**Что такое проверка подлинности?**

Проверка подлинности — это процесс установления личности пользователя или службы, которым требуется доступ к ресурсу. Она связана с запросом допустимых учетных данных у стороны, выполняющей вход. Это основа для создания субъекта безопасности, используемого для управления доступом и удостоверениями. Она определяет, является ли пользователь тем, кем представляется.

**Что такое авторизация?**

Проверка подлинности устанавливает личность пользователя, а авторизация — это процесс определения уровня доступа для пользователя или службы, прошедших проверку подлинности. Она указывает, к каким данным разрешено получить доступ и что с ними можно делать.

**Azure Active Directory (Azure AD)** предоставляет службы идентификации, позволяющие пользователям входить в облачные приложения Майкрософт и ваши собственные облачные приложения.

**Сравнение Azure AD и Active Directory**

В локальных средах Active Directory на Windows Server предоставляет службу управления удостоверениями и доступом, которую администрирует ваша организация. Azure AD — это облачная служба управления удостоверениями и доступом от корпорации Майкрософт.

**Azure AD предназначен для следующих пользователей:**

-ИТ-администраторы

-Разработчики приложений

-Пользователи

-Подписчики веб-служб

**Azure AD предоставляет следующие службы:**

-Аутентификация

Сюда входят проверки удостоверения для доступа к приложениям и ресурсам. Она также включает в себя предоставление таких функциональных возможностей, как самостоятельный сброс пароля, многофакторная проверка подлинности, пользовательский список запрещенных паролей и службы смарт-блокировки.

-Единый вход

Единый вход позволяет вам запоминать только одно имя пользователя и пароль для доступа к нескольким приложениям. Единое удостоверение привязывается к пользователю, что упрощает модель безопасности. Когда пользователь переходит на другую должность или увольняется из организации, изменения прав доступа производятся только в этом удостоверении, благодаря чему значительно сокращаются усилия, затрачиваемые на изменение или отключение учетных записей.

-Управление приложениями

Вы можете управлять облачными и локальными приложениями с помощью Azure AD. Такие возможности, как Application Proxy, приложения SaaS, портал "Мои приложения" (также называется панелью доступа) и единый вход, повышают удобство работы пользователей.

-Управление устройствами

Azure AD поддерживает не только учетные записи отдельных пользователей, но и регистрацию устройств. Регистрация позволяет управлять устройствами с помощью таких средств, как Microsoft Intune. Это также позволяет политикам условного доступа на основе устройств разрешать попытки доступа только от известных устройств независимо от учетной записи пользователя, запрашивающего доступ.

**Единый вход** позволяет пользователю выполнять вход один раз и использовать эти учетные данные для доступа к нескольким ресурсам и приложениям от разных поставщиков.

**Как подключить Active Directory к Azure AD?**

Самым популярным методом является использование Azure AD Connect. Azure AD Connect синхронизирует удостоверения пользователей между Active Directory в локальной среде и Azure AD.

**Многофакторная проверка подлинности** — это процесс, при котором во время входа в систему пользователь видит дополнительную форму идентификации. Примерами являются ввод кода на телефоне или сканирование отпечатка пальца.

Элементы для прохождения проверки подлинности делятся на следующие категории:

-что-то, что известно пользователю;

Это может быть адрес электронной почты и пароль.

-Что-то, что имеется у пользователя

Это может быть код, отправленный на мобильный телефон пользователя.

-натура самого пользователя.

Обычно какая-то биометрическая характеристика, например, отпечаток пальца или изображение лица, функции распознавания которых имеются на многих мобильных устройствах.

**Многофакторная идентификация Microsoft Azure AD** — это служба Майкрософт, которая предоставляет возможности многофакторной проверки подлинности.

**Следующие службы предоставляют возможности Многофакторной идентификации Microsoft Azure AD:**

-Azure Active Directory

-Многофакторная идентификация для Office 365

**Условный доступ** — это средство, которое используется Azure Active Directory, чтобы разрешить (или запретить) доступ к ресурсам на основе сигналов удостоверений. Это сигналы о личности пользователя, расположении пользователя и об устройстве, с которого пользователь запрашивает доступ.

