|  |  |  |
| --- | --- | --- |
| **Контрольный лист СЕРВЕР** |  |  |

|  |  |  |
| --- | --- | --- |
| **1. Общая информация** | | |
| **1.1. Имя АРМ** | **1.2. Домен** | **1.3. Имя пользователя** |
| S-DC-01 | sf33.local | SF33\admin |

|  |  |  |
| --- | --- | --- |
| **2. Операционная система** | | |
| **2.1. Выпуск ОС** | **2.2. Архитектура** | **2.3. Версия** |
| Microsoft Windows Server 2022 Standard | 64-bit | 10.0.20348 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **3. Сетевая конфигурация** | | | | |
| **3.1. Имя адаптера** | **3.2. IP адрес** | **3.3. Gateway** | **3.4. DNS** | **3.5. MAC** |
| Ethernet | 192.168.94.10 | 192.168.94.20 | 192.168.94.10 192.168.94.11 192.168.94.20 | 32-A5-37-DB-AA-6F |

|  |  |  |  |
| --- | --- | --- | --- |
| **4. Служба времени** | | | |
| **4.1. Служба NTP** | **4.2. IP NTP** | **4.3. Time zone** | **4.4. Последняя синхронизация** |
| Служба работает | 0.pool.ntp.org | (UTC+03:00) Moscow, St. Petersburg | None |

|  |  |  |  |
| --- | --- | --- | --- |
| **5. Обновления ОС** | | | |
| **5.1. Служба WSUS** | **5.2. Сервер WSUS IP** | **5.3. Последние обновления** | **5.4. Общее число обновлений** |
| Служба работает (Статус: 'Running') | None | KB5031590 from 28.10.2023 KB5031993 from 14.01.2024 KB5031364 from 28.10.2023 | 3 |

|  |  |  |  |
| --- | --- | --- | --- |
| **6. Учетные записи** | | | |
| **6.1. Имя** | **6.2. Статус** | **6.3. Членство в группах** | **6.4. Описание** |
| Admin | Активен | Administrators |  |
| Administrator | Отключен | Administrators | Built-in account for administering the computer/domain |
| Bind | Активен | None |  |
| Guest | Отключен | Guests | Built-in account for guest access to the computer/domain |
| Krbtgt | Отключен | Denied RODC Password Replication Group | Key Distribution Center Service Account |
| User01 | Активен | None | Basic user |
| User02 | Активен | None | Basic user |
| User03 | Активен | None | Basic user |
| User04 | Активен | None |  |
| User04.Sec | Активен | None | Security Engineer |

|  |  |  |
| --- | --- | --- |
| **7. Группы** | | |
| **7.1. Имя** | **7.2. Члены группы** | **7.3. Стандартная** |
| Access Control Assistance Operators |  | Нет |
| Account Operators |  | Нет |
| Administrators | Administrator admin Enterprise Admins Domain Admins | Нет |
| Allowed RODC Password Replication Group |  | Нет |
| Backup Operators |  | Нет |
| Cert Publishers |  | Нет |
| Certificate Service DCOM Access |  | Нет |
| Cryptographic Operators |  | Нет |
| DHCP Administrators |  | Нет |
| DHCP Users |  | Нет |
| Denied RODC Password Replication Group | krbtgt Domain Controllers Schema Admins Enterprise Admins Cert Publishers Domain Admins Group Policy Creator Owners Read-only Domain Controllers | Нет |
| Distributed COM Users |  | Нет |
| DnsAdmins |  | Нет |
| Event Log Readers |  | Нет |
| Guests | Guest Domain Guests | Нет |
| Hyper-V Administrators |  | Нет |
| IIS\_IUSRS | IUSR | Да |
| Incoming Forest Trust Builders |  | Нет |
| KAVWSEE Administrators |  | Нет |
| Network Configuration Operators |  | Нет |
| Performance Log Users |  | Нет |
| Performance Monitor Users |  | Нет |
| Pre-Windows 2000 Compatible Access | Authenticated Users | Нет |
| Print Operators |  | Нет |
| RAS and IAS Servers |  | Нет |
| RDS Endpoint Servers |  | Нет |
| RDS Management Servers |  | Нет |
| RDS Remote Access Servers |  | Нет |
| Remote Desktop Users |  | Нет |
| Remote Management Users |  | Нет |
| Replicator |  | Нет |
| Server Operators |  | Нет |
| Storage Replica Administrators |  | Нет |
| Terminal Server License Servers |  | Нет |
| Users | INTERACTIVE Authenticated Users Domain Users | Нет |
| Windows Authorization Access Group | ENTERPRISE DOMAIN CONTROLLERS | Нет |

|  |  |  |
| --- | --- | --- |
| **8. Общие папки** | | |
| **8.1. Название ресурса** | **8.2. Путь** | **8.3. Описание** |
| ADMIN$ | C:\Windows | Remote Admin |
| C$ | C:\ | Default share |
| IPC$ |  | Remote IPC |
| NETLOGON | C:\Windows\SYSVOL\sysvol\sf33.local\SCRIPTS | Logon server share |
| SYSVOL | C:\Windows\SYSVOL\sysvol | Logon server share |

|  |  |  |  |
| --- | --- | --- | --- |
| **9. АВЗ** | | | |
| **9.1. Название АВЗ** | **9.2. Версия** | **9.3. Сервер** | **9.4. Актуальность баз** |
| None | None | None | None |

|  |  |  |  |
| --- | --- | --- | --- |
| **10. Программное обеспечение** | | | |
| **№ п/п** | **10. 1. Название ПО** | **10.2 Версия** | **10.3 Входит в перечень** |
| 1. | Microsoft Edge | 122.0.2365.92 | Нет |
| 2. | Microsoft Edge Update | 1.3.185.21 | Нет |
| 3. | Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.32.31326 | 14.32.31326.0 | Нет |
| 4. | Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.32.31326 | 14.32.31326.0 | Нет |
| 5. | Microsoft Visual C++ 2022 X64 Additional Runtime - 14.32.31326 | 14.32.31326 | Нет |
| 6. | Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.32.31326 | 14.32.31326 | Нет |
| 7. | Microsoft Visual C++ 2022 X86 Additional Runtime - 14.32.31326 | 14.32.31326 | Нет |
| 8. | Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.32.31326 | 14.32.31326 | Нет |
| 9. | QEMU guest agent | 105.0.2 | Нет |
| 10. | SPICE Guest Tools 0.141 | 0.141 | Нет |
| 11. | Spice webdavd 2.4 (64-bit) | 2.4.0 | Нет |
| 12. | UsbDk Runtime Libraries | 1.0.22 | Нет |
| 13. | usbredirect 0.13.0 (64-bit) | 0.13.0 | Нет |
| 14. | Virtio-win-driver-installer | 0.1.229 | Нет |
| 15. | VMware Tools | 12.1.0.20219665 | Нет |
| 16. | Wazuh Agent | 4.5.4 | Нет |

