

Hyper-V components (Windows 10 19H1)

Drivers	
WDAG special:	
hvsiftr.sys	- Windows Defender Application Guard Filter Driver
Hyper-V Network:	
vmnswtch.sys	- VmSwitch Extensibility Filter
VmSwitchProxy.sys	- VMSWITCH Proxy Driver
VmSwitchNIC.sys	- VmSwitch NIC Proxy Driver
vmnswtch.sys	- Microsoft Network Virtualization Service Provider
l2bridge.sys	- Network driver for bridging packets between mbx, wifi, and ethernet networks
vfpext.sys	- Microsoft Azure VFP Extension
NdisVirtualBus.sys (guest)	- Microsoft Virtual Network Adapter Enumerator
Windows Container:	
wcifs.sys	- Windows Container Isolation FS Filter Driver
Hyper-V sockets:	
hvssocktcontrol.sys	- Microsoft Hyper-V Socket Provider Control Driver
hvssockt.sys (host, guest)	- Microsoft Hyper-V Socket Provider
Hyper-V storage:	
storvsp.sys	- Storage Vsp Driver
passthrparser.sys	- Storage VSP Parser (registered calling storvsp\VstorRegisterParser)
vhdparser.sys	- Native VHD parser
vhdparscr.sys	- Proxy VHD parser
vpclvsp.sys	- Virtual PCI VSP Driver (Microsoft Hyper-V PCI Server)
storvsc.sys	- Storage VSC Driver
Hyper-V vmbus:	
vmbkmclcr.sys	- Hyper-V VMBus Root KMCL
vmbkmcl.sys (guest)	- Hyper-V VMBus KMCL
vmbusr.sys	- Microsoft Hyper-V Virtual Machine Bus Root Driver
vmbus.sys (guest)	- Microsoft Hyper-V Virtual Machine Bus Child Driver
VMBusHID.sys (guest)	- Microsoft VMBus HID Miniport
Hyper-V devices (guest):	
hyperkbd.sys	- Microsoft VMBus Synthetic Keyboard Driver
HyperVideo.sys	- Microsoft VMBus Video Device Miniport Driver (Microsoft Hyper-V Video device)
Hyper-V core	
winhvr.sys	- Windows Hypervisor Root Interface Driver
winhv.sys (guest)	- Windows Hypervisor Guest Interface Driver
vid.sys	- Microsoft Hyper-V Virtualization Infrastructure Driver
hvservice.sys	- Hypervisor Boot Driver
hvx64.exe	- Hypervisor
hvcrash.sys (guest)	- Hyper-V Crashdump (guest device "Microsoft Hyper-V Crashdump driver")
vidump.sys	- VHD Miniport Driver
vmgscounter.sys (guest)	- Virtual Machine Generation Counter
vmgid.sys (guest)	- Virtual machine guest infrastructure driver
Hyper-V core (installed only with full Hyper-V role):	
pcip.sys	- Microsoft PCI Proxy Driver
Synth3dVsp.sys	- Microsoft RemoteFX Synth3D Video VSP
ramparser.sys	- RAM parser
vmnsvcext.sys	- Hyper-V Secure Virtualization Component module
lunparser.sys	- lun parser
Hyper-V core (Windows 10 20H1):	
vkcrnlntvsc.sys (guest)	- Microsoft Hyper-V NT Kernel Integration VSC Driver
vkcrnlntvsp.sys	- Microsoft Hyper-V NT Kernel Integration VSP Driver

