Internet Engineering Task Force (IETF)
Request for Comments: 8341
STD: 91
Obsoletes: 6536
Category: Standards Track
ISSN: 2070-1721

A. Bierman
YumaWorks
M. Bjorklund
Tail-f Systems

March 2018

Модель управления доступом NETCONF

Network Configuration Access Control Model

Аннотация

Стандартизация интерфейсов настройки конфигурации сети для использования с протоколами NETCONF[1] или RESTCONF требует структурированной и защищённой рабочей среды, которая пригодна для использования человеком и может поддерживать оборудование разных производителей. Для этого нужны стандартные механизмы ограничения доступа к протоколам NETCONF и RESTCONF для отдельных пользователей заданным подмножеством всех операций и содержимого NETCONF и RESTCONF. Данный документ определяет такую модель управления доступом.

Данный документ отменяет RFC 6536.

Статус документа

Этот документ является проектом стандарта (Internet Standards Track).

Документ является результатом работы IETF[2] и представляет собой согласованное мнение сообщества IETF. Документ был вынесен на публичное рассмотрение и одобрен для публикации IESG[3]. Дополнительная информация о документах Internet Standard представлена в разделе 2 документа RFC 7841.

Информация о текущем статусе этого документа, обнаруженных ошибках и способах обратной связи может быть найдена по ссылке https://www.rfc-editor.org/info/rfc8341.

Оглавление

[1]Network Configuration.
[2]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[3]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

1. Введение

Протоколы NETCONF и RESTCONF не обеспечивают каких-либо стандартных механизмов ограничения доступа пользователей к протокольным операциям и содержимому.

Существует необходимость интероперабельного управления доступом к выбранным администратором частям содержимого NETCONF и RESTCONF в рамках отдельного сервера.

Этот документ решает вопросы управления доступом к операциям и содержимому протоколов NETCONF [RFC6241] и RESTCONF [RFC8040]. Документ включает три основных раздела.

1. Цели управления доступом.
2. Модель управления доступом для NETCONF (NACM).
3. Модель данных YANG (ietf-netconf-acm.yang).

YANG версии 1.1 [RFC7950] добавляет две новых конструкции, для которых требуется специальный контроль доступа. Оператор action похож на оператор rpc, за исключением того, что он размещается в узле данных. Оператор notification также может размещаться в узле данных.

1.1. Терминология

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

Приведённые ниже термины определены в [RFC8342] и не переопределяются здесь:

- datastore - хранилище данных;
- configuration datastore – хранилище конфигурации;
- conventional configuration datastore – традиционное (обычное) хранилище данных конфигурации;
- candidate configuration datastore – хранилище будущей конфигурации, хранилище-кандидат;
- running configuration datastore – хранилище рабочей конфигурации;
- startup configuration datastore - хранилище стартовой конфигурации;
- operational state datastore – хранилище рабочего состояния;
- client - клиент;
- server - сервер.

Приведённые ниже термины определены в [RFC6241] и не переопределяются здесь:

- protocol operation - протокольная операция;
- session - сессия;
- user - пользователь.

Приведённые ниже термины определены в [RFC7950] и не переопределяются здесь:

- action - действие;
- data node - узел данных;
- data definition statement - оператор определения данных.

Приведённые ниже термины определены в [RFC8040] и не переопределяются здесь:

- data resource - ресурс данных;
- datastore resource - ресурс хранилища данных;
- operation resource - операционный ресурс;
- target resource - целевой ресурс.

Приведённый ниже термин определён в [RFC7230] и не переопределяется здесь:

- request URI - идентификатор запроса.

Ниже приведены определения других используемых в документе терминов.

access control – контроль доступа
Защитное свойство, обеспечиваемое сервером, который позволяет администратору ограничивать доступ к протокольным операциям и данным на основе различных критериев.

access control model (ACM) – модель контроля доступа
Концептуальная модель, используемая для настройки и отслеживания процедур управления доступом, которые администратор хочет применить в конкретной политике контроля доступа.

access control rule – правило контроля доступа
Критерий, используемый для решения вопроса о предоставлении доступа к конкретной операции.

access operation – операция доступа
Способ получения запросом доступа к концептуальному объекту (none - нет, read - чтение, create - создание, delete - удаление, update - обновление или execute - исполнение).

data node hierarchy и иерархия узла данных
Иерархия узлов данных, указывающая конкретный узел action или notification в хранилище данных.

recovery session – сеанс восстановления
Специальная административная сессия, имеющая неограниченный доступ NETCONF без применения каких-либо правил контроля. Механизмы, используемые сервером для определения того, что сеанс является восстановительным, зависят от реализации и выходят за рамки этого документа.

write access – доступ для записи
Общее обозначение операций create, delete и update.

1.2. Отличия от RFC 6536

Процедуры и модель данных NACM были обновлены для поддержки новых возможностей моделирования в версии языка YANG 1.1. Операторы action и notification могут использоваться с узлами данных для определения операций и уведомлений в конкретной модели данных.

Важным применением этих новых операторов YANG является повышение детализации контроля доступа по сравнению с возможностями, предоставляемыми операторами верхнего уровня rpc и notification. Новые операторы action и notification используются внутри узлов данных и доступ к действиям или уведомлениям может быть ограничен для конкретных узлов данных.

Добавлена поддержка протокола RESTCONF, операции которого похожи на протокольные операции NETCONF, что позволило просто сопоставить имеющиеся процедуры и модель данных NACM.

Было разъяснено поведение доступа к узлу данных при совпадении пути для включения соответствующих нисходящих узлов указанного пути.

Разъяснено поведение в части прав доступа к операции <edit-config> для указания того, что право записи не требуется для узлов данных, которые неявно меняются за счёт побочных эффектов (типа вычисления операторов YANG when или неявного удаления при создании узла данных в другой ветви оператора YANG choice).

Раздел «Вопросы безопасности» был обновлён в соответствии с документом «YANG module security guidelines» [YANG-SEC]. Отметим, что модуль YANG в этом документе не определяет новых операций RPC.

2. Цели управления доступом

В этом разделе описаны цели разработки модели управления доступом к NETCONF, представленной в разделе 3.

2.1. Точки управления доступом

NETCONF позволяет разработчикам серверов добавлять свои протокольные операции и язык моделирования данных YANG поддерживает это. Операции могут быть определены в стандартных или фирменных модулях YANG.

Невозможно спроектировать ACM для NETCONF, основанную лишь на статическом наборе стандартных протокольных операций, определённых в самом NETCONF, подобно некоторым другим протоколам. Поскольку могут быть приняты

некие допущения о произвольных операциях протокола, архитектурные компоненты сервера NETCONF требуется защитить в трёх концептуальных точках контроля.

Эти точки контроля показаны на рисунке 1 и кратко описаны ниже.

Протокольные операции
Разрешение на вызов конкретных операций протокола.

Хранилище данных
Разрешение считывать и/или изменять конкретные узлы данных внутри хранилища.

Уведомления
Разрешение получать уведомления о конкретных типах событий.

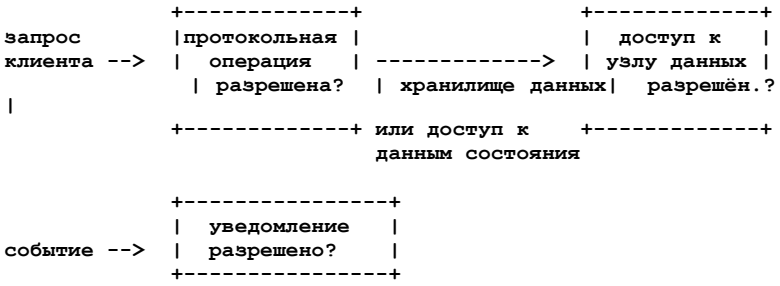

Рисунок 1.

2.2. Простота

Есть опасение, что сложная ACM не получит широкого распространения по причине трудностей с использованием. Конфигурация системы контроля доступа должна быть как можно более простой. Простые задачи общего назначения должны легко настраиваться и не требовать специальных знаний. Для более сложных задач могут применяться дополнительные механизмы, требующие определённого опыта.

Единый набор правил контроля доступа должен обеспечивать возможность управления вызовами всех операций протокола NETCONF, доступом к хранилищам и уведомлениями о любых событиях.

Контроль доступа должен определяться с помощью небольшого и понятного набора разрешений и при этом должен обеспечивать полное управления доступом к хранилищам данных.

2.3. Процедурный интерфейс

NETCONF использует модель RPC[1] и расширяемый набор протокольных операций. Требуется контроль доступа для любой возможной операции протокола.

2.4. Доступ к хранилищу данных

Необходимо контролировать доступ к конкретным узлам и субдеревьям в хранилище данных независимо от протокольных операций (стандартных или фирменных), используемых для доступа к хранилищу.

2.5. Пользователи и группы

Требуется возможность настройки правил доступа для одного пользователя или настраиваемой группы пользователей.

В ACM требуется поддержка концепции административных групп, позволяющей чётко различать учётные записи администраторов (root account) и других пользователей с меньшими привилегиями. Администратор должен иметь возможность настройки групп.

Необходима возможность передачи полномочий по сопоставлению пользователей с группами централизованному серверу (например, RADIUS [RFC2865] [RFC5607]). Поскольку проверка подлинности выполняется транспортным уровнем и RADIUS выполняет аутентификацию предоставление полномочий сервису одновременно, от транспортного протокола требуется способность сообщать набор имён групп, связанных с пользователем сервера. Администратору необходимо обеспечить возможность отключить использование этих имён групп в ACM.

2.6. Обслуживание

Требуется обеспечить возможность отключения части или всех процедур выполнения модели контроля доступа без удаления каких-либо правил.

2.7. Возможности настройки

Требуются подходящие механизмы настройки и управления, позволяющие упростить администратору все аспекты управления поведением ACM. Для этого нужна стандартная модель данных, подходящая для использования с протокольной операцией <edit-config>. Требуется поддержка правил управления доступом для ограничения доступа к конкретным субдеревьям внутри конфигурационного хранилища.

