a file or stream of text event sources and posts them to the EVM daemon for distribution
- most common command sequence for event retrieval
`evmget | evmsort | evmshow`

Retrieving Stored Events: `evmget`

```
evmget [ -A [-t show-template]
        [-s sort-spec] ]
        [-f filter-string]
        [-C channel-list]
```

`-f filter_expr` Outputs only events that match the `filter_expr`

```
# evmget -f "[ priority >= 600 ]"
```

- A specification of a set of interesting events
- Format: " [keyword expr] "

- Possible values for keyword are:

```
Name
Priority (from 0 to 700)
Timestamp
Age
BEFore
SINce
Event_ID
...
```

Complex EVM event filters

- A complex filter is composed of two or more simple filters
- Event filters can be direct or indirect

```
@filename:filtername
```

- Examples

```
"[name sys.unix.binlog] & [pri >= 500]"
```

```
"[name sys.unix.syslog] and  
[time 2005:4:5:*:*:*:*]"
```

```
"@sys:advfs"
```

the filter named advfs contained in a filter file named sys or sys.evf in /usr/share/evm/filters

Displaying Events Using evmshow



- `evmshow` accepts one or more EVM events and outputs them in the requested format

```
# evmshow [[-d | -D | -x ]
           [-t show-template]
           [-T timespec] | -r]
           [-c config-file]
           [-f filter-expr] [-F]
           [-k skip-count] [-n show-count]
           [filename | -]
```

EVM show template



- a string that may contain event data item specifiers of the form `@item_name[%width]`
 - `@timestamp`
 - `@priority`
 - `@name`
 - `@@` (the event's formatted text)
 - E.g. "`@timestamp [@priority] @name @@`"
- `EVM_SHOW_TEMPLATE` environment variable

Sorting Events Using evmsort



- Reads a stream of events and sorts them according to supplied criteria

```
evmsort [-s sort-spec]
        [-A [-t show-template]]
        [filename | -]
```

- The sort order can be specified by supplying a `sort_spec`

```
@key_item[+|-] [ :@key_item[+|-] ]
```

`key_item` is the name of any EVM standard data item

Using the -A Option to Simplify the Command String



- most common command sequence for event retrieval

```
evmget | evmsort | evmshow
```

```
# evmget -A
```

automatically pipes the output to other EVM commands

```
# evmget -f '[pri >= 600]' | evmsort -s \
  "priority-:timestamp+" | evmshow | more
```

```
# evmget -A -f '[pri >= 600]' -s \
  "priority-:timestamp+" | more
```

Monitoring Events Using evmwatch



evmwatch

Outputs specified events as they arrive

```
evmwatch [-A] [-f filter_expr]
[-t show_template]
```

```
# evmwatch -i | \
    evmshow -t "@name @priority @"
```