-Условный доступ помогает ИТ-администраторам:

-Предоставить пользователям возможность продуктивной работы в любом месте в любое время.

-Защитить активы организации.

**Условный доступ полезен, когда вы хотите:**

-Требовать многофакторную проверку подлинности для доступа к приложению.

Можно указать, требуется ли многофакторная проверка подлинности для всех пользователей или только для некоторых, например администраторов.

Также можно указать, применяется ли многофакторная проверка подлинности ко всем сетям или только к ненадежным.

-Требовать доступ к службам только через утвержденные клиентские приложения.

Например, вы можете разрешить пользователям доступ к службам Office 365 с мобильного устройства, если они используют утвержденные клиентские приложения, например Outlook Mobile.

-Требовать от пользователя доступа к приложению только с управляемых устройств.

Управляемое устройство — это устройство, которое соответствует стандартам безопасности и соответствия требованиям.

-Блокировать доступ из ненадежных источников, например из неизвестных или неожиданных расположений.

Термин **система управления** описывает общий процесс установки правил и политик, а также контроля над соблюдением этих правил и политик.

**Управление доступом на основе ролей Azure (Azure RBAC)** – это система, суть которой заключается в том, что Azure предоставляет встроенные роли, описывающие общие правила доступа для облачных ресурсов. Кроме того, вы можете определять собственные роли. Каждая роль имеет набор прав доступа, связанных с этой ролью. Управление доступом на основе ролей применяется к **области**, которая представляет собой ресурс или набор ресурсов.

**К областям относятся:**

-Группа управления (коллекция нескольких подписок).

-Одна подписка.

-Группа ресурсов.

-Один ресурс.

**Используйте Azure RBAC, если вам требуется:**

-предоставление одному пользователю разрешения на управление виртуальными машинами в подписке, а другому — на управление виртуальными сетями;

-предоставление группе администраторов базы данных разрешения на управление базами данных SQL в подписке;

-предоставление пользователю разрешения на управление всеми ресурсами в группе ресурсов, включая виртуальные машины, веб-сайты и подсети;

-Предоставление приложению доступа ко всем ресурсам в группе ресурсов.

**К кому применяется Azure RBAC?**

-ИТ-администраторы. Эта группа отвечает за ИТ-ресурсы локально и в облаке. Группе требуется полный контроль над всеми ресурсами.

-Резервное копирование и аварийное восстановление. Эта группа отвечает за управление работоспособностью регулярного резервного копирования и запуск восстановления данных или системы.

-Затраты и выставление счетов. Сотрудники этой группы отслеживают затраты на технологии и составляют отчеты. Они также управляют внутренними бюджетами организации.

-Служба безопасности. Эта группа отслеживает инциденты безопасности, связанные с технологиями, и реагирует на них. Этой группе требуется постоянный доступ к файлам журнала и оповещениям системы безопасности.

**Как управлять разрешениями Azure RBAC?**

Чтобы управлять правами доступа, можно воспользоваться областью **Управление доступом (IAM) на портале Azure.** Здесь отображаются сведения о том, кто и к какой области имеет доступ и какие роли применяются. Здесь же можно предоставлять и отменять доступ.

**Блокировки ресурсов** предотвращают случайное удаление или изменение ресурсов.

**Как управлять блокировками ресурсов?**

Блокировками ресурсов можно управлять с помощью портала Azure, PowerShell, Azure CLI или из шаблона Azure Resource Manager.

**Какие уровни блокировки доступны?**

Вы можете применять блокировки к подписке, группе ресурсов или отдельному ресурсу. Можно установить уровень блокировки **CanNotDelete** или **ReadOnly**.

-**CanNotDelete** означает, что полномочные пользователи по-прежнему могут читать и изменять ресурсы, но не могут удалить ресурс, не удалив блокировку.

-**ReadOnly** означает, что полномочные пользователи могут читать ресурсы, но не могут удалять или изменять их. Применение этой блокировки аналогично предоставлению всем полномочным пользователям только разрешений, которые дает роль Читатель в Azure RBAC.

