РЕАЛИЗАЦИЯ АВТОРИЗАЦИИ В РАМКАХ ВЕБ-СЕРВЕРА APACHE

Ю. А. Юлин, А. М. Бармин, И. А. Пищулин

ФГУП «РФЯЦ-ВНИИЭФ», г. Саров Нижегородской обл.

Введение

В настоящее время ведется работа по созданию и сертификации дистрибутива ОС для эксплуатации на супер-ЭВМ в защищенном исполнении класса «1Б».

Это подразумевает реализацию в рамках операционной системы средств защиты информации для удовлетворения требований 3-го класса средств вычислительной техники и 2-го уровня контроля отсутствия недекларированных возможностей.

Сертификация будет проводиться по требованиям безопасности информации ФСТЭК России и Министерства Обороны РФ.

Так как, веб-сервисы являются неотъемлемой частью создаваемого стека системного программного обеспечения, организация авторизованного доступа к веб-сервисам является обязательным требованием согласно нормативным документам государственного регулятора ФСТЭК России.

Задачи

Для организации авторизованного доступа необходимо выполнить процедуры идентификации, аутентификации и авторизации.

Идентификация – процедура распознавания субъекта по его идентификатору [1].

Аутентификация – процедура проверки подлинности субъекта, для того чтобы узнать что субъект именно тот, за кого он себя выдает [2].

Авторизация – это предоставление субъекту прав на выполнение определенных действий [3]. При авторизации субъекта выполняются задачи, связанные с организацией начала работы уже идентифицированного и аутентифицированного субъекта доступа. Происходит создание системного окружения и назначение атрибутов безопасности.

Схема функционирования веб-сервисов в рамках супер-ЭВМ

Рассмотрим схему функционирования веб-сервисов (рис. 1) в рамках супер-ЭВМ. В упрощенном виде супер-ЭВМ состоит из управляющих серверов, вычислительной среды, системы хранения данных и фронт серверов, являющиеся точкой входа для пользователей. Данные компоненты супер-ЭВМ соединены между собой высокоскоростной коммуникационной средой. Для получения веб-сервисов, располагающихся на фронт серверах, пользователи со своих рабочих станций посредством браузеров делают запросы, которые передаются по внутренней сети предприятия к фронт серверам. Для работы веб-сервисов необходим веб-сервер.

Веб-сервер Apache

Выбор веб-сервера был сделан в пользу Apache. Данный веб-сервер распространяется абсолютно бесплатно, и его лицензия позволяет конечному пользователю редактировать исходный код. Он является кроссплатформенным, поддерживает операционные системы Linux, BSD, MacOS, Windows и др. [4]. Имеет поддержку протоколов шифрования SSL и TSL для веб-сайтов, требующих повышенной безопасности. Существуют различные модули мультипроцессинга, позволяющие адаптировать веб-сервер под свою операционную систему для достижения наилучшей производительности.

Техническая поддержка Apache доступна на множестве сайтов благодаря его широкой распространенности.

Существует множество модулей, добавляющих к Apache поддержку различных языков программирования таких как PHP, Perl и Python и других.

Netcraft – организация, предоставляющая разного рода аналитическую информацию, опубликовала статистику на март 2017 года по доле веб-серверов на активных сайтах. По данной статистике веб-сервер Apache занимает более 45 % [5].

Готовые решения в рамках Apache

Для решения поставленных задач были проанализированы имеющиеся решения в рамках веб-сервера Apache.

Модуль mod_authnz_pam реализует идентификацию и аутентификацию посредством PAM. PAM – это набор библиотек, которые объединяют различные низкоуровневые механизмы аутентификации в виде единого высокоуровнего API [6].

Модуль mod_authnz_ldap реализует идентификацию и аутентификацию посредством LDAP. LDAP – это сетевой сервис, представляющий централизованные средства доступа к автоматизированной системе [7].

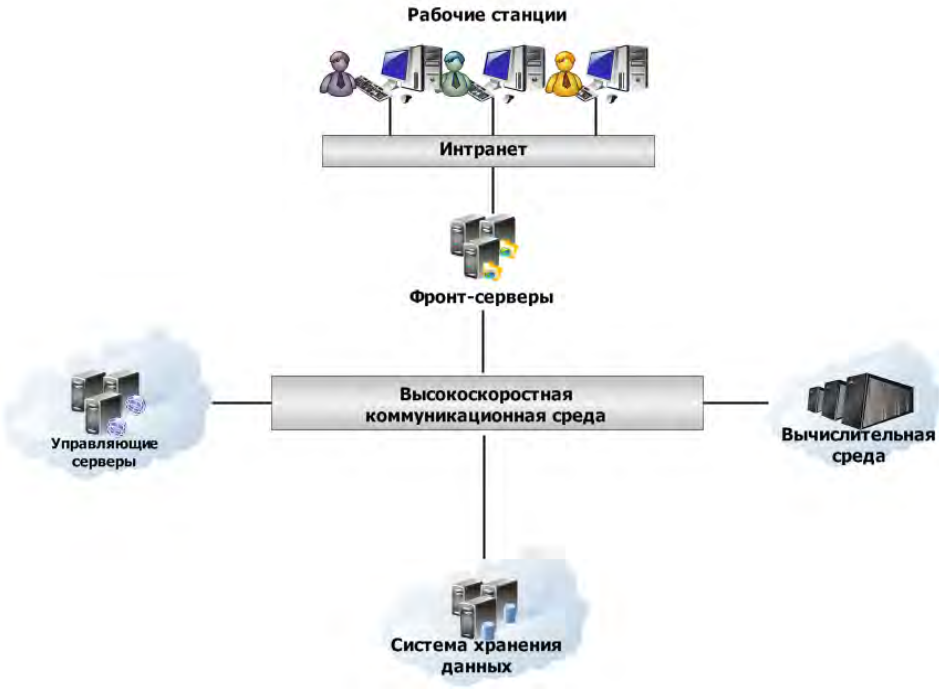

Рис. 1. Схема функционирования веб-сервисов

Модуль mod_auth_kerb – реализует идентификацию и аутентификацию посредством Kerberos. Kerberos – это сетевой протокол аутентификации [8].

