



WALLIX РАЗРЕШЕНИЯ ПО
КИБЕРБЕЗОПАСНОСТИ И УПРАВЛЕНИЮ
ДОСТУПА К ИНФОРМАЦИОННОЙ СИСТЕМЕ

Докладчик: Бозоров С.





Два опытных учредителя у руля



Jean-Noël de Galzain

Основатель и председатель правления

Основатель Aurora, сервисной компании, проданной Business & Decision в 2003 году.
Председатель-учредитель клуба HEXATRUST
Заместитель председателя бизнес-кластера «Систематический Парижский регион»



Amaury Rosset

Соучредитель и финансовый директор

Четыре года в Hachette Filipacchi Media в качестве финансового контролера, менеджера проектов в Азиатско-Тихоокеанском регионе (Гонконг), а затем помощника издателя гонконгских и китайских изданий Группы.
Основатель агентства мультимедийных коммуникаций XLAB.

01

PRIVILEGED ACCESS MANAGEMENT:

ПОСЛЕДНЕЕ ПОКОЛЕНИЕ

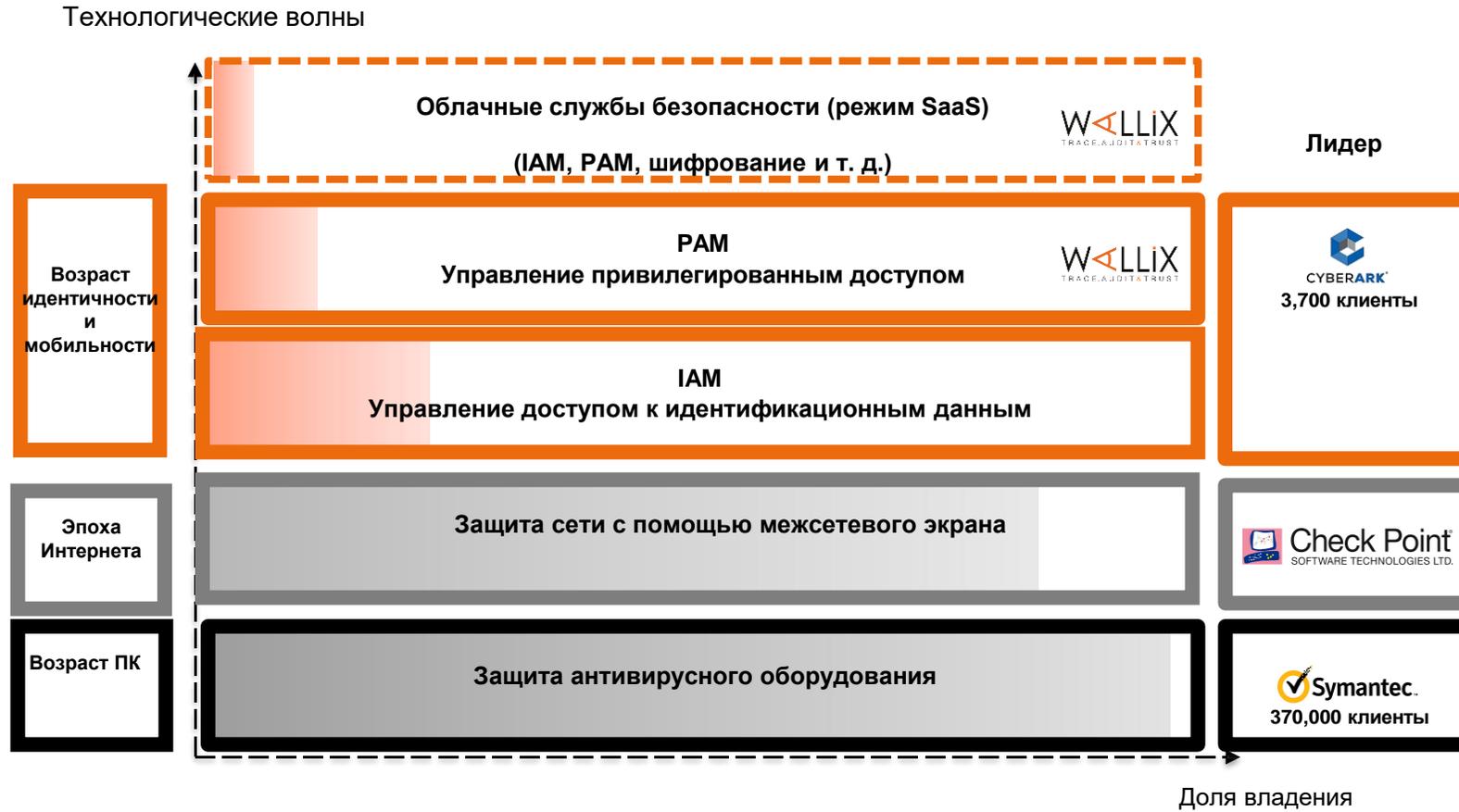
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

