

Оглавление

От издательства.....	22
О научном редакторе русскоязычного издания	22
Предисловие	23
Кому адресована книга.....	23
Структура издания	24
Как извлечь наибольшую пользу из книги	26
Файлы с примерами кода.....	26
Цветные иллюстрации	26
Условные обозначения	27
Об авторе.....	27
О научном редакторе	28
Глава 1. Основы Active Directory	29
Современный подход к управлению доступом.....	29
Что такое идентичность	32
Будущее управления идентификацией и доступом.....	33
Рост киберпреступности.....	34
Безопасность на основе нулевого доверия (Zero Trust)	36
Беспарольная аутентификация.....	38
Цифровое удостоверение личности.....	39
Гибридная идентификация и службы доменов Active Directory	40
Преимущества использования Active Directory	45
Централизованное хранилище данных	48
Репликация данных.....	48
Высокая доступность.....	49
Безопасность.....	49
Возможности аудита	49
Система единого входа	49

Изменение схемы	50
Построение запросов и индексирование.....	50
Основные сведения о компонентах Active Directory	51
Логические компоненты	51
Физические компоненты.....	59
Основные сведения об объектах Active Directory	62
Глобальные уникальные идентификаторы и идентификаторы безопасности	64
Отличительные имена.....	66
Роли серверов Active Directory	66
Резюме.....	68
Глава 2. Службы доменов Active Directory 2022.....	69
Функции AD DS 2022	70
Нежелательность применения функциональных уровней леса и домена Windows Server 2003	71
Нежелательность применения службы репликации файлов	72
Управление привилегированным доступом	73
Эволюция киберпреступности	75
Как связаны PAM и AD DS 2022	85
Логика управления привилегированным доступом (PAM).....	85
Динамическое членство в группах	88
Windows Hello для бизнеса.....	90
Улучшение временной синхронизации	92
PowerShell 7	93
Резюме.....	94
Глава 3. Проектирование инфраструктуры Active Directory	95
Что делает систему хорошей.....	95
Новые требования бизнеса	96
Исправление ошибок унаследованного решения	97
Сбор требований бизнеса	98
Определение границ зон безопасности	99
Определение физической структуры компьютерной сети.....	99
Проектирование структуры леса	101
Модель с одним лесом.....	101
Модель с несколькими лесами	102
Создание структуры леса	103
Автономность	103
Изоляция.....	103

Выбор модели проектирования леса	104
Организационная модель проектирования леса	105
Ресурсная модель проектирования леса	105
Модель леса с ограниченным доступом	108
Проектирование доменной структуры	109
Одиночный домен	110
Региональный домен	110
Домен филиала/сайта	111
Количество доменов	111
Выбор имен доменов	112
Корневой домен леса	113
Определение функциональных уровней домена и леса	114
Проектирование структуры OU	115
Проектирование физической топологии Active Directory	116
Физические и виртуальные контроллеры доменов	117
Размещение контроллера домена	119
Размещение глобального сервера каталогов	119
Проектирование гибридной идентичности	120
Подход к переходу в облачную среду	123
Определение потребностей предприятия	124
Синхронизация	127
Совместная ответственность	130
Стоимость	130
Резюме	131
Глава 4. Система доменных имен Active Directory 2022	132
Что такое DNS	133
Иерархические структуры имен	134
Администраторы доменов верхнего уровня (администраторы TLD)	135
Как работает DNS	138
Проектирование инфраструктуры DNS	141
Объединение AD DS с существующей инфраструктурой DNS	142
Несвязанное пространство имен	142
Развертывание новой интегрированной в AD инфраструктуры DNS	143
Основные компоненты DNS	143
Записи DNS	143
Зоны	146

