

КОД  
ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ



# КАК КОНТРОЛИРОВАТЬ ДЕЙСТВИЯ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ?

Максим ЛУГАНСКИЙ  
*Micro Focus*

# IAM-решения от Micro Focus (ранее - Novell, NetIQ)

## Identity

Identity Manager  
Identity Governance  
eDirectory  
IGA as-a-Service

## Access

Access Manager  
Advanced Authentication  
SecureLogin  
Self Service Password Reset  
Access as-a-Service

## Privilege

Privileged Account Manager  
Directory & Resource Administrator  
Group Policy Administrator  
Change Guardian  
Security Solutions for IBM i

# Привилегированные учетные записи

- Учетные записи, имеющие расширенный доступ к важной информации в организации:
  - Доступ к файлам и директориям на чтение и запись
  - Установка и запуск приложений и исполняемых скриптов
  - Изменение настроек и конфигураций
  - Создание новых учетных записей, изменение прав доступа
- Сервисные и системные учетные записи:
  - Root
  - Administrator
  - db\_admin
  - sysdba и т.д.
- Пользователи, кому в соответствии с ролью или особыми знаниями предоставлен более глубокий доступ к информации
  - Начальник отдела
  - Администратор специфической корпоративной системы

# Чем больше привилегий, тем выше риск



**Внешние угрозы**



**Внутренние угрозы**



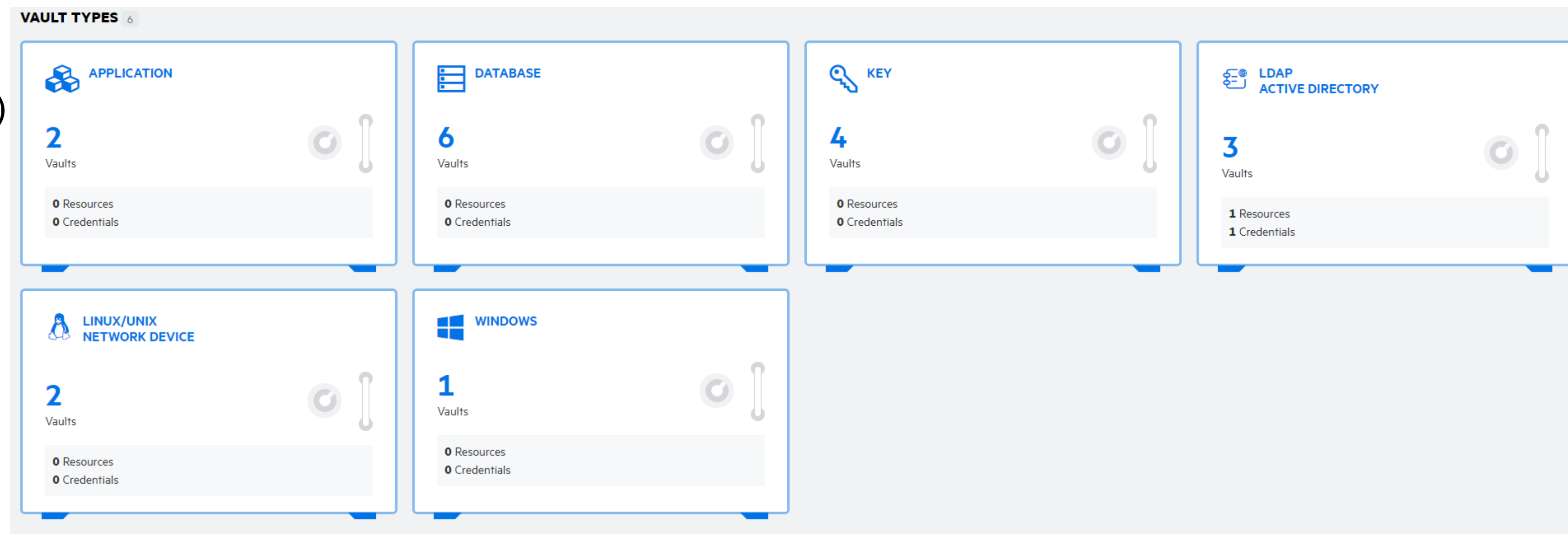
**Несоответствие требованиям**

# Micro Focus Privileged Account Manager (PAM)

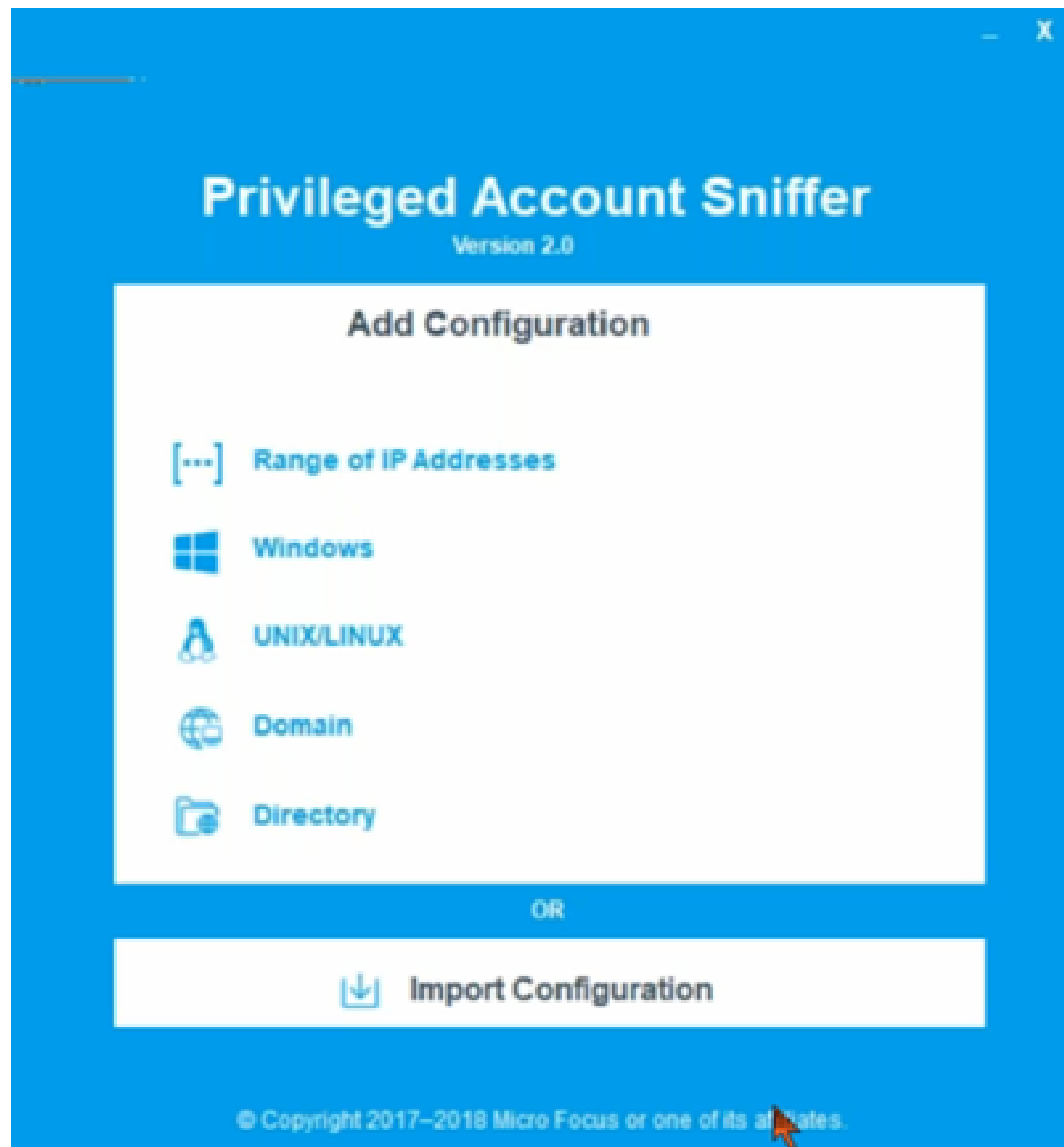
- Централизованный инструмент для управления созданием и мониторингом привилегированных учетных записей
- Обнаружение имеющихся привилегированных учетных записей
  - Опрос различных типов устройств в сети
  - Вывод информации в виде CSV-файла, возможен импорт в PAM
- Гибкие механизмы контроля сессий
  - Настраиваемые правила отнесения сессий к подлежащим контролю
  - «Белые» и «черные» списки вводимых команд
  - Настраиваемые уровни риска для различных команд
- Аудит действий
  - Кто, когда, куда и под какой учетной записью заходил
  - Видеозапись сессий с возможностью контекстного поиска
  - Снятие скриншотов во время сессии
- «Аудит аудиторов»
  - Логирование действий администраторов системы PAM

