Общество с ограниченной ответственностью «Звезда»
ООО «Звезда»
125124, г. Москва, ул. 3-я Ямского Поля, д. 32
ОГРН 1217700119702
ИНН 7730263051/КПП 771401001
Тел.: 8 (495) 668-86-00

ОКПД2 62

ОКС 35.080

УТВЕРЖДАЮ
Генеральный директор
ООО «Звезда»
_____ Мироненко Р.В.
«2» мая 2023 г.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

ВСТРАИВАЕМОЙ ГИПЕРКОНВЕРГЕНТНОЙ ВИРТУАЛИЗАЦИИ, ВКЛЮЧАЮЩЕЕ ГИПЕРВИЗОР 1ГО ТИПА И СИСТЕМУ УПРАВЛЕНИЯ И МОНИТОРИНГА ГИПЕРКОНВЕРГЕНТНЫМ ВЫЧИСЛИТЕЛЬНЫМ КЛАСТЕРОМ

«ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «ЗВЕЗДА» АЛЬКОР»

Руководство по безопасности ПО

RU.ВНРЯ.00003-01 ЭД

Оглавление

Введение

Звезда Алькор — это программное обеспечение для управления кластером виртуализации. Вы должны быть системным администратором, знакомым с принчипами работы операционных систем и средами виртуализации перед его использованием.

Различные компоненты Звезда Алькор имеют справочные страницы и интерактивную справку. Однако это руководство поможет вам ознакомиться с системой, объяснив наиболее распространенные операции, сгруппированные по назначению.

Архитектура безопасности в ПО Звезда Алькор

ПО Звезда Алькор был разработан для работы на внутренних доверенных системах. Таким образом, модель безопасности работает по принципу «все или ничего».

До версии 2.3 весь код ПО Звезда Алькор выполнялся от имени пользователя root. Начиная с версии 2.4 можно запускать все демоны, кроме демона узла и демона мониторинга, от имени пользователя без полномочий root, указав имена пользователей и группы во время сборки. Демон узла по-прежнему требует привилегий root для создания логических томов, устройств DRBD, запуска экземпляров и т. д. Команды кластера могут выполняться от имени root или пользователями в группе, указанной во время сборки. Демону мониторинга требуются привилегии суперпользователя, чтобы иметь возможность доступа и представления информации, доступной только для суперпользователя (например, вывод команды xm Xen).

Для хоста, на котором установлено программное обеспечение ПО Звезда Алькор, но не присоединено к кластеру, никаких изменений в системе не происходит.

Для хоста, присоединившегося к кластеру, есть очень важные изменения:

- У хоста будет заменен ключ хоста SSH на ключ кластера (тот, который был у исходного узла при создании кластера).
- Новый открытый ключ будет добавлен в файл author_keys root, предоставляя root-доступ ко всем узлам кластера. Приватная часть ключа также распространяется на все узлы. Старые файлы переименовываются.
- Связь между узлами шифруется с использованием SSL/TLS. Общий ключ и сертификат совместно используются всеми узлами кластера. В настоящее время CA не используется.

Демон узла ПО Звезда Алькор будет принимать запросы RPC от любого хоста, который является главным кандидатом в кластере, и в результате этих запросов он будет выполнять следующие операции:

- выполнение команд в каталоге /etc/alkor/hooks;
- создание дисков DRBD между ним и IP-адресом, который ему сказали;
- перезаписать определенный список файлов на хосте.

Как только узел присоединен, он становится равным всем другим узлам в кластере по отношению к SSH и равным всем узлам-кандидатам, не являющимся главными, по отношению к RPC, а безопасность кластера определяется самым слабым узел.

Обратите внимание, что только ключ SSH позволит другим машинам выполнять любую команду на этом узле; метод RPC будет работать только:

- четко определенные команды для создания, удаления, активации логических томов, устройств drbd, запуска/остановки экземпляров и т. д.;
- запускать четко определенные команды SSH на других узлах в кластере

- скрипты в каталоге /etc/alkor/hooks
- скрипты в каталоге /etc/alkor/restricted-commands, если эта функция была включена во время сборки (см. ниже)

Поэтому важно убедиться, что содержимое каталогов /etc/alkor/hooks и /etc/alkor/restricted-commands находится под наблюдением и может быть заполнено только надежными источниками.

Запрещенные команды

Функция ограниченных команд позволяет администратору выполнять любые команды в каталоге /etc/alkor/restricted-commands, если эта функция была включена во время сборки, с учетом следующих ограничений:

- Нельзя передавать параметры
- Нельзя передавать абсолютный или относительный путь, только имя файла
- Каталог /etc/alkor/restricted-commands должен принадлежать пользователю root:root и иметь режим 0755 или более строгий.
- Исполняемые файлы должны быть обычными файлами или символическими ссылками и должны выполняться пользователем root:root

Обратите внимание, что невозможно перечислить содержимое каталога, и существует преднамеренная задержка при попытке выполнить несуществующую команду (для замедления атак по словарю).