**Как удалить или изменить заблокированный ресурс?**

Хотя блокировка помогает предотвратить случайные изменения, вы все же можете вносить изменения, выполнив двухэтапный процесс. Чтобы изменить заблокированный ресурс, необходимо сначала снять блокировку.

**Azure Blueprints** может автоматически снова устанавливать блокировку ресурсов, если она будет удалена.

**Один из способов упорядочить связанные ресурсы** — разместить их в отдельных подписках. Группы ресурсов также можно использовать для управления связанными ресурсами. **Теги ресурсов** предоставляют дополнительные сведения, или метаданные, о ресурсах. Задачи, для которых нужны эти метаданные:

-Управление ресурсами. Теги позволяют работать с ресурсами, связанными с конкретными рабочими нагрузками, средами, подразделениями и владельцами.

-Управление затратами и оптимизация. Теги позволяют группировать ресурсы, чтобы вы могли составлять отчеты о затратах, распределять внутренние центры затрат, отслеживать бюджеты и прогнозировать затраты.

-Управление операциями. Теги позволяют группировать ресурсы в соответствии с тем, насколько важна их доступность для вашего бизнеса. Это группирование помогает формулировать соглашения об уровне обслуживания (SLA). Соглашение об уровне обслуживания — это гарантия уровня доступности и производительности, согласованного вами и вашими пользователями.

-Обеспечение безопасности. Теги позволяют классифицировать данные по уровню безопасности (например, общедоступные или конфиденциальные).

-Система управления и соответствие нормативным требованиям. Теги позволяют определять ресурсы, которые соответствуют требованиям системы управления или нормативным требованиям, например, стандарту ISO 27001. Теги также могут использоваться для обеспечения соблюдения стандартов. Например, вы можете требовать, чтобы все ресурсы были помечены именем владельца или отдела.

-Оптимизация и автоматизация рабочей нагрузки. Теги позволяют визуализировать все ресурсы, участвующие в сложных развертываниях. Например, можно пометить ресурс именем соответствующей рабочей нагрузкой или приложения, и использовать программное обеспечение, такое как Azure DevOps, для выполнения автоматизированных задач с этими ресурсами.

**Тег ресурса состоит из имени и значения.** Каждому ресурсу Azure можно назначить один или несколько тегов.

**Политика Azure** — это служба в Azure, которая позволяет создавать и назначать политики для контроля и аудита ресурсов, а также управлять ими. Эти политики гарантируют соблюдение различных правил и действий с конфигурациями ресурсов, что обеспечивает соответствие этих конфигураций корпоративным стандартам.

**Реализация политики в Политике Azure состоит из трех этапов:**

1.Создать определение политики.

Определение политики выражает, что следует оценивать и какие действия следует предпринять. Например, вы можете запретить развертывание виртуальных машин в определенных регионах Azure.

**Примеры определений политик:**

--Разрешенные номера SKU виртуальной машины.

--Допустимые расположения.

--Необходимо включить многофакторную проверку подлинности для учетных записей с разрешениями на запись для вашей подписки.

--Функция CORS не должна разрешать всем ресурсам доступ к вашим веб-приложениям.

--На ваших компьютерах должны быть установлены обновления системы.

2.Назначить определение ресурсам.

Чтобы реализовать определения политики, необходимо назначить определения ресурсам. Назначение политики — это определение политики в рамках определенной области. Эта область может быть группой управления (коллекцией нескольких подписок), одной подпиской или группой ресурсов.

Назначения политик наследуются всеми дочерними ресурсами в этой области. То есть политики, применяемые к группе ресурсов, применяются также ко всем ресурсам в этой группе. Вы можете исключить подобласть из назначения политики, если она не должна распространяться на некоторые дочерние ресурсы.

3.Проверить результаты оценки.

При оценке условия для существующих ресурсов каждый ресурс помечается как соответствующий или не соответствующий требованиям. Вы можете просматривать результаты по несоответствующим ресурсам и принимать необходимые меры.

