```
ÿþ2025-03-11 06:26:41 AUTO-INFO: ***********************VM Evidence Bot Started************************
2025-03-11 06:26:41 AUTO-INFO: Selected VM Template : GBL-W2K22STD-GEN-TMP
2025-03-11 06:26:41 AUTO-INFO: VM Port Group : 5D-DVPG-PC-INFRA-SER-1117
VM Rollback bot started
If the Database is Installed, this bot will unistall SQL Database and Decomission the Server
2025-03-11 11:30:39 AUTO-INFO: VM W5DSECP002 is  available
2025-03-11 11:30:44 AUTO-INFO: The VM is already Part of the Domain
WARNING: TEM computer name W5DSECP002 is not found in api result- Exception calling "GetResult"
with "0" argument(s): "No such host is known" System.Xml.XmlDocument
2025-03-11 11:30:54 AUTO-INFO: VM W5DSECP002 is  availabe
2025-03-11 11:30:54 AUTO-INFO: VM W5DSECP002 is in True
2025-03-11 11:30:54 AUTO-INFO: Stopping the VM ..
2025-03-11 11:36:56 AUTO-INFO: The VM Stopped Sucessfully
2025-03-11 11:36:56 AUTO-INFO: The Removal of the VM Started ..
2025-03-11 11:36:56 AUTO-INFO: Deleting the VM W5DSECP002 is Successfull
2025-03-11 11:38:16 AUTO-INFO: W5DSECP002 does not exist in CMDB
2025-03-11 11:38:16 AUTO-INFO: Based on the instructions, Roll back bot removed all the monitoring and
backup clients and completed successfully with no error reported
VM Rollback bot Ended
2025-03-11 11:38:21 AUTO-INFO: ***********************VM Evidence Bot Started************************
2025-03-11 11:38:21 AUTO-INFO: Selected VM Template : GBL-W2K22STD-GEN-TMP
2025-03-11 11:38:21 AUTO-INFO: VM Port Group : 5D-DVPG-PC-INFRA-SER-1117
VM Rollback bot started
If the Database is Installed, this bot will unistall SQL Database and Decomission the Server
2025-03-12 03:27:42 AUTO-INFO: VM W5DSECP002 is  available
2025-03-12 03:27:55 AUTO-INFO: The VM is already Part of the Domain
2025-03-12 03:27:55 AUTO-INFO: Removing the Server from the Domain
2025-03-12 03:28:03 AUTO-INFO: Removing the Server from the Domain completed Sucessfully
2025-03-12 03:28:03 AUTO-INFO: Restarting the Server to make the changes in the VM
2025-03-12 03:33:09 AUTO-INFO: Restarting the Server to the server completed succesfully
WARNING: TEM computer name W5DSECP002 is not found in api result- W5DSECP002 : This operation
returned because the timeout period expired W5DSECP002 : DNS server failure System.Xml.XmlDocument
2025-03-12 03:33:19 AUTO-INFO: VM W5DSECP002 is  availabe
2025-03-12 03:33:19 AUTO-INFO: VM W5DSECP002 is in True
2025-03-12 03:33:19 AUTO-INFO: Stopping the VM ..
2025-03-12 03:39:21 AUTO-INFO: The VM Stopped Sucessfully
2025-03-12 03:39:21 AUTO-INFO: The Removal of the VM Started ..