Поскольку для ПО Звезда Алькор эта функциональность не нужна и предоставляется только как способ помочь администрировать или восстанавливать узлы, решение о том, включать или нет функцию ограниченных команд, принимается администратором.

По умолчанию эта функция отключена.

Кластерные проблемы безопасности

Как упоминалось выше, существует несколько способов связи между узлами кластера:

- На основе SSH для трафика большого объема, такого как дампы изображений, или для низкоуровневых команд, например. перезапуск демона узла ПО Звезда Алькор
- Связь RPC между мастером и узлами
- DRBD трафик репликации диска в реальном времени
- Трафик SSH (после первоначального входа в систему на новом узле) общим ключом SSH для всего кластера.

Связь RPC между мастером и узлами защищена с помощью шифрования SSL/TLS. Сервер должен иметь общий сертификат SSL/TLS для всего кластера. Выступая в качестве клиента, узлы используют индивидуальный сертификат SSL/TLS. При входящих запросах сервер проверяет, является ли сертификат клиента сертификатом главного кандидата, сверяя его отпечаток со

списком известных сертификатов главного кандидата. Мы решили не использовать ЦС (пока), чтобы упростить обработку ключей.

Трафик DRBD не защищен шифрованием, так как DRBD его не поддерживает. Поэтому рекомендуется реализовать межсетевой экран на уровне хоста или использовать отдельный диапазон IP-адресов для трафика DRBD (это поддерживается в ПО Звезда Алькор за счет использования вторичного интерфейса), который не маршрутизируется за пределы кластера. Соединения DRBD защищены от ошибочных подключений к другим машинам (что может произойти из-за проблем с программным обеспечением) и от

Отслеживание соединений с других машин с использованием общего секрета, которым обмениваются запросы RPC от мастера к узлам при настройке устройства.

Главный демон

Инструменты командной строки для управления связью с демоном выполняются через сокет UNIX, чьи разрешения сбрасываются на 0660 после прослушивания, но перед обслуживанием запросов. Эта защита на основе разрешений задокументирована и работает в Linux, но не является переносимой; однако в настоящее время ПО Звезда Алькор не работает в системах, отличных от Linux.

Демон luxid

Демон luxid (автоматически включается, если confd включен во время сборки) обслуживает локальные (сокет UNIX) запросы о конфигурации во время выполнения. Ответить на них означает поговорить с другими узлами кластера точно так же, как это делает masterd. См. примечания для masterd относительно защиты на основе разрешений.

Демон conf

В ПО Звезда Алькор демон confd (если он включен во время сборки) обслуживает инициированные сетью запросы о частях конфигурации статического кластера.

Если ПО Звезда Алькор не настроен (во время сборки) на использование отдельных пользователей, confd имеет доступ ко всем файлам, связанным с ПО Звезда Алькор (включая внутренние SSL-сертификаты RPC). Это делает его немного более чувствительным к ошибкам (удаленный злоумышленник может получить прямой доступ к внутрикластерному RPC), поэтому для усиления безопасности рекомендуется:

- отключите confd во время сборки, если он (и luxid) не нужен в вашей настройке.
- настроить ПО Звезда Алькор (во время сборки) для использования отдельных пользователей, чтобы демон confd также не имел доступа к сертификатам SSL/TLS сервера.

- добавьте правила брандмауэра для защиты порта confd или привяжите его к доверенному адресу. Убедитесь, что все узлы могут получить доступ к демону, поскольку этого требует демон мониторинга.

Демон мониторинга

Демон мониторинга предоставляет информацию о состоянии и производительности кластера по протоколу HTTP. В настоящее время он не зашифрован и не аутентифицирован, поэтому настоятельно рекомендуется установить надлежащие правила брандмауэра для предотвращения нежелательного доступа.

Демон мониторинга работает от имени пользователя root, поскольку ему необходимо иметь доступ к привилегированной информации (такой как состояние экземпляров, предоставленное гипервизором Xen). Тем не менее последствия для безопасности смягчаются тем фактом, что агент предоставляет только функции отчетности, без возможности фактического изменения состояния кластера.

Удаленный API

Начиная с ПО Звезда Алькор 2.0, трафик удаленного API по умолчанию шифруется с использованием SSL/TLS. Он поддерживает обычную аутентификацию в соответствии с RFC 2617. Пользователям могут быть предоставлены различные возможности. Подробности можно найти в документации RAPI.

Пути для сертификата, закрытого ключа и файлов CA, необходимых для SSL/TLS, будут установлены во время настройки источника. Симлинки или параметры командной строки могут использоваться для использования разных файлов.