# Credential Vault – централизованное хранилище паролей

- Безопасное зашифрованное "хранилище" для учетных данных (логинов и паролей), ключей и т.п.
- Workflow запроса и предоставления учетных данных из Credential Vault
- Хранение различных типов учетных данных:
  - Доменные учетные записи
  - Серверы
  - Сетевое оборудование
  - Приложения (классические, веб)
  - Базы данных
  - Облачные службы
- Автоматическая ротация паролей



# Обнаружение привилегированных учетных записей







# Аудит действий

## DETAILS




AUDIT ID: **D11B13E4-4D4E-6F40-9A5B-1B07466F5C67** [Copy ID](#)

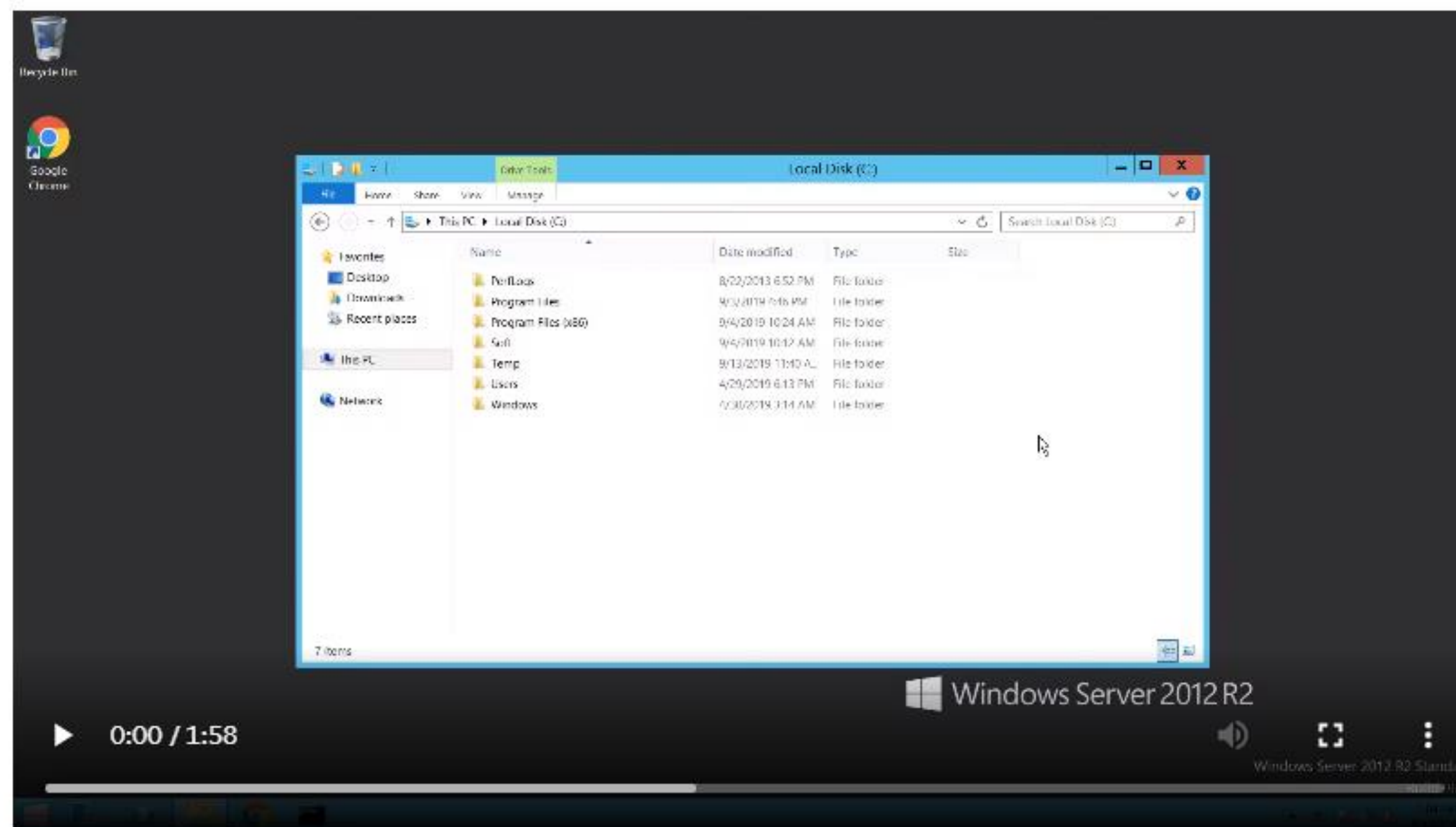
COMMAND: <RDP> RDP

1 OVERVIEW 2 KEYSTROKES 3 SCREENSHOTS 4 **VIDEOS**

Video File:

All  Filtered Events