КИБЕРБЕЗОПАСНОСТИ

WALLIX
TRACE, AUDIT & TRUST



НОВАЯ ЭРА КИБЕРБЕЗОПАСНОСТИ

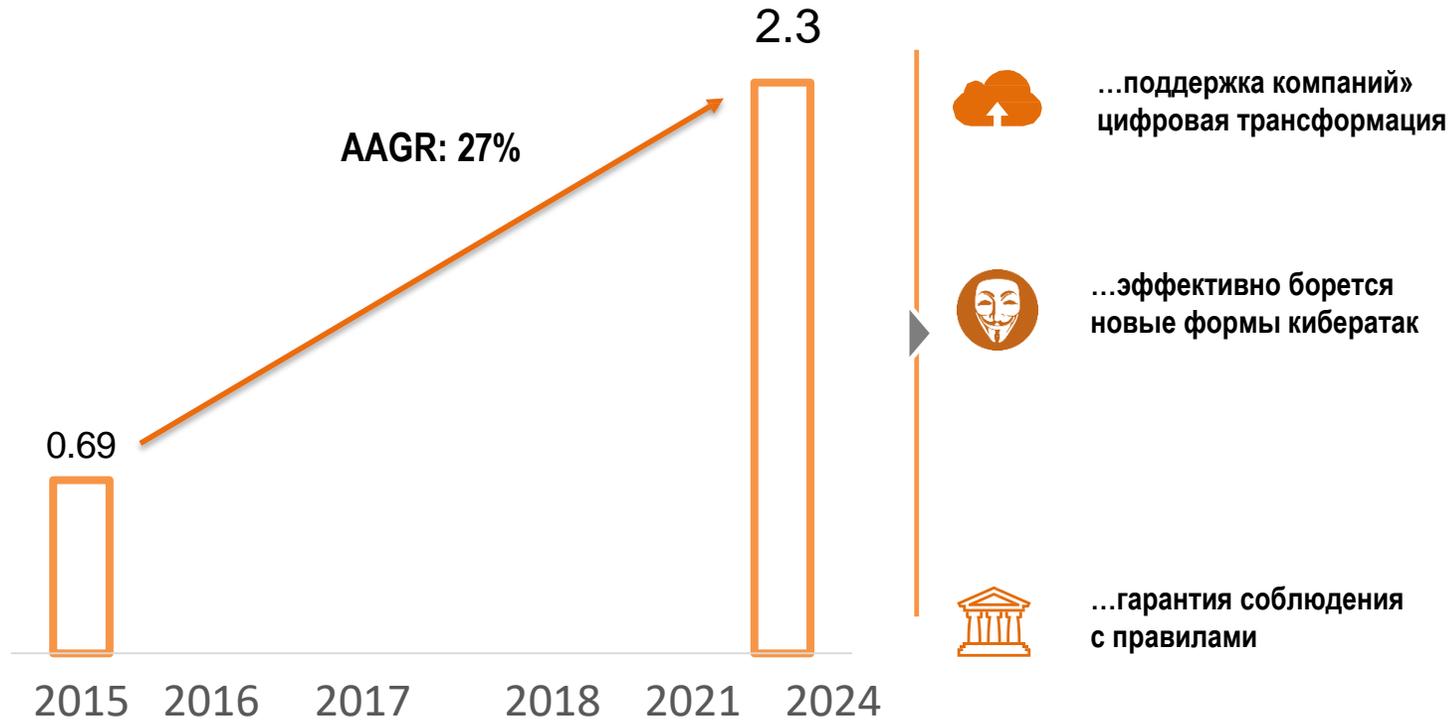




УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМ ДОСТУПОМ: ЦЕЛЕВАЯ РЫНОЧНАЯ СТОИМОСТЬ 2 МЛРД ДОЛЛАРОВ В 2021 ГОДУ

РАМ, решение для...

\$ миллиарды



Источник: Гартнер

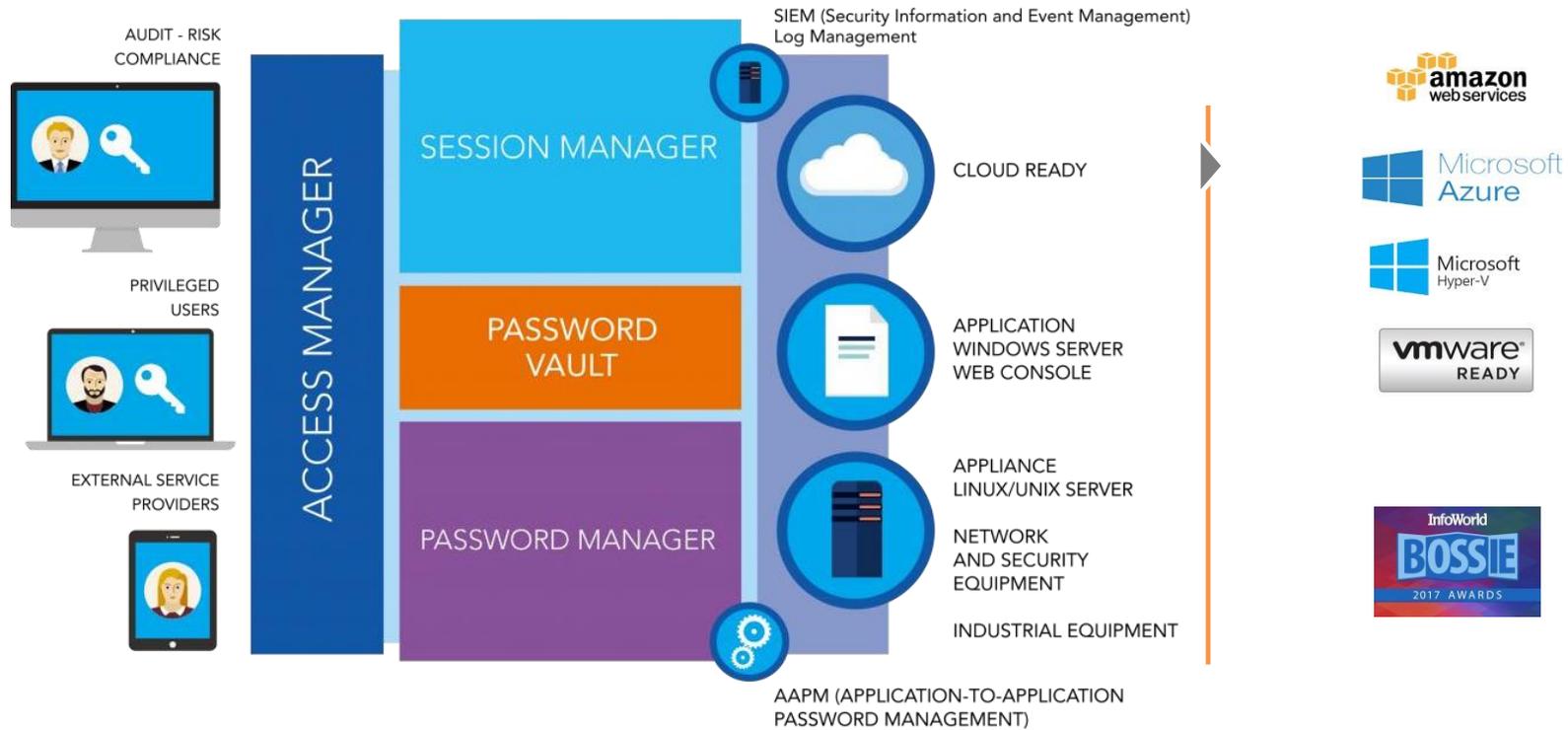


НОВЫЙ ВЫЗОВ: ЗАЩИТА КОРПОРАТИВНОЙ ДЕЯТЕЛЬНОСТИ ЛИЧНОСТЬ, ДОСТУП И ДАННЫЕ





WALLIX BASTION: КОМПЛЕКТ ОБЛАЧНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ



БАСТИОН ВАЛЛИКС: ОСНОВНЫЕ СИЛЬНЫЕ СТОРОНЫ



* Премиальный сертификат безопасности, выданный Французским национальным агентством кибербезопасности (ANSSI)



