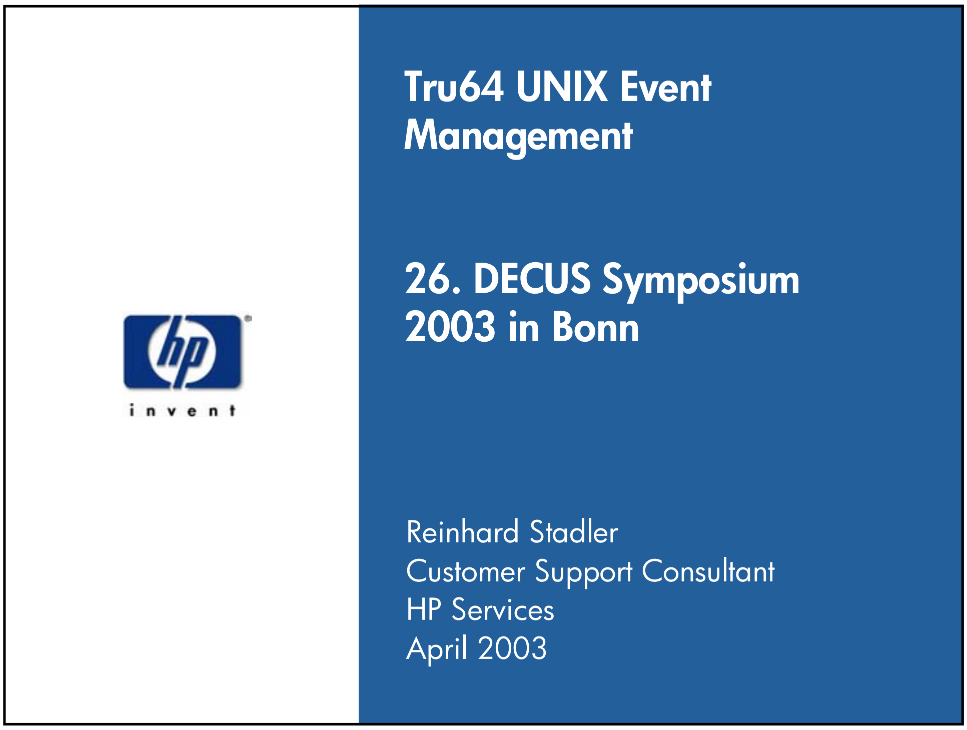
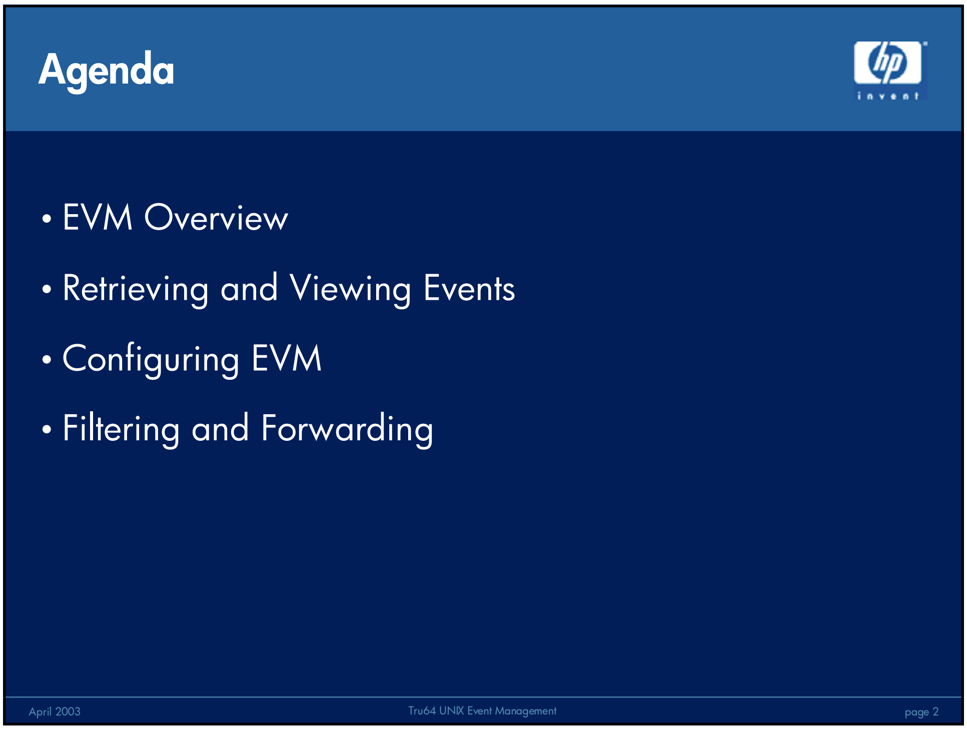


Tru64 UNIX Event Management

26. DECUS Symposium 2003 in Bonn

Reinhard Stadler
Customer Support Consultant
HP Services
April 2003



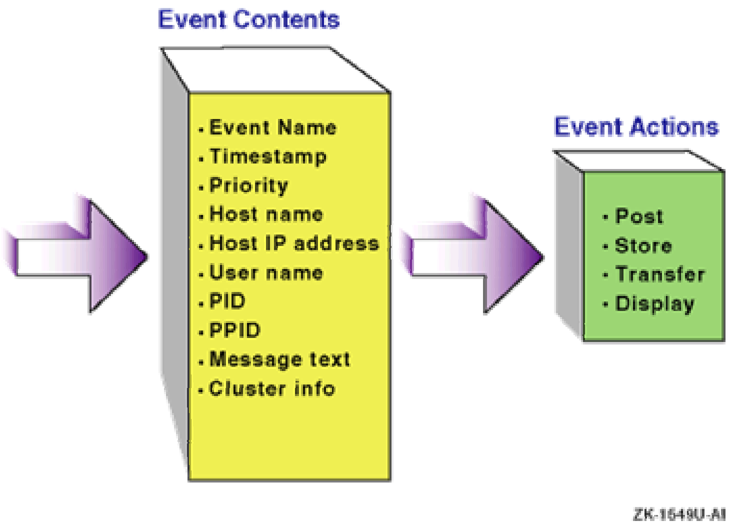
Agenda

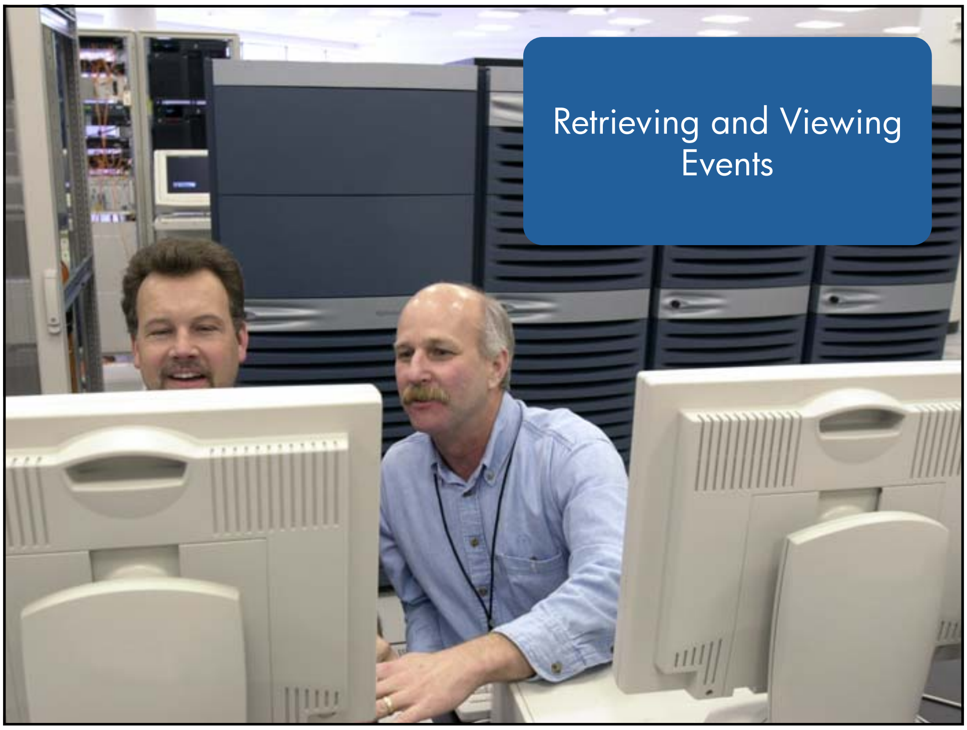
- EVM Overview
- Retrieving and Viewing Events
- Configuring EVM
- Filtering and Forwarding