-  Left mouse click Program Manager [Program Manager](SysListView32 :: FolderView) Left mouse click\n  
Sep 13, 2019, 1:05:27 PM
-  Left mouse double click Program Manager [Program Manager] (SysListView32 :: FolderView) Left mouse double click\n  
Sep 13, 2019, 1:05:27 PM
-  Open file C:\\\\Users\\\\lugansky\\\\Desktop\\\\003.txt  
Sep 13, 2019, 1:05:27 PM



# Аудит действий

## DETAILS

AUDIT ID: **D11B13E4-4D4E-6F40-9A5B-1B07466F5C67** [Copy ID](#)

COMMAND: <RDP> RDP

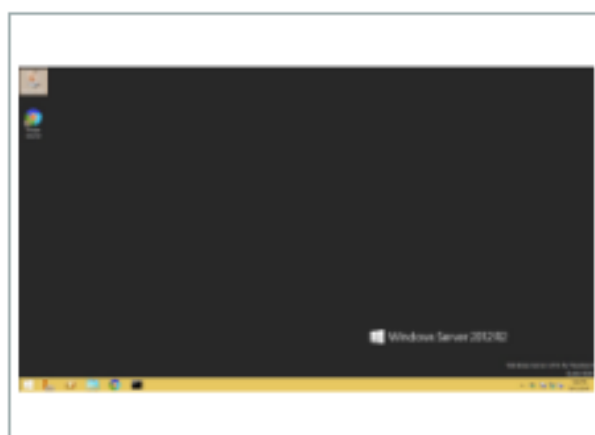
- 1 OVERVIEW
- 2 KEYSTROKES
- 3 SCREENSHOTS**
- 4 VIDEOS

▶ SLIDESHOW

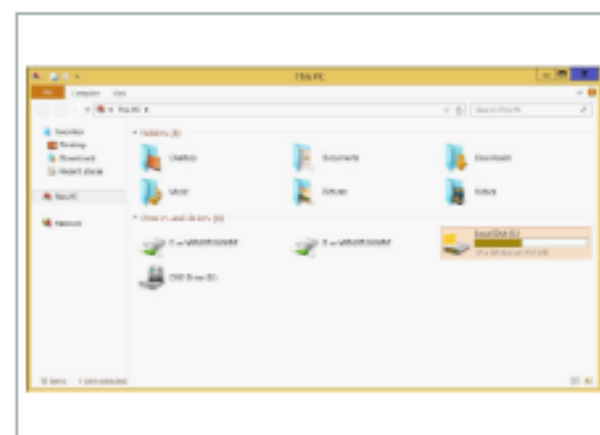
🔍 Search by date



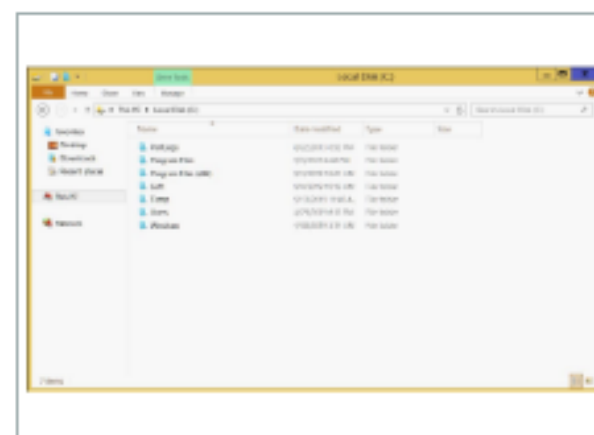
[Fri Sep 13 2019 13:04:54 GMT+0300 \(Arabian Standard Time\)](#)