ОБЛАЧНОЕ РЕШЕНИЕ ДЛЯ СЛУЖБ БЕЗОПАСНОСТИ



DataPeps

Сквозное шифрование/решение E2EE,
обеспечивающее защиту данных во
всех приложениях



РЫНОК ШИФРОВАНИЯ

ОЦЕНИВАЕТСЯ В 2 МЛРД ДОЛЛАРОВ*

Готов к GDPR

- Соответствие GDPR
- Защищает данные даже в случае кибератаки — данные непригодны для использования

Программное обеспечение как

- Технология, приобретенная путем покупки активов MLState
- **Простое развертывание (SDK, плагин Outlook)**
- Две совместные платформы :

FENTEC



ANBLIC



02

2013-2017: Эксплуатационные
характеристики WALLIX PAM

WALLiX
TRACE, AUDIT & TRUST



Централизованный контроль и мониторинг привилегированного доступа к конфиденциальным активам

Хакеры используют привилегированные учетные записи для проникновения и распространения внутри организаций. Управление привилегированным доступом (PAM) является основополагающим активом для смягчения кибератак. WALLIX PAM — ведущее решение PAM, которое обеспечивает надежную безопасность и контроль привилегированного доступа к критически важной ИТ-инфраструктуре. Как решение без агентов, WALLIX PAM может быть легко развернуто от локальной инфраструктуры до частных и публичных облачных инфраструктур. WALLIX PAM также доступен в качестве услуги, предлагающей более экономичный и менее ресурсоемкий вариант.



Особенности и возможности

Уменьшить поверхность атаки

- Автоматически обнаруживайте активы и удаляйте все локальные привилегированные учетные записи
- Настройте правила авторизации для контроля доступа к критически важным системам
- Используйте наименее необходимые привилегии для выполнения задач
- Атрибут привилегий «Just in Time» для авторизованных пользователей

Управляйте секретами

- Безопасное хранение секретов пользователей-людей и не-людей
- Обновляйте пароли с автоматической ротацией на основе времени и/или использования
- Удаляйте пароли с дисков

Контрольные сеансы

- Мониторинг сеансов в режиме реального времени с помощью Session Sharing
- Запись всех сеансов и извлечение связанных метаданных для анализа
- Подача сигналов тревоги после обнаружения вредоносной активности и завершение сеансов

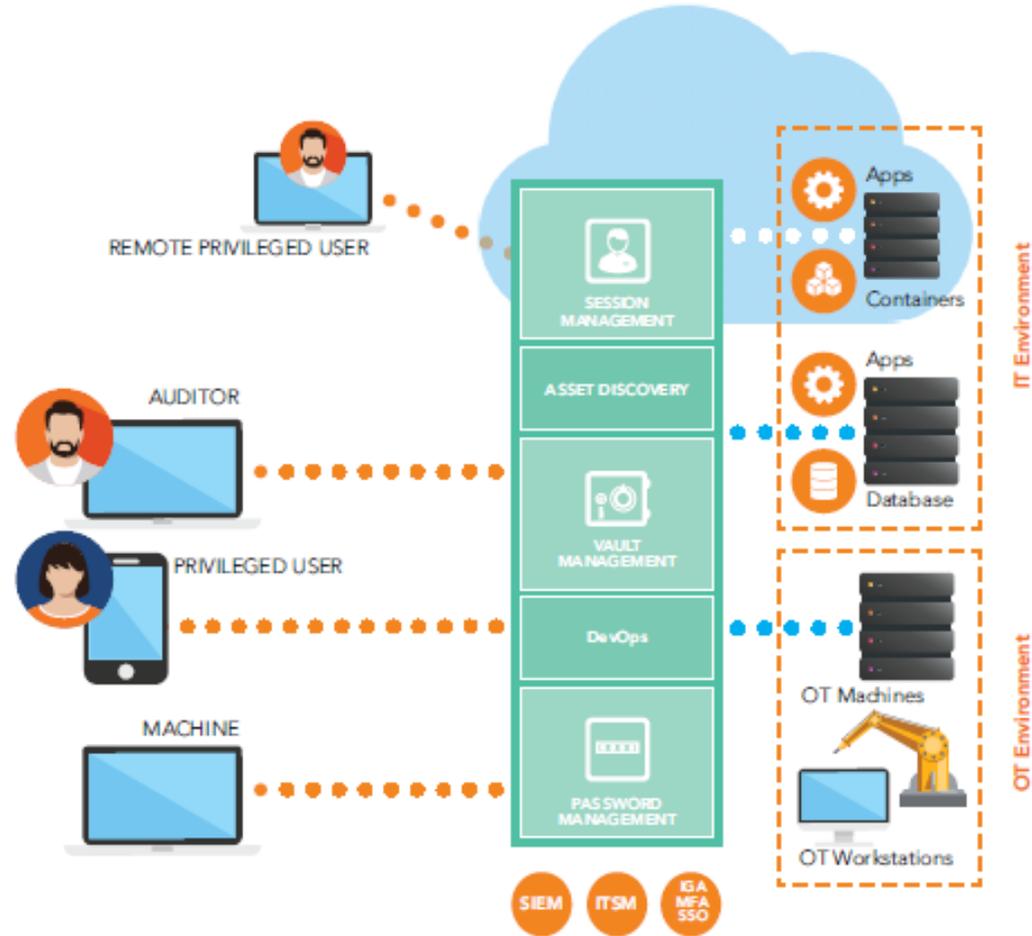
Аудиторская деятельность

- Управляйте KPI с помощью отчетов и панелей мониторинга
- Сопоставляйте подозрительное поведение с интеграцией SIEM
- Быстро развертывайте без прерывания ежедневных рабочих процессов



WALLIX BASTION: КОМПЛЕКТ ОБЛАЧНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Как это работает





WALLIX BASTION: КОМПЛЕКТ ОБЛАЧНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Преимущества



Обезвредить внутренние и внешние угрозы

Централизуйте безопасность
Управление привилегированные пользователи и критические системы.



Развернуть во всех окружающая среда

Беспрпятственно интегрируйтесь в локальные, гибридные и облачный инфраструктуры. WALLIX также предлагает доставку SaaS ПАМ.



Безопасный по мере того, как ты растешь

Масштабируйте свой инфраструктура без всякого риска.



Обеспечить нормативное Согласие

Избегайте штрафов, защита и отслеживание критических доступ к данным.



Безопасный доступ без VPN, без общих паролей и без ущерба для безопасности!