EVM Features

- 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

Event Model

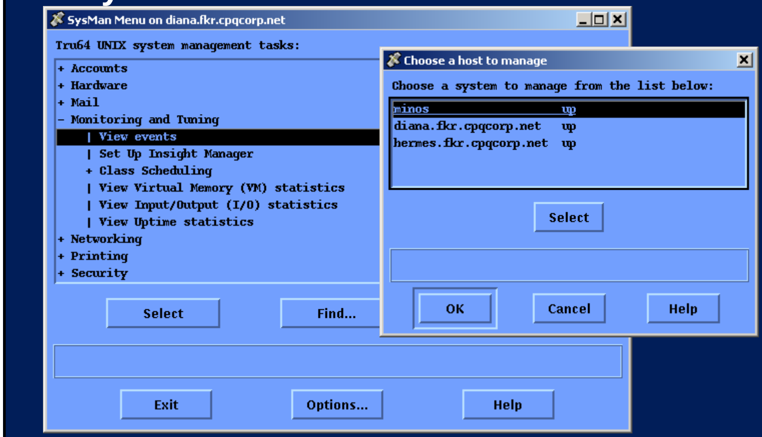




Retrieving and Viewing Events

Using the SysMan Event Viewer

```
# sysman &
```



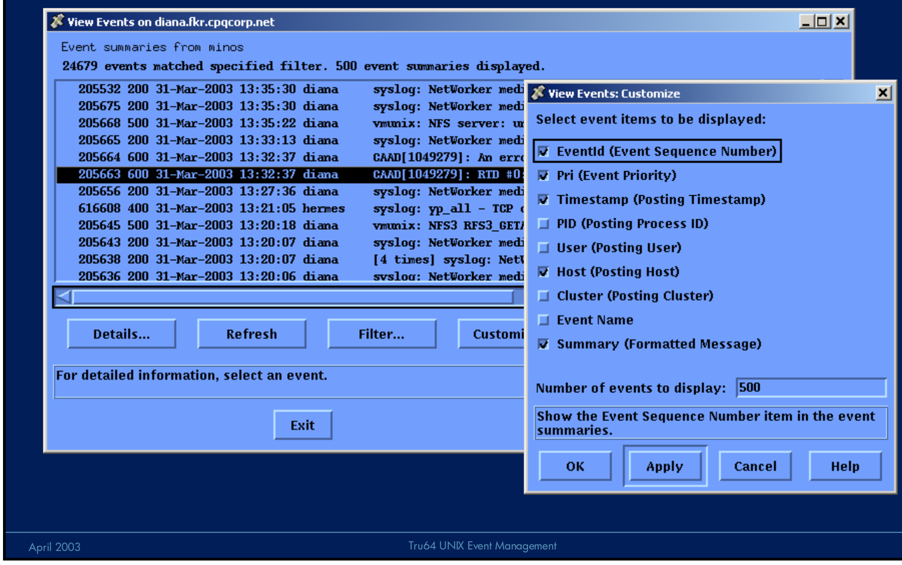
SysMan Menu on diana.fkr.cpqcorp.net

```
Tru64 UNIX system management tasks:
+ Accounts
+ Hardware
+ Mail
- Monitoring and Tuning
    | View events
    | Set Up Insight Manager
    + Class Scheduling
    | View Virtual Memory (VM) statistics
    | View Input/Output (I/O) statistics
    | View Uptime statistics
+ Networking
+ Printing
+ Security
```

Choose a host to manage

```
Choose a system to manage from the list below:
minos                   up
diana.fkr.cpqcorp.net   up
hermes.fkr.cpqcorp.net  up
```

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 13:35:30 diana     syslog: NetWorker medi
   205675 200 31-Mar-2003 13:35:30 diana     syslog: NetWorker medi
   205668 500 31-Mar-2003 13:35:22 diana     vmunix: NFS server: u
   205665 200 31-Mar-2003 13:33:13 diana     syslog: NetWorker medi
   205664 600 31-Mar-2003 13:32:37 diana     CAAD[1049279]: An erro
   205663 600 31-Mar-2003 13:32:37 diana     CAAD[1049279]: RTD #0:
   205656 200 31-Mar-2003 13:27:36 diana     syslog: NetWorker medi
   616608 400 31-Mar-2003 13:21:05 hermes    syslog: yp_all - TCP c
   205645 500 31-Mar-2003 13:20:18 diana     vmunix: NFS3 RFS3_GETA
   205643 200 31-Mar-2003 13:20:07 diana     syslog: NetWorker medi
   205638 200 31-Mar-2003 13:20:07 diana     [4 times] syslog: Net
   205636 200 31-Mar-2003 13:20:06 diana     syslog: NetWorker medi
```

For detailed information, select an event.

View Events: Customize

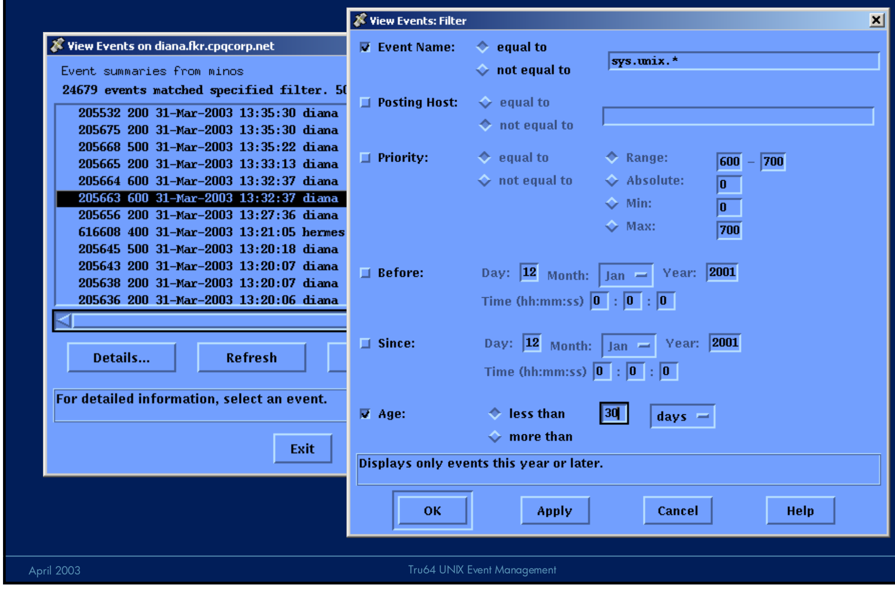
Select event items to be displayed:

- ☑ 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
- ☑ Summary (Formatted Message)

Number of events to display: 500

Show the Event Sequence Number item in the event summaries.

Using the SysMan Event Viewer



View Events on diana.fkr.cpqcorp.net

