NAME

sadmind – distributed system administration daemon

SYNOPSIS

sadmind [–**c** *keywords*] [–**i** *secs*] [–**l** [*logfile*]] [–**O** *OW_path_name*] [–**S** *security_level*] [–**v**]

AVAILABILITY

SUNWadmfw

DESCRIPTION

sadmind is the daemon used by **Solstice AdminSuite** applications to perform distributed system administration operations.

The **sadmind** daemon is started automatically by the **inetd** daemon whenever a request to invoke an operation is received. The **sadmind** daemon process continues to run for 15 minutes after the last request is completed, unless a different idle-time is specified with the –**i** command line option. The **sadmind** daemon may be started independently from the command line, for example, at system boot time. In this case, the –**i** option has no effect; **sadmind** continues to run, even if there are no active requests.

The **sadmind** daemon process can be configured to write tracing information into a log file by specifying the –**c** and –**l** command line options. The –**c** option specifies a comma-separated list of keywords indicating the types of information to be logged. The following keywords may be useful to you as an administrator:

System-Info Includes messages about when the **sadmind** daemon was started and stopped.

Requests Includes messages about which operations **sadmind** invoked and when.

Errors Includes messages about errors that occurred during the daemon execution.

* Includes all possible log messages.

The –**l** option enables logging and optionally specifies the path and file name of the log file. If no log file is specified, the default log file **/var/adm/admin.log** is used.

OPTIONS

The following command line options may be useful to you as an administrator when starting the **sadmind** daemon:

–**c** *keywords* Specify the types of information to be logged as a comma-separated list of keywords. The default is to log all types of messages.

–**i** *secs* Specify the number of seconds for **sadmind** to stay up after the last request is completed. The default is 15 minutes (900 seconds). If *secs* is 0 or over 10,000,000, **sadmind** stays up forever. –**i** only applies when **sadmind** is started by the **inetd** daemon. You may want **sadmind** to run permanently (or for extended durations) on systems that are frequently administered by applications using **sadmind** (for example, a server managed through **Host Manager**) to improve application performance.

–l[*logfile*] Enable logging and optionally define the path name to the distributed system administration log file. The default log file is:
/var/adm/admin.log

–O *OW_path_name* Define the path name to the OpenWindows home directory. If this option is not specified, the **sadmind** daemon will use the OpenWindows home directory defined in the **OPENWINHOME** environment variable, if defined; the home directory specified in the **/etc/OPENWINHOME** file, if it exists; or the default directory **/usr/openwin**. When the **sadmind** daemon is started by the **inetd** daemon, the environment variable **OPENWINHOME** is typically not defined. If the OpenWindows home directory is not one of the path names specified (**/usr/openwin** or in the file **/etc/OPENWINHOME**), the –**O** option must be added to the **sadmind** entry in the **inetd.conf**(4) configuration file.

–S *security_level* Define the level of security to be used by the **sadmind** daemon when checking a client's right to perform an operation on the server system. Security level specifies the authentication mechanism used to provide and check the client's identity. The client's identity must be authenticated by the specified mechanism for **sadmind** to accept his or her request. The system-wide authentication requirements set by the security level may take precedence over any operation-specific requirements. Consequently, the security level can be used system-wide to ensure that all operations meet minimum authentication requirements, regardless of the requirements assigned specifically to an operation. In addition, the security level determines whether **sadmind** will perform authorization access control checking.

Security level may be one of the following:

0 Set authentication type to **NONE**. All clients' user and group identities are set to the **nobody** identity by **sadmind** (see *Solstice AdminSuite 2.1 User's Guide*). If access is granted to **nobody**, **sadmind** executes the operation. Use this level only for testing.

1 Set authentication type to **WEAK**. Clients' user and group identities are set by **sadmind** from their authentication credentials. Client identities are accepted by **sadmind** when they have satisfied either **AUTH_SYS** or **AUTH_DES** authentication mechanisms. The authenticated client identity is checked by **sadmind** for authorization to execute the operation. If an operation calls for a stronger security level, **sadmind** demotes the user identity to **nobody**, and then checks whether **nobody** is authorized to execute the operation. Since **AUTH_SYS** client credentials are easily forged, this level should be used only in relatively secure environments. No check is done that the user ID of the client represents the same user on the server system as on the client system. It is assumed that user and group identities are set up consistently on the network. This security level is the default.

2 Set authentication type to **STRONG**. Clients' user and group identities are set by **sadmind** from their authentication credential mappings (effectively, user and group IDs from **netid.byname** for **NIS**, or **cred** table for **NIS+**). Client identities are accepted by **sadmind** only when they have satisfied the **AUTH_DES** authentication mechanism. The **sadmind** daemon checks whether the client identity is authorized to execute the operation. This level provides the most secure environment for executing distributed administration operations. It overrides any weaker level specific to an operation. A **DES** credential must exist for the host running the **sadmind** daemon and all administration client user identities.

−v Enable the writing of log messages to the system logger, **syslogd**. Messages logged include fatal errors encountered while attempting to start the **sadmind** daemon process and those specified by the **−c** trace message keywords.

EXAMPLES

By default, the line in **/etc/inetd.conf** that starts **sadmind** appears as follows:

100232/10 tli rpc/udp wait root /usr/sbin/sadmind sadmind

To make a network as secure as possible, change the line to:

100232/10 tli rpc/udp wait root /usr/sbin/sadmind sadmind −S 2

To minimize delays due to starting up **sadmind**, change the line to include the **−i** option:

100232/10 tli rpc/udp wait root /usr/sbin/sadmind sadmind −i 86400

In this example, the duration that **sadmind** remains up after the last operation request was completed is extended to 24 hours (86,400 seconds). Extending the timeout period may enhance performance on servers and workstations that frequently run or are administered by applications that use the **sadmind** daemon (for example, **Solstice AdminSuite** applications such as **Host Manager**).

FILES

/var/adm/admin.log distributed system administration default log file
/etc/inetd.conf internet servers database file

SEE ALSO

inetd(1M), **rpcbind**(1M), **inetd.conf**(4)

Solstice AdminSuite 2.1 User's Guide

NOTES

Whenever **inetd** fails to start **sadmind**, re-register the RPC number for **sadmind**, 100232, with **rpcbind** by sending the **inetd** process a **SIGHUP** signal:

example% kill −HUP *pid*

or

example% kill −1

Sometimes **inetd** does not start **sadmind** in response to system administration requests, even though the **inetd.conf** file has the correct entry for the **sadmind** daemon. This can happen when **sadmind** is started manually from the command line and takes over the previous registration of the **sadmind** RPC number, 100232, by **inetd**. When the manually-started **sadmind** daemon is terminated, the **sadmind** RPC number, 100232, is de-registered with **rpcbind**. Consequently, system administration requests are ignored by **inetd**.