Серверы условной пересылки	150
Политики DNS.....	151
Защищенный клиент DNS по протоколу HTTPS (DoH).....	154
Рабочие режимы сервера DNS	154
Передачи зон.....	155
Делегирование DNS.....	156
Поставщики служб DNS.....	158
Резюме.....	158
Глава 5. Назначение ролей главных операций.....	160
Роли FSMO	161
Владелец операций схемы.....	161
Владелец операций доменных имен	162
Владелец операций эмулятора PDC	162
Владелец операций RID	164
Владелец операций инфраструктуры домена	164
Назначение ролей FSMO	165
Логическая и физическая топология Active Directory	165
Обеспечение связи.....	168
Количество контроллеров доменов	169
Емкость	169
Рекомендации.....	170
Перемещение ролей FSMO	171
Захват ролей FSMO	173
Резюме.....	175
Глава 6. Миграция в Active Directory 2022	176
Предварительные условия для установки AD DS	176
Требования к оборудованию	176
Требования к виртуализированной среде.....	177
Дополнительные требования	179
Методы установки AD DS	181
Сценарии развертывания AD DS.....	183
Настройка корневого домена нового леса	183
Настройка дополнительного контроллера домена.....	187
Планирование миграции AD	191
Жизненный цикл миграции	193
Аудит.....	194

Логическая и физическая топология AD	194
Проверка работоспособности AD.....	195
Аудит приложений.....	200
Планирование.....	201
Реализация	203
Резюме.....	211
Глава 7. Управление объектами Active Directory.....	212
Инструменты и методы управления объектами	213
Windows Admin Center	213
Центр администрирования Active Directory	217
Консоль ADUC MMC	222
Администрирование объектов AD с помощью PowerShell.....	225
Создание, изменение и удаление объектов в AD.....	225
Создание объектов компьютеров	228
Изменение объектов AD.....	230
Удаление объектов AD	231
Поиск объектов в AD	232
Поиск объектов с помощью PowerShell	235
Предотвращение случайного удаления объектов.....	236
Корзина AD	237
Резюме.....	239
Глава 8. Управление пользователями, группами и устройствами.....	240
Атрибуты объектов.....	241
Пользовательские атрибуты	244
Синхронизация пользовательских атрибутов с Azure AD	249
Учетные записи пользователей	253
Управляемые учетные записи служб (MSA).....	255
Групповые управляемые учетные записи служб (gMSA).....	256
Деинсталляция MSA.....	258
Группы.....	258
Область группы.....	259
Преобразование групп.....	260
Настройка групп.....	261
Устройства и другие объекты.....	264
Рекомендации.....	265
Резюме.....	266

Глава 9. Проектирование организационной структуры	267
Применение OU	268
Организация объектов.....	268
Групповые политики.....	269
Контейнеры по сравнению с OU	271
Группы Active Directory по сравнению с OU	272
Модели проектирования OU	272
Модель контейнеров.....	273
Модель типов объектов.....	274
Функциональная модель.....	276
Географическая модель	278
Модель отделов.....	280
Гибридная модель	282
Управление структурой OU	285
Делегирование управления	286
Резюме.....	289
Глава 10. Управление групповыми политиками	290
Преимущества групповых политик.....	290
Следование стандартам.....	291
Автоматизация административных задач	291
Предотвращение изменений системных настроек пользователями	292
Гибкость определения целей.....	292
Неизменность цели.....	292
Возможности групповых политик	293
Объекты групповых политик.....	294
Контейнер групповой политики	294
Шаблон групповой политики	297
Обработка групповых политик	298
Наследование групповых политик	302
Конфликты групповых политик.....	304
Сопоставление и статус групповых политик	307
Административные шаблоны	309
Фильтрация групповых политик.....	311
Фильтры безопасности.....	311
Фильтры WMI	315
Глобальные параметры групповых политик.....	319

Адресация на уровне элементов.....	322
Закольцованная обработка	324
Рекомендации по применению групповых политик	326
Полезные групповые политики	328
Резюме.....	334
Глава 11. Службы Active Directory, часть 1	335
Обзор AD LDS	336
Области применения LDS	337
Разработка приложений	337
Размещаемые приложения	337
Хранилища распределенных данных для интегрированных с AD приложений.....	338
Миграция из других служб каталогов	338
Установка службы LDS.....	338
Репликация AD.....	344
FRS по сравнению с DFSR	344
Сайты AD и репликация.....	346
Сайты.....	348
Подсети	349
Каналы сайтов	349
Межсайтовые мосты	349
Управление сайтами AD и другими компонентами.....	350
Управление сайтами	351
Управление каналами сайта	352
Серверы-плацдармы.....	356
Управление подсетями	357
Как работает репликация	357
Проверка согласованности данных (KCC)	359
Как происходит обновление.....	360
Резюме.....	362
Глава 12. Службы Active Directory, часть 2	363
Понятие доверия в Active Directory	363
Направление доверия	364
Транзитивное доверие по сравнению с нетранзитивным.....	365
Типы доверия Active Directory	365
Создание доверия Active Directory	366

