

Защита внутренней сети: McAfee VirusScan Enterprise 8.0i и ePolicy Orchestrator 3.5

Этот курс позволит приобрести навыки в установке и настройке основных продуктов McAfee для защиты внутренней сети организации: McAfee VirusScan® Enterprise 8.0i и Installation Designer 8.0. С помощью детальных лабораторных работ слушатели курса научатся развертывать и администрировать данные продукты, используя средство централизованного управления McAfee ePolicy Orchestrator® (ePO™) 3.5.



Необходимые навыки

Общее понимание теории вирусов и антивирусных технологий.

Лабораторные работы

Все темы сопровождаются лабораторными упражнениями, специально разработанными для увеличения отдачи от курса. Лабораторные работы в классе предоставляют основной практический опыт, необходимый для установки, настройки и управления антивирусными продуктами McAfee.

Материалы курса

- Учебное пособие

Продолжительность

- 4 дня

После прохождения курса слушатели смогут

- Устанавливать и настраивать McAfee Installation Designer 8.0
- Описывать компоненты и возможности McAfee ePolicy Orchestrator
- Инсталлировать ePO 3.5
- Запускать консоль ePO, создавать дерево директории и распространять программное обеспечение
- Развертывать и управлять агентами ePO
- Развертывать и управлять VirusScan Enterprise 8.0i с помощью ePO
- Запускать отчеты ePO
- Описывать, как ePO взаимодействует с Microsoft SQL
- Развертывать и управлять хранилищами ePO
- Создавать хранилище на основе супер-агента ePO
- Развертывать систему глобального обновления и управлять глобальными обновлениями DAT-файлов
- Добавлять обновления для программных продуктов в ePO
- Создавать собственные запросы
- Поддерживать ePO

Рекомендуемые следующие курсы

Для расширения знаний и навыков по управлению антивирусными продуктами McAfee рекомендуется пройти следующие учебные курсы:

- Антивирусное администрирование McAfee GroupShield (TRN-AVD-201-TCL)
- Антивирусное администрирование McAfee WebShield (TRN-AVD-301-TCL)

Контактная информация

Associates
Телефон: +7 (095) 730 7476
E-mail: education@associates.ru

Программа курса

День первый

Обзор VirusScan

- Свойства и особенности
- Стратегия доверительного соединения
- Компоненты VirusScan
- Дополнительные утилиты
- Common Framework

Установка

- Аппаратные и программные требования
- Привилегии, необходимые для установки
- Методы и возможности установки
- Процесс инсталляции и uninstall.ini
- Установка на кластер-сервер
- Файлы и директории VirusScan
- Восстановление и удаление
- *Лабораторная работа: установка VirusScan с помощью графического интерфейса*
- *Лабораторная работа: установка и удаление VirusScan с помощью командной строки*

Настройки

- Доступ к VirusScan
- Консоль
- Задачи и политики по умолчанию
- Защита доступа с помощью блокировки портов
- Защита файлов, ресурсов общего доступа и папок
- Правила защиты доступа по умолчанию
- Создание правил
- Защита от переполнения буфера и исключения
- Защита от нежелательных программ
- Настройка фонового сканера
- Компонент скрипт-сканер
- Исключения из области сканирования для Microsoft Exchange и Lotus Domino
- Защита опасных и безопасных процессов
- Проверка обнаружения вирусов
- Сканирование электронной почты в момент приема и по запросу
- Сканер по запросу и планировщик
- Сканирование из командной строки
- Пользовательский интерфейс и возможности удаленного администрирования
- *Лабораторная работа: создание и тестирование правил блокировки портов*
- *Лабораторная работа: настройка и тестирование защиты файлов, ресурсов общего доступа и папок*
- *Лабораторная работа: тестирование защиты от переполнения буфера*
- *Лабораторная работа: тестирование политик для нежелательных программ*
- *Лабораторная работа: определение настроек сканера по умолчанию*

- *Лабораторная работа: настройка сканирования для опасных и безопасных процессов*
- *Лабораторная работа: защита пользовательского интерфейса паролем*

