Иерархия Серверов администрирования, офисов и агентов обновлений

AK/SC позволяет организовать Серверы администрирования в иерархию «главный — подчиненный», в которой каждый Сервер администрирования может иметь несколько подчиненных Серверов администрирования в рамках многоуровневой иерархической структуры. Такое построение структуры предоставляет следующие преимущества:

- Снижение нагрузки на Сервер администрирования: в отличие от использования одного сервера, клиенты распределяются по разным серверам, в зависимости от топологии сети и/или организационной структуры, что понижает нагрузку на каждый из серверов.
- Улучшение и упрощение координации между удаленными филиалами: отсутствует необходимость поддержания постоянного соединения между всеми офисами и с каждым клиентом.
- Административные права могут предоставляться более гибко, в соответствии с топологией сети и/или организационной структурой.

Возможные недостатки:

- Каждый Сервер администрирования требует наличия собственной базы данных.
- Не все объекты поддерживают иерархию (например, хранилища, выборки событий, файлы на карантине, резервные копии и необработанные файлы).

Для достижения указанных выше целей можно предложить три сценария. Выбор одного из них будет основываться на топологии сети и/или структуре организации.

Одноуровневая иерархия

Задачи и политики можно создавать на главном Сервере администрирования и отправлять их на подчиненные Серверы администрирования, с предоставлением возможности изменения некоторых параметров, и создания политик и задач на уровне подчиненных Серверов. В некоторых случаях есть смысл подключать к главному Серверу администрирования только подчиненные Серверы администрирования, без подключения клиентов. Так как в условиях чрезвычайно интенсивного взаимодействия между серверами и клиентами данные от подчиненных серверов, необходимые для создания отчетов, попадают в общую очередь данных от клиентов, ожидающих обработки, что приводит к задержкам в управлении антивирусным решением. В этом случае главный Сервер администрирования будет работать только как сервер управления и для составления отчетов, не взаимодействуя с управляемыми узлами.

Многоуровневая иерархия

Задачи и политики, как и в предыдущем сценарии, можно создавать на главном Сервере и отправлять на подчиненные Серверы (второго уровня) с предоставлением возможности изменения некоторых параметров и создания политик и задач на уровне подчиненных Серверов. Эта же схема повторяется на следующем уровне подчиненных Серверов в иерархии.

Независимые Серверы администрирования с использованием профилей подключения

Этот сценарий предполагает, что иерархия отсутствует, а серверы управляются независимо. Мобильные узлы могут подключаться к Серверам администрирования в соответствии с различными параметрами — такими как изменение IP-адреса DNS/WINS/DHCP-серверов или шлюза по умолчанию, изменение подсети и т. д.
На самом деле нет необходимости устанавливать в каждый удаленный филиал, офис или подсеть подчиненный Сервер администрирования, особенно, если речь идет о филиалах с небольшим количеством клиентов и/или не имеющих серверного оборудования. В некоторых случаях могут использоваться агенты обновлений (управляемые узлы, выделенные для хранения и распространения обновлений, установочных пакетов, групповых задач и политик).

Ниже приведен пример подобной архитектуры с описанными ранее схемами:

Другая распространенная ситуация — множество небольших удаленных офисов, соединенных с головным филиалом каналами связи с низкой пропускной способностью.

В такой ситуации возможны два варианта:

- Использовать большое количество агентов обновлений. Теоретически сервер AK/SC может управлять несколькими тысячами агентов обновлений, но эта возможность не тестировалась. Поэтому разумно было бы создать структуру групп, и использовать один агент обновлений для нескольких офисов, если это возможно.
- Отсутствие агентов обновления в офисах, вызванное теми или иными причинами (хотя подобное и не рекомендуется). Здесь следует учесть тот факт, что каналы связи будут загружены во время некоторых операций, особенно на этапе начального развертывания, а также при обновлениях. Поэтому нужно заранее продумать начальное развертывание (возможно, потребуется применить сторонние средства установки или добавить Агент администрирования в образ системы, что также применимо и для предыдущего случая), и рассмотреть возможность обновления через Интернет, если подключение это позволяет.

