

ANCHOR COMPLETE SUPPORT PACK TECHNICAL SPECIFICATION

This document defines exactly what is and is not included in this support pack. An overview of the areas of support provided and technique used is presented followed by a detailed schedule of scope and definitions.

THE GOAL OF ANCHOR COMPLETE

The goal of Anchor Complete support pack is to allow Anchor to take control of your server and manage at a very high level, every aspect including the hardware, operating systems and applications. It encompasses a wide range of different preventative maintenance and ongoing support activities geared towards maximising the availability of hosted services.

AVAILABILITY MONITORING

A centralised monitoring system automatically checks to see if the nominated services are responding within a designated time. A failure to respond due to either the performance of the application or the availability will trigger an alert.

Alerts are delivered to technical staff both via audible and visual alarms in the NOC and SMS notification when they are offsite.

Any change of state of any service is logged. Historic reports can be generated to show exactly when the availability of a service or server has changed and the total amount of down that has occurred against any service.

Availability monitoring is performed at three levels:

- Network connection monitoring,
- Application layer monitoring via network
- Application layer monitoring via a local reporting agent.

The information available at each level varies respectively. A breakdown of monitoring points is provided in the schedule.

TREND ANALYSIS

Performance related data points are logged on your server. Time series graphs (MRTG style) are generated from this data. Anchor can view data across a rolling 12 month period. Most recent periods contain detailed reports with data averaging occurring increasingly over time.

Trend analysis reports are used to assist with diagnosis of problems and identification of most appropriate upgrade points to resolve performance bottlenecks.

HOST INTEGRITY MONITORING

Osiris is a Host Integrity Monitoring System that periodically monitors servers for change. It maintains detailed logs of changes to the file system, user and group lists, resident kernel modules, and more.

Osiris keeps Anchor apprised of possible attacks and/or nasty little trojans. The purpose here is to isolate changes that indicate a break-in or a compromised system

All changes are investigated by hand (on business days).

If changes are expected, the change log is approved and the current state is accepted and used as the baseline for the next scan.

PATCHING AND UPDATES

Anchor monitors the patches and updates released by the operating system vendor for the supported applications.

The most recent vendor supplied security patches are applied as soon as practical. Application of patches may be delayed where the application of the update has the capacity to interfere with business requirements.

FAULT RECTIFICATION

If any of the monitored services fail, multiple Anchor staff are notified immediately by Email, Instant messaging, and SMS. Notifications continue and are escalated until the problem is acknowledged and fixed.

All problems are also analysed to not only restore the service to but to find the root cause of the failure and prevent re-occurrence.

MANAGED HARDWARE

In the event that monitoring systems detect a disruption to service which Anchor investigates and finds to be a hardware fault, Anchor will replace the failed components.



A full inventory of spare components is maintained onsite to permit rapid replacement of failed components.

CONFIGURATION MANAGEMENT

Anchor complete covers a certain level of configuration and security management of your server.

Configuration management covers only supported applications (as noted in the schedule).

Control of the critical applications on your server are performed via centralised configuration management service (cfengine). This service permits inclusion of all changes in a revision control system and permits automation of many common functions. The fine grained control over configuration results in increased stability, reliability and accountability.

Root level access cannot be provided on systems configured with cfengine due to the conflicts caused by direct local modifications. Limited sudo access may be provided in specific cases.

SUPPORTED APPLICATIONS

The services described under the Anchor Complete support pack in respect to installation, configuration, patching, updating and fault rectification are limited to the list of supported applications provided in the schedule below.

Different levels of application support at the installation, configuration and update points are provided as noted in the schedule.

It is impossible to provide support to an unrestricted list of applications as part of a standard support plan. The applications supported represent the overwhelming majority of those which are commonly used for Internet facing applications.

Support of most other applications can be provided under Anchor Custom Support.

SUPPORT SYSTEMS

During business hours (8am to 6pm) support is provided via telephone and email. All email requests are tracked via an automated ticketing system to ensure appropriate escalation and response.

All requests and changes are documented internally by Anchor.

After hours emergency support is provided 24 x 7 via telephone only. Support after hours is provided for the purpose of resolving problems which cause outages, it is not provided for general configuration changes, provisioning or advice.

Support may be further limited in scope where client side development activities result in recurring failure of supported services.