2025-03-12 03:39:21 AUTO-INFO: Deleting the VM W5DSECP002 is Successfull
2025-03-12 03:40:42 AUTO-INFO: W5DSECP002 does not exist in CMDB
2025-03-12 03:40:46 AUTO-INFO: IP has been released into Avaiable IP Pool
2025-03-12 03:40:46 AUTO-INFO: Based on the instructions, Roll back bot removed all the monitoring and
backup clients and completed successfully with no error reported
VM Rollback bot Ended
2025-03-12 04:43:38 AUTO-INFO: ***********************VM Evidence Bot Started************************
2025-03-12 04:43:38 AUTO-INFO: Selected VM Template : GBL-W2K22STD-GEN-TMP
2025-03-12 04:43:38 AUTO-INFO: VM Port Group : 5D-DVPG-PC-INFRA-SER-1117
VM Rollback bot started
If the Database is Installed, this bot will unistall SQL Database and Decomission the Server
2025-03-18 07:41:32 AUTO-INFO: VM W5DSECP002 is  available
2025-03-18 07:41:45 AUTO-INFO: The VM is already Part of the Domain
2025-03-18 07:41:45 AUTO-INFO: Removing the Server from the Domain
2025-03-18 07:42:00 AUTO-INFO: Removing the Server from the Domain completed Sucessfully
2025-03-18 07:42:00 AUTO-INFO: Restarting the Server to make the changes in the VM
```

```
2025-03-18 07:47:05 AUTO-INFO: Restarting the Server to the server completed succesfully
9840810
https://w0btem001:52311/api/computer/9840810
Computer is fetched from the TEM Console and below are the properties of computer name
Name                                 #text
----                               -----
Computer Name                           W5DSECP002
OS                                  Win2022 10.0.20348.2700 (21H2)
CPU                                 2800 MHz Xeon Gold 6342
Last Report Time                       Tue, 18 Mar 2025 11:39:56 +0000

Locked                               No
BES Relay Selection Method                  Manual
Relay                                w0btem001.myl.com:52311
Relay Name of Client                     W5DSECP002.myl.com
DNS Name                              W5DSECP002.myl.com
Active Directory Path                     CN=W5DSECP002,OU=HUN,OU=Servers,DC=myl,DC=com

Client Administrators                    __op_1000
Client Administrators                    __op_1001
Client Administrators                    __op_1002
Client Administrators                    __op_1003
Client Administrators                    __op_1005
Client Administrators                    __op_1006
Client Administrators                    __op_1008
Client Administrators                    __op_1009
Client Administrators                    __op_1010
Client Administrators                    __op_1012
Client Administrators                    __op_1013
Client Administrators                    __op_1016
Client Administrators                    __op_1017
Client Administrators                    __op_1019
Client Administrators                    __op_1020
Client Administrators                    __op_1022
Client Administrators                    __op_1023
Client Administrators                    __op_1024
Client Administrators                    __op_1026
Client Administrators                    __op_1027
Client Administrators                    __op_1028
Client Administrators                    __op_1029
Client Administrators                    __op_1030
Client Administrators                    __op_1031
Client Administrators                    __op_1032
Client Administrators                    __op_1033
Client Administrators                    __op_1034
Client Administrators                    __op_1036
Client Administrators                    __op_1038
Client Administrators                    __op_1039
Client Administrators                    __op_1041
Client Administrators                    __op_196
Client Administrators                    __op_221
Client Administrators                    __op_257
Client Administrators                    __op_277
```

Client Administrators	__op_292
Client Administrators	__op_294
Client Administrators	__op_296
Client Administrators	__op_303
Client Administrators	__op_304
Client Administrators	__op_316
Client Administrators	__op_318
Client Administrators	__op_323
Client Administrators	__op_324
Client Administrators	__op_325
Client Administrators	__op_335
Client Administrators	__op_349
Client Administrators	__op_351
Client Administrators	__op_356
Client Administrators	__op_360
Client Administrators	__op_364
Client Administrators	__op_366
Client Administrators	__op_367
Client Administrators	__op_378
Client Administrators	__op_38
Client Administrators	__op_380
Client Administrators	__op_382
Client Administrators	__op_390
Client Administrators	__op_392
Client Administrators	__op_396
Client Administrators	__op_399
Client Administrators	__op_4
Client Administrators	__op_40
Client Administrators	__op_401
Client Administrators	__op_402
Client Administrators	__op_403
Client Administrators	__op_404
Client Administrators	__op_405
Client Administrators	__op_406
Client Administrators	__op_409
Client Administrators	__op_41
Client Administrators	__op_410
Client Administrators	__op_411
Client Administrators	__op_412
Client Administrators	__op_413
Client Administrators	__op_414
Client Administrators	__op_415
Client Administrators	__op_416
Client Administrators	__op_417
Client Administrators	__op_418
Client Administrators	__op_419
Client Settings	Location By Subnet=
Client Settings	_BESClient_Download_NormalStageDiskLimitMB=2048
Client Settings	_BESClient_Download_PreCacheStageDiskLimitMB=2048
Client Settings	_BESClient_LastShutdown_Reason=Service manager stop request

```
Client Settings                         _BESClient_Upgrade_UTF8Settings=1

Client Settings                         _BESClient_UploadManager_BufferDirectory=C:\Program Files
(x86)\B...