Контроллеры доменов только для чтения (RODC)	376
Ведение базы данных Active Directory	379
Файл ntds.dit	380
Файл edb.log	381
Файл edb.chk	381
Файл temp.edb	381
Автономная дефрагментация	382
Резервное копирование и восстановление Active Directory	383
Предотвращение случайного удаления объектов	384
Корзина Active Directory	385
Моментальные снимки Active Directory	386
Резервное копирование системного состояния Active Directory	388
Резюме	390
Глава 13. Службы сертификатов	391
Как работает PKI	392
Сравнение симметричных и асимметричных ключей	392
Цифровое шифрование	392
Цифровые подписи	393
Подписание, шифрование и расшифровка	394
Сертификаты SSL	398
Типы центров сертификации	400
Взаимодействие сертификатов с цифровыми подписями и шифрованием	400
Примеры использования сертификатов	401
Компоненты AD CS	403
Центр сертификации	403
Веб-служба регистрации сертификатов	404
Политика веб-службы регистрации сертификатов	404
Служба регистрации в центре сертификации через интернет	404
Служба регистрации сетевых устройств	404
Сетевой ответчик	405
Типы ЦС	405
Планирование PKI	406
Внутренние и публичные ЦС	406
Определение правильных типов объектов	407
Длина криптографического ключа	408
Алгоритмы хеширования	408

Период действия сертификата	408
Иерархия ЦС	408
Высокая доступность	408
Выбор шаблонов сертификатов	409
Границы ЦС	409
Модели развертывания PKI	409
Одноуровневая модель	409
Двухуровневая модель	410
Трехуровневая модель	412
Настройка PKI	414
Настройка изолированного корневого ЦС	414
DSConfigDN	415
Местоположение CDP	415
Местоположение AIA	418
Временные рамки ЦС	419
Временные рамки CRL	419
Новый CRL	420
Публикация данных корневого ЦС в Active Directory	420
Настройка выдающего ЦС	421
Издание сертификата для выдающего ЦС	422
Задачи завершения конфигурации	423
Местоположение CDP	423
Местоположение AIA	423
Временные рамки ЦС и CRL	423
Шаблоны сертификатов	424
Запрос сертификатов	427
Миграция AD CS с Windows Server 2008 R2 на Windows Server 2022	429
Демонстрационная среда	429
Резервное копирование конфигурации существующего ЦС (Windows Server 2008 R2)	431
Установка роли AD CS на новый сервер под управлением Windows 2022	432
Восстановление конфигурации предыдущего ЦС	433
Тестирование	434
Аварийное восстановление AD CS	436
Методы аварийного восстановления	437
Резюме	440

Глава 14. Службы федерации	441
Как работает AD FS.....	442
Что такое утверждение.....	446
Язык разметки деклараций безопасности (SAML).....	447
Доверие WS.....	447
Федерация WS.....	447
Компоненты AD FS.....	448
Служба федерации.....	448
Что нового в AD FS 2022	450
Прокси-служба веб-приложения.....	451
База данных конфигурации AD FS	451
Типы топологии при развертывании AD FS	452
Один сервер федерации.....	453
Один сервер федерации и один прокси-сервер веб-приложения	454
Несколько серверов федерации и несколько прокси-серверов веб-приложения с сервером SQL.....	456
Развертывание AD FS	458
Записи DNS.....	458
Сертификаты SSL.....	459
Установка роли AD FS.....	459
Установка WAP	461
Конфигурация приложения, поддерживающего утверждения, с новыми серверами федерации.....	462
Создание отношения доверия с проверяющей стороной.....	463
Конфигурация прокси-сервера веб-приложения	466
Интеграция с Azure MFA.....	467
Предварительные требования	468
Создание сертификата в ферме AD FS для подключения к Azure MFA	468
Разрешение серверам AD FS подключаться к клиенту Azure MFA	469
Разрешение ферме AD FS использовать Azure MFA.....	469
Разрешение Azure MFA выполнять аутентификацию	470
Федерация Azure AD с AD FS	472
Регистрация федерации в Azure AD.....	472
Создание доверия федерации между Azure AD и AD FS.....	473
Конфигурация Azure AD Connect.....	475
Тестирование.....	478
Резюме.....	480