Images:	
WDAG special:	
hnsdiag.exe	- Hyper-V Host Network Service Diagnostics Tool
hvsimgmr.exe	- Windows Defender Application Guard Manager
hvsiproxyapp.exe	- No information
hvsidpclient.exe	- Windows Defender Application Guard Manager RDP Client
hvsidp.exe	- Windows Defender Application Guard Proxy services
hvsievaluator.exe	- Windows Defender Application Guard Policy evaluator
HvsiSettingsWorker.exe	- Run inside WDAG. Apply HVSI settings
wdagtool.exe (tool)	- Tool for reset/suspend/resume WDAG container
Containers:	
CExecSvc.exe	- Container Execution Agent
cmdiag.exe	- Container Manager Diagnostics Tool
cmimageworker.exe	- Container image worker process
vmcompute.exe	- Hyper-V Host Compute Service
VmComputeAgent.exe	- Hyper-V Guest Compute Service
wesetupagent.exe	- Utility VM Setup Agent
hcsdiag.exe (tool)	- Hyper-V Host Compute Service Diagnostics Tool
Hyper-V network:	
vfpctrl.exe (tool)	- VFP control and diagnostics utility
nmbind.exe (tool)	- Hyper-V Network Core Bind Application
nmscrub.exe (tool)	- Display information about VMSwitch
nvspinfo.exe (tool)	- Display information about VmSwitch
Hyper-V Core	
vmwp.exe	- Virtual Machine Worker Process
Windows Sandbox special:	
WindowsSandbox.exe	- Windows Sandbox launcher
Hyper-V Core (installed only with full Hyper-V role):	
hvc.exe (tool)	- Hyper-V Command Line Tool
hnsdiag.exe	- Hyper-V Host Network Service Diagnostics Tool
rdvgm.exe	- RemoteFX Desktop Virtual Graphics Manager
vmplatformca.exe	- Hyper-V Certificate Authority Trustlet
vmnsp.exe	- Virtual Machine Security Process
vmconnect.exe	- Virtual Machine Connection
vmms.exe	- Virtual Machine Management Service

Services:	
Created	
CmService	- Container Manager Service
gcs	- Hyper-V Guest Compute Service
hns	- Host Network Service
hvsics	- Application Guard Container Service
nvagent	- Network Virtualization Service
vmcompute	- Hyper-V Host Compute Service
Started	
HvHost	- HV Host Service
gpsvc	- Group Policy Client (PC is not domain joined)
Hyper-V Core (installed only with full Hyper-V role) created:	
HgClientService	- Host Guardian Client Service
vmms	- Hyper-V Virtual Machine Management
HVHost	- HV Host Service

