NETAPP TECHNICAL REPORT

Управление Role-Based доступом в Data ONTAP 7G

Ron Demery, NetApp

December 2009 | TR-3358

Коротко о главном:

Данный документ адресован администраторам системы хранения, администраторам системы безопасности, и системным администраторам. Он описывает представленную в Data ONTAP® 7G ролевую систему разграничения доступа (RBAC), и содержит обзор преимуществ ее использования, а также некоторые примеры решения с ее помощью задач разграничения администраторского доступа к системе хранения.

Оглавление

1 Что такое Role-Based Access Controls?

Ролевая модель разграничения доступа (Role-based access controls, или RBAC) - это метод управления набором действий, которые может осуществить над оборудованием пользователь или администратор.

Исторически сложилось так, что многие операционные системы позволяли любому пользователю, который имел доступ к OS, выполнять на ней любые действия. Многие системы не различали пользователей между собой вообще. Большинство ныне существующих операционных систем обеспечивают, как минимум, возможность создания нескольких различных пользователей, каждого с отдельным именем и паролем. Когда у OS появилась возможность различать пользователей, стало возможным разграничивать возможности этих пользователей по уровням доступа к файлам директориям, и другим системным объектам. Хороший пример это права на доступ к файлам в системах UNIX® (и в протоколе NFS) или списки контроля доступа (*access control lists*, ACL) используемые в системах семейства Windows® (и протокола CIFS).

Но кроме доступа к файлам, разграничение доступа требуется ряду других действий. Например, только системный администратор должен иметь право добавлять новых пользователей в систему. С этой позиции становится ясно, что пользователи, получающие доступ к системе, делятся на две основных категории, или роли: *администраторы* и *не-администраторы*.

Определить ряд функций для доступа «только администраторам» - хорошая стартовая точка, но требуется решить ряд дополнительных проблем. В большинстве организаций бывает несколько различных системных администраторов, в ряде случаев некоторые из них имеют более высокие права, чем другие. Выборочно назначая и отбирая права для каждого пользователя, вы можете настроить желаемый уровень доступа для такого администратора в системе. Как пример реализации, Microsoft® Windows обеспечивает такую возможность. Проблема, с которой вы неизбежно столкнетесь в таком случае при увеличении количества пользователей и администраторов, состоит в трудности и длительности индивидуальной настройки набора прав, соответствующего каждому такому пользователю.

Ролевая модель управления разграничением доступа решает эту задачу путем создания специального набора возможностей (роли), вместо назначения их какому-то конкретному пользователю. Пользователи помещаются в группу, на основании их рабочих функций, а каждой группе назначается та или иная роль, необходимая для выполнения нужного круга работ. При использовании такого метода, единственная требуемая настройка состоит в том, чтобы поместить нужного пользователя в правильные группы; пользователь унаследует из настроек группы все нужные возможности доступа, так как они назначены всем членам его группы.

2 Как работает RBAC в Data ONTAP?

Хотя общая концепция ролевой модели разграничения доступа реализована на множестве операционных систем и приложений, детали того, как именно реализованы методы RBAC в каждом конкретном случае весьма разнятся.

Этот раздел описывает специфику терминологии и архитектуры, используемой в Data ONTAP; очень важно целиком понять концепцию и определения перед тем, как конфигурировать RBAC в Data ONTAP, в особенности если вы уже имеете опыт использования RBAC в других системах и ПО, так как терминология или архитектура может отличаться от того, с чем вы имели дело ранее в других реализациях или системах.

2.1 Пользователи (Users)

Локальный пользователь (*user*) определен как учетная запись, которая аутентифицируется на системе хранения NetApp®.

Доменный пользователь (*domain user*) определен как «не-локальный» пользователь, который принадлежит домену Windows, и аутентифицируется средствами домена.

Оба типа пользователя, как «пользователь (локальный)», так и «доменный пользователь» представляют собой отдельного аутентифицированного человека. Хотя можно определить пользователя или доменного пользователя как какую-то программу, или общий аккаунт нескольких человек, это не является обычным способом использования, и мы не станем углубляться в эту тему здесь.

Как обычный локальный пользователь, так и доменный пользователь, подразумевается авторизованным системным администратором. Обычные пользователи, «не-администраторы», которые получают доступ к файлам по CIFS или NFS, или которые работают на клиентской системе, монтируя LUN-ы по FCP или iSCSI, не обсуждаются в этом документе. Они не имеют возможности попасть в систему или управлять Data ONTAP, пока они не будут специально определены как *users* или *domain user* с помощью команды `useradmin`.