2.8. Идентификация требующего защиты содержимого

Одним из важнейших аспектов документации для модели данных и одной из наиболее важных проблем развёртывания является идентификация связанного с безопасностью содержимого. Это относится к протокольным операциям NETCONF, а не просто к данным или уведомлениям.

Чувствительные в плане безопасности объекты необходимо указывать в разделе RFC «Вопросы безопасности». Это хорошо, но не достаточно в силу приведённых ниже причин.

[1]Remote Procedure Call - вызов удалённых процедур.

- Такой подход, ограничивающийся документированием, вынуждает администраторов изучать RFC и определять наличие потенциальных рисков, вносимых моделью данных.
- Если риски безопасности идентифицированы, администратор должен дополнительно изучить текст RFC и узнать способы снижения рисков.
- ACM на каждом сервере требуется настроить для снижения рисков безопасности, например, требуя привилегированного доступа к операциям чтения и записи для конкретных данных, указанных в разделе «Вопросы безопасности».
- Если ACM не настроена заранее, возникает интервал уязвимости между загрузкой новой модели данных а настройкой, включением и отладкой новых правил контроля доступа для этой модели.

Часто администраторы просто хотят отключить разрешенный по умолчанию доступ к защищённому содержимому, что на сервере невозможно внести неадекватные или вредоносные изменения. Это позволяет использовать по умолчанию более мягкие правила без существенного риска для безопасности.

Разработчик модели данных должен быть способен использовать машиночитаемые операторы для идентификации содержимого, которое требуется защитить по умолчанию. Это даёт клиенту и серверу средства автоматической идентификации связанные с моделью данных риски безопасности путём запрета доступа к деликатным данным пока пользователю не предоставлено явное разрешение выполнять запрошенную операцию доступа.

3. Модель управления доступом для NETCONF (NACM)

3.1. Обзор

В этом разделе представлен общий обзор структуры модели управления доступом. Описана модель обработки протокольных сообщений NETCONF и концептуальные требования к контролю доступа в рамках модели.

3.1.1. Свойства

Возможности модели NACM перечислены ниже.

- Обеспечивается независимый контроль доступа к RPC, действиям,данным и уведомлениям.
- Поддерживается концепция восстановительных сессий, но конфигурация сервера для решения таких задач выходит за рамки этого документа. Такие сессии выполняются в обход всех правил доступа для того, чтобы инициализировать или исправить конфигурацию NACM.
- Используется просто и понятный набор разрешений для хранилища данных.
- Поддержка меток безопасности YANG (например, оператор nacm:default-deny-write) позволяет автоматически исключать доступ к чувствительным данным по умолчанию.
- Обеспечиваются раздельные режимы, используемые по умолчанию для чтения, записи и выполнения.
- Правила контроля доступа применяются к настраиваемым группам пользователей.
- Процедуры выполнения контроля доступа могут быть отключены в процессе работы без удаления каких-либо правил (для отлаживания при возникновении проблем).
- Клиент может обеспечивать подсчёт отвергнутых запросов на выполнение протокольных операций и запись в хранилище данных.
- Используются простые неограниченные идентификаторы экземпляров YANG для настройки правил доступа к конкретным узлам данных.

3.1.2. Внешние зависимости

Для целей сетевого управления в этом документе используются протоколы NETCONF [RFC6241] и RESTCONF [RFC8040].

Язык моделирования данных YANG [RFC7950] служит для определения моделей данных, используемых с NETCONF или RESTCONF. YANG также используется для моделей данных в этом документе.

3.1.3. Модель обработки сообщения

На рисунке 2 показана концептуальная модель потока сообщений, включая точки, где применяется контроль доступа в процессе обработки сообщений NETCONF.

Операции RESTCONF отображаются на модель контроля доступа по методу HTTP и классу ресурсов, используемому в операции. Например, метод POST для ресурса данных считается доступом для записи в узел, а метод POST для операции считается доступом operation.

Прямоугольник pre-read data node acc. ctl на рисунке указывает групповой доступ для чтения, поскольку он относится к предкам узла данных для действия или уведомления. Например, если действие определено как /interfaces/interface/reset-interface, группа должна иметь полномочия (1) читать /interfaces и /interfaces/interface, а также (2) выполнять /interfaces/interface/reset-interface.

Приведённая ниже последовательность концептуальных шагов обработки верхнего уровня выполняется для каждого принятого сообщения <rpc> при включённом контроле доступа.

- Для каждой активной сессии контроль доступа выполняется индивидуально для всех сообщений <rpc> (кроме <close-session>), полученных сервером, если сессия не идентифицирована как восстановительная.

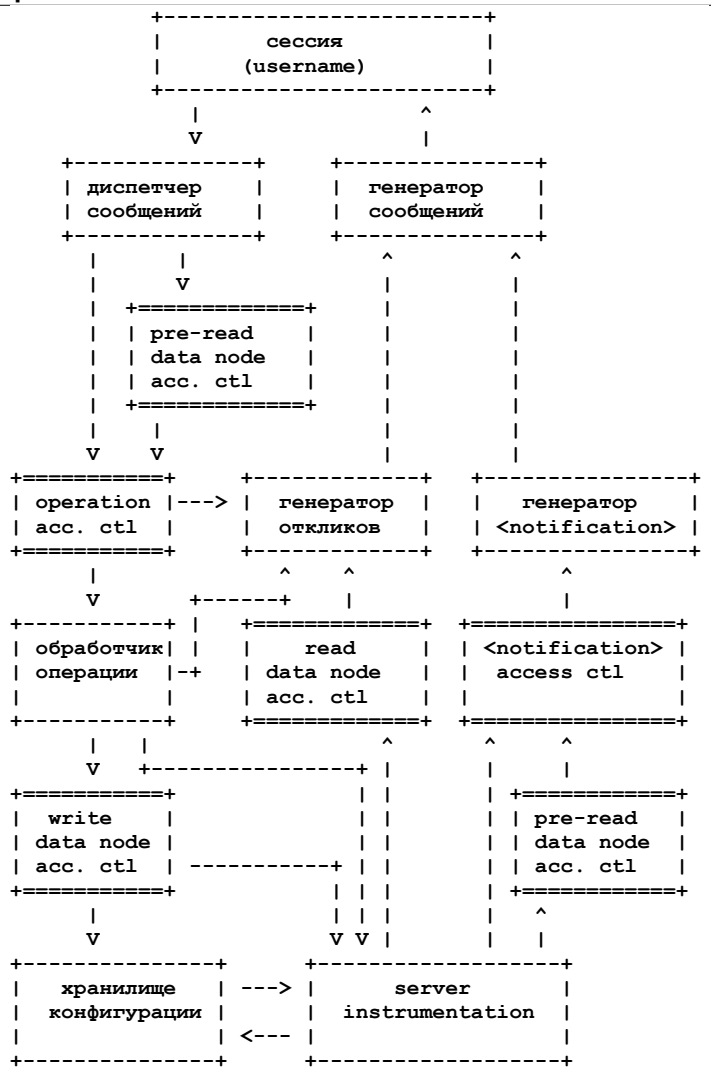

Рисунок 2.

- Если вызвана операция <action>, определённая в [RFC7950], доступ к чтению требуется для всех экземпляров в иерархии узлов данных, идентифицирующих указанное действие в хранилище данных, а также требуется доступ к исполнению для узла action. Если пользователь не имеет права читать все указанные узлы данных и выполнять действие, запрос отвергается с возвратом ошибки access-denied.
- В остальных случаях, если пользователь не имеет права выполнять указанную операцию протокола, запрос отвергается с возвратом ошибки access-denied.
- При осуществлении протокольной операцией доступа к хранилищу данных, сервер проверяет наличие у пользователя полномочий для доступа к узлам этого хранилища. Если пользователь не имеет полномочий для выполнения запрошенной операции доступа, запрос отвергается с возвратом ошибки access-denied.

Приведённая ниже последовательность концептуальных шагов обработки выполняется для каждого события с генерацией уведомления при включённом контроле доступа.

- Серверное оборудование генерирует уведомление для определённой подписки.
- Если в субдереве данных задан оператор notification, как указано в [RFC7950], доступ к чтению требуется для всех экземпляров в иерархии узлов данных, идентифицирующих указанное уведомление в хранилище данных, а также к чтению узла notification. Если пользователь не имеет полномочий для чтения всех заданных узлов данных и узла notification, уведомление для этой подписки отбрасывается.
- Если notification является оператором верхнего уровня, элемент, выполняющий контроль доступа, проверяет тип связанного с уведомлением события и при отсутствии у пользователя полномочий на чтение, уведомление для этой подписки отбрасывается.

3.2. Доступ к хранилищу данных

Одни и те же правила контроля доступа применяются ко всем хранилищам данных, которые поддерживают NACM, например, хранилищу-кандидату или хранилищу рабочей конфигурации.

Все обычные хранилища данных и рабочее хранилище контролируются NACM. Локальные и удалённые файлы или хранилища, доступ к которым осуществляется через параметр <url>, не контролируются NACM.

3.2.1. Отображение новых хранилищ данных в NACM

Возможно, что с течением времени будут определены новые хранилища данных для использования с NETCONF. NACM **может** применяться к другим хранилищам, в которых права доступа определены подобно NACM. Для применения NACM к новому хранилищу данных, для такого хранилища должно быть определено отображение на права

доступа NACM CRUDX[1]. Возможно, что применима будет лишь часть прав доступа NACM. Например, для хранилищ с доступом только на чтение могут потребоваться лишь контроль поиска информации. Операции и права доступа, не поддерживающие модель NACM CRUDX, выходят за рамки этого документа. Хранилищу данных не требуется использовать NACM, например, спецификация хранилища может определять другой метод или не применять контроль доступа совсем.

3.2.2. Права доступа

Для контроля доступа ко всем протокольным операциям, включая фирменные расширения стандартного набора операций протокола, достаточно небольшого набора жёстко заданных прав доступа к хранилищу.

