МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ

ОДЕССКИЙ Национальный политехнический университет

Институт компьютерных систем

Кафедра Информационных технологий

GRID технологии

Вариант №16

Тема: «Службы хранения данных. Виртуальная сеть Azure.»

Выполнил:

студент группы АД-171

Поликарпов А.В.

Проверил:

Гришин С.И.

Одесса 2019

# Что такое виртуальная сеть Azure?

Виртуальная сеть Azure позволяет ресурсам Azure различных типов (например, виртуальным машинам Azure) обмениваться данными друг с другом, через локальные сети и через Интернет. Виртуальная сеть ограничена одним регионом Azure. [Регион](https://azure.microsoft.com/global-infrastructure/regions/) Azure — это набор центров обработки данных, развернутых в пределах периметра, определяемого задержкой, и соединенных между собой выделенной региональной сетью с низкой задержкой.

Виртуальные сети состоят из подсетей. Подсеть — это диапазон IP-адресов в виртуальной сети. Подсети, как и виртуальные сети, не выходят за пределы одного региона Azure.

Несколько виртуальных сетей из разных регионов можно подключить между собой с помощью пиринга виртуальных сетей.

Виртуальная сеть Azure предоставляет описанные ниже основные возможности.

## Изоляция и сегментирование

Вы можете реализовать несколько виртуальных сетей в пределах [подписки](https://docs.microsoft.com/ru-ru/azure/azure-glossary-cloud-terminology?toc=%2fazure%2fvirtual-network%2ftoc.json#subscription) и [региона](https://docs.microsoft.com/ru-ru/azure/azure-glossary-cloud-terminology?toc=%2fazure%2fvirtual-network%2ftoc.json#region) Azure.Все виртуальные сети изолированы друг от друга. Для каждой виртуальной сети можно сделать следующее:

* Указать пользовательское пространство частных IP-адресов, в котором используются общедоступные и частные адреса (RFC 1918). Azure назначает ресурсам в виртуальной сети частный IP-адрес из определенного вами адресного пространства.
* Разделить виртуальную сеть на подсети и выделить каждой из них часть адресного пространства виртуальной сети.
* Использовать разрешение имен Azure или указать собственный DNS-сервер, который будут использовать ресурсы в виртуальной сети.

## Обмен данными через Интернет

По умолчанию все ресурсы в виртуальной сети могут устанавливать исходящие подключения к Интернету. Можно также установить входящее подключение к ресурсу, присвоив ему общедоступный IP-адрес, или общедоступный экземпляр Load Balancer.Общедоступный IP-адрес или общедоступную подсистему балансировки нагрузки также можно использовать для управления исходящими подключениями.

## Обмен данными через локальные ресурсы

Локальные компьютеры и сети можно подключить к виртуальной сети, используя любое сочетание следующих способов:

* **Виртуальная частная сеть (VPN) типа "точка — сеть".** Устанавливается между виртуальной сетью и отдельным компьютером в вашей сети. Необходимо настроить подключение для каждого компьютера, который требуется подключить к виртуальной сети. Этот тип подключения идеально подходит для новичков, не умеющих работать в Azure, или для разработчиков, так как при его использовании существующую сеть почти не нужно менять. Обмен данными между компьютером и виртуальной сетью осуществляется через Интернет с помощью зашифрованного туннеля.Дополнительные сведения см. в разделе о [VPN-подключении "точка — сеть"](https://docs.microsoft.com/ru-ru/azure/vpn-gateway/vpn-gateway-about-vpngateways?toc=%2fazure%2fvirtual-network%2ftoc.json#P2S).
* **VPN-подключение типа "сеть — сеть".** Устанавливается между локальным VPN-устройством и VPN-шлюзом Azure, развернутым в виртуальной сети. Используя такой тип соединения, авторизованные локальные ресурсы могут получить доступ к виртуальной сети. Обмен данными между локальным VPN-устройством и VPN-шлюзом Azure осуществляется через Интернет с помощью зашифрованного туннеля.Дополнительные сведения см. в разделе о [VPN-подключении "сеть — сеть"](https://docs.microsoft.com/ru-ru/azure/vpn-gateway/vpn-gateway-about-vpngateways?toc=%2fazure%2fvirtual-network%2ftoc.json#s2smulti).
* **Azure ExpressRoute.** Устанавливается между вашей сетью и Azure через участник ExpressRoute. Это подключение является закрытым. Трафик не проходит через Интернет. Дополнительные сведения см. в разделе [ExpressRoute (частное подключение)](https://docs.microsoft.com/ru-ru/azure/vpn-gateway/vpn-gateway-about-vpngateways?toc=%2fazure%2fvirtual-network%2ftoc.json#ExpressRoute).

