Модель администрирования схем разграничения доступа в облачных инфраструктурах

Model of administration of access control schemes in cloud infrastructures

Саенко / Saenko I.
Игорь Борисович
(ibsaen@mail.ru)
доктор технических наук, профессор.
ФГКВОУ ВО «Военная академия связи имени Маршала Советского Союза С. М. Буденного» (ВАС им. С. М. Буденного) МО РФ.
г. Санкт-Петербург

Бирюков / Biryukov M.
Михаил Александрович
(urgent.ma@gmail.ru)
ВАС им. С. М. Буденного, адъюнкт.
г. Санкт-Петербург

Ефимов / Efimov V.
Вячеслав Викторович
(vve@loniis.ru)
кандидат технических наук, доцент.
Филиал ФГУП «Ленинградское отделение центрального научно-исследовательского института связи» (ЛО ЦНИИС),
и. о. директора.
г. Санкт-Петербург

Ясинский / Yasinsky S.
Сергей Александрович
(yasinsky777@mail.ru)
доктор технических наук, доцент.
Филиал ФГУП ЛО ЦНИИС,
научный консультант.
г. Санкт-Петербург

Ключевые слова: разграничение доступа – access control; облачная инфраструктура – cloud infrastructure; схема разграничения доступа – access control scheme; имитационная модель – simulated model; RBAC.

Рассматривается новый подход к оценке администрирования схем разграничения доступа в облачных инфраструктурах. Определяются условия реконфигурации исходной схемы разграничения доступа. Приводится описание имитационной модели администрирования схемы разграничения доступа. Обсуждаются результаты применения имитационного моделирования к решению задачи оценки схемы доступа в облачных инфраструктурах. Предлагается способ определения условий реконфигурации схемы разграничения доступа.

The article describes new approach to evaluation of administration of access control schemes in cloud infrastructures. Conditions for reconfiguration of the initial access control scheme are defined. A simulated model of administration of an access control scheme is described. Results of simulation modeling application to the solution of the problem of evaluation of the access scheme in cloud infrastructures are discussed. The article proposes a method for definition of conditions for access control scheme reconfiguration.

Введение

Стремительное распространение облачных инфраструктур среди автоматизированных систем различного назначения, наблюдаемое сегодня в отечественном IT-секторе, повышение совокупной стоимости активов, устройств, программного обеспечения и критически важных данных в таких системах, а также значительное увеличение количества воздействующих на них компьютерных атак – все это определяет актуальность задач обеспечения безопасности и разграничения доступа к информационным ресурсам облачных вычислительных инфраструктур.

Согласно исследованиям, проведенным аналитиками российской компании iKS-Consulting, за период с 2015 года по 2020 год российский рынок облачных услуг должен вырасти в три раза и составить 78,6 миллиарда рублей (http://www.audit-it.ru/news/soft/887749.html). К числу ключевых тенденций развития облачных инфраструктур относят дальнейшее увеличение их возможностей по обеспечению надежности, безопасности, производительности, управляемости и масштабируемости. Таким образом, вопросы обеспечения безопасности, а разграничение доступа является составной частью безопасности, стоят на одном из первых мест.

Облачная вычислительная инфраструктура (или просто «облачная инфраструктура») – это модель сете-

вого доступа в режиме «по требованию», которая предполагает использование вычислительных ресурсов не рабочей станции пользователя, на которой работает пользователь, а сторонней инфраструктуры [1]. Данная модель в первую очередь направлена на повышение доступности вычислительных ресурсов. В свою очередь модель разграничения доступа (access control model) проверяет полномочия субъектов доступа и предоставляет (или не предоставляет) доступ к запрашиваемым объектам. В связи с тем, что облачная инфраструктура является, как правило, мультиарендной средой (multi-tenant environment) [2], риск реализации несанкционированного доступа к критическим активам и ресурсам в облачной инфраструктуре значительно увеличивается.

