Сервис непрерывного обследования Softline High Safety

Softline
Дербеневская наб., д.7, стр. 8,
г. Москва, Россия, 115114

+7(495) 232-00-23
premier@softline.ru
www.softline.ru

Версия документа
1.0

Код услуги
SL10-00005

Решение

На основе собственной экспертизы и многолетнего опыта мы трансформировали флагманский продукт обследования инфраструктуры Премьер Сервисов в полностью автоматизированное SaaS-решение «Непрерывное обследование», которое способно накапливать, обрабатывать и перекрестно анализировать большие объёмы технических данных различных типов без участия инженера Софтлайн. Решение помогает выявить в среде заказчика технические и операционные риски, а также проблемы разных видов, которые трудно или невозможно обнаружить вручную или с помощью решений для мониторинга.

В основе решения «Непрерывное обследование» лежит платформа Softline Assessment, которая обеспечивает сбор, обработку и корреляцию информации о параметрах конфигурации, данных производительности и сообщениях из журналов событий, предоставляя всестороннюю оценку состояния ИТ-инфраструктуры, включая проверку соответствия лучшим практикам производителя, а также детальные рекомендации по устранению найденных проблем.

Для сбора данных используется доступный в исходном коде компонент Softline Assessment, разворачиваемый на выделенном компьютере в среде заказчика, работающий по заданному расписанию. Второй компонент Softline Assessment отвечает за обработку и перекрестный анализ тысяч параметров и сотен миллионов строк динамических характеристик обследуемой системы.

Softline Assessment зарегистрирована в реестре российского ПО, данные заказчиков хранятся на территории РФ в изолированных друг от друга виртуальных средах, аутентификация обеспечивается через отечественных провайдеров.

Преимущества

- Сокращение срока старта оценки состояния системы и получения результатов - **первый** срез данных уже **через 8 часов**, далее по расписанию
- Возможность настроить необходимую частоту сбора и анализа данных
- Отслеживание хронологии появления и закрытия проблем
- Разностный анализ между несколькими срезами сбора данных
- Непрерывный контроль над состоянием системы: производительность, безопасность, технические проблемы в динамике
- Рекомендации по оптимизации конфигурации системы для повышения ее производительности без дополнительной закупки или обновления оборудования
- Обнаружение известных уязвимостей для защиты от получения несанкционированного доступа к системе
- Как результат, снижение рисков простоя системы и затрат на ее обслуживание

Результаты

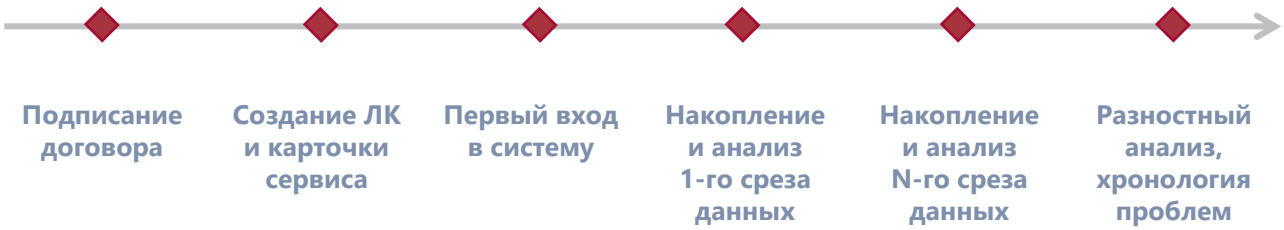
- Просмотр всех собранных данных и результатов анализа онлайн в интерфейсе Личного Кабинета Заказчика (ЛК) с возможностью полнотекстового поиска.
- Автоматически генерируемый пакет итоговых документов по результатам каждого среза сбора и анализа данных с возможностью оффлайн просмотра:
  - паспорт системы;
  - план устранения проблем и рисков;
  - результаты анализа данных с детализацией каждой проблемы и риска, обнаруженных во время обследования, в том числе описание, ссылки на документы поставщиков и третьих лиц, а также рекомендации по устранению с указанием конкретных элементов инфраструктуры.

Срок хранения в ЛК **сырых данных** составляет 90 календарных дней с момента загрузки, **обработанных данных** —180 календарных дней с момента окончания подписки.

Под сырыми данными понимаются данные, загруженные в результате работы утилиты сбора и содержимое закладки «Обмен файлами», максимальный объем хранения – 500 Gb.

Под обработанными данными понимаются результаты анализа сырых данных и содержимое закладки «Итоговые документы».

Жизненный цикл



Доступные опции:

- Экспертное сопровождение - дополнительный анализ, передача знаний, обсуждение плана устранения проблем (2 дня удаленно, инженер Софтлайн).
- Устранение обнаруженных проблем - внесение изменений в соответствии с согласованным планом работ (5 дней очно или удаленно, инженер Софтлайн).