|  |  |
| --- | --- |
| **11. Парольная политика** | |
| **11.1. Принудительный выход по истечении времени через:** | Never |
| **11.2. Минимальный срок действия пароля (дней):** | 1 |
| **11.3. Максимальный срок действия пароля (дней):** | 42 |
| **11.4.** **Минимальная длина пароля:** | 7 |
| **11.5. Хранение неповторяющихся паролей:** | 24 |
| **11.6. Блокировка после ошибок ввода пароля:** | Never |
| **11.7.** **Длительность блокировки (минут):** | 10 |
| **11.8.** **Сброс счетчика блокировок через (минут):** | 10 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Замечания по разделам** | | □ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10 □ 11 □ 12 □ 13 □ 14 □ 15 □ 16 □ 17 | | | | |
| **Дополнительно** | |  | | | | |
|  | | | | | | |
|  | | | | | | |
| **СЕРВЕР требованиям соответствует** | | | | □ Да □ Нет |  | |
| **Заполнил**  **(ФИО, подпись, дата)** |  | |  | **Ознакомлен (ФИО, подпись, дата)** |  |  |
| «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_20 | | | «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_20 | |

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ УКАЗАНА В ПРИЛОЖЕНИИ № 1

Приложение № 1

|  |  |  |
| --- | --- | --- |
| **12. Автозагрузка** | | |
| **№ п/п** | **Название ПО** | **Расположение** |
| 1. | AzureArcSetup | C:\Windows\AzureArcSetup\Systray\AzureArcSysTray.exe |
| 2. | SecurityHealth | C:\Windows\system32\SecurityHealthSystray.exe |
| 3. | VMware User Process | "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr |

|  |  |  |  |
| --- | --- | --- | --- |
| **13. Планировщик заданий** | | | |
| **№ п/п** | **Название задания** | **Статус** | **Автор задания** |
| 1. | MicrosoftEdgeUpdateTaskMachineCore | Ready | None |
| 2. | MicrosoftEdgeUpdateTaskMachineSys | Ready | SF33\admin |
| 3. | MicrosoftEdgeUpdateTaskMachineUA | Ready | None |

