АИС

ЛР 1 – Windows Server

Основные плюсы серверов под управлением Windows — относительная простота администрирования, достаточно большой пласт информации, мануалов и ПО. Кроме того, вы не сможете обойтись без сервера на Windows, если в экосистеме компании есть программное обеспечения или решения, использующие библиотеки и части ядра систем Microsoft. Также сюда можно добавить технологию RDP для доступа пользователя к серверным приложениям и общую универсальность системы. Кроме того, Windows Server обладает облегченной версией без GUI с ресурсопотреблением на уровне Linux-дистрибутива.

В минусы Winserver можно записать сразу два параметра: стоимость лицензии и потребление ресурсов. Среди всех серверных ОС Windows Server наиболее прожорлива и требует минимум одно ядро процессора и от полутора до трех гигабайт оперативной памяти просто для работы ядра и стандартных служб. Эта система не подходит для маломощных конфигураций, а также имеет ряд уязвимостей, связанных с RDP и политиками групп и пользователей.

Active Directory – служба каталогов от корпорации Microsoft для операционных систем семейства Windows Server. Служба позволяет администраторам использовать групповые политики для обеспечения единообразия настройки пользовательской рабочей среды, разворачивать ПО на множестве компьютеров через групповые политики или посредством System Center Configuration Manager, устанавливать обновления операционной системы, прикладного и серверного программного обеспечения на всех компьютерах в сети, используя службу обновления Windows Server. AD хранит данные о ресурсах (компьютерах, пользователях, серверах, сетевых и периферийных устройствах и т.д.) и настройки среды в централизованной базе данных.

Основные возможности Windows AD:

– **единая база регистрации пользователей, которая хранится централизованно на одном либо нескольких серверах**; таким образом, при появлении нового сотрудника в офисе вам нужно будет всего лишь завести ему учетную запись на сервере и указать, на какие рабочие станции он сможет получать доступ;

− поскольку **все ресурсы домена индексируются**, это дает возможность простого и **быстрого поиска для пользователей**; например, если нужно найти цветной принтер в отделе;

− совокупность применения разрешений NTFS, групповых политик и делегирования управления позволит вам тонко настроить и распределить права между участниками домена;

− **перемещаемые профили пользователей** дают возможность хранить важную информацию и настройки конфигурации на сервере; фактически, если пользователь, обладающий перемещаемым профилем в домене, сядет работать за другой компьютер и введет свои имя пользователя и пароль, он увидит свой рабочий стол с привычными ему настройками;

− с помощью групповых политик вы можете изменять настройки операционных систем пользователей, от разрешения пользователю устанавливать обои на рабочем столе до настроек безопасности, а также распространять по сети программное обеспечение, например, Volume Shadow Copy client и т. п.;

− многие программы (прокси-серверы, серверы баз данныхи др.) не только производства Microsoft на сегодняшний день научились использовать доменную аутентификацию, таким образом, вам не придется создавать еще одну базу данных пользователей, а можно будет использовать уже существующую;

− использование **Remote Installation Services** облегчает установку систем на рабочие места, но, в свою очередь, работает только при внедренной службе каталогов.

Контроллер домена будет выполнять функции аутентификации пользователей и устройств в сети, а также выступать в качестве хранилища базы данных. При попытке использовать любой из объектов (ПК, сервер, принтер) сети, выполняется обращение к контроллеру домена, который либо разрешает это действие (есть необходимые права), либо блокирует его.

Рабочая группа – это логическая группировка компьютеров, объединенных общим именем для облегчения навигации в пределах сети, при этом принципиально важно, что каждый в рабочей группе равноправен (т. е. сеть получается одноранговой) и поддерживает собственную локальную базу данных