Сбор и загрузка данных

Настройка сбора и загрузки данных по заданному расписанию для дальнейшего автоматизированного анализа осуществляется инженерами Заказчика в соответствии с инструкцией, доступной в ЛК.

Машина сбора

- ОС Windows Server 2012 / Windows 8 или выше;
- подключение к домену AD;
- PowerShell 5.0 или выше;
- права администратора в соответствующих технологиях

Исходящие подключения по разрешённым портам

Брандмауэр

- WinRM — 5985/TCP для каждой обследуемой системы Windows;
- Active Directory — 389/TCP, 636/TCP, 53/UDP, 53/TCP, 445/TCP к контроллерам домена;
- Дополнительные порты для подключения к обследуемым технологиям

HTTPS (порт 443) защищённый канал

Облачный портал sla.premier.softline.ru

Обработка и анализ данных

Доступ к ресурсам предприятия

Обследуемые системы

- Windows Server
- Active Directory
- SQL Server
- IIS
- SharePoint Server

Поддерживаемые технологии

Непрерывное обследование инфраструктуры **Windows Active Directory:**

- предоставит информацию об используемой среде Active Directory, включая аудит конфигурации и параметров, в том числе устаревших;
- выявит текущие проблемы, влияющие на работоспособность и производительность Active Directory;
- поможет найти проблемы, способные повлиять на работоспособность Active Directory в будущем;
- выявит угрозы безопасности, которые могут привести к компрометации всей инфраструктуры;
- включает проведение опроса по операционной эффективности для выявления особенностей внутренних процессов организации и определения их влияния на топологию Active Directory;
- включает анализ используемых протоколов аутентификации и определение случаев, когда используются недостаточно надежные протоколы;
- позволяет отслеживать хронологию появления и закрытия проблем, сравнивать результаты анализа нескольких срезов данных.

Непрерывное обследование инфраструктуры **SharePoint Server**:

- предоставит анализ топологии фермы серверов SharePoint;
- проверит рекомендации по усилению безопасности для серверов SharePoint в зависимости от роли, которую играет каждый сервер;
- позволит убедиться, что операции резервного копирования и восстановления в SharePoint Server выполняются успешно, и что среда защищена от потери данных или нарушения непрерывности обслуживания;
- проверит, что текущая стратегия обновления оптимальна для среды SharePoint Server;
- позволит убедиться, что настройки безопасности для учетных записей и служб SharePoint соответствуют принципу минимальных привилегий.
- позволяет отслеживать хронологию появления и закрытия проблем, сравнивать результаты анализа нескольких срезов данных.

Непрерывное обследование инфраструктуры **Exchange Server:**

- предоставит информацию об используемой среде Exchange Server, включая аудит конфигурации и параметров, в том числе устаревших;
- выявит текущие проблемы, влияющие на работоспособность и производительность Exchange Server;
- поможет найти проблемы, способные повлиять на работоспособность Exchange Server в будущем;
- выявит угрозы безопасности, которые могут привести к компрометации всей инфраструктуры;
- включает анализ используемых протоколов аутентификации и определение случаев, когда используются недостаточно надежные протоколы;
- позволяет отслеживать хронологию появления и закрытия проблем, сравнивать результаты анализа нескольких срезов данных.

Непрерывное обследование инфраструктуры **SQL Server**:

- предоставит информацию об используемой среде SQL Server, в том числе результаты аудита конфигурации и параметров, включая производительность серверов СУБД, хранилищ данных и сети;
- выявит текущие проблемы, влияющие на работоспособность и производительность SQL Server;
- поможет найти проблемы, способные повлиять на работоспособность SQL Server в будущем;
- предоставит данные о системах и процедурах мониторинга (информационных панелях, метриках, пороговых значениях, скорости ответа);
- предоставит данные о процессах резервного копирования и аварийного восстановления (задания, расписания, соответствие SLA).
- позволяет отслеживать хронологию появления и закрытия проблем, сравнивать результаты анализа нескольких срезов данных.

Непрерывное обследование инфраструктуры **Skype for Business Server:**

- предоставит анализ топологии серверов Skype for Business;
- проверит рекомендации по усилению безопасности для серверов Skype for Business в зависимости от роли, которую играет каждый сервер;
- позволит убедиться, что операции резервного копирования и восстановления в Skype for Business Server выполняются успешно и что среда защищена от потери данных или нарушения непрерывности обслуживания;
- проверит, что текущая стратегия обновления оптимальна для среды Skype for Business Server;
- позволит убедиться, что настройки безопасности для учетных записей и служб Skype for Business соответствуют принципу минимальных привилегий;
- позволяет отслеживать хронологию появления и закрытия проблем, сравнивать результаты анализа нескольких срезов данных.