|  |  |  |  |
| --- | --- | --- | --- |
| **14. Роли и компоненты** | | | |
| **№ п/п** | **Название роли** | **Статус** | **Описание** |
| 1. | AD-Domain-Services | Installed | Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process. |
| 2. | AzureArcSetup | Installed | Provides the services that are needed to configure Azure Arc. |
| 3. | DHCP | Installed | Dynamic Host Configuration Protocol (DHCP) Server enables you to centrally configure, manage, and provide temporary IP addresses and related information for client computers. |
| 4. | DNS | Installed | Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together. |
| 5. | FileAndStorage-Services | Installed | File and Storage Services includes services that are always installed, as well as functionality that you can install to help manage file servers and storage. |
| 6. | File-Services | Installed | File and iSCSI Services provides technologies that help you manage file servers and storage, reduce disk space utilization, replicate and cache files to branch offices, move or fail over a file share to another cluster node, and share files by using the NFS protocol. |
| 7. | FS-FileServer | Installed | File Server manages shared folders and enables users to access files on this computer from the network. |
| 8. | GPMC | Installed | Group Policy Management is a scriptable Microsoft Management Console (MMC) snap-in, providing a single administrative tool for managing Group Policy across the enterprise. Group Policy Management is the standard tool for managing Group Policy. |
| 9. | NET-Framework-45-Core | Installed | .NET Framework 4.8 provides a comprehensive and consistent programming model for quickly and easily building and running applications that are built for various platforms including desktop PCs, Servers, smart phones and the public and private cloud. |
| 10. | NET-Framework-45-Features | Installed | .NET Framework 4.8 provides a comprehensive and consistent programming model for quickly and easily building and running applications that are built for various platforms including desktop PCs, Servers, smart phones and the public and private cloud. |
| 11. | NET-Framework-Core | Removed | .NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes. |
| 12. | NET-WCF-Services45 | Installed | Windows Communication Foundation (WCF) Activation uses Windows Process Activation Service to invoke applications remotely over the network by using protocols such as HTTP, Message Queuing, TCP, and named pipes. Consequently, applications can start and stop dynamically in response to incoming work items, resulting in application hosting that is more robust, manageable, and efficient. |
| 13. | NET-WCF-TCP-PortSharing45 | Installed | TCP Port Sharing allows multiple net.tcp applications to share a single TCP port. Consequently, these applications can coexist on the same physical computer in separate, isolated processes, while sharing the network infrastructure required to send and receive traffic over a TCP port, such as port 808. |
| 14. | PowerShell | Installed | Windows PowerShell enables you to automate local and remote Windows administration. This task-based command-line shell and scripting language is built on the Microsoft .NET Framework. It includes hundreds of built-in commands and lets you write and distribute your own commands and scripts. |
| 15. | PowerShellRoot | Installed | Windows PowerShell enables you to automate local and remote Windows administration. This task-based command-line shell and scripting language is built on the Microsoft .NET Framework. It includes hundreds of built-in commands and lets you write and distribute your own commands and scripts. |
| 16. | PowerShell-V2 | Removed | Windows PowerShell 2.0 Engine includes the core components from Windows PowerShell 2.0 for backward compatibility with existing Windows PowerShell host applications. |
| 17. | RSAT | Installed | Remote Server Administration Tools includes snap-ins and command-line tools for remotely managing roles and features. |
| 18. | RSAT-AD-AdminCenter | Installed | Active Directory Administrative Center provides users and network administrators with an enhanced Active Directory data management experience and a rich graphical user interface (GUI) to perform common Active Directory object management tasks. |
| 19. | RSAT-ADDS | Installed | Active Directory Domain Services (AD DS) Tools includes snap-ins and command-line tools for remotely managing AD DS. |
| 20. | RSAT-ADDS-Tools | Installed | Active Directory Domain Services Snap-Ins and Command-Line Tools includes Active Directory Users and Computers, Active Directory Domains and Trusts, Active Directory Sites and Services, and other snap-ins and command-line tools for remotely managing Active Directory domain controllers. |
| 21. | RSAT-AD-PowerShell | Installed | The Active Directory module for Windows PowerShel and the tools it provides can be used by Active Directory administrators to manage Active Directory Domain Services (AD DS) at the command line. |
| 22. | RSAT-AD-Tools | Installed | Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS) Tools includes snap-ins and command-line tools for remotely managing AD DS and AD LDS. |
| 23. | RSAT-DHCP | Installed | DHCP Server Tools includes the DHCP MMC snap-in, DHCP server netsh context and Windows PowerShell module for DHCP Server. |
| 24. | RSAT-DNS-Server | Installed | DNS Server Tools includes the DNS Manager snap-in, dnscmd.exe command-line tool and Windows PowerShell module for DNS Server. |
| 25. | RSAT-Role-Tools | Installed | Role Administration Tools includes snap-ins and command-line tools for remotely managing roles. |
| 26. | Storage-Services | Installed | Storage Services provides storage management functionality that is always installed and cannot be removed. |
| 27. | System-DataArchiver | Installed | Provides services to collect and archive Windows Server system data. |
| 28. | WoW64-Support | Installed | Includes all of WoW64 to support running 32-bit applications on Server Core installations. This feature is required for full Server installations. Uninstalling WoW64 Support will convert a full Server installation into a Server Core installation. |
| 29. | XPS-Viewer | Installed | The XPS Viewer is used to read, set permissions for, and digitally sign XPS documents. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **15. Службы** | | | | | |
| **№ п/п** | **Название службы** | **Режим запуска** | **Статус** | **Имя службы** | **Путь** |
| 1. | Active Directory Domain Services | Автоматически | Выполняется | NTDS | C:\Windows\System32\lsass.exe |
| 2. | Active Directory Web Services | Автоматически | Выполняется | ADWS | C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe |
| 3. | ActiveX Installer (AxInstSV) | Отключена | Остановлена | AxInstSV | C:\Windows\system32\svchost.exe -k AxInstSVGroup |
| 4. | AllJoyn Router Service | Вручную | Остановлена | AJRouter | C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p |
| 5. | App Readiness | Вручную | Остановлена | AppReadiness | C:\Windows\System32\svchost.exe -k AppReadiness -p |
| 6. | Application Identity | Вручную | Остановлена | AppIDSvc | C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p |
| 7. | Application Information | Вручную | Выполняется | Appinfo | C:\Windows\system32\svchost.exe -k netsvcs -p |
| 8. | Application Layer Gateway Service | Вручную | Остановлена | ALG | C:\Windows\System32\alg.exe |
| 9. | Application Management | Вручную | Остановлена | AppMgmt | C:\Windows\system32\svchost.exe -k netsvcs -p |
| 10. | AppX Deployment Service (AppXSVC) | Вручную | Выполняется | AppXSvc | C:\Windows\system32\svchost.exe -k wsappx -p |
| 11. | Auto Time Zone Updater | Отключена | Остановлена | tzautoupdate | C:\Windows\system32\svchost.exe -k LocalService -p |
| 12. | Background Intelligent Transfer Service | Вручную | Остановлена | BITS | C:\Windows\System32\svchost.exe -k netsvcs -p |
| 13. | Background Tasks Infrastructure Service | Автоматически | Выполняется | BrokerInfrastructure | C:\Windows\system32\svchost.exe -k DcomLaunch -p |