Большинство предприятий полагаются на внешних поставщиков услуг для выполнения удаленных задач, требующих привилегированного доступа к их ИТ- или ОТ-сети. Половина из них не имеет реестра доступа третьих лиц к своей сети, практически не имеет возможности наблюдать и контролировать свой удаленный цифровой доступ. Удаленный доступ WALLIX One помогает удовлетворить новые требования к обеспечению и обеспечению безопасного доступа для внешних поставщиков услуг, которым необходим доступ к критически важной инфраструктуре, управляемой WALLIX One.



Функции

- Полное разделение каталога для внешних поставщиков (точно в срок без добавления удостоверений в корпоративный AD)
- Дальнейшее применение корпоративной политики безопасности
- Делегирование управления владельцам бизнеса
- Самостоятельный сброс пароля (SSPR)
- Никакого VPN для установки и управления, никаких дополнительных билетов для ИТ-персонала.



Полная видимость внешнего удаленного доступа

- Полная видимость внешнего удаленного доступа
- Создание авторизованного доступа в режиме реального времени
- Единый веб-портал со встроенными веб-клиентами RDP и SSH.
- Контроль и прозрачность деятельности третьих лиц
- Соответствие стандартам и рекомендациям Французского национального агентства по безопасности и информационным технологиям (ANSSI), а также бизнес-стандартам, гигиене безопасности.
- Нет общих паролей

03

2013-2017: РАЗВЕРТЫВАНИЕ И
АДМИНИСТРИРОВАНИЕ

WALLiX
TRACE, AUDIT & TRUST



1. Настройка собственного сервера WALLIX Bastion

Будет использоваться образ сервера VMWare, который WALLIX размещает на своем веб-сайте.

а. Скачать Bastion можно по следующему адресу:

<https://cloud.wallix.com/index.php/s/sT2xwYrgyWNX7ke?path=%2FBastion%209.0.2.9>

1 - Выберите «VM VMware», затем загрузите файл «bastion-9.0.2.9-vmware.tbz».

2 - Распакуйте файл «bastion-9.0.2.9-vmware.tbz», чтобы получить локальные образы «bastion-9.0.2.9-vmware.ova» для развертывания.

б) Установите Wallix Bastion из локального образа.

Устройство WALLIX Bastion поставляется в следующей заводской конфигурации:

- IP-адрес eth0: 192.168.10.5
- Шлюз по умолчанию: 192.168.10.1
- Логин и пароль системной учетной записи: "wabadmin"/"SecureWabAdmin"
- Логин и пароль учетной записи администратора WALLIX Bastion: «admin»/«admin»



WALLIX BASTION: УСТАНОВКА/НАСТРОЙКА WALLIX BASTION

Шаги:

1 — Импортируйте файл «bastion-16-vmware.ova» в VMware Workstation

2 - Включите это виртуальное устройство WALLIX Bastion, выберите устройство по умолчанию «WALLIX Bastion 16».

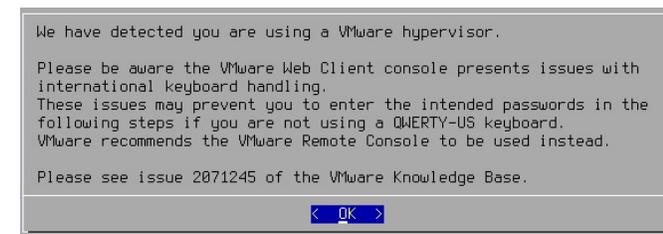
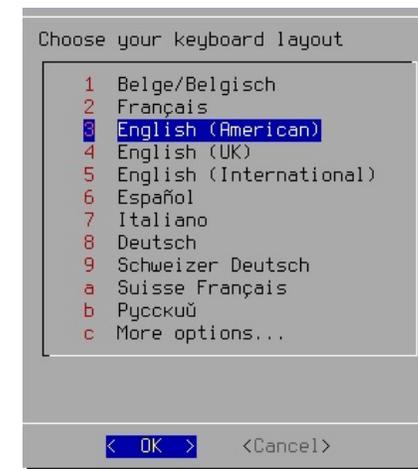
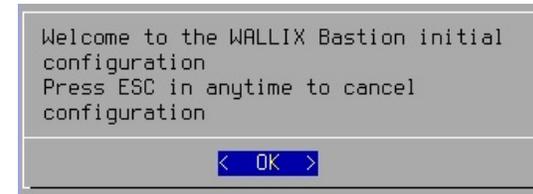


WALLIX BASTION: УСТАНОВКА/НАСТРОЙКА WALLIX BASTION

3 - Отобразится окно начальной конфигурации WALLIX Bastion, как на следующем изображении. Нажмите «ОК», чтобы продолжить.

4 - В настройках клавиатуры выберите «Английский (американский)», нажмите «ОК».

5 — Нажмите «ОК», когда конфигурация Bastion будет обнаружена в VMware.





WALLIX BASTION: УСТАНОВКА/НАСТРОЙКА WALLIX BASTION

6 - Введите пароль по умолчанию для пользователя «wadmin», а именно: SecureWabAdmin

Enter current wadmin password

-

< OK > <Cancel>

7 - Bastion попросит вас создать новый пароль для «wadmin»

Enter new wadmin password

Use up/down arrows (or control/N, control/P) to move between fields.
Use TAB to navigate between controls (fields and buttons)

Type new password : ██████████

Retype new password : ██████████

< OK > <Cancel>

7.1 - Затем отображается сообщение после успешной смены пароля пользователя wadmin.

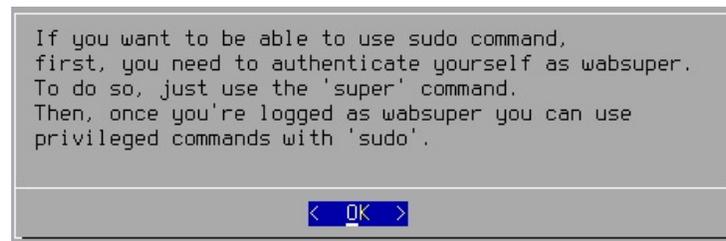
Password changed for user wadmin

< OK >

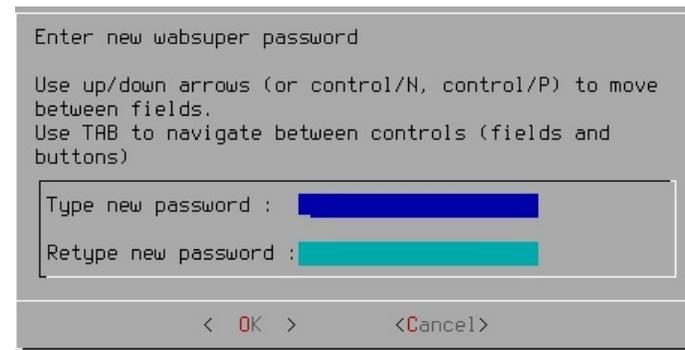


WALLIX BASTION: УСТАНОВКА/НАСТРОЙКА WALLIX BASTION

7.2 - Появится панель уведомлений об использовании команды 'sudo', требующей учетной записи супер-администратора "wabsuper". Нажмите «OK» на этой панели (ниже):



8 - Введите и подтвердите новый пароль wabsuper.