Непрерывное обследование инфраструктуры **MECM/SCCM:**

- предоставит информацию об используемой инфраструктуре MECM/SCCM, включая аудит конфигураций и параметров;
- выявит текущие проблемы, влияющие на работоспособность и производительность серверной части MECM/SCCM;
- поможет определить проблемы со здоровьем клиентов MECM/SCCM;
- поможет найти проблемы, способные повлиять на работоспособность MECM/SCCM в будущем;
- выявит угрозы безопасности, которые могут привести к компрометации всей инфраструктуры;
- позволяет отслеживать хронологию появления и закрытия проблем, сравнивать результаты анализа нескольких срезов данных.

Приложение A. Сбор данных

Требования к рабочей станции для сбора данных

Для проведения обследования должна быть выделена как минимум одна рабочая станция, на которой будет работать программное обеспечение Softline Assessment.

Требования к оборудованию

- Процессор x64, частота 2,0 ГГц, 4 ядра или более;
- 16 ГБ ОЗУ;
- 100 ГБ свободного места на диске для сбора данных (рекомендуется SSD).

Требования к программному обеспечению

- ОС Windows Server 2012 / Windows 8 или выше;
- подключение к домену AD;
- PowerShell 5.0 или выше;
- на доменных компьютерах, не являющихся контроллерами Active Directory, должны быть установлены модули PowerShell для Active Directory, Group Policy и DNS;
- добавить исключения антивируса для %ProgramData%\Softline\SLA и папки, в которую был распакован компонент сбора данных Softline Assessment.

Проверка обновлений в автономном режиме

Для проверки установленных обновлений необходима последняя версия файла Wsusscn2.cab, которую можно скачать: http://go.microsoft.com/fwlink/?linkid=74689. Файл должен храниться в %ProgramData%\Softline\SLA\CommonFiles (если папка не существует, ее следует создать).

Требования к инфраструктуре

На брандмауэрах между рабочей станцией для сбора данных и обследуемыми системами должны быть открыты следующие номера портов.

Active Directory

- WinRM — 5985/TCP для каждой обследуемой системы Windows;
- Active Directory — 389/TCP, 636/TCP, 53/UDP, 53/TCP, 445/TCP, 9389/TCP для каждого контроллера домена.

Необходима учетная запись со следующими правами доступа:

- права локального администратора на каждой обследуемой системе (включая хосты гипервизора, если обследуемая система расположена на Microsoft Hyper-V);
- права Enterprise Admins и Domain Admins к каждому дочернему домену.

SharePoint Server

- WinRM — 5985/TCP для каждой обследуемой системы Windows;
- Active Directory — 389/TCP, 636/TCP, 53/UDP, 53/TCP, 445/TCP к контроллерам домена;

- SQL Server — 1433/TCP, 1434/UDP и пользовательские порты, если они настроены в среде заказчика.

Необходима учетная запись со следующими правами доступа:

- права локального администратора на каждом сервере фермы SharePoint (включая хосты гипервизора, если обследуемая система расположена на Microsoft Hyper-V);
- права Domain Users для доступа к лесу Active Directory;
- роль sysadmin на экземплярах SQL, где размещены базы данных SharePoint;
- участие в группе администраторов фермы SharePoint.

Exchange Server

- WinRM — 5985/TCP для каждой обследуемой системы Windows;
- Active Directory — 389/TCP, 636/TCP, 53/UDP, 53/TCP, 445/TCP к контроллерам домена.

Необходима учетная запись со следующими правами доступа:

- права локального администратора на каждом сервере Exchange (включая хосты гипервизора, если обследуемая система расположена на Microsoft Hyper-V);
- права Domain Users для доступа к лесу Active Directory;
- права Organization Management для леса Active Directory.

SQL Server

- WinRM — 5985/TCP для каждой обследуемой системы Windows;
- Active Directory — 389/TCP, 636/TCP, 53/UDP, 53/TCP, 445/TCP к контроллерам домена;
- SQL Server — 1433/TCP, 1434/UDP и пользовательские порты, если они настроены в среде заказчика.

Необходима учетная запись со следующими правами доступа:

- права локального администратора на каждом сервере SQL (включая хосты гипервизора, если обследуемая система расположена на Microsoft Hyper-V);
- права Domain Users для доступа к лесу Active Directory;
- роль sysadmin для каждого обследуемого экземпляра SQL Server.

Skype for Business

- WinRM — 5985/TCP для каждой обследуемой системы Windows;
- Active Directory — 389/TCP, 636/TCP, 53/UDP, 53/TCP, 445/TCP к контроллерам домена;
- SQL Server — 1433/TCP, 1434/UDP и пользовательские порты, если они настроены в среде заказчика.

Необходима учетная запись со следующими правами доступа:

- права локального администратора на каждом сервере топологии Skype for Business (включая хосты гипервизора, если обследуемая система расположена на Microsoft Hyper-V);
- права Domain Users для доступа к лесу Active Directory;
- роль sysadmin на экземплярах SQL, где размещены базы данных Skype for Business;
- участие в группе администраторов Skype for Business.