Для подробностей смотрите главу «How to Manage Users» в **System Administration Guide**.

2.2 Группы (Groups)

Группа (*group*) определена как несколько пользователей или доменных пользователей. Группе можно назначить одну или несколько ролей. Важно помнить, что группа, заданная в Data ONTAP, существует отдельно от групп, заданных в другом контексте, например на сервере Microsoft Active Directory. Это так, даже если группа в Data ONTAP имеет то же самое имя, что и группа, созданная где-то еще в системе.

Когда вы создаете нового локального или доменного пользователя, то Data ONTAP требует определить членство в группе. По этой причине лучше всего создать нужные группы до того, как вы начнете заводить локальных или доменных пользователей.

Группы, имеющиеся по умолчанию: *administrators*, *backup operators*, *compliance administrators*, *guests*, *power users*, и *users*.

Для подробностей смотрите главу «How to Manage Groups» в **System Administration Guide**.

2.3 Роли (Roles)

Ролью (*role*) называется именованный набор возможностей (*capabilities*). OS Data ONTAP имеет несколько предопределенных по умолчанию ролей, а пользователь может создавать дополнительные роли, или изменять имеющиеся.

Роли по умолчанию это: *admin*, *audit*, *backup*, *compliance*, *none*, *power*, и *root*.

Для подробностей смотрите главу «How to Manage Roles» в **System Administration Guide**.

2.4 Возможности (Capabilities)

Возможность (*capability*) определена как способность, данная роли, выполнять команду, или совершить определенное действие.

Таблица 1) Типы Capability.

Тип Capability	Описание
api	Дает определенной роли возможность выполнить вызов Data ONTAP API. Тип api-* включает в себя все вызовы Data ONTAP API. Эти команды доступны только вместе с login-http-admin, так что, в общем случае, любые команды api-* должны также включать в себя возможность логина. Формат этих команд: api-<ontap-api-command>, где определяются соответствующие команды и подкоманды. Так, например, можно дать право только вывести список подкоманд, например api-system-get-info, или исполнить команду и ее подкоманды, например api-system-get-* , или даже api-system-*. api-* дает определенной роли все возможности вызова API. api-api_call_family-* дает определенной роли возможности всех вызовов API в семействе api_call_family. api-api_call Дает определенной роли возможность вызова процедуры api_call. Внимание: Для более точной настойки набора возможностей набора команд api вы можете пользоваться возможностями задания подкоманд. Пользователю с возможностями api также требуется возможность login-http-admin для выполнения выполнения вызова API.
cli	Дает определенной роли возможность выполнить одну или более команду в интерфейсе командной строки (CLI) Data ONTAP. Категория cli-* включает в себя все команды, которые пользователь может выполнить войдя в системную консоль с помощью telnet, системной консоли (COM), rsh, или ssh. Формат этих команд cli-<command>* , что означает разрешение всех команд и подкоманд. (cli-<command> означало бы команду, но БЕЗ подкоманд.) Возможности (capability) для определенных команд, таких как exportfs, должны иметь следующий синтаксис: cli-exportfs*. Это означает разрешение доступа из командной строки к команде exportfs и всем ее подкомандам. cli-export* внешне выглядит аналогично, однако НЕ разрешена. cli-* дает заданной роли права на выполнение всех доступных команд CLI. cli-cmd* дает заданной роли права на выполнение всех команд, связанных с командой cmd. Например, следующая команда дает заданной роли права на выполнение всех команд vol: useradmin role modify status_gatherer -a cli-vol* Внимание: Пользователь с заданными возможностями cli также нуждается, по крайней мере, в одной возможности login, чтобы иметь возможность выполнять команды в CLI.
compliance	Дает определенной роли возможность выполнять операции, связанные с работой compliance. Строка compliance-* дает определенной роли все возможности, связанные с compliance. compliance-privileged-delete дает определенной роли возможности выполнять привилегированное удаление данных compliance. Внимание: Возможности compliance (compliance-*) включены в набор возможностей по умолчанию для преконфигурированной роли compliance. Возможности compliance не могут быть удалены у роли compliance, или добавлены другим ролям.
filerview	Дает определенной роли возможность read-only доступа к FilerView®. Эта возможность (capability) включает в себя только filerview-readonly, которые дают заданным ролям права просматривать, но не изменять управляемые объекты в системе, управляемой через FilerView. Внимание: Нет преконфигурированой роли или группы для доступа read-only к