```
Event summaries from minos
24679 events matched specified filter. 50
   205532 200 31-Mar-2003 13:35:30 diana
   205675 200 31-Mar-2003 13:35:30 diana
   205668 500 31-Mar-2003 13:35:22 diana
   205665 200 31-Mar-2003 13:33:13 diana
   205664 600 31-Mar-2003 13:32:37 diana
   205663 600 31-Mar-2003 13:32:37 diana
   205656 200 31-Mar-2003 13:27:36 diana
   616608 400 31-Mar-2003 13:21:05 hermes
   205645 500 31-Mar-2003 13:20:18 diana
   205643 200 31-Mar-2003 13:20:07 diana
   205638 200 31-Mar-2003 13:20:07 diana
   205636 200 31-Mar-2003 13:20:06 diana
```

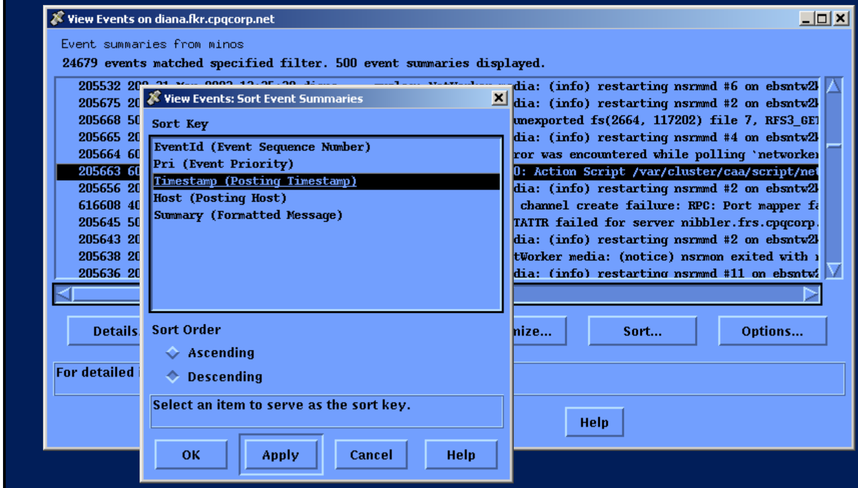
For detailed information, select an event.

View Events: Filter

- ☑ Event Name: ◇ equal to ◇ not equal to — sys.unix.*
- ☐ Posting Host: ◇ equal to ◇ not equal to
- ☐ Priority: ◇ equal to ◇ not equal to — ◇ Range: 600 – 700; ◇ Absolute: 0; ◇ Min: 0; ◇ Max: 700
- ☐ Before: Day: 12 Month: Jan Year: 2001 Time (hh:mm:ss) 0 : 0 : 0
- ☐ Since: Day: 12 Month: Jan Year: 2001 Time (hh:mm:ss) 0 : 0 : 0
- ☑ Age: ◇ less than ◇ more than 30 days

Displays only events this year or later.

Using the SysMan Event Viewer



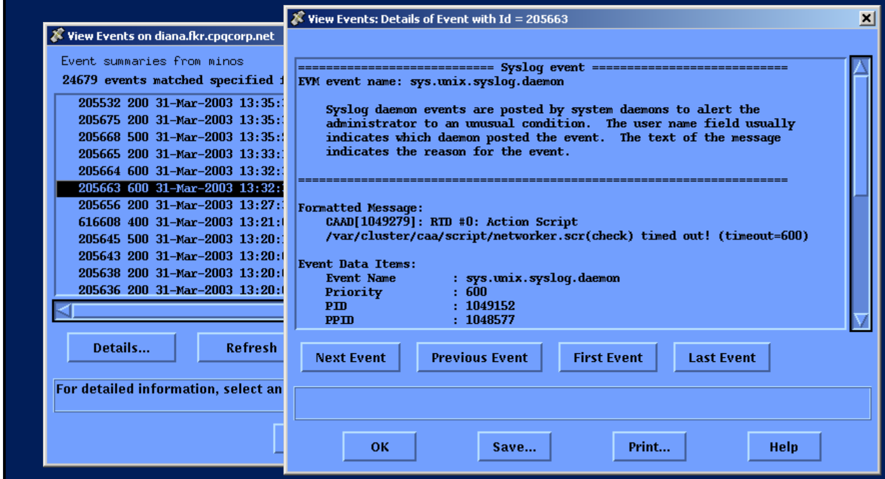
```
Event summaries from minos
24679 events matched specified filter. 500 event summaries displayed.
  205532 20...dia: (info) restarting nsrmmd #6 on ebsntw2
  205675 20...dia: (info) restarting nsrmmd #2 on ebsntw2
  205668 50...unexported fs(2664, 117202) file 7, RFS3_GE
  205665 20...dia: (info) restarting nsrmmd #4 on ebsntw2
  205664 60...ror was encountered while polling `networke
  205663 60...0: Action Script /var/cluster/caa/script/ne
  205656 20...dia: (info) restarting nsrmmd #2 on ebsntw2
  616608 40... channel create failure: RPC: Port mapper f
  205645 50...TATTR failed for server nibbler.frs.cpqcorp
  205643 20...dia: (info) restarting nsrmmd #2 on ebsntw2
  205638 20...tWorker media: (notice) nsrmon exited with
  205636 20...dia: (info) restarting nsrmmd #11 on ebsntw
```

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

Select an item to serve as the sort key.

For detailed

Using the SysMan Event Viewer



```
Event summaries from minos
24679 events matched specified f
  205532 200 31-Mar-2003 13:35:
  205675 200 31-Mar-2003 13:35:
  205668 500 31-Mar-2003 13:35:
  205665 200 31-Mar-2003 13:33:
  205664 600 31-Mar-2003 13:32:
  205663 600 31-Mar-2003 13:32:
  205656 200 31-Mar-2003 13:27:
  616608 400 31-Mar-2003 13:21:
  205645 500 31-Mar-2003 13:20:
  205643 200 31-Mar-2003 13:20:
  205638 200 31-Mar-2003 13:20:
  205636 200 31-Mar-2003 13:20:
```

For detailed information, select an

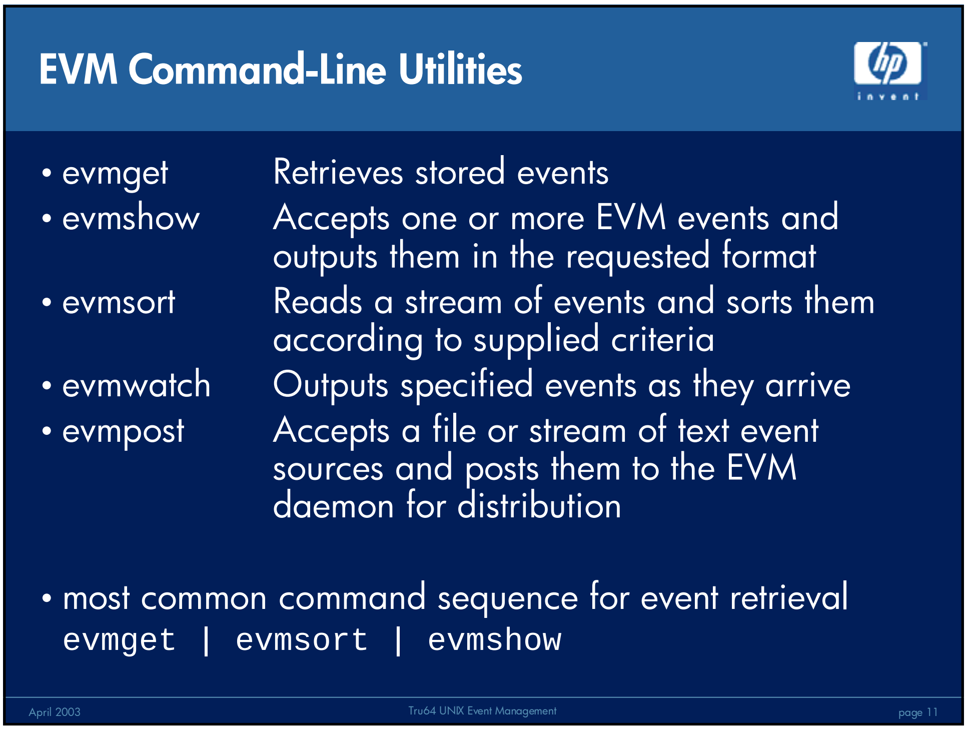
```
============================ Syslog event ============================
EVM event name: sys.unix.syslog.daemon

    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
```

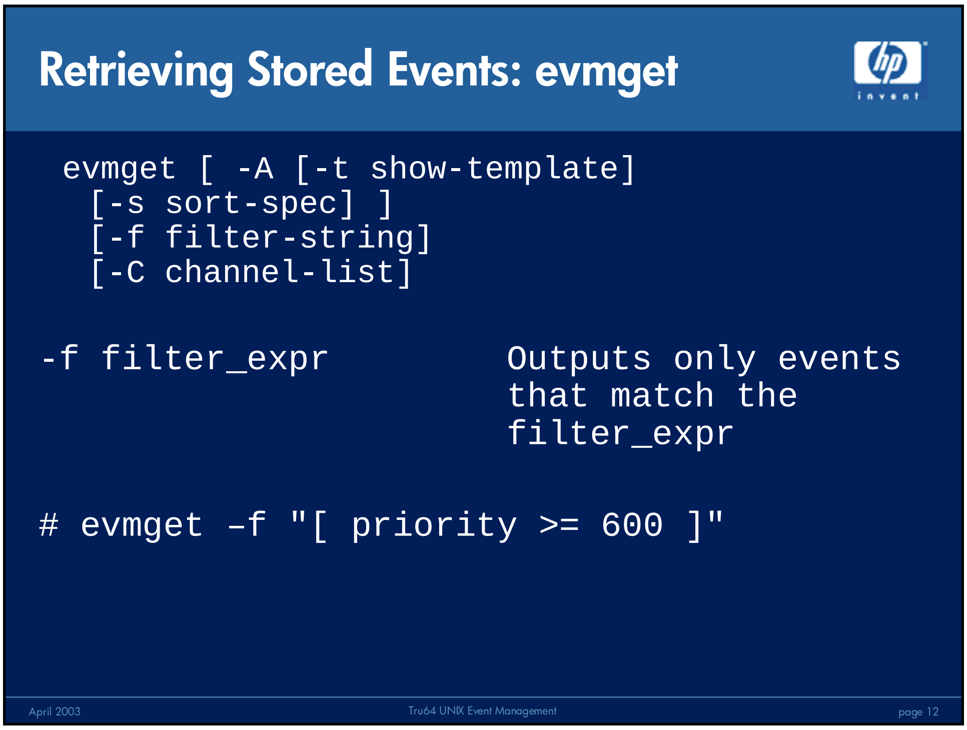


EVM Command-Line Utilities

• 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
```