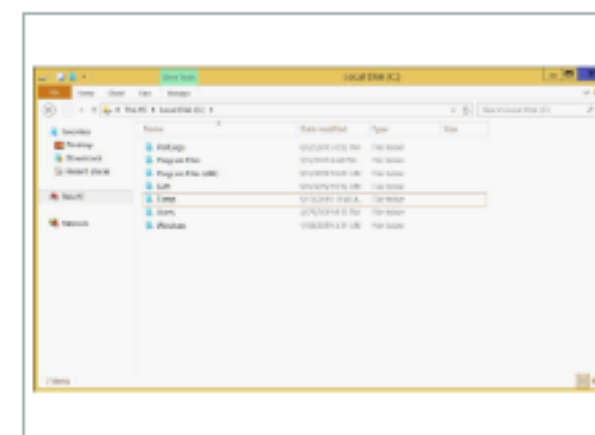
[Fri Sep 13 2019 13:04:55 GMT+0300 \(Arabian Standard Time\)](#)



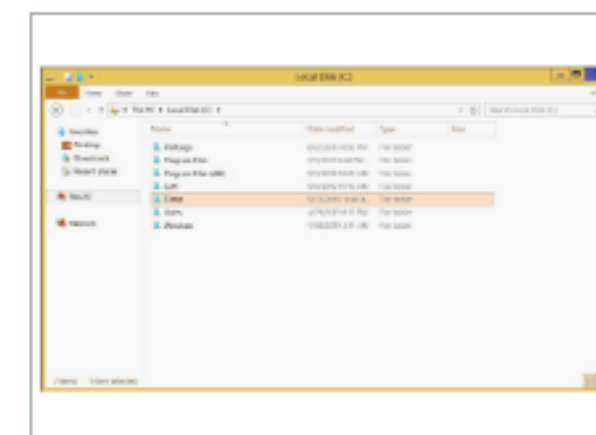
[Fri Sep 13 2019 13:04:59 GMT+0300 \(Arabian Standard Time\)](#)