	FilerView. Вы должны назначить возможности `filerview-readonly` роли, а затем добавить ее в группу, до того, как вы создадите пользователя в такой группе.
`login`	Дает определенной роли возможность произвести логин с помощью telnet, console, rsh, ssh, или http-admin. `login-*` дает определенной роли возможность сделать логин по всем поддерживаемым протоколам. `login-protocol` дает определенной роли возможность сделать логин по определенному протоколу. Поддерживаемые протоколы: `login-telnet` дает определенной роли возможность сделать логин по Telnet. `login-console` дает определенной роли возможность сделать логин в serial console, по последовательному кабелю, включенному в контроллер. `login-rsh` дает определенной роли возможность сделать логин по rsh. `login-ssh` дает определенной роли возможность сделать логин по ssh. `login-http-admin` дает определенной роли возможность сделать логин по HTTP. `login-snmp` дает определенной роли возможность сделать логин по SNMPv3. `login-ndmp` дает определенной роли возможность сделать NDMP requests.
`security`	Дает определенной роли возможности, связанные с управлением безопасностью, такие как смена паролей других пользователей, или возможность вызова команды CLI `priv set advanced`. `security-*` дает определенной роли все security-возможности. `security-capability` дает определенной роли следующие security-возможности: `security-api-vfiler` Обычным образом клиент посылает вызов Data ONTAP API непосредственно в соответствующий vFiler™, если ему нужно выполнить его на конкретном vFiler. Обладание возможностью `security-api-vfiler` необходимо для того, чтобы послать вызов Data ONTAP API в физическую систему хранения, которая перенаправит его в нужный vFiler для исполнения. По умолчанию только `root` и члены группы `administrators` имеют эту возможность. `security-passwd-change-others` дает определенной роли возможности менять пароли пользователям с равными или меньшими возможностями. По умолчанию только `root` и члены группы `administrators` имеют эту возможность. `security-priv-advanced` дает определенной роли возможности доступа к команде `priv set advanced` интерфейса CLI. Это необходимо для запуска команд группы `advanced`, не использующихся в обычном процессе администрирования. Пожалуйста, обсудите со специалистом NetApp необходимость использования команд группы `advanced`. По умолчанию только `root` и члены группы `administrators` имеют эту возможность. `security-load-lclgroups` дает определенной роли возможности перезагрузить файл `lclgroups.cfg`. По умолчанию только `root` и члены группы `administrators` имеют эту возможность. `security-complete-user-control` дает определенной роли возможности создавать, изменять и удалять пользователей, группы и роли с большими возможностями. Эти пользователи обычно имеют доступ только к `cli-useradmin*` и сопутствующим командам, хотя они могут дать себе большие права. По умолчанию только `root` и члены группы `administrators` имеют эту возможность.

2.5 Все вместе

Пользователи являются членами групп, группы имеют одну или более ролей, каждая роль имеет набор возможностей. Таким способом Data ONTAP позволяет вам создать гибкие политики безопасности, соответствующие вашим организационным требованиям.

Все конфигурирование ролевой модели управления доступом производится с помощью команды useradmin, входящей в Data ONTAP. Например, добавление или изменение параметров

пользователя делается с помощью команд `useradmin user add` или `useradmin user modify`. Примеры использования приведены в главе 5 этого документа.

Так как локальные пользователи и доменные пользователи должны быть членами групп, а группам должны быть назначены одна или более ролей, наилучший порядок будет создать в первую очередь роли; затем создать группы, и назначить нужные им роли; и, наконец, создать пользователей, сделав их членами соответствующих групп.

Подробная документация о том, как использовать команду useradmin для определения локальных и доменных пользователей, групп и ролей, смотрите в **Data ONTAP System Administration Guide**. Данный документ не предполагает собой замену информации в официальном руководстве **System Administration Guide**.

3 Интеграция с Microsoft Active Directory

Возможность определить доменных пользователей, которые будут аутентифицироваться в домене Active Directory, вместо локальных средств Data ONTAP, это мощный инструмент управления большими средами хранения данных. Большинство промышленных компьютерных систем уже имеют и используют инфраструктуру Active Directory, поэтому администраторы системы хранения и другие пользователи, которым необходим административный доступ к системе хранения, обычно уже имеют учетную запись в инфраструктуре Active Directory. Использование такой возможности аутентификации вместо создания отдельной локальной учетной записи на самой системе хранения имеет ряд преимуществ:

- Свойства учетной записи администратора (username, password) одинаковы как при входе в систему хранения, так и в любую Windows-систему инфраструктуры. Когда пароль меняется, то это сразу же действует как на всех Windows-системах, так и на системах хранения.
- Изменение пароля администратора в Active Directory также «меняет» его на всех системах хранения, входящих в IT-инфраструктуру. Это значительно упрощает управление сложными инфраструктурами с большим количеством входящих в нее систем хранения.
- Использование политики безопасности, реализованной в Active Directory, может помочь и в правильном использовании учетной записи, например, заставляя администратора регулярно менять пароль, строго задав условия, такие как длину пароля, частоту смены его, недопустимость использования подбираемых по словарю слов, и так далее.
- Когда администратор покидает организацию, блокирование учетной записи этого администратора в Active Directory также вызывает блокирование доступа для этой учетной записи и на всех системах хранения организации.