В настоящий момент известно множество моделей разграничения доступа, используемых в облачных инфраструктурах. Совокупность настроек модели разграничения доступа образует схему разграничения доступа. В ходе администрирования схем разграничения доступа поочередно решаются две задачи: первоначальное проектирование схемы и реконфигурация схемы [3]. Первая задача заключается в формировании первичной схемы и решается, как правило, до начала работы в автоматизированной системе. В ходе работы в автоматизированной системе состав объектов и субъектов доступа претерпевает изменения, что вызывает необходимость своевременной реконфигурации первичной схемы разграничения доступа. Эти вопросы решаются второй задачей. При этом сложность решения второй задачи увеличивается пропорционально количеству объектов и субъектов доступа. В результате при администрировании схемы разграничения доступа возможно появление ошибок, влияющих на доступность ресурсов облачной инфраструктуры.

Цель настоящей работы заключается в разработке модели администрирования схемы разграничения доступа, позволяющей оценить выполнение критериев доступности и определять критические значения количества изменений схемы разграничения доступа, при достижении которых необходимо выполнение первоначального проектирования схемы. Модель позволяет повысить эффективность управления доступом и, соответственно, безопасность облачной инфраструктуры.

Разграничение доступа в облачных инфраструктурах

Основными причинами, по которой многие компании не решаются переходить на облачные решения, являются вопросы безопасности. Опасения относительно сохранности конфиденциальных данных, относящихся как к коммерческой тайне, так и к персональным данным клиентов, до сих пор остаются главным препятствием широкого внедрения облачных технологий. Между тем, сами провайдеры уже давно уделяют первостепенное внимание безопасности, считая необходимым не только неформальное соответствие современным требованиям, но и получение формальных сертификатов соответствия известным стандартам, например международному стандарту по информационной безопасности ISO/IEC 27001.

Управление элементами облачной инфраструктуры, такими как сеть, сервера, операционные системы, системы хранения и индивидуальные пользовательские приложения, осуществляется, как правило, провайдером предоставляемого сервиса. Так как при этом зачастую используются различные методы виртуализации, возникает необходимость обеспечения адекватной защиты инфраструктуры в соответствии с требованиями регулятора. Однако в настоящее время пока еще нет утвержденных регулятором требований к защите подобных инфраструктур. Поэтому предполагается, что защиту облачной инфраструктуры провайдер производит самостоятельно.

В облачной инфраструктуре действия пользователя имеют случайный и непрерывный характер, что значительно затрудняет управление ресурсами и усложняет обеспечение безопасности системы в целом. В соответствии с вышеизложенным, остро встает проблема эффективного администрирования схем разграничения доступа к ресурсам облачных инфраструктур.

Рассмотрим наиболее распространенные модели разграничения доступа, ориентированные на использование в облачных инфраструктурах.

Наиболее распространенной является ролевая модель (Role-Based Access Control, RBAC) [4]. В модели RBAC администратор безопасности производит формирование и назначение ролей и построение иерархии ролей. В соответствии с назначенными ролями определяются разрешенные полномочия пользователей. Каждая роль формируется, исходя из задач пользователя. Роль содержит минимально необходимый набор полномочий, которые необходимы пользователю для выполнения своих функциональных обязанностей. Полномочия могут добавляться или удаляться по усмотрению администратора. Модель RBAC получила широкое распространение в облачных структурах в связи с тем, что она тесно связана с процессами идентификации пользователей облачных хранилищ и сервисов.

В последнее время появились разновидности традиционной модели RBAC, такие как Task-RBAC, Trust-RBAC и Temporal-RBAC. В модели Task-RBAC для более детального управления доступом назначаемые полномочия основываются не только на ролях, но и на задачах, которые входят в функциональные обязанности пользователей [5]. В этой модели роль может выключать целый ряд задач. Администраторы безопасности могут использовать задачи для реализации активного разграничения доступа, а роли – для пассивного. Однако управление разграничением доступа вырождается с увеличением количества задач.

Модель Trust-RBAC основывается на концепции доверенного управления, разработанной для определения доверительных отношений между перспек-

тивными транзакциями [6]. Эта концепция призвана решать различные проблемы безопасности, но пока не получила практического применения.

В некоторых случаях роль может быть доступна в течение ограниченного времени. Более того, временный характер может носить не только роль, но и связи внутри самой роли. Эти факторы учитывает модель Temporal-RBAC, в которой роли и зависимости внутри ролей активируются с заданной периодичностью [7].