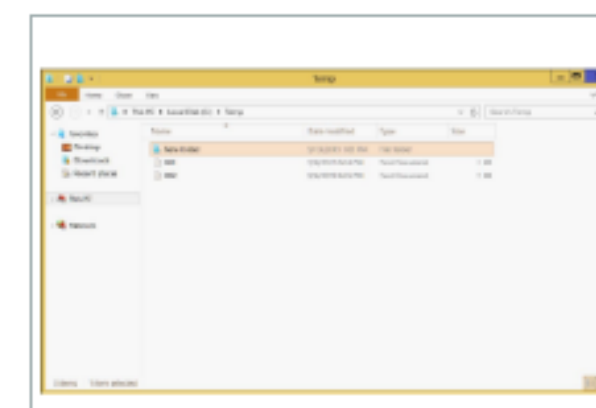
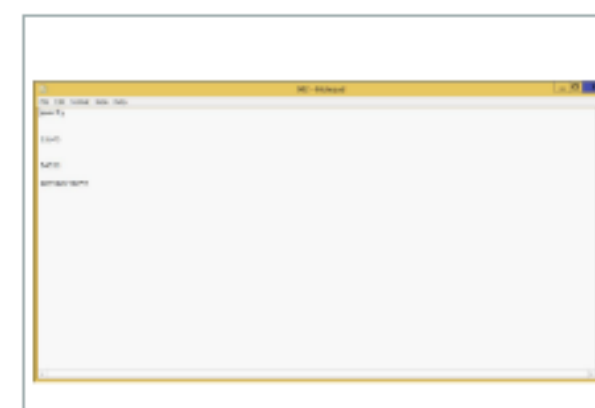
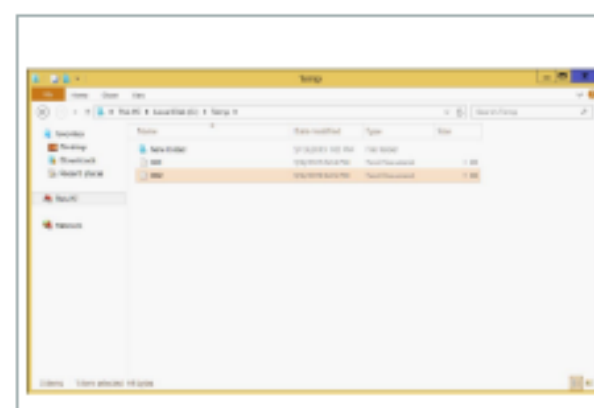
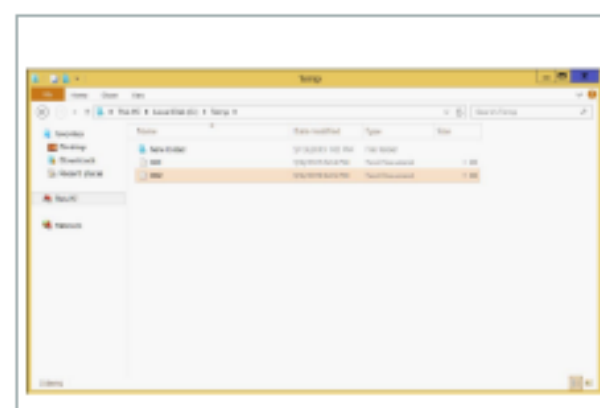
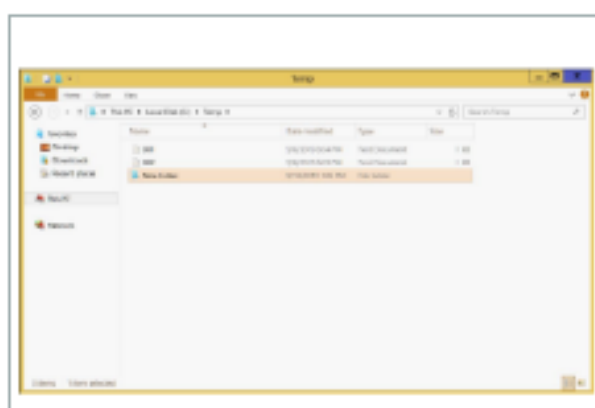
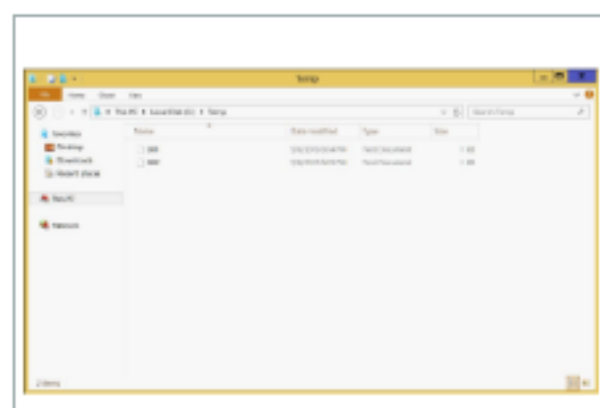
[Fri Sep 13 2019 13:04:59 GMT+0300 \(Arabian Standard Time\)](#)



[Fri Sep 13 2019 13:05:00 GMT+0300 \(Arabian Standard Time\)](#)



[Fri Sep 13 2019 13:05:01 GMT+0300 \(Arabian Standard Time\)](#)