учетных записей пользователей (Security Accounts Manager, SAM). Отсюда вытекает основная проблема, которая не позволяет использовать рабочие группы в крупных корпоративных сетях. Действительно, вход в защищенную систему является обязательным, а непосредственный и сетевой входы принципиально различаются (непосредственный контролируется локальным компьютером, а сетевой — удаленным), то, например, пользователю, вошедшему на компьютер Comp1 под локальной учетной записью User1, будет отказано в доступе к принтеру, установленному на компьютере Comp2, поскольку в его локальной базе нет пользователя с именем User1. Таким образом, для обеспечения «прозрачного» взаимодействия в рабочей группе нужно создавать одинаковые учетные записи с одинаковыми паролями на всех компьютерах, где работают пользователи и расположены ресурсы. В ОС Windows для рабочих групп предусмотрен специальный режим: «Использовать простой общий доступ к файлам», позволяющий обойти указанную проблему (данный режим включен по умолчанию)

Домены–это основная логическая единица построения. В сравнении с рабочими группами домены AD – это группы безопасности, имеющие единую базу регистрации, тогда как рабочие группы – это всего лишь логическое объединение машин. AD использует для именования и службы поиска DNS (Domain Name Server – сервер имен домена), а не WINS (Windows Internet Name Service – сервис имен Internet), как это было в ранних версиях NT. Таким образом, имена компьютеров в домене имеют вид, например, buh.work.com, где buh – имя компьютера в домене work.com

Группы пользователей и компьютеров – используются для административных целей и имеют такой же смысл, как и при использовании на локальных машинах в сети. В отличие от OU, к группам нельзя применять групповые политики, но для них можно делегировать управление. В рамках схемы Active Directory выделяют два вида групп: **группы безопасности** (применяются для разграничения прав доступа к объектам сети) и **группы распространения** (применяются в основном для рассылки почтовых сообщений, например, в сервере Microsoft Exchange Server).

Они подразделяются по области действия:

− универсальные группы могут включать в себя пользователей в рамках леса, а также другие универсальные группы или глобальные группы любого домена в лесу;

− глобальные группы домена могут включать в себя пользователей домена и другие глобальные группы этого же домена; − локальные группы домена используются для разграничения прав доступа, могут включать в себя пользователей домена, а также универсальные группы и глобальные группы любого домена в лесу;

− локальные группы компьютеров – группы, которые содержит SAM (security account manager) локальной машины. Область их распространения ограничивается только данной машиной, но они могут включать в себя локальные группы домена, в котором находится компьютер, а также универсальные и глобальные группы своего домена или другого, которому они доверяют.

Лес Active Directory – определяет набор одного или нескольких доменов, использующих одни и те же схему, конфигурацию и глобальный каталог. Кроме этого, все домены участвуют в двусторонних транзитивных отношениях доверия.

Схема – схема Active Directory используется совместно всеми доменами в пределах леса. Схема — это конфигурационная информация, которая управляет структурой и содержимым каталога.

Конфигурация– конфигурация определяет логическую структуру леса, например, число и конфигурацию сайтов в пределах леса.

Глобальный каталог– глобальный каталог можно воспринимать в виде справочника для леса. Глобальный каталог содержит информацию о всех объектах леса включая информацию о расположении объектов.

Доверие – доверие предоставляет различным доменам возможность работать вместе. Без доверия домены работают как отдельные сущности, то есть пользователи из домена А не смогут получать доступ к ресурсам в домене В. Если отношение доверия устанавливается между доменами таким образом,

что домен В доверяет домену А, то пользователи домена А смогут получать доступ к ресурсам домена В, если у них есть соответствующие разрешения.

Существует три основных типа отношений доверия:

Транзитивные – транзитивные отношения доверия создаются автоматически между доменами одного леса. Они позволяют пользователям любого домена потенциально получать доступ к ресурсам любого другого домена этого леса, если у пользователей есть соответствующие права доступа.

Shortcut – это отношение доверия между доменами одного леса, которые уже имеют транзитивное отношение доверия. Такое отношение доверия предоставляет более быструю аутентификацию и проверку доступа к ресурсам между несоседними доменами леса.

Внешние – внешние отношения доверия позволяют доменам из различных лесов совместно использовать ресурсы. Такие отношения доверия не являются транзитивными, то есть они относятся только к тем доменам, для которых они создавались.

