

Component Summary

AdminUX offers a wide array of task specific components in one comprehensive package. Each component is responsible for a specific area of system security or automation and can report the results of its scans to a central location for monitoring purposes. All components work together to ensure optimal system performance.

ServerGuard – This server-based intrusion detection system monitors your system for security breaches. Whether it's unusual activity on server ports, defaced static web pages, or unauthorized access, ServerGuard is on the job 24 x 7 x 365. A daily security diary is created for quick and easy review of potential security issues.

Failsafe System – The AdminUX Failsafe System creates local archive copies of mission-critical system files. These files are automatically restored if they are moved or deleted. Applications files can be included.

Performance Analyst – Your server's performance is constantly monitored using information derived from Unix SAR reports and other resource monitors. Performance is analyzed using our own unique algorithms. Behavior outside established

parameters will create an alarm event to notify the System Administrator of potential problems.

Resource Risk Forecaster (RRF) – Automatically analyzes collected data and provides a long-range forecast on the risk of exhausting a system resource (filesystem space or swap space). RRF provides the hard data managers need to plan for the upgrades necessary to keep your operations smooth and your business competitive in the market place.

Intellipublish™ – A designated “publish” server can advertise AdminUX updates to other registered AdminUX servers. Each registered server acknowledges if it requires the update, pulls it from the publish server, and automatically installs it during normal processing. Intellipublish enables you to upgrade AdminUX across your network with a single download.

Process Manager – AdminUX monitors server process daemons 24 x 7 to ensure proper system operation. Failed process daemons can be automatically restarted. Runaway and orphaned processes are also monitored and can be “killed” by the Process Manager when authorized to do so.

Component Summary

Policy Distribution Manager (PDM)

The PDM allows the user to setup and maintain an entity called "Workgroup" which is a logical collection of other hosts running AdminUX. Once you have selected a Workgroup, any policy change to a matrix on the local host can be automatically distributed to all AdminUX hosts in the selected workgroup.

Remote Server Synchronous Shutdown (RSSS) – Very useful in large environments, this component enables an Administrator to shut down multiple occurrences of an operating system across a network securely using one shutdown command.

Application Event Interface – AdminUX monitors application logs for significant events. This interface can also be configured to create customized alarm events based on application behavior. This feature enables you to use AdminUX as your single event notification system.

Event Logger – All significant server events are logged in AdminUX's extensive logging system. Log information is useful for trend and performance analysis. Vital system information contained in the logs can be maintained for up to a year. Forensic information maintained in AdminUX logs can be used to

determine the root cause of system problems or failures.

Log Synchronizer – AdminUX logs can be copied securely from many AdminUX-managed servers to a consolidated log server. This allows an administrator to troubleshoot a system even if it isn't currently on-line.

Logs Manager – This component, which must be licensed to operate, is designed to create a centralized log archive. Not to be confused with the Log Synchronizer, which is designed specifically to archive AdminUX logs, the Logs Manager can archive thousands of files to one or more central storage systems regardless of how the file was created.

File Examiner – Routine "housekeeping" tasks like garbage file or core dump removal are performed by this component.

Network Examiner – AdminUX will "ping" designated devices and check the status of local interfaces including their collision rates and packet errors. Device behavior outside established parameters triggers a network event alarm.

Component Summary

DataArchiver – Using GNU tools provided in the AdminUX distribution, you may backup data using nine different backup queues can be processed to as many as nine different devices either in serial or parallel. Data can be sent from any AdminUX managed server to the AdminUX server running the DataArchiver across your intranet or the Internet.

Alert Delivery Manager – AdminUX generates alarms and sends user notifications when the server's system administration policies are violated. Alarms are sent via email, digital page, fax, or any other method that provides a command line interface.

AdminUX Control Panel (ACP) – AdminUX is designed to allow configuration and operation from a command line prompt. This is ideal for systems that may only provide telnet access. Where a Graphical User Interface (GUI) is preferred, the ACP is a self-contained Tcl/Tk application that operates under any X-window session to provide a point-and-click tree-based menu for modifying AdminUX's default policies.

Alarms Monitor Console (AMC) – Using any standards-compliant browser, the AMC monitors system alarms for any number of AdminUX-managed servers from any location.

PHP server-side scripting makes it useful where corporate security policy restricts Java script or Active-X controls. The color-coded display follows industry standards for alarm severity.

Enterprise Management Console (EMC) Option – AdminUX can integrate with major enterprise management systems like OpenView, Tivoli®, and UniCenter®. Using standard SNMP interfaces, AdminUX can send its alarm event information to the centralized management consoles provided by these popular network management systems.

User Manager – Once AdminUX is installed on your system, user administration may be done through AdminUX in order to take advantage of features such as time zone setting, login restrictions, birthdays, or the ease of use of the menu for performing user administration tasks.