ИНТЕРНЕТ РЕДАКЦИЯ рекомендаций по организации технического обслуживания ТИКСЕР БЕССТ v.4.x

Введение

Настоящая ИНТЕРНЕТ РЕДАКЦИЯ рекомендаций по организации технического обслуживания ТИКСЕР БЕССТ v.4.x описывает процесс установки и конфигурирования "типового коммуникационного сервера Белонина Сергея Станиславовича" и операционной системы CentOS, под управлением которой он должен функционировать

Настоящая ИНТЕРНЕТ РЕДАКЦИЯ рекомендаций по организации технического обслуживания ТИКСЕР БЕССТ v.4.x предназначена для ознакомления посетителя сайта с возможностями, заложенными в «Типовом коммуникационном сервере Белонина Сергея Станиславовича, версия 4.x»

Условия распространения

Отказ от ответственности

Внимание !!! Ниже в настоящем разделе дублируются основные пункты отказа от ответственности из лицензионного договора

Правообладатель не берет на себя никаких обязательств (в том числе не берет на себя обязательства по обеспечению пригодности данных материалов для каких либо целей, по соответствию настоящих материалов пользовательским ожиданиям, по обеспечению правдивости и непротиворечивости настоящих материалов), также автор не несет никакой ответственности, связанной с настоящими материалами

Использующий настоящие материалы принимает на себя всю ответственность за использование или неиспользование настоящих материалов полностью или в любой их части, а также за результаты использования или неиспользования настоящих материалов полностью или в любой их части, включая любые непосредственные и любые опосредованные результаты, в том числе упущенную, недополученную прибыль, вред имиджу или деловой репутации

Использующий настоящие материалы соглашается, что не имеет и не будет иметь в будущем никаких претензий к автору настоящих материалов, связанных условиями распространения или содержимым настоящих материалов

ВНИМАНИЕ !!! В случае непринятия настоящих условий во всех деталях использовать настоящие материалы запрещается

рекомендации по организации технического обслуживания ТИКСЕР БЕССТ v.4.x

Ниже приводятся рекомендации по организации коммерческого технического обслуживания типовых коммуникационных серверов ТИКСЕР БЕССТ v.4.x у клиентов. Конечное же решение о предоставляемом клиенту пакете сервисов поставщик принимает самостоятельно

В регламент техобслуживания рекомендуется включать следующие мероприятия:

- контроль доступности по сети, контроль DNS сервера
- контроль свободного места (утилизация и файловые ноды)
- контроль резервного копирования базы, каталога LDAP и конфигурационных областей, а также относ в сторону
- контроль журналов работы операционной системы на предмет перезагрузок, аппаратных ошибок, ошибок в типовых сервисах
- контроль утилизации ресурсов (статистики) ОС на предмет выявления узких мест
- анализ журналов продукта на предмет выявления ошибок
- контроль работоспособности функций продукта (почта, прокси, управление пользователями, управление LDAP, доступность консоли WEB,сетевой фильтр)
- контроль целостности системных областей (перечень файлов, объекты с SUID и SGID, соответствие подписям md5 в пакетах, при наличии - сравнение с md5 и sha1 слепками объектов системных областей, выверка списка пакетов)
- контроль попыток вторжения (анализ отчётов и журналов на предмет подключений на запрещённые порты, попыток подбора паролей)
- опционально - обновление платформы из репозитария

В пакет предоставляемой клиенту по результатам технического обслуживания и анализа работы системы рекомендуется включать следующие отчёты:

- отчёт и рекомендации о проведении технического обслуживания
- отчёт и рекомендации по IP трафику
- отчёт и рекомендации по использованию ресурсов прокси сервера
- отчёт и рекомендации по использованию почтовой системы
- отчет и рекомендации по нарушениям целостности и попыткам вторжения

– отчёт и рекомендации по утилизации ресурсов ОС

Описание процедур технического обслуживания

контроль доступности по сети, контроль DNS сервера

для контроля доступности сервера по сети отработать команды PING

ping любой внутренней машины (с сервера)
ping внешний_IP_адрес_сервера (из Интернет)
ping ns.имя_домена_клиента (из Интернет)
ping mx.имя_домена_клиента (из Интернет)
ping stat.имя_домена_клиента (из Интернет)
ping ns.имя_домена_клиента (с сервера)
ping mx.имя_домена_клиента (с сервера)
ping ldap.имя_домена_клиента (с сервера)
ping proxy.имя_домена_клиента (с сервера)
ping stat.имя_домена_клиента (с сервера)