Ресурсная запись (RR – Resource Record) – единица хранения и передачи информации в DNS, включающая в себя следующие элементы (поля):

− Имя (Name) – имя домена, к которому относится запись;

− TTL (Time To Live) – допустимое время хранения записи неответственным сервером;

− Тип (Type) – параметр, определяющий назначение и формат записи в поле данных (Rdata);

− Класс (Class)– тип сети передачи данных (подразумевается возможность DNS работать с типами сетей, отличных от TCP/IP);

− Длина поля данных (Rdlen);

− Поле данных (Rdata) – содержание и формат поля зависят от типа записи.

Ниже представлены типы ресурсных записей (зоны), используемые чаще всего:

− A (IPv4 Address Record – адресная запись) – связывает доменное имя с IPv4-адресом хоста;

− AAAA (IPv6 Address Record) – связывает доменное имя с IPv6-адресом хоста (аналогично A-записи);

− CNAME (Canonical Name Record – каноническая запись имени) – используется для перенаправления на другое доменное имя;

− MX (Mail Exchange – почтовый обменник) – ссылается на почтовый сервер, обслуживающий домен;

− NS (NameServer– сервер имен) – ссылается на DNS-сервер, ответственный за домен;

− TXT – текстовое описание домена. Зачастую требуется для выполнения специфических задач (например, подтверждения права собственности на домен при привязке его к почтовому сервису);

− PTR (Point to Reverse – запись указателя) – связывает IP-адрес машины с доменом, используется преимущественно для проверки сторонними почтовыми сервисами отправляемых через эту машину электронных писем на отношение к домену, указанному в параметрах почтового сервера. При несоответствии этих параметров письмо проверяется более тщательно по другим критериям

Обратный просмотр DNS (англ. reverseDNSlookup)–обращение к особой доменной зоне для определения имени узла по его IP-адресу с помощью PTR-записи.

Для выполнения запроса адрес узла переводится в обратную нотацию:

IPv4-адрес 192.168.0.1 превращается в 1.0.168.192.in-addr.arpa.

Благодаря иерархической модели управления именами появляется возможность делегировать управление зоной владельцу диапазона IP-адресов. Для этого в записях авторитетного DNS-сервера указывают, что за зону CCC.BBB.AAA.in-addr.arpa (то есть за сеть AAA.BBB.CCC.000/24) отвечает отдельный сервер.

Количество PTR-записей, описывающих разные имена, на один адрес не ограничивается спецификациями, но может ограничиваться размером UDPпакета, так как DNS-сервер инкапсулирует свой ответ в UDP. В большинстве случаев для одного IP-адреса создаётся только одна PTR-запись, но бывает и так, что их создаётся множество – например, когда IP-адрес используется для нескольких виртуальных серверов с разными именами.

ЛР 2 – Zabbix

Контрольные вопросы:

1. Что такое zabbix, каково назначение системы?

Zabbix — это система мониторинга и управления сетями и IT-инфраструктурой. Ее назначение состоит в наблюдении за состоянием различных компонентов системы, сборе и анализе данных о производительности, а также предоставлении уведомлений и отчетов об аномалиях или проблемах в системе.

В набор приложений Zabbix входит агент для удаленного мониторинга серверов, также возможен мониторинг через SNMP, ICMP или TCP, а также других протоколов. Можно настроить мониторинг с помощью агента и получать максимум информации, или просто проверять доступность с помощью одного из возможных протоколов.

2. Какие основные варианты мониторинга систем?

для удаленного мониторинга серверов, также возможен мониторинг через SNMP, ICMP или TCP, а также других протоколов. Можно настроить мониторинг с помощью агента и получать максимум информации, или просто проверять доступность с помощью одного из возможных протоколов.

3. Чем отличается snmpv1 от snmpv3?

SNMPv1 (Simple Network Management Protocol version 1) и SNMPv3 отличаются в основном по следующим параметрам:

Безопасность: SNMPv3 предоставляет расширенные механизмы аутентификации и шифрования для обеспечения безопасности передачи данных, в то время как SNMPv1 не предоставляет эти функции.

Аутентификация: SNMPv3 поддерживает различные методы аутентификации, такие как HMAC-MD5 и HMAC-SHA, в то время как SNMPv1 использует простую аутентификацию на основе комьюнити-строк.