Облачная инфраструктура, как правило, состоит из нескольких автономных корпоративных автоматизированных систем с различными моделями безопасности. Поэтому для безопасной эксплуатации мультиарендной среды необходим достаточно гибкий механизм разграничения доступа, поддерживающий гетерогенные структуры. В качестве модели доступа для таких структур может выступать атрибутивная модель доступа (Attribute-Based Access Control, ABAC) [8]. Эта модель выделяет атрибуты объектов, действий, субъектов и условий доступа. Для предоставления доступа с помощью модели ABAC значения атрибутов сравниваются с политикой безопасности и принимается решение о предоставлении доступа.

Так как среди рассмотренных выше моделей наиболее широкое применение получила модель RBAC, эта модель будет использоваться для разработки модели администрирования схемы разграничения доступа.

Постановка задачи на разработку модели администрирования схемы разграничения доступа

В настоящее время моделирование является основным методом исследований во всех областях знаний и научно обоснованным методом оценок характеристик сложных систем, в частности, управления доступом, используемого для принятия решений в различных сферах деятельности [9].

Анализ характеристик процессов функционирования системы разграничения доступом с помощью аналитических методов наталкивается на значительные трудности, приводящие к необходимости существенного упрощения моделей и получению недостоверных результатов. Поэтому представляется целесообразным для моделирования работы со схемой разграничения доступа использовать имитационную модель.

В таблице 1 приведено сравнение известных систем имитационного моделирования по их функциональным возможностям. Выбор систем, а также функций, учитываемых для сравнительной оценки, производился на основе анализа данных, представленных в [10, 11].

Реализация имитационной модели для ролевого разграничения доступа возможна только с использованием двух подходов – агентного и дискретно-событийного. Поэтому, исходя из данных сравнительной

Таблица 1

Сравнение систем имитационного моделирования

№ п/п	Функции	Системы имитационного моделирования									
		Extend	iThink	VenSim	PowerSim	Pilgrim	Process Charter	Arena	Business Studio	GPSS/W	**AnyLogic**
1	Компоновочные блоки	+				+		+	+		+
2	CASE-средства		+			+					
3	Потоковые диаграммы		+	+	+			+			+
4	Блок-схемы						+	+	+	+	
5	Архитектура «документ – вид»									+	
6	Поддержка анализа результатов	+	+	+		+		+	+	+	+
7	Авторское моделирование	+	+			+		+	+	+	+
8	Стратегическое планирование	+									
9	Модели бизнес-процессов	+						+	+		+
10	Реинжиниринг предприятия		+						+		
11	Модели системной динамики			+				+			
12	Непрерывное моделирование				+					+	
13	Модели динамических систем					+				+	
14	Дискретное моделирование		+				+	+		+	+
15	Дискретно-событийное моделирование										+
16	Агентное моделирование										+

оценки, можно сделать вывод, что наиболее подходящим средством имитационного моделирования для RBAC выступает программная система AnyLogic.

Имитационная модель администрирования схемы разграничения доступа RBAC в облачной инфраструктуре, разработанная на основе AnyLogic, имеет блочный вид и отражает работу администратора безопасности со следующими множествами:

$U = \{u_i\}, i = 1,..,n, n = |U|$ – множество пользователей облачной инфраструктуры;

$R = \{r_j\}, j = 1,..,m, m = |R|$ – множество ролей модели RBAC;

$O = \{o_k\}, k = 1,..,l, l = |O|$ – множество объектов доступа облачной инфраструктуры.

Тогда выражение

$$ChRD_{\text{тр}} = \langle U, O \rangle \quad (1)$$

определяет требуемую (эталонную) схему разграничения доступа, а выражение

$$ChRD_{\text{адм}} = \langle U, O, R \rangle \quad (1)$$

определяет схему разграничения доступа, сконфигурированную администратором безопасности.