Глава 15. Службы управления правами	481
Что такое AD RMS	482
Компоненты AD RMS	486
Службы доменов Active Directory	487
Кластер AD RMS.....	487
Веб-сервер.....	488
SQL Server	488
Клиент AD RMS	489
Службы сертификатов Active Directory	489
Как работает AD RMS.....	489
Как разворачивать AD RMS.....	493
Один лес и один кластер.....	493
Один лес и несколько кластеров.....	493
AD RMS в нескольких лесах.....	494
Взаимодействие AD RMS и AD FS.....	496
Конфигурация AD RMS.....	497
Настройка корневого кластера AD RMS.....	497
Служба Azure Information Protection	508
Классификация данных.....	508
Службы управления правами Azure (Azure RMS).....	512
Резюме.....	517
Глава 16. Рекомендации по обеспечению безопасности	
Active Directory.....	518
Аутентификация.....	519
Протокол Kerberos.....	519
Аутентификация в среде AD.....	523
Делегирование полномочий.....	524
Стандартные роли администраторов AD	526
Использование ACL объектов	526
Применение метода делегирования управления в AD	529
Реализация детальных политик паролей	532
Ограничения	533
Результирующий набор политик.....	534
Конфигурация	534
Атаки Pass-the-hash	536
Группа безопасности Protected Users.....	538

Ограниченный режим администратора для RDP.....	541
Политики аутентификации и их контейнеры.....	545
Политики аутентификации	545
Контейнеры политик аутентификации.....	545
Создание политик аутентификации.....	546
Создание контейнеров политик аутентификации.....	547
Безопасный протокол LDAP.....	550
Характеристики безопасного LDAP.....	551
Активация безопасного LDAP	551
Управление паролями локальных администраторов Microsoft (LAPS).....	553
Рассмотрение предварительных условий.....	555
Установка Microsoft LAPS	555
Обновление схемы AD	557
Изменение разрешений объекта компьютера	558
Назначение разрешений на доступ к паролям группам	559
Установка CSE на компьютеры	560
Создание GPO для настроек LAPS.....	561
Тестирование.....	563
Локальная служба Azure AD Password Protection.....	564
Прокси-сервер Azure AD Password Protection	564
DC-агент Azure AD Password Protection.....	565
Как Azure AD Password Protection взаимодействует с AD?	566
Конфигурация	566
Тестирование.....	568
Резюме.....	569

Глава 17. Расширенное управление Active Directory

с помощью PowerShell	570
Управление Active Directory с помощью PowerShell: подготовка	571
PowerShell 7.....	573
Команды и сценарии управления AD	574
Репликация	575
Репликация специфического объекта.....	580
Пользователи и группы.....	581
Время последнего входа в систему.....	581
Отчет о дате последнего входа в систему.....	581
Отчет о сбоях при входе в систему.....	582
Обнаружение заблокированной учетной записи.....	584

Отчет об истечении срока действия паролей	584
Просмотр членства в административных группах высокого уровня.....	586
Неактивные учетные записи	589
Пользователи с бессрочными паролями	591
PowerShell в Azure Active Directory	592
Установка	593
Общие команды	594
Управление пользователями.....	595
Управление группами	601
Microsoft Graph.....	604
Microsoft Graph Explorer.....	605
Резюме.....	611