Управление доступом: SNMPv3 предлагает возможности управления доступом, позволяющие указывать права доступа для различных пользователей и групп, что обеспечивает более гибкую конфигурацию доступа к данным.

4. Какие основные сложности при настройке мониторинга в zabbix?

- Корректная настройка агентов мониторинга на целевых устройствах.

- Конфигурация правил и триггеров для определения нормального и аномального поведения системы.
- Установка и настройка шаблонов мониторинга для различных типов компонентов системы.
- Оптимизация производительности системы Zabbix для обработки большого объема данных мониторинга.
- Настройка уведомлений и оповещений для оперативного реагирования на проблемы.

5. Что такое тригеры в заббикс?

Триггеры - это условия, определяющие аномальное или нежелательное состояние системы. Они определяются на основе значений мониторируемых параметров и позволяют генерировать оповещения или выполнять автоматические действия при наступлении определенных условий. Триггеры могут быть настроены для различных метрик, таких как процент использования CPU, доступность сетевого устройства и других параметров, позволяя операторам системы быстро реагировать на проблемы.

6. Какие варианты оповещения администратора предусмотрены в заббикс?

- Отправка уведомлений по электронной почте.
- Отправка SMS-сообщений.
- Интеграция с системами мгновенных сообщений (например, Slack, Telegram).
- Генерация автоматических событий и активаций командных файлов или сценариев.

7. Назовите минимум 3 другие системы мониторинга.

Nagios: Популярная система с открытым исходным кодом для мониторинга сети и сервисов.

Prometheus: Система мониторинга с открытым исходным кодом, специализирующаяся на сборе метрик и алертинге.

SolarWinds: Коммерческая система мониторинга, предоставляющая широкий спектр инструментов для мониторинга сети, приложений и серверов.

8. Какие Операционные системы можно мониторить с помощью заббикс?

Windows, MacOS и Linux

9. Что такое MIB?

MIB (Management Information Base) — это структурированное представление данных, используемых для управления сетевыми устройствами, которые поддерживают протокол SNMP (Simple Network Management Protocol). MIB определяет структуру данных, которые могут быть запрошены и изменены через SNMP. Он содержит набор объектов, и каждый объект имеет имя и уникальный идентификатор (OID), который используется для доступа к нему.

10. Что такое авто обнаружение компонент?

Автообнаружение компонентов в Zabbix - это процесс автоматического обнаружения и регистрации новых устройств, хостов, служб и приложений в системе мониторинга. Zabbix может сканировать сеть и применять различные методы обнаружения, такие как сканирование портов, ICMP-пинги, SNMP-запросы и другие, чтобы определить доступные цели мониторинга. Это упрощает процесс добавления и настройки новых компонентов в системе мониторинга без необходимости ручного ввода каждого элемента.

11. В какой единицы измерения отображается загрука CPU операционной системы в zabbix?

Загрузка CPU операционной системы в Zabbix отображается в процентах (%).

12. Что такое комплексный экран в zabbix?

это пользовательский интерфейс, который позволяет объединить несколько графиков, таблиц и элементов управления на одной странице. Он предоставляет возможность создания настраиваемых мониторинговых дашбордов, где можно отображать и анализировать различные параметры и метрики в едином окне.

Zabbix - это универсальный инструмент мониторинга, который используется для отслеживания работы серверов, сетевого оборудования и приложений. Он способен быстро реагировать на внештатные ситуации и предупреждать возможные проблемы с нагрузкой. Система Zabbix состоит из нескольких компонентов, включая основной сервер, базы данных, веб-интерфейс и агенты. Основной сервер получает, обрабатывает и анализирует данные, которые затем

сохраняются в базе данных. Веб-интерфейс обеспечивает доступ к настройкам Zabbix, а агенты отвечают за сбор данных с мониторируемых устройств. Zabbix позволяет собирать статистику и действовать в соответствии с заранее настроенными правилами и условиями

ЛР 3 – SSL

1. Что такое Удостоверяющий центр?

Удостоверяющий центр (УЦ) - это доверенная организация, которая выпускает и управляет цифровыми сертификатами. Он играет важную роль в системе публичного ключа (Public Key Infrastructure, PKI) и используется для проверки подлинности и целостности электронной информации.