Posting Message Events Using evmpost

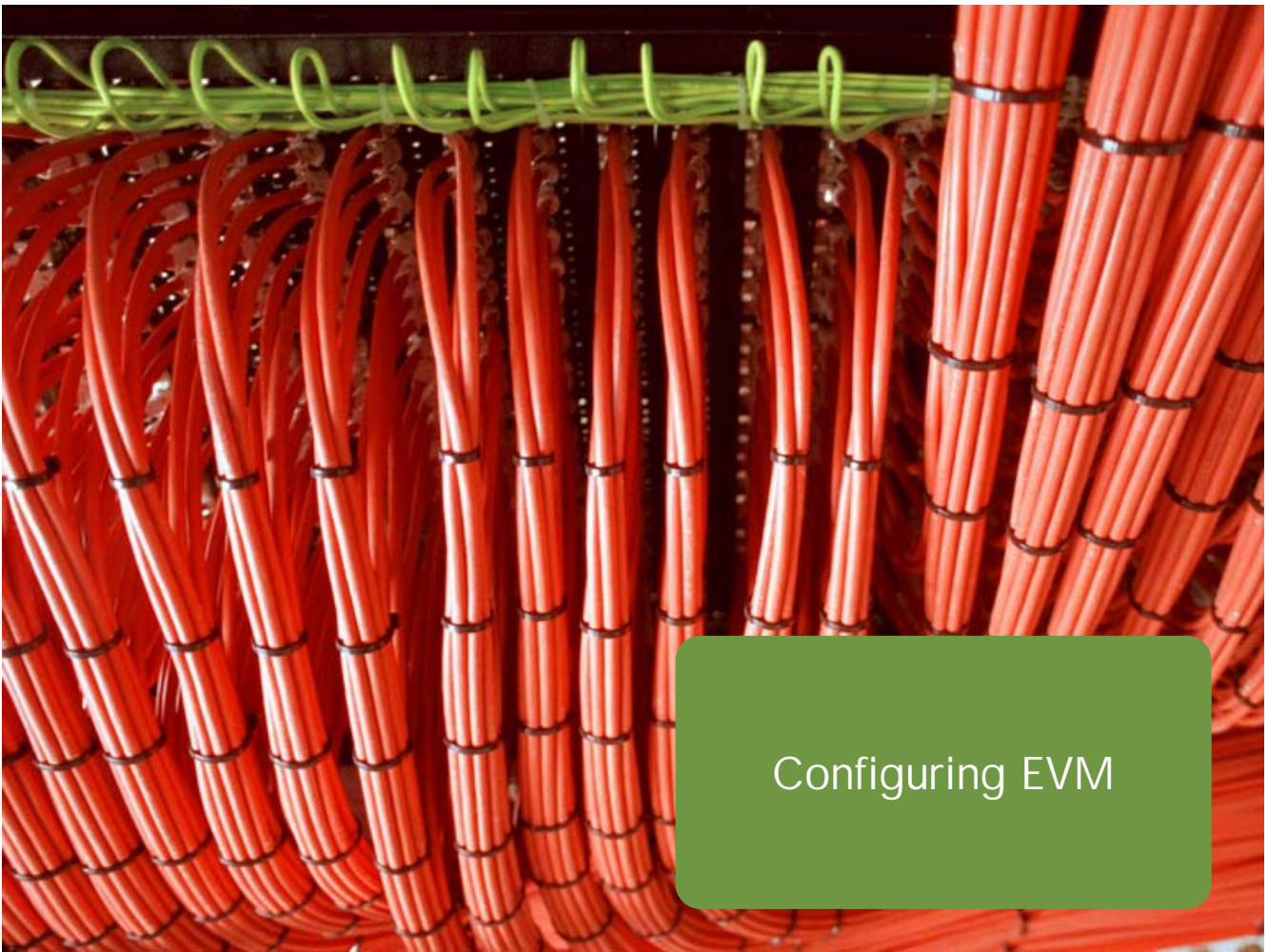


evmpost

Accepts a file or stream of text event sources and posts them to the EVM daemon for distribution