Сравнивая с AK8, в SC9 внесены некоторые улучшения и изменения:

- В SC9 агент обновления по умолчанию автоматически назначается на каждые 100 узлов в группе. Компьютер, выполняющий роль агента обновлений, выбирается по нескольким параметрам: наиболее мощный процессор (определяется с использованием специального алгоритма сравнения процессоров, запускаемого на узлах), не является ноутбуком (проверяется наличие или отсутствие аккумулятора), имеет 1 ГБ свободного дискового пространства. Если оказывается, что на компьютере агента обновлений меньше 300 МБ свободного пространства, или он неактивен более 24 часов, или перемещен в другую группу — роль агента обновлений с него снимается. Такое автоматическое назначение может быть отключено.
- Теперь агенты обновлений могут выполнять опрос сети, что оказывается полезным, когда какие-либо узлы оказываются за NAT и Сервер администрирования не имеет прямого доступа к ним.
- Добавлен отчет о действиях агента обновлений.
- Стало возможным определять периоды времени, в которые Агент администрирования может синхронизироваться с Сервером администрирования, что позволяет снизить сетевой трафик и нагрузку на сервер в течение этих периодов.
- Был добавлен резервный порт для зашифрованных соединений Консоли к Серверу администрирования (по умолчанию TCP 13291), который обеспечивает возможность без проблем подключаться к серверу во время пиковых нагрузок. Если Консоль используется локально, соединение устанавливается через этот порт по умолчанию.
- Стало возможным использовать до 10 виртуальных Серверов администрирования без специального ключа, активирующего функциональность Service Provider Edition. Основное назначение виртуального Сервера — добиться полного разделения ролей, чего AK8 позволял достичь лишь частично. Это не позволяет снизить нагрузку на сервер. Виртуальные Серверы администрирования, в отличие от подчиненных Серверам администрирования, расположены на одном компьютере с главным Сервером администрирования. В действительности они являются логическими объектами с перечисленными ниже ограничениями:
    - Они используют одну базу данных вместе с главным Сервером администрирования.
    - Для них невозможно создать подчиненные Серверы (включая виртуальные).
    - Они не имеют собственных задач резервирования и восстановления.
    - Они не имеют собственных задач обновления.
    - Виртуальные Серверы могут сканировать сеть только с помощью агентов обновлений.
    - Невозможно переместить управляемые узлы между главным Сервером администрирования и виртуальными Серверами с помощью перетаскивания — для этого необходимо создать специальную задачу.
    - Для того чтобы перезапустить виртуальный Сервер, требуется перезапустить главный Сервер администрирования, вследствие чего перезапустятся все размещенные на нем виртуальные Серверы.
- Добавлена поддержка Virtual Desktop Infrastructure (VDI). Теперь Агент администрирования на временной виртуальной машине, созданной из образа, может иметь специальный флаг. Когда подобная машина в штатном порядке отключается, Агент уведомляет сервер SC, и машина удаляется из списка. В случае нештатного отключения машина удаляется из списка по истечении определенного периода неактивности. Это позволяет избежать ситуации, в которой сервер SC оказывается загружен большим числом записей о машинах, которые создаются и удаляются каждый день.

- В AK8 можно было задать период окончания видимости компьютера. По умолчанию он составлял 60 минут. Этот параметр определяет время, в течение которого после отключения от Сервера администрирования управляемый узел будет считаться видимым. В SC9 этот интервал не определяется в свойствах Сервера администрирования, и равен 3–3,5 периодам синхронизации.
- Была добавлена веб-консоль Kaspersky Security Center Web-Console 9.0. Это веб-приложение, которое обеспечивает функции простого управления, мониторинга и составления отчетов без необходимости установки локальной консоли. Приложение использует веб-сервер Apache HTTP Web Server 2.2 и может быть установлено на один сервер с SC либо на отдельный. Microsoft IIS не поддерживается. С помощью этой консоли можно устанавливать защищенное соединение с главным Сервером администрирования и с виртуальными Серверами администрирования.
- Агенты обновлений работаю как односторонние посредники между сервером управления и управляемыми узлами. Они используются для распространения установочных пакетов, обновлений, синхронизации групп и т. п. Если управляемый узел должен выполнить синхронизацию по расписанию или отправить события, он устанавливает соединение напрямую с Сервером администрирования. Недоступность Сервера администрирования для всех узлов иногда вызывает неудобство, поэтому в SC9 была добавлена функциональность шлюза соединений, что превратило агенты обновлений в полноценные шлюзы, работающие в обоих направлениях соединения. Создание цепей таких шлюзов невозможно.