Libraries:	
SysWOW64 WDAG modules:	
hvscontainerservice.dll	- Windows Defender Application Guard Container Service
hvsfiletrust.dll	- HVSI file trust lib.
hvsimgps.dll	- Windows Defender Application Guard Proxy Stub Dll
hvsiofficeiconoverlayshellxextension.dll	- Microsoft Office inside WDAG auxiliary library
WDAG Special:	
hvscontainerservice.dll	- Windows Defender Application Guard Container Service
hvsidspdvclient.dll	- HVSI DVC (dynamic virtual channel) library. Used by hvsidpclient.exe
hvsfiletrust.dll	- HVSI file trust lib. Used by hvsimgmr.exe
HvsiMachinePolicies.dll	- Get settings for HVSI from registry
hvsimgps.dll	- Windows Defender Application Guard Proxy Stub Dll
hvsiofficeiconoverlayshellxextension.dll	- Microsoft Office inside WDAG auxiliary library
HvsiSettingsProvider.dll	- Windows Defender Application Guard Hvsi Settings Provider.dll. Used by hvsimgmr.exe, hvsidpclient.exe, HvsiSettingsWorker.exe, hvscontainerservice.dll
hvsigpext.dll	- Windows Defender Application Guard Group Policy Extension
AuditSettingsProvider.dll	- HVSI audit settings provider dll (Microsoft.Windows.HVSI.AuditSettings)
Windows Sandbox special:	
madrid.dll	- Madrid Client Library
Windows container:	
cmclient.dll	- Windows Container Manager client library
vmcompute.dll	- Hyper-V Host Compute Service Library
vmcomputeeventlog.dll	- Hyper-V Compute Event Log Resource Dll
VmComputeProxy.dll	- Hyper-V Compute Component Proxy
hnsproxy.dll	- Host Network Service proxy library
HostNetSvc.dll	- Host Network Service
CmService.dll	- Container Manager Service
computestorage.dll	- Hyper-V Host Compute Service Storage Library
Hyper-V Network:	
NetMgmtF.dll	- Host Network Management
NvAgent.dll	- Network Virtualization Agent
vmisf.dll	- Hyper-V Virtual Switch Driver Interface Library
vmisfcore.dll	- Hyper-V Virtual Switch Driver Core Interface Library
vmisfproxystub.dll	- IVmsManagementEvents Interface Proxy/Stub
VmSynthNic.dll	- Microsoft Synthetic Network Card
gns.dll	- Guest Network Service
Hyper-V devices:	
vmndynmem.dll	- Microsoft Dynamic Memory Controller
vmnicx.dll	- Microsoft Flexible IO Device
vmnicore.dll	- Virtual Machine Integration Service Core Devices
vmnmem.dll	- Microsoft Virtual Persistent Memory Controller
vmserial.dll	- Microsoft Serial Device
vmsemb.dll	- Microsoft Virtual SMB Device
vmvsnhstor.dll	- Microsoft Synthetic Storage Adapter
vmuiddevices.dll	- Microsoft VM UI Devices
VrdUmed.dll	- Virtual Render Device UMED
gpubpdev.dll	- Microsoft VM Chipset Devices
vmchipset.dll	- Microsoft VM Chipset Devices
Hyper-V Core:	
ActivationVdev.dll	- Loaded by vmwp.exe. Service guest Microsoft Hyper-V Activation component virtual device
sbresources.dll	- Microsoft Hyper-V Secure Boot Resources
rdp4vs.dll	- Virtual Machine Remoting Services API
UtilityVmSysprep.dll	- Utility VM Sysprep Plugin
vmbuspiper.dll	- VmBus User Mode Pipe DLL
vmbusvdev.dll	- Microsoft Virtual Machine Bus Device
VmCrashDump.dll	- Microsoft VM Crash Dump Device
vmwp.exe	- Hyper-V Component Proxy
vmusrv.dll	- User-mode SRV
vmvirtio.dll	- Hyper-V Virtio Infrastructure
vmwpcrtl.dll	- Virtual Machine Control Module
vmwpevents.dll	- Hyper-V VMWP Event Log Resource Dll
vmfpapi.dll	- VM Filtering Platform User Mode API Library
vp9b.dll	- Plan9 File System (Probably, WSL stuff, used by vmsemb.dll)
Hyper-V services (guest):	
icsvc.dll	- Virtual Machine Integration Component Service
icsvext.dll	- Virtual Machine Integration Component Service
Hyper-V API Wrappers	
vid.dll	- Microsoft Hyper-V Virtualization Infrastructure Driver Library
winhvpplatform.dll	- Hyper-V Hypervisor User-Mode API Library
winhvemulation.dll	- Hyper-V Instruction Emulator User-Mode API Library
API Schema	
{GUID}_HyperV-ComputeLegacy.dll	- ApiSet Schema Extension DLL
{GUID}_HyperV-ComputeStorage.dll	- ApiSet Schema Extension DLL
{GUID}_HyperV-ComputeCore.dll	- ApiSet Schema Extension DLL
{GUID}_HyperV-ComputeNetwork.dll	- ApiSet Schema Extension DLL
{GUID}_HyperV-DeviceVirtualization.dll	- ApiSet Schema Extension DLL
{GUID}_HyperV-ComputeNetwork.dll	- ApiSet Schema Extension DLL
Other Hyper-V related stuff:	
rdvmmtransport.dll	- Rdv Vm Transport Endpoints
Hyper-V Core (installed only with full Hyper-V role):	
C:\Windows\SysWOW64\RdvgmProxy.dll	- RemoteFX Rdvgm COM proxy dll
C:\Windows\SysWOW64\vmstaging.dll	(I exported function - IsFeatureEnabled)
HyperV\SysprepProvider.dll	- Hyper-V Sysprep Plugin
hgatest.dll	- Part of Host Guardian Client Service. Used by hgscntplugin.dll
hgclientservice.dll	- Host Guardian Client Service
hgclientservicecps.dll	- Part of Host Guardian Client Service. Has COM interface GUID IID_IHgAttestation and IID_IHgKeyProtection
hgscntplugin.dll	- HostGuardianClientPluginAttestation
HgsClientWmi.dll	- WMIv2 Provider for the Host Guardian Service Client
HostGuardianServiceClientResources.dll	- HostGuardianServiceClientResources
NetMgmtF.dll	- Host Network Management
rdp4vs.dll	- Virtual Machine Remoting Services API
NvAgent.dll	- Network Virtualization Agent.
rtpm.dll	- Remote TPM Library
RdvgmProxy.dll	- RemoteFX Rdvgm COM proxy dll
RdvGpuInfo.dll	- Microsoft RemoteFX GPU Info Library
RcmoteFileBrowse.dll	- Hyper-V remote file browser data source.
TpmEngUM.dll	- TPM Win32 user-mode engine
synth3dvideoproxy.dll	- RemoteFX COM proxy dll
vmstaging.dll	(I exported function - IsFeatureEnabled)
vmvsnh3dvideo.dll	- Microsoft Synthetic 3D Video Device
vmvsnhfcvdev.dll	- Microsoft Synthetic Fibre Channel Adapter
vmtpm.dll	- Microsoft TPM Device
VmDataStore.dll	- VmDataStore Module
vmdebug.dll	- Microsoft Debug Device
vmcicvdev.dll	- Make allocation/unloading PCI device from pool
vmemulateddevices.dll	- Microsoft VM Emulated Devices
VmEmulatedNic.dll	- Microsoft Emulated Network Card
VmEmulatedStorage.dll	- Microsoft Emulated Storage
vmhgs.dll	- Hyper-V Host Guardian Service Client Library
vmiadv.dll	- Remote Desktop Services VDI Vdev
vsconfig.dll	- Virtual Machine Configuration Module
vmicvdev.dll	- Virtual Machine Integration Service Devices
vmmsprox.dll	- Hyper-V Virtual Machine Manager Proxy
C:\Program Files\Hyper-V\	VmConnect, Vhd attaching utility