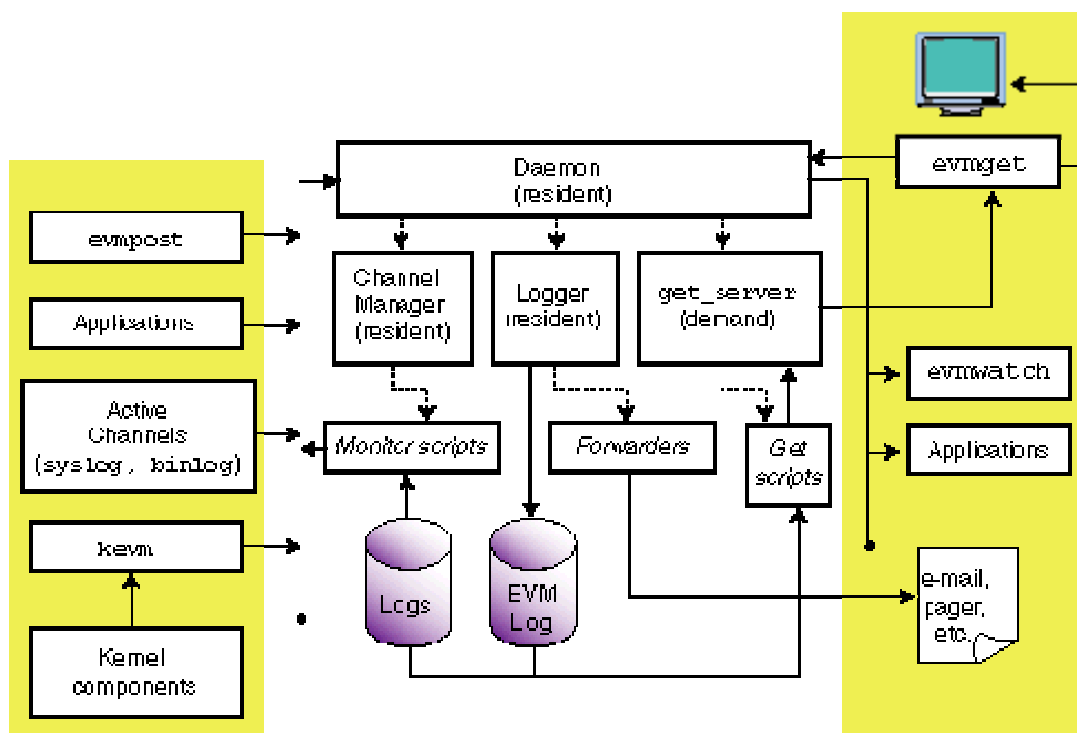
```
# evmpost [ -f <file> | - ]
```

```
# echo 'event {name ... }' | evmpost
```



Configuring EVM

EVM Component Model



ZIG-1371U-A1

The EVM daemon



- The primary component of EVM
 - Starts the logger
 - Starts the channel manager
 - Receives events from posters and distributes them to subscribers
- Default configuration file </etc/evmdaemon.conf>

The Channel Manager



- Runs channel monitor scripts and cleanup scripts
- For each channel a selection of functions may be defined
 - `fn_get` invoked by `evmget_srv`
 - `fn_details` used by `evmshow -d`
 - `fn_explain` used by `evmshow -x`
 - `fn_monitor` monitors the status of a channel
 - `fn_cleanup` archives or purges logs
 - `mon_period` monitor period
- Configuration file </etc/evmchannel.conf>

- Runs as a resident process
- Subscribes to a selected set of events
 - Stores them in managed log files for later retrieval
 - Writes high-priority events to the system console
 - Forwards selected events
(e.g. sends mail to the system administrator when high-priority events occur)
- configuration file [/etc/evmlogger.conf](#)

Forwarding Events

- Specific events can trigger any user defined action (e.g. alarms, scripts, ...)
- „forward“ statement in the evm logger configuration
- Should be placed in `/var/evm/adm/config/logger`
- Example:
 - trigger a script if NIFF detects a NW interface failure
- [netrain.conf](#)

- `/var/evm/evmlog` event logs
 `evmlog.yyyymmdd[_nn]`
- System-supplied definition files:
 - `/usr/share/evm/channels`
 - `/usr/share/evm/filters`
 - `/usr/share/evm/templates`
- Installation of new definition files:
 - `/var/evm/adm/templates`
 - `/var/evm/adm/channels`
 - `/var/evm/adm/filters`
- Secondary logger configuration files
 - `/var/evm/adm/config/logger`

Define a new Event

- Create a template file to define the new event(s)
 - The syntax of a template file is identical to the syntax used to post an event
- Save the template file in `/var/evm/adm/templates` (create subdirectories if necessary)
- Instruct the EVM daemon to reload its configuration
- Verify template registration by using the **`evmwatch -i`**
- You can now post your new event(s) and retrieve it from storage

Questions



i n v e n t