Client Settings                         _BESClient_WindowsOS_EnableSupersededEval=1

Client Settings                         __Client_Role_398498=1
Client Settings                         __Client_Role_473289=1
Client Settings                         __Client_Role_473292=0
Client Settings                         __Client_Role_473293=1
Client Settings                         __Client_Role_473324=1
Client Settings                         __Client_Role_483194=1
Client Settings                         __Client_Role_488835=0
Client Settings                         __Client_Role_488837=0
Client Settings                         __Client_Role_488914=0
Client Settings                         __Client_Role_491844=1
Client Settings                         __Client_Role_514306=0
Client Settings                         __Client_Role_600997=0
Client Settings                         __Client_Role_660716=0
Client Settings                         __Client_Role_883399=1
Client Settings                         __LockState=false
Client Settings
__Relay_Control_RootServer=http://w0btem001.myl.com:52311/cgi-bin...
Client Settings                         __Relay_Control_Server1=http://w0btem001.myl.com:52311

Client Settings                         __Relay_Control_Server2=
IP Address                              10.6.176.142
Subscribed Sites                         http://sync.bigfix.com/cgi-bin/bfgather/advancedpatching

Subscribed Sites                         http://sync.bigfix.com/cgi-bin/bfgather/assetdiscovery

Subscribed Sites                         http://sync.bigfix.com/cgi-bin/bfgather/besinventory

Subscribed Sites                         http://sync.bigfix.com/cgi-bin/bfgather/bessupport

Subscribed Sites
http://w0btem001.myl.com:52311/cgi-bin/bfgather.exe/CustomSite_Da...
Subscribed Sites
http://w0btem001.myl.com:52311/cgi-bin/bfgather.exe/CustomSite_Pa...
Subscribed Sites
http://w0btem001.myl.com:52311/cgi-bin/bfgather.exe/CustomSite_So...
Subscribed Sites                         http://sync.bigfix.com/cgi-bin/bfgather/bessecurity

Subscribed Sites                         http://sync.bigfix.com/cgi-bin/bfgather/ibmlicensereporting

Subscribed Sites                         http://sync.bigfix.com/cgi-bin/bfgather/patchingsupport

Subscribed Sites                         http://sync.bigfix.com/cgi-bin/bfgather/serverautomation

Subscribed Sites                         http://sync.bigfix.com/cgi-bin/bfgather/softwaredistribution

Subscribed Sites                         http://sync.bigfix.com/cgi-bin/bfgather/updateswindowsapps
```

Subscribed Sites	http://sync.bigfix.com/cgi-bin/bfgather/updateforwinappextend
Subscribed Sites	http://w0btem001.myl.com:52311/cgi-bin/bfgather.exe/actionsite
Subscribed Sites	http://w0btem001.myl.com:52311/cgi-bin/bfgather.exe/mailboxsite98...