Модель CRUDX может поддерживать все протокольные операции:

- создание - позволяет клиенту добавлять новые экземпляры узлов данных в хранилище;
- чтение - позволяет клиенту читать экземпляры данных из хранилища или получать уведомления о событиях;
- обновление - позволяет клиенту обновлять имеющиеся экземпляры узлов данных в хранилище;
- удаление - позволяет клиенту удалять экземпляры узлов данных из хранилища;
- eXec - позволяет клиенту выполнять операции.

3.2.3. Методы RESTCONF

Протокол RESTCONF использует методы HTTP для выполнения операций с хранилищами данных, подобно протоколу NETCONF. Процедуры NACM разрабатывались для протокола NETCONF, поэтому методы RESTCONF были отображены на операции NETCONF для целей обработки контроля доступа. Процедуры исполнения правил, описанные в этом документе, применимы к обоим протоколам, если явно не указано иное.

При обработке запросов RESTCONF к ресурсам данных нужно рассматривать URI запросов, как описано ниже.

- Для запросов HEAD и GET любые узлы данных, являющиеся предками узлов целевого ресурса, для целей контроля доступа считаются частью поискового запроса.
- Для запросов PUT, PATCH и DELETE любые узлы данных, являющиеся предками узлов целевого ресурса, для целей контроля доступа на считаются частью запроса на редактирование. Операцией доступа для таких запросов считается none (нет операции). Редактирование начинается с целевого ресурса.
- Для запросов POST к ресурсам данных любые узлы данных, указанные в URI запроса, включая целевой ресурс, для целей контроля доступа не считаются частью запроса на редактирование. Операцией доступа для таких запросов считается none. Редактирование начинается на дочернем узле целевого ресурса, заданного в теле сообщения.

Контроль доступа применяется для всех запросов RESTCONF. В приведённой ниже таблице приведены сопоставления запросов с операциями протокола NETCONF. Значение none показывает, что операция NACM не применяется к данному методу RESTCONF.

Таблица 1. Сопоставление методов RESTCONF с NETCONF.

Метод	***Класс ресурсов***	***Операция NETCONF***	***Операция доступа***
OPTIONS	все	none	none
HEAD	все	<get>, <get-config>	read
GET	все	<get>, <get-config>	read
POST	хранилище, данные	<edit-config>	create
POST	операция	заданная операция	execute
PUT	данные	<edit-config>	create, update
PUT	хранилище	<copy-config>	update
PATCH	данные, хранилище	<edit-config>	update
DELETE	данные	<edit-config>	delete

3.2.4. Операции <get> и <get-config>

Права доступа NACM не связаны напрямую с протокольными операциями <get> и <get-config>, а применяются ко всем операциям <rpc>, которые приводить к операции read для целевого хранилища данных. В этом параграфе описано, как эти права доступа применяются к конкретным операциям доступа, поддерживаемым протокольными операциями <get> и <get-config>.

Узлы данных, к которым клиент не имеет доступа на чтение, просто опускаются вместе с их потомками из сообщения <rpc-reply>. Это делается для того, чтобы обеспечить возможность корректной работы фильтров NETCONF для <get> и <get-config> вместо возврата ошибки access-denied в результате срабатывания фильтров при отсутствии полномочий на чтение некоторых узлов данных. Для целей фильтрации NETCONF критерии выбора применяются к подмножеству узлов, которые пользователь имеет право читать, а не ко всему хранилищу данных.

3.2.5. Операция <edit-config>

Права доступа NACM не связаны напрямую с атрибутом «операции» <edit-config>, хотя они похожи. Права доступа NACM применяются ко всем протокольным операциям, которые в результате будут приводить к определённой операции доступа к целевому хранилищу данных. В это параграфе описано как эти права доступа применяются к конкретным операциям доступа, поддерживаемым протокольной операцией <edit-config>.

Если реальной операцией доступа для отдельного узла данных является none (т. е. default-operation=none), контроль доступа для этого узла не применяется. Это требуется для того, чтобы разрешить доступ к субдереву в более крупной структуре данных. Например, пользователь может иметь полномочия на создание новых записей в списке /interfaces/interface, но не иметь полномочий для создания или удаления его родительского контейнера (/interfaces).

[1]Create, Read, Update, Delete, eXec - создание, чтение, обновление, удаление, исполнение.

Если контейнер /interfaces уже имеется в целевом хранилище, при редактировании списка /interfaces/interface эффективной операцией для узла /interfaces будет none.

Если протокольная операция будет приводить к созданию узла в хранилище данных, а пользователь не имеет полномочий на операцию create для этого узла, операция будет отвергнута с ошибкой access-denied.

Если протокольная операция будет приводить к удалению узла в хранилище данных, а пользователь не имеет полномочий на операцию delete для этого узла, операция будет отвергнута с ошибкой access-denied.

Если протокольная операция будет приводить к изменению узла в хранилище данных, а пользователь не имеет полномочий на операцию update для этого узла, операция будет отвергнута с ошибкой access-denied.

Операция <edit-config> для слияния или замены может включать узлы данных, которые являются неизменяемой частью имеющегося хранилища данных. Например, узел container или list может служить для именования, но не изменения соответствующего узла в хранилище. Такие неизменяемые узлы данных игнорируются сервером и не требуют от клиента каких-либо прав доступа.

Операция <edit-config> для слияния может включать узлы данных, но не включать отдельные дочерние узлы, которые присутствуют в хранилище. Эти отсутствующие узлы данных в области действия операции слияния <edit-config> игнорируются сервером и не требуют от клиента каких-либо прав доступа.

Содержимое конкретных узлов с ограничениями доступа **недопустимо** включать в какие-либо элементы откликов <rpc-error>.

Операция <edit-config> может приводить к неявному созданию или удалению узлов в результате неявных побочных эффектов запрошенной операции. Например выражение оператора YANG when может давать разные результаты, в зависимости от которых узлы данных могут создаваться или удаляться или при создании узла данных в одной из ветвей оператора YANG choice узлы в других вариантах этого оператора могут неявно удаляться. Для узлов данных, которые неявно изменяются в результате побочных эффектов другой разрешённой операции, не требуется прав доступа NACM.

3.2.6. Операция <copy-config>

Контроль доступа для операции <copy-config> требует специального рассмотрения, поскольку эта операция позволяет администратору полностью заменить содержимое целевого хранилища.

Если источником протокольной операции <copy-config> является хранилище рабочей конфигурации, а целью - хранилище стартовой конфигурации, от клиента требуется лишь доступ к выполнению операции <copy-config>.

В остальных случаях используются приведённые ниже правила.

- Если источником операции <copy-config> является хранилище, узлы данных, к которым у клиента нет доступа на чтение, просто опускаются.
- Если целью операции <copy-config> является хранилище данных, клиенту нужен доступ к обновляемым узлам. В частности должны выполняться приведённые ниже условия.
    - Если протокольная операция ведёт к созданию узла в хранилище, а пользователь не имеет для этого узла права на создание (create), протокольная операция отвергается с ошибкой access-denied.
    - Если протокольная операция ведёт к удалению узла в хранилище, а пользователь не имеет для этого узла права на удаление (delete), протокольная операция отвергается с ошибкой access-denied.
    - Если протокольная операция ведёт к обновлению узла в хранилище, а пользователь не имеет для этого узла права на обновление (update), протокольная операция отвергается с ошибкой access-denied.

3.2.7. Операция <delete-config>

Доступ к протокольной операции <delete-config> по умолчанию отвергается. Лист exec-default не применяется к этой операции протокола. Для разрешения вызова этой операции правила контроля доступа должны быть заданы явно, если сессия не является восстановительной.

3.2.8. Операция <commit>

Сервер **должен** точно определить узлы в хранилище рабочей конфигурации, которые реально отличаются от представляемых, и проверять права доступа create, update и delete лишь для этого набора узлов, который может оказаться пустым.

Например, если сессия может читать все хранилище, но изменять лишь один лист, эта сессия должна иметь право редактирования и представления (commit) лишь для этого листа.

3.2.9. Операция <discard-changes>

От клиента требуется лишь право выполнять протокольную операцию <discard-changes>. Прав доступа к хранилищу не требуется.

3.2.10. Операция <kill-session>

Операция <kill-session> не меняет хранилища напрямую, однако она позволяет из одной сессии прервать другую, которая могла редактировать хранилище данных.

Доступ к протокольной операции <kill-session> по умолчанию отвергается. Лист exec-default не применяется к этой операции протокола. Для разрешения вызова этой операции правила контроля доступа должны быть заданы явно, если сессия не является восстановительной.

3.3. Компоненты модели

В этом разделе определены концептуальные компоненты, относящиеся к модели контроля доступа.

3.3.1. Пользователи

Пользователь (user) является концептуальным элементом, с которым связаны полномочия доступа, предоставленные для отдельной сессии. Пользователь указывается строкой (именем), которая уникальна в масштабе сервера.

Как описано в [RFC6241], строка имени пользователя выводится из транспортного уровня в процессе организации сессии. Если транспортный уровень не может проверить подлинность пользователя, сессия прерывается.

3.3.2. Группы

Доступ к конкретной операции протокола NETCONF предоставляется для сессии. Сессия связана с группой (т. е. не с пользователем).

Группы идентифицируются по именам. Имена уникальны в масштабе сервера.

Контроль доступа применяется на уровне группы. Группа может быть пустой или включать некоторое число членов.

Члены группы идентифицируются строками имён пользователей.

Один и тот же пользователь может быть членом множества групп.

3.3.3. Сеанс восстановления при аварии

Сервер **может** поддерживать механизм восстановительных сессий, которые выполняются в обход применения контроля доступа. Это полезно для ограничения начального доступа и починки неисправной конфигурации контроля доступа.

3.3.4. Глобальные элементы исполнения

Имеется пять глобальных элементов управления, которые помогают при выполнении контроля доступа.

3.3.4.1. Переключатель enable-nacm

Глобальный переключатель enable-nacm служит для включения и отключения процедур контроля доступа. Когда этот переключатель имеет значение true, все запросы проверяются на соответствие правилам контроля доступа и выполняются только разрешённые запреты на доступ. При значении глобального переключателя false все запросы на доступ разрешены.