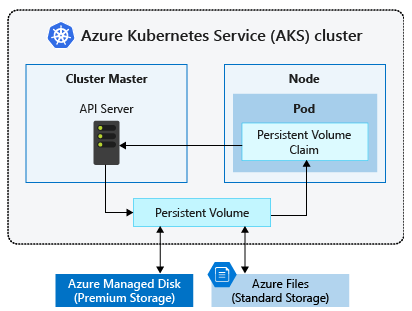
## Фильтрация сетевого трафика

Сетевой трафик между подсетями можно фильтровать следующими способами:

* **Группы безопасности.** Группы безопасности сети и приложения могут содержать несколько правил безопасности относительно входящего и исходящего трафика, что позволяет фильтровать его по исходному и конечному IP-адресу, порту и протоколу.Дополнительные сведения см. в разделах о [группах безопасности сети](https://docs.microsoft.com/ru-ru/azure/virtual-network/security-overview#network-security-groups) и [группах безопасности приложений](https://docs.microsoft.com/ru-ru/azure/virtual-network/security-overview#application-security-groups).
* **Виртуальные сетевые модули.** Виртуальный сетевой модуль представляет собой виртуальную машину, которая выполняет сетевую функцию (например, брандмауэр, оптимизация WAN и др.). Список доступных сетевых виртуальных модулей, которые можно развернуть в виртуальной сети, см. на странице [Azure Marketplace](https://azuremarketplace.microsoft.com/marketplace/apps/category/networking?page=1&subcategories=appliances).

**Возможности хранения данных в Службе Azure Kubernetes (AKS)**

Приложениям, работающим в Службе Azure Kubernetes (AKS), может потребоваться хранить и извлекать данные. Для некоторых рабочих нагрузок приложений можно использовать быстрое локальное хранилище данных на узле, которое не требуется после удаления элементов pod. Другим рабочим нагрузкам приложений может требоваться постоянное хранилище на обычных томах данных, размещенных на платформе Azure. Нескольким элементам pod может потребоваться совместно использовать одни тома данных или повторно подключать тома данных, если pod перенесен на другой узел. Наконец, может потребоваться внедрить конфиденциальные данные или данные конфигурации приложения в элементы pod.



## Рис. 1 - элементы pod

## **Тома**

Приложениям часто нужна возможность хранить и извлекать данные. Так как Kubernetes обычно рассматривает отдельные pod как временные, высвобождаемые ресурсы, доступны различные подходы для использования и хранения данных приложений. Тома представляет способ хранения, извлечения и сохранения данных элементов pod на протяжении жизненного цикла приложения.

Традиционные тома для хранения и извлечения данных создаются как ресурсы Kubernetes, обслуживаемые службой хранилища Azure. Можно вручную создавать эти тома данных и напрямую назначать их элементам pod или настроить Kubernetes для их автоматического создания. Эти тома данных могут использовать диски Azure или файлы Azure.

* Диски Azure можно использовать для создания ресурсов DataDisk в Kubernetes. Диски могут использовать службу хранилища Azure ценовой категории "Премиум" на основе высокопроизводительных дисков SSD или службу хранилища Azure ценовой категории "Стандартный" на основе обычных жестких дисков. Для большинства производственных рабочих нагрузок и рабочих нагрузок разработки следует использовать службу хранилища ценовой категории "Премиум". Диски Azure подключаются в режиме ReadWriteOnce, поэтому они доступны только одному узлу.Для томов хранилища, к которым одновременно могут обращаться несколько узлов, следует использовать файлы Azure.
* Файлы Azure можно использовать для подключения к элементам pod общей папки SMB 3.0, размещенной в учетной записи хранения Azure. Служба файлов обеспечивает обмен данными между несколькими узлами и элементами pod. В настоящее время служба файлов позволяет использовать только службу хранилища Azure ценовой категории "Стандартный на основе обычных жестких дисков.

В Kubernetes тома могут представлять собой не просто традиционный диск, используемый для хранения и извлечения данных. Тома Kubernetes могут также применяться для внедрения в pod данных, используемых контейнерами. Распространенные дополнительные типы томов в Kubernetes приведены ниже.