MECM/SCCM

- WinRM — 5985/TCP для каждой обследуемой системы Windows;
- Active Directory — 389/TCP, 636/TCP, 53/UDP, 53/TCP, 445/TCP к контроллерам домена;
- SQL Server — 1433/TCP, 1434/UDP и пользовательские порты, если они настроены в среде заказчика;
- HTTP/HTTPS — 80/TCP, 443/TCP;
- RPC, RPCDYNAMIC — 135/TCP, 135/UDP, 49152-65535/TCP, 49152-65535/UDP.

Необходима учетная запись со следующими правами доступа:

- права локального администратора на каждом сервере MECM/SCCM (включая хосты гипервизора, если обследуемая система расположена на Microsoft Hyper-V);
- встроенная роль Full Administrator для MECM/SCCM с настройкой безопасности «All instances of the objects that are related to the assigned security role»;
- роль sysadmin на экземплярах SQL, где размещены базы данных MECM/SCCM, WSUS, SSRS/ Power BI, относящиеся к инфраструктуре MECM/SCCM;
- права Domain Users для доступа к лесу Active Directory.

Требования для целевых систем

- ОС Windows Server 2008 R2 / Windows 8 или выше;
- PowerShell 2.0 или выше;
- возможность удаленного выполнения команд PowerShell;
- брандмауэр на локальной системе должен разрешать входящие соединения по порту 5985/TCP с рабочей станции для сбора данных;
- не менее 50 ГБ свободного места на диске;
- для правильного сбора информации об установленных обновлениях должен быть запущен Центр обновления Windows;
- на всех обследуемых серверах в Event Viewer проверить размер журналов событий для категорий smbserver\audit и ntlm\operational (значение = 1073728 Kb)

  application and services\microsoft\windows\ntlm\operational

  application and services\microsoft\windows\smbserver\audit

- включенные счетчики процессов с идентификаторами процессов (тип REG_DWORD)

  HKLM\System\CurrentControlSet\Services\Perfproc\Performance\ProcessNameFormat = 2

  HKLM\System\CurrentControlSet\Services\Perfproc\Performance\ThreadNameFormat = 2

  После установки значений необходимо перезапустить службу Performance and Alerts Logs (Журналы и оповещения производительности).

Собираемые данные

Программное обеспечение Softline Assessment собирает информацию из разных источников, чтобы получить полноценную картину поведения системы, включая неожиданные, на первый взгляд, зависимости, которые тем не менее могут быть причиной различных проблем и рисков.

При сборе данных не вносится никаких изменений в конфигурацию системы, а сопутствующие «накладные расходы» не оказывают влияние на производительность.

Собираемые данные хранятся в открытых форматах, что позволяет заказчику просматривать их в любое время:

- журналы событий: EVTX;
- счетчики производительности: BLG;
- другие данные конфигурации: JSON.

Собирается следующая информация (список периодически дополняется по мере появления новых функций программного обеспечения Softline Assessment):

Конфигурация компьютера: версия операционной системы, информация о гипервизоре, версия/дата выпуска BIOS, таблица соответствия системных ресурсов ACPI (архитектура NUMA), план электропитания, файл подкачки, устройства и драйверы, драйверы мини-фильтров.

Операционная система: набор применяемых политик, использование выгружаемого/невыгружаемого пула памяти, список установленных и необходимых обновлений, установленное программное обеспечение, конфигурации IIS (при наличии), настройки сетевых адаптеров и привязки протоколов, журналы событий системы, приложений и безопасности, параметры реестра, счетчики производительности, ресурсы отказоустойчивого кластера, списки контроля доступа для привилегированных файлов, настройки синхронизации времени, файловые системы, точки монтирования, информация о блочных устройствах, запланированные задачи, службы и списки контроля доступа для исполняемых файлов службы.

Безопасность: локальные пользователи и группы, права доступа, общие ресурсы и разрешения, настройки и правила брандмауэра, настройки аудита, общедоступная информация о сертификатах, выданных для компьютера, частота установки обновлений, результаты углубленного анализа списков контроля доступа для папок операционной системы и папок, используемых для служб и запланированных задач.

Active Directory: основные параметры домена и леса, важные сведения о группах безопасности, включая членство, сведения об объектах, важных для работы Active Directory и обеспечения безопасности Active Directory, информация о групповой политике из Active Directory и SYSVOL, сведения о сайтах и доверительных отношениях, сведения о пользователях и компьютерах из Active Directory.

Виртуализация: если обследуемая система расположена на Microsoft Hyper-V, то информация о системе виртуализации автоматически добавляется в собираемые данные. С системы виртуализации будут собраны технические данные о конфигурации компьютера, операционной системе и безопасности.