для контроля корректности функционирования DNS отработать команду NSLOOKUP

nslookup
> ns.имя_домена_клиента (должен быть выведен соответствующий имени внешний IP сервера клиента)
> mx.имя_домена_клиента (должен быть выведен соответствующий имени внешний IP сервера клиента)
> set TYPE=MX
> имя_домена_клиента (должен быть выведен внешний IP сервера клиента как обработчика почты для домена)
> quit

при **запуске с внешней машины** (из Интернет) должен отражаться внешний IP адрес сервера, при **запуске с сервера** или из локальной сети с рабочей станции с корректно сконфигурированным

указателем на сервер DNS должен отображаться внутренний IP адрес сервера

контроль свободного места (утилизация и файловые ноды)

для контроля необходимо на сервере отработать команды DF, отражающие утилизацию ёмкости дисков и утилизацию файловых дескрипторов

df -k
df -i

в случае, если утилизация какого либо из разделов высока, найти наиболее объёмные каталоги и файлы можно командами

cd имя_каталога_для_анализа ; du -sk * | sort -n

которые выведут размер каждого элемента каталога, включая и файлы, и каталоги. При необходимости детализации нужно войти в проблемный каталог и вызвать те же команды

контроль резервного копирования базы

Включённый в состав продукта механизм создания резервных копий реализует резервирование данных базы, каталога LDAP и конфигурационных файлов по установленному списку. Стартовый скрипт расположен по пути /usr/local/cosiculs/sbin/start_backup.sh. Создаваемые резервные копии сохраняются в каталоге /usr/local/cosiculs/backup

Для обеспечения возможности восстановления системы имеет смысл сконфигурировать стартовый скрипт создания резервных копий на периодическое выполнение в планировщике операционной системы. В процессе проведения технического обслуживания необходимо проанализировать журнал планировщика операционной системы и содержимое каталога для хранения резервных копий. Также

полезно вынести копии созданных резервных копий на отдельный от сервера носитель для более надёжного хранения резервных копий

контроль журналов работы операционной системы

В процессе проведения очередного технического обслуживания имеет смысл проанализировать журналы операционной системы, расположенные в каталоге /var/log/ на предмет перезагрузок, аппаратных ошибок, ошибок в типовых сервисах. В случае типовой настройки первой целью является журнал /var/log/messages. Т.к. для предотвращения разрастания журналов может быть использована ротация, может потребоваться проанализировать также ротированные части журналов

контроль утилизации ресурсов ОС

Контроль статистик операционной системы призван в первую очередь ответить на вопрос - хватает ли аппаратных ресурсов, и если не хватает - то чего именно. Другим вопросом является мониторинг активности использования аппаратных ресурсов как косвенных показателей возможных узких мест в программных компонентах

Контроль статистики ОС является комплексным мероприятием и должен быть организован специалистами технической поддержки. В ТИКСЕР БЕССТ версии 4.0 выделенный инструментарий для проведения анализа утилизации ресурсов ОС не предусмотрен, однако такие компоненты существуют в родительской системе КоСиКУЛС БЕССТ и их добавление планируется в следующей версии ТИКСЕР БЕССТ

На момент подготовки настоящих рекомендаций авторское введение в тему сбора и анализа статистики утилизации ОС доступно по адресу http://www.ourorbits.org/itview/articles/system_stats.shtml

анализ журналов продукта

Журналы ТИКСЕР БЕССТ располагаются в каталоге /var/log/cosiculs, и их анализ в процессе проведения технического обслуживания может выявить какие - либо аномалии в поведении сервера

контроль работоспособности функций продукта

Основные функции сервера должны быть проверены в процессе проведения технического обслуживания - создание, изменение и удаление пользователя в хранилище UNIX и каталоге LDAP, создание лимитирующих записей в биллинговой системе прокси сервера, правил в почтовой компоненте, приём и отправку электронной корреспонденции, доступ к WEB ресурсам через прокси сервис, функционирование сетевого фильтра, формирование отчётов каждой из компонент

контроль системных областей и попыток вторжения

Для проведения части контролирующих мероприятий потребуется **создание слепков** сервера (первоначальных и последующих). Если организация технической поддержки планируется организовывать, снятие слепков удобно сделать сразу после установки сервера

список установленных пакетов необходимо сохранить в отдельный файл командой

rpm -qa | sort > полный_путь_к_файлу

соответствие относящихся к RPM пакетам файлов и метрик, хранящихся в базе пакетов, необходимо сохранить в отдельный файл командами

rpm -V -a > полный_путь_к_файлу

конфигурационные каталоги/файлы удобнее всего скопировать из каталога /usr/local/cosiculs/backup после запуска скрипта резервного копирования ТИКСЕР БЕССТ v.4.x