BES Root Server	w0btem001.myl.com (0)
License Type	Server
Agent Type	Native
Device Type	Server
Agent Version	10.0.7.52
User Name	m676096_sadm
RAM	8192 MB
Free Space on System Drive	96777 MB
Total Size of System Drive	122227 MB
BIOS	03/26/2024
Subnet Address	10.6.176.128
InWindow (TEM Servers)	n/a
ID	9840810
Computer Type	Virtual
MAC Address	00-50-56-84-ba-e0
__Patch_Group	Setting Missing
WINUPTIME	8697
Uptime	6 days, 00:57:54.578
Qualys Agent Version	Not Installed
CrowdStrike Agent Version-Linux	NA
Qualys-Agent Version-Linux	NA
SCOM Windows Vesion	10.19.10014.0
BESCLient Installation Path	C:\Program Files (x86)\BigFix Enterprise\BES Client
RedCloack- Windows	Not Installed
CPU Vendor	GenuineIntel
CPU Model	GenuineIntel
CPU Type	0
Number of Cores of CPUs	4
Number of CPUs	2
Brand string of CPU	Intel(R) Xeon(R) Gold 6342 CPU @ 2.80GHz
RedCloak Version- Linux	NA
Computer Type	Virtual
Serial Number	VMware-42 04 38 39 58 69 44 19-a9 7a cb 00 b3 61 46 9c
BESCLient Startup Type	auto
SQL Running Status	False
VIA_Oracle _Windows Database	False
Oracle Databae Installed status- Linux	False
MSSQL Management Studio instaled services	No SQL Installed
SEP Version	14.3.8289.5000
VIA_NetBack Version_Linux	Not Installed
Via_Patch Installed Date_KB ID	W5DSECP002, KB5039889, 9/13/2024
Via_Patch Installed Date_KB ID	W5DSECP002, KB5012170, 12/29/2022

```
Via_Patch Installed Date_KB ID                     W5DSECP002, KB5042881, 9/13/2024

Via_Patch Installed Date_KB ID                     W5DSECP002, KB5043167, 9/13/2024

VIA_SplunkUF Service Status for Win                Not Installed
VIA_SplunkUF Service Status for Linux              Not Installed
VIA_SCOM_UR5 Version                               10.19.10211.0
VIA_CarbonBlack_App Control_Windows_Service Status Not Installed

VIA_Computer manufacturers                         VMware, Inc.
VIA_Computer Model                                 VMware20,1
VIA_CarbonBlack_App Control_Linux_Service Status   Not Installed

VIA_Carbon Black App Control_Agent version_Windows Not Installed

VIA_QuestBackupAgentAD_AgentVersion                Not Installed

VIA_Active Directory Agent Status                  False
VIA_SplunkUF Service Service Status                Not Installed
VIA_Uptime>100Days                                 False
VIA_VMTools Version_Windows                        12.4.5.23787635

Via_Azure Connected Machine Windows Agent          Not Installed

VIA_HotFix ID and Date                             KB5039889 - 9/13/2024
VIA_HotFix ID and Date                             KB5012170 - 12/29/2022
VIA_HotFix ID and Date                             KB5042881 - 9/13/2024
VIA_HotFix ID and Date                             KB5043167 - 9/13/2024
Installed patch Date_Testing                       Tue, 18 Mar 2025 11:40:02 +0000

VCPU                                               4
VIA_OSEdition_Standard or DataCenter               ServerStandard

/etc/dnf.conf Data                                 File not found
VIA_Quest Forest Recovery Windows Agent            Not Installed

VIA_Quest Toad _Windows                            Not Installed
VIA_kb2919355                                      KB2919355 Not Installed
VIA_Server local time                              12:40:03 +0100 Tue, 18 Mar 2025

VIA_JAVA Version_Windows                           Not Installed
VIA_JAVA_Installation Path_Windows                 Not Installed
VIA_JAVA_Publisher_Name_Vendor_Windows             Not Installed

VIA_Windows_Oracle__Java Display name              Not Installed

VIA_Browser Analysis                               Firefox: Not Installed | Chrome: Not Installed | Edge:
Version 12...
VIA_/etc/sudoers.d/                                Directory does not exist
VIA_FeatureSettingsOverride_Value                  8264
VIA_FeatureSettingsOverrideMask_Value              3
VIA_Windows_Oracle_Java Version                    Not Installed
```

```
VIA_Linux_Java Version                        Java version not found
VIA_SQL Services Data                         N/A
Distance to BES Relay                         User-defined error: unknown
_BESClient_UsageManager_EnableAppUsage            User-defined error: not set

_BESClient_UsageManager_EnableAppUsageSummary      User-defined error: not set

_BESClient_UsageManager_EnableAppUsageSummaryApps  User-defined error: not set

_BESClient_UsageManager_OperatorApps              User-defined error: not set

Location By IP Range_13th July 2016               User-defined error: not set

Location By IP Range                          User-defined error: not set
Server Environment                            The operator "prod" is not defined.