Kaspersky Security Network

SC9 и KES8 тесно интегрированы с Kaspersky Security Network (KSN), которая является облачной базой данных репутации файлов и URL-адресов (AK8 и KAV 6.0 MP4 не интегрированы с KSN). Миллионы ее участников по всему миру предоставляют KSN информацию о подозрительных действиях. Эти данные комбинируются с собственными списками «Лаборатории Касперского», содержащими миллиарды записей о файлах и веб-ресурсах с заданным уровнем надежности. Это позволяет улучшить точность определений компонентов Файловый-антивирус (OAS и ODS), Веб-антивирус, Контроль приложений и Системный монитор на клиентской стороне в случае использования KES8. Эта технология не является новой для «Лаборатории Касперского», поскольку она уже в течение нескольких лет используется в домашних продуктах.

Основные преимущества:

- Более быстрый, по сравнению с традиционными методами, такими как сигнатурый или эвристический анализ, ответ на новые угрозы.
- Снижение вероятности ложных срабатываний.
- Никакие конфиденциальные данные пользователей не отправляются в облачную среду.
- Географические ограничения отсутствуют.

С технической точки зрения это работает следующим образом. Управляемый узел с установленным KES8 перехватывает файлы с помощью драйвера klif.sys и сканирует их с использованием традиционных методов (сигнатурных анализ -> эвристический анализ). Кроме того, возможно

выполнение проверки этого файла в соответствии с данными из облака, причем, вердикт, полученный этим способом, отменяет вердикт, полученный KES8 самостоятельно.

Сначала узел проверяет свой локальный кэш (1) -> если там нет информации, он отправляет запрос на сервер SC на порт TCP 13111, выполняющего функцию прокси-сервера KSN, а также KSN-кэша (2) -> прокси-сервер KSN проверяет свой кэш (3) -> если здесь нет информации, прокси-сервер KSN отправляет запрос на порт TCP 443 серверов KSN в облаке -> прокси-сервер KSN получает ответ от облака и отправляет его узлу. Результат запроса кэшируется на прокси-сервере KSN и на локальном узле.

Каждая запись в кэше имеет собственное значение времени жизни (TTL). Если следующий запрос возникает до истечения этого периода, ответ будет получен из локального кэша или кэша прокси-сервера KSN. Если следующий запрос поступает по истечении времени жизни записи в кэше, выполняется описанная выше операция. KSN работает только с исполняемыми файлами (PE) и URL-адресами. Кроме того, можно настроить управляемые узлы на отправку запросов напрямую в облако (5), но в этом случае нельзя будет использовать кэш прокси-сервера KSN, и объем трафика увеличится. Это возможно, только если управляемые узлы имеют доступ к Интернету.

Серверы KSN не получают никакой конфиденциальной информации со стороны клиента, кроме информации, оговоренной в лицензионном соглашении, а имеено:

- информацию о версии и типе установленного ПО «Лаборатории Касперского»;
- информацию о версии установленной операционной системы;
- информацию обо всех проверенных объектах: хэш-суммы файлов (MD5) и URL-адреса, а также о решении продукта относительно их;
- информацию о любых объектах, которые, возможно, являются вредоносными программами: размер, дата создания, цифровые подписи файлов, внутренний идентификатор папки, содержащей объект, сработавшая сигнатура, идентификатор сработавшей защитной подсистемы продукта «Лаборатории Касперского» и причины, по которой объект был сочтен потенциально вредоносным.

Необходимо отметить, что KSN не использует Агенты администрирования и Агенты обновлений, поэтому при наличии большого количества удаленных офисов с плохой связью с головным филиалом и отсутствием Сервера администрирования есть смысл настроить управляемые узлы на прямое подключение к облаку KSN, если их подключение к Интернету лучше, чем связь между офисами.

Трафик KSN меняется динамически, и его объем может варьироваться в зависимости от многих факторов: программы, работающие на узле, включенные модули, содержимое кэша и т. п. В целом для узла примерно с 450 000 объектов сканирования объем трафика приблизительно составит:

Сценарий
Всего байт
Исходящий трафик, байт
Входящий трафик, байт

Полное сканирование (без кэша)
504 000
247 713
255 270
Нормальное функционирование (в час)
136 754
80 645
56 108

На периоды нормального функционирования нужно запланировать следующий уровень нагрузки на каналы связи для трафика KSN между Security Center и клиентскими узлами:

Ширина канала связи до базы данных
10 %
использование канала связи
20 %
использование канала связи
30 %
использование канала связи
40 %
использование канала связи
Количество клиентских узлов
32
Кбит/с
11
23
34
45
64
Кбит/с
23
45
68
91
128
Кбит/с
45
91
136
182
384
Кбит/с
136
272
408
545

768
Кбит/с
272
545
817
1089
1544
Кбит/с
547
1095
1642
2190

Что касается воздействия KSN на время сканирования, то тесты показывают, что время полного сканирования с отключенной технологией кэширования и функцией «Сканировать только новые и измененные файлы» в различных ситуациях (от ~170 000 файлов (370 ГБ) до 265 000 файлов (440 ГБ)) не зависит от использования KSN.