Данные, собираемые с Active Directory

- Настройки центра сертификации (алгоритм шифрования, время, права доступа, точки публикации списков отзывов, опубликованные шаблоны сертификатов и т. п.);
- Тип и параметры активного сертификата центра сертификации;
- Параметры центра сертификации, указанные через capolicy.inf;
- Шаблоны сертификатов из контейнера AD (CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration);
- Информация по пользовательским учетным записям и категоризация пользователей по уровню влияния на системы и безопасность на основе:
    - Привилегий пользователей в обследуемых системах;
    - Вхождения в локальные привилегированные группы;
    - Членства во встроенных в AD группах безопасности;
    - Делегации полномочий на критические LDAP-объекты;
    - Наличия прав на редактирование высокоуровневых групповых политик.
- Данные счетчиков производительности с контроллеров домена:
    - Данные счетчиков операционной системы:
        - \Processor Information(*)*
        - \Memory*
        - \Process(*)*
        - \.NET CLR Memory(*)*
        - \PhysicalDisk(*)*
        - \LogicalDisk(*)*
        - \System*
        - \Paging File(*)*
    - Данные счетчиков сетевой подсистемы:
        - \Network Interface(*)*
        - \TCPv4\Connection Failures
        - \TCPv6\Connection Failures
        - \TCPv4\Connections Reset
        - \TCPv6\Connections Reset
    - Данные счетчиков работы службы DFS-R:
        - \DFS Replicated Folders(*)\Total Files Received
        - \DFS Replicated Folders(*)\Size of Files Received
        - \DFS Replicated Folders(*)\Conflict Space In Use
        - \DFS Replicated Folders(*)\RDC Bytes Received

- Данные счетчиков службы DNS:
  - \DNS\Total Query Received/sec
  - \DNS\Total Response Sent/sec
  - \DNS\UDP Query Received/sec
  - \DNS\UDP Response Sent/sec
- Данные счетчиков работы базы данных AD и протоколов аутентификации:
  - \NTDS\Base searches/sec
  - \NTDS\Database adds/sec
  - \NTDS\Database deletes/sec
  - \NTDS\Database modifys/sec
  - \NTDS\Database recycles/sec
  - \NTDS\Digest Binds/sec
  - \NTDS\NTLM Binds/sec
  - \NTDS\Negotiated Binds/sec
  - \NTDS\LDAP Writes/sec
  - \NTDS\LDAP Active Threads
  - \NTDS\LDAP Bind Time
  - \NTDS\LDAP Client Sessions
  - \NTDS\LDAP Closed Connections/sec
  - \NTDS\LDAP New Connections/sec
  - \NTDS\LDAP New SSL Connections/sec
  - \NTDS\LDAP Page Search Cache entries count
  - \NTDS\LDAP Page Search Cache size
  - \NTDS\LDAP Searches/sec
  - \NTDS\LDAP Successful Binds/sec
  - \NTDS\LDAP UDP operations/sec
  - \NTDS\DS Directory Reads/sec
  - \NTDS\DS Directory Searches/sec
  - \NTDS\DS Directory Writes/sec
  - \NTDS\DS Name Cache hit rate
  - \NTDS\DS Client Binds/sec
  - \NTDS\DS Client Name Translations/sec
  - \NTDS\DRA Inbound Bytes Total/sec
  - \NTDS\DRA Outbound Bytes Total/sec
  - \NTDS\DRA Outbound Objects/sec

- \NTDS\DRA Outbound Properties/sec
- \NTDS\DRA Outbound Values Total/sec
- \NTDS\DRA Inbound Link Values/sec
- \NTDS\DRA Inbound Objects Applied/sec
- \NTDS\DRA Inbound Objects Filtered/sec
- \NTDS\DRA Inbound Objects/sec
- \NTDS\DRA Inbound Properties Total/sec
- \NTDS\DRA Inbound Sync Link Deletion/sec

- Значения следующих веток реестра ОС Windows:
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NtFrs\Parameters
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBIOS\Parameters
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc\Parameters
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Performance
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DfsrRo\Instances
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DFSR\Parameters
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DfsDriver\Instances
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dfsc\Parameters
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dfs\Parameters
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ldap
  - HKEY_LOCAL_MACHINE\Software\Policies\\Microsoft
  - HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\W32time\Parameters
  - HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\W32Time\Config