Однако было бы неразумно предоставлять доступ к управлению системы хранения всем аутентифицированным учетным записям Active Directory. Очевидно, что только небольшое подмножество всех учетных записей в AD это администраторы, и только небольшое подмножество всех администраторов в большой организации занимаются управлением системами хранения. Любая система, которая обеспечивает прозрачную аутентификацию в Active Directory без разделения на авторизованных администраторов и все прочих пользователей рискует столкнуться с серьезными проблемами в безопасности. Чтобы избежать такой проблемы, Data ONTAP аутентифицирует через Active Directory администратора только в том случае, если он определен как доменный пользователь (domain user) с помощью команды `useradmin`.

Чтобы воспользоваться всеми преимуществами возможностей при миграции учетных записей администратора системы хранения с локальной на доменную систему:

- Убедитесь, что ваша система хранения работает под Data ONTAP 7G или новее.
- Воспользуйтесь командой `useradmin user delete` ,чтобы удалить локальных пользователей и их пароли.
- Воспользуйтесь командой `useradmin domainuser add` для того, чтобы дать доступ авторизованным в Active Directory учетным записям администраторов.

4 Возможности (Capabilities)

Возможности (capabilities) связанные с ролью, могут быть определены из семейства `cli` и/или из семейства `api`. Список возможностей (capabilities) различен в разных версиях Data ONTAP.

4.1 Возможности семейства Application Programming Interface (API)

Данный список взят из Manage ONTAP® SDK 3.5.1. Подробная информация о Manage ONTAP SDK имеется на сайте NOW™.

Пример назначения возможности доступа к функции aggr из интерфейса api:

```
filer*> useradmin role add newrole –a login-http-admin,api-aggr*
```

Data ONTAP API используется для доступа и управления системой хранения NetApp. Это проприетарный набор API. Этот набор включает в себя API для управления средствами безопасности (security management), управления лицензиями (license management), резервным копированием и восстановлением, репликацией данных, архивации данных, и так далее.

Таблица 2) Возможности (capability) API и их описание.

API capability	Описание
clone	Управление процессами клонирования файлов и суб-файлов
consistency	Управление consistency group
dfm	Настройки северной части DataFabric® Manager
disk	Операции с диском
ems	Доступ к API для event management system (EMS)
fc	Конфигурирование адаптеров Fibre Channel
fcp	Управление протоколом Fibre Channel
fcpport	Доступ к API управления протоколом Fibre Channel
file	Доступ к API управления операциями с файловой системой
fpolicy	Управление файловыми политиками и файлами
ic	Доступ к API управления интерконнектом кластера
igroup	Доступ к API управления операциями с initiator group
ipspace	Доступ к API управления ipspace
iscsi	Управление и наблюдение iSCSI
license	Управление лицензиями
lock	Конфигурирование и управление менеджером блокировок
lun	Доступ к API управления и наблюдения LUN-ов
nameservice	Доступ к API управления службой имен
net	Доступ к управлению сетью в Data ONTAP
nfs	Конфигурирование и управление NFS
options	Управление значениями параметров опций

perf	Доступ к счетчикам производительности различных объектов
portset	Доступ к установкам портов
priority	Доступ к API управления планировщиком приоритетов
qtree	Управление qtree
quota	Доступ к API управления квотами
reallocate	Доступ к управлению LUN, файловой оптимизации и реаллокации
rsh	Доступ по rsh
ses	Операции со SCSI enclosure services
sis	Управление дедупликацией
snaplock	Управление SnapLock®
snapmirror	Управление SnapMirror®
snapshot	Управление снэпшотами
snapvault	Управление SnapVault®
snmp	Управление SNMP и получение данных MIB
software	Управление и получение информации о установленном ПО
storage-adapter	Доступ к операциям со storage adapter
system	Доступ к API получения информации о системе
useradmin	Доступ к API конфигурирования и управления пользователями
vfiler	Управление и конфигурирование для vFiler
volume	Доступ к информации о томе и его управлению
wafl	Доступ к API для работы прикладных функций агентов

4.2 Возможности семейства Command Line Interface (CLI)

Данный список взят из руководства **Data ONTAP 7.3 Commands: Manual Page Reference, Volume 1**.