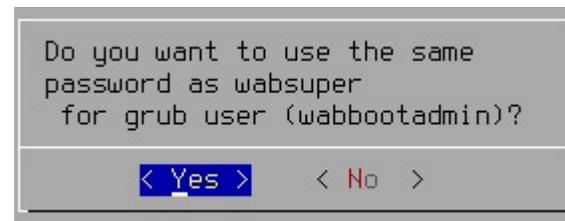
8.1 После успешной смены пароля пользователя wabsuper появится сообщение.



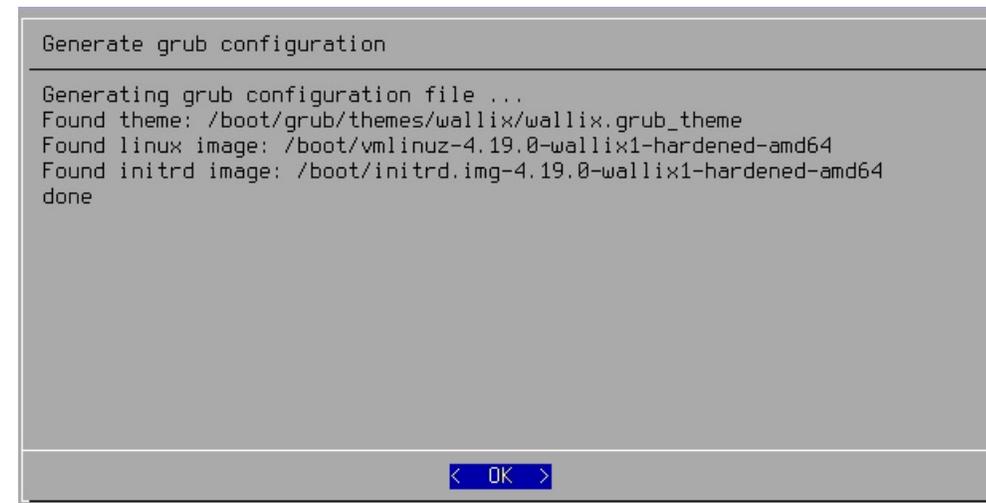


WALLIX BASTION: УСТАНОВКА/НАСТРОЙКА WALLIX BASTION

9 - Нажмите «Да», чтобы использовать тот же пароль пользователя «wabsuper» для системной учетной записи «wabrootadmin».



10 - Bastion инициирует создание файлов конфигурации



11 - Нажмите «ОК», когда Bastion уведомит вас о необходимости нового пользователя: «wabupgrade», функция которого заключается в том, чтобы разрешить безопасное обновление вашей установки Bastion.





WALLIX BASTION: УСТАНОВКА/НАСТРОЙКА WALLIX BASTION

12 - Нажмите «ОК» в сообщении выше, затем на появившейся панели (см. ниже) введите и подтвердите пароль учетной записи wabupgrade.

Enter new wabupgrade password

Use up/down arrows (or control/N, control/P) to move between fields.
Use TAB to navigate between controls (fields and buttons)

Type new password :

Retype new password :

< OK > < Cancel >

12.1 - Установщик отобразит сообщение после успешного создания нового пароля.