- События из следующих журналов ОС Windows для последующего комплексного анализа работоспособности системы и возможных рисков в ее функционировании:
  - Application;
  - Security;
  - System;
  - DFS Replication:
  - Directory Service;
  - DNS Server;
  - Microsoft-Windows-NTLM/Operational;
  - Microsoft-Windows-SMBServer/Audit.
- Информация об использовании устаревших и/или небезопасных протоколов, полученная на основе накопленного и предварительно настроенного аудита использования протоколов аутентификации:
  - NTLM V1;
  - LDAP Simple Bind (без SSL/TLS);
  - Использование NTLM там, где должен и может использоваться Kerberos.
- Информация об использовании слабых протоколов учетными записями с высокими привилегиями, выявленная с помощью категоризации пользователей по уровню привилегий;
- Информация об объектах AD, таких как пользователь, компьютер, корень домена, DNS-зоны, объекты групповых политик, дополнительные парольные политики. Анализ настроек аутентификации, зарегистрированных сервисных имен (SPN), время последних активностей объектов безопасности;
- Схема Active Directory;
- Информация по следующим DN'ам и анализ делегирования разрешений на предмет выявления дополнительных привилегированных УЗ:
  - Domain Root
  - CN=Policies, CN=System
  - OU=Domain Controllers
  - CN=Public Key Services,CN=Services,CN=Configuration
  - CN=AdminSDHolder,CN=System
  - CN=LostAndFound
  - CN=RegisteredDevices
  - CN=Managed Service Accounts
  - CN=Password Settings Container,CN=System
  - CN=RID Manager$,CN=System
  - CN=DFSR-GlobalSettings,CN=System
  - CN=File Replication Service,CN=System
  - CN=Infrastructure
  - CN=MicrosoftDNS,CN=System
  - CN=WMIPolicy,CN=System
  - CN=Partitions
  - CN=Configuration
  - CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration
  - CN=Sites,CN=Configuration

Данные, собираемые с SharePoint Server

- Список серверов фермы и их роли;
- Версии установленных накопительных обновлений для SharePoint;
- Список веб-приложений и их параметры;
- Список баз данных фермы и их параметры;
- Настройки системы ведения журнала и сроки хранения файлов журналов;
- Настройки безопасности фермы и ее компонентов;
- Реестр ошибок заданий сервиса таймера;
- Данные счетчиков производительности SharePoint:
    - \HTTP Service Request Queues(*)\CurrentQueueSize
    - \HTTP Service Request Queues(*)\MaxQueueItemAge
    - \ASP.NET\Application Restarts
    - \ASP.NET\Requests Queued
    - \ASP.NET\Requests Rejected
    - \ASP.NET\Request Wait Time
    - \ASP.NET\Worker Process Restarts
    - \ASP.NET Applications(*)\Requests/Sec
    - \.NET CLR Memory(*)\# Bytes in all Heaps
    - \.NET CLR Memory(*)\% Time in GC
    - \SharePoint Foundation(*)\Current Page Requests
    - \SharePoint Foundation(*)\Executing Sql Queries
    - \SharePoint Foundation(*)\Executing Time/Page Request
    - \SharePoint Foundation(*)\Reject Page Requests Rate
    - \SharePoint Foundation(*)\Responded Page Requests Rate
    - \SharePoint Foundation(*)\Sql Query Executing time
    - \SharePoint Foundation(*)\Throttled Page Requests

Данные, собираемые с SQL Server

- Данные счетчиков производительности счётчика баз данных
    - \SQLServer:Buffer Manager*
    - \SQLServer:Buffer Node(*)*
    - \SQLServer:Catalog Metadata(*)*
    - \SQLServer:Exec Statistics\
    - \SQLServer:Latches*
    - \SQLServer:Locks(*)*
    - \SQLServer:Database Replica(*)*
    - \SQLServer:Availability Replica(*)*
    - \SQLServer:Buffer Node(*)*
    - \SQLServer:Catalog Metadata(*)*
    - \SQLServer:Exec Statistics*
    - \SQLServer:Latches*
    - \SQLServer:Locks(*)*
    - \SQLServer:Memory Manager*
    - \SQLServer:General Statistics*
    - \SQLServer:SQL Statistics*
    - \SQLServer:Transactions*
    - \SQLServer:Wait Statistics(*)*
    - \SQLServer:Memory Node(*)*
    - \SQLServer:Databases(*)*
    - \SQLServer:Access Methods*
- Служебная информация по каждой базе данных
- Журналы ошибок, запусков регламентных заданий и авторизации
- Статистика ожиданий
- Информация о файлах баз данных и журналах транзакций
- Установленные компоненты
- Информация о прилинкованных серверах
- Данные о конфигурации службы SQL Server
- Журнал резервного копирования
- Статистика виртуальных файловых журналов (VLF)
- Результаты DMV
- Журнал агента
- Данные XEvents