| 14. | BalloonService | Автоматически | Выполняется | BalloonService | "C:\Program Files\Virtio-Win\Balloon\blnsvr.exe" |
| 15. | Base Filtering Engine | Автоматически | Выполняется | BFE | C:\Windows\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p |
| 16. | Bluetooth Support Service | Вручную | Остановлена | bthserv | C:\Windows\system32\svchost.exe -k LocalService -p |
| 17. | Capability Access Manager Service | Вручную | Выполняется | camsvc | C:\Windows\system32\svchost.exe -k appmodel -p |
| 18. | CaptureService\_111ae3 | Вручную | Остановлена | CaptureService | C:\Windows\system32\svchost.exe -k LocalService -p |
| 19. | Certificate Propagation | Вручную | Остановлена | CertPropSvc | C:\Windows\system32\svchost.exe -k netsvcs |
| 20. | Client License Service (ClipSVC) | Вручную | Остановлена | ClipSVC | C:\Windows\System32\svchost.exe -k wsappx -p |
| 21. | Clipboard User Service\_111ae3 | Автоматически | Выполняется | cbdhsvc | C:\Windows\system32\svchost.exe -k ClipboardSvcGroup -p |
| 22. | CNG Key Isolation | Вручную | Выполняется | KeyIso | C:\Windows\system32\lsass.exe |
| 23. | COM+ Event System | Автоматически | Выполняется | EventSystem | C:\Windows\system32\svchost.exe -k LocalService -p |
| 24. | COM+ System Application | Вручную | Остановлена | COMSysApp | C:\Windows\system32\dllhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235} |
| 25. | Connected Devices Platform Service | Автоматически | Выполняется | CDPSvc | C:\Windows\system32\svchost.exe -k LocalService -p |
| 26. | Connected Devices Platform User Service\_111ae3 | Автоматически | Выполняется | CDPUserSvc | C:\Windows\system32\svchost.exe -k UnistackSvcGroup |
| 27. | Connected User Experiences and Telemetry | Автоматически | Выполняется | DiagTrack | C:\Windows\System32\svchost.exe -k utcsvc -p |
| 28. | ConsentUX User Service\_111ae3 | Вручную | Остановлена | ConsentUxUserSvc | C:\Windows\system32\svchost.exe -k DevicesFlow |
| 29. | Contact Data\_111ae3 | Вручную | Остановлена | PimIndexMaintenanceSvc | C:\Windows\system32\svchost.exe -k UnistackSvcGroup |
| 30. | CoreMessaging | Автоматически | Выполняется | CoreMessagingRegistrar | C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p |
| 31. | Credential Manager | Вручную | Остановлена | VaultSvc | C:\Windows\system32\lsass.exe |
| 32. | CredentialEnrollmentManagerUserSvc\_111ae3 | Вручную | Остановлена | CredentialEnrollmentManagerUserSvc | C:\Windows\system32\CredentialEnrollmentManager.exe |
| 33. | Cryptographic Services | Автоматически | Выполняется | CryptSvc | C:\Windows\system32\svchost.exe -k catdbsvcs -p |
| 34. | Data Sharing Service | Вручную | Остановлена | DsSvc | C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 35. | DCOM Server Process Launcher | Автоматически | Выполняется | DcomLaunch | C:\Windows\system32\svchost.exe -k DcomLaunch -p |
| 36. | dcsvc | Вручную | Остановлена | dcsvc | C:\Windows\system32\svchost.exe -k netsvcs -p |
| 37. | Delivery Optimization | Вручную | Остановлена | DoSvc | C:\Windows\System32\svchost.exe -k NetworkService -p |
| 38. | Device Association Service | Вручную | Остановлена | DeviceAssociationService | C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 39. | Device Install Service | Вручную | Остановлена | DeviceInstall | C:\Windows\system32\svchost.exe -k DcomLaunch -p |
| 40. | Device Management Enrollment Service | Вручную | Остановлена | DmEnrollmentSvc | C:\Windows\system32\svchost.exe -k netsvcs -p |
| 41. | Device Management Wireless Application Protocol (WAP) Push message Routing Service | Отключена | Остановлена | dmwappushservice | C:\Windows\system32\svchost.exe -k netsvcs -p |
| 42. | Device Setup Manager | Вручную | Выполняется | DsmSvc | C:\Windows\system32\svchost.exe -k netsvcs -p |
| 43. | DeviceAssociationBroker\_111ae3 | Вручную | Остановлена | DeviceAssociationBrokerSvc | C:\Windows\system32\svchost.exe -k DevicesFlow -p |
| 44. | DevicePicker\_111ae3 | Отключена | Остановлена | DevicePickerUserSvc | C:\Windows\system32\svchost.exe -k DevicesFlow |
| 45. | DevicesFlow\_111ae3 | Вручную | Остановлена | DevicesFlowUserSvc | C:\Windows\system32\svchost.exe -k DevicesFlow |
| 46. | DevQuery Background Discovery Broker | Вручную | Остановлена | DevQueryBroker | C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 47. | DFS Namespace | Автоматически | Выполняется | Dfs | C:\Windows\system32\dfssvc.exe |
| 48. | DFS Replication | Автоматически | Выполняется | DFSR | C:\Windows\system32\DFSRs.exe |
| 49. | DHCP Client | Автоматически | Выполняется | Dhcp | C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p |
| 50. | DHCP Server | Автоматически | Выполняется | DHCPServer | C:\Windows\system32\svchost.exe -k DHCPServer -p |
| 51. | Diagnostic Policy Service | Автоматически | Выполняется | DPS | C:\Windows\System32\svchost.exe -k LocalServiceNoNetwork -p |
| 52. | Diagnostic Service Host | Вручную | Выполняется | WdiServiceHost | C:\Windows\System32\svchost.exe -k LocalService -p |
| 53. | Diagnostic System Host | Вручную | Выполняется | WdiSystemHost | C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 54. | Display Policy Service | Автоматически | Выполняется | DispBrokerDesktopSvc | C:\Windows\system32\svchost.exe -k LocalService -p |
| 55. | Distributed Link Tracking Client | Вручную | Остановлена | TrkWks | C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 56. | Distributed Transaction Coordinator | Автоматически | Выполняется | MSDTC | C:\Windows\System32\msdtc.exe |
| 57. | DNS Client | Автоматически | Выполняется | Dnscache | C:\Windows\system32\svchost.exe -k NetworkService -p |
| 58. | DNS Server | Автоматически | Выполняется | DNS | C:\Windows\system32\dns.exe |
| 59. | Downloaded Maps Manager | Отключена | Остановлена | MapsBroker | C:\Windows\System32\svchost.exe -k NetworkService -p |
| 60. | DS Role Server | Вручную | Остановлена | DsRoleSvc | C:\Windows\System32\lsass.exe |
| 61. | Embedded Mode | Вручную | Остановлена | embeddedmode | C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 62. | Encrypting File System (EFS) | Автоматически | Выполняется | EFS | C:\Windows\System32\lsass.exe |
| 63. | Enterprise App Management Service | Вручную | Остановлена | EntAppSvc | C:\Windows\system32\svchost.exe -k appmodel -p |
| 64. | Extensible Authentication Protocol | Вручную | Остановлена | EapHost | C:\Windows\System32\svchost.exe -k netsvcs -p |
| 65. | File Replication | Отключена | Остановлена | NtFrs | C:\Windows\system32\ntfrs.exe |
| 66. | Function Discovery Provider Host | Вручную | Остановлена | fdPHost | C:\Windows\system32\svchost.exe -k LocalService -p |
| 67. | Function Discovery Resource Publication | Вручную | Остановлена | FDResPub | C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p |
| 68. | Geolocation Service | Отключена | Остановлена | lfsvc | C:\Windows\system32\svchost.exe -k netsvcs -p |
| 69. | GraphicsPerfSvc | Отключена | Остановлена | GraphicsPerfSvc | C:\Windows\System32\svchost.exe -k GraphicsPerfSvcGroup |
| 70. | Group Policy Client | Автоматически | Выполняется | gpsvc | C:\Windows\system32\svchost.exe -k netsvcs -p |
| 71. | Human Interface Device Service | Вручную | Остановлена | hidserv | C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 72. | HV Host Service | Вручную | Остановлена | HvHost | C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 73. | Hyper-V Data Exchange Service | Вручную | Остановлена | vmickvpexchange | C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 74. | Hyper-V Guest Service Interface | Вручную | Остановлена | vmicguestinterface | C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 75. | Hyper-V Guest Shutdown Service | Вручную | Остановлена | vmicshutdown | C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 76. | Hyper-V Heartbeat Service | Вручную | Остановлена | vmicheartbeat | C:\Windows\system32\svchost.exe -k ICService -p |
| 77. | Hyper-V PowerShell Direct Service | Вручную | Остановлена | vmicvmsession | C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 78. | Hyper-V Time Synchronization Service | Вручную | Остановлена | vmictimesync | C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p |