SCHEDULE OF ANCHOR COMPLETE SUPPORT SCOPE AND DEFINITIONS

Server hardware	
Component testing	Memory is tested for 48 hours using Memtest before deployment. Chassis (including motherboard, I/O controllers), CPU and disc drives are tested for 5 days using the Cerberus Test Control System before deployment.
Spares inventory	An inventory of spare components of same or compatible specification is maintained onsite for all deployed servers.
Operating Systems supported	
Linux	Red Hat Enterprise Linux
Windows	Windows Server 2003 Web edition, STD, Enterprise Edition
Software installation support	
Operating system supplied packages	Installed by Anchor as requested by the client.
Third party packaged applications supported by Anchor:	JBoss, Sun JRE, Zope, Pylons, DRDB, Horde Webmail, MDAemon, Ruby on Rails
Third party non-packaged applications	Provided under Anchor Custom Support.
Software upgrade support	
Operating system supplied packages	Upgraded by Anchor. Resolution of significant impacts resulting from upgrades treated as Anchor Custom Support.
Third party packaged applications supported by Anchor:	JBoss, Sun JRE, Zope, Pylons, DRDB, Horde Webmail, MDAemon
Third party non-packaged applications	Provided under Anchor Custom Support.
Application configuration support	
Web servers	Apache, IIS, Mongrel, Lighttpd
Mail servers	Sendmail, Postfix, IIS
Database servers	MySQL, PostgreSQL, MS SQL 2000/05
FTP	VsFTPD, ProFTP, IIS
SSH	OpenSSH
Application servers	Tomcat,
DNS	Bind
Misc	SVN, CVS, Squid, Terminal services
Monitoring	
Trend Analysis monitoring	Disk I/O activity, load, CPU usage, memory usage, disc space usage, logged in users, number of running processes, network interface traffic
Availability: Network checks	Ping, Terminal services
Availability: Application layer network checks	SSH, HTTP, DNS, POP3, IMAP, NTP, FTP, SMTP, Individual websites, up to 5 other network facing applications as noted by the client.
Availability: Local agent checks	Postfix mail queue size, NRPE daemon, disk space, Postgresql, MySQL, load, Tomcat(4/5), kernel version, firewall status, swap, MSSQL, RAID status, HTTP current connection count.
Host Integrity Monitoring	The following directories are scanned for changes: /bin, /sbin, /boot, /usr, /lib, /lib64
	Note: Monitoring of some services are specific to the operating system. Actual services monitored varies accordingly.
Fault rectification	
Restarting failed services	Response provided to monitored and supported applications
Reconfiguration of failed services	Analysis and rectification provided by Anchor. Included in scope of support unless repetitive unresolved faults are found to be directly resulting from client actions.

Configuration management	
Centralised configuration management (cfengine)	Cfengine controls aspects of the following: Amanda backup client, Apache configuration, logging, website statistics, SSL certificates and passphrase support, APT/up2date/yum, arptables, BIND nameservers, payment gateways, /etc/fstab, Horde webmail system, /etc/inittab configuration for mgetty, Common system binary symbolic links, LDAP client/server configuration, Killing off and disabling unnecessary daemons, Dovecot/imapd/pop3d, Filtergen, Tomcat/jpackage, Mailman, Mysql, PostgreSQL, Postfix, Vsftpd, General system security, PAM, tcpwrappers control, SNMP and SSHD. Cfengine is not used on Windows systems.
Security management	Firewall management, host access control, authorisation control, disabling of unneeded services, security hardening, user/group management.
Performance management	
Application performance research and analysis	Provided under Anchor Custom Support.
Client requested application performance changes	Specific application configuration changes made where exact settings advised client only.
Diagnosis of hardware limitations	Analysis is carried out as requested to identify which components of the server hardware in terms of processor, memory or discs (I/O) may be limiting the performance of the hosted applications. Recommended changes are provided at the conclusion.
Limits on configuration requests	
Total configuration time per month	In addition to all of the preventative maintenance and monitoring activities each month, an allowance of 3 hours is made for configuration change requests. Requests exceeding this time period may be billed as Anchor Custom Support.
Patching and updates	
Software updates	Critical security updates to critical applications are applied outside of business hours. Target time for application is 24 hours from receipt. Critical and non-critical security updates to non-critical applications are applied during business hours as soon as possible. Target time for application is 24 hours from receipt. Critical applications are those deemed as having a high level of dependence on the end user application or where the risk of service instability resulting from the application of the update is high.
Kernel updates	Kernel updates are scheduled to occur with advance notification outside of business hours. Target time for application is 3-7 days from receipt. Windows updates generally require a full system reboot and are treated as kernel updates.
Migration	
Migration of services/data from/to external hosts, data between different application, versions or platforms or formats.	Provided under Anchor Custom Support