3.3.4.2. Переключатель read-default

Переключатель read-default определяет принятый по умолчанию режим доступа к получению данных в откликах и уведомлениях. Когда глобальный переключатель enable-nacm имеет значение true, данный переключатель используется при отсутствии совпадений с правилами контроля доступа, которые явно разрешают или запрещают доступ к запрошенному хранилищу данных или типу уведомления.

Когда этот глобальный переключатель имеет значение permit и нет совпадения с правилом контроля доступа к хранилищу для чтения или получения уведомлений о событиях, такой доступ разрешён.

Когда этот глобальный переключатель имеет значение deny и нет совпадения с правилом контроля доступа к хранилищу для чтения или получения уведомлений о событиях, доступ отвергается. Это означает, что запрошенные данные не будут переданы клиенту (см п. 11 в параграфе 3.4.5).

3.3.4.3. Переключатель write-default

Переключатель write-default определяет принятый по умолчанию режим доступа к изменению конфигурационных данных. Когда глобальный переключатель enable-nacm имеет значение true, данный переключатель используется при отсутствии совпадений с правилами контроля доступа, которые явно разрешают или запрещают доступ для записи в запрошенное хранилище.

Когда этот глобальный переключатель имеет значение permit и нет совпадения с правилом контроля доступа к хранилищу для записи, такой доступ разрешён.

Когда этот глобальный переключатель имеет значение deny и нет совпадения с правилом контроля доступа к записи в запрошенное хранилище, такой доступ отвергается (см п. 12 в параграфе 3.4.5).

3.3.4.4. Переключатель exec-default

Переключатель exec-default определяет принятый по умолчанию режим доступа к выполнению протокольных операций. Когда глобальный переключатель enable-nacm имеет значение true, данный переключатель используется при отсутствии совпадений с правилами контроля доступа, которые явно разрешают или запрещают доступ к исполнению запрошенной операции протокола NETCONF.

Когда этот глобальный переключатель имеет значение permit и нет совпадения с правилом контроля доступа к запрошенной операции протокола NETCONF, такой доступ разрешён.

Когда этот глобальный переключатель имеет значение deny и нет совпадения с правилом контроля доступа к запрошенной операции протокола NETCONF, такой доступ отвергается (см п. 12 в параграфе 3.4.4 и п. 13 в параграфе 3.4.5).

3.3.4.5. Переключатель enable-external-groups

Когда этот глобальный переключатель имеет значение true, имена групп, сообщённые транспортным уровнем для сессии, используются вместе с заданными локально именами групп для определения правил контроля доступа в сессии.

При значении этого переключателя false имена групп, сообщённые транспортным уровнем, игнорируются NACM.

3.3.5. Правила контроля доступа

В NACM доступны 4 типа правил, перечисленные ниже.

module – правило для модуля
: Управляет доступом к определениям в модуле YANG, указанном именем.

protocol operation – правило для протокольной операции
: Управляет доступом к конкретной операции протокола, указанной именем и модулем YANG.

data node – правило для узла данных
: Управляет доступом к конкретному узлу данных (и его потомкам), указанному путём в концептуальном документе XML для узла данных.

Notification – правило для уведомлений
: Управляет доступом к конкретному типу уведомлений, указанному именем и модулем YANG.

3.4. Процедуры исполнения контроля доступа

Необходимо выполнить 6 этапов проверки, 4 из которых относятся к модели обработки сообщений NETCONF (параграф 3.1.3):

1. начальные операции;
2. организация сессии;
3. обработка ошибок access-denied;
4. проверка пригодности входящих сообщений RPC;
5. проверка доступа к узлу данных;
6. полномочия для исходящих <notification>.

Кроме того, нужно учитывать стартовый режим сервера NETCONF, организацию сессии, а также процедуры обработки ошибок access-denied.

Сервер **должен** использовать правила контроля доступа, действовавшие в момент начала обработки сообщения. Правила обработки сообщения **должны** действовать в течение всего процесса обработки.

3.4.1. Начальные операции

При первом запуске сервера NETCONF конфигурация контроля доступа может отсутствовать. Если это не так, серверу **недопустимо** разрешать какой-либо доступ для записи в любой сессии, кроме восстановительной.

Правила контроля доступа применяются каждый раз, когда пользовательская сессия инициирует запрос. Контроль доступа не применяется для инициированных сервером запросов доступа типа начальной загрузки хранилища рабочей конфигурации при старте.

3.4.2. Организация сессии

Модель контроля доступа применяется к чётко сформированному содержимому XML, передаваемому между клиентом и сервером после организации сессии и успешного обмена сообщениями <hello>.

Когда сессия организована и подлинность пользователя подтверждена, транспортный уровень передаёт имя пользователя и (возможно пустой) набор групп, связанных с пользователем, серверу NETCONF. Сервер будет применять правила контроля доступа на основе имени пользователя, имён групп и конфигурационных данных, хранящихся на сервере.

3.4.3. Обработка ошибок access-denied

Тег ошибки access-denied генерируется в тех случаях, когда система контроля доступа отвергает запрос на вызов протокольной операции или выполнение той или иной операции доступа к хранилищу конфигурации.

Серверу **недопустимо** включать какую-либо информацию, которую клиенту не разрешено читать, в элементы <error-info> откликов <rpc-error>.

3.4.4. Проверка входящих сообщений RPC

На рисунке 3 показана базовая концептуальная структура модели обработки контроля доступа для входящих сообщений NETCONF <rpc> на сервере.

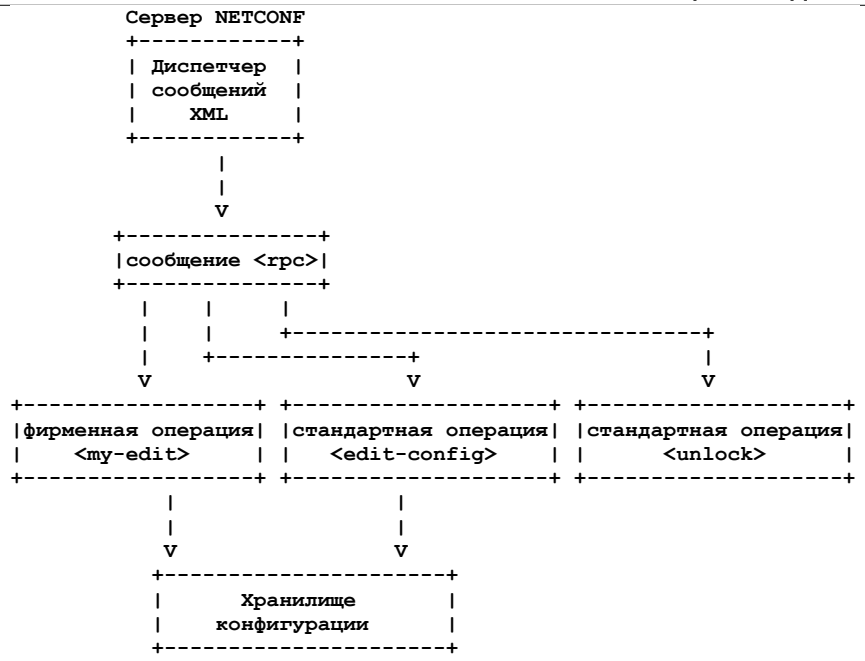

Рисунок 3.

Контроль доступа начинается с диспетчера сообщений.

После проверки сервером пригодности элемента <rpc>, определения пространства имён URI и имени элемента, запрашивающего протокольную операцию сервер проверяет права пользователя на вызов протокольной операции.

Сервер **должен** отдельно разрешать каждую операцию протокола, выполняя перечисленные ниже шаги.

1. Если лист enable-nacm имеет значение false, протокольная операция разрешена.
2. Если запрашивающая сессия определена как восстановительная, протокольная операция разрешена.
3. Если запрошена операция NETCONF <close-session>, протокольная операция разрешена.
4. Проверяются все записи group для поиска в них записи user-name, значение которой совпадает с именем пользователя для сделавшей запрос сессии. Если лист enable-external-groups имеет значение true, эти группы добавляются в список групп, предоставленный транспортным уровнем.
5. Если групп не найдено, переход к п. 10.
6. Обрабатываются все записи rule-list в порядке их размещения в конфигурации. Если в rule-list элемент leaf-list для групп не совпадает ни с одной из групп пользователя, обрабатывается следующий элемент rule-list.
7. Для каждого найденного элемента rule-list обрабатываются все записи по порядку, пока не будет найдено правило, соответствующее запрошенной операции доступа. Правило считается соответствующим при выполнении всех перечисленных ниже условий.
   - Лист module-name в правиле имеет значение * или совпадает с именем модуля YANG, где определена протокольная операция.
   - (1) правило не имеет rule-type или (2) rule-type имеет значение protocol-operation, а rpc-name имеет значение * или совпадает с именем запрошенной операции протокола.
   - Лист access-operations в правиле имеет установленный бит exec или специальное значение *.
8. Если соответствующее правило найдено, проверяется лист action. Если он имеет значение permit, протокольная операция разрешена, в противном случае она отвергается.
9. Этот пункт соответствует ситуации, когда не найдено совпадающего правила ни в одной записи rule-list.
10. Если запрошенная протокольная операция определена в модуле YANG, анонсированном в возможностях сервера, и оператор rpc содержит оператор nacm:default-deny-all, протокольная операция отвергается.
11. Если протокольная операция является операцией протокола NETCONF <kill-session> или <delete-config>, эта операция отвергается.
12. Если лист exec-default имеет значение permit, протокольная операция разрешена, иначе она отвергается.