**Инициатива Политики Azure** — это способ группирования связанных политик в один набор. Определение инициативы содержит все определения политики, чтобы отслеживать соответствие требованиям для более значимой цели.

В инициативу *Включения мониторинга в центре безопасности Azure* входят следующие определения политики:

-Мониторинг баз данных SQL без шифрования в Центре безопасности. Эта политика отслеживает базы данных и серверы SQL без шифрования.

-Мониторинг уязвимостей ОС в центре безопасности. Эта политика отслеживает серверы, которые не соответствуют настроенному базовому плану уязвимости ОС.

-Мониторинг отсутствия защиты конечных точек в Центре безопасности. Эта политика отслеживает серверы без установленного агента защиты конечных точек.

**Как определить инициативу?**

Вы можете определять инициативы на портале Azure или в программах командной строки. На портале Azure можно выполнить поиск в списке встроенных инициатив, уже предоставляемых Azure. Вы также можете создать собственное определение пользовательской политики.

**Azure Blueprints** позволяет определить повторяемый набор средств управления и стандартных ресурсов Azure, необходимых вашей организации, чтобы вам не пришлось настраивать такие компоненты, как Политика Azure, для каждой новой подписки. С помощью этого инструмента группы разработчиков могут быстро создавать и развертывать новые среды, зная, что они создаются в соответствии с требованиями организации, и использовать ряд встроенных компонентов для ускорения разработки и развертывания.

**Azure Blueprints осуществляет оркестрацию развертывания различных шаблонов ресурсов и других артефактов, таких как:**

-Назначения ролей

-Назначения политик

-Шаблоны Azure Resource Manager

-Группы ресурсов

**Реализация схемы в Azure Blueprints осуществляется за три шага:**

1.Создание схемы Azure Blueprints.

2.Назначение схемы.

3.Отслеживание назначений схемы.

Каждый компонент в определении схемы называется **артефактом**.

**ISO 27001** — это стандарт, который применяется к безопасности ИТ-систем, опубликованный Международной организацией по стандартизации.

Платформа **Cloud Adoption Framework** для Azure предоставляет проверенные рекомендации по переходу в облако. Cloud Adoption Framework позволяет создавать и внедрять технологические и бизнес-стратегии, необходимые для успешной работы в облаке.

Cloud Adoption Framework состоит из инструментов, документации и проверенных методик. Cloud Adoption Framework включает следующие этапы:

1.Определение стратегии.

2.Составление плана.

3.Подготовка организации.

4.Внедрение облака.

5.Управление и администрирование облачных сред.

**Определение стратегии**

Здесь вы обдумываете, почему переходите в облако и что хотите получить от этой миграции.

**При определении стратегии облачного бизнеса необходимо понимать экономику облака и учитывать влияние на бизнес, время выполнения работ, глобальный охват, производительность и многое другое. Последовательность действий на этом этапе.**

1.Определение и документирование причин.

2.Документирование результатов бизнеса.

3.Оцените финансовые соображения: оцените цели и определите ожидаемую прибыль от конкретного вложения.

4.Понимание технических соображений: оцените эти технические соображения при выборе и завершении вашего первого технического проекта.

**Составление плана.** **Последовательность действий на этом этапе.**

1.Цифровые активы. Проведите инвентаризацию существующих цифровых активов и рабочих нагрузок, которые планируете перенести в облако.

2.Первоначальное организационное выравнивание. Привлеките к проекту по миграции подходящих сотрудников с технической точки зрения и с точки зрения управления облаком.

3.План развития навыков. Разработайте план, который поможет сотрудникам развивать навыки, необходимые для работы в облаке.

4.План внедрения облака. Создайте комплексный план, объединяющий группы разработки, эксплуатации и бизнеса, направленный на общую цель внедрения облака.

**Подготовка организации. Последовательность действий на этом этапе.**

1.Руководство по настройке Azure. Ознакомьтесь с руководством по настройке Azure, чтобы узнать о средствах и подходах, используемых при создании зоны размещения.