Vid.sys - KMDF driver.	
/vdfhandle 0x00006ff998fe4d48 dt FxFileObject 0xffff9006670102b0 dx -r1 (WdId 1000!_FILE_OBJECT *)0xffff90066748d580 [+0x058] FileName : "\C3F653D8-DBBE-41BD-8D91-B6CBB537C03C" [Type: _UNICODE_STRING]	
/vdfhandle 0x00006ff9981c8d18 dt FxFileObject 0xffff900667c372e0 dx -r1 (WdId 1000!_FILE_OBJECT *)0xffff9006671526c0 [+0x058] FileName : "\c3f653d8-4bbe-41bd-8d91-b6cbb537c03c" [Type: _UNICODE_STRING]	
FsContext field of both file objects points to Prtn object. It is a main descriptor of created partition	
0: kd> dc 0xffff900665e85000 L4 - Prtn object ffff900665e85000 6e747250 00000000 00000000 00000000 Prtn.....	

Configs:	
C:\Windows\System32\HvsiSettingsProviders\AuditPol_ContainerCreate.xml	
C:\Windows\System32\HvsiSettingsProviders\AuditPol_ContainerRealtime.xml	
C:\Windows\System32\HvsiSettingsProviders\HvsiMachinePolicies_ContainerCreate.xml	
C:\Windows\System32\HvsiSettingsProviders\HvsiMachinePolicies_ContainerRealtime.xml	
C:\Windows\System32\HvsiSettingsProviders\HvsiUserPolicies_ContainerCreate.xml	
C:\Windows\System32\HvsiSettingsProviders\HvsiUserPolicies_ContainerRealtime.xml	
C:\Windows\System32\HvsiSettingsProviders\WDATP_ContainerCreate.xml	
C:\ProgramData\Microsoft\WDAG\CentennialAppTemplates\MicrosoftCentennialOfficeWin32.xml	
C:\ProgramData\Microsoft\WDAG\CentennialAppTemplates\MicrosoftCentennialOfficeWin64.xml	
Code Integrity settings. You can reconfigure CI inside WDAG container and can run any program if you replace file to another policy.	
C:\Windows\System32\HvsiSettingsProviders\CodeIntegrity\SIPPolicy.p7b	
C:\Windows\System32\HvsiSettingsProviders\CodeIntegrity\SIPPolicy_office.p7b	