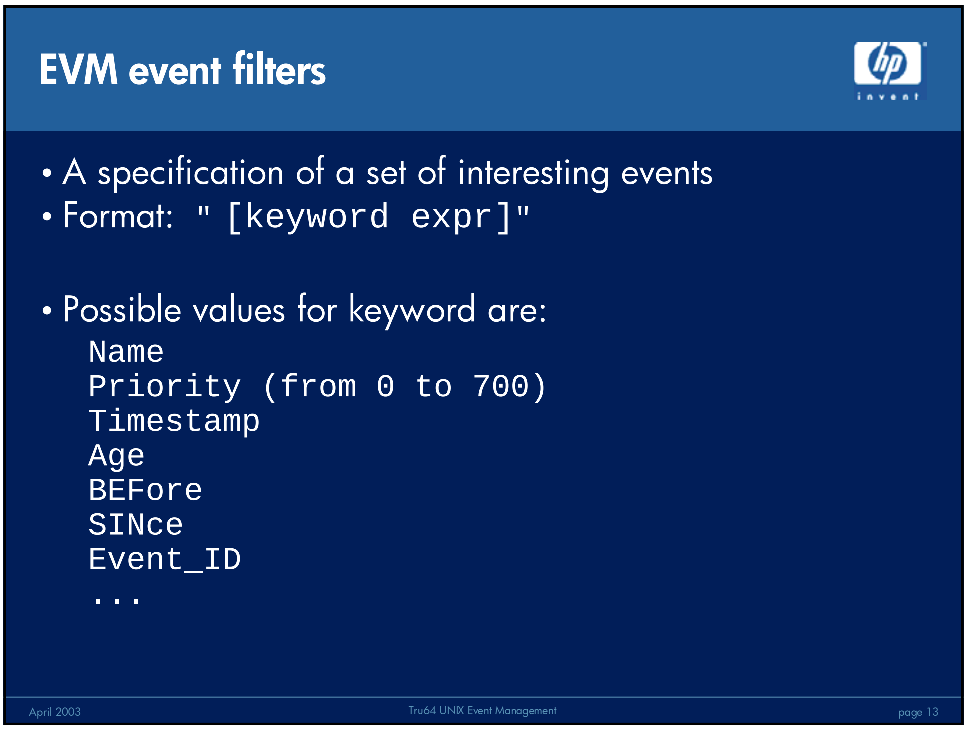


Retrieving Stored Events: evmget

```
 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 ]"
```

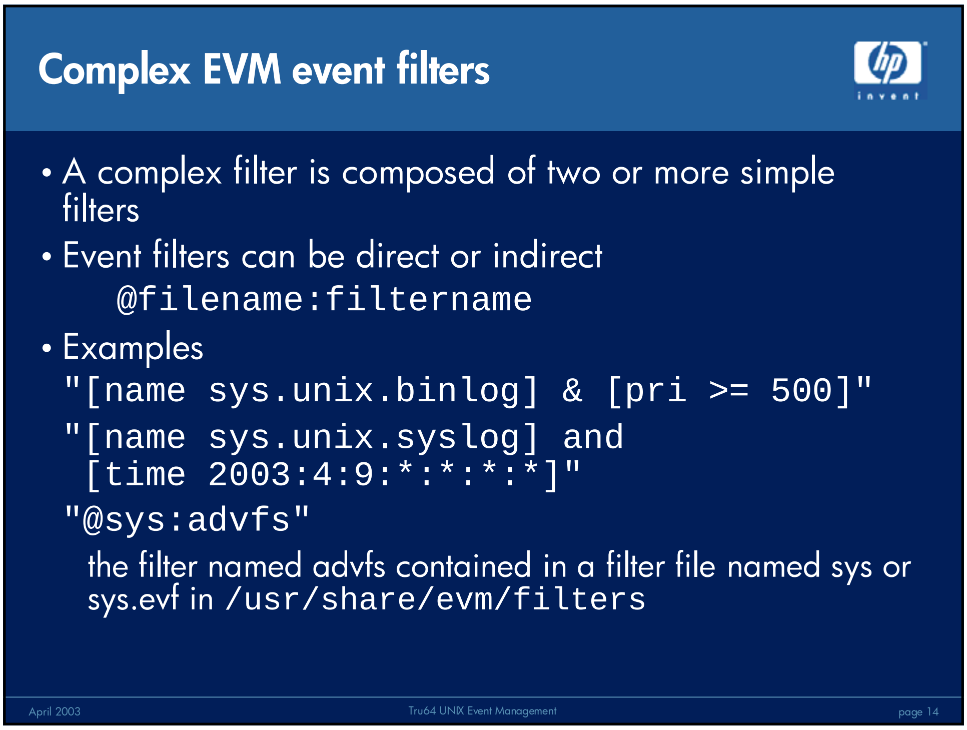


EVM event filters

- 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

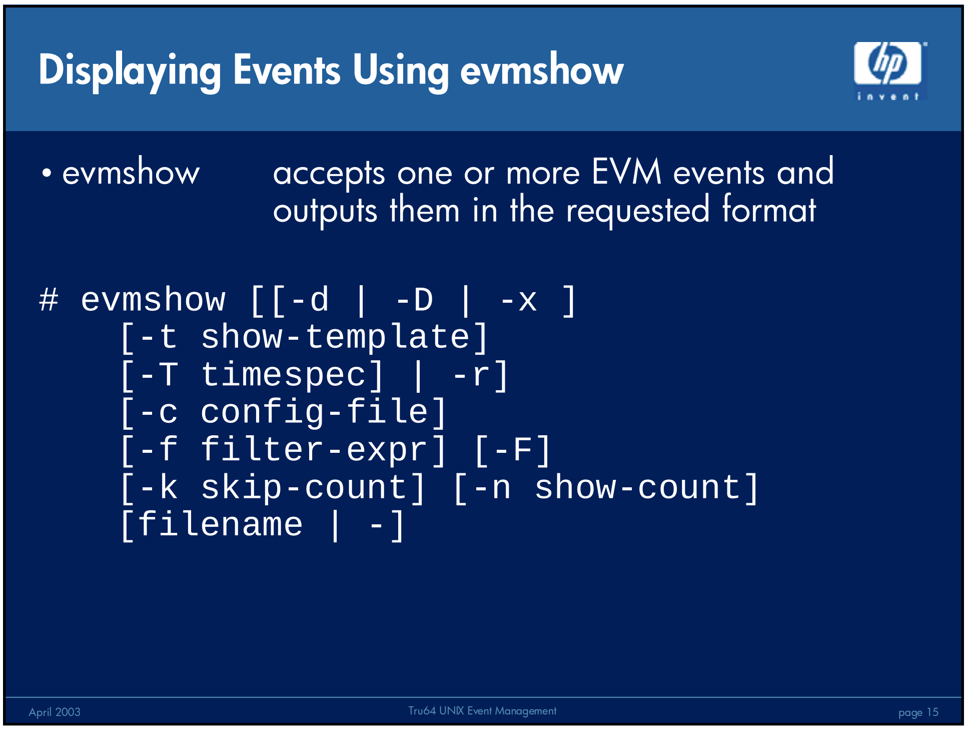
- A complex filter is composed of two or more simple filters
- Event filters can be direct or indirect

```
  @filename:filtername
```

- Examples

```
"[name sys.unix.binlog] & [pri >= 500]"
"[name sys.unix.syslog] and
 [time 2003:4:9:*:*:*:*]"
"@sys:advfs"
```