2.Целевая зона Azure. Начните создавать подписки Azure, которые поддерживают основные сферы вашего бизнеса. Целевая зона включает в себя облачную инфраструктуру, а также возможности управления, учета и безопасности.

3.Развитие целевой зоны. Настройте целевые зоны, чтобы они соответствовали вашим потребностям в эксплуатации, управлении и безопасности.

4.Рекомендации. Начните с проверенных рекомендаций, которые помогут обеспечить масштабируемость и выполнимость задач по миграции в облако.

**Внедрение облака**

Cloud Adoption Framework разделяет этот этап на две части: миграция и инновации.

**Миграция. Этап миграции состоит из следующих шагов.**

1.Перенос первой рабочей нагрузки. Используйте руководство по миграции Azure для развертывания первого проекта в облаке.

2.Сценарии миграции. Используйте дополнительные подробные руководства для изучения более сложных сценариев миграции.

3.Рекомендации. Ознакомьтесь с контрольным списком рекомендаций по миграции в облако Azure, чтобы убедиться, что вы придерживаетесь рекомендуемых методов.

4.Улучшения процесса. Определите, как можно масштабировать процесс миграции и затратить меньше усилий.

**Инновации. Этап инноваций состоит из следующих шагов.**

1.Договоренность о ценности для бизнеса. Убедитесь, что инвестиции в инновации добавляют ценность для бизнеса и соответствуют потребностям клиентов.

2.Руководство по инновациям Azure. Воспользуйтесь этим руководством, чтобы ускорить разработку и воплотить вашу идею в минимально жизнеспособном продукте (MVP).

3.Рекомендации. Прежде чем двигаться дальше, убедитесь, что ваш прогресс соответствует рекомендациям.

4.Циклы обратной связи. Регулярно общайтесь с клиентами, чтобы убедиться в том, что вы учитываете их потребности в своей работе.

**Контроль и администрирование облачных сред**

На этом этапе вы разрабатываете стратегии управления облаком. С течением времени облачные активы будут изменяться, как и процессы и политики системы управления облаком. Необходимо создать устойчивые решения, которые можно постоянно оптимизировать.

**Управление. Этап миграции управления состоит из следующих шагов.**

1.Методология. Обдумайте, как в итоге должно выглядеть решение, а затем последовательно определите методологию: от первых шагов до полного управления облаком.

2.Тестирование производительности. Используйте средство оценки производительности системы управления, чтобы оценить текущее и будущее состояние и определить ожидания от применения платформы.

3.Первоначальная основа системы управления. Создайте минимально жизнеспособный продукт, который отражает первые шаги вашего плана по управлению.

4.Совершенствование первоначальной основы системы управления. Постепенно добавляйте элементы управления, которые устраняют реальные риски, по мере продвижения к итоговому решению.

**Управление: Этап управления состоит из следующих шагов.**

1.Определение базовых показателей управления. Определите минимальные обязательства по управлению операциями. Базовый план управления — это минимальный набор средств и процессов, которые должны применяться к каждому ресурсу в среде.

2.Определение бизнес-обязательств. Задокументируйте поддерживаемые рабочие нагрузки, чтобы определить операционные обязательства в соответствии с бизнес-целями и согласовать инвестиции в решения по управлению облаком для каждой рабочей нагрузки.

3.Расширение базовых показателей управления. Применяйте рекомендации для постепенного улучшения первоначальных базовых показателей управления.

4.Расширенные принципы эксплуатации и проектирования. Для рабочих нагрузок, требующих более высокого уровня бизнес-обязательств, выполните более тщательное изучение архитектуры, чтобы соблюсти требования к устойчивости и надежности.

**Создание стратегии управления подписками**

Существует три основных аспекта, которые следует учитывать при создании подписок и управлении ими: выставление счетов, управление доступом и ограничения подписки.

Вы можете создать один отчет по выставлению счетов для каждой подписки. Если у вас есть несколько отделов и вы хотите оформить "возвратный платеж" для расходов на облако, можно организовать подписки по отделам или проектам.