2. В чем отличие открытого ключа и сертификата?

Открытый ключ (public key) - это криптографический ключ, который используется для шифрования данных или проверки цифровой подписи. Сертификат содержит открытый ключ, а также информацию о его владельце, выдавшем органе и сроке его действия. Отличие между открытым ключом и сертификатом заключается в том, что сертификат содержит дополнительные данные и информацию, подтверждающую подлинность открытого ключа.

3. Какой функционал несет закрытый ключ?

Закрытый ключ (private key) используется для расшифровки данных, создания цифровой подписи или установления безопасного соединения. Он должен быть хранен в секрете и не должен быть доступен посторонним лицам. Функционал закрытого ключа включает генерацию цифровых подписей, дешифрование зашифрованных данных и установление безопасного соединения с использованием протоколов шифрования.

4. В чем особенности Формата сертификата *.pfx?

Формат сертификата *.pfx (Personal Information Exchange) является одним из форматов для хранения и передачи сертификатов и соответствующих закрытых ключей. Файл формата *.pfx обычно защищен паролем и может содержать цепочку сертификатов, закрытый ключ и дополнительные сведения.

5. Какие УЦ являются доверенными?

Доверенные удостоверяющие центры (Trusted Certificate Authorities) являются организациями, которым доверяют большинство клиентских устройств и программного обеспечения. Они выпускают сертификаты и гарантируют, что открытые ключи, содержащиеся в сертификатах, связаны с определенными

субъектами. Некоторые известные доверенные УЦ включают VeriSign, Comodo, Let's Encrypt, Digicert и другие.

6. Что такое список отозванных сертификатов?

Список отозванных сертификатов (Certificate Revocation List, CRL) - это список сертификатов, которые были отозваны УЦ до истечения их срока действия. CRL содержит информацию о сертификатах, подлежащих отзыву, и используется для проверки подлинности сертификатов перед их использованием.

7. Можно ли с помощью одного закрытого ключа создать несколько сертификатов?

Нет, каждый сертификат обычно связан с конкретным открытым и закрытым ключом. Для каждого сертификата требуется пара ключей - открытый и закрытый.

8. Какова основная уязвимость в шифровании с открытым ключом?

Основная уязвимость в шифровании с открытым ключом связана с возможностью подмены открытого ключа. Если злоумышленник заменяет открытый ключ на свой собственный, то он может перехватывать и расшифровывать зашифрованные сообщения или создавать ложные цифровые подписи от имени других пользователей.

9. Какие основные форматы файлов открытого ключа и сертификата?

Основные форматы файлов открытого ключа включают X.509 (обычно с расширением .cer или .pem), PGP (Pretty Good Privacy, с расширением .asc или .pgp) и SSH(.pub). Форматы файлов сертификатов включают X.509 (обычно с расширением .cer или .pem), PKCS#12 (с расширением .pfx) и другие.

10. Что такое цепочка сертификатов УЦ?

Цепочка сертификатов УЦ (Certificate Chain) представляет собой иерархическую серию сертификатов, начиная от конечного сертификата и до корневого сертификата УЦ. Цепочка сертификатов позволяет проверить подлинность сертификата путем проверки подписей цепочки от конечного сертификата до доверенного корневого сертификата.

11. Каким образом сертификаты попадают в список отозванных?

Сертификаты попадают в список отозванных, когда УЦ обнаруживает, что сертификат больше не является доверенным или его закрытый ключ

скомпрометирован. При обнаружении таких ситуаций УЦ отзывает сертификат и включает его в CRL или в список отозванных сертификатов, чтобы клиенты могли проверить его статус перед использованием.

12. Как производится браузером проверка сертификата?

Проверка сертификата браузером включает несколько шагов. Браузер проверяет цепочку сертификатов от конечного сертификата до доверенного корневого сертификата, проверяя подписи каждого сертификата. Он также проверяет действительность сертификата, срок его действия и его статус в списке отозванных сертификатов. Если сертификат прошел успешную проверку, браузер отображает зеленую пиктограмму или замок, указывая на безопасное соединение с веб-сайтом.