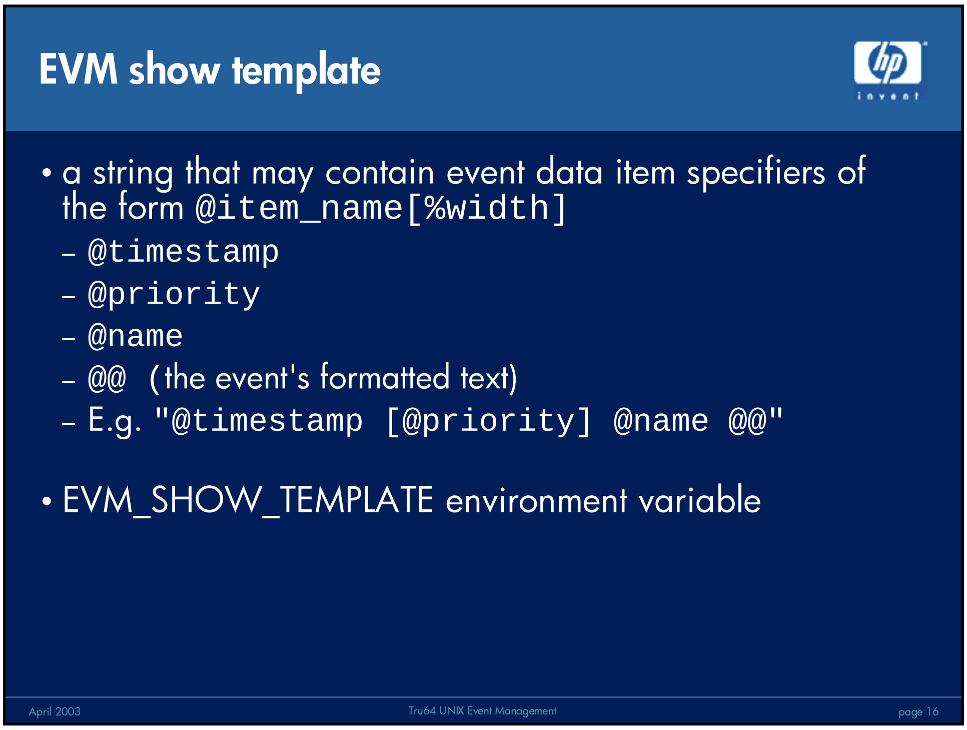
  the filter named advfs contained in a filter file named sys or sys.evf in `/usr/share/evm/filters`



Displaying Events Using evmshow

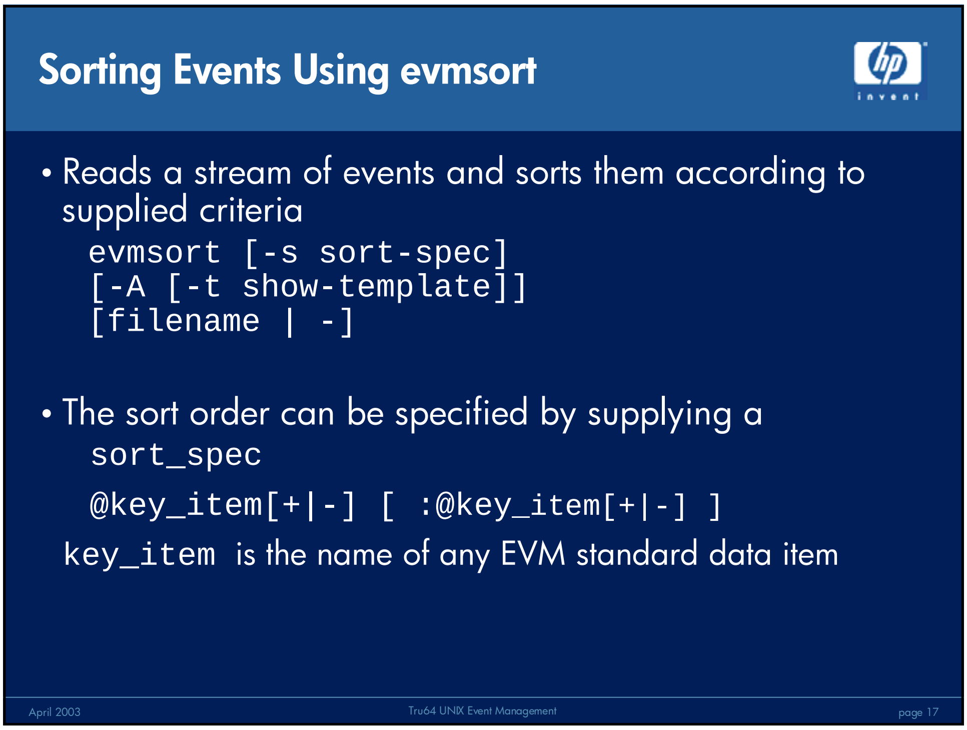
- evmshow accepts one or more EVM events and outputs them in the requested format

```
# 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

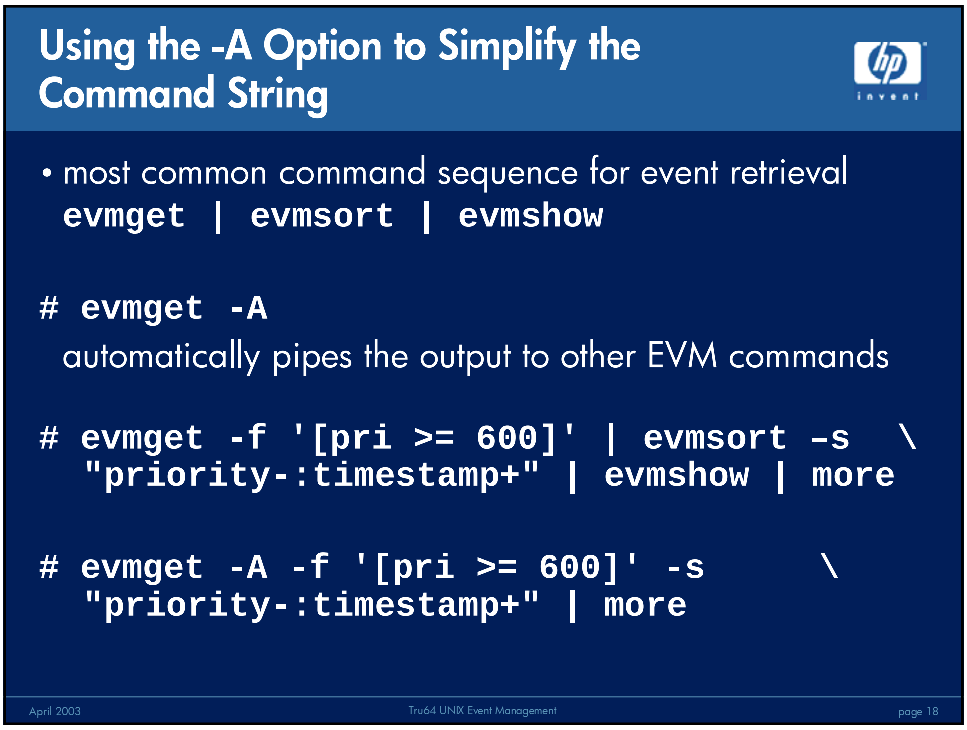
- Reads a stream of events and sorts them according to supplied criteria

```
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

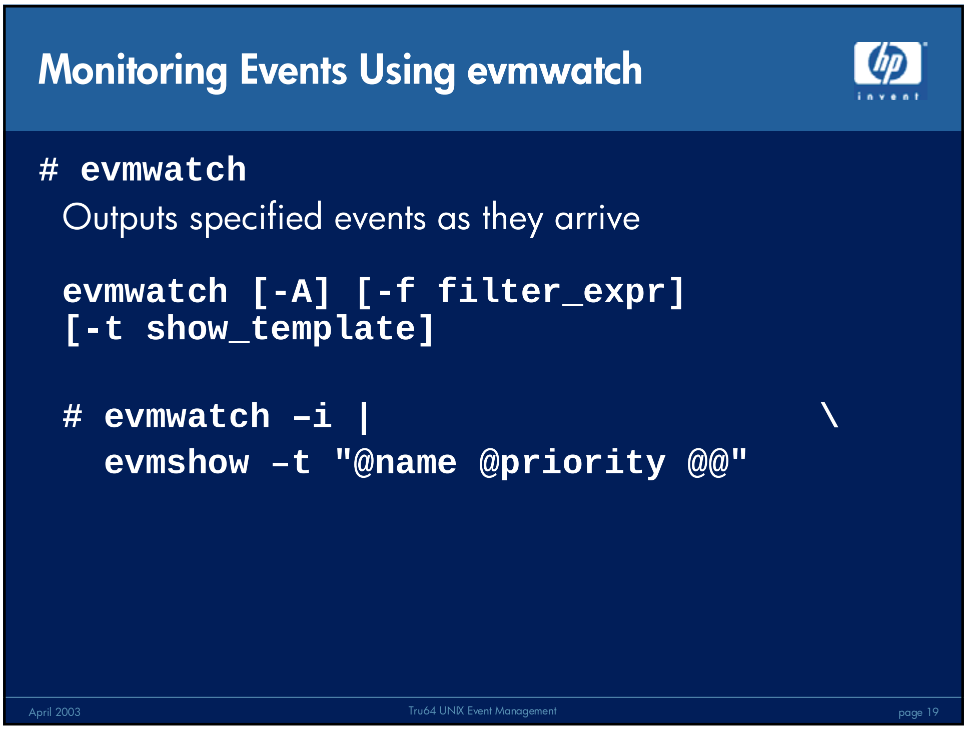
evmget | evmsort | evmshow

```
# 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
```