Задача администрирования схемы разграничения доступа в облачной инфраструктуре заключается в следующем:

– первоначальное проектирование (конфигурация) схемы $ChRD_{\text{адм}}$, удовлетворяющей требованиям по обеспечению безопасного и доступного разграничения доступа к ресурсам;

– использование $ChRD_{\text{адм}}$ для обеспечения требуемой доступности;

– своевременное реконфигурация схемы $ChRD_{\text{адм}}$ в схему вида

$$ChRD_{\text{адм}}^{\text{ркфг}} = \langle ChRD_{\text{адм}}, U', O', R' \rangle, \quad (3)$$

где U', O', R – множество пользователей, ресурсов и ролей, соответственно, измененные в процессе ее администрирования.

Для принятия решения о реконфигурации схемы разграничения доступа необходимо оценить критичность влияния изменений, вносимых администратором безопасности в первичную схему разграничения доступа и определить достаточные условия реконфигурации.

В качестве показателя критичности предлагается взять «коэффициент ошибки доступа» $K_{\text{ош}}$, который характеризуется вероятностью возникновения отказа в доступе $(P_{\text{НОД}})$ и вероятностью несанкционированного доступа $(P_{\text{НСД}})$ при единичном воздействии на схему доступа $ChRD_{\text{адм}}$ следующим образом:

$$K_{\text{ош}} = 1 - (1 - P_{\text{НСД}})(1 - P_{\text{НОД}}). \quad (4)$$

Целью моделирования является определение выполнения условий достаточности для выполнения реконфигурации исходной схемы. К схемам разграничения доступа предъявляются требования по доступности, указанные в таблице 2 [12].

Выражения для расчета значений показателей доступности разграничения доступа являются следующими:

$$P_{\text{НСД}} = \frac{N_{\text{ош}}^{\text{г дост}}}{N_{\text{общ}}}, \quad (5)$$

$$P_{\text{НОД}} = \frac{N_{\text{ош}}^{\text{отк}}}{N_{\text{общ}} - N_{\text{прав}}^{\text{отк}}}, \quad (6)$$

где $N_{\text{общ}}$ – общее количество запросов доступа, $N_{\text{ош}}^{\text{дост}}$ – количество ошибочно разрешенных запросов, $N_{\text{ош}}^{\text{отк}}$ – количество ошибочных отказов в доступе, $N_{\text{прав}}^{\text{отк}}$ – количество обоснованных отказов в доступе.

Таким образом, достаточным условием принятия решения по реконфигурации схемы разграничения доступа RBAC будет превышение ею требований по доступности, приведенных в таблице 2.

Таблица 2

Показатели доступности схем разграничения доступа и требования, предъявляемые к ним

Наименование показателя	Обозначение	Характеристика показателя	Допустимые значения
Вероятность несанкционированного доступа	$P_{\text{НСД}}$	$P_{\text{НСД}} \le P_{\text{НСД доп}}$ определяет вероятность ошибок 1-го рода	$P_{\text{НСД доп}} = 10^{-3}$
Вероятность необоснованного отказа в доступе	$P_{\text{НОД}}$	$P_{\text{НОД}} \le P_{\text{НОД доп}}$ определяет вероятность ошибок 2-го рода	$P_{\text{НОД доп}} = 10^{-2}$