Если пользователь не уполномочен вызывать операцию протокола, генерируется сообщение <rpc-error> с приведённой ниже информацией.

error-tag
access-denied

error-path
Указывает запрошенную операцию. Приведённый ниже пример представляет операцию <edit-config> в базовом пространстве имён NETCONF.

```
<error-path
  xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0">
    /nc:rpc/nc:edit-config
</error-path>
```

Если доступ к хранилищу произошёл (напрямую или за счёт побочного эффекта протокольной операции), сервер **должен** перехватить операцию доступа и убедиться, что пользователь уполномочен на выполнение запрошенной операции доступа к указанным данным, как описано в параграфе 3.4.5.

3.4.5. Проверка доступа к узлу данных

Если (1) осуществляется доступ к узлу данных или (2) к узлу привязано действие или уведомление, сервер **должен** гарантировать, что пользователь уполномочен выполнять запрошенную операцию доступа read, create, update, delete или execute для указанного узла данных.

Если запрошено выполнение действия, сервер **должен** гарантировать, что пользователь уполномочен выполнять операцию доступа execute.

Если генерируется привязанное к узлу уведомление, сервер **должен** гарантировать, что пользователь уполномочен выполнять операцию доступа read для запрошенного уведомления.

Этапы проверки полномочий доступа к узлу данных перечислены ниже.

1. Если лист enable-nacm имеет значение false, доступ разрешён.
2. Если запрашивающая сессия определена как восстановительная, доступ разрешён.
3. Проверяются все записи group для поиска в них записи user-name, значение которой совпадает с именем пользователя для сделавшей запрос сессии. Если лист enable-external-groups имеет значение true, эти группы добавляются в список групп, предоставленный транспортным уровнем.
4. Если групп не найдено, переход к п. 9.
5. Обрабатываются все записи rule-list в порядке их размещения в конфигурации. Если в rule-list элемент leaf-list для групп не совпадает ни с одной из групп пользователя, обрабатывается следующий элемент rule-list.
6. Для каждого найденного элемента rule-list обрабатываются все записи по порядку, пока не будет найдено правило, соответствующее запрошенной операции доступа. Правило считается соответствующим при выполнении всех перечисленных ниже условий.
   - Лист module-name в правиле имеет значение * или совпадает с именем модуля YANG, где определена протокольная операция.
   - (1) правило не имеет rule-type или (2) rule-type имеет значение data-node, а path соответствует запрашиваемому узлу данных, действия или уведомления. Путь считается соответствующим, если запрошенный узел является узлом, заданным этим путём, или наследником такого узла.
   - Для операции read лист access-operations в правиле имеет установленный бит read или специальное значение *.
   - Для операции create лист access-operations в правиле имеет установленный бит create или специальное значение *.
   - Для операции delete лист access-operations в правиле имеет установленный бит delete или специальное значение *.
   - Для операции update лист access-operations в правиле имеет установленный бит update или специальное значение *.
   - Для операции execute лист access-operations в правиле имеет установленный бит exec или специальное значение *.
7. Если соответствующее правило найдено, проверяется лист action. Если он имеет значение permit, протокольная операция разрешена, в противном случае она отвергается. Для операции read отказ (denied) означает, что запрошенные данные не возвращаются в отклике.
8. Этот пункт соответствует ситуации, когда не найдено совпадающего правила ни в одной записи rule-list.
9. Если запрошенный узел данных для операции read определён в модуле YANG, анонсированном в возможностях сервера и оператор определения данных содержит оператор nacm:default-deny-all, запрошенный узел данных и все его наследники не включаются в отклик.
10. Если запрошенный узел данных для операции write определён в модуле YANG, анонсированном в возможностях сервера, и оператор определения данных содержит оператор nacm:default-deny-write или nacm:default-deny-all, запрошенная операция отвергается для узла данных и всех его наследников.
11. Если для операции read лист read-default имеет значение permit, запрошенный узел включается в отклик, в противном случае запрошенный узел и все его потомки не включаются в отклик.
12. Если для операции write лист write-default имеет значение permit, запрос разрешается, иначе отвергается.
13. Если для операции execute лист exec-default имеет значение permit, запрос разрешается, иначе отвергается.

3.4.6. Предоставление полномочий для исходящего уведомления

Настройка правил контроля доступа для узлов-наследников связанного с событием уведомления выходит за рамки документа. Если пользователь уполномочен получать уведомление о события данного типа, он уполномочен также получать все содержащиеся в нем данные.

Если уведомление задано в субдереве данных, как указано в [RFC7950], требуется доступ для чтения к уведомлению. Обработка продолжается в соответствии с параграфом 3.4.5.

На рисунке 4 показана концептуальная модель обработки для исходящих сообщений <notification>.

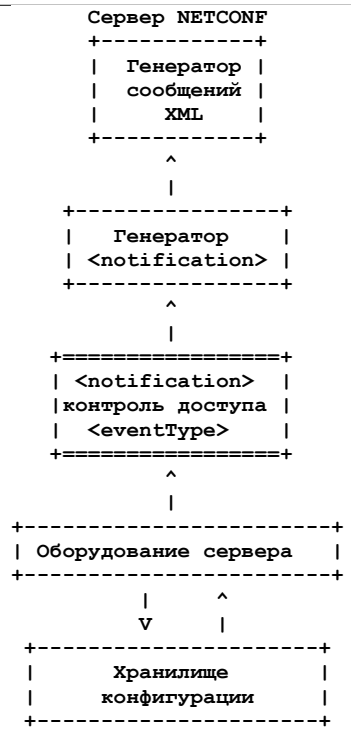

Рисунок 4.

Для генерации уведомления по указанной подписке [RFC5277] полномочия выдаются в соответствии с приведённым ниже описанием.

1. Если лист enable-nacm имеет значение false, уведомление разрешено.
2. Если сессия определена как восстановительная, уведомление разрешено.
3. Если уведомление относится к типу NETCONF <replayComplete> или <notificationComplete> [RFC5277], оно разрешено.
4. Проверяются все записи group для поиска в них записи user-name, значение которой совпадает с именем пользователя для сделавшей запрос сессии. Если лист enable-external-groups имеет значение true, эти группы добавляются в список групп, предоставленный транспортным уровнем.
5. Если групп не найдено, переход к п. 10.
6. Обрабатываются все записи rule-list в порядке их размещения в конфигурации. Если в rule-list элемент leaf-list для групп не совпадает ни с одной из групп пользователя, обрабатывается следующий элемент rule-list.
7. Для каждого найденного элемента rule-list обрабатываются все записи по порядку, пока не будет найдено правило, соответствующее запрошенной операции доступа. Правило считается соответствующим при выполнении всех перечисленных ниже условий.
   - Лист module-name в правиле имеет значение * или совпадает с именем модуля YANG, где определено уведомление.
   - (1) правило не имеет rule-type или (2) rule-type имеет значение notification, а notification-name имеет значение * или совпадает с именем уведомления.
   - Лист access-operations в правиле имеет установленный бит read или специальное значение *.
8. Если соответствующее правило найдено, проверяется лист action. Если он имеет значение permit, протокольная уведомление разрешено, в противном случае оно отбрасывается.
9. Этот пункт соответствует ситуации, когда не найдено совпадающего правила ни в одной записи rule-list.
10. Если запрошенное уведомление определено в модуле YANG, анонсированном в возможностях сервера, и оператор notification содержит оператор nacm:default-deny-all, уведомление для соответствующей подписки отбрасывается.
11. Если для лист read-default имеет значение permit, уведомление разрешено, в противном случае оно отвергается.

3.5. Определения модели данных

3.5.1. Организация данных

На приведённом ниже рисунке показана структура и содержимое модуля NACM YANG.

```
module: ietf-netconf-acm
  +--rw nacm
     +--rw enable-nacm?              boolean
     +--rw read-default?             action-type
     +--rw write-default?            action-type
     +--rw exec-default?             action-type
     +--rw enable-external-groups?   boolean
```

```
      +--ro denied-operations         yang:zero-based-counter32
      +--ro denied-data-writes        yang:zero-based-counter32
      +--ro denied-notifications      yang:zero-based-counter32
      +--rw groups
      |  +--rw group* [name]
      |     +--rw name          group-name-type
      |     +--rw user-name*    user-name-type
      +--rw rule-list* [name]
         +--rw name      string
         +--rw group*    union
         +--rw rule* [name]
            +--rw name                  string
            +--rw module-name?          union
            +--rw (rule-type)?
            |  +--:(protocol-operation)
            |  |  +--rw rpc-name?             union
            |  +--:(notification)
            |  |  +--rw notification-name?    union
            |  +--:(data-node)
            |     +--rw path                  node-instance-identifier
            +--rw access-operations?    union
            +--rw action                action-type
            +--rw comment?              string
```

3.5.2. Модуль YANG

Приведённый ниже модуль YANG задаёт нормативное содержимое NETCONF, которое **должно** поддерживаться сервером.