Password changed for user wabupgrade

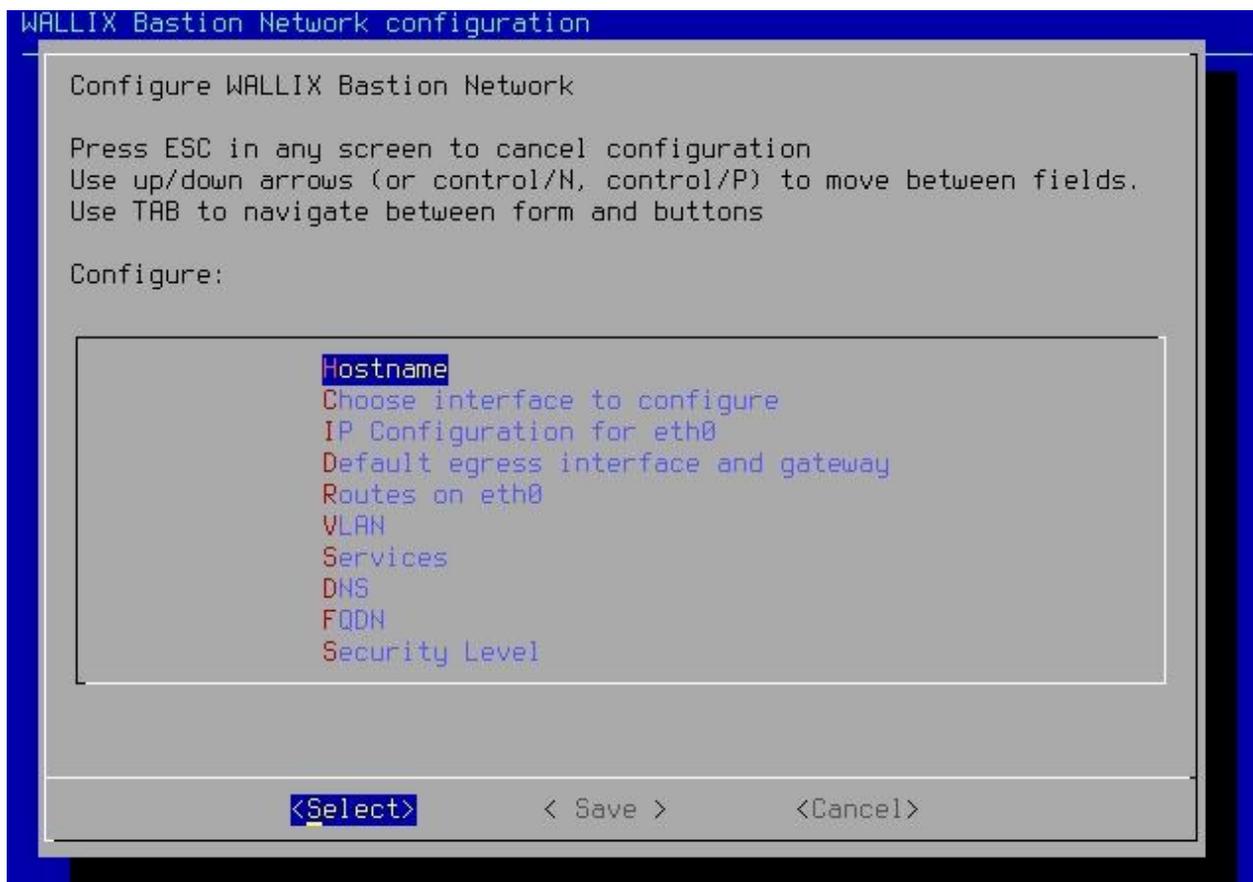
< OK >

13 - Далее вам будет предложено настроить сеть WALLIX Bastion (как на изображении ниже). Нажмите «Да».

Do you want to configure WALLIX Bastion network?

< Yes > < No >

14 — Настройте важную сетевую информацию/элементы, такие как имя хоста, IP-адрес для eth0.

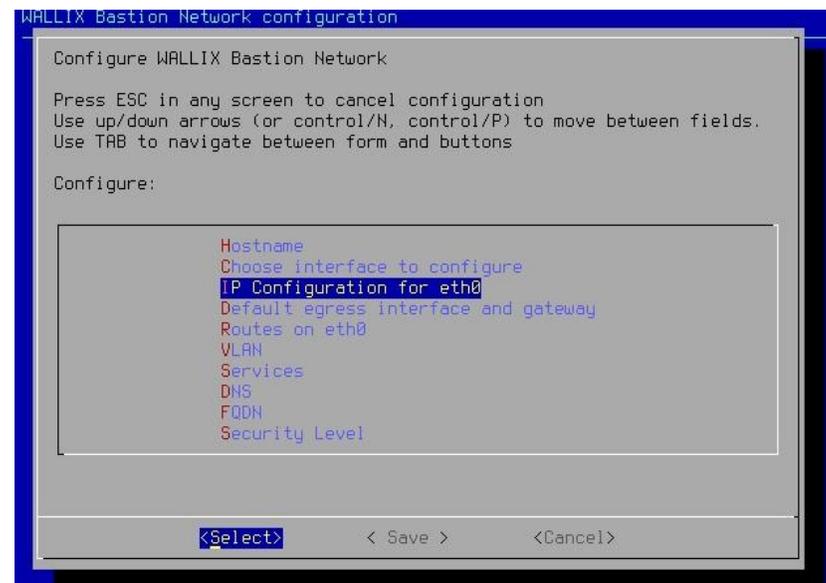


В поле «Имя хоста» введите имя хоста Bastion.

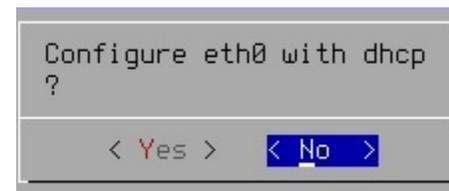




14.1 — Определите IP-адрес для eth0:



14.1.1 Нажмите «Выбрать», затем нажмите «Нет», чтобы отключить DHCP.





WALLIX BASTION: УСТАНОВКА/НАСТРОЙКА WALLIX BASTION

14.1.2 - Измените IP-адрес Bastion по умолчанию на ваш локальный IP-адрес (например, «192.168.1.5 – Шлюз: 192.168.1.1) и нажмите «ОК».

ПРИМЕЧАНИЕ: Это будет IP-адрес Bastion, используемый для входа в веб-интерфейс (GUI) WALLIX Bastion.

15 - После сохранения настроенного сетевого IP-адреса Bastion появится сообщение, как показано на рисунке ниже:

Нажмите «ОК», чтобы закрыть это сообщение и вернуться в меню.

```
static configuration for eth0

Use up/down arrows (or control/N, control/P) to move
between fields.
Use TAB to navigate between controls (fields and
buttons)

Address: 192.168.10.5
Gateway: 192.168.10.1
Netmask: 255.255.255.0

< OK > <Cancel>
```

```
Network
Configuration
updated

< OK >
```



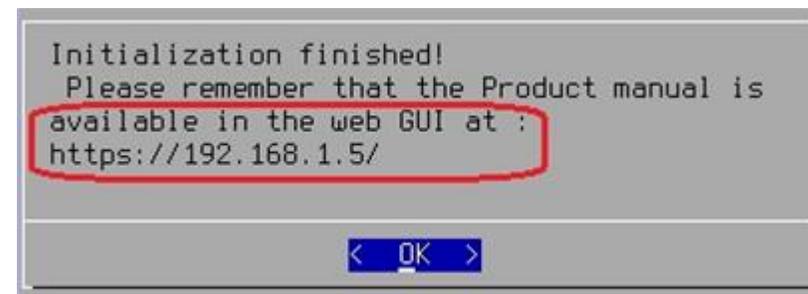
WALLIX BASTION: УСТАНОВКА/НАСТРОЙКА WALLIX BASTION

16 - Введите полное доменное имя (FQDN) Bastion, используя его локальный IP-адрес или доменное имя устройства.

16.1 - Появится сообщение, подтверждающее установку FQDN. Нажмите OK, чтобы закрыть его.

17 - Bastion сгенерирует модули и веб-GUI на основе только что настроенных вами элементов. Появится сообщение с индикатором выполнения, как на изображении ниже:

После завершения генерации модулей указанное выше сообщение с индикатором выполнения закроется, и появится следующий экран, напоминающий вам, где найти руководство по продукту и получить доступ к веб-интерфейсу.



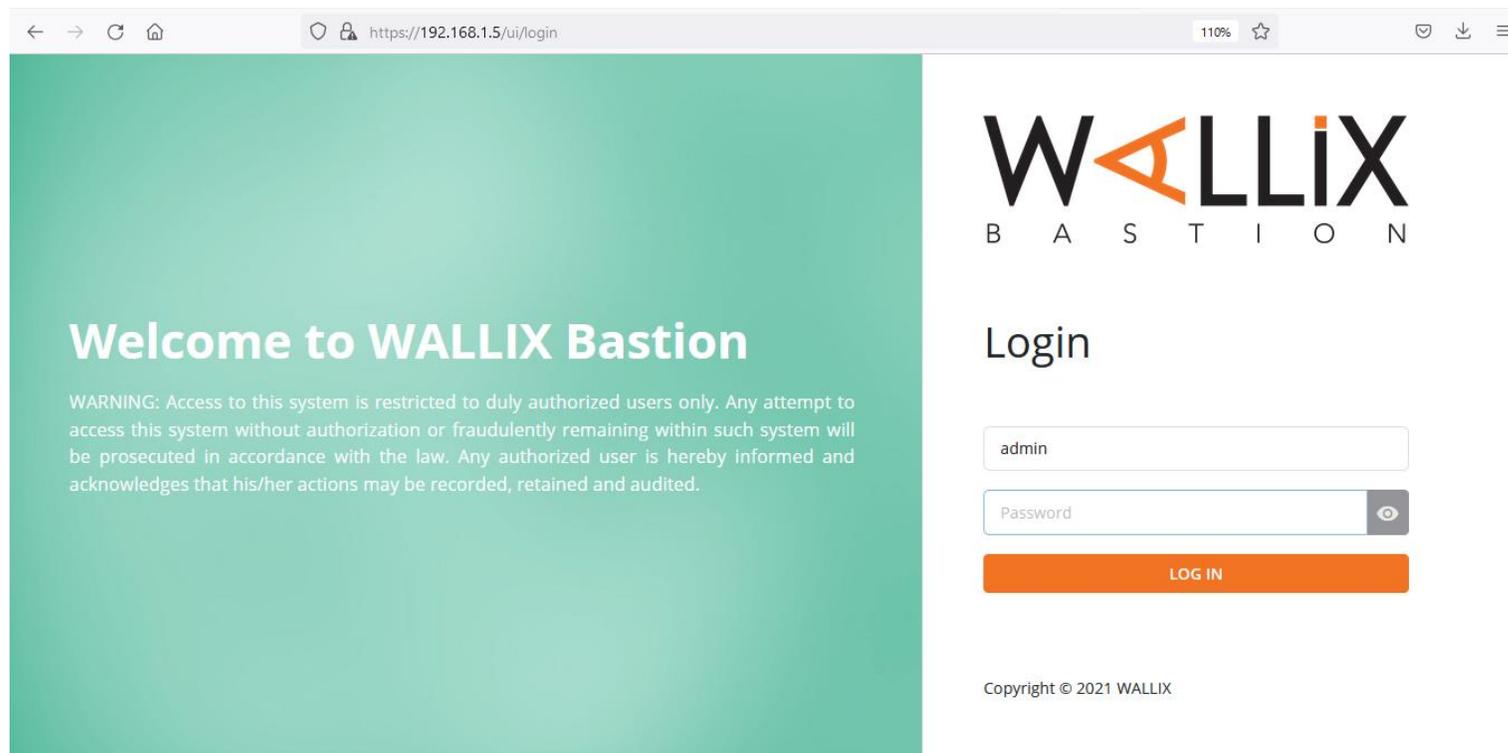


WALLIX BASTION: НАСТРОЙКА АУТЕНТИФИКАЦИИ LDAP С ПОМОЩЬЮ ВЕБ-ИНТЕРФЕЙСА WALLIX BASTION

Начальная конфигурация для пользователя-администратора Bastion:

Откройте панель браузера по адресу <https://192.168.1.5/ui/login>, затем войдите в систему как администратор, используя следующие учетные данные по умолчанию:

- Имя пользователя: админ
- Пароль: админ





WALLIX BASTION: НАСТРОЙКА АУТЕНТИФИКАЦИИ LDAP С ПОМОЩЬЮ ВЕБ-ИНТЕРФЕЙСА WALLIX BASTION

- Введите **парольную фразу** для защиты системы и нажмите «Применить», затем нажмите «Да», чтобы подтвердить использование этой парольной фразы.

The screenshot shows the WALLIX Bastion web interface. The left sidebar contains the WALLIX logo and a 'Configuration' menu with 'Encryption' selected. The main content area is titled 'Configuration > Encryption'. At the top right, the user is logged in as 'admin Product Super Administrator'. A light blue warning box contains the following text: 'The encryption feature of Bastion secures sensitive data (target account passwords, etc.) by using a strong cryptographic algorithm. The algorithm uses a confidential encryption key unique to your Bastion. The definition of a passphrase involves a more complex access to Bastion and raises the protection of your data as no malicious users who do not know the passphrase can access your product. Moreover, at each system reboot, connections using Bastion proxies will not be usable as long as the passphrase is not entered by an administrator in the Web administration interface. After the encryption initialization phase, we highly recommend you to back up Bastion at least once to keep a copy of the encryption key in a safe place. If you do not perform this action and the passphrase is lost, you will no longer be able to access your data on remote storage.' Below the warning box, the 'Initialization' section is titled 'Please enter a passphrase to protect your system.' and includes a note: '(You will be prompted to enter this passphrase to unlock your system after each reboot)'. The form has two input fields: 'Passphrase*' and 'Passphrase confirmation*', each with a toggle for visibility. Below the form, there is an 'OR' separator and a checkbox labeled 'No, I do not want a passphrase protection'. An orange 'Apply' button is at the bottom of the form. The bottom left of the interface shows 'Bastion Version 9.0.2'.

Появится предупреждающее сообщение (см. изображение ниже) о том, что если пароль утерян/забыт, то система будет недоступна, если только ключ шифрования не сохранен в надежном месте.



WALLIX BASTION: НАСТРОЙКА АУТЕНТИФИКАЦИИ LDAP С ПОМОЩЬЮ ВЕБ-ИНТЕРФЕЙСА WALLIX BASTION

После успешного сохранения парольной фразы, созданной администратором Bastion, отобразится следующий экран:

The screenshot displays the Wallix Bastion web interface. On the left is a vertical navigation menu with the following items: Dashboards, My authorizations, Audit, Users, Targets, Authorizations, Session management, Password management, Configuration, System, and Import/Export. At the bottom of the menu, it says "Bastion Version 9.0.2".

The main content area features a "Welcome" message. It states: "Your **Login** and your **User name** appear at the top right of the page. You can perform the following actions from this page:"

- Click on to open a contextual menu from which you can access the **My Preferences** page to select your language or **Logout**.
- Click on to access the online **Help**.
- Click on to display the **Notifications** window.
- Click on the left menu entries to access the features. This menu can be collapsed.

Below the welcome message is a button labeled "Do not show again".

At the bottom of the main content area, there are four large, colored buttons for navigation:

- List Devices** (teal button)
- List Applications** (blue button)
- List Accounts** (orange button)
- List Users** (dark grey button)

The top right corner of the interface shows a home icon, a notification bell, a help icon, and a user profile for "admin Product Super Administrator".



WALLIX BASTION: НАСТРОЙТЕ СЕРВЕР SDIDP LDAP В WALLIX BASTION

1 - Перейдите в раздел Конфигурация -> Внешние аутентификации и добавьте новую аутентификацию LDAP для нашего сервера LDAP (например, «ldapservers»), используя информацию о сервере SDIdP ниже:

- Сервер IdP: 192.168.1.20
- LDAP-порт 389
- Метод привязки: используйте «простой» или «анонимный»
- Включите опцию «Active Directory» (ПРИМЕЧАНИЕ: в настоящее время пользователь MagicEndpoint не будет работать при отключении этой опции)

The screenshot shows the Wallix Bastion web interface for configuring external authentication. The browser address bar shows the URL: `https://192.168.1.5/ui/configuration/external-authentications`. The left sidebar contains a navigation menu with the following items: Dashboards, My authorizations, Audit, Users, Targets, Authorizations, Session management, Password management, Configuration (highlighted), Configuration options, Time frames, External authentications (highlighted), LDAP/AD domains, and Notifications. The main content area is titled "Configuration" and features an "Edit this authentication" button. The configuration details for the selected authentication are as follows:

- Authentication type: LDAP
- Authentication name: ldapservers
- Server: 192.168.1.20
- Port: 389
- Timeout (s): 20.0
- Base DN: CN=New2K19
- Login attribute: sAMAccountName
- User name attribute: sAMAccountName
- Bind method: simple
- Active Directory:
- Encryption: None
- User: hp
- Description: --

At the bottom, there is a section for "Two-Factor Authentication (2FA)" with a checkbox for "Use primary domain name" which is currently unchecked.



WALLIX BASTION: НАСТРОЙТЕ СЕРВЕР SDIDP LDAP В WALLIX BASTION

Проверьте соединение LDAP, чтобы убедиться, что Bastion может успешно получить доступ к серверу SDIdP, как показано на рисунке ниже:

The screenshot displays the Wallix Bastion configuration interface. On the left is a navigation menu with items: Dashboards, My authorizations, Audit, Users, Targets, Authorizations, Session management, Password management, and Configuration (highlighted). The main area is titled 'Configuration' and shows 'Edit external authentication' settings:

- Authentication type *: LDAP
- Authentication name *: ldapserver
- Server *: 192.168.1.20
- Port *: 389
- Timeout (s) *: 20.0
- Active Directory:
- Encryption: None StartTLS SSL
- Base DN (dc=...)*: CN=New2K19
- Login attribute *: SA
- User name attribute *: SA
- Bind method: s
- User *: h
- Password *: •••••
- Description:

A white dialog box is overlaid on the configuration, displaying a globe icon, the IP address '192.168.1.5', and the message 'LDAP connection succeeded.' with an 'OK' button.



WALLIX BASTION: НАСТРОЙТЕ СЕРВЕР SDIDP LDAP В WALLIX BASTION

Создайте домен LDAP/AD:

- 1 - В меню «Конфигурация > Домены LDAP/AD» нажмите «Добавить домен».
- 2 - В разделе «Доступный каталог» выберите указанное выше имя внешней аутентификации LDAP (например, «ldapsver») и используйте настройки по умолчанию для атрибутов пользователя / параметров X509.

The screenshot shows the 'Add LDAP/AD domain' configuration page in the Wallix Bastion interface. The page is titled 'Add LDAP/AD domain' and is part of the 'Configuration' section. The user is logged in as 'admin Product Super Administrator'. The form includes the following fields and options:

- Bastion domain name ***: BastionDN
- Description**: (empty text area)
- Default domain**: (checked)
- LDAP/AD domain name ***: New2K19
- Directory ***: A selection interface with two columns: 'Available Directories' and 'Selected Directories'. The 'Available Directories' column contains 'Active Direc'. The 'Selected Directories' column contains 'ldapsver'. There are 'Select all' and 'Delete all' buttons at the bottom of each column.



WALLIX BASTION: НАСТРОЙТЕ СЕРВЕР SDIDP LDAP В WALLIX BASTION

🏠 > Configuration🔔 ? 👤 admin Product Super Admin

- Password management
- Configuration**
- Configuration options
- Time frames
- External authentications
- LDAP/AD domains**
- Notifications
- Local password policy
- Connection messages
- X509 configuration
- API keys
- License

User attributes

Group attribute:

Display name attribute:

Email attribute:

Default email domain *:

Language attribute:

Default language *:

X509 options

X509 authentication:

If this option is selected, users can only authenticate on the domain through X509 authentication method.

Matching condition:

Condition to match a domain with the X509 certificate
E.g.: `${issuer_o}--Organisation || ${issuer_cn}--CommonName && ${subject_ou}=OrganisationalUnit`
Operator "&&" (i.e. AND) has precedence over operator "||" (i.e. OR).
Values are case sensitive whereas variables are not.
Available variables: `issuer{c_l_o_ou_sn_st_email}`, `subject{c_cn_l_o_ou_sn_st_email_uid}`, `mail{0..N}`, `msupn{0..N}`, `dns{0..N}`, `username`

Search filter:

LDAP/AD search filter
Expressed in LDAP filter syntax. Any variables listed below field "Matching condition" can be used.

Domain name to match SAN Email:

Only for X509 authentication with an AD server



WALLIX BASTION: НАСТРОЙТЕ СЕРВЕР SDIDP LDAP В WALLIX BASTION

Создайте группу пользователей:

- В меню Пользователи -> Группы нажмите «Добавить группу» (например, «Группы FE»).
- Добавьте доменное имя Bastion «BastionDN» в LDAP/Domain выше (не добавляйте пользователей Bastion в эту группу)

The screenshot displays the WALLIX Bastion web interface for configuring a user group. The left sidebar shows the navigation menu with 'Groups' selected. The main content area is titled 'Users > Groups' and shows a form for creating a new group named 'FE Groups'. The 'Description' field is empty. The 'Time frames' dropdown is set to 'alltime'. Below, there are two columns: 'Available Users' and 'Selected Users'. The 'Available Users' column contains the user 'admin'. At the bottom, there are fields for 'LDAP authentication mapping', 'Profile' (set to 'USER'), 'LDAP/AD domain name' (set to 'BastionDN'), and 'LDAP group'. The 'Action' dropdown is set to 'kill' and the 'Subprotocol' dropdown is set to 'SSH_SHELL_SESSION / X11_SESSION'. The 'Apply' button is highlighted in orange.

Спасибо за внимание!