Обновление

- Обзор
- Типы обновлений
- Обновления сигнатур и сканирующего механизма
- Другие обновления
- Стратегия обновлений
- Веб-сайты McAfee
- Опции защиты в процессе обновления
- Обновление по умолчанию
- Задача и процесс автоматического обновления
- Инкрементальные обновления
- Настройка и планирование автоматических обновлений
- Редактирование списка хранилищ обновлений
- Альтернативные методы обновлений
- Задача зеркалирования
- *Лабораторная работа: создание ftp-сервера для обновлений*
- *Лабораторная работа: зеркалирование удаленного сервера с локальным хранилищем*
- *Лабораторная работа: редактирование списка хранилищ обновлений*
- *Лабораторная работа: настройка и планирование автоматических обновлений*

День второй

Стратегия и политика

- Корпоративная стратегия
- Развертывание антивирусной политики
- Соответствие, применение и видимость
- Продукты, управляемые с помощью ePO
- Компоненты и процессы ePO

Установка

- Требования и факторы окружения
- Виды развертывания
- Сервер и база данных
- Обновление до ePO 3.5
- Процесс установки
- Консоль и интерфейс ePO
- *Лабораторная работа: установка ePO 3.5*
- *Лабораторная работа: доступ к консоли ePO*

Агент ePO

- Требования для установки и поддерживаемые платформы
- Развертывание агентов через консоль
- Развертывание агентов с помощью скриптов
- Другие методы развертывания
- Файлы агента ePO
- Настройка инсталляционного пакета агента

- Использование мастера для малого бизнеса
- Доступ к журналам агента
- Взаимодействие агента
- Принудительная активация агента
- Суперагент
- *Лабораторная работа: создание сайта для агента ePO*
- *Лабораторная работа: принудительная активация агента*
- *Лабораторная работа: доступ к журналам агента*
- *Лабораторная работа: чтение журналов агента*

День третий

Директория

- Понятие директории
- Методы построения директории
- Сайты, группы и наследование
- Определение объектов директории
- Методы создания директории
- Опрос Active Directory
- Фильтрация на основе IP-адресов
- Поиск незащищенных систем
- *Лабораторная работа: роли администраторов ePO*
- *Лабораторная работа: IP-фильтрация*
- *Лабораторная работа: использование задачи опроса Active Directory*
- *Лабораторная работа: использование сенсора обнаружения незащищенных систем*

Политики, свойства и задачи

- Движение политик и наследование
- Концепция политик
- Взаимодействие и политики агента
- Варианты обновления агента
- Политики продуктов
- Импорт и экспорт политик
- System Compliance Profiler
- Возможности Entercept
- Сайт, группа и свойства компьютера
- Задачи обновления клиента
- *Лабораторная работа: настройка политик агента и обзор наследования*
- *Лабораторная работа: подтверждение применения политик*
- *Лабораторная работа: проверка свойств компьютера*
- *Лабораторная работа: установка политик VirusScan*
- *Лабораторная работа: обзор собранных событий агента*
- *Лабораторная работа: добавление задачи сканирования для VirusScan*

Задачи и хранилища сервера ePO

- Обзор хранилищ
- Требования для установки и поддерживаемые платформы хранилищ
- Управление обновлениями
- Возможности обновления для мобильных компьютеров
- Выборочное обновление
- Главное и распределенные хранилища
- Источник и резервные хранилища
- Создание хранилищ
- Управление продуктами в хранилище
- Типы задач и определения
- Проверка соответствия
- Задачи наполнения и репликации
- Выбор хранилища
- Простые топологии
- Глобальное обновление при репликации хранилища на основе суперагента
- *Лабораторная работа: добавление дистрибутивов в хранилище*
- *Лабораторная работа: развертывание VirusScan через ePO*
- *Лабораторная работа: создание задач наполнения и репликации*
- *Лабораторная работа: использование глобального обновления*

День четвертый

Отчеты ePO

- Доступ к базе данных ePO
- Ограничения авторизации
- Опции базы данных
- Фильтрация директории
- Фильтрация событий
- Типы и интерфейс отчетов
- Отчеты о заражении и покрытии
- Развертывание отчетов
- Настройка отчетов и сохранение настроек
- Добавление отчетов
- Типы запросов
- Запуск запросов
- Проверка запросов
- Добавление запросов
- *Лабораторная работа: запуск запросов и отчетов*
- *Лабораторная работа: составление и добавление запросов*

Поддержка и мониторинг ePO

- Серверные события и счетчики быстрого действия
- Операции над директорией
- Настройка SQL-аутентификации ePO
- Резервное копирование и восстановление
- *Лабораторная работа: резервное копирование и восстановление базы данных*