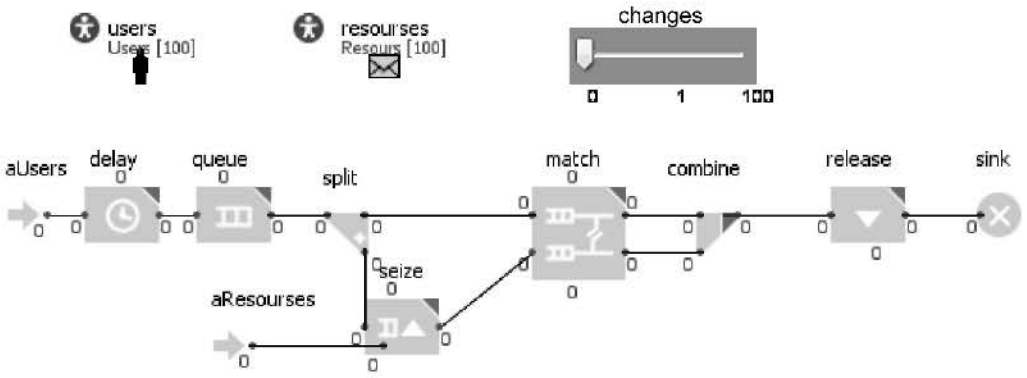

Рис. 1. Структура модели администрирования схемы разграничением доступа

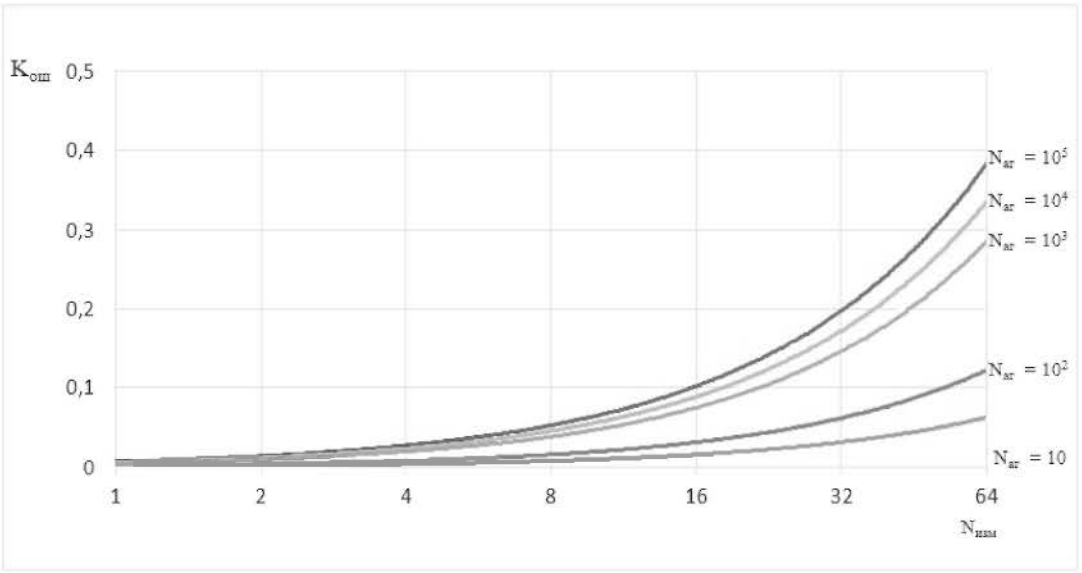

Рис. 2. Зависимость коэффициента ошибки доступа от количества изменений в схеме доступа

Модель схемы управления разграничением доступа

На рис. 1 изображена предлагаемая имитационная модель администрирования схемы разграничения доступа. Модель имитирует процесс администрирования первоначальной конфигурации схемы разграничения доступа $ChRD_{адм}$, разработанную администратором безопасности.

Модель характеризуется следующими ключевыми элементами:

– схема $ChRD_{адм}$, определена в переменных агентного типа aUsers и aResourses;

– механизм ролей реализован двумерными массивами в агентах aUsers и aResourses;

– блоки delay, queue определяют время поступления запросов доступа и очередь запросов соответственно;

– доступ пользователя к определенному ресурсу формируется в блоке split;

– поиск запрошенного ресурса осуществляется в блоке seize;

– проверка полномочий пользователя, определяемых схемой (1) на доступ к ресурсу, выполняет блок match;

– блок combine считает факты доступа/отказа в доступе;

– освобождение ресурсов происходит в блоке release;

– критерий changes определяет количество вносимых изменений в первоначально сконфигурированную схему доступа и принимает значения от 1 до 100.

Экспериментальная оценка модели

Результаты экспериментальной оценки функционирования имитационной модели администрирования схемы разграничения доступа представлены на рис. 2, где показаны зависимости коэффициента ошибки доступа ($K_{ош}$) от количества изменений в схеме доступа ($N_{изм}$) при различных значениях количества агентов моделируемой схемы (N_{ar}). Количество изменений, вносимых в первичную схему разграничения доступа, изменялось от одного до 64. При моделировании количество агентов изменялось от 1 до 105 для каждого заданного количества изменений схемы разграничения доступа.