Пример назначения возможности доступа к функции aggr из интерфейса cli:

```
filer*> useradmin role add newrole –a login-ssh,cli-aggr*
```

Таблица 3) Возможности (capability) CLI и их описание.

CLI Capability	Описание
acpadmin	Доступ к команде управления alternate control path administrator
aggr	Доступ к управлению aggregates, их копированию и отображению статуса
arp	Доступ к управлению и отображению address resolution
backup	Доступ к управлению созданием резервной копии
bmc	Доступ к командам использования baseboard management controller (BMC)
bootfs	Доступ к командам доступа к boot file system
charmap	Доступ к команде управления per-volume character maps
cf	Доступ к управлению кластерными операциями takeover и giveback
cifs-*	Доступ к командам управления CIFS
cifs-access	Управление share-level access control
cifs-adupdate	Обновление учетной записи системы хранения в Active Directory
cifs-audit	Управление аудитом CIFS
cifs-broadcast	Команды вывода сообщений на пользовательские станции
cifs-changefilerpwd	Управление расписанием смены доменных паролей на системе хранения
cifs-comment	Отображение или смена описания сервера CIFS
cifs-domaininfo	Отображение информации о домене
cifs-help	Управление выводом справки для команд CIFS
cifs-homedir	Управление путями CIFS home directory
cifs-lookup	Преобразование имени в SID и наоборот

cifs-nbalias	Управление алиасами CIFS NetBIOS
cifs-prefdc	Конфигурирование и отображение предпочтительного контроллера CIFS
cifs-resetdc	Сброс соединения CIFS с контроллером домена
cifs-restart	Перезапуск сервиса CIFS
cifs-sessions	Информация о текущей активности CIFS
cifs-setup	Конфигурирование сервиса CIFS
cifs-shares	Конфигурация и отображение данных о CIFS shares
cifs-sidcache	Очистка кэша CIFS SID-to-name
cifs-stat	Печать статистики работы CIFS
cifs-terminate	Прерывание работы сервиса CIFS
cifs-testdc	Тестирование соединения системы хранения с контроллером домена
cifs-top	Отображение активности клиентов CIFS
clone	Управление клонированием файлов и субфайлов
config	Команды управления конфигурированием
date	Отображение и установка даты и времени
dd	Копирование блоков данных
df	Отображение свободного места на дисках
disk	Команды управления конфигурацией RAID
disk_fw_update	Доступ к обновлению дискового firmware
disktest	Доступ к командам тестирования состояния дисков
dlm	Доступ к управлению динамически загружаемыми модулями
dns	Отображение информации DNS и управление подсистемой DNS
download	Доступ к установке новой версии Data ONTAP
dump	Доступ к команде резервного копирования файловой системы
echo	Отображение аргументов командной строки
ems	Доступ к управлению командами *Data ONTAP event management system*
environment	Отображение информации о физических компонентах системы хранения
exportfs	Доступ к командам экспорта и управления NFS-ресурсами
fcadmin	Доступ к командам управления адаптерами Fibre Channel
fcdiag	Доступ к командам диагностики FC
fcp	Доступ к командам управления Fibre Channel target и FCP target protocol
fcstat	Доступ к статистике Fibre Channel
fctest	Доступ к команде тестирования Fibre Channel environment
file	Доступ к команде управления индивидуальными файлами
filestats	Доступ к команде сбора статистики использования файлов
flexcache	Доступ к командам томов FlexCache®
floppyboot	Описывает выборы вариантов меню при загрузке с floppy
fpolicy	Доступ к конфигурированию политик файлов
fsecurity	Доступ к командам fsecurity
fsecurity-apply	Создает security job на основе файла определений и применяет ее
fsecurity-cancel	Останавливает выполняющуюся fsecurity job
fsecurity-help	Отображает описание и примеры использования команд fsecurity
fsecurity-remove-guard	Удаляет storage-level access guard с тома или qtree
fsecurity-show	Отображает настройки security для файла или папки
fsecurity-status	Отображает статус выполняемой fsecurity job
ftp	Доступ к статистике FTP
ftpd	Доступ к File transfer protocol daemon
halt	Доступ к возможности остановить систему
help	Доступ к выводу подсказки по использованию команд