APAC                                       User-defined error: not set
Environment Details                           User-defined error: not set
In Maintenance Window                          Singular expression refers to nonexistent object.

MSSQL Edition                                 Singular expression refers to nonexistent object.

MSSQL Patch Level                             Singular expression refers to nonexistent object.

Secondary Relay                               Singular expression refers to nonexistent object.

VIA_JavaVersion_Linux_CMD                        The operator "rpm" is not defined.

VIA_NetBack Version_Windows                      Singular expression refers to nonexistent object.

Splunk_Sudo_Wasim                              The operator "false endif" is not defined.

Installed Applications for Unix                The operator "volumes" is not defined.

/root space in MB's                           Singular expression refers to nonexistent object.

VIA_Linux_Patch Installed Date                  Singular expression refers to nonexistent object.

VIA_JavaVersion_Linux_RPM                        The operator "rpm" is not defined.

Fetched Computer Name is matching with the given CI Name
https://w0btem001:52311/api/computer/9840810
ok
TEMAgentRemoval:Success
2025-03-18 07:48:31 AUTO-INFO: VM W5DSECP002 is  availabe
2025-03-18 07:48:31 AUTO-INFO: VM W5DSECP002 is in True
2025-03-18 07:48:31 AUTO-INFO: Stopping the VM ..
2025-03-18 07:54:33 AUTO-INFO: The VM Stopped Sucessfully
2025-03-18 07:54:33 AUTO-INFO: The Removal of the VM Started ..
2025-03-18 07:54:34 AUTO-INFO: Deleting the VM W5DSECP002 is Successfull
2025-03-18 07:55:53 AUTO-INFO: W5DSECP002 does not exist in CMDB
2025-03-18 07:55:57 AUTO-INFO: IP has been released into Avaiable IP Pool
2025-03-18 07:55:57 AUTO-INFO: Based on the instructions, Roll back bot removed all the monitoring and
backup clients and completed successfully with no error reported
```

```
VM Rollback bot Ended
2025-03-19 05:45:55 AUTO-INFO: ***********************VM Evidence Bot Started************************
2025-03-19 05:45:55 AUTO-INFO: Selected VM Template : GBL-W2K22STD-GEN-TMP
2025-03-19 05:45:55 AUTO-INFO: VM Port Group : 5D-DVPG-PC-INFRA-SER-1117
2025-03-19 07:34:52 AUTO-INFO: Server CI Name : W5DSECP002
2025-03-19 07:34:54 AUTO-INFO: VM location: 5D-HUNGARY/vm/AutoBuild
2025-03-19 07:34:54 AUTO-INFO: VMWare vCenter Name : wb5vc001
2025-03-19 07:34:54 AUTO-INFO: Cluster Name : 5DHADRS001
2025-03-19 07:34:55 AUTO-INFO: Datastore Name : 5D-5DHADRS002-N5DVSVM002-NFS008
2025-03-19 07:34:55 AUTO-INFO: Operating System and Edition : Microsoft Windows Server 2022 (64-bit)
2025-03-19 07:34:55 AUTO-INFO: CPU : 4
2025-03-19 07:34:55 AUTO-INFO: RAM : 8
2025-03-19 07:34:56 AUTO-INFO: VM hotplug status: @{Name=W5DSECP002; MemoryHotAddEnabled=True;
CpuHotAddEnabled=True; CpuHotRemoveEnabled=False}
2025-03-19 07:34:56 AUTO-INFO: Template Change Number: CHG0141159
2025-03-19 12:34:58 AUTO-INFO: ********HOSTNAME********
2025-03-19 12:34:58 AUTO-INFO: HOSTNAME: W5DSECP002
2025-03-19 12:34:58 AUTO-INFO: ********Server Accessibility Remote Desktop*******
Status   Name               DisplayName                           PSComputerName

------   ----               -----------                           -------------
Running  TermService        Remote Desktop Services               W5DSECP002

2025