Данные, собираемые с Exchange Server

- Данные счетчиков доступа Exchange к LDAP:
  - \MSExchange ADAccess Domain Controllers(*)\LDAP Read Time
  - \MSExchange ADAccess Domain Controllers(*)\LDAP Search Time
  - \MSExchange ADAccess Processes(*)\LDAP Read Time
  - \MSExchange ADAccess Processes(*)\LDAP Search Time
- Данные счетчиков для баз данных:
  - \MSExchange Database ==> Instances(*)\I/O Database Reads (Attached) Average Latency
  - \MSExchange Database ==> Instances(*)\I/O Database Writes (Attached) Average Latency
  - \MSExchange Database ==> Instances(*)\I/O Log Writes Average Latency
  - \MSExchange Database ==> Instances(*)\I/O Database Reads (Recovery) Average Latency
  - \MSExchange Database ==> Instances(*)\I/O Database Writes (Recovery) Average Latency
  - \MSExchange Database ==> Instances(*)\I/O Database Reads (Attached)/sec
  - \MSExchange Database ==> Instances(*)\I/O Database Writes (Attached)/sec
  - \MSExchange Database ==> Instances(*)\I/O Log Writes/sec
  - \MSExchange Active Manager(_total)\Database Mounted
- Данные счетчиков RPC:
  - \MSExchange RpcClientAccess\RPC Averaged Latency
  - \MSExchange RpcClientAccess\RPC Requests
  - \MSExchange RpcClientAccess\Active User Count
  - \MSExchange RpcClientAccess\Connection Count
  - \MSExchange RpcClientAccess\RPC Operations/sec
  - \MSExchange RpcClientAccess\User Count
- Счетчики Information Store:
  - \MSExchangeIS Store(*)\RPC Requests
  - \MSExchangeIS Client Type(*)\RPC Average Latency
  - \MSExchangeIS Store(*)\RPC Average Latency
  - \MSExchangeIS Store(*)\RPC Operations/sec
  - \MSExchangeIS Client Type(*)\RPC Operations/sec

- Данные счетчиков Client Access:
  - \MSExchange ActiveSync\Requests/sec
  - \MSExchange ActiveSync\Ping Commands Pending
  - \MSExchange ActiveSync\Sync Commands/sec
  - \MSExchange Availability Service\Availability Requests (sec)
  - \MSExchange OWA\Current Unique Users
  - \MSExchange OWA\Requests/sec
  - \MSExchangeAutodiscover\Requests/sec
  - \MSExchangeWS\Requests/sec
  - \Web Service(_Total)\Current Connections
  - \Web Service(Default Web Site)\Current Connections
  - \Web Service(_Total)\Connection Attempts/sec
  - \Web Service(_Total)\Other Request Methods/sec
- Файлы настроек серверов и веб-приложений (.conf);
- Данные по всем почтовым ящикам и их настройкам;
- Данные о конфигурации Exchange Server (настройки и версия Microsoft Exchange Server, настройки DAG, настройки организации, настройки почтового потока и транспорта, данные о БД (расположение, размер), настройки политик ограничения – Throttling Policy).

Данные, собираемые с Skype for Business Server

- Информация об SSL-сертификатах;
- Топология Skype for Business;
- Версия Skype Cumulative Update;
- Версия SQL Update;
- Настройки политик Skype;
- Настройки конфигурации Skype;
- Статистика звонков из базы мониторинга (если таковая имеется).

Для анализа качества Media (MQA) также собираются данные сессий аудио/видеозвонков, конференций, SIP-телефонии из базы данных Skype Monitoring, которые включают:

- Дату, время медиа-сессий за последние 2 недели;
- Список всех участников (SIP URI пользователей из атрибутов AD MsRtcSip);
- Версии и конфигурации клиентов;
- Информацию о звуковом оборудовании клиентов (гарнитуры, звуковые устройства и их драйверы);
- Сетевую информацию (IP-адрес, шлюз, маршрут медиа, параметры звонка, протоколы);
- Информацию о качестве звонков (TCP/UDP статистика, потери фрагментов, задержки).

Данные, собираемые с SCCM/MECM

- Данные о статусах и настройках сервисов, относящихся к SCCM/MECM:
  - SMS Agent Host
  - SMS_EXECUTIVE
  - SMS_SITE_COMPONENT_MANAGER
  - SMS_SITE_VSS_WRITER
  - SMS_NOTIFICATION_SERVER
  - SMS_SITE_BACKUP
  - SMS_SYSTEM_HEALTH_VALIDATOR
  - SMS_SITE_SQL_BACKUP
- Объекты WMI из следующих пространств имен:
  - Root\CCM
  - Root\SCCMDP
  - Root\SMS
- Значения следующих веток реестра:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CCM
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CCMSetup
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server
- Файлы журналов SCCM/MECM с серверов сайтов, систем сайтов и клиентов;
- Статусные сообщения с серверов сайтов;
- Информация о количестве файлов в папках Inboxes\Outboxes;
- Данные о конфигурациях серверов SQL:
  - Версия MS SQL Server;
  - Параметры сервера;
  - Членство в кластере или группе AlwaysOn.
- Информация, получаемая SQL-запросами из базы данных SCCM/MECM:
  - Коды сайтов, их тип и текущий статус;
  - Статус пакетов обновлений SCCM/MECM;
  - Список всех сайт-систем сайтов;
  - Количество клиентов для каждого сайта;
  - Количество MP для каждого сайта;
  - Количество клиентов для каждой MP;
  - Количество клиентов для каждой SUP;
  - Количество DP и Pull DP для каждого сайта;