hostname	Доступ к установке имени системы хранения
httpstat	Доступ к выводу статистики HTTP
ifconfig	Доступ к конфигурированию параметров сетевых интерфейсов
ifinfo	Доступ к выводу статистики уровня драйвера сетевого интерфейса
ifstat	Доступ к выводу статистики уровня устройства сетевого интерфейса
igroup	Доступ к управлению initiator groups
ipsec	Доступ к управлению базой сертификатов ipsec и выводу статистики
ipspace	Доступ к операциям с ipspace
iscsi	Доступ к управлению сервисом iSCSI
iswt	Управление драйвером iSCSI software target (ISWT)
keymgr	Доступ к управлению ключами и сертификатами
license	Доступ к сервису управления лицензиями Data ONTAP
lock	Доступ к управлению lock records
logger	Доступ к записи сообщений в системный лог
logout	Позволяет пользователю завершить сессию telnet
lun	Доступ к командам управления lun-ами
man	Доступ к страницам системного мануала
maxfiles	Доступ к команде увеличения максимального числа файлов на томе
memerr	Выводит число ошибок памяти
mt	Доступ к команде управления магнитной лентой
nbtstat	Доступ к информации о соединениях NetBIOS over TCP
ndmpcopy	Доступ к команде переноса директорий с помощью NDMP
ndmpd	Доступ к управлению сервисом NDMP
ndp	Доступ к контролю за протоколом IPv6 neighbor discovery protocol
netdiag	Доступ к выполнению команды сетевой диагностики
netstat	Доступ к выводу сетевого статуса
nfs	Доступ к включению и выключению протокола NFS и Kerberos V5 for NFS
nfsstat	Доступ к статистике NFS
nis	Доступ к информации NIS
options	Доступ к выводу или установке опций системы хранения
orouted	Доступ к old network routing daemon
partner	Доступ к данным партнер-ноды в случае кластерного тэйковера
passwd	Доступ к изменению пароля локального администратора
ping	Доступ к отсылке пакетов ICMP ECHO_REQUEST
ping6	Доступ к отсылке пакетов ICMPv6 ECHO_REQUEST
pktt	Доступ к команде включения трассировки пакетов IP на системе хранения
portset	Доступ к командам управления portsets
priority	Доступ к командам управления приоритетами для ресурсов
priv	Доступ к привилегированным командам
qtree	Доступ к командам создания и управления qtrees
quota	Доступ к командам установки квот
rdate	Доступ к установке даты с удаленной машины
rdfile	Доступ к команде чтения файла на WAFL
reallocate	Доступ к команде реаллокации блоков файла, LUN, тома и aggregate
reboot	Доступ к команде остановки и перезапуска системы
restore	Доступ к команде восстановления данных на файловой системе
rlm	Доступ к команде работы с remote LAN module (RLM)
rmc	Доступ к командам работы с remote management controller
route	Доступ к ручному управлению таблицы маршрутизации
routed	Доступ к управлению RIP and router discovery routing daemon

rshstat	Доступ к команде вывода информации о активных сессиях rsh
rtsold	Доступ к демону router solicitation daemon
san	Доступ к командам работы с SAN
sasadmin	Доступ к командам управления адаптером Serial Attached SCSI (SAS)
sasstat	Доступ к командам вывода статистики адаптера Serial Attached SCSI (SAS)
savecore	Доступ к команде записи core dump
sectrace	Доступ к управлению правами на трассирование файлов
secureadmin	Доступ к команде безопасного администрирования системы
setup	Доступ к обновлению конфигурации системы хранения
sftp	Доступ к статистике SFTP (SSH File Transfer Protocol)
shelfchk	Доступ к команде проверки соединения между контроллером и дисками
sis	Доступ к командам управления процессами дедупликации (SIS)
snap	Доступ к командам управления и использования снэпшотов
snaplock	Доступ к командам SnapLock
snapmirror	Доступ к командам SnapMirror
snapvault	Доступ к командам SnapVault
snmp	Установка и запрос переменных SNMP
software	Доступ к команде установки/обновления Data ONTAP
source	Доступ к команде чтении и выполнения последовательности команд
stats	Доступ к команде сбора и вывода статистической информации
storage	Доступ к команде управления дисками и адаптерами SCSI/Fibre Channel
sysconfig	Доступ к команде вывода системной конфигурации
sysstat	Доступ к команде вывода статистики производительности
timezone	Доступ к команде установки и использования local time zone
traceroute	Доступ к команде вывода пути IP-пакетов
traceroute6	Доступ к команде вывода пути IP-пакетов для IPv6
ups	Доступ к управлению устройствами бесперебойного питания (UPS)
uptime	Отображение длительности работы системы
useradmin	Доступ к управлению доступом к системе хранения
version	Вывод данных о версии Data ONTAP
vfiler	Доступ к операциям с vFiler
vif	Доступ к конфигурации virtual network interface
vlan	Доступ к управлению конфигурациями интерфейса VLAN
vol	Доступ к командам управления томами, копированию и показу статуса
vscan	Доступ к антивирусному сканированию
wcc	Доступ к управлению WAFL credential cache
wrfile	Доступ к записи файла на WAFL
ypcat	Отображение значения из NIS database
ypgroup	Отображение группы кэшированных локально записей NIS server
ypmatch	Отображение соответствующих значений из NIS database
ypwhich	Отображение сервера NIS если NIS включен