| 79. | Hyper-V Volume Shadow Copy Requestor | Вручную | Остановлена | vmicvss | C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 80. | IKE and AuthIP IPsec Keying Modules | Автоматически | Выполняется | IKEEXT | C:\Windows\system32\svchost.exe -k netsvcs -p |
| 81. | Internet Connection Sharing (ICS) | Отключена | Остановлена | SharedAccess | C:\Windows\System32\svchost.exe -k netsvcs -p |
| 82. | Intersite Messaging | Автоматически | Выполняется | IsmServ | C:\Windows\System32\ismserv.exe |
| 83. | IP Helper | Автоматически | Выполняется | iphlpsvc | C:\Windows\System32\svchost.exe -k NetSvcs -p |
| 84. | IPsec Policy Agent | Вручную | Выполняется | PolicyAgent | C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted -p |
| 85. | KDC Proxy Server service (KPS) | Вручную | Остановлена | KPSSVC | C:\Windows\system32\svchost.exe -k KpsSvcGroup |
| 86. | Kerberos Key Distribution Center | Автоматически | Выполняется | Kdc | C:\Windows\System32\lsass.exe |
| 87. | KtmRm for Distributed Transaction Coordinator | Вручную | Остановлена | KtmRm | C:\Windows\System32\svchost.exe -k NetworkServiceAndNoImpersonation -p |
| 88. | Link-Layer Topology Discovery Mapper | Отключена | Остановлена | lltdsvc | C:\Windows\System32\svchost.exe -k LocalService -p |
| 89. | Local Session Manager | Автоматически | Выполняется | LSM | C:\Windows\system32\svchost.exe -k DcomLaunch -p |
| 90. | McpManagementService | Вручную | Остановлена | McpManagementService | C:\Windows\system32\svchost.exe -k McpManagementServiceGroup |
| 91. | Microsoft (R) Diagnostics Hub Standard Collector Service | Вручную | Остановлена | diagnosticshub.standardcollector.service | C:\Windows\system32\DiagSvcs\DiagnosticsHub.StandardCollector.Service.exe |
| 92. | Microsoft Account Sign-in Assistant | Вручную | Выполняется | wlidsvc | C:\Windows\system32\svchost.exe -k netsvcs -p |
| 93. | Microsoft App-V Client | Отключена | Остановлена | AppVClient | C:\Windows\system32\AppVClient.exe |
| 94. | Microsoft Edge Elevation Service (MicrosoftEdgeElevationService) | Вручную | Остановлена | MicrosoftEdgeElevationService | "C:\Program Files (x86)\Microsoft\Edge\Application\122.0.2365.92\elevation\_service.exe" |
| 95. | Microsoft Edge Update Service (edgeupdate) | Автоматически | Остановлена | edgeupdate | "C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /svc |
| 96. | Microsoft Edge Update Service (edgeupdatem) | Вручную | Остановлена | edgeupdatem | "C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /medsvc |
| 97. | Microsoft iSCSI Initiator Service | Вручную | Остановлена | MSiSCSI | C:\Windows\system32\svchost.exe -k netsvcs -p |
| 98. | Microsoft Key Distribution Service | Вручную | Остановлена | KdsSvc | C:\Windows\system32\lsass.exe |
| 99. | Microsoft Passport | Вручную | Остановлена | NgcSvc | C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 100. | Microsoft Passport Container | Вручную | Остановлена | NgcCtnrSvc | C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p |
| 101. | Microsoft Software Shadow Copy Provider | Вручную | Остановлена | swprv | C:\Windows\System32\svchost.exe -k swprv |
| 102. | Microsoft Storage Spaces SMP | Вручную | Остановлена | smphost | C:\Windows\System32\svchost.exe -k smphost |
| 103. | Microsoft Store Install Service | Вручную | Остановлена | InstallService | C:\Windows\System32\svchost.exe -k netsvcs -p |
| 104. | MicrosoftEdgeUpdateSys64 | Автоматически | Выполняется | MicrosoftEdgeUpdateSys64 | C:\Windows\MicrosoftEdgeUpdateSys64.exe |
| 105. | Net.Tcp Port Sharing Service | Отключена | Остановлена | NetTcpPortSharing | C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe |
| 106. | Netlogon | Автоматически | Выполняется | Netlogon | C:\Windows\system32\lsass.exe |
| 107. | Network Connection Broker | Вручную | Выполняется | NcbService | C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 108. | Network Connections | Вручную | Остановлена | Netman | C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 109. | Network Connectivity Assistant | Вручную | Остановлена | NcaSvc | C:\Windows\System32\svchost.exe -k NetSvcs -p |
| 110. | Network List Service | Вручную | Выполняется | netprofm | C:\Windows\System32\svchost.exe -k LocalService -p |
| 111. | Network Location Awareness | Автоматически | Выполняется | NlaSvc | C:\Windows\System32\svchost.exe -k NetworkService -p |
| 112. | Network Setup Service | Вручную | Остановлена | NetSetupSvc | C:\Windows\System32\svchost.exe -k netsvcs -p |
| 113. | Network Store Interface Service | Автоматически | Выполняется | nsi | C:\Windows\system32\svchost.exe -k LocalService -p |
| 114. | Offline Files | Отключена | Остановлена | CscService | C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 115. | OpenSSH Authentication Agent | Отключена | Остановлена | ssh-agent | C:\Windows\System32\OpenSSH\ssh-agent.exe |
| 116. | Optimize drives | Вручную | Остановлена | defragsvc | C:\Windows\system32\svchost.exe -k defragsvc |
| 117. | Payments and NFC/SE Manager | Отключена | Остановлена | SEMgrSvc | C:\Windows\system32\svchost.exe -k LocalService -p |
| 118. | Performance Counter DLL Host | Вручную | Остановлена | PerfHost | C:\Windows\SysWow64\perfhost.exe |
| 119. | Performance Logs & Alerts | Вручную | Выполняется | pla | C:\Windows\System32\svchost.exe -k LocalServiceNoNetwork -p |
| 120. | Plug and Play | Вручную | Выполняется | PlugPlay | C:\Windows\system32\svchost.exe -k DcomLaunch -p |
| 121. | Portable Device Enumerator Service | Вручную | Остановлена | WPDBusEnum | C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted |
| 122. | Power | Автоматически | Выполняется | Power | C:\Windows\system32\svchost.exe -k DcomLaunch -p |
| 123. | Print Spooler | Автоматически | Выполняется | Spooler | C:\Windows\System32\spoolsv.exe |
| 124. | Printer Extensions and Notifications | Вручную | Остановлена | PrintNotify | C:\Windows\system32\svchost.exe -k print |
| 125. | PrintWorkflow\_111ae3 | Вручную | Остановлена | PrintWorkflowUserSvc | C:\Windows\system32\svchost.exe -k PrintWorkflow |
| 126. | Problem Reports Control Panel Support | Вручную | Остановлена | wercplsupport | C:\Windows\System32\svchost.exe -k netsvcs -p |
| 127. | Program Compatibility Assistant Service | Автоматически | Выполняется | PcaSvc | C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 128. | QEMU Guest Agent | Автоматически | Выполняется | QEMU-GA | "C:\Program Files\Qemu-ga\qemu-ga.exe" -d --retry-path |
| 129. | QEMU Guest Agent VSS Provider | Вручную | Остановлена | QEMU Guest Agent VSS Provider | C:\Windows\system32\dllhost.exe /Processid:{2BCD010C-3749-4056-96A7-2907FDDF8BA0} |
| 130. | Quality Windows Audio Video Experience | Вручную | Остановлена | QWAVE | C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p |
| 131. | Radio Management Service | Отключена | Остановлена | RmSvc | C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted |
| 132. | Remote Access Auto Connection Manager | Вручную | Остановлена | RasAuto | C:\Windows\System32\svchost.exe -k netsvcs -p |
| 133. | Remote Access Connection Manager | Автоматически | Выполняется | RasMan | C:\Windows\System32\svchost.exe -k netsvcs |
| 134. | Remote Desktop Configuration | Вручную | Остановлена | SessionEnv | C:\Windows\System32\svchost.exe -k netsvcs -p |
| 135. | Remote Desktop Services | Вручную | Остановлена | TermService | C:\Windows\System32\svchost.exe -k termsvcs |
| 136. | Remote Desktop Services UserMode Port Redirector | Вручную | Остановлена | UmRdpService | C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 137. | Remote Procedure Call (RPC) | Автоматически | Выполняется | RpcSs | C:\Windows\system32\svchost.exe -k rpcss -p |
| 138. | Remote Procedure Call (RPC) Locator | Вручную | Остановлена | RpcLocator | C:\Windows\system32\locator.exe |
| 139. | Remote Registry | Автоматически | Выполняется | RemoteRegistry | C:\Windows\system32\svchost.exe -k localService -p |
| 140. | Resultant Set of Policy Provider | Вручную | Остановлена | RSoPProv | C:\Windows\system32\RSoPProv.exe |
| 141. | Routing and Remote Access | Отключена | Остановлена | RemoteAccess | C:\Windows\System32\svchost.exe -k netsvcs |