Эксперимент показал, что даже при незначительном изменении схемы доступа администратором (блок changes) значения выражений (4), (5) и (6) выходят за рамки предъявляемых требований.

Заключение

Предлагаемый подход к определению условий осуществления реконфигурации схемы разграничения доступа (управляющего воздействия) основан на имитационном моделировании процесса администрирования схемы. Результаты моделирования показали, что в облачной инфраструктуре с большим числом пользователей практически любое изменение схемы разграничения доступа может приводить к значительному увеличению ошибок доступа к облачным ресурсам. Следовательно, можно сделать вывод, что в облачных инфраструктурах целесообразно аккумулировать изменения, связанные с ресурсами, полномочиями и ролями пользователей и осуществлять оперативную реконфигурацию схемы разграничения доступа только в автоматизированном режиме, исключающем появление ошибок, свойственных «ручному» администрированию.

Дальнейшие исследования связываются с разработкой модели оперативной реконфигурации схемы разграничения доступа облачной инфраструктуры и созданием на ее основе для администратора безопасности соответствующего средства специального программного обеспечения.

Литература

1. Zhang, P. Access control research on data security in cloud computing / P. Zhang, J. Xu, H. Muazu, W. Mao // Proceedings of the IEEE 16th International Conference on Communication Technology (ICCT). – 2015. – P. 873–877.

2. Ngo, C. Multi-tenant attribute-based access control for cloud infrastructure services / C. Ngo, Y. Demchenko, C. de Laat // Journal of information security and applications. – 2016. – Vol. 27–28. – P. 65–84.

3. Котенко, И. В. Генетические алгоритмы для булевой матричной факторизации применительно к задачам разграничения доступа в компьютерных сетях / И.В. Котенко, И.Б. Саенко // Пятнадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2016 (3–7 октября 2016 года, г. Смоленск): Труды конференции. Т.3. – Смоленск: Универсум, 2016. – С. 98–106.

4. Saenko, I. Reconfiguration of RBAC schemes by genetic algorithms / I. Saenko, I. Kotenko // Intelligent Distributed Computing X. Studies in Computational Intelligence. Springer-Verlag, Vol. 678. Proceedings of 10th International Symposium on Intelligent Distributed Computing – IDC'2016. Paris, France. 7–9 October, 2016. – Springer-Verlag, 2017. – P. 89–98.

5. Sejong, O. Task Role-Based Access Control Model / O. Sejong, P. Seog // Information Systems. – 2003. – No. 6. – P. 533–562.

6. Enhancing trust management in cloud environment / C. Soon-Keow [et al.] // Proceedings of the International Conference on Innovation, Management and Technology Research. – 2014. – P. 314–321.

7. Muthurajkumar, S. Intelligent temporal role based access control for data storage in cloud database / S. Muthurajkumar, M. Vijayalakshmi, A. Kannan // Proceedings of the IEEE Sixth International Conference on Advanced Computing (ICoAC). – 2014. – P. 184–188.

8. Yang, T.-C. An A-RBAC mechanism for a multi-tenancy cloud environment / T.-C. Yang, M.-H. Guo // Proceedings of the 2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE). – P. 1–5.

9. Брусакова, И. А. Имитационное моделирование в информационных системах: Учеб. пособие / И.А. Брусакова. – СПб.: СПбГИЭУ, 2004. – 151 с.

10. Борщев, А. В. Применение имитационного моделирования в России – состояние на 2007 г. / А.В. Борщев // Сборник докладов III Всероссийской научно-практической конференции «Имитационное моделирование. Теория и практика» (ИММОД-2007). Санкт-Петербург, 17–19 октября 2007. Т. 1. – С. 11–16.

11. Аксенов, К. А. Теория и практика средств поддержки принятия решений: монография / К.А. Аксенов // Гамбург: LAP LAMBERT Academic Publishing, 2011. – 341 с.

12. Авраменко, В. С. Модель для количественной оценки защищенности информации от несанкционированного доступа в автоматизированных системах по комплексному показателю / В.С. Авраменко, А.В. Козленко // Труды СПИИРАН. – 2010. – № 2 (13). – С. 172–181.