5 Примеры использования

Ролевая модель разграничения доступа в Data ONTAP имеет достаточную гибкость, чтобы соответствовать требованиям почти любой IT-системы.

Как ее использовать будет зависеть от локальной политики безопасности и организационной структуры. Ниже мы приведем несколько примеров того, как RBAC может быть использована для увеличения степени безопасности и управляемости в крупной IT-системе.

Использование команды USERADMIN ROLE

```
useradmin role add role_name [-c comments] -a capability1[,...,capabilityN]
```

```
useradmin role modify role_name [-c comments] [-a capability1,...,capabilityN]
```

Команды `role add` и `role modify` используются для добавления и изменения административных ролей. На имя роли распространяются все ограничения, определенные для имени пользователя.

Опция `-a` определяет возможности, которые будут разрешены (allowed) данной роли. Эта опция полностью удаляет все текущие возможности, имеющиеся у роли, и заменяет их на указанные.

Опция `-c` задает комментарий (comment) для заданной роли. На комментарий для роли распространяются все ограничения, что и на комментарий к имени пользователя.

```
useradmin role delete role_name
```

Команда `role delete` используется для удаления административных ролей.

```
useradmin role list [role_name ]
```

Команда `role list` используется для вывода списка административных ролей. Указание имени роли приводит к выводу только указанной роли, вывод печатается в формате, показанном ниже:

```
Name:    none
Info:    Default role for no privileges.
Allowed Capabilities:
```

(В приведенном выводе видно, что роль «none» не имеет никаких возможностей (*capabilities*).)

```
Name:    power
Info:    Default role for power user privileges.
Allowed Capabilities: cli-cifs*,cli-exportfs*,cli-nfs*,cli-useradmin*,api-cifs-*,api-
nfs-*,login-telnet,login-http-admin,login-rsh,login-ssh,api-system-api-*
```

5.1 Создание SNMP ADMINISTRATOR

Создадим две роли, одну с возможностью запустить на системе хранения rsh, и выполнить команду help, и другую, которой разрешен логин любым доступным методом, и выполнение любой команды SNMP. Группе «snmp_admins» разрешен вход на систему хранения и запуск команды help через telnet, rsh, SNMPv3, и так далее, и выполнение запросов get и get next. Пользователь «wilma» наследует эти возможности из группы.

```
useradmin role add rsh_help -a login-rsh,cli-help*
```

```
useradmin role add snmp_commands -a login-*,cli-snmp*,api-snmp-*
```

```
useradmin group add snmp_admins -r rsh_help,snmp_commands
```

```
useradmin user add wilma -g snmp_admins
```

5.2 Создание пользователя, которому разрешено делать SNMP REQUEST

Пример показывает создание роли и группы, которой разрешено выполнять SNMP requests. Клиент storeMgr наследует эту возможность.

```
useradmin role add snmp_requests -a login-snmp

useradmin group add snmp_managers -r snmp_requests

useradmin user add storeMgr -g snmp_managers
```

5.3 Создание пользователя, без права доступа к консоли

Пользователь без прав доступа к консоли не сможет выполнять команды управления системой хранения, требующие CLI. Эти локальные пользователи должны быть помещены в локальные группы, не имеющие никаких ролей, содержащих такие возможности. Чтобы посмотреть имеет ли пользователь доступ, выведите список и проверьте включенные для него возможности. Если пользователь находится в группе с возможностями `cli-*` и `login-*`, то такой пользователь будет иметь доступ к консоли. Следующая команда помещает пользователя в группу, не имеющую никаких возможностей (*capabilities*), что означает отнятие всех привилегий.

```
useradmin user modify myuser -g "Guests"

useradmin user list myuser
```

5.4 Настройка доступа через System Manager

Netapp System Manager, это графическая утилита управления системой хранения. Допустим, мы хотим специальному администратору позволить использовать эту утилиту с доступом «только для просмотра». Для того, чтобы выполнить это требование, надо создать специальную роль с правами на logon и с доступом view-only. Пример содержит необходимые возможности (*capabilities*) и роли, для настройки учетной записи «только просмотр» для контейнера «storage» дерева NetApp System Manager.