Hvsigpext.dll - Winlogon GP Extension	
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{9650FDBC-053A-4715-AD14-FC2DC65E8330}.	
WDAG Policy Parameters:	
AllowHvsiCpTracker	
EnableClipboard	
EnablePrinters	
EnableCameraMicrophoneRedirection	
EnablePersistence	
EnableVirtualGPU	
AppHVSIClipboardSettings	
AppHVSIClipboardFileType	
AppHVSIPrintingSettings	
BlockNonEnterpriseContent	
AllowCameraMicrophoneRedirection	
AuditApplicationGuard	
AllowPersistence	
AllowVirtualGPU	
FileTrustCriteria	
FileTrustOriginRemovableMedia	
FileTrustOriginNetworkShare	
FileTrustOriginMarkOfTheWeb	

VSMB	
Many files inside WDAG opened with VSMB prefix:	
rdbss.sys (Redirected Drive Buffering SubSystem Driver): \VSMB-{dcc079ae-60ba-4d07-847c-3493609c0870}\SharedMemory\$ RxAcquireFileForNtCreateSection RxCreateRxContext RxWaitForStableViewOnFcbAndAcquireRundown	
wcifs.sys (Windows Container Isolation FS Filter Driver): \Device\vmmsmb\VSMB-{dcc079ae-60ba-4d07-847c-3493609c0870}\os\WcSetupVmsbUnionContext RtlInitUnicodeString(&v23 + 24, L"\Device\vmmsmb\VSMB-{dcc079ae-60ba-4d07-847c-3493609c0870}\os\"); FltGetVolumeFromName(Globals, &v23 + 24, &v28); FltGetVolumeInstanceFromName(Globals, &v28, &::DestinationString, &v27) FltAttachVolume(Globals, &v28, &::DestinationString, &v27)	
ntoskrnl.exe : \Device\VBUS\{4d12e519-17a0-4ae4-8ea4-5270fc6abdb7}-{dcc079ae-60ba-4d07-847c-3493609c0870}-0000 IoPnpInitializeBootDrivers SbpaAddTransportToInstance	
vmcompute.exe (Hyper-V Host Compute Service): \\?\VMSMB\VSMB-{dcc079ae-60ba-4d07-847c-3493609c0870}\%ls ComputeService:HyperVContainer::BuildHostedContainerConfiguration ComputeService::Management::ProxyUtils::ConvertRs4SettingsDocument ComputeService::Management::Details::GetRs4GuestModifyRequest ComputeService::ContainerDefinition::ApplyHiveStackSettings ComputeService::Storage::BuildVSMBPipePath ComputeService::ContainerUtilities::AddMappedPipe ComputeService::ContainerUtilities::AttachFilterToVolume	
VmComputeAgent.exe (Hyper-V Guest Compute Service): \\?\VMSMB\VSMB-{dcc079ae-60ba-4d07-847c-3493609c0870}\%ls ComputeService:ContainerUtilities::AddMappedPipe ComputeService::ContainerUtilities::AttachFilterToVolume ComputeService::ContainerDefinition::ApplyHiveStackSettings ComputeService::ContainerUtilities::NormalizeMappedDirectory	
CmService.dll (Container Manager Service library): \\?\VMSMB\VSMB-{dcc079ae-60ba-4d07-847c-3493609c0870}\Container::Manager::Hcs::Details::BuildVSMBPipePath	
rdsdwmldr.dll (Microsoft Remote Desktop Services Desktop Composition Component): \Device\vmmsmb\VSMB-{dcc079ae-60ba-4d07-847c-3493609c0870}\SharedMemory\$\CreateVmSharedMemorySection NtCreateFile NtCreateSection	
rdsvxmaudio.dll : \Device\vmmsmb\VSMB-{dcc079ae-60ba-4d07-847c-3493609c0870}\SharedMemory\$\OpenVmSharedMemorySection2 NtCreateFile NtCreateSection	