Механизм SuExec позволяет выполнять смену системного окружения процесса, исполняющего сценарий.

Модуль ITK позволяет выполнять смену системного окружения веб-сервисов.

В таблице наглядно представлены готовые решения и задачи, которые они реализуют.

Модули mod_authnz_pam и mod_authnz_ldap реализуют идентификацию и аутентификацию. Из авторизации они реализует только доступ либо ограничение доступа к веб-сервису. Смену системного окружения процесса и установку мандатных атрибутов данные модули не реализует.

Модуль mod_auth_kerb реализует только идентификацию и аутентификацию.

Механизм SuExec и модуль ITK не реализуют идентификацию и аутентификацию. Из авторизации реализуют только смену системного окружения процесса. Установку мандатных атрибутов не поддерживают.

Как видим в полном объеме ни одно из средств не реализует поставленные задачи. По этой причине был реализован собственный модуль mod_authnz_aramid.

Модели функционирования процессов Apache

Веб-сервер Apache имеет несколько стабильных моделей функционирования процессов [4]. Данные модели реализованы в виде модулей и представляют собой интерфейс между запущенным сервером Apache и ОС, а также служат для оптимизации Apache под различные платформы.

В настоящее время используется две основные модели – это Prefork и Worker. Также, имеется сравнительно новый модуль – Event, который только недавно перешел из стадии экспериментального в стабильный.

Готовые решения

	Идентификация	Аутентификация	Авторизация
mod_authnz_pam	+	+	+/-
mod_authnz_ldap	+	+	+/-
mod_auth_kerb	+	+	-
SuExec	-	-	+/-
ITK	-	-	+/-

Для разработки была выбрана модель Prefork. На данный момент это наиболее распространенная модель, и по умолчанию Apache устанавливается именно с ней. Одним из важнейших преимуществ данной модели является её надежность и безопасность, в силу того, что каждый процесс изолирован друг от друга.

Схема работы модуля mod_authnz_aramid

Клиент со своего рабочего места посредством браузера делает запрос, который отправляется по протоколу HTTP на сервер. Сервер обрабатывает данный запрос, и делает ответ.

Модуль mod_authnz_aramid взаимодействует с библиотеками PAM, lbc, libzos.

PAM – это набор библиотек, объединяющие различные низкоуровневые механизмы аутентификации в виде единого высокоуровневого API.

Libc – это стандартная библиотека языка Си, посвященная заголовочным файлам [9].

Libzos – это библиотека для работы с мандатным контекстом ЗОС Арамид.

Пришедший запрос проходит стадии идентификации и аутентификации посредством API библиотеки PAM. Далее происходит получение идентификатора пользователя и группы и смена пользовательского и группового идентификатора процесса, обрабатывающего запрос. Далее происходит получение мандата пользователя и смена мандата процесса при помощи API библиотеки libzos. Дальнейший процесс обработки запроса выполняется Apache.

Настройки модуля mod_authnz_aramid

В настройке модуля можно выделить два этапа:

- настройки для веб-сервера;
- настройки для PAM.

Настройки веб-сервера располагаются в файле aramid.conf. В нем располагаются три основные директивы данного модуля: AuthBasicProvider со значением pam – означает, что аутентификация будет проходить с помощью PAM API; AuthPAMService со значением apache – указывает конфигурационный файл PAM для данной аутентификации; директива Requireco значением system-env определяет провайдера авторизации.

Настройки для PAM располагаются в файле mod_authnz_aramid. В нем указано использовать файл политик для системной аутентификации.

Заключение

В результате проделанной работы были реализованы механизмы идентификации, аутентификации, авторизации и настройки привилегированного системного окружения процессов в рамках веб-сервера Apache; обеспечено функционирование веб-сервисов в рамках ЗОС Арамид.

В планах реализовать PAM-Aramid для модели функционирования процессов Event, а также реализовать поддержку сетевого протокола аутентификации Kerberos.

Литература

1. Идентификация (информационные системы), [в интернете]. Available: https://ru.wikipedia.org/wiki/Идентификация_(информационные_системы).
2. Аутентификация, [в интернете]. Available: https://ru.wikipedia.org/wiki/Аутентификация.
3. Авторизация, [в интернете]. Available: https://ru.wikipedia.org/wiki/Авторизация
4. Apache HTTP Server, [в интернете]. Available: https://ru.wikipedia.org/wiki/Apache_HTTP_Server.
5. W3Tech: доля nginx в мире выросла до трети, Apache упал ниже половины, [в интернете]. Available: https://habrahabr.ru/post/326248/.
6. Pluggable Authentication Modules, [в интернете]. Available: https://ru.wikipedia.org/wiki/Pluggable_Authentication_Modules.
7. LDAP, [в интернете]. Available:https://ru.wikipedia.org/wiki/LDAP.
8. Kerberos, [в интернете]. Available: https://ru.wikipedia. org/wiki/Kerberos.
9. Стандартная библиотека языка Си, [в интернете]. Available: https://ru.wikipedia.org/wiki/ Стандартная_библиотека_языка_Си.