Внимание: Этот пример использует возможности NetApp System Manager 1.0.1 и Data ONTAP 7.3.2.

Создание ролей

В примере создаются семь ролей; можно также использовать только одну роль со всеми необходимыми возможностями (*capabilities*). Разбивка их по ролям была сделана для простоты и иллюстративности.

Создаем роль для входа (login). Эта роль позволяет доступ к контроллеру системы хранения:

```
useradmin role add nsm-login -a login-http-admin,api-system-get-*
```

Создаем общую роль «view-only». Эта роль имеет все общие возможности для доступа к контейнеру «storage» в NetApp System Manager GUI:

```
useradmin role add nsm-view –a api-aggr-list-info,api-disk-sanown-list-info,api-license-list-info,api-options-get,api-perf-object-get-instances,api-snmp-status,api-volume-list-info*,cli-priv,api-aggr-options-list-info,api-aggr-check-spare-low
```

Создаем роль для просмотра контейнера «volumes»:

```
useradmin role add nsm-volumes-view -a api-volume-get-root-name,api-snapshot-reserve-list-info,api-volume-get-language,api-volume-options-list-info,cli-date
```

Создаем роль для просмотра контейнера «shared folders»:

```
useradmin role add nsm-sharedfolders-view -a api-cifs-share-list-iter*,api-nfs-exportfs-list-rules,api-cifs-session-list-iter*
```

Создаем роль для просмотра контейнера «qtrees»:

```
useradmin role add nsm-qtree-view -a api-qtree-list-iter*
```

Создаем роль для просмотра контейнера «disks»:

```
useradmin role add nsm-disk-view -a api-system-cli,api-disk-list-info,cli-options
```

Создаем роль для просмотра контейнера «aggregates»:

```
useradmin role add nsm-aggr-view -a api-aggr-get-root-name,api-snapshot-list-info
```

Вывод команды `useradmin role list` должен выглядеть следующим образом:

```
Name:    nsm-aggr-view
Info:
Allowed Capabilities: api-aggr-get-root-name,api-snapshot-list-info
Name:    nsm-disk-view
Info:
Allowed Capabilities: api-system-cli,api-disk-list-info,cli-options
Name:    nsm-login
Info:
Allowed Capabilities: login-http-admin,api-system-get-*
Name:    nsm-qtree-view
Info:
Allowed Capabilities: api-qtree-list-iter*
Name:    nsm-sharedfolders-view
Info:
Allowed Capabilities: api-cifs-share-list-iter*,api-nfs-exportfs-list-rules,api-cifs-session-list-iter*
Name:    nsm-view
Info:
Allowed Capabilities: api-aggr-check-spare-low,api-aggr-list-info,api-aggr-options-list-info,api-disk-sanown-list-info,api-license-list-info,api-options-get,api-perf-object-get-instances,api-snmp-status,api-volume-list-info*,cli-priv,security-priv-advanced,cli-registry
Name:    nsm-volumes-view
Info:
Allowed Capabilities: api-volume-get-root-name,api-snapshot-reserve-list-info,api-volume-get-language,api-volume-options-list-info,cli-date
```

Создание группы

Когда все нужные роли уже созданы, необходимо создать группу.

```
useradmin group add nsm-storage-view -r nsm-login,nsm-view,nsm-volumes-view,nsm-sharedfolders-view,nsm-qtree-view,nsm-disk-view,nsm-aggr-view
```

Минимальный набор ролей для группы «view-only» это роли `nsm-login` и `nsm-view`.

Создание или добавление пользователя группе

Это действие делается с помощью команд `useradmin user` или `useradmin domainuser`.

6 Выводы

Ролевая схема разграничения доступа в Data ONTAP позволяет администраторам системы хранения и администраторам безопасности назначать административные права согласно политике безопасности организации. Она может помочь достичь соответствия внутренним политикам безопасности компании, защитить от риска случайного изменения конфигурации неавторизованным на это сотрудником, а также иных случаев «пользовательских ошибок». Кроме этого, с ее помощью можно организовать делегирование полномочий администратора без риска допуска неподготовленного сотрудника к деструктивным командам.