RAPI по умолчанию привязывается ко всем интерфейсам и разрешает запросы только для чтения без необходимости аутентификации. В случае, если один из интерфейсов, к которому привязывается RAPI, является общедоступным, это позволит любому человеку в мире прочитать состояние кластера, раскрывая потенциально полезные данные, такие как имена экземпляров, их IP-адреса и т. д. Поскольку RAPI daemon также находится на главном узле, DoS-атаки могут привести к сбоям в работе ПО Звезда Алькор или проблемам с экземплярами, расположенными на главном узле.

Мы рекомендуем вам уменьшить поверхность атаки, либо поместив RAPI в среду, где вы можете контролировать доступ к нему, либо, если вам нужно сделать его общедоступным, используйте различные параметры демона RAPI, чтобы ограничить функциональность только тем, что вам нужно. Параметры демона RAPI лучше всего добавлять в /etc/default/ПО Звезда Алькор, переменную RAPI_ARGS. Некоторыми примерами ситуаций, когда вы можете захотеть раскрыть RAPI, являются перемещения экземпляров между кластерами, которые можно выполнить только через RAPI.

Если вы вообще не используете RAPI, мы рекомендуем вам заблокировать его, привязав к петлевому интерфейсу. Это можно сделать, передав параметр -b 127.0.0.1 демону RAPI. Запрещать запуск RAPI или делать его недоступным на главном узле не рекомендуется, так как

наблюдатель выполняет проверки работоспособности и пытается повторно перезапустить демон.

Если вы собираетесь использовать RAPI и сделать его общедоступным, обязательно используйте флаг --require-authentication, отключающий анонимные HTTP-запросы.

В настоящее время ПО Звезда Алькор не может адекватно защитить пользователей от DoS-атак на основе повторного согласования параметров HTTPS на стороне клиента из-за отсутствия в библиотеке Python OpenSSL необходимых функций. Чтобы защитить себя от них, необходимо использовать HTTPS-прокси, правильно обрабатывающий это (например, nginx). Полезные опции для настройки RAPI для работы с прокси:

-p PORT для разрешения использования прокси порта RAPI по умолчанию.

--no-ssl для отключения SSL, так как он все равно будет обрабатываться прокси

Межкластерные перемещения экземпляров

Для перемещения экземпляров между кластерами разные кластеры должны иметь возможность взаимодействовать друг с другом по защищенному каналу. До ПО Звезда Алькор 2.1 включительно кластеры были автономными объектами и не знали о других кластерах. С ПО Звезда Алькор 2.2 кластеры могут обмениваться данными, если токены (сертификат шифрованиясъел) ранее был обменен доверенной третьей стороной.

KVM-безопасность

При запуске экземпляров KVM в ПО Звезда Алькор доступны три модели безопасности: «None», «Пользователь» и «Пул».

В соответствии с моделью безопасности экземпляры «none» по умолчанию запускаются от имени пользователя root. Это означает, что если экземпляр взломан, он сможет владеть хост-узлом и, следовательно, кластером ПО Звезда Алькор. Это модель по умолчанию и единственная доступная для ПО Звезда Алькор

В модели безопасности «Пользователь» экземпляр запускается от имени пользователя, указанного параметром гипервизора «security_domain». Это упрощает запуск всех экземпляров в качестве непривилегированных пользователей и позволяет вручную назначать определенных пользователей для определенных экземпляров или наборов экземпляров. Если у указанного пользователя нет разрешений, экземпляру с нарушенной тюрьмой потребуется некоторое локальное повышение привилегий, прежде чем он сможет взять на себя управление узлом и кластером. Тем не менее, взломанный экземпляр может повлиять на другие экземпляры, работающие под тем же пользователем.

В модели безопасности «пул» глобальный пул uid на уровне кластера используется для запуска каждого экземпляра на одном и том же узле под другим пользователем. uid в пуле кластера можно установить с помощью alkor-cluster init и alkor-cluster Modify, и они должны соответствовать существующим пользователям на всех узлах. Затем ПО Звезда Алькор выделит по одному экземпляру для каждого экземпляра по мере необходимости. Таким образом,

экземпляр взломанной тюрьмы не сможет повлиять на любой другой. Поскольку ПО Звезда Алькор распределяет пользователей случайным образом для каждого узла, в этом режиме нет возможности убедиться, что конкретный экземпляр всегда запускается от имени определенного пользователя. Используйте для этого режим «пользователь».

В дополнение к этим мерам предосторожности, если вы хотите, чтобы экземпляры не отправляли трафик в сеть вашего узла, вы можете использовать правило iptables, например:

```
iptables -A ВЫВОД -m owner --uid-owner <uid>[-<uid>] -j ЖУРНАЛ \
  --log-prefix "ПО Звезда Алькор uid pool user network traffic"
iptables -A ВЫВОД -m owner --uid-owner <uid>[-<uid>] -j DROP
```

Это не повлияет на обычный трафик экземпляра (который исходит от tapX, выделенного для экземпляра, и может быть отфильтрован или подвергнут соответствующим маршрутам политики), но остановит любой пользовательский трафик, который может исходить от взломанного экземпляра.