Подписка — это граница развертывания для ресурсов Azure. Каждая подписка связана с клиентом Azure Active Directory. Каждый клиент предоставляет администраторам возможность настроить детализированный доступ через определенные роли с помощью управления доступом на основе ролей Azure.

В подписках существуют ограничения ресурсов. Например, максимальное количество сетевых каналов Azure ExpressRoute на одну подписку — 10. Эти ограничения следует учитывать на этапе проектирования. Если потребуется превысить эти ограничения, добавьте дополнительные подписки. Если вы достигли жестко заданного ограничения, его нельзя увеличить.

**Заявление о конфиденциальности Майкрософт** объясняет, какие личные данные обрабатывает корпорация Майкрософт, как она их обрабатывает и в каких целях.

Заявление о конфиденциальности распространяется на все службы, веб-сайты, приложения, программное обеспечение, серверы и устройства корпорации Майкрософт. Этот список включает все, от корпоративных и серверных продуктов до домашних устройств и программного обеспечения, которыми пользуются учащиеся учебных заведений.

**Условия использования веб-служб (OST)** — это юридическое соглашение между корпорацией Майкрософт и клиентом. В OST подробно излагаются обязательства обеих сторон относительно обработки и защиты данных клиентов и персональных данных. OST применяются, в частности, к веб-службам корпорации Майкрософт, предоставляемым по подписке, включая Azure, Dynamics 365, Office 365 и Bing Maps.

**Дополнение к защите данных (DPA)** более подробно определяет условия обработки и защиты данных для веб-служб. Эти условия включают следующее:

-Соблюдение законов.

-Раскрытие обработанных данных.

-Защиту данных, включая практики и политики обеспечения безопасности, шифрование данных, доступ к данным, обязанности клиентов и соответствие требованиям аудита.

-Перенос, хранение и удаление данных.

**Центр управления безопасностью** отображает принципы Майкрософт по поддержанию целостности данных в облаке и информацию о том, как Майкрософт реализует и поддерживает безопасность, конфиденциальность, соответствие требованиям и прозрачность во всех облачных продуктах и службах Майкрософт. Центр управления безопасностью является важной частью инициативы доверенного облака Майкрософт и предоставляет поддержку по юридическим вопросам и соответствию требованиям.

**Центр управления безопасностью содержит:**

-Подробные сведения о безопасности, конфиденциальности, соответствию требованиям, политикам, возможностям и практикам в облачных продуктах Майкрософт.

-Дополнительные материалы по каждой теме.

-Ссылки на блоги по обеспечению безопасности, конфиденциальности и соответствию требованиям и предстоящие мероприятия.

**Документация по обеспечению соответствия требованиям Azure** содержит подробную документацию по юридическим и нормативным стандартам и обеспечению соответствия требованиям в Azure.

Здесь вы найдете предложения для соответствия требованиям в следующих категориях:

-Глобальный

-Государственные организации США

-Финансовые услуги

-Здравоохранение

-Мультимедиа и производство

-Региональные

**Стандарт безопасности данных индустрии платежных карт (Payment Card Industry Data Security Standard, PCI DSS).** Этот глобальный стандарт, известный как PCI DSS, направлен на предотвращение мошенничества за счет усиления контроля над данными кредитных карт.

В **Документации по обеспечению соответствия требованиям Azure** можно получить доступ к дополнительным материалам о соответствии требованиям.

**Azure для государственных организаций** — это отдельный экземпляр Microsoft Azure. Он решает задачи федеральных ведомств США, органов власти штатов, местной администрации и их поставщиков решений по обеспечению безопасности и соответствия требованиям. Azure для государственных организаций обеспечивает физическую изоляцию от любых развертываний, не относящихся к правительству США, и предоставляет проверенный персонал из американских граждан.

**Azure для Китая (21Vianet)** управляется компанией 21Vianet. Это физически отделенный экземпляр облачных служб, расположенный в Китае. Обслуживание и управление транзакциями Azure для Китая (21Vianet) независимо выполняется компанией Shanghai Blue Cloud Technology Co., Ltd. ("21Vianet"), дочерней компанией Beijing 21Vianet Broadband Data Center Co., Ltd.