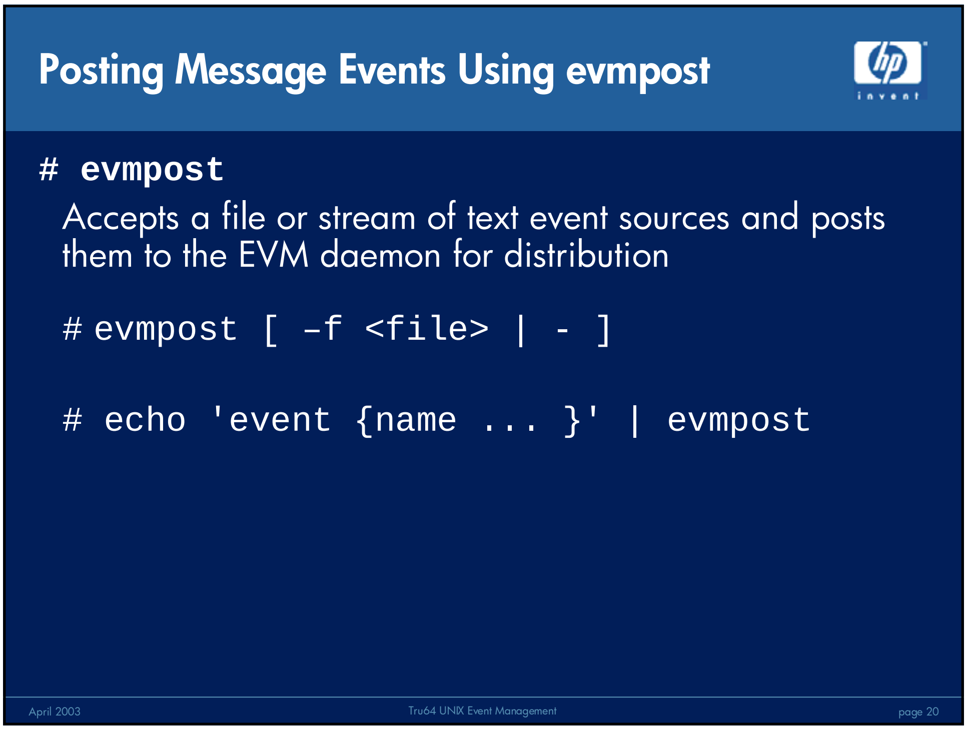
Monitoring Events Using evmwatch

```
# evmwatch
```

Outputs specified events as they arrive

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

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



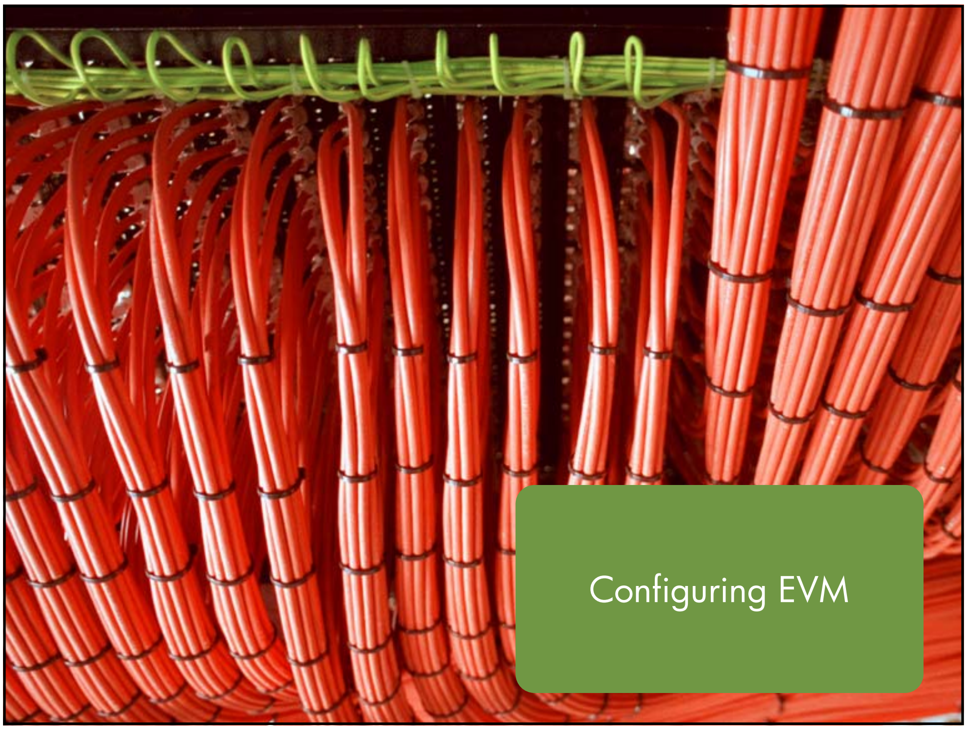
Posting Message Events Using evmpost

```
# evmpost
```