| 142. | RPC Endpoint Mapper | Автоматически | Выполняется | RpcEptMapper | C:\Windows\system32\svchost.exe -k RPCSS -p |
| 143. | Secondary Logon | Вручную | Остановлена | seclogon | C:\Windows\system32\svchost.exe -k netsvcs -p |
| 144. | Secure Socket Tunneling Protocol Service | Вручную | Выполняется | SstpSvc | C:\Windows\system32\svchost.exe -k LocalService -p |
| 145. | Security Accounts Manager | Автоматически | Выполняется | SamSs | C:\Windows\system32\lsass.exe |
| 146. | Sensor Data Service | Отключена | Остановлена | SensorDataService | C:\Windows\System32\SensorDataService.exe |
| 147. | Sensor Monitoring Service | Вручную | Остановлена | SensrSvc | C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p |
| 148. | Sensor Service | Вручную | Остановлена | SensorService | C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 149. | Server | Автоматически | Выполняется | LanmanServer | C:\Windows\System32\svchost.exe -k smbsvcs |
| 150. | Shared PC Account Manager | Отключена | Остановлена | shpamsvc | C:\Windows\System32\svchost.exe -k netsvcs -p |
| 151. | Shell Hardware Detection | Автоматически | Выполняется | ShellHWDetection | C:\Windows\System32\svchost.exe -k netsvcs -p |
| 152. | Smart Card | Вручную | Остановлена | SCardSvr | C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation |
| 153. | Smart Card Device Enumeration Service | Отключена | Остановлена | ScDeviceEnum | C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted |
| 154. | Smart Card Removal Policy | Вручную | Остановлена | SCPolicySvc | C:\Windows\system32\svchost.exe -k netsvcs |
| 155. | SNMP Trap | Вручную | Остановлена | SNMPTRAP | C:\Windows\System32\snmptrap.exe |
| 156. | Software Protection | Автоматически | Выполняется | sppsvc | C:\Windows\system32\sppsvc.exe |
| 157. | Special Administration Console Helper | Вручную | Остановлена | sacsvr | C:\Windows\System32\svchost.exe -k netsvcs -p |
| 158. | SPICE VDAgent | Автоматически | Выполняется | vdservice | "C:\Program Files (x86)\SPICE Guest Tools\64\vdservice.exe" |
| 159. | Spice webdav proxy | Автоматически | Остановлена | spice-webdavd | "C:\Program Files\SPICE webdavd\bin\spice-webdavd.exe" -p 9843 |
| 160. | Spot Verifier | Вручную | Остановлена | svsvc | C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 161. | SSDP Discovery | Отключена | Остановлена | SSDPSRV | C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p |
| 162. | State Repository Service | Автоматически | Выполняется | StateRepository | C:\Windows\system32\svchost.exe -k appmodel -p |
| 163. | Still Image Acquisition Events | Вручную | Остановлена | WiaRpc | C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 164. | Storage Service | Автоматически | Выполняется | StorSvc | C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 165. | Storage Tiers Management | Вручную | Остановлена | TieringEngineService | C:\Windows\system32\TieringEngineService.exe |
| 166. | SysMain | Автоматически | Выполняется | SysMain | C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 167. | System Event Notification Service | Автоматически | Выполняется | SENS | C:\Windows\system32\svchost.exe -k netsvcs -p |
| 168. | System Events Broker | Автоматически | Выполняется | SystemEventsBroker | C:\Windows\system32\svchost.exe -k DcomLaunch -p |
| 169. | System Guard Runtime Monitor Broker | Вручную | Остановлена | SgrmBroker | C:\Windows\system32\SgrmBroker.exe |
| 170. | Task Scheduler | Автоматически | Выполняется | Schedule | C:\Windows\system32\svchost.exe -k netsvcs -p |
| 171. | TCP/IP NetBIOS Helper | Вручную | Выполняется | lmhosts | C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p |
| 172. | Telephony | Вручную | Остановлена | tapisrv | C:\Windows\System32\svchost.exe -k NetworkService -p |
| 173. | Themes | Автоматически | Выполняется | Themes | C:\Windows\System32\svchost.exe -k netsvcs -p |
| 174. | Time Broker | Вручную | Выполняется | TimeBrokerSvc | C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p |
| 175. | Touch Keyboard and Handwriting Panel Service | Вручную | Выполняется | TabletInputService | C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 176. | Udk User Service\_111ae3 | Вручную | Остановлена | UdkUserSvc | C:\Windows\system32\svchost.exe -k UdkSvcGroup |
| 177. | Update Orchestrator Service | Автоматически | Выполняется | UsoSvc | C:\Windows\system32\svchost.exe -k netsvcs -p |
| 178. | UPnP Device Host | Отключена | Остановлена | upnphost | C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p |
| 179. | User Access Logging Service | Автоматически | Выполняется | UALSVC | C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 180. | User Data Access\_111ae3 | Вручную | Остановлена | UserDataSvc | C:\Windows\system32\svchost.exe -k UnistackSvcGroup |
| 181. | User Data Storage\_111ae3 | Вручную | Остановлена | UnistoreSvc | C:\Windows\System32\svchost.exe -k UnistackSvcGroup |
| 182. | User Experience Virtualization Service | Отключена | Остановлена | UevAgentService | C:\Windows\system32\AgentService.exe |
| 183. | User Manager | Автоматически | Выполняется | UserManager | C:\Windows\system32\svchost.exe -k netsvcs -p |
| 184. | User Profile Service | Автоматически | Выполняется | ProfSvc | C:\Windows\system32\svchost.exe -k netsvcs -p |
| 185. | VirtIO-FS Service | Вручную | Остановлена | VirtioFsSvc | "C:\Program Files\Virtio-Win\VioFS\virtiofs.exe" |
| 186. | Virtual Disk | Вручную | Выполняется | vds | C:\Windows\System32\vds.exe |
| 187. | VMware Alias Manager and Ticket Service | Автоматически | Выполняется | VGAuthService | "C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe" |
| 188. | VMware Snapshot Provider | Вручную | Остановлена | vmvss | C:\Windows\system32\dllhost.exe /Processid:{68F84A1B-86C5-4461-9A69-F897E5C70663} |
| 189. | VMware SVGA Helper Service | Автоматически | Выполняется | vm3dservice | C:\Windows\system32\vm3dservice.exe |
| 190. | VMware Tools | Автоматически | Остановлена | VMTools | "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" |
| 191. | Volume Shadow Copy | Вручную | Остановлена | VSS | C:\Windows\system32\vssvc.exe |
| 192. | WalletService | Отключена | Остановлена | WalletService | C:\Windows\System32\svchost.exe -k appmodel -p |
| 193. | Warp JIT Service | Вручную | Остановлена | WarpJITSvc | C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted |
| 194. | Wazuh | Автоматически | Выполняется | WazuhSvc | "C:\Program Files (x86)\ossec-agent\wazuh-agent.exe" |
| 195. | Web Account Manager | Вручную | Выполняется | TokenBroker | C:\Windows\system32\svchost.exe -k netsvcs -p |
| 196. | Windows Audio | Вручную | Остановлена | Audiosrv | C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p |
| 197. | Windows Audio Endpoint Builder | Вручную | Остановлена | AudioEndpointBuilder | C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 198. | Windows Biometric Service | Вручную | Остановлена | WbioSrvc | C:\Windows\system32\svchost.exe -k WbioSvcGroup |
| 199. | Windows Camera Frame Server | Вручную | Остановлена | FrameServer | C:\Windows\System32\svchost.exe -k Camera |
| 200. | Windows Camera Frame Server Monitor | Вручную | Остановлена | FrameServerMonitor | C:\Windows\System32\svchost.exe -k CameraMonitor |
| 201. | Windows Connection Manager | Автоматически | Выполняется | Wcmsvc | C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p |
| 202. | Windows Defender Advanced Threat Protection Service | Вручную | Остановлена | Sense | "C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe" |
| 203. | Windows Defender Firewall | Автоматически | Выполняется | mpssvc | C:\Windows\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p |
| 204. | Windows Encryption Provider Host Service | Вручную | Остановлена | WEPHOSTSVC | C:\Windows\system32\svchost.exe -k WepHostSvcGroup |
| 205. | Windows Error Reporting Service | Вручную | Остановлена | WerSvc | C:\Windows\System32\svchost.exe -k WerSvcGroup |
| 206. | Windows Event Collector | Вручную | Остановлена | Wecsvc | C:\Windows\system32\svchost.exe -k NetworkService -p |
