Средство криптографической защиты информации "Континент TLS-сервер". Версия 2.1 Комментарии к релизу 2.1.1.141

Документ содержит описание основных возможностей, особенностей работы и ограничений применения изделия "Средство криптографической защиты информации "Континент TLS-сервер". Версия 2" (далее – СКЗИ "Континент TLS-сервер", Сервер), которые необходимо учитывать при его эксплуатации.

Оглавление

1. Изменения и новые возможности

Ниже приводятся сведения об изменениях и новых возможностях СКЗИ "Континент TLS-сервер" версии 2.1 (релиз 2.1.1.141) по сравнению с сертифицированным ФСБ России СКЗИ "Континент TLS VPN Сервер" версии 1.2 (релиз 1.2.1).

1.1. Версия 2.1

1. Появилась возможность настройки порта сервера управления, прокси и туннеля.

2. Реализован мониторинг по протоколу SNMP.

3. Добавлена возможность не корректировать HTTP-перенаправления в Proxy.

4. Добавлена двухфакторная аутентификация с использованием auth.as.

5. Появилась возможность использовать сертификаты с разными алгоритмами ГОСТ для Издателя и Субъекта, а также для Клиента и Сервера.

6. Появилась возможность скачивания системного журнала из Web.

7. Добавлена возможность настройки тайм-аута в туннеле.

8. При формировании запроса на серверный сертификат добавлен выбор типа субъекта для возможности формирования запроса на сертификат, соответствующего требованиям к квалифицированным сертификатам.

9. К возможностям сетевой диагностики добавлена команда TCPdump.

10. В качестве алгоритма формирования электронной подписи в сертификате сервера допускается только ГОСТ Р.34.10-2012. При этом сервер поддерживает работу с пользовательскими и корневыми сертификатами по ГОСТ Р.34.10-2001 до момента истечения их срока действия.

1.2. Версия 2.0

1. Разработан новый пользовательский интерфейс.

2. Реализована поддержка защищаемых ресурсов с NTLM-аутентификацией.

3. Для приложений портала внедрена технология единого входа Single Sign-On.

4. В портальном приложении появилась возможность добавления кнопок меню.

5. Выполнена поддержка доменов поиска для DNS.

6. Появилась возможность выбора языка интерфейса в главном меню локального управления.

7. Лицензии в кластере, не привязанные к конкретному серверу, разделяются между всеми доступными серверами кластера равномерно.

8. В режимах HTTPS-прокси и портала приложений у администратора появилась возможность редактировать текст ответа от защищаемого ресурса.

2. Ограничения на поддержку аппаратных и программных средств

1	Ключевые устройства		• Рутокен ЭЦП; • USB-флеш-накопитель
2	Аппаратные платформы	IPC-1000-TLS	DV-031D
		IPC-50-TLS	LN-010C
		IPC-3000-TLS	LN-021B
		IPC-500-TLS	LN-015D

3. Особенности работы и ограничения

1. При восстановлении из резервной копии удаляются все настройки SSH, если они привязаны к другому кластеру. Лицензии, привязанные к другому кластеру, отвязываются от серверов.

2. После обновления с предыдущей версии сервер может оказаться в заблокированном состоянии. В этом случае после обновления следует проверить состояние блокировки и при необходимости разблокировать сервер вручную.

3. При обновлении Сервера в составе кластера средствами локального управления возможна задержка появления локального меню после его перезапуска. В этом случае следует нажать любую клавишу.

4. В запросе на создание серверного сертификата доменное имя сервера должно быть написано прописными буквами (допускается использование IP-адреса). Использование заглавных букв запрещается.

5. Для входа в веб-управление с помощью браузера Internet Explorer версия браузера должна быть 10 или выше (рекомендуется IE 11).

6. Использование защищаемым ресурсом старой версии NTLM-аутентификации не поддерживается.

7. Microsoft Active Directory, по умолчанию, имеет ограничения в 1000 записей в ответ на запросы LDAP. Если на сервере существует более тысячи групп, то для использования данного Сервера в качестве LDAP для TLS-сервера, требуется либо изменить данный параметр, либо ограничить выборку с помощью Base DN.

8. Отображение параметров дисковых разделов по SNMP для платформ, имеющих RAID, поддерживается частично.

9. Существует проблем загрузки ключевых контейнеров с USB-флеш-накопителей, которые содержат мастер-ключ, созданный на основе версии 1.2.1. Для их загрузки установите сначала версию 1.2.1, загрузите ключ и установите более свежую версию ПО. Ключ при перезагрузке не будет уничтожен, так как хранится в ПАК "Соболь".

10. Если используемый порт Портала отличается от стандартного (443) и защищаемый сайт содержит ссылки на самого себя, то корректная работа Портала возможна только при использовании TLS Client 2.

11. При выполнении обновления или возврату к предыдущей версии ПО с помощью веб-управления будет разорвана связь между интерфейсом клиента и Серверу. Для возобновления связи закройте браузер и подсоединитесь к обновленному Серверу заново.

12. После выполнения обновления до версии 2.1 все списки CRL будут удалены из базы. Для продолжения работы необходимо загрузить их вручную или дождаться их автоматического обновления.

13. Во время операции проверки сертификатов, все операции по применению изменений отложены. Поэтому существует возможность, что изменения, внесенные администратором, будут применены не сразу. Также не сразу можно будет подсоединить подчиненный сервер в кластер. Данная операция запускает раз в сутки, ночью, а также при старте сервера и восстановления из резервной

копии. Время данной операции зависит от количества всех сертификатов на сервере и может занимать от нескольких секунд до получаса.

14. Для работоспособности сервера после загрузки резервной копии необходимо дождаться завершения процесса проверки сертификатов (он может занимать от нескольких секунд до получаса в зависимости от количества сертификатов) и загрузки CRL (автоматически по расписанию или загрузить их вручную).

15. Обновление средствами удаленного управления возможно только для одиночного сервера. Серверы в составе кластера версии 2.1.1 следует обновлять методом локальной установки новой версии с загрузкой сохраненной резервной копии.

Компания "Код Безопасности"

Почтовый адрес:	115127, Россия, Москва, а/я 66
Телефон:	8-495-982-30-20
E-mail:	info@securitycode.ru
Сайт:	https://www.securitycode.ru