* emptyDir — этот том обычно используется в качестве временного хранилища для pod.Все контейнеры в pod могут обращаться к данных в томе. Данные, записанные в том этого типа, хранятся только в течение времени существования pod. Этот том удаляется вместе с pod. Как правило, этот том использует базовое локальное дисковое хранилище узла, но может существовать и только в памяти узла.
* Secret — этот том используется для внедрения в pod конфиденциальных данных, например паролей. Сначала создается Secret с помощью API Kubernetes. При определении pod или развертывания можно запросить определенный Secret. Secret предоставляются только узлам, на которых запланирован запуск элемента pod, требующего этот Secret. Secret сохраняется в tmpfs, а не записывается на диск. При удалении с узла последнего pod, которому нужен секрет, данный Secret удаляется из tmpfs. Тома Secret хранятся в указанном пространстве имен и доступны только элементам pod в этом пространстве имен.
* configMap — этот тип тома используется для внедрения в элементы pod пар свойств "ключ-значение", например сведений о конфигурации приложения. Вместо того, чтобы определить данные конфигурации приложения в образе контейнера, их можно определить как ресурс Kubernetes, который можно легко обновлять и применять к новым экземплярам pod по мере их развертывания. Как и при использовании Secret, сначала следует создать ConfigMap с помощью API Kubernetes. Затем этот ConfigMap можно запросить при определении pod или развертывания. Тома ConfigMap хранятся в указанном пространстве имен и доступны только элементам pod в этом пространстве имен.

## **Постоянные тома**

Тома, которые определяются и создаются в ходе жизненного цикла pod, существуют только до удаления pod. Нередко элементам pod нужно сохранить используемое ими хранилище, если pod переносится на другой узел во время события обслуживания, особенно в наборах с отслеживанием состояния. Постоянный том — это ресурс хранилища, для создания и управления которым используется API Kubernetes. Этот том может существовать после истечения времени существования отдельного pod.

Для работы постоянного тома используются диски или файлы Azure. Как отмечалось в предыдущем разделе о томах, выбор дисков или файлов часто определяется потребностью в параллельном доступе к данным или необходимым уровнем производительности.

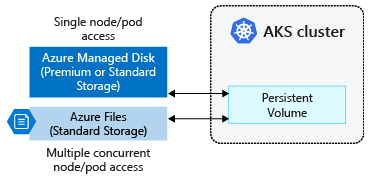


Рис. 2

Постоянный том может быть создан статически администратором кластера или может быть создан динамически сервером API Kubernetes. Если запланирован запуск элемента pod, запрашивающего хранилище, которое в настоящее время недоступно, Kubernetes может создать базовое хранилище на основе дисков или файлов Azure и подключить его к pod. Для динамической подготовки используется класс StorageClass. С его помощью можно определить, какой тип хранилища Azure необходимо создать.

## Классы хранилищ

Чтобы определить различные ценовые категории хранилищ, например "Премиум" и "Стандартный", можно создать класс StorageClass. Кроме того, класс StorageClass определяет политику reclaimPolicy. Эта политика reclaimPolicy управляет поведением базового ресурса хранилища Azure, когда pod удаляется и постоянный том может больше не требоваться. Базовый ресурс хранилища можно удалить или сохранить для использования другим pod в будущем.

В AKS создаются два начальных класса StorageClasses.

* default — использует службу хранилища Azure ценовой категории "Стандартный" для создания управляемого диска. Политика освобождения указывает, что базовый диск Azure удаляется при удалении pod, который его использовал.
* managed-premium — использует службу хранилища Azure ценовой категории "Премиум" для создания управляемого диска. Политика освобождения также указывает, что базовый диск Azure удаляется при удалении pod, который его использовал.

Если для постоянного тома не указан класс StorageClass, используется StorageClass по умолчанию. При запросе постоянных томов убедитесь, что они используют именно то хранилище, которое вам нужно. Можно создать класс StorageClass для удовлетворения дополнительных потребностей с помощью kubectl.

## **Утверждения постоянного тома**

## Утверждение PersistentVolumeClaim запрашивает хранилище на основе диска или файла, использующее определенный класс StorageClass, режим доступа и размер. Если ресурс для выполнения утверждения согласно определенному классу StorageClass отсутствует, сервер API Kubernetes может динамически подготовить базовый ресурс хранилища в Azure.Определение pod включает в себя подключение тома после его присоединения к pod.

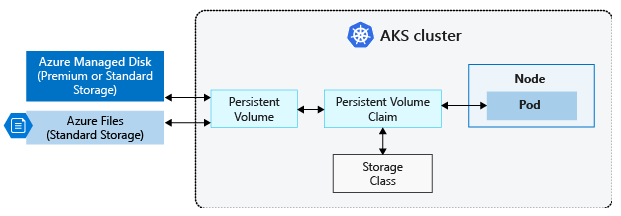


Рис. 3 - подключение тома после его присоединения к pod

Том PersistentVolume привязывается к утверждению PersistentVolumeClaim после назначения элементу pod запрашиваемого доступного ресурса хранилища. Постоянные тома и утверждения сопоставляются как один к одному.

При создании определения pod указывается утверждение постоянного тома для запроса требуемого хранилища. Затем указывается подключение volumeMount для приложений, предназначенное для чтения и записи данных.