| 207. | Windows Event Log | Автоматически | Выполняется | EventLog | C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p |
| 208. | Windows Font Cache Service | Автоматически | Выполняется | FontCache | C:\Windows\system32\svchost.exe -k LocalService -p |
| 209. | Windows Image Acquisition (WIA) | Вручную | Остановлена | StiSvc | C:\Windows\system32\svchost.exe -k imgsvc |
| 210. | Windows Insider Service | Отключена | Остановлена | wisvc | C:\Windows\system32\svchost.exe -k netsvcs -p |
| 211. | Windows Installer | Вручную | Остановлена | msiserver | C:\Windows\system32\msiexec.exe /V |
| 212. | Windows License Manager Service | Вручную | Остановлена | LicenseManager | C:\Windows\System32\svchost.exe -k LocalService -p |
| 213. | Windows Management Instrumentation | Автоматически | Выполняется | Winmgmt | C:\Windows\system32\svchost.exe -k netsvcs -p |
| 214. | Windows Media Player Network Sharing Service | Вручную | Остановлена | WMPNetworkSvc | "C:\Program Files\Windows Media Player\wmpnetwk.exe" |
| 215. | Windows Modules Installer | Вручную | Остановлена | TrustedInstaller | C:\Windows\servicing\TrustedInstaller.exe |
| 216. | Windows Push Notifications System Service | Автоматически | Выполняется | WpnService | C:\Windows\system32\svchost.exe -k netsvcs -p |
| 217. | Windows Push Notifications User Service\_111ae3 | Автоматически | Выполняется | WpnUserService | C:\Windows\system32\svchost.exe -k UnistackSvcGroup |
| 218. | Windows PushToInstall Service | Отключена | Остановлена | PushToInstall | C:\Windows\System32\svchost.exe -k netsvcs -p |
| 219. | Windows Remote Management (WS-Management) | Автоматически | Выполняется | WinRM | C:\Windows\System32\svchost.exe -k NetworkService -p |
| 220. | Windows Search | Отключена | Остановлена | WSearch | C:\Windows\system32\SearchIndexer.exe /Embedding |
| 221. | Windows Security Service | Вручную | Остановлена | SecurityHealthService | C:\Windows\system32\SecurityHealthService.exe |
| 222. | Windows Time | Автоматически | Выполняется | w32time | C:\Windows\system32\svchost.exe -k LocalService |
| 223. | Windows Update | Вручную | Выполняется | wuauserv | C:\Windows\system32\svchost.exe -k netsvcs -p |
| 224. | Windows Update Medic Service | Вручную | Остановлена | WaaSMedicSvc | C:\Windows\system32\svchost.exe -k wusvcs -p |
| 225. | WinHTTP Web Proxy Auto-Discovery Service | Вручную | Выполняется | WinHttpAutoProxySvc | C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p |
| 226. | Wired AutoConfig | Вручную | Остановлена | dot3svc | C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p |
| 227. | WMI Performance Adapter | Вручную | Остановлена | wmiApSrv | C:\Windows\system32\wbem\WmiApSrv.exe |
| 228. | Workstation | Автоматически | Выполняется | LanmanWorkstation | C:\Windows\System32\svchost.exe -k NetworkService -p |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **16. Журнал «Система»** | | | | | |
| **ID** | **Дата и время** | **Источник** | **Тип события** | **№ события** | **Описание** |
| 5 | 23.03.2024 22:10:23 | Microsoft-Windows-Security-Kerberos | Error | 36742 | The Kerberos client received a KRB\_AP\_ERR\_TKT\_NYV error from the server s-dc-01$. This indicates that the ticket presented to that server is not yet v... |
| 12 | 11.02.2024 23:20:37 | Microsoft-Windows-Time-Service | Warning | 33176 | Time Provider NtpClient: This machine is configured to use the domain hierarchy to determine its time source, but it is the AD PDC emulator for the do... |
| 47 | 11.02.2024 22:37:58 | Microsoft-Windows-Time-Service | Warning | 33088 | Time Provider NtpClient: No valid response has been received from manually configured peer time.windows.com after 8 attempts to contact it. This peer ... |
| 134 | 22.02.2024 12:12:12 | Microsoft-Windows-Time-Service | Warning | 33413 | NtpClient was unable to set a manual peer to use as a time source because of DNS resolution error on '0.pool.ntp.org,'. NtpClient will try again in 15... |
| 135 | 23.02.2024 19:48:00 | Microsoft-Windows-Time-Service | Warning | 34022 | NtpClient was unable to set a manual peer to use as a time source because of duplicate error on '2.pool.ntp.org'. The same time source '0.pool.ntp.org... |
| 153 | 11.02.2024 22:45:14 | disk | Warning | 33121 | The IO operation at logical block address 0x6f30a0 for Disk 0 (PDO name: \Device\00000020) was retried. |
| 1014 | 11.02.2024 22:35:10 | Microsoft-Windows-DNS-Client | Warning | 33038 | Name resolution for the name 10.230.203.192.in-addr.arpa. timed out after none of the configured DNS servers responded. |
| 1046 | 11.02.2024 22:34:42 | Microsoft-Windows-DHCP-Server | Error | 33029 | The DHCP/BINL service on the local machine, belonging to the Windows Administrative domain sf33.local, has determined that it is not authorized to sta... |
| 1056 | 11.02.2024 22:37:49 | Microsoft-Windows-DHCP-Server | Warning | 33084 | The DHCP service has detected that it is running on a DC and has no credentials configured for use with Dynamic DNS registrations initiated by the DHC... |
| 1058 | 17.03.2024 15:40:21 | Microsoft-Windows-GroupPolicy | Error | 34997 | The processing of Group Policy failed. Windows attempted to read the file \\sf33.local\sysvol\sf33.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984F... |
| 1059 | 11.02.2024 22:34:42 | Microsoft-Windows-DHCP-Server | Error | 33028 | The DHCP service failed to see a directory server for authorization. |
| 5774 | 22.02.2024 12:13:12 | NETLOGON | Error | 33425 | The dynamic registration of the DNS record 'f48c1d48-480f-496e-99ad-e237a8959029.\_msdcs.sf33.local. 600 IN CNAME s-dc-01.sf33.local.' failed on the fo... |
| 5775 | 23.03.2024 23:18:20 | NETLOGON | Error | 37603 | The dynamic deletion of the DNS record '\_ldap.\_tcp.gc.\_msdcs.sf33.local. 600 IN SRV 0 100 3268 s-dc-01.sf33.local.' failed on the following DNS server... |
| 5781 | 11.02.2024 23:06:31 | NETLOGON | Warning | 33146 | Dynamic registration or deletion of one or more DNS records associated with DNS domain 'sf33.local.' failed. These records are used by other computer... |
| 6038 | 11.02.2024 22:52:16 | LsaSrv | Warning | 33135 | Microsoft Windows Server has detected that NTLM authentication is presently being used between clients and this server. This event occurs once per boo... |
| 7034 | 11.02.2024 22:38:21 | Service Control Manager | Error | 33094 | The Spice webdav proxy service terminated unexpectedly. It has done this 1 time(s). |
| 10005 | 16.03.2024 23:41:23 | Microsoft-Windows-DistributedCOM | Error | 34737 | DCOM got error "1115" attempting to start the service wuauserv with arguments "Unavailable" in order to run the server:  {E60687F7-01A1-40AA-86AC-DB1C... |
| 10010 | 23.03.2024 22:21:07 | Microsoft-Windows-DistributedCOM | Error | 37065 | The server {9BA05972-F6A8-11CF-A442-00A0C90A8F39} did not register with DCOM within the required timeout. |
| 10016 | 11.02.2024 22:36:05 | Microsoft-Windows-DistributedCOM | Warning | 33057 | The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID   {21B896BF-008D-4D01-A27B... |
| 10020 | 11.02.2024 22:34:40 | Microsoft-Windows-DHCP-Server | Warning | 33026 | This computer has at least one dynamically assigned IPv6 address.For reliable DHCPv6 server operation, you should use only static IPv6 addresses. |
| 10028 | 11.02.2024 23:08:55 | Microsoft-Windows-DistributedCOM | Error | 33157 | DCOM was unable to communicate with the computer 192.168.94.11 using any of the configured protocols; requested by PID 684 (C:\Windows\system32\d... |
| 10149 | 22.02.2024 17:05:49 | Microsoft-Windows-WinRM | Warning | 33832 | The WinRM service is not listening for WS-Management requests.      User Action    If you did not intentionally stop the service, use the following co... |
| 10154 | 11.02.2024 22:34:37 | Microsoft-Windows-WinRM | Warning | 33018 | The WinRM service failed to create the following SPNs: WSMAN/s-dc-01.sf33.local; WSMAN/s-dc-01.      Additional Data    The error received was 1355: %... |
| 40970 | 23.03.2024 22:17:22 | LsaSrv | Warning | 37008 | The Security System has detected a downgrade attempt when contacting the 3-part SPN      cifs/s-dc-01.sf33.local/sf33.local@sf33.local      with error... |