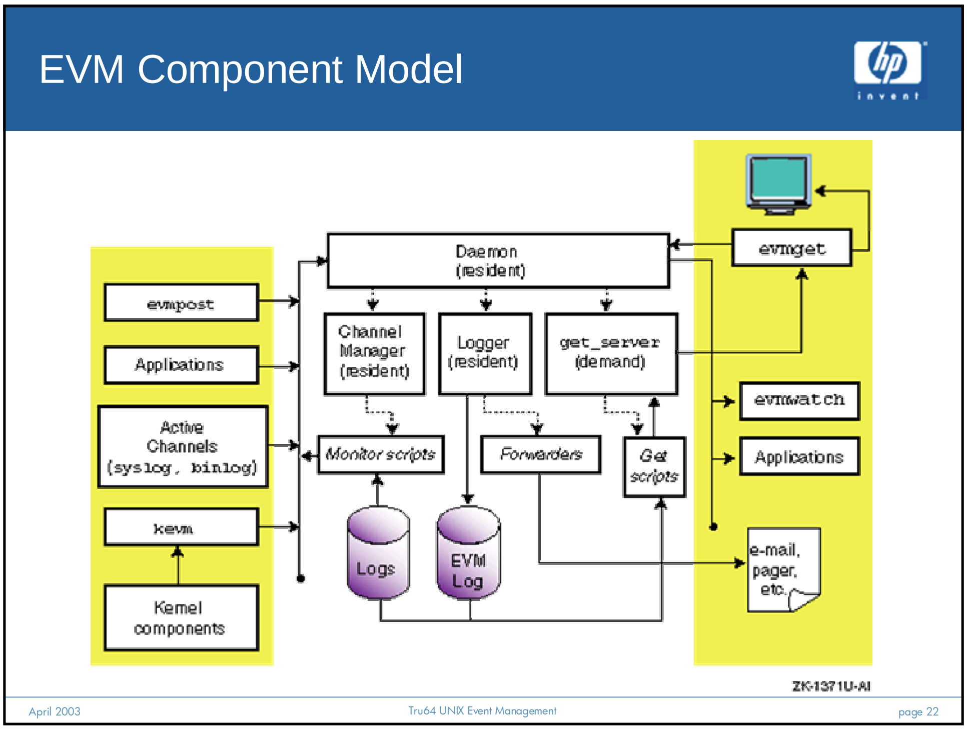
Accepts a file or stream of text event sources and posts them to the EVM daemon for distribution

```
# evmpost [ –f <file> | - ]

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

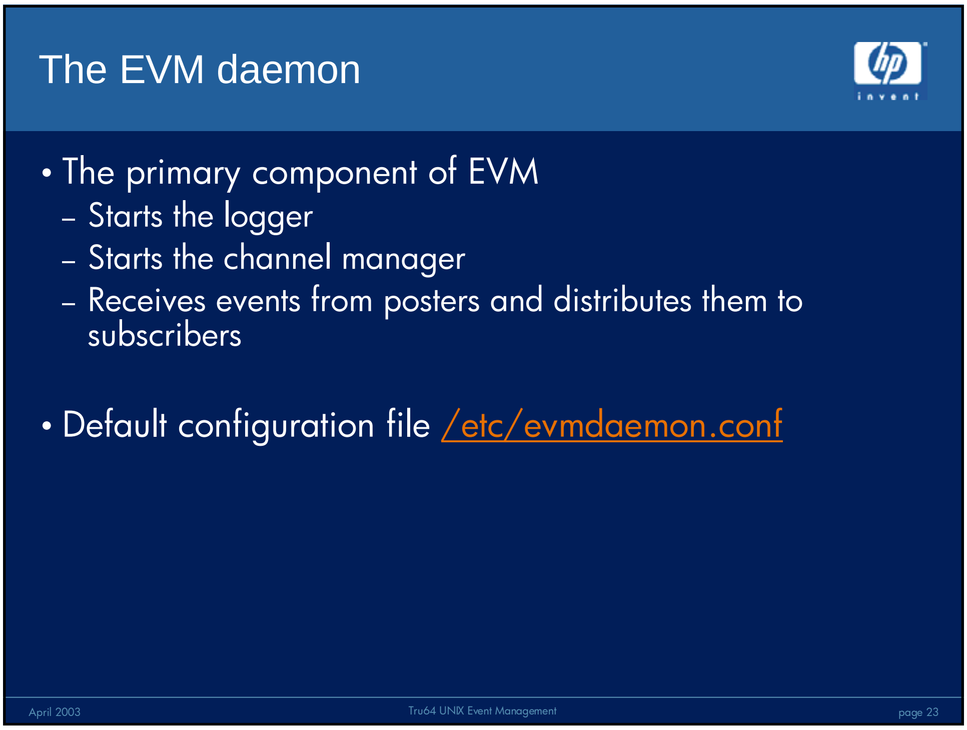


Configuring EVM



EVM Component Model

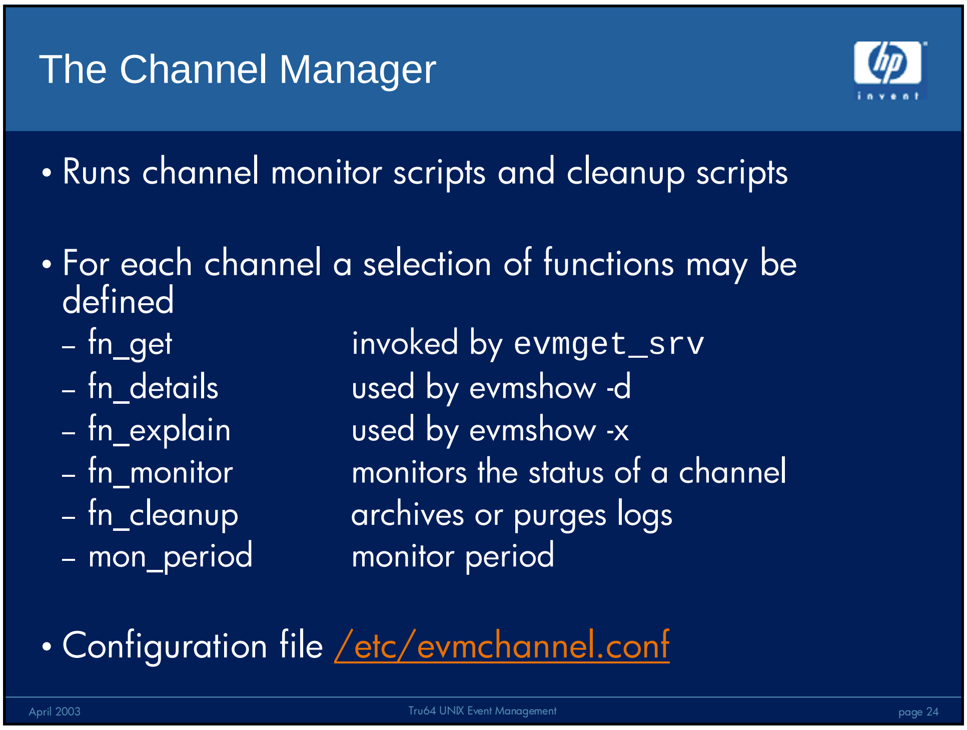
April 2003 Tru64 UNIX Event Management page 22



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

April 2003 Tru64 UNIX Event Management page 23



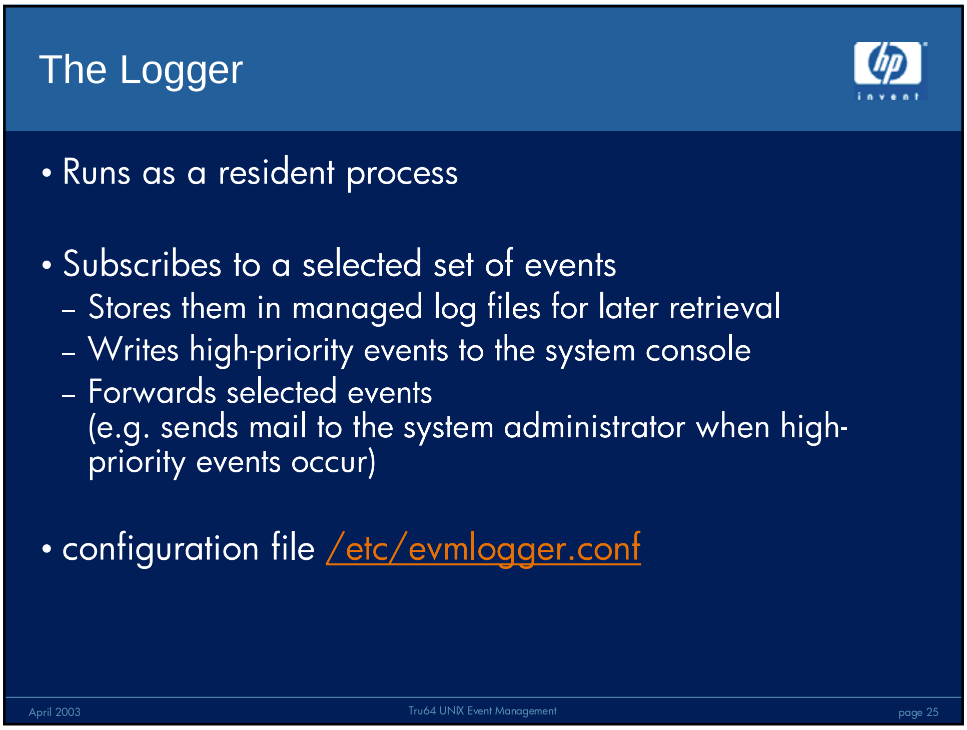
The Channel Manager

- 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

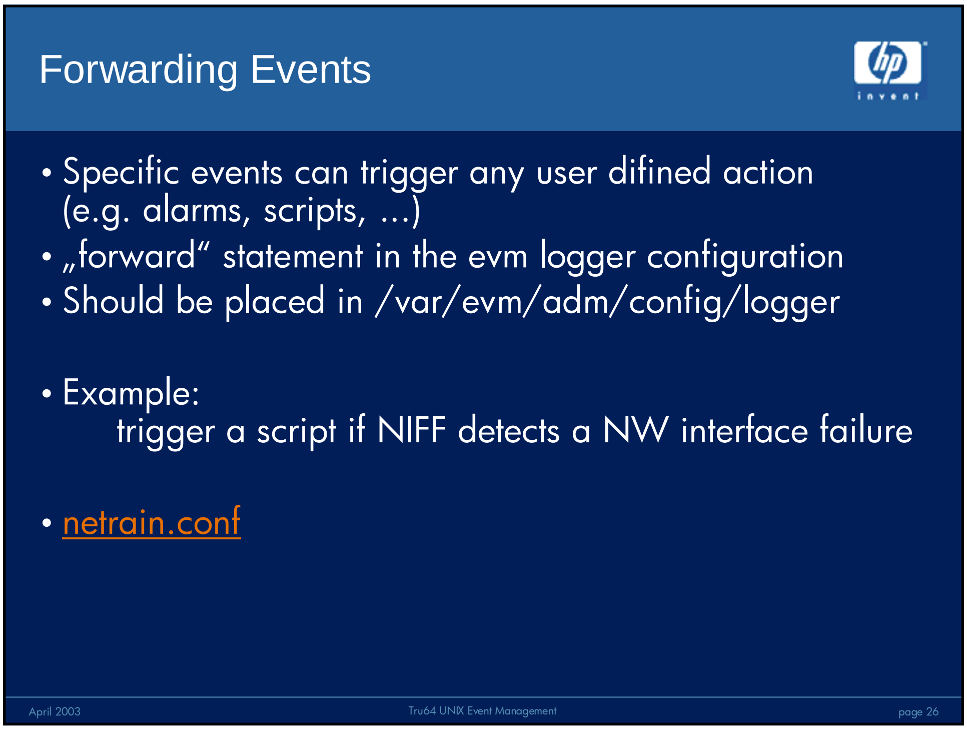
- Configuration file /etc/evmchannel.conf

April 2003 Tru64 UNIX Event Management page 24