- Расширенные свойства каждой DP;
- Пакеты и их статусы для каждой DP;
- Конфигурация задач обслуживания сайтов;
- Статусы компонентов SCCM/MECM;
- Расширенная информация об обновлениях:
    - Используемые продукты/классификации обновлений;
    - Информация о настройках и размещении точек SUP;
    - Статусы синхронизации точек SUP;
    - Статусы синхронизации обновлений;
    - Источники обновлений.
- Расширенная информация о коллекциях:
    - Перечень запросов для коллекций;
    - Правила Include/Exclude для коллекций;
    - Коллекции с прямым членством;
    - Список пустых коллекций;
    - Коллекции с ручным режимом обновления;
    - Инкрементальные коллекции.
- Информация о клиентах:
    - Настройки клиентов;
    - Клиенты с дублирующимися GUID;
    - Дублирующиеся MAC-адреса;
    - Дублирующиеся SMBIOS GUID;
    - Клиенты с недостаточным объемом памяти;
    - Версии клиентов;
    - Статусы клиентов.

- Информация о границах и группах границ;
- Детальная информация о межсайтовой репликации DRS;
- Содержимое Site Control File.
- События из следующих журналов ОС Windows для последующего комплексного анализа:
    - Application;
    - System.
- Дополнительно собираемые данные счетчиков:
    - \SMS Discovery Data Manager\User DDRs Processed/minute

- \SMS Discovery Data Manager\Total User DDRs Processed
- \SMS Discovery Data Manager\Total User DDRs Enqueued
- \SMS Discovery Data Manager\Total Non-User DDRs Processed
- \SMS Discovery Data Manager\Total Non-User DDRs Enqueued
- \SMS Discovery Data Manager\Total Client Registration Requests Processed
- \SMS Discovery Data Manager\Total Bad User DDRs Processed
- \SMS Discovery Data Manager\Total Bad Non-User DDRs Processed
- \SMS Discovery Data Manager\Non-User DDRs Processed/minute

- \SMS Server Availability(*)\Total Requests
- \SMS Server Availability(*)\Successful Requests
- \SMS Server Availability(*)\Failed Requests
- \SMS Server Availability(*)\Avg. Request Latency

- \SMS In-Memory Queues(*)\Total Objects Enqueued
- \SMS In-Memory Queues(*)\Total Objects Dequeued

- \SMS Executive Thread States(*)\Yielding Thread Count
- \SMS Executive Thread States(*)\Sleeping Thread Count
- \SMS Executive Thread States(*)\Running Thread Count
- \SMS Inbox(*)\File Current Count

- \SMS Inventory Data Loader\Total MIFs Processed
- \SMS Inventory Data Loader\Total MIFs Enqueued
- \SMS Inventory Data Loader\Total Bad MIFs Processed
- \SMS Inventory Data Loader\MIFs Processed/minute
- \SMS Inventory Data Loader\Average MIF size (KB)

- \SMS Standard Sender(*)\Total Bytes Sent
- \SMS Standard Sender(*)\Total Bytes Failed
- \SMS Standard Sender(*)\Total Bytes Attempted
- \SMS Standard Sender(*)\Sending Thread Count
- \SMS Standard Sender(*)\Current Bytes Being Sent
- \SMS Standard Sender(*)\Average Bytes/sec

- \SMS Outbox(*)\Total Files Copied
- \SMS Outbox(*)\Total File Copy Failures
- \SMS Outbox(*)\Files Copied/min
- \SMS Outbox(*)\File Current Count

- \SMS Scheduler(*)\Number of Send Requests
- \SMS Scheduler(*)\Number of Jobs
- \SMS Software Metering Processor\Total SWM Usage Records Processed
- \SMS Software Metering Processor\Total SWM Usage Processing Threads
- \SMS Software Metering Processor\Total SWM Usage Files Enqueued
- \SMS Software Metering Processor\Total Bad SWM Usage Files Processed
- \SMS Software Metering Processor\SWM Usage Records Processed/minute

- \SMS State System\Total Message Records Processed
- \SMS State System\Total Message Files Processed
- \SMS State System\Total Invalid Message Records Processed
- \SMS State System\Total Bad Message Files Processed
- \SMS State System\Summary Task Running
- \SMS State System\Message Records Processed/min
- \SMS State System\Message File Records PreProcessed/min
- \SMS State System\Message File Processing Threads

- \SMS Status Messages(*)\Written To SMS Database
- \SMS Status Messages(*)\Reported To Application Event Log
- \SMS Status Messages(*)\Replicated At Normal Priority
- \SMS Status Messages(*)\Replicated At Low Priority
- \SMS Status Messages(*)\Replicated At High Priority
- \SMS Status Messages(*)\Received
- \SMS Status Messages(*)\Processed/sec
- \SMS Status Messages(*)\Corrupt

- \SMS WSUS Sync Manager\Total Updates Written
- \SMS WSUS Sync Manager\Average Updates Written/min