Модуль YANG ietf-netconf-acm импортирует определения типов из [RFC6991].

```
<CODE BEGINS> file "ietf-netconf-acm@2018-02-14.yang"
module ietf-netconf-acm {

  namespace "urn:ietf:params:xml:ns:yang:ietf-netconf-acm";

  prefix nacm;

  import ietf-yang-types {
    prefix yang;
  }

  organization
    "IETF NETCONF (Network Configuration) Working Group";

  contact
    "WG Web:   <https://datatracker.ietf.org/wg/netconf/>
     WG List:  <mailto:netconf@ietf.org>

     Author:   Andy Bierman
               <mailto:andy@yumaworks.com>

     Author:   Martin Bjorklund
               <mailto:mbj@tail-f.com>";

  description
    "Модель управления доступом NETCONF.

     Copyright (c) 2012 - 2018 IETF Trust and the persons
     identified as authors of the code.  All rights reserved.

     Распространение и использование в исходной или двоичной форме
     с изменениями или без таковых разрешается в соответствии с
     упрощённой лицензией BSD, изложенной в параграфе 4.c документа
     IETF Trust's Legal Provisions Relating to IETF Documents
     (https://trustee.ietf.org/license-info).

     Данная версия модуля YANG является частью RFC 8341, где правовые
     вопросы рассмотрены более полно.";

  revision "2018-02-14" {
    description
      "Добавлена поддержка действий и уведомлений YANG 1.1, привязанных
       к узлам данных. Уточнено использование расширений NACM в других
       моделях данных.";
    reference
      "RFC 8341: Network Configuration Access Control Model";
  }

  revision "2012-02-22" {
    description
      "Initial version.";
    reference
      "RFC 6536: Network Configuration Protocol (NETCONF)
                 Access Control Model";
  }
```

```
  /*
   * Extension statements
   */

  extension default-deny-write {
    description
      "Служит для индикации того, что узел модели данных
       представляет деликатный параметр безопасности системы.

       При наличии этого расширения сервер NETCONF будет разрешать
       запись для узла лишь указанным «сеансам восстановления». Для
       прочих пользователей требуется явное правило контроля доступа.

       Если используется модуль NACM, он должен быть включён (т. е.
       объект /nacm/enable-nacm должен иметь значение true) или это
       расширение будет игнорироваться.

       Расширение default-deny-write МОЖЕТ присутствовать лишь в
       операторе определения данных. В иных случаях оно игнорируется.";
  }

  extension default-deny-all {
    description
      "Используется для указания того, что узел модели данных управляет
       очень деликатным параметром безопасности.

       При наличии этого расширения сервер NETCONF будет разрешать
       запись для узла лишь указанным «сеансам восстановления». Для
       прочих пользователей требуется явное правило контроля доступа.

       Если используется модуль NACM, он должен быть включён (т. е.
       объект /nacm/enable-nacm должен иметь значение true) или это
       расширение будет игнорироваться.

       Расширение default-deny-all МОЖЕТ присутствовать лишь в
       операторе определения данных, операторе rpc или notification.
       statement. В иных случаях оно игнорируется.";
  }

  /*
   * Производные типы
   */

  typedef user-name-type {
    type string {
      length "1..max";
    }
    description
      "Строка общего назначения для имени пользователя.";
  }

  typedef matchall-string-type {
    type string {
      pattern '\*';
    }
    description
      "Строка, содержащая один символ *, используется для
       представления всех возможных значений отдельного листа,
       использующего этот тип данных.";
  }

  typedef access-operations-type {
    type bits {
      bit create {
        description
          "Любая операция протокола, создающая новый узел данных.";
      }
      bit read {
        description
          "Любая операция протокола или уведомление, возвращающие
           значение узла данных.";
      }
      bit update {
        description
          "Любая операция протокола, изменяющая узел данных.";
      }

      bit delete {
        description
          "Любая операция протокола, удаляющая узел данных.";
      }
      bit exec {
        description
          "Выполнение заданной операции протокола.";
      }
    }
```

```
      description
        "Операция доступа.";
    }

    typedef group-name-type {
      type string {
        length "1..max";
        pattern '[^\*].*';
      }
      description
        "Имя группы администраторов, в которую можно назначить
         пользователей.";
    }

    typedef action-type {
      type enumeration {
        enum permit {
          description
            "Запрошенное действие разрешено.";
        }
        enum deny {
          description
            "Запрошенное действие отвергнуто.";
        }
      }
      description
        "Действие, выполняемое сервером при соответствии
         конкретному правилу.";
    }

    typedef node-instance-identifier {
      type yang:xpath1.0;
      description
        "Путь, используемый для представления строки идентификатора
         специального узла данных, действия или уведомления.

         Значением идентификатора экземпляра узла является
         выражение YANG instance-identifier без ограничений.

         Применяются те же правила, что и instance-identifier,
         за исключением необязательности предикатов ключей. При
         отсутствии предиката node-instance-identifier представляет
         все возможные экземпляры сервера для этого ключа.

         Это выражение XML Path Language (XPath) оценивается в описанном
         ниже контексте.

            -  Набор деклараций пространств имён включает те, что находятся
               в области действия элемента leaf, где используется тип.

            -  Набор привязок переменных содержит одну переменную USER,
               которая указывает имя пользователя текущей сессии.

            -  Библиотекой функций служит библиотека ядра, но следует
               отметить, что синтаксические ограничения instance-identifier
               не разрешают функций.

            -  Узлом контекста является корневой узел дерева данных.

         Доступное дерево включает действия и уведомления, привязанные
         к узлам данных.";
    }

    /*
     * Операторы определения данных
     */

    container nacm {
      nacm:default-deny-all;

      description
        "Параметры для модели управления доступом NETCONF.";

      leaf enable-nacm {
        type boolean;
        default "true";
        description
          "Разрешает или запрещает выполнение всех операций
           контроля доступа NETCONF. Значение true включает
           управление, false отключает.";
      }

      leaf read-default {
        type action-type;
        default "permit";
        description
```

```
      "Решает вопрос предоставления доступа на чтение при
       отсутствии подходящего правила для конкретного запроса.";
    }

    leaf write-default {
      type action-type;
      default "deny";
      description
        "Решает вопрос предоставления доступа на создание,
         изменение или удаление при отсутствии подходящего
         правила для конкретного запроса.";
    }

    leaf exec-default {
      type action-type;
      default "permit";
      description
        "Решает вопрос предоставления доступа на исполнение при
         отсутствии подходящего правила для конкретного запроса.";
    }

    leaf enable-external-groups {
      type boolean;
      default "true";
      description
        "Падает, будет ли сервер использовать группы, переданные
         транспортным уровнем NETCONF при назначении пользователя для
         набора групп NACM. Если этот лист имеет значение false, все
         имена групп, сообщённые транспортным уровнем, сервер игнорирует.";
    }

    leaf denied-operations {
      type yang:zero-based-counter32;
      config false;
      mandatory true;
      description
        "Число случаев отказа от выполнения протокольных операций
         с момента последней перезагрузки сервера.";
    }

    leaf denied-data-writes {
      type yang:zero-based-counter32;
      config false;
      mandatory true;
      description
        "Число случаев отказа от выполнения протокольной операции
         изменения хранилища данных  с момента последней
         перезагрузки сервера.";
    }

    leaf denied-notifications {
      type yang:zero-based-counter32;
      config false;
      mandatory true;
      description
        "Число случаев отказа от предоставления подписки на
         уведомления с момента последней перезагрузки сервера.";
    }

    container groups {
      description
        "Группы контроля доступа NETCONF.";

      list group {
        key name;

        description
          "Запись для одной группы NACM. Этот список будет
           включать лишь заданные в конфигурации, а не полученные
           от транспортных протоколов записи.";

        leaf name {
          type group-name-type;
          description
            "Имя группы, связанной с этой записью.";
        }

        leaf-list user-name {
          type user-name-type;
          description
            "Каждая запись указывает имя пользователя - члена
             группы, связанной с записью.";
        }
      }
    }
```

```
    list rule-list {
      key name;
      ordered-by user;
      description
        "Упорядоченный набор правил контроля доступа.";

      leaf name {
        type string {
          length "1..max";
        }
        description
          "Произвольное имя, назначенное для rule-list.";
      }
      leaf-list group {
        type union {
          type matchall-string-type;
          type group-name-type;
        }
        description
          "Список административных групп, которым будут
           назначены права доступа, заданные списком rule.

           * указывает, что запись применяется ко всем группам.";
      }

      list rule {
        key name;
        ordered-by user;
        description
          "Одно правило управления доступом.

           Правила обрабатываются в заданном пользователем порядке до
           первого совпадения. Совпадением считается соответствие
           module-name, rule-type и access-operations запросу. Если
           правило соответствует, лист action определяет
           предоставление доступа.";

        leaf name {
          type string {
            length "1..max";
          }
          description
            "Произвольное имя, назначенное для правила.";
        }

        leaf module-name {
          type union {
            type matchall-string-type;
            type string;
          }
          default "*";
          description
            "Имя модуля, связанного с данным правилом.

             Этот лист даёт совпадение, если он имеет значение * или
             объект, требующий доступа, определён в модуле с заданным
             именем.";
        }
        choice rule-type {
          description
            "Этот выбор будет соответствовать, если все листья в правиле
             соответствуют запросу. При отсутствии листьев выбор
             соответствует всем запросам.";
          case protocol-operation {
            leaf rpc-name {
              type union {
                type matchall-string-type;
                type string;
              }
              description
                "Этот лист (leaf) считается соответствующим, если он имеет
                 значение * или его значение совпадает с именем запрошенной
                 протокольной операции.";
            }
          }
          case notification {
            leaf notification-name {
              type union {
                type matchall-string-type;
                type string;
              }
              description
                "Этот лист (leaf) считается соответствующим, если он имеет
                 значение * или его значение совпадает с именем запрошенного
                 уведомления.";
            }
```

```
            }

            case data-node {
              leaf path {
                type node-instance-identifier;
                mandatory true;
                description
                  "Идентификатор экземпляра, связанный с узлом данных,
                   действием или уведомлением, контролируемым данным
                   правилом.

                   Идентификаторы экземпляров данных конфигурации или
                   состояния начинаются в узла данных верхнего уровня.
                   Для этого типа значения пути нужен полный идентификатор
                   экземпляра.

                   Специальное значение / указывает все содержимое хранилища.";
              }
            }
          }

          leaf access-operations {
            type union {
              type matchall-string-type;
              type access-operations-type;
            }
            default "*";
            description
              "Операции доступа, связанные с этим правилом.

               Лист будет соответствовать, если он имеет значение * или
               бит, соответствующий запрашиваемой операции, установлен.";
          }

          leaf action {
            type action-type;
            mandatory true;
            description
              "Действие по управлению доступом, связанное с правилом.
               Если определено, что правило соответствует конкретному
               запросу, этот объект указывает, принимается или
               отвергается запрос.";
          }

          leaf comment {
            type string;
            description
              "Текстовое описание правила доступа.";
          }
        }
      }
    }
  }

<CODE ENDS>
```

4. Взаимодействие с IANA

Этот документ повторно использует URI для ietf-netconf-acm в реестре IETF XML.