|  |  |  |  |
| --- | --- | --- | --- |
| **17. Журнал «Безопасность»** | | | |
| **№ события** | **Дата и время** | **ID** | **Описание** |
| 203223 | 26.03.2024 20:45:08 | 4776 | The computer attempted to validate the credentials for an account. |
| 202934 | 26.03.2024 20:40:16 | 4776 | The computer attempted to validate the credentials for an account. |
| 202930 | 26.03.2024 20:40:16 | 4776 | The computer attempted to validate the credentials for an account. |
| 199368 | 23.03.2024 22:59:37 | 4776 | The computer attempted to validate the credentials for an account. |
| 199027 | 23.03.2024 22:47:08 | 4776 | The computer attempted to validate the credentials for an account. |
| 198603 | 23.03.2024 22:25:52 | 4625 | An account failed to log on. |
| 198592 | 23.03.2024 22:25:29 | 4625 | An account failed to log on. |
| 198589 | 23.03.2024 22:25:24 | 4625 | An account failed to log on. |
| 196788 | 20.03.2024 15:25:00 | 4625 | An account failed to log on. |
| 190882 | 20.03.2024 8:30:41 | 4625 | An account failed to log on. |
| 190881 | 20.03.2024 8:30:41 | 4625 | An account failed to log on. |
| 190337 | 19.03.2024 16:47:23 | 4776 | The computer attempted to validate the credentials for an account. |
| 189154 | 19.03.2024 15:21:39 | 4776 | The computer attempted to validate the credentials for an account. |
| 185304 | 17.03.2024 15:49:08 | 4776 | The computer attempted to validate the credentials for an account. |
| 185147 | 17.03.2024 15:40:21 | 4776 | The computer attempted to validate the credentials for an account. |
| 185026 | 17.03.2024 15:36:09 | 4625 | An account failed to log on. |
| 185025 | 17.03.2024 15:36:05 | 4625 | An account failed to log on. |
| 184751 | 16.03.2024 23:39:32 | 4625 | An account failed to log on. |
| 184327 | 16.03.2024 23:30:18 | 4625 | An account failed to log on. |
| 184068 | 23.02.2024 20:35:54 | 4776 | The computer attempted to validate the credentials for an account. |
| 183618 | 23.02.2024 20:05:50 | 4776 | The computer attempted to validate the credentials for an account. |
| 183602 | 23.02.2024 20:05:30 | 4724 | An attempt was made to reset an account's password. |
| 183598 | 23.02.2024 20:05:30 | 4722 | A user account was enabled. |
| 178365 | 22.02.2024 12:18:11 | 4776 | The computer attempted to validate the credentials for an account. |
| 177405 | 11.02.2024 22:55:27 | 4776 | The computer attempted to validate the credentials for an account. |
| 177401 | 11.02.2024 22:55:24 | 4722 | A user account was enabled. |
| 177399 | 11.02.2024 22:55:24 | 4725 | A user account was disabled. |
| 177397 | 11.02.2024 22:55:24 | 4724 | An attempt was made to reset an account's password. |
| 177393 | 11.02.2024 22:55:24 | 4776 | The computer attempted to validate the credentials for an account. |
| 177387 | 11.02.2024 22:55:24 | 4776 | The computer attempted to validate the credentials for an account. |
| 177355 | 11.02.2024 22:52:20 | 4776 | The computer attempted to validate the credentials for an account. |
| 177350 | 11.02.2024 22:52:17 | 4776 | The computer attempted to validate the credentials for an account. |
| 177344 | 11.02.2024 22:52:16 | 4724 | An attempt was made to reset an account's password. |
| 177343 | 11.02.2024 22:52:16 | 4722 | A user account was enabled. |
| 177339 | 11.02.2024 22:52:16 | 4776 | The computer attempted to validate the credentials for an account. |
| 177333 | 11.02.2024 22:52:16 | 4776 | The computer attempted to validate the credentials for an account. |