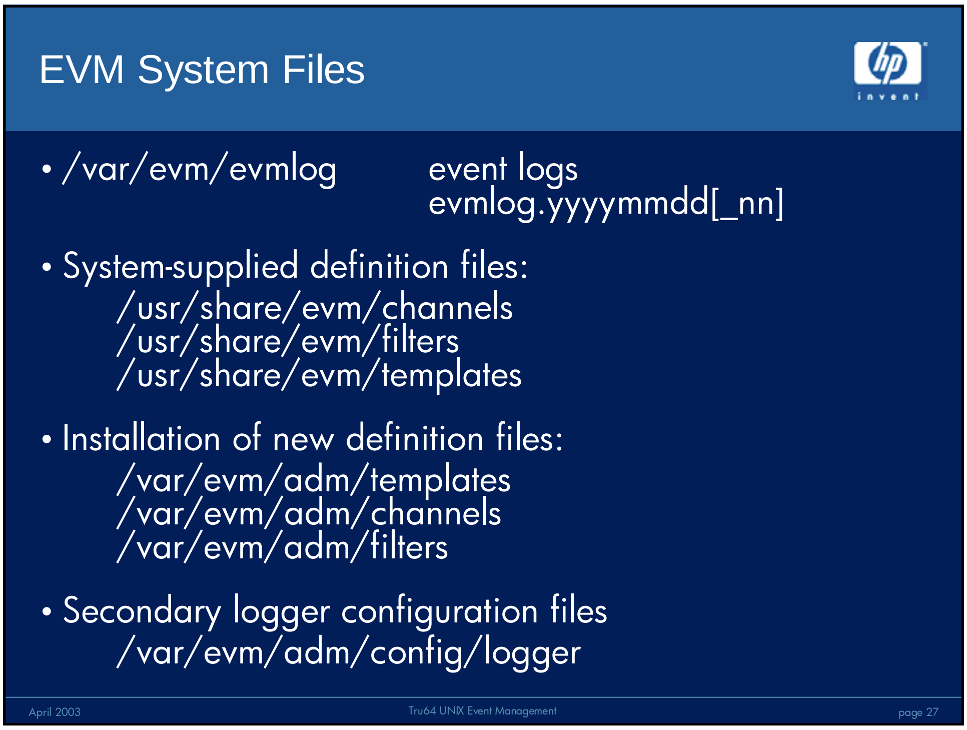
The Logger

- 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

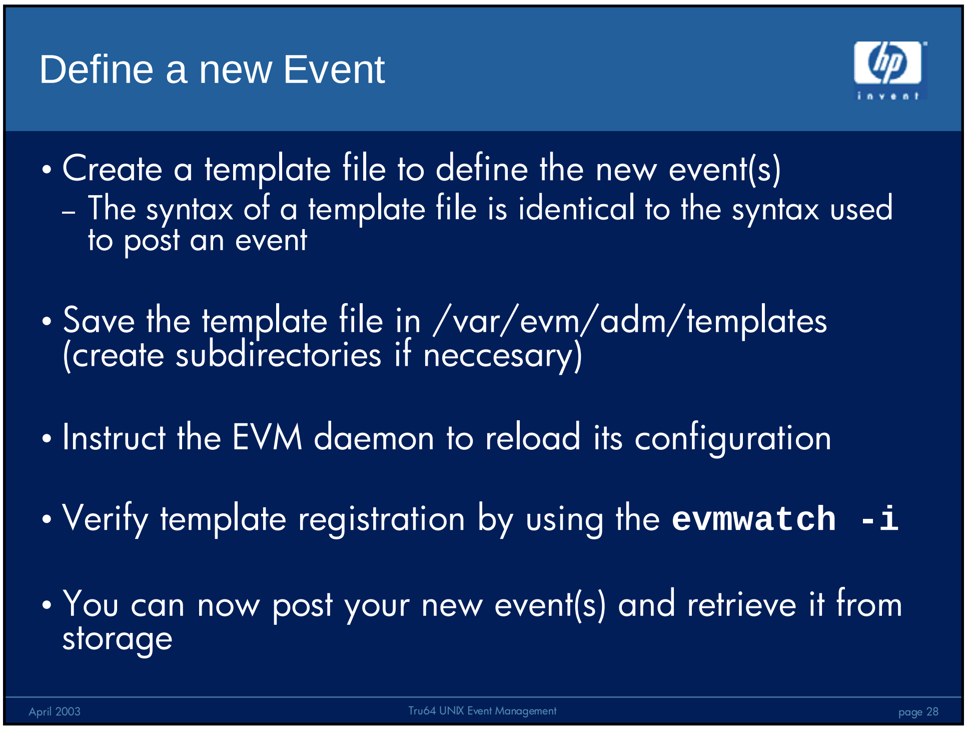
- Specific events can trigger any user difined action (e.g. alarms, scripts, ...)
- „forward“ statement in the evm logger configuration
- Should be placed in /var/evm/adm/config/logger
- Example:
  trigger a script if NIFF detects a NW interface failure
- netrain.conf



EVM System Files

- /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

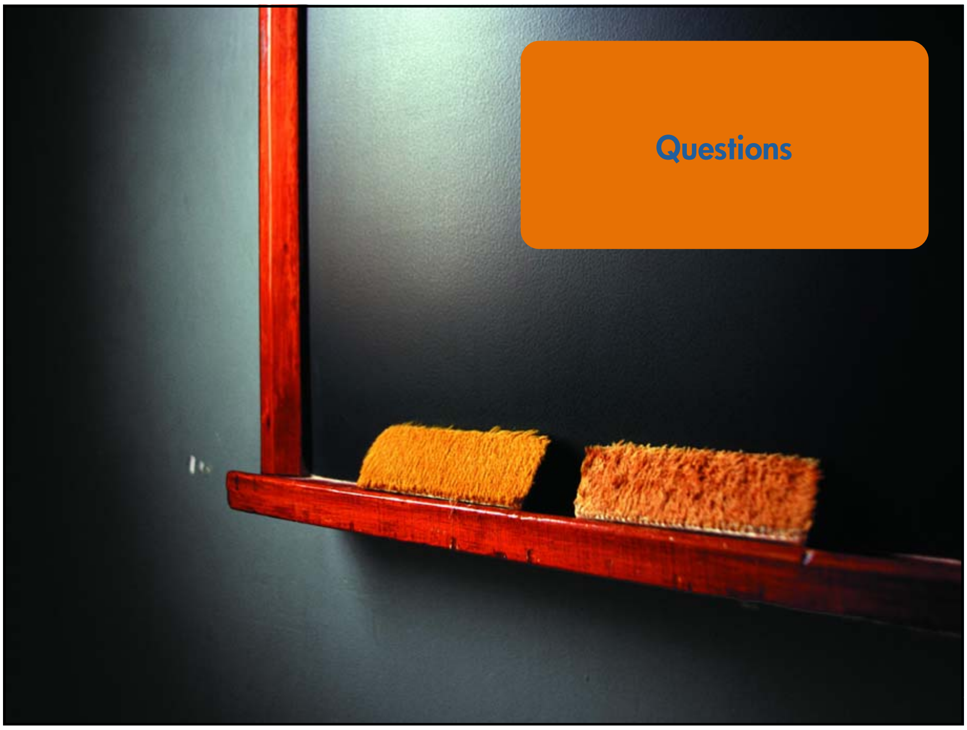
April 2003 Tru64 UNIX Event Management page 27



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 neccesary)
- 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

April 2003 Tru64 UNIX Event Management page 28



Questions

hp

invent