Документ обновляет регистрацию модуля в реестре YANG Module Names ссылкой на данный RFC вместо RFC 6536 для ietf-netconf-acm. В соответствии с форматом в [RFC6020] регистрируются приведённые ниже параметры.

```
Name: ietf-netconf-acm
Namespace: urn:ietf:params:xml:ns:yang:ietf-netconf-acm
Prefix: nacm
Reference: RFC 8341
```

5. Вопросы безопасности

Описанный в этом документе модуль YANG определяет схему для данных, которая разработана для обеспечения доступа с помощью протоколов сетевого управления типа NETCONF [RFC6241] или RESTCONF [RFC8040]. Нижним уровнем NETCONF является защищённый транспорт и обязательным для реализации является защищённый транспорт SSH[1] [RFC6242]. Нижним уровнем RESTCONF является протокол HTTPS и обязательный для реализации транспорт TLS [RFC5246].

Модель контроля доступа NETCONF [RFC8341] обеспечивает способы ограничения доступа для отдельных пользователей NETCONF или RESTCONF к предопределённому подмножеству всех доступных протокольных операций и содержимого NETCONF или RESTCONF.

Имеется риск, связанный с недостаточным контролем доступа для опций RESTCONF и методов PATCH. Риск заключается в том, что отклик на OPTIONS и PATCH может варьироваться в зависимости от наличия или отсутствия ресурса, соответствующего пути URL. Это может быть использовано для тривиальной проверки наличия или отсутствия значений в дереве. Поэтому серверу **недопустимо** менять свои отклики в зависимости от существования ресурса, что может показать наличие или отсутствие экземпляров ресурса. В частности, не следует выдавать какую-

[1]Secure Shell.

либо информацию об экземпляре без уверенности в том, что клиент имеет полномочия, требуемые для такого доступа. Предполагается, что сервер всегда возвращает отклик об ошибке access-denied.

Для многих узлов данных, определённых в этом модуле YANG, возможна запись/создание/удаление (т. е. config имеет значение true, установленное по умолчанию). Такие узлы могут считаться чувствительными или уязвимыми в некоторых сетевых средах. Операции записи (например, edit-config) в такие узлы без надлежащей защиты могут оказывать негативное влияние на работу сети. Ниже перечислены субдеревья и узлы данных с указанием их чувствительности/уязвимости:

- /nacm: все субдерево /nacm связано с безопасностью (см. подробности в последующих параграфах).

Далее очерчены вопросы, которые администратору нужно рассмотреть при настройке сервера NETCONF с NACM.

5.1. Настройка и мониторинг NACM

Настройка системы контроля доступа очень важна для безопасности системы. Сервер может не разрешать пользователям никакой настройки отдельный частей системы контроля типа глобального уровня защиты или групп, которым разрешён. доступ к системным ресурсам.

По умолчанию выполнение NACM включено. По умолчанию доступ read разрешён. для всего содержимого хранилища данных (пока в определении данных не задано nacm:default-deny-all), доступ exec разрешён. для безопасных операций протокола. Администратор должен обеспечить включение NACM, а также решить, правильно ли настроены принятые по умолчанию параметры. Нужно убедиться в корректности настройки перечисленных ниже узлов данных и параметров:

- /nacm/enable-nacm (по умолчанию true)
- /nacm/read-default (по умолчанию permit)
- /nacm/write-default (по умолчанию deny)
- /nacm/exec-default (по умолчанию permit)

Администратору нужно ограничить доступ для записи ко всем настраиваемым объектам внутри этой модели данных.

Если разрешена запись для настройки конфигурации правил контроля доступа, нужны меры предотвращения нарушений при выполнении правил контроля доступа. Например, если правила контроля доступа NACM нужно редактировать напрямую в хранилище рабочей конфигурации (т. е. поддерживается и применяется возможность writable-running), нужно принять меры предотвращения непреднамеренного доступа во время редактирования.

Администратор должен убедиться, что трансляция зависящего от транспорта или реализации отождествления пользователя в имя пользователя NACM однозначна и корректна. Это требование подробно описано в параграфе 2.2 [RFC6241].

Администратор должен знать, что структуры данных YANG, представляющие правила контроля доступа (/nacm/rule-list и /nacm/rule-list/rule), упорядочены клиентом. Сервер будет проверять правила контроля доступа в соответствии с их относительным концептуальным порядком в хранилище рабочей конфигурации.

Отметим, что структура данных /nacm/groups содержит имена административных групп, используемых сервером. Эти имена групп могут настраиваться локально и/или через внешний протокол типа RADIUS [RFC2865] [RFC5607].

Для определения имён групп администратор должен понимать свойства безопасности всех внешних протоколов, используемых транспортным уровнем. Например, если протокол не обеспечивает защиты от MITM-атак[1], атакующий может подставить имена групп, которые будут затем включены в конфигурацию NACM так, что пользователь получит избыточные полномочия. В таких случаях администратор может отключить такие имена групп, установив для /nacm/enable-external-groups значение false.

Некоторые из доступных для чтения узлов данных в этом модуле YANG могут оказаться чувствительными или уязвимыми в отдельных сетевых средах. Для таких узлов важно контролировать доступ на чтение (например, с помощью get, get-config или notification). Ниже перечислены чувствительные/уязвимые субдеревья и узлы данных:

- /nacm/enable-nacm
- /nacm/read-default
- /nacm/write-default
- /nacm/exec-default
- /nacm/enable-external-groups
- /nacm/groups
- /nacm/rule-list

Администратор должен ограничить возможность чтения перечисленных выше объектов этой модели данных, поскольку они раскрывают конфигурацию контроля доступа, которая может содержать деликатные сведения.

5.2. Общие вопросы настройки конфигурации

Имеется риск того, что вызов нестандартных протокольных операций будет приводить к недокументированным побочным эффектам. Администратор должен задать правила контроля доступа так, чтобы хранилище конфигурации было защищено от таких побочных эффектов.

Для сессии с некоторыми правами записи (например, вызов <edit-config>), но без какого-либо доступа к конкретному субдереву с конфиденциальными данными можно определить наличие или отсутствие таких данных. Это можно

[1]Man-in-the-middle - перехват и изменение пакетов с участием человека.

сделать путём повторяющихся вызовов некой операции редактирования (создание, обновление или удаление) с возможным получением отклика access-denied. Такая «ловля на живца» может определить наличие или отсутствие конкретных чувствительных данных даже без наличия поля error-path в отклике <rpc-error>.

Набор возможностей сервера NETCONF может меняться с течением времени. В таких случаях возникает риск добавления на устройстве новых протокольных операций, уведомлений и/или содержимого хранилища. Администратор должен убедиться в том, что правила контроля доступа в этом случае подходят для новых условий. Механизмы обнаружения смены возможностей NETCONF на конкретном устройстве выходят за рамки документа.

Возможно, что само определение модели данных (например, оператор YANG when) будет помогать при несанкционированном доступе определить присутствие и даже значение узлов деликатных данных путём проверки наличия и значений разных узлов данных.

Возможно, что само определение модели данных (например, оператор YANG when или choice) позволит сессии неявно создавать или удалять узлы, для которых сессия не имеет прав записи, за счёт побочных эффектов при обработке разрешённой операции <edit-config>.

Существует риск того, что нестандартные протокольные операции или даже стандартная операция <get> могут возвращать данные, которые являются «псевдонимом» или «копией» конфиденциальных данных из другого объекта. Может просто существовать множество определений модели данных, которые раскрывают или даже настраивают базовое серверное оборудование.

Модель данных может содержать внешние ключи (например, YANG leafref), которые раскрывают значения из другой структуры данных. Администратор должен осознавать деликатность моделей данных с узлами leafref. Это влечёт за собой поиск всех объектов leafref, которые «указывают» на деликатные данные (т. е. значений операторов path), явно или неявно включая узлы конфиденциальных данных.

Определение процедур исполнения контроля доступа для базового оборудования, которое может использоваться для поддержки работы сервера NETCONF, выходит за рамки документа. Администратор может идентифицировать выполняемые сервером протокольные операции и решить вопросы применения для них контроля доступа.

Этот документ включает необязательное использование механизма сессий восстановления, который может применяться для обхода правил контроля доступа в критических ситуациях типа конфигурационных ошибок NACM, которые полностью блокируют доступ к серверу. Настройка и идентификация такого механизма сеансов восстановления зависит от реализации и выходит за рамки этого документа. Администратор должен знать все механизмы сеансов восстановления, доступные на сервере и убедиться в их надлежащем использовании.

Сессия может нарушать управление конфигурацией даже без права записи в конфигурацию просто путём блокировки хранилища. Это может делаться для обеспечения стабильности всей или части конфигурации во время операций извлечения данных или возникать в результате DoS-атаки[1]. Сервер не может различить эти два случая. Администратор может ограничить доступ к исполнению (exec) для перечисленных ниже протокольных операций:

- <lock>
- <unlock>
- <partial-lock>
- <partial-unlock>

5.3. Устройство модели данных

Разработчикам нужно чётко указать все деликатные данные, уведомления и протокольные операции, определённые в модуле YANG. Для таких определений должен присутствовать оператор nacm:default-deny-write или nacm:default-deny-all в дополнение к чёткому описанию рисков безопасности.

Протокольные операции должны быть подобающим образом документированы разработчиком модели данных, чтобы администраторы понимали на какие узлы данных (если они есть) влияют операции протокола и какая информация (если она есть) возвращается в сообщении <rpc-reply>.

Модель данных должна быть устроена так, чтобы для входных параметров протокольных операций не требовались разные уровни доступа. Использования базовых протокольных операций следует избегать, определяя вместо них отдельные операции протокола, если требуются разные уровни доступа.

6. Литература

6.1. Нормативные документы

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.

[RFC5277] Chisholm, S. and H. Trevino, "NETCONF Event Notifications", RFC 5277, DOI 10.17487/RFC5277, July 2008, <https://www.rfc-editor.org/info/rfc5277>.

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <https://www.rfc-editor.org/info/rfc6020>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[1]Denial-of-service - отказ в обслуживании.

[RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", RFC 6242, DOI 10.17487/RFC6242, June 2011, <https://www.rfc-editor.org/info/rfc6242>.