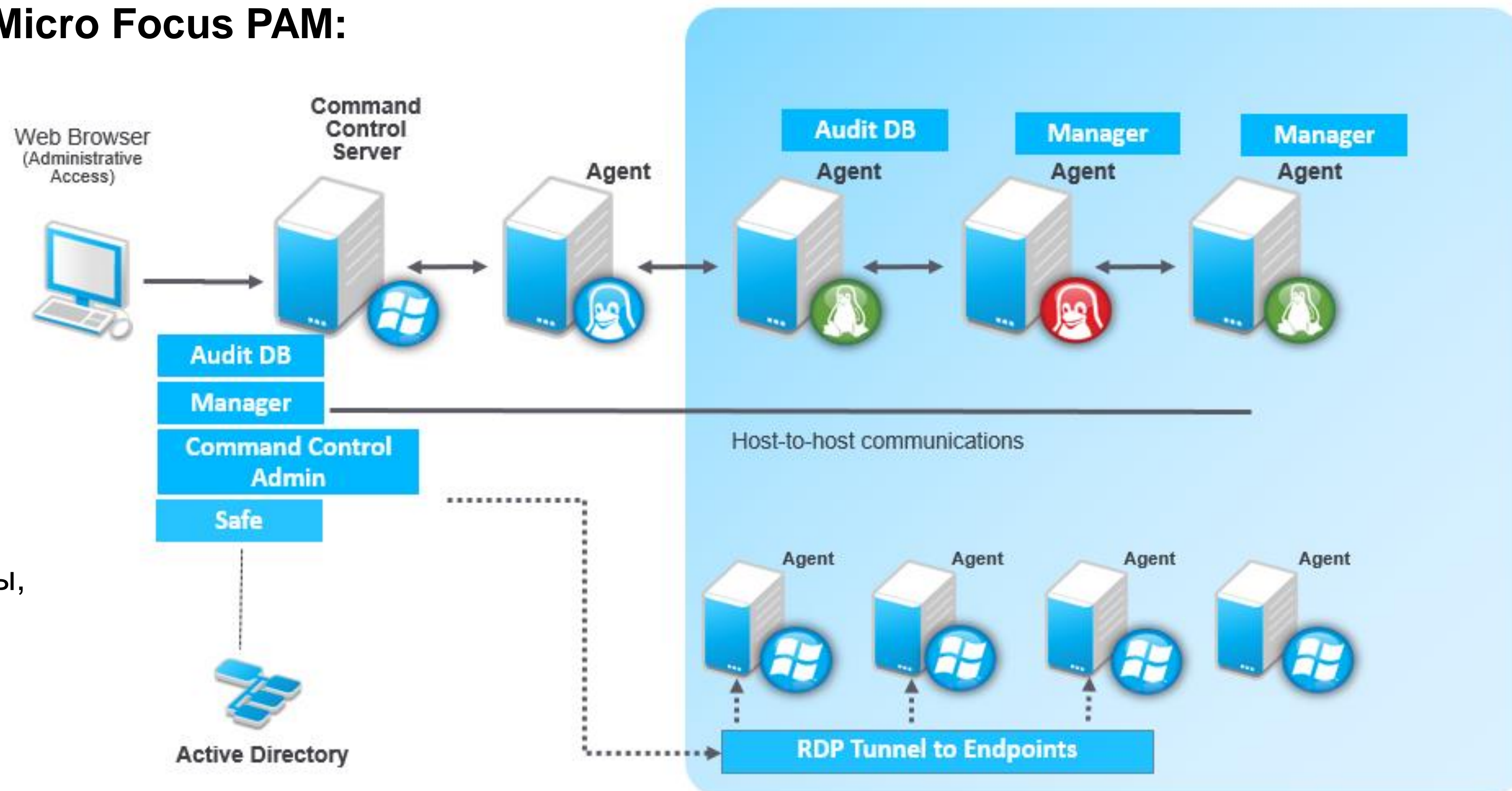


< PREVIOUS SESSION    NEXT SESSION >    ✕ CLOSE

# Модульная архитектура Micro Focus PAM

## Варианты развертывания Micro Focus PAM:

- Через агента
  - Windows, Linux, UNIX, Mac
  - Подробный мониторинг
- Безагентно (через «Jump server»)
  - Если ОС не поддерживается
  - Установка на устройства, на которые нет возможности установить агент (коммутаторы, маршрутизаторы и т.д.)



# Интеграция с другими IAM-решениями от Micro Focus

## Identity

Identity Manager  
Identity Governance  
eDirectory  
IGA as-a-Service

## Access

Access Manager  
Advanced Authentication  
SecureLogin  
Self Service Password Reset  
Access as-a-Service

## Privilege

Privileged Account Manager  
Directory & Resource Administrator  
Group Policy Administrator  
Change Guardian  
Security Solutions for IBM i

# Лицензирование Micro Focus RAM

- Состав спецификации на ПО Micro Focus:
  - Лицензии (бессрочные)
  - Сертификат на техподдержку (24x7, минимум 1 год)
- Базовая лицензия Micro Focus IAM (покупается в кол-ве 1 шт. на заказчика на всю линейку IAM)
- Лицензия RAM по кол-ву управляемых НЕпользовательских устройств
  - Серверы, сетевые устройства, приложения, виртуальные машины и т.д.
- Лицензия RAM по кол-ву управляемых пользовательских устройств
  - ПК, ноутбуки и т.п.

— #CODEIB —

**СПАСИБО ЗА ВНИМАНИЕ**



**Maxim.Lugansky@microfocus.com**

**+7 915 010 42 96**