список объектов файловой системы с установленными дополнительными битами необходимо сохранить в отдельный файл командой

find /etc /boot /bin /lib /sbin /usr/etc /usr/bin /usr/sbin /usr/lib /usr/libexec /usr/local/etc /usr/local/bin /usr/local/sbin /usr/local/lib /usr/local/libexec \(-perm -04000 -o -perm -02000 -o -perm -01000\) -exec ls -ald '{}' \; > полный_путь_к_файлу

список хэшей md5 и sha1 для системных и конфигурационных файлов необходимо сохранить в отдельный файл командами

find /etc /boot /bin /lib /sbin /usr/etc /usr/bin /usr/sbin /usr/lib /usr/libexec /usr/local/etc /usr/local/bin /usr/local/sbin /usr/local/lib /usr/local/libexec -type f -exec md5sum '{}' \; > полный_путь_к_файлу

find /etc /boot /bin /lib /sbin /usr/etc /usr/bin /usr/sbin /usr/lib /usr/libexec /usr/local/etc /usr/local/bin /usr/local/sbin /usr/local/lib /usr/local/libexec -type f -exec sha1sum '{}' \; > полный_путь_к_файлу

список файлов и каталогов с временем установки и модификации необходимо сохранить в отдельный файл командами

ls -Rail / > полный_путь_к_файлу

Все эти данные необходимо скопировать на защищенный носитель независимо от сервера для последующего сравнения с аналогичными данными, периодически собираемыми в процессе эксплуатации сервера. Удобно организовать сбор всех данных слепка в один

скрипт, а последующее сравнение организовать отдельным скриптом, перебирающим соответствующие файлы слепков и сравнивающий их командой

diff полный_путь_начального_слепка полный_путь_слепка_N

Кроме сравнения собранных слепков полезно установить и периодически запускать **пакеты обнаружения руткитов**, например chkrootkit и rkhunter. Для еще более полного анализа системы оптимально использовать инструменты, наиболее удобные проводящему техническое обслуживание специалисту, например специализированные Live CD

В общем случае допустимо проводить сравнения слепков и запуск антируткит- пакетов непосредственно на работающем сервере, однако в сложных случаях правильно проводить исследования и проверки, потушив сервер и подключив его диск к отдельному компьютеру для исключения возможного влияния внедрённого вредоносного программного обеспечения

обновление платформы

Архитектура ТИКСЕР БЕССТ v.4.x подразумевает «достаточно хорошее» соответствие базовым принципам обеспечения безопасности решения - пользователи не имеют возможности войти на сервер локальной сессией, запущены только требуемые для обеспечения функциональности сервисы, установлен усечённый набор пакетов, активирован сетевой фильтр и авторизация пользователей в сервисах, не используются излишние для решения расширенные функции

Следствием такой организации является относительно небольшое количество «точек риска», через которые может быть проведено проникновение в систему. В контексте задачи обеспечения отказоустойчивости и взломостойкости ТИКСЕР БЕССТ v.4.x требуется организовать мониторинг появления уязвимостей у относительно небольшого количества пакетов, к которым в первую

очередь относится ядро с встроенным стеком IP и сетевым фильтром, и слушающие сеть сервисы - DNS сервер bind, DHCP сервер, почтовый сервис exim. Второй, менее критичной, линией внимания являются основные библиотеки (glibc, zlib и т.п.) и прочие активные сервисы - squid, ulogd, postgree sql, и обновление пакета и антивирусных баз clamav

Используемый в качестве базовой платформы дистрибутив Linux CentOS 5.3 является пакетно - ориентированным и обеспечен регулярно обновляемым репозитарием пакетов. ТИКСЕР БЕССТ v.4.x уже сконфигурирован на использование штатных репозитариев, что позволяет максимально просто проводить обновление пакетов операционной системы, однако решение о проведении обновления по хорошему должно предваряться проведением обновлений в тестовой лаборатории, дабы не порушить работающую промышленную систему

Непосредственно проведение обновления как на тестовой, так и на боевой системах (при условии подключения сервера к Интернет) выполняется командой yum с ключами:

- для просмотра доступных пакетов **yum list**
- для вывода списка пакетов с доступными обновлениями **yum check-update**
- для обновления одного пакета **yum update имя_пакета**
- для обновления всех установленных пакетов **yum update**

Таким образом перед проведением обновлений введённого в промышленную эксплуатацию решения рекомендуется оттестировать работоспособность решения после проведения обновлений на тестовой системе. Такое тестирование должен проводить специалист, проводящий техническое обслуживание у клиентов - ведь именно ему отвечать перед клиентом за проведённые на серверах клиента действия. Для случая использование у клиентов однотипных решений тестовая система может быть развёрнута у поставщика в единственном экземпляре