Глава 18. Гибридная идентификация612

Распространение локальной AD на Azure AD	613
Оценка существующих требований бизнеса.....	614
Оценка плана инфраструктуры организации	617
Оценка требований безопасности.....	618
Выбор версии Azure AD.....	620
Выбор метода регистрации.....	621
Синхронизация хеша паролей.....	621
Федерация с Azure AD	624
Сквозная аутентификация.....	624
Система единого входа Azure AD Seamless SSO	626
Синхронизация между локальной AD и доменом под управлением Azure AD.....	629
Azure AD Connect.....	630
Топология развертывания Azure AD Connect.....	631
Вспомогательный сервер.....	632
Облачная синхронизация Azure AD Connect.....	634
Предварительные условия облачной синхронизации Azure AD Connect	635
Конфигурация облачной синхронизации Azure AD Connect	637
Пошаговое руководство по интеграции локальной среды AD с Azure AD.....	643
Создание виртуальной сети.....	644
Настройка домена под управлением Azure AD	646
Добавление сведений о сервере DNS в виртуальную сеть	650
Создание учетной записи глобального администратора для Azure AD Connect.....	652

Настройка Azure AD Connect	653
Установка агента сквозной аутентификации	653
Конфигурация Azure AD Connect	655
Синхронизация хешей учетных данных NTLM и Kerberos с Azure AD	659
Активация безопасного протокола LDAP для домена под управлением Azure AD DS.....	660
Активация безопасного протокола LDAP	665
Разрешение трафика по безопасному протоколу LDAP	666
Тестирование.....	669
Отказоустойчивость Azure AD DS с наборами реплик	673
Настройка новой группы ресурсов для дополнительного набора реплик	676
Настройка новой виртуальной сети для дополнительного набора реплик	676
Настройка глобальной одноранговой сети VNet между двумя виртуальными сетями.....	677
Создание набора реплик домена под управлением Azure AD DS.....	678
Резюме.....	681
Глава 19. Аудит и мониторинг	683
Аудит и мониторинг AD с помощью встроенных инструментов и техник Windows	684
Средство просмотра событий Windows.....	685
Пользовательские представления	685
Журналы Windows.....	686
Журналы приложений и служб.....	687
Подписки.....	687
Журналы событий AD DS.....	688
Файлы журналов AD DS.....	688
Аудит AD.....	689
Аудит доступа к службе каталогов.....	691
Аудит изменений службы каталогов	692
Аудит репликации службы каталогов.....	692
Детальный аудит репликации службы каталогов	693
Демонстрация.....	693
Просмотр событий	694
Настройка подписок на события	698
Журналы событий безопасности из контроллеров доменов.....	702
Включение политик расширенного аудита безопасности	703

Внедрение расширенного аудита.....	705
Просмотр событий с помощью PowerShell.....	705
Microsoft Defender for Identity.....	707
Что такое Microsoft Defender for Identity	708
Преимущества Defender for Identity.....	709
Архитектура Microsoft Defender for Identity	713
Предварительные условия для Microsoft Defender for Identity.....	714
Развертывание.....	718
Azure AD Connect Health	718
Предварительные условия.....	719
Конфигурация	719
Резюме.....	725
Глава 20. Устранение неполадок.....	726
Устранение проблем репликации AD DS	727
Выявление проблем репликации.....	727
Средство просмотра событий	728
System Center Operations Manager	732
Инструменты для устранения проблем репликации.....	732
Устаревшие объекты.....	736
Строгая согласованность репликации	738
Удаление устаревших объектов.....	738
Проблемы с репликацией DFS.....	738
Проверка соединения	741
Статус общей папки SYSVOL.....	741
Статус репликации DFS	742
Фатальный сбой DFSR из-за некорректного выключения контроллера домена (идентификатор события 2213).....	743
Новизна содержимого	743
Не заслуживающая доверия репликация DFS	744
Заслуживающая доверия репликация DFS.....	746
Устранение проблем с групповыми политиками	748
Принудительная обработка групповых политик.....	749
Результирующий набор политики (RSoP)	750
GPRESULT	750
Мастер результатов групповой политики	752
Мастер моделирования групповой политики.....	754

Общие проблемы Azure AD Connect.....	759
Проблемы сетевых соединений.....	760
Ошибки синхронизации	762
Дублированные атрибуты	762
Несоответствие данных	762
Сбой проверки данных.....	764
Длинные атрибуты.....	764
Конфликт существующих ролей администраторов.....	764
Устранение неполадок с Azure AD Connect.....	765
Устранение неполадок, связанных с базой данных AD DS.....	767
Проверка целостности для обнаружения нарушений базы данных на низком уровне.....	769
Резюме.....	771
Приложение. Дополнительные источники	772