Сетевая нагрузка
Основная сетевая нагрузка возникает в следующих ситуациях:
— начальное развертывание продукта;
— начальное обновление базы данных антивируса;
— подключение клиентов к серверу AK/SC;
— регулярное обновление базы данных антивируса;
— обработка событий на сервере AK/SC.

Ниже приведены точные значения для AK8 и KAV 6.0 MP4 в описанных выше ситуациях.

Сценарий
Трафик с клиента на сервер
Трафик с сервера на клиент
Общий трафик
Начальное развертывание Агента администрирования 8.0 CF1
0,4 МБ
14 МБ
14,4 МБ
KAV 6.0 MP4 CF1, начальное
развертывание (с обновленными
4 МБ
94 МБ
98 МБ
базами данных)

Сценарий
Трафик с клиента на сервер
Трафик с сервера на клиент

Общий трафик
Начальное обновление баз данных антивируса*
0,5 МБ
9 МБ
9,5 МБ
Проверка видимости
5 КБ
6 КБ
11 КБ
Синхронизация**
8–20 КБ
11–50 КБ
20–70 КБ
Регулярное обновление базы данных антивируса*
35 КБ
300 КБ
355 КБ
Обработка события «Обнаружен вирус»
9,4 КБ
6,3 КБ
15,7 КБ

- Значения зависят от версии антивируса и базы данных и могут слегка отличаться.
    - Значения могут отличаться в различных ситуациях и при изменении параметров.

Начальное развертывание Kaspersky Anti-Virus 6.0 MP4 CF1 с использованием многоадресного режима агентов обновлений. Этот режим позволяет уменьшить объем трафика в N раз, где N — общее число управляемых узлов в группе администрирования.
Трафик от агента обновлений на
сервер
Трафик от сервера
на агент обновлений
Трафик многоадресной
доставки от агента обновлений на
все клиенты
Общий трафик
4 МБ
94 МБ
103 МБ
201 МБ

Трафик для SC9 и KES8 в целом не отличается от AK8 и KAV 6.0 MP4:
Сценарий
Трафик с клиента на сервер
Трафик с сервера на клиент

Общий трафик
Обработка одного события
7–8 КБ
7–8 КБ
14–15 КБ
Обнаружение угроз (тест EICAR)
27 КБ
26 КБ
53 КБ
9 событий по обнаружению угроз
100 КБ
53 КБ
153 КБ
Задача «Новое сканирование на вирусы»
9–17 КБ
13–19 КБ
22–36 КБ
(по умолчанию)
Новая политика
(сходная по параметрам по умолчанию)
27–42 КБ
37–48 КБ
65–90 КБ

Сценарий
Трафик с клиента на сервер
Трафик с сервера на клиент
Общий трафик
Синхронизация после изменения
одного параметра
политики
11 КБ
13 КБ
24 КБ
Синхронизация после изменения
одного параметра
групповой задачи
10 КБ
13 КБ
23 КБ
Начальная синхронизация после
Установки NA9+KES8, включая
политику по умолчанию и 3
групповые задачи
369 КБ
464 КБ

833 КБ
Проверка видимости
9 КБ
7 КБ
16 КБ
Синхронизация по требованию без изменений на управляемом
узле
47 КБ
16 КБ
63 КБ
Установка NA9
387 КБ
14,8 МБ
15,2 МБ
Установка KES8 с использованием
NA9
1,8 МБ
270 МБ
272 МБ
Установка пакета
NA9+KES8
2,2 МБ
284,8 МБ
287 МБ
Начальное обновление
баз данных антивируса*
1,4 МБ
33,9 МБ
35,3 МБ
Ежедневные обновления антивируса
(инкрементное обновление
с интервалом в 20 часов)*
0,5 МБ
10 МБ
10,5 МБ
Общий ежедневный трафик
(с обновлениями, без обнаружения сети и KSN)
3 МБ
15 МБ
18 МБ

- Значения могут слегка различаться.