[RFC6991] Schoenwaelder, J., Ed., "Common YANG Data Types", RFC 6991, DOI 10.17487/RFC6991, July 2013, <https://www.rfc-editor.org/info/rfc6991>.

[RFC7230] Fielding, R., Ed., and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, DOI 10.17487/RFC7230, June 2014, <https://www.rfc-editor.org/info/rfc7230>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8342] Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K., and R. Wilton, "Network Management Datastore Architecture (NMDA)", RFC 8342, DOI 10.17487/RFC8342, March 2018, <https://www.rfc-editor.org/info/rfc8342>.

[W3C.REC-xml-20081126] Bray, T., Paoli, J., Sperberg-McQueen, M., Maler, E., and F. Yergeau, "Extensible Markup Language (XML) 1.0 (Fifth Edition)", World Wide Web Consortium Recommendation REC-xml-20081126, November 2008, <https://www.w3.org/TR/2008/REC-xml-20081126>.

6.2. Дополнительная литература

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, DOI 10.17487/RFC2865, June 2000, <https://www.rfc-editor.org/info/rfc2865>.

[RFC5607] Nelson, D. and G. Weber, "Remote Authentication Dial-In User Service (RADIUS) Authorization for Network Access Server (NAS) Management", RFC 5607, DOI 10.17487/RFC5607, July 2009, <https://www.rfc-editor.org/info/rfc5607>.

[YANG-SEC] IETF, "YANG Security Guidelines", <https://trac.ietf.org/trac/ops/wiki/yang-security-guidelines>.

Приложение A. Примеры использования

Приведённые ниже фрагменты XML [W3C.REC-xml-20081126] служат лишь примерами настройки NACM для решения некоторых задач контроля доступа.

A.1. Пример <groups>

Требуется хотя бы одна запись <group>, чтобы правила контроля доступа могли использоваться.

Приведённый ниже фрагмент XML показывает произвольные группы и не предназначен для практического применения.

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  <groups>
    <group>
      <name>admin</name>
      <user-name>admin</user-name>
      <user-name>andy</user-name>
    </group>

    <group>
      <name>limited</name>
      <user-name>wilma</user-name>
      <user-name>bam-bam</user-name>
    </group>

    <group>
      <name>guest</name>
      <user-name>guest</user-name>
      <user-name>guest@example.com</user-name>
    </group>
  </groups>
</nacm>
```

Этот пример включает три группы:

```
admin: два пользователя с именами admin и andy
limited: два пользователя с именами wilma и bam-bam
guest: два пользователя с именами guest и guest@example.com.
```

A.2. Пример правила для модуля

Правила модуля служат для контроля доступа ко всему содержимому, определённому в конкретном модуле. Правило модуля имеет установленный лист module-name, но не имеет установленных узлов из выбора rule-type.

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  <rule-list>
    <name>guest-acl</name>
    <group>guest</group>
    <rule>
      <name>deny-ncm</name>
      <module-name>ietf-netconf-monitoring</module-name>
```

```
        <access-operations>*</access-operations>
        <action>deny</action>
        <comment>
            Не позволяет гостям получить доступ к данным
            мониторинга NETCONF.
        </comment>
      </rule>
    </rule-list>

    <rule-list>
      <name>limited-acl</name>
      <group>limited</group>
      <rule>
        <name>permit-ncm</name>
        <module-name>ietf-netconf-monitoring</module-name>
        <access-operations>read</access-operations>
        <action>permit</action>
        <comment>
            Позволяет считывать данные мониторинга NETCONF.
        </comment>
      </rule>
      <rule>
        <name>permit-exec</name>
        <module-name>*</module-name>
        <access-operations>exec</access-operations>
        <action>permit</action>
        <comment>
            Позволяет вызывать поддерживаемые операции сервера.
        </comment>
      </rule>
    </rule-list>

    <rule-list>
      <name>admin-acl</name>
      <group>admin</group>
      <rule>
        <name>permit-all</name>
        <module-name>*</module-name>
        <access-operations>*</access-operations>
        <action>permit</action>
        <comment>
            Даёт группе admin полный доступ к операциям и данным.
        </comment>
      </rule>
    </rule-list>
  </nacm>
```

Этот пример демонстрирует 4 правила:

```
deny-ncm: предотвращает доступ группы guest к считыванию данных
   мониторинга в модуле YANG ietf-netconf-monitoring.
permit-ncm: позволяет группе limited читать модуль YANG
   ietf-netconf-monitoring.
permit-exec: позволяет группе limited вызывать любые протокольные
   операции, поддерживаемые сервером.
permit-all: предоставляет группе admin полный доступ к содержимому
   сервера. Далее не будет правил, соответствующих группе admin,
   поскольку это правило для модуля.
```

A.3. Пример правила для протокольной операции

Правила протокольных операций служат для управления доступом к конкретным операциям протокола.

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  <rule-list>
    <name>guest-limited-acl</name>
    <group>limited</group>
    <group>guest</group>
    <rule>
      <name>deny-kill-session</name>
      <module-name>ietf-netconf</module-name>
      <rpc-name>kill-session</rpc-name>
      <access-operations>exec</access-operations>
      <action>deny</action>
      <comment>
        Не позволяет группам limited и guest 'убить' чужую сессию.
      </comment>
    </rule>
    <rule>
      <name>deny-delete-config</name>
      <module-name>ietf-netconf</module-name>
      <rpc-name>delete-config</rpc-name>
      <access-operations>exec</access-operations>
      <action>deny</action>
      <comment>
         Не позволяет группам limited и guest удалять конфигурации.
      </comment>
    </rule>
```

```
    </rule-list>

    <rule-list>
      <name>limited-acl</name>
      <group>limited</group>
      <rule>
        <name>permit-edit-config</name>
        <module-name>ietf-netconf</module-name>
        <rpc-name>edit-config</rpc-name>
        <access-operations>exec</access-operations>
        <action>permit</action>
        <comment>
          Позволяет группе limited редактировать конфигурацию.
        </comment>
      </rule>
    </rule-list>
  </nacm>
```

Этот пример содержит правила для трёх операций:

```
  deny-kill-session: предотвращает вызов группами limited и guest
     протокольной операции NETCONF <kill-session>.
  deny-delete-config: предотвращает вызов группами limited и guest
     протокольной операции NETCONF <delete-config>.
  permit-edit-config: разрешает группе limited вызывать операцию
     NETCONF <edit-config>. Это правило не будет работать, пока не
     установлено значение deny для листа exec-default.
```

A.4. Пример правила для узла данных

Правила узла данных служат для контроля доступа к конкретным (config и non-config) узлам данных в содержимом NETCONF, предоставляемом сервером.

```
  <nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
    <rule-list>
      <name>guest-acl</name>
      <group>guest</group>
      <rule>
        <name>deny-nacm</name>
        <path xmlns:n="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
          /n:nacm
        </path>
        <access-operations>*</access-operations>
        <action>deny</action>
        <comment>
          Запрет для группы guest доступа к данным /nacm.
        </comment>
      </rule>
    </rule-list>

    <rule-list>
      <name>limited-acl</name>
      <group>limited</group>
      <rule>
        <name>permit-acme-config</name>
        <path xmlns:acme="http://example.com/ns/netconf">
          /acme:acme-netconf/acme:config-parameters
        </path>
        <access-operations>
          read create update delete
        </access-operations>
        <action>permit</action>
        <comment>
          Предоставление группе limited полного доступа к
          конфигурационным параметрам acme NETCONF. Показана
          длинная форма access-operations вместо сокращённой.
        </comment>
      </rule>
    </rule-list>

    <rule-list>
      <name>guest-limited-acl</name>
      <group>guest</group>
      <group>limited</group>
      <rule>
        <name>permit-dummy-interface</name>
        <path xmlns:acme="http://example.com/ns/itf">
          /acme:interfaces/acme:interface[acme:name='dummy']
        </path>
        <access-operations>read update</access-operations>
        <action>permit</action>
        <comment>
          Разрешает группам limited и guest чтение и обновление
          для интерфейса dummy.
        </comment>
      </rule>
    </rule-list>
```

```
    <rule-list>
      <name>admin-acl</name>
      <group>admin</group>
      <rule>
        <name>permit-interface</name>
        <path xmlns:acme="http://example.com/ns/itf">
          /acme:interfaces/acme:interface
        </path>
        <access-operations>*</access-operations>
        <action>permit</action>
        <comment>
          Разрешает группе admin полный доступ к интерфейсам acme.
        </comment>
      </rule>
    </rule-list>
  </nacm>
```

Этот пример содержит 4 правила для узлов данных:

```
deny-nacm: предотвращает доступ группы guest к субдереву /nacm.
permit-acme-config: разрешает для группы limited доступ read-write
   к acme <config-parameters>.
permit-dummy-interface: разрешает для групп limited и guest доступ
   read-update к записи acme <interface> с именем dummy. Запись не
   может быть создана или удалена этими группами, можно лишь менять её.
permit-interface: даёт группе admin доступ read-write ко всем записям
   acme <interface>.
```

A.5. Пример правила для уведомления

Правила уведомлений служат для контроля доступа к уведомлениям о конкретном типе событий.

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  <rule-list>
    <name>sys-acl</name>
    <group>limited</group>
    <group>guest</group>
    <rule>
      <name>deny-config-change</name>
      <module-name>acme-system</module-name>
      <notification-name>sys-config-change</notification-name>
      <access-operations>read</access-operations>
      <action>deny</action>
      <comment>
        Не позволяет группам guest и limited получать
        уведомления о смене конфигурации.
      </comment>
    </rule>
  </rule-list>
</nacm>
```

Этот пример показывает одно правило для уведомлений:

```
deny-config-change: предотвращает отправку в группы limited и
   guest уведомлений о событиях типа acme <sys-config-change>.
```

Адреса авторов

Andy Bierman

YumaWorks

685 Cochran St.

Suite #160

Simi Valley, CA 93065

United States of America

Email: andy@yumaworks.com

Martin Bjorklund

Tail-f Systems

Email: mbj@tail-f.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru