



















Отчет_аудит_10.1.1.3

Легенда

-  нет уязвимостей
-  доступна информация
-  низкий уровень
-  средний уровень (подозрение)
-  средний уровень
-  высокий уровень (подозрение)
-  высокий уровень
-  критический уровень (подозрение)
-  критический уровень
-  заблокированный сервис
-  недоступный сервис
-  неидентифицированный сервис
-  необработанный сервис
-  узел не проверялся
-  узел проверен не полностью (снят с ошибкой)
-  узел проверен не полностью (прервано пользователем)
-  ограничение лицензии
-  ограничение прав

Описание вектора CVSS, версия 2

A:C	при успешной эксплуатации злоумышленник может сделать систему полностью недоступной
A:N	эксплуатация уязвимости не влияет на доступность системы
A:P	эксплуатация уязвимости ведет к сбоям в доступности системы или к уменьшению производительности
AC:H	для эксплуатации уязвимости нужны особые условия, или уязвимая конфигурация редко встречается на практике
AC:L	для эксплуатации уязвимости не требуются особые условия
AC:M	для эксплуатации уязвимости нужна дополнительная информация или нестандартная конфигурация уязвимого ПО
Au:M	для эксплуатации уязвимости злоумышленник должен несколько (два и более) раз пройти аутентификацию
Au:N	для эксплуатации уязвимости проходить аутентификацию не требуется
Au:NR	для эксплуатации уязвимости проходить аутентификацию не требуется
Au:S	для эксплуатации уязвимости злоумышленник должен пройти аутентификацию в системе
AV:A	для успешной эксплуатации уязвимости злоумышленник должен иметь доступ к соседней сети
AV:L	для успешной эксплуатации уязвимости злоумышленник должен иметь физический доступ к системе или локальную учетную запись
AV:N	данная уязвимость может эксплуатироваться удаленно
AV:R	данная уязвимость может эксплуатироваться удаленно
B:N	веса угроз одинаковы
C:C	эксплуатация уязвимости влечет полное разглашение конфиденциальных данных
C:N	эксплуатация уязвимости не затрагивает конфиденциальные данные системы
C:P	эксплуатация уязвимости влечет существенное разглашение конфиденциальных данных
E:F	для данной уязвимости доступен эксплойт, который может быть применен в большинстве ситуаций
E:H	данную уязвимость можно эксплуатировать с помощью легко переносимого, автономного кода, или эксплойт не нужен
E:ND	данная метрика не влияет на оценку
E:P	доступен "Proof of Concept" код (эксплойт, описывающий концепцию эксплуатации), или существует стратегия атаки, которая неприменима в большинстве систем.
E:POC	доступен "Proof of Concept" код (эксплойт, описывающий концепцию эксплуатации), или существует стратегия атаки, которая неприменима в большинстве систем. Для использования этого эксплойта требуется внести в него значительные изменения, чтобы требует соответствующих навыков от злоумышленника.
E:U	эксплуатация уязвимости возможна теоретически
I:C	эксплуатация уязвимости влечет полное нарушение целостности системы
I:N	эксплуатация уязвимости не затрагивает целостность системы
I:P	эксплуатация уязвимости ведет к частичному нарушению целостности системы
RC:C	данная уязвимость подтверждена производителем или автором технологии эксплуатации уязвимости
RC:ND	данная метрика не влияет на оценку
RC:UC	достоверность наличия данной уязвимости не подтверждена
RC:UR	сообщения о данной уязвимости предоставлены несколькими неофициальными источниками
RL:ND	данная метрика не влияет на оценку
RL:O	доступно официальное обновление или исправление от производителя
RL:OF	для данной уязвимости доступно официальное обновление или исправление от производителя
RL:T	для данной уязвимости доступно официальное временное обновление
RL:TF	для данной уязвимости доступно официальное временное обновление
RL:U	для данной уязвимости обновление или исправление недоступно или не может быть применено
RL:W	для данной уязвимости доступно неофициальное решение, которое предоставлено третьей стороной


Описание вектора CVSS, версия 3

A:H	Полная потеря доступности. Злоумышленник способен вызвать полный отказ в доступе к ресурсам атакуемого компонента; этот отказ является либо устойчивым (длится, пока злоумышленник продолжает атаку), либо постоянным (сохраняется даже после завершения атаки).
------------	--

A:L	Происходит снижение производительности или перебои в доступности ресурса. Хотя возможна многократная эксплуатация уязвимости, злоумышленник не способен вызвать полный отказ в обслуживании законных пользователей.
A:N	Воздействие на доступность атакуемого компонента отсутствует.
AC:H	Успех атаки зависит от условий, находящихся вне контроля злоумышленника.
AC:L	Не существует специальных условий доступа и особых обстоятельств. Злоумышленник может рассчитывать на успешное повторение атаки в отношении уязвимого компонента.
AV:A	Уязвимый компонент также привязан к сетевому стеку, но атака ограничена той же совместно используемой физической (например, Bluetooth, IEEE 802.11) или логической (например, локальной IP-подсетью) сетью и не может быть произведена через границы уровня 3 модели OSI (например, маршрутизатор).
AV:L	Уязвимый компонент не привязан к сетевому стеку, а маршрут проникновения злоумышленника пролегает через возможности чтения/записи/выполнения.
AV:N	Уязвимый компонент привязан к сетевому стеку, а маршрут проникновения злоумышленника пролегает через уровень 3 (сетевой уровень) модели взаимосвязи открытых систем (OSI).
AV:P	Уязвимость может эксплуатироваться при физическом доступе, и злоумышленнику для достижения своей цели необходимо физическое взаимодействие с уязвимым компонентом.
C:H	Полная потеря конфиденциальности, приводящая к тому, что все ресурсы атакуемого компонента становятся доступными злоумышленнику.
C:L	Возможен доступ к некоторой информации для ограниченного пользования, но злоумышленник не имеет контроля над тем, какую именно информацию он получит, или масштабы потерь невелики либо их последствия не носят массового характера.
C:N	Потеря конфиденциальности в атакуемом компоненте нет.
E:F	Доступен функциональный код эксплойта, применимый в большинстве ситуаций, где существует уязвимость.
E:H	Существующий функциональный автономный код или эксплойт не требуется (запуск производится вручную), и детали широко известны. Код эксплойта работает в любой ситуации или его активная доставка осуществляется автономным агентом (например, червем или вирусом).
E:P	Доступен код эксплойта, доказывающий правильность концепции, или существует демонстрация атаки, неприменимая в большинстве систем.
E:U	Код эксплойта не доступен или эксплуатация возможна лишь теоретически.
E:X	Присвоение этого значения показателю не влияет на оценку.
I:H	Полная потеря целостности или защиты.
I:L	Возможно изменение данных, но злоумышленник не имеет контроля над последствиями изменения или масштабы изменения ограничены.
I:N	Потеря целостности в атакуемом компоненте нет.
PR:H	Злоумышленник должен быть авторизован и располагать привилегиями, предоставляющими значительный (например, административный) контроль над уязвимым компонентом, который может затрагивать настройки и файлы в масштабе всего компонента.
PR:L	Злоумышленник должен быть авторизован и располагать ограниченными привилегиями, предоставляющими базовые пользовательские возможности, которые в нормальном случае распространяются только на настройки и файлы самого пользователя.
PR:N	Злоумышленник может не иметь авторизации перед атакой и, соответственно, не нуждается в доступе к каким-либо настройкам или файлам для ее осуществления.
RC:C	Имеются подробные сообщения или уязвимость функционально воспроизводима (например, существуют функциональные эксплойты).
RC:R	Опубликованы существенные подробности, но исследователи либо не уверены до конца в первопричине, либо не имеют доступа к исходному коду, чтобы окончательно подтвердить все взаимодействия, которые могут привести к рассматриваемому результату.
RC:U	Имеются сообщения о фактах воздействия на системы, указывающие на существование уязвимости.
RC:X	Присвоение этого значения показателю не влияет на оценку.
RL:O	Доступно полноценное решение от разработчика, который либо выпустил официальное исправление, либо предоставил обновление.
RL:T	Доступно официальное временное исправление. Например, разработчик выпустил оперативное исправление или временное программное средство либо опубликовал обходной прием.
RL:U	Решение либо недоступно, либо его невозможно применить.
RL:W	Доступно неофициальное решение, которое предоставлено третьей стороной.
RL:X	Присвоение этого значения показателю не влияет на оценку.
S:C	Эксплуатируемая уязвимость может воздействовать на ресурсы за рамками привилегий, предусмотренных уязвимым компонентом. В этом случае уязвимый и атакуемый компоненты различаются.
S:U	Эксплуатируемая уязвимость может воздействовать только на ресурсы под контролем того же субъекта авторизации. В этом случае уязвимый и атакуемый компоненты совпадают.
UI:N	Существует возможность эксплуатации уязвимой системы без взаимодействия с каким-либо пользователем.
UI:R	Для успешной эксплуатации этой уязвимости требуются те или иные действия со стороны пользователя.

Параметры отчета	
Тип отчета	Информация
Тип данных	Уязвимость Audit
Исходные данные	По скану
Состав описания уязвимостей	Все
Количество строк в рейтинге:	10
Достоверность результатов	Любая (все результаты)
Включить уязвимости, помеченные как ложное срабатывание	Нет
Ограничение количества строк, отображаемых в результатах	50
Разбивать отчет на части	Не разбивать отчет
Содержание отчета	Легенда; Проверенные узлы; Уязвимые службы/ПО; Все службы/ПО; Уязвимость узлов; Состояние транспортных

Данные, включенные в отчет		
задача	узлов	сканов
Задача_10.1.1.3_аудит	1	1
Итого:	1	1

	Статистика	
	Статистика уязвимостей	
Нет данных		
	Уязвимость объектов	
Нет данных		
	Распределение уровней опасности	
Нет данных		



Проверенные узлы



узел	начало	конец	время	интегральная уязвимость
10.1.1.3	30.07.2025 15:07:27	30.07.2025 15:11:45	00:04:18	0

Интегральная уязвимость определяется по формуле: $N7 * 7 + N5 * 5 + N3 * 3 + N6 + N4 + N2 + N1$, где:

N7 - количество уязвимостей критического уровня

N6 - количество подозрений на уязвимость критического уровня

N5 - количество уязвимостей высокого уровня

N4 - количество подозрений на уязвимость высокого уровня

N3 - количество уязвимостей среднего уровня

N2 - количество подозрений на уязвимость среднего уровня

N1 - количество уязвимостей низкого уровня



Рейтинг уязвимых узлов



Нет данных



Рейтинг уязвимых служб/ПО



Нет данных













































Рейтинг уязвимостей



Уязвимость	CVE	Количество
------------	-----	------------

i	Перечень уязвимых служб/ПО	⬇
	Нет данных	

i	Перечень неуязвимых служб/ПО		↓
	IP-адрес 10.1.1.3	Имя из задачи 10.1.1.3	Служб и ПО: 435
<div data-bbox="309 244 539 2123"> <ul style="list-style-type: none">  Hardware Information  MySQL Server  Network Configuration  Operating System  Linux Kernel  adwaita-cursor-theme  adwaita-icon-theme  Apache HTTP Server  apr  apr-devel  apr-util  apr-util-devel  aspell  atk  at-spi2-atk  at-spi2-core  avahi-glib  avahi-libs  bash  bind-libs  bind-license  bind-utils  binutils  blktrace  bluez  bluez-libs  bpftool  bzip2  bzip2-libs  ca-certificates  cairo  cairo-gobject  c-ares  chrony  colord-libs  coreutils  cpio  cryptsetup  cryptsetup-libs  cups-libs  curl </div>			

- cyrus-sasl
- cyrus-sasl-devel
- cyrus-sasl-gssapi
- cyrus-sasl-lib
- cyrus-sasl-plain
- dbus
- dbus-broker
- dbus-common
- dbus-libs
- dbus-tools
- dconf
- dnf
- dnf-data
- dnf-plugins-core
- dracut
- dracut-network
- e2fsprogs
- e2fsprogs-libs
- ed
- elfutils-default-yama-scope
- elfutils-libelf
- elfutils-libs
- emacs-filessystem
- exempi
- exiv2
- exiv2-libs
- expat
- expat-devel
- expect
- file
- file-libs
- firewallld
- firewallld-filessystem
- flac-libs
- flatpak
- flatpak-selinux
- flatpak-session-helper
- fontconfig
- freetype
- fri bidi
- fuse
- fuse-libs
- gd
- gdk-pixbuf2
- gdk-pixbuf2-modules

- geoclue2
- gettext
- gettext-libs
- giflib
- git-core
- glib2
- glibc
- glibc-common
- glibc-langpack-en
- glib-networking
- gnupg2
- gnutls
- gobject-introspection
- graphite2
- graphviz
- grep
- grub2-common
- grub2-pc
- grub2-pc-modules
- grub2-tools
- grub2-tools-minimal
- gsettings-desktop-schemas
- gstreamer1
- gstreamer1-plugins-base
- gtk2
- gtk3
- gtk-update-icon-cache
- gzip
- harfbuzz
- httpd
- httpd-core
- httpd-devel
- httpd-filesystem
- httpd-tools
- info
- initscripts
- jbig2dec-libs
- json-c
- json-glib
- kernel-uek
- kexec-tools
- kpartx
- krb5-libs
- krb5-pkinit
- krb5-workstation

- libappstream-glib
- libarchive
- libatomic
- libbasicobjects
- libblkid
- libcanberra
- libcanberra-gtk2
- libcanberra-gtk3
- libcap
- libcollection
- libcom_err
- libcomps
- libcurl
- libdb
- libdb-devel
- libdhash
- libdnf
- libdrm
- libepoxy
- libexif
- libfontenc
- libgcc
- libgcrypt
- libgexiv2
- libglvnd
- libglvnd-egl
- libglvnd-glx
- libgomp
- libgs
- libgsf
- libgxps
- libibverbs
- libICE
- libicu
- libini_config
- libipa_hbac
- libjpeg-turbo
- libkadm5
- libksba
- libldb
- libmount
- libmspack
- libndp
- libnghttp2
- libnl3

- libnl3-cli
- libosinfo
- libpath_utils
- libpcap
- libpng
- libproxy
- libref_array
- librelp
- librepo
- libreport-filessystem
- librsvg2
- librsvg2-tools
- libseccomp
- libsecret
- libsepol
- libsmbclient
- libsndfile
- libsolv
- libsoup
- libss
- libssh
- libssh-config
- libsss_certmap
- libsss_idmap
- libsss_nss_idmap
- libsss_sudo
- libtalloc
- libtasn1
- libtasn1-devel
- libtasn1-tools
- libtdb
- libtevent
- libtiff
- libtirpc
- libtool-ltdl
- libuser
- libuuid
- libuv
- libvorbis
- libwayland-client
- libwayland-cursor
- libwayland-egl
- libwayland-server
- libwbclient
- libwebp

- libX11
- libX11-common
- libX11-xcb
- libXaw
- libxcb
- libXcursor
- libXfixes
- libXi
- libxkbcommon
- libxml2
- libXpm
- libXrandr
- libXrender
- libxslt
- libXt
- libXtst
- libXv
- libXxf86vm
- libyaml
- Linux
- logrotate
- lua-libs
- lz4-libs
- lzo
- mariadb-connector-c
- memcached
- mercurial
- mesa-dri-drivers
- mesa-filesystem
- mesa-libEGL
- mesa-libgbm
- mesa-libGL
- mesa-libglapi
- microcode_ctl
- mod_lua
- mod_ssl
- ModemManager-glib
- ncurses
- ncurses-base
- ncurses-libs
- nettle
- NetworkManager
- NetworkManager-libnm
- NetworkManager-team
- NetworkManager-tui

- newt
- nodejs
- nspr
- nss
- nss-softokn
- nss-softokn-freebl
- nss-sysinit
- nss-util
- oniguruma
- openjpeg2
- openldap
- openldap-devel
- openssh
- openssh-clients
- openssh-server
- openssl
- openssl-devel
- openssl-lib
- open-vm-tools
- oraclelinux-release
- oracle-logos
- orc
- osinfo-db
- osinfo-db-tools
- p11-kit
- p11-kit-server
- p11-kit-trust
- PackageKit
- PackageKit-glib
- pam
- pam_krb5
- pango
- pcre
- pcre2
- pcre2-syntax
- perl-Compress-Raw-Bzip2
- perl-Compress-Raw-Zlib
- perl-Digest-SHA
- perl-Errno
- perl-interpreter
- perl-IO
- perl-libs
- perl-Math-Complex
- perl-Net-DNS
- perl-parent

- perl-Pod-Escapes
- perl-Pod-Html
- perl-Pod-Simple
- php
- php-cli
- php-common
- php-gd
- php-ldap
- php-mbstring
- php-mysqlnd
- php-opcache
- php-pdo
- php-pear
- php-process
- php-pspell
- php-xml
- pipewire
- pipewire-libs
- pixman
- plymouth
- plymouth-core-libs
- plymouth-scripts
- policycoreutils
- polkit
- polkit-libs
- poppler
- poppler-glib
- poppler-utils
- popt
- procps-ng
- python3
- python3-cryptography
- python3-dnf
- python3-dnf-plugins-core
- python3-gobject-base
- python3-hawkey
- python3-libcomps
- python3-libdnf
- python3-librepo
- python3-libs
- python3-libxml2
- python3-perf
- python3-pip
- python3-pip-wheel
- python3-psutil

- python3-rpm
- python3-setuptools
- python3-setuptools-wheel
- python3-urllib3
- python-unversioned-command
- quota
- realmd
- redis
- rpm
- rpm-build-libs
- rpm-libs
- rpm-plugin-selinux
- rpm-plugin-systemd-inhibit
- rsync
- rsyslog
- rsyslog-gnutls
- rsyslog-gssapi
- rsyslog-logrotate
- rsyslog-relp
- rtkit
- samba-client-libs
- samba-common
- samba-common-libs
- selinux-policy
- selinux-policy-targeted
- setroubleshoot-plugins
- setroubleshoot-server
- setup
- shadow-utils
- shared-mime-info
- sos
- sqlite
- sqlite-devel
- sqlite-libs
- sssd
- sssd-ad
- sssd-client
- sssd-common
- sssd-common-pac
- sssd-ipa
- sssd-kcm
- sssd-krb5
- sssd-krb5-common
- sssd-ldap
- sssd-proxy

- stunnel
- sudo
- systemd
- systemd-libs
- systemd-pam
- systemd-rpm-macros
- systemd-udev
- tar
- tcl
- tcpdump
- tk
- totem-pl-parser
- tracker
- unzip
- upower
- util-linux
- vim-common
- vim-enhanced
- vim-filesystem
- vim-minimal
- webkit2gtk3-jsc
- webrtc-audio-processing
- wget
- xdg-desktop-portal
- xdg-desktop-portal-gtk
- xfsprogs
- xkeyboard-config
- xmlsec1
- xmlsec1-openssl
- xz
- xz-libs
- yum
- yum-utils
- zlib



Имя из задачи
10.1.1.3

Уязвимых
служб/ПО:

Транспорты: LDAP MML MongoDB NotesRPC ODBC DB2 ODBC MSSQL ODBC MySQL ODBC Oracle ODBC PostgreSQL
ODBC Sybase ODBC Teradata ODBC Tibero RPC Filesystem RPC Registry RPC Remote Engine SAP GUI SAP HANA SAP
HTTP SAPRFC SSH1 SSH2 TELNET VMWARE vCenter VMWARE WMI FILESYSTEM WMI API REGISTRY WMI XEN XENRPC [подробнее](#) >>

Распределение уровней опасности



Завершение сканирования:	30.07.2025 15:11:45
Задача:	Задача_10.1.1.3_аудит
Версия сканера:	40948
Имя сканера:	Default Scanner on SECURITY-
	HPLAPT
сканирования:	00:04:18
сканирования:	30.07.2025 15:07:27
Дост оверность сканирования:	высокая

■ Hardware Information

Количество: **16**

Номер процессора: 0

Информация о устройстве

Параметр	Значение
Model name:	Intel(R) Xeon(R) Gold 6248R CPU @ 3.00GHz
Vendor:	GenuineIntel
Frequency:	2992 MHz
Cache:	36608 KB
Architecture:	x86_64
CPUID level:	22
CPU family:	6
Model:	85
FPU:	yes
FPU exception:	yes
Stepping:	0
Flags:	fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid avx512f avx512dq rdseed adx smap clflushopt clwb avx512cd avx512bw avx512vl xsaveopt xsavec xsaves arat pku ospke md_clear flush_l1d arch_capabilities

Номер процессора: 1

Информация о устройстве

Параметр	Значение
Model name:	Intel(R) Xeon(R) Gold 6248R CPU @ 3.00GHz
Vendor:	GenuineIntel
Frequency:	2992 MHz
Cache:	36608 KB
Architecture:	x86_64
CPUID level:	22
CPU family:	6
Model:	85
FPU:	yes
FPU exception:	yes
Stepping:	0

Flags:	fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid avx512f avx512dq rdseed adx smap clflushopt clwb avx512cd avx512bw avx512vl xsaveopt xsavec xssaves arat pku ospke md_clear flush_l1d arch_capabilities
--------	---

Номер процессора: 10

Информация о устройстве

Параметр	Значение
Model name:	Intel(R) Xeon(R) Gold 6248R CPU @ 3.00GHz
Vendor:	GenuineIntel
Frequency:	2992 MHz
Cache:	36608 KB
Architecture:	x86_64
CPUID level:	22
CPU family:	6
Model:	85
FPU:	yes
FPU exception:	yes
Stepping:	0
Flags:	fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid avx512f avx512dq rdseed adx smap clflushopt clwb avx512cd avx512bw avx512vl xsaveopt xsavec xssaves arat pku ospke md_clear flush_l1d arch_capabilities

Номер процессора: 11

Информация о устройстве

Параметр	Значение
Model name:	Intel(R) Xeon(R) Gold 6248R CPU @ 3.00GHz
Vendor:	GenuineIntel
Frequency:	2992 MHz
Cache:	36608 KB
Architecture:	x86_64
CPUID level:	22
CPU family:	6
Model:	85
FPU:	yes
FPU exception:	yes
Stepping:	0
Flags:	fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid avx512f avx512dq rdseed adx smap clflushopt clwb avx512cd avx512bw avx512vl xsaveopt xsavec xssaves arat pku ospke md_clear flush_l1d arch_capabilities

Номер процессора: 12

Информация о устройстве

Параметр	Значение
Model name:	Intel(R) Xeon(R) Gold 6248R CPU @ 3.00GHz
Vendor:	GenuineIntel
Frequency:	2992 MHz
Cache:	36608 KB
Architecture:	x86_64
CPUID level:	22
CPU family:	6
Model:	85
FPU:	yes
FPU exception:	yes
Stepping:	0
Flags:	fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid avx512f avx512dq rdseed adx smap clflushopt clwb avx512cd avx512bw avx512vl xsaveopt xsavec xsave_arat pku ospke md_clear flush_l1d arch_capabilities

Номер процессора: 13

Информация о устройстве

Параметр	Значение
Model name:	Intel(R) Xeon(R) Gold 6248R CPU @ 3.00GHz
Vendor:	GenuineIntel
Frequency:	2992 MHz
Cache:	36608 KB
Architecture:	x86_64
CPUID level:	22
CPU family:	6
Model:	85
FPU:	yes
FPU exception:	yes
Stepping:	0
Flags:	fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid avx512f avx512dq rdseed adx smap clflushopt clwb avx512cd avx512bw avx512vl xsaveopt xsavec xsave_arat pku ospke md_clear flush_l1d arch_capabilities

Номер процессора: 14

Информация о устройстве

Параметр	Значение
Model name:	Intel(R) Xeon(R) Gold 6248R CPU @ 3.00GHz
Vendor:	GenuineIntel
Frequency:	2992 MHz
Cache:	36608 KB
Architecture:	x86_64
CPUID level:	22
CPU family:	6
Model:	85
FPU:	yes
FPU exception:	yes
Stepping:	0

Flags:	fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid avx512f avx512dq rdseed adx smap clflushopt clwb avx512cd avx512bw avx512vl xsaveopt xsavec xsave arat pku ospke md_clear flush_l1d arch_capabilities
--------	---

Номер процессора: 15

Информация о устройстве

Параметр	Значение
Model name:	Intel(R) Xeon(R) Gold 6248R CPU @ 3.00GHz
Vendor:	GenuineIntel
Frequency:	2992 MHz
Cache:	36608 KB
Architecture:	x86_64
CPUID level:	22
CPU family:	6
Model:	85
FPU:	yes
FPU exception:	yes
Stepping:	0
Flags:	fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid avx512f avx512dq rdseed adx smap clflushopt clwb avx512cd avx512bw avx512vl xsaveopt xsavec xsave arat pku ospke md_clear flush_l1d arch_capabilities

Номер процессора: 2

Информация о устройстве

Параметр	Значение
Model name:	Intel(R) Xeon(R) Gold 6248R CPU @ 3.00GHz
Vendor:	GenuineIntel
Frequency:	2992 MHz
Cache:	36608 KB
Architecture:	x86_64
CPUID level:	22
CPU family:	6
Model:	85
FPU:	yes
FPU exception:	yes
Stepping:	0
Flags:	fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid avx512f avx512dq rdseed adx smap clflushopt clwb avx512cd avx512bw avx512vl xsaveopt xsavec xsave arat pku ospke md_clear flush_l1d arch_capabilities

Номер процессора: 3

Информация о устройстве

Параметр	Значение
Model name:	Intel(R) Xeon(R) Gold 6248R CPU @ 3.00GHz
Vendor:	GenuineIntel
Frequency:	2992 MHz
Cache:	36608 KB
Architecture:	x86_64
CPUID level:	22
CPU family:	6
Model:	85
FPU:	yes
FPU exception:	yes
Stepping:	0
Flags:	fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid avx512f avx512dq rdseed adx smap clflushopt clwb avx512cd avx512bw avx512vl xsaveopt xsavec xssaves arat pku ospke md_clear flush_l1d arch_capabilities

Номер процессора: 4

Информация о устройстве

Параметр	Значение
Model name:	Intel(R) Xeon(R) Gold 6248R CPU @ 3.00GHz
Vendor:	GenuineIntel
Frequency:	2992 MHz
Cache:	36608 KB
Architecture:	x86_64
CPUID level:	22
CPU family:	6
Model:	85
FPU:	yes
FPU exception:	yes
Stepping:	0
Flags:	fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid avx512f avx512dq rdseed adx smap clflushopt clwb avx512cd avx512bw avx512vl xsaveopt xsavec xssaves arat pku ospke md_clear flush_l1d arch_capabilities

Номер процессора: 5

Информация о устройстве

Параметр	Значение
Model name:	Intel(R) Xeon(R) Gold 6248R CPU @ 3.00GHz
Vendor:	GenuineIntel
Frequency:	2992 MHz
Cache:	36608 KB
Architecture:	x86_64
CPUID level:	22
CPU family:	6
Model:	85
FPU:	yes
FPU exception:	yes
Stepping:	0

Flags:	fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid avx512f avx512dq rdseed adx smap clflushopt clwb avx512cd avx512bw avx512vl xsaveopt xsavec xsaves arat pku ospke md_clear flush_l1d arch_capabilities
--------	--

Номер процессора: 6

Информация о устройстве

Параметр	Значение
Model name:	Intel(R) Xeon(R) Gold 6248R CPU @ 3.00GHz
Vendor:	GenuineIntel
Frequency:	2992 MHz
Cache:	36608 KB
Architecture:	x86_64
CPUID level:	22
CPU family:	6
Model:	85
FPU:	yes
FPU exception:	yes
Stepping:	0
Flags:	fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid avx512f avx512dq rdseed adx smap clflushopt clwb avx512cd avx512bw avx512vl xsaveopt xsavec xsaves arat pku ospke md_clear flush_l1d arch_capabilities

Номер процессора: 7

Информация о устройстве

Параметр	Значение
Model name:	Intel(R) Xeon(R) Gold 6248R CPU @ 3.00GHz
Vendor:	GenuineIntel
Frequency:	2992 MHz
Cache:	36608 KB
Architecture:	x86_64
CPUID level:	22
CPU family:	6
Model:	85
FPU:	yes
FPU exception:	yes
Stepping:	0
Flags:	fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid avx512f avx512dq rdseed adx smap clflushopt clwb avx512cd avx512bw avx512vl xsaveopt xsavec xsaves arat pku ospke md_clear flush_l1d arch_capabilities

Номер процессора: 8

Информация о устройстве

Параметр	Значение
Model name:	Intel(R) Xeon(R) Gold 6248R CPU @ 3.00GHz
Vendor:	GenuineIntel
Frequency:	2992 MHz
Cache:	36608 KB
Architecture:	x86_64
CPUID level:	22
CPU family:	6
Model:	85
FPU:	yes
FPU exception:	yes
Stepping:	0
Flags:	fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid avx512f avx512dq rdseed adx smap clflushopt clwb avx512cd avx512bw avx512vl xsaveopt xsavec xsave_arat pku ospke md_clear flush_l1d arch_capabilities

Номер процессора: 9

Информация о устройстве

Параметр	Значение
Model name:	Intel(R) Xeon(R) Gold 6248R CPU @ 3.00GHz
Vendor:	GenuineIntel
Frequency:	2992 MHz
Cache:	36608 KB
Architecture:	x86_64
CPUID level:	22
CPU family:	6
Model:	85
FPU:	yes
FPU exception:	yes
Stepping:	0
Flags:	fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid avx512f avx512dq rdseed adx smap clflushopt clwb avx512cd avx512bw avx512vl xsaveopt xsavec xsave_arat pku ospke md_clear flush_l1d arch_capabilities



Информация

Информация о памяти

ID: 425320

Информация о памяти

Параметр	Значение
RAM:	31601 MB (33135616000 B)
SWAP:	Unknown



Информация

Информация о сетевых картах

ID: 425335

VMware vmxnet3 virtual NIC driver - 00:50:56:01:0f:d0

Информация о сетевых картах

Параметр	Значение
Name:	VMware vmxnet3 virtual NIC driver

Vendor:	VMware, Inc.
Interface name:	ens192
Status:	UP
MAC:	00:50:56:01:0f:d0
Type:	Ethernet

■ MySQL Server • Версия: 8.0.42 Percona Edition Путь: \$Resources(51115)\$: /usr/\$Resources(69990)\$: /var/lib/mysql/



Информация
Процесс MySQL
ID: 184814

Процесс MySQL

Процесс MySQL					
mysql	2082	1	2	14:59 ?	00:00:11 /usr/sbin/mysqld



Информация
Содержимое конфигурационных файлов (my.cnf)
ID: 184716

Файлы конфигурации (my.cnf)

Путь	Содержимое
------	------------

/etc/my.cnf	<pre> [client] port=3306 socket=/var/lib/mysql/mysql.sock default-character-set=utf8mb4 [mysqld_safe] nice=0 socket=/var/lib/mysql/mysql.sock log-error=/var/log/mysql/error.log [mysqld] server-id=1 authentication_policy="*,," disable_log_bin percona_telemetry_disable=1 user=mysql port=3306 basedir=/usr datadir=/var/lib/mysql socket=/var/lib/mysql/mysql.sock pid-file=/var/run/mysql/mysql.pid tmpdir=/tmp secure-log-path=/var/lib/mysql-files skip-external-locking default-storage-engine=innodb transaction-isolation=READ-COMMITTED max_allowed_packet=16M myisam-recover-options=BACKUP explicit_defaults_for_timestamp=1 max_binlog_size=100M sql_mode="" table_open_cache=4096 thread_cache_size=32 key_buffer_size=16M join_buffer_size=2M sort_buffer_size=2M thread_stack=512K max_heap_table_size=32M tmp_table_size=32M innodb_file_per_table innodb_buffer_pool_size=32M innodb_flush_log_at_trx_commit=2 innodb_flush_method=O_DIRECT innodb_strict_mode=OFF innodb_redo_log_capacity=128M innodb_default_row_format=DYNAMIC character-set-server=utf8mb4 collation-server=utf8mb4_0900_ai_ci init-connect="SETNAMEutf8mb4COLLATEutf8mb4_0900_ai_ci" skip-name-resolve tls_version=TLSv1.2,TLSv1.3 [system_default_sect] MinProtocol=TLSv1.2 [mysqldump] quick quote-names max_allowed_packet=16M default-character-set=utf8mb4 [mysql] [isamchk] key_buffer=16M !includedir/etc/mysql/conf.d/ </pre>
/etc/mysql/conf.d/bvat.cnf	<pre> [mysqld] innodb_buffer_pool_size=14336M max_connections=125 table_open_cache=14336 thread_cache_size=128 max_heap_table_size=128M tmp_table_size=128M key_buffer_size=196M join_buffer_size=24M sort_buffer_size=24M bulk_insert_buffer_size=2M myisam_sort_buffer_size=24M </pre>
/etc/mysql/conf.d/logging.cnf	<pre> [mysqld_safe] log-error=/var/log/mysql/error.log [mysqld] log-error=/var/log/mysql/error.log general_log=0 slow_query_log=0 sync_binlog=0 </pre>

/etc/mysql/conf.d/z_bx_custom.cnf

```
[mysqld]
max_connections=150
wait_timeout=60
interactive_timeout=60
innodb_buffer_pool_size=8192M
tmp_table_size=256M
max_heap_table_size=256M
table_open_cache=10200
open_files_limit=10200
innodb_open_files=10200
thread_pool_size=16
innodb_log_file_size=768M
innodb_buffer_pool_instances=6
join_buffer_size=16M
sort_buffer_size=16M
read_buffer_size=1M
read_rnd_buffer_size=2M
optimizer_search_depth=0
```



Информация

Файлы конфигурации (my.cnf)

ID: 184714

Файлы конфигурации

Путь	Статус
/etc/my.cnf	Файл существует
/etc/mysql/conf.d/bvat.cnf	Файл существует
/etc/mysql/conf.d/logging.cnf	Файл существует
/etc/mysql/conf.d/z_bx_custom.cnf	Файл существует
/etc/mysql/my.cnf	Файл не найден
/usr//my.cnf	Файл не найден
/var/lib/mysql//my.cnf	Файл не найден

Network Configuration • Версия: Network Configuration



Информация

ARP-таблица

ID: 189419

ARP-таблица

Пункт назначения	MAC-адрес	Интерфейс	Тип
10.1.1.1	00:50:56:b0:d9:83	ens192	dynamic



Информация

MAC-адрес сканируемого адаптера

ID: 180245

Описание

Сканирование узла проводится через интерфейс с данным MAC-адресом.

00:50:56:01:0f:d0



Информация

Дополнительная информация

ID: 189313

Информация

Параметр	Значение
Hostname:	new-mile.by
Default gateway:	10.1.1.1
DNS server:	8.8.8.8, 1.1.1.1



Информация

Доступные сетевые подключения

ID: 4424673

Количество: **2**

ens192

Сетевые подключения

Параметр	Значение
Name:	ens192
Type:	ether
Status:	UP
Address:	IPv4 - 10.1.1.3(/24) & IPv6 - fe80::250:56ff:fe01:fd0 (/64)
MAC:	00:50:56:01:0f:d0
DHCP status:	IPv4 - dhclient not working & IPv6 - dhclient not working
Adapter name:	VMware vmxnet3 virtual NIC driver
Adapter vendor:	VMware, Inc.
Default interface:	Yes

lo

Сетевые подключения

Параметр	Значение
Name:	lo
Type:	loopback
Status:	UP
Address:	IPv4 - 127.0.0.1(/8) & IPv6 - ::1 (/128)
MAC:	00:00:00:00:00:00
DHCP status:	IPv4 - dhclient not working & IPv6 - dhclient not working



Информация


Имя устройства Unix (Hostname)

ID: 604649

Описание

Имя устройства Unix (Hostname)

new-mile.by



Информация

Открытые порты по прослушиваемым адресам

ID: 401021

Количество: 5

Прослушиваемый IP-адрес (*)

ТСР-порты

Протокол	IP-адрес	Порт	Процесс	Пользователь
tcp (IPv4)	*	10050	Нет информации	Нет информации
tcp (IPv4)	*	3306	Нет информации	Нет информации
tcp (IPv4)	*	33060	Нет информации	Нет информации

Прослушиваемый IP-адрес ([::])

ТСР-порты

Протокол	IP-адрес	Порт	Процесс	Пользователь
tcp (IPv6)	[::]	22	Нет информации	Нет информации

Прослушиваемый IP-адрес ([::1])

UDP-порты

Протокол	IP-адрес	Порт	Процесс	Пользователь
udp (IPv6)	[::1]	323	Нет информации	Нет информации

Прослушиваемый IP-адрес (0.0.0.0)

ТСР-порты

Протокол	IP-адрес	Порт	Процесс	Пользователь
tcp (IPv4)	0.0.0.0	22	Нет информации	Нет информации

tcp (IPv4)	0.0.0.0	443	nginx/1084, nginx/1083, nginx/1082, nginx/1081, nginx/1080, nginx/1079, nginx/1078, nginx/1077	bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix
tcp (IPv4)	0.0.0.0	80	nginx/1084, nginx/1083, nginx/1082, nginx/1081, nginx/1080, nginx/1079, nginx/1078, nginx/1077	bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix
tcp (IPv4)	0.0.0.0	8070	nginx/1084, nginx/1083, nginx/1082, nginx/1081, nginx/1080, nginx/1079, nginx/1078, nginx/1077	bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix
tcp (IPv4)	0.0.0.0	8893	nginx/1084, nginx/1083, nginx/1082, nginx/1081, nginx/1080, nginx/1079, nginx/1078, nginx/1077	bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix
tcp (IPv4)	0.0.0.0	8894	nginx/1084, nginx/1083, nginx/1082, nginx/1081, nginx/1080, nginx/1079, nginx/1078, nginx/1077	bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix

Прослушиваемый IP-адрес (127.0.0.1)

TCP-порты

Протокол	IP-адрес	Порт	Процесс	Пользователь
tcp (IPv4)	127.0.0.1	8077	nginx/1084, nginx/1083, nginx/1082, nginx/1081, nginx/1080, nginx/1079, nginx/1078, nginx/1077	bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix
tcp (IPv4)	127.0.0.1	8081	Нет информации	Нет информации
tcp (IPv4)	127.0.0.1	8887	Нет информации	Нет информации
tcp (IPv4)	127.0.0.1	8888	Нет информации	Нет информации
tcp (IPv4)	127.0.0.1	8895	nginx/1084, nginx/1083, nginx/1082, nginx/1081, nginx/1080, nginx/1079, nginx/1078, nginx/1077	bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix

UDP-порты

Протокол	IP-адрес	Порт	Процесс	Пользователь
udp (IPv4)	127.0.0.1	323	Нет информации	Нет информации



Информация

Список открытых портов

ID: 180293

Список открытых портов

Протокол	IP-адрес	Порт	Процесс	Пользователь
tcp (IPv4)	*	10050	Нет информации	Нет информации
tcp (IPv4)	*	3306	Нет информации	Нет информации
tcp (IPv4)	*	33060	Нет информации	Нет информации
tcp (IPv4)	0.0.0.0	22	Нет информации	Нет информации

tcp (IPv4)	0.0.0.0	443	nginx/1084, nginx/1083, nginx/1082, nginx/1081, nginx/1080, nginx/1079, nginx/1078, nginx/1077	bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix
tcp (IPv4)	0.0.0.0	80	nginx/1084, nginx/1083, nginx/1082, nginx/1081, nginx/1080, nginx/1079, nginx/1078, nginx/1077	bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix
tcp (IPv4)	0.0.0.0	8070	nginx/1084, nginx/1083, nginx/1082, nginx/1081, nginx/1080, nginx/1079, nginx/1078, nginx/1077	bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix
tcp (IPv4)	0.0.0.0	8893	nginx/1084, nginx/1083, nginx/1082, nginx/1081, nginx/1080, nginx/1079, nginx/1078, nginx/1077	bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix
tcp (IPv4)	0.0.0.0	8894	nginx/1084, nginx/1083, nginx/1082, nginx/1081, nginx/1080, nginx/1079, nginx/1078, nginx/1077	bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix
tcp (IPv4)	127.0.0.1	8077	nginx/1084, nginx/1083, nginx/1082, nginx/1081, nginx/1080, nginx/1079, nginx/1078, nginx/1077	bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix
tcp (IPv4)	127.0.0.1	8081	Нет информации	Нет информации
tcp (IPv4)	127.0.0.1	8887	Нет информации	Нет информации
tcp (IPv4)	127.0.0.1	8888	Нет информации	Нет информации
tcp (IPv4)	127.0.0.1	8895	nginx/1084, nginx/1083, nginx/1082, nginx/1081, nginx/1080, nginx/1079, nginx/1078, nginx/1077	bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix, bitrix
tcp (IPv6)	:::	22	Нет информации	Нет информации
udp (IPv4)	127.0.0.1	323	Нет информации	Нет информации
udp (IPv6)	:::1	323	Нет информации	Нет информации



Информация
Таблица маршрутизации
ID: 189418

Таблица маршрутизации

Пункт назначения	Шлюз	Интерфейс	Источник	Метрика
10.1.1.0/24	None	ens192	kernel	100
::1	None	lo	kernel	256
default	10.1.1.1	ens192	static	100
fe80::/64	None	ens192	kernel	1024

■ Operating System • Версия: **Oracle Linux Server 9.6**



Информация
TCP Wrappers и межсетевой экран
ID: 4424622

Краткое описание

Рекомендуется настроить TCP Wrappers и межсетевой экран для ограничения доступа.

Описание

TCP Wrappers и межсетевые экраны в данной рекомендации представлены совместно, поскольку они похожи и функционально дополняют друг друга.

TCP Wrappers:

Ограничивая доступ к серверу, вы уменьшаете риск от совершения атак удаленными злоумышленниками. Для серверов, подключенных к сети Интернет и предоставляющих службы для сети Интернет, ограничение доступа может быть невозможным или бессмысленным. Внутренние серверы, серверы с ограниченным доступом и рабочие станции должны разрешать доступ только из авторизованных сетей.

Межсетевой экран:

Использование межсетевых экранов имеет следующие преимущества:

Защита от скомпрометированных систем в локальной сети;

Глубокая защита, т.к. злоумышленник должен пройти два межсетевых экрана (граничный и на системе), чтобы произвести успешную атаку на систему;

Очень хорошо настроенный контроль над тем, какие системы могут и какие не могут иметь доступ к вашей системе.

Рекомендуется устанавливать межсетевой экран на все компьютеры и на серверы.

Проверка	Результат
Доступ к серверу запрещен из всех сетей	Да
Доступ к серверу разрешен из авторизованных сетей	Да
Объект	Ошибка
/etc/hosts.allow	Не существует такого файла или каталога
/etc/hosts.deny	Не существует такого файла или каталога

Как исправить

Настройте TCP Wrappers и межсетевой экран для ограничения доступа.



Информация

Блокирование системных учетных записей

ID: 4424627

Краткое описание

Рекомендуется заблокировать системные учетные записи.

Описание

Системные учетные записи не связаны с пользователями, поэтому их стоит создавать таким образом, чтобы они не имели доступа к командной оболочке. Для этого заблокируйте эти учетные записи или настройте для них не существующие командные оболочки. Эти записи могут быть удалены, если компьютеры не используют соответствующие им демоны/службы, хотя рекомендуется просто их отключить.

Проверка	Результат
Системные учетные записи заблокированы	Нет
Незаблокированные системные аккаунты	
adm	
apache	
bin	
daemon	
dbus	
ftp	
games	
halt	
lp	
mail	
mysql	
operator	
rtkit	
shutdown	
sshd	
sync	
tcpdump	
tss	

Как исправить

Заблокируйте системные учетные записи.



Информация

Доступ к системной консоли

ID: 4424626

Краткое описание

Рекомендуется ограничить доступ к системной консоли с использованием учетной записи суперпользователя.

Описание

Доступ в систему с учетной записью суперпользователя должен быть запрещен, кроме доступа через консоль в экстренных случаях. Во всех остальных ситуациях для получения дополнительных прав администратор должен войти в систему с непривилегированной учетной записью и затем использовать определенный механизм авторизации (через `su` или `sudo`), чтобы повысить уровень своих привилегий. При возникновении проблем эти механизмы, как минимум, предоставляют возможность провести аудит.

Настройка	Значение	Требование
Параметр "AllowRemoteRoot" в файле /etc/X11/gdm/gdm.conf	Объект не найден	false
Параметр "AllowRemoteRoot" в файле /etc/X11/gdm/gdm.conf	Объект не найден	false
Параметр "AllowRoot" в файле /etc/X11/gdm/gdm.conf	Объект не найден	false
Параметр "AllowRoot" в файле /etc/X11/gdm/gdm.conf	Объект не найден	false
Параметр "Use24Clock" в файле /etc/X11/gdm/gdm.conf	Объект не найден	true
Параметр "Use24Clock" в файле /etc/X11/gdm/gdm.conf	Объект не найден	true
Проверка	Результат	
Доступ к консоли с учетной записью root ограничен	Да	
Объект	Ошибка	
/etc/securetty	Не существует такого файла или каталога	

Как исправить

Ограничьте доступ с использованием учетной записи суперпользователя.



Информация
Запуск ОС в виртуальном окружении
ID: 186241

Результаты проверки

Проверка	Результат
ОС запущена в виртуальном окружении	Неизвестно

Ошибки

Объект	Текст ошибки
dmidecode	# dmidecode 3.6 /sys/firmware/dmi/tables/smbios_entry_point: Permission denied Scanning /dev/mem for entry point. Can't read memory from /dev/mem



Информация
Использование capabilities для исполняемых файлов
ID: 175486

Список исполняемых файлов, имеющих capabilities

Имя файла	Capabilities
/usr/bin/arping	cap_net_raw=p
/usr/bin/clockdiff	cap_net_raw=p
/usr/bin/newgidmap	cap_setgid=ep
/usr/bin/newuidmap	cap_setuid=ep
/usr/libexec/gstreamer-1.0/gst-ptp-helper	cap_net_bind_service,cap_net_admin,cap_sys_nice=ep
/usr/sbin/mtr-packet	cap_net_raw=ep
/usr/sbin/suexec	cap_setgid,cap_setuid=ep



Информация
Использование PAM
ID: 4424633

Краткое описание

Рекомендуется использовать PAM для повышения уровня сложности паролей.

Описание

Это позволяет использовать аутентификацию PAM и определить сложность пароля (также с помощью DISA SRR (GEN000600/620/640/800)). Минимальное количество требуемых символов - 1 (при необходимости может быть увеличена до 2 или 3). Это количество относится к символам верхнего и нижнего регистров, цифрам и специальным символам, которые вместе составляют пароль. Минимальная длина пароля - 9 символов, т.к. эта длина существенно увеличивает время, необходимое на подбор пароля с помощью современных инструментов. Примечание: Изменения, касающиеся сложности пароля, внесенные в /etc/pam.d/system-auth будут активированы сценарием, описанным ниже. Но эти изменения будут перезаписаны, если выполнить authconfig. Утилита authconfig не может распознать или сохранить сделанные изменения.

Настройка	Значение	Требование
/etc/pam.d/system-auth dcredit	-	2
/etc/pam.d/system-auth lcredit	-	2
/etc/pam.d/system-auth minlen	-	9
/etc/pam.d/system-auth ocredit	-	2
/etc/pam.d/system-auth retry	-	3
/etc/pam.d/system-auth ucredit	-	2

Объект	Тип объекта	Владелец	Группа	Права владельца	Права группы	Права остальных
/etc/pam.d/system-auth	file	root	root	rw-	r--	r--

Как исправить

Увеличьте уровень сложности паролей.

Ссылки

http://www.deer-run.com/~hal/sysadmin/pam_cracklib.html



Информация

Использование дискового пространства

ID: 430005

Дисковое пространство

Точка монтирования	Устройство	Емкость, Мб	Занято, Мб	Свободно, Мб	Занято, %
/	/dev/sda1	301289	4810	281103	2%



Информация

Количество попыток входа до блокировки учетной записи

ID: 4424637

Краткое описание

Рекомендуется настроить блокировку учетной записи после трех последовательных неудачных попыток зарегистрироваться в системе.

Описание

Политика безопасности, согласно которой учетная запись блокируется после нескольких последовательных неудачных попыток регистрации, является установившейся практикой.

Проверка	Результат
Файл /etc/pam.d/system-auth настроен безопасно	Нет

Объект	Тип объекта	Владелец	Группа	Права владельца	Права группы	Права остальных
/etc/pam.d/system-auth	file	root	root	rw-	r--	r--

Как исправить

Установите требуемое значение.

Ссылки

<http://www.puschitz.com/SecuringLinux.shtml/>



Информация

Ограничение доступа к команде su

ID: 4424630

Краткое описание

Рекомендуется максимально ограничить доступ к учетной записи суперпользователя с использованием команды su.

Описание

Команда su предоставляет возможность получить права других пользователей системы. Эта команда часто используется для получения прав суперпользователя и для запуска команд от имени суперпользователя.

Если ограничить доступ к учетной записи суперпользователя, то даже пользователи, которые знают пароль суперпользователя, не смогут получить права суперпользователя, если у них нет физического доступа к консоли сервера или если они не состоят в группе wheel. Это повышает уровень безопасности системы и предотвращает несанкционированный доступ к системе.

Проверка		Результат				
Доступ к аккаунту суперпользователя через su ограничен в/etc/pam.d/su		Нет				
Группа wheel существует		Да				
Объект	Тип объекта	Владелец	Группа	Права владельца	Права группы	Права остальных
/etc/pam.d/su	file	root	root	rw-	r--	r--
/etc/security/access.conf	file	root	root	rw-	r--	r--

Как исправить

Ограничьте доступ с использованием учетной записи суперпользователя.



Информация

Ограничение удаленного доступа к X Server

ID: 4424625

Краткое описание

Рекомендуется запретить использование порта 6000/tcp по умолчанию.

Описание

X-серверы получают сообщения по порту 6000/tcp от удаленных клиентов, которые запущены на других системах. Однако X Windows использует небезопасный протокол аутентификации, поэтому злоумышленник, у которого может получить неавторизованный доступ к локальному X-серверу, может скомпрометировать систему. Вызов опции "-nolisten tcp" приводит к тому, что X-сервер не будет прослушивать порт 6000/tcp по умолчанию. Благодаря этому авторизованные удаленные X-клиенты также не отображают окна в локальной системе. Однако пересылка X-событий через SSH будет по-прежнему осуществляться в стандартном режиме. Более предпочтительным и безопасным является именно этот метод передачи результатов от удаленных X-клиентов.

Проверка	Результат
X Server не прослушивает TCP-порт 6000	Нет
/etc/X11/xdm/Xservers содержит строку "-nolisten tcp"	Нет
/etc/X11/xinit/xserverrc содержит строку "-nolisten tcp"	Нет
Объект	Ошибка
/etc/X11/gdm/gdm.conf	Не существует такого файла или каталога
/etc/X11/xdm/Xservers	Не существует такого файла или каталога
/etc/X11/xinit/xserverrc	Не существует такого файла или каталога

Как исправить

Запретите использование порта 6000/tcp по умолчанию.



Информация

Опции монтирования файловых систем

ID: 175482

Точка монтирования	Имя устройства	Опции монтирования
/	/dev/sda1	rw,relatime



Информация

Параметры ядра ОС

ID: 190643

Количество: 9

abi

Параметры

Параметр	Значение
abi.vsyscall32	1

crypto

Параметры

Параметр	Значение
crypto.fips_enabled	0

crypto.fips_name	Oracle Linux 9 Unbreakable Enterprise Kernel 8 Crypto API
crypto.fips_version	6.12.0-101.33.4.3.el9uek.x86_64

debug

Параметры

Параметр	Значение
debug.exception-trace	1
debug.kprobes-optimization	1

dev

Параметры

Параметр	Значение
dev.cdrom.autoclose	1
dev.cdrom.autoeject	0
dev.cdrom.check_media	0
dev.cdrom.debug	0
dev.cdrom.info	CD-ROM information, Id: cdrom.c 3.20 2003/12/17; drive name: sr0; drive speed: 1; drive # of slots: 1; Can close tray: 1; Can open tray: 1; Can lock tray: 1; Can change speed: 1; Can select disk: 0; Can read multisession: 1; Can read MCN: 1; Reports media changed: 1; Can play audio: 1; Can write CD-R: 1; Can write CD-RW: 1; Can read DVD: 1; Can write DVD-R: 1; Can write DVD-RAM: 1; Can read MRW: 1; Can write MRW: 1; Can write RAM: 1
dev.cdrom.lock	1
dev.hpet.max-user-freq	64
dev.mac_hid.mouse_button2_keycode	97
dev.mac_hid.mouse_button3_keycode	100
dev.mac_hid.mouse_button_emulation	0
dev.raid.speed_limit_max	200000
dev.raid.speed_limit_min	1000
dev.scsi.logging_level	0
dev.tty.ldisc_autoload	1
dev.tty.legacy_tiocsti	1

fs

Параметры

Параметр	Значение
fs.aio-max-nr	65536
fs.aio-nr	2561
fs.binfmt_misc.status	enabled
fs.dentry-state	40775 30604 45 0 6603 0
fs.dir-notify-enable	1
fs.epoll.max_user_watches	7194156
fs.fanotify.max_queued_events	16384
fs.fanotify.max_user_groups	128
fs.fanotify.max_user_marks	261810
fs.file-max	9223372036854775807
fs.file-nr	2112 0 9223372036854775807
fs.inode-nr	34472 440
fs.inode-state	34472 440 0 0 0 0
fs.inotify.max_queued_events	16384
fs.inotify.max_user_instances	128
fs.inotify.max_user_watches	246226
fs.lease-break-time	45

fs.leases-enable	1
fs.mount-max	100000
fs.mqueue.msg_default	10
fs.mqueue.msg_max	10
fs.mqueue.msgsize_default	8192
fs.mqueue.msgsize_max	8192
fs.mqueue.queues_max	256
fs.negative-dentry-limit	0
fs.nr_open	1073741816
fs.overflowgid	65534
fs.overflowuid	65534
fs.pipe-max-size	1048576
fs.pipe-user-pages-hard	0
fs.pipe-user-pages-soft	16384
fs.protected_fifos	1
fs.protected_hardlinks	1
fs.protected_regular	1
fs.protected_symlinks	1
fs.quota.allocated_dquotes	0
fs.quota.cache_hits	0
fs.quota.drops	0
fs.quota.free_dquotes	0
fs.quota.lookups	0
fs.quota.reads	0
fs.quota.syncs	0
fs.quota.writes	0
fs.suid_dumpable	2

kernel

Параметры

Всего строк — 132, показаны 50 строк

Параметр	Значение
kernel.acct	4 2 30
kernel.acpi_video_flags	0
kernel.arch	x86_64
kernel.auto_msgmni	0
kernel.bootloader_type	114
kernel.bootloader_version	2
kernel.bpf_stats_enabled	0
kernel.cap_last_cap	40
kernel.core_file_note_size_limit	4194304
kernel.core_pattern	usr/lib/systemd/systemd-coredump %P %u %g %s %t %c %h %d
kernel.core_pipe_limit	16
kernel.core_sort_vma	0
kernel.core_uses_pid	1
kernel.ctrl-alt-del	0
kernel.dmesg_restrict	1
kernel.domainname	(none)
kernel.firmware_config.force_sysfs_fallback	0
kernel.firmware_config.ignore_sysfs_fallback	0
kernel.ftrace_dump_on_oops	0
kernel.ftrace_enabled	1
kernel.hardlockup_all_cpu_backtrace	0
kernel.hardlockup_panic	1
kernel.hostname	new-mile.by
kernel.hung_task_all_cpu_backtrace	0
kernel.hung_task_check_count	4194304
kernel.hung_task_check_interval_secs	0
kernel.hung_task_panic	0
kernel.hung_task_timeout_secs	120
kernel.hung_task_warnings	10
kernel.io_delay_type	0

kernel.io_uring_disabled	0
kernel.io_uring_group	-1
kernel.kexec_load_disabled	0
kernel.kexec_load_limit_panic	-1
kernel.kexec_load_limit_reboot	-1
kernel.keys.gc_delay	300
kernel.keys.maxbytes	20000
kernel.keys.maxkeys	200
kernel.keys.persistent_keyring_expiry	259200
kernel.keys.root_maxbytes	25000000
kernel.keys.root_maxkeys	1000000
kernel.kptr_restrict	1
kernel.ksplice.init_trace_safe	1
kernel.max_lock_depth	1024
kernel.max_rcu_stall_to_panic	0
kernel.modprobe	/sbin/modprobe
kernel.modules_disabled	0
kernel.msg_next_id	-1
kernel.msgmax	8192
kernel.msgmnb	16384

Всего строк — 132, показаны 50 строк

net

Параметры

Всего строк — 784, показаны 50 строк

Параметр	Значение
net.core.bpf_jit_enable	1
net.core.busy_poll	0
net.core.busy_read	0
net.core.default_qdisc	fq_codel
net.core.dev_weight	64
net.core.dev_weight_rx_bias	1
net.core.dev_weight_tx_bias	1
net.core.devconf_inherit_init_net	0
net.core.fb_tunnels_only_for_init_net	0
net.core.flow_limit_cpu_bitmap	00000000,00000000,00000000,00000000
net.core.flow_limit_table_len	4096
net.core.gro_normal_batch	8
net.core.high_order_alloc_disable	0
net.core.max_skb_frags	17
net.core.mem_pcpu_rsv	256
net.core.message_burst	10
net.core.message_cost	5
net.core.netdev_budget	300
net.core.netdev_budget_usecs	2000
net.core.netdev_max_backlog	1000
net.core.netdev_rss_key	67:b0:0d:ca:69:da:eb:1f:b7:15: fb:4a:0c:72:70:50:06:5d:55:14: 50:44:0f:76:94:bf:83:fd:00:f1: 7f:5a:c6:5b:2c:a8:e3:08:18:8c: f9:d5:e0:9e:99:b0:67:36:05:11:f4:05
net.core.netdev_tstamp_prequeue	1
net.core.netdev_unregister_timeout_secs	10
net.core.optmem_max	81920
net.core.rmem_default	229376
net.core.rmem_max	229376
net.core.rps_default_mask	00000000,00000000,00000000,00000000
net.core.rps_sock_flow_entries	0
net.core.skbf_defer_max	64
net.core.somaxconn	4096
net.core.tstamp_allow_data	1
net.core.txrehash	1
net.core.warnings	0

net.core.wmem_default	229376
net.core.wmem_max	229376
net.core.xfrm_acq_expires	30
net.core.xfrm_aevent_etime	10
net.core.xfrm_aevent_rseqth	2
net.core.xfrm_larval_drop	1
net.ipv4.cipso_cache_bucket_size	10
net.ipv4.cipso_cache_enable	1
net.ipv4.cipso_rbm_optfmt	0
net.ipv4.cipso_rbm_strictvalid	1
net.ipv4.conf.all.accept_local	0
net.ipv4.conf.all.accept_redirects	1
net.ipv4.conf.all.accept_source_route	0
net.ipv4.conf.all.arp_accept	0
net.ipv4.conf.all.arp_announce	0
net.ipv4.conf.all.arp_evict_nocarrier	1
net.ipv4.conf.all.arp_filter	0

Всего строк — 784, показаны 50 строк

user

Параметры

Параметр	Значение
user.max_cgroup_namespaces	126238
user.max_fanotify_groups	128
user.max_fanotify_marks	261810
user.max_inotify_instances	128
user.max_inotify_watches	246226
user.max_ipc_namespaces	126238
user.max_mnt_namespaces	126238
user.max_net_namespaces	126238
user.max_pid_namespaces	126238
user.max_time_namespaces	126238
user.max_user_namespaces	126238
user.max_uts_namespaces	126238

vm

Параметры

Параметр	Значение
vm.admin_reserve_kbytes	8192
vm.compact_unevictable_allowed	1
vm.compaction_proactiveness	20
vm.dirty_background_bytes	0
vm.dirty_background_ratio	10
vm.dirty_bytes	0
vm.dirty_expire_centisecs	3000
vm.dirty_ratio	30
vm.dirty_writeback_centisecs	500
vm.dirtytime_expire_seconds	43200
vm.enable_soft_offline	1
vm.extfrag_threshold	500
vm.hugetlb_optimize_vmemmap	1
vm.hugetlb_shm_group	0
vm.laptop_mode	0
vm.legacy_va_layout	0
vm.lowmem_reserve_ratio	256 256 32 0 0
vm.madv_doexec_flag	201
vm.max_map_count	65530
vm.memfd_noexec	0
vm.memory_failure_early_kill	0
vm.memory_failure_recovery	1
vm.min_free_kbytes	67584

vm.min_slab_ratio	5
vm.min_unmapped_ratio	1
vm.mmap_min_addr	65536
vm.nr_hugepages	0
vm.nr_hugepages_mempolicy	0
vm.nr_overcommit_hugepages	0
vm.numa_stat	1
vm.numa_zonelist_order	Node
vm.oom_dump_tasks	1
vm.oom_kill_allocating_task	0
vm.overcommit_kbytes	0
vm.overcommit_memory	0
vm.overcommit_ratio	50
vm.page-cluster	3
vm.page_lock_unfairness	5
vm.panic_on_oom	0
vm.percpu_pagelist_high_fraction	0
vm.stat_interval	1
vm.swappiness	30
vm.unprivileged_userfaultfd	0
vm.user_reserve_kbytes	131072
vm.vfs_cache_pressure	100
vm.watermark_boost_factor	15000
vm.watermark_scale_factor	10
vm.zone_reclaim_mode	0



Информация
Пароль LILO/GRUB
ID: 4424634

Краткое описание

Рекомендуется установить пароль LILO/GRUB.

Описание

В большинстве Linux-систем стандартный начальный загрузчик позволяет злоумышленнику нарушить стандартный процесс загрузки. Описанные ниже действия позволяют загружать систему в обычном режиме, при этом пароль запрашивается только тогда, когда пользователь пытается изменить процесс загрузки, отправляя команды LILO или GRUB. Не забудьте заменить <password> на соответствующий пароль.

Проверка	Результат
Параметр "Password" установлен в файле /etc/grub.conf	Нет
Параметр "Restricted password" установлен в файле /etc/lilo.conf	Нет

Объект	Тип объекта	Владелец	Группа	Права владельца	Права группы	Права остальных
/etc/inittab	file	root	root	rw-	г--	г--

Объект	Ошибка
/etc/grub.conf	Не существует такого файла или каталога
/etc/lilo.conf	Не существует такого файла или каталога

Как исправить

Установите пароль LILO/GRUB.



Информация
Переход в режим sudo
ID: 4424636

Краткое описание

Рекомендуется установить и настроить sudo.

Описание

sudo позволяет системному администратору делегировать полномочия на осуществление действий группе пользователей. Часто уровень привилегий при этом существенно повышается, - например, пользователь получает право на перезагрузку веб-сервера. Если настройки сервера часто изменяются (или в сервере присутствует ошибка, из-за которой часто происходит аварийный сбой), то необходимость каждый раз вызывать системного администратора для перезапуска становится обременительной. sudo позволяет администратору делегировать право осуществлять одно подобное действие с правами суперпользователя, при этом другие права не передаются.

После установки sudo необходимо ее настроить с помощью visudo. В visudo встроена проверка на ошибки. Как

показывает опыт, если /etc/sudoers выходит из строя (из-за использования vi без функции проверки ошибок, встроенной в visudo), то восстановление может оказаться затруднительным.

Проверка				Результат		
Разрешения для членов группы "wheel" установлены в файле /etc/sudoers				Нет		
Объект	Тип объекта	Владелец	Группа	Права владельца	Права группы	Права остальных
/etc/sudoers	file	root	root	г--	г--	---

Как исправить
Установите и настройте sudo.

Информация


Поиск учетных записей с пустыми паролями
ID: 4424628

Краткое описание
Рекомендуется проверить, что все учетные записи имеют непустые пароли.

Описание
Учетная запись с пустым паролем означает, что кто угодно может войти в систему, вообще не предоставляя пароля. Все учетные записи должны быть защищены стойкими паролями или заблокированы.

Ошибки	
Объект	Ошибка
/etc/shadow	Нет доступа

Как исправить
Убедитесь, что все учетные записи имеют непустые пароли.

Информация

Политика паролей
ID: 4424638

Краткое описание
Рекомендуется установить параметры истечения срока действия активных учетных записей.

Описание
Пользователи должны регулярно менять пароли.
Пароль изменялся каждые -М дней (для всех учетных записей, кроме системных).
После смены пароля устанавливается запрет на замену пароля в течение -m дней.
Пользователи получают предупреждение за -W дней до истечения срока действия своих паролей.
Учетная запись блокируется через -I дней после истечения срока действия пароля.

Параметр	Значение	Рекомендуемое значение
/etc/login.defs -> PASS_MAX_DAYS	99999	<= 90
/etc/login.defs -> PASS_MIN_DAYS	0	>= 7
/etc/login.defs -> PASS_MIN_LEN	Параметр не найден	>= 6
/etc/login.defs -> PASS_WARN_AGE	7	28

Существующие учетные записи				
Имя пользователя	-M	-m	-W	-I
adm	-	-	-	-
apache	-	-	-	-
bin	-	-	-	-
bitrix	-	-	-	-
chrony	-	-	-	-
daemon	-	-	-	-
dbus	-	-	-	-
flatpak	-	-	-	-
ftp	-	-	-	-
games	-	-	-	-
geoclue	-	-	-	-
halt	-	-	-	-
libstoragemgmt	-	-	-	-
lp	-	-	-	-
mail	-	-	-	-

memcached	-	-	-	-
mysql	-	-	-	-
nginx	-	-	-	-
nobody	-	-	-	-
operator	-	-	-	-
pipewire	-	-	-	-
polkitd	-	-	-	-
redis	-	-	-	-
root	-	-	-	-
rtkit	-	-	-	-
saslauth	-	-	-	-
setroubleshoot	-	-	-	-
shutdown	-	-	-	-
sshd	-	-	-	-
sssd	-	-	-	-
sync	-	-	-	-
systemd-coredump	-	-	-	-
tcpdump	-	-	-	-
tss	-	-	-	-
zabbix	-	-	-	-

Права доступа к файлам и директориям

Объект	Тип объекта	Владелец	Группа	Права владельца	Права группы	Права остальных
/etc/login.defs	file	root	root	rw-	r--	r--

Как исправить

Установите параметры истечения срока действия.



Информация

Программное обеспечение, связанное со сценарием загрузки

ID: 4424635

Краткое описание

Рекомендуется удалить неиспользуемое программное обеспечение.

Описание

Наиболее эффективным способом избавиться от большинства неиспользуемого программного обеспечения является выявление неиспользуемых запущенных служб, хранящихся в каталоге загрузки /etc/init.d.

Состояние пакета

Пакет	Состояние
initscripts	установлен
systemd	установлен

Как исправить

Удалите неиспользуемое программное обеспечение.



Информация

Служба SSH

ID: 425325

Краткое описание

Рекомендуется настроить SSH.

Описание

Рекомендуемые настройки предусмотрены для того, чтобы обеспечить надежные стандартные настройки для клиента и для сервера SSH. В частности, ssh-клиент и sshd-сервер настроены на использование только протокола SSH protocol 2, т.к. в протоколе SSH protocol 1 были обнаружены уязвимости, связанные с безопасностью. Это может привести к проблемам с совместимостью с узлами, которые используют протокол SSH protocol 1.

Настройка	Значение	Рекомендуемое значение
Параметр "HostbasedAuthentication" в файле /etc/ssh/sshd_config	cat: /etc/ssh/sshd_config: Permission denied	no
Параметр "IgnoreRhosts" в файле /etc/ssh/sshd_config	cat: /etc/ssh/sshd_config: Permission denied	yes
Параметр "PermitEmptyPasswords" в файле /etc/ssh/sshd_config	cat: /etc/ssh/sshd_config: Permission denied	no
Параметр "PermitRootLogin" в файле /etc/ssh/sshd_config	cat: /etc/ssh/sshd_config: Permission denied	no

Объект	Тип объекта	Владелец	Группа	Права владельца	Права группы	Права остальных
/etc/ssh/ssh_config	file	root	root	rw-	r--	r--
/etc/ssh/sshd_config	file	root	root	rw-	---	---

Информация о группе

Идентификатор	Список членов группы
2	daemon

dbus**Информация о группе**

Идентификатор	Список членов группы
81	dbus

dialout**Информация о группе**

Идентификатор	Список членов группы
18	

disk**Информация о группе**

Идентификатор	Список членов группы
6	

flatpak**Информация о группе**

Идентификатор	Список членов группы
597	flatpak

floppy**Информация о группе**

Идентификатор	Список членов группы
19	

ftp**Информация о группе**

Идентификатор	Список членов группы
50	ftp

games**Информация о группе**

Идентификатор	Список членов группы
20	

geoclue**Информация о группе**

Идентификатор	Список членов группы
598	geoclue

input**Информация о группе**

Идентификатор	Список членов группы
104	

kmem**Информация о группе**

Идентификатор	Список членов группы
9	

kvm

Информация о группе

Идентификатор	Список членов группы
36	

libstoragemgmt

Информация о группе

Идентификатор	Список членов группы
994	libstoragemgmt

lock

Информация о группе

Идентификатор	Список членов группы
54	

lp

Информация о группе

Идентификатор	Список членов группы
7	lp

mail

Информация о группе

Идентификатор	Список членов группы
12	mail

map

Информация о группе

Идентификатор	Список членов группы
15	

mem

Информация о группе

Идентификатор	Список членов группы
8	

memcached

Информация о группе

Идентификатор	Список членов группы
596	memcached

mysql

Информация о группе

Идентификатор	Список членов группы
27	mysql

nginx

Информация о группе

Идентификатор	Список членов группы

991	nginx
-----	-------

nobody

Информация о группе

Идентификатор	Список членов группы
65534	nobody

percona-telemetry

Информация о группе

Идентификатор	Список членов группы
1000	daemon

pipewire

Информация о группе

Идентификатор	Список членов группы
599	pipewire

polkitd

Информация о группе

Идентификатор	Список членов группы
998	polkitd

printadmin

Информация о группе

Идентификатор	Список членов группы
997	

redis

Информация о группе

Идентификатор	Список членов группы
992	redis

render

Информация о группе

Идентификатор	Список членов группы
105	

root

Информация о группе

Идентификатор	Список членов группы
0	shutdown, root, halt, sync, operator

rtkit

Информация о группе

Идентификатор	Список членов группы
172	rtkit

saslauth

Информация о группе

Идентификатор	Список членов группы
76	saslauth

setroubleshoot

Информация о группе

Идентификатор	Список членов группы
995	setroubleshoot

sgx

Информация о группе

Идентификатор	Список членов группы
106	

slocate

Информация о группе

Идентификатор	Список членов группы
21	

ssh_keys

Информация о группе

Идентификатор	Список членов группы
101	

sshd

Информация о группе

Идентификатор	Список членов группы
74	sshd

sssd

Информация о группе

Идентификатор	Список членов группы
996	sssd

sys

Информация о группе

Идентификатор	Список членов группы
3	

systemd-coredump

Информация о группе

Идентификатор	Список членов группы
999	systemd-coredump

systemd-journal

Информация о группе

Идентификатор	Список членов группы
190	

tape

Информация о группе

Идентификатор	Список членов группы
33	

tcpdump

Информация о группе


Идентификатор	Список членов группы
72	tcpdump

tss

Информация о группе

Идентификатор	Список членов группы
59	tss

Всего строк — 57, показаны 50 строк



Информация

Список пользователей системы

ID: 425318

Количество: **35**

adm

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
3	adm	/var/adm	/sbin/nologin	adm

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
4	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

apache

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
48	Apache	/usr/share/httpd	/sbin/nologin	apache

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
48	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

bin

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
1	bin	/bin	/sbin/nologin	bin

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
1	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
600	Bitrix user	/home/bitrix	/bin/bash	bitrix

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
600	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

Environment

SHELL=/bin/bash
HISTCONTROL=ignoredups
HOSTNAME=new-mile.by
HISTSIZE=0
PWD=/home/bitrix
LOGNAME=bitrix
XDG_SESSION_TYPE=ttty
MOTD_SHOWN=pam
HOME=/home/bitrix
LANG=C
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:mi=01;37;41:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.webp=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.fic=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=01;36:*.au=01;36:*.flac=01;36:*.m4a=01;36:*.mid=01;36:*.midi=01;36:*.mka=01;36:*.mp3=01;36:*.mpc=01;36:*.ogg=01;36:*.ra=01;36:*.wav=01;36:*.oga=01;36:*.opus=01;36:*.spx=01;36:*.xspf=01;36:
PROMPT_COMMAND=echo -ne "\033]0;\${USER}@\${HOSTNAME}%.*;\007"
SSH_CONNECTION=192.168.200.115 20129 10.1.1.3 22
BITRIX_ENV_TYPE=general
XDG_SESSION_CLASS=user
TERM=ansi
LESSOPEN= /usr/bin/lesspipe.sh %s
USER=bitrix
BITRIX_VA_VER=9.0.7
SHLVL=0
XDG_SESSION_ID=23
XDG_RUNTIME_DIR=/run/user/600
SSH_CLIENT=192.168.200.115 20129 22
DEBUGINFOD_IMA_CERT_PATH=/etc/keys/ima:
which_declare=declare -f
XDG_DATA_DIRS=/home/bitrix/.local/share/flatpak/exports/share:/var/lib/flatpak/exports/share:/usr/local/share:/usr/share
PATH=/home/bitrix/.local/bin:/home/bitrix/bin:/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/600/bus
MAIL=/var/spool/mail/bitrix
SSH_TTY=/dev/pts/1
BASH_FUNC_which%%=() { (alias; eval \${which_declare}) /usr/bin/which --tty-only --read-alias --read-functions --show-tilde --show-dot \$@ }
_=/usr/bin/env

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
993	chrony system user	/var/lib/chrony	/sbin/nologin	chrony

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
993	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

daemon

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
2	daemon	/sbin	/sbin/nologin	percona-telemetry, daemon

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
2	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

dbus

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
81	System message bus	/	/sbin/nologin	dbus

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
81	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

flatpak

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
597	Flatpak system helper	/	/usr/sbin/nologin	flatpak

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
597	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

ftp

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
----------------------------	------------	------------------	---------------------------	--------

14	FTP User	/var/ftp	/sbin/nologin	ftp
----	----------	----------	---------------	-----

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
50	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

games

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
12	games	/usr/games	/sbin/nologin	users

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
100	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

geoclue

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
598	User for geoclue	/var/lib/geoclue	/sbin/nologin	geoclue

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
598	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

halt

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
7	halt	/sbin	/sbin/halt	root

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
0	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

libstoragemgmt

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
994	daemon account for libstoragemgmt	/	/usr/sbin/nologin	libstoragemgmt

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
994	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

lp

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
4	lp	/var/spool/lpd	/sbin/nologin	lp

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
7	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

mail

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
8	mail	/var/spool/mail	/sbin/nologin	mail

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
12	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

memcached

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
596	memcached daemon	/	/sbin/nologin	memcached

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
596	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

mysql

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
27	Percona Server	/var/lib/mysql	/bin/false	mysql

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
27	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

nginx

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
990	Nginx web server	/var/lib/nginx	/sbin/nologin	nginx

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
991	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

nobody

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
65534	Kernel Overflow User	/	/sbin/nologin	nobody

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
65534	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

operator

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
11	operator	/root	/sbin/nologin	root

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
0	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

pipewire

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
599	PipeWire System Daemon	/run/pipewire	/usr/sbin/nologin	pipewire

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
599	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
-----------------------------	-------------------

No access	No access
-----------	-----------

polkitd

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
998	User for polkitd	/	/sbin/nologin	polkitd

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
998	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

redis

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
992	Redis Database Server	/var/lib/redis	/sbin/nologin	redis

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
992	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

root

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
0	root	/root	/bin/bash	root

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
0	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

rtkit

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
172	RealtimeKit	/	/sbin/nologin	rtkit

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
172	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

saslauth

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
991	Saslauthd user	/run/saslauthd	/sbin/nologin	saslauth

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
76	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

setroubleshoot

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
996	SELinux troubleshoot server	/var/lib/setroubleshoot	/usr/sbin/nologin	setroubleshoot

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
995	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

shutdown

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
6	shutdown	/sbin	/sbin/shutdown	root

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
0	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

sshd

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
74	Privilege-separated SSH	/usr/share/empty.sshd	/usr/sbin/nologin	sshd

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
74	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

sssd

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
997	User for sssd	/	/sbin/nologin	sssd

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
996	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

sync

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
5	sync	/sbin	/bin/sync	root

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
0	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

systemd-coredump

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
999	systemd Core Dumper	/	/sbin/nologin	systemd-coredump

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
999	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

tcpdump

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
72		/	/sbin/nologin	tcpdump

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
72	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

tss

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
59	Account used for TPM access	/	/usr/sbin/nologin	tss

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
59	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access

zabbix

Информация о пользователе

Идентификатор пользователя	Полное имя	Домашний каталог	Пользовательская оболочка	Группы
595	Zabbix Monitoring System	/var/lib/zabbix	/sbin/nologin	zabbix

Дополнительная информация

Primal GID	PasswordIsSet	PasswordNotBlocked	PasswordNotEmpty	PasswordMaxDays	PasswordMinDays	PasswordWarnDays	PasswordLastChanged
595	No access	No access	No access	No access	No access	No access	No access

Linux attributes

AccountExpiredAfterDisabled	AccountDisabledAt
No access	No access



Информация

Стандартные службы

ID: 4424621

Краткое описание

Рекомендуется отключить неиспользуемые стандартные службы.

Описание

При использовании SSH необходимость в основанных на xinetd службах пропадает, так как SSH предоставляет механизм безопасного входа и средства передачи файлов в систему и из нее. Рекомендуемые действия отключают все стандартные службы, которые обычно включены в xinetd.

Состояние служб

Служба	Состояние
chargen	не установлено
chargen-udp	не установлено
cups	не установлено
cups-lpd	не установлено
daytime	не установлено
daytime-udp	не установлено
echo	не установлено
echo-udp	не установлено
eklogin	не установлено
ekrb5-telnet	не установлено
finger	не установлено
gssftp	не установлено
imap	не установлено
imaps	не установлено
ipop2	не установлено
ipop3	не установлено
klogin	не установлено
krb5-telnet	не установлено
kshell	не установлено
ktalk	не установлено
ntalk	не установлено
pop3s	не установлено
rexec	не установлено
rlogin	не установлено
rsh	не установлено
rsync	не установлено

servers	не установлено
services	не установлено
sgi_fam	не установлено
talk	не установлено
telnet	не установлено
tftp	не установлено
time	не установлено
time-udp	не установлено
vsftpd	не установлено
wu-ftp	не установлено

Как исправить

Отключите неиспользуемые стандартные службы.

Статусы транспортов

IP-адрес

10.1.1.3

Имя из задачи

10.1.1.3

Статусы транспортов

LDAP

отключен в профиле

MML

отключен в профиле

MongoDB

отключен в профиле

NotesRPC

отключен в профиле

ODBC DB2

отключен в профиле

ODBC MSSQL

отключен в профиле

ODBC MySQL

отключен в профиле

ODBC Oracle

отключен в профиле

ODBC PostgreSQL

отключен в профиле

ODBC Sybase

отключен в профиле

ODBC Teradata

отключен в профиле

ODBC Tiberio

отключен в профиле

RPC

отключен в профиле

RPC Filesystem

отключен в профиле

RPC Registry

отключен в профиле

Remote Engine

отключен в профиле

SAP GUI

отключен в профиле

SAP HANA

отключен в профиле

SAP HTTP

отключен в профиле

SAPRFC

отключен в профиле

SSH1

ошибка инициализации на сканере

SSH2

критических ошибок нет

TELNET

отключен в профиле

VMWARE

отключен в профиле

VMWARE vCenter

отключен в профиле

WMI

отключен в профиле

WMI FILESYSTEM

отключен в профиле

WMI REGISTRY

отключен в профиле

XEN

отключен в профиле

XENRPC

отключен в профиле

vSphere API

отключен в профиле

vSphere API vCenter

отключен в профиле

Ошибки транспортов

SSH1

Экземпляр	Описание ошибки	Статус ошибки
DEFAULT	Ошибка инициализации	7

Конец отчета MaxPatrol (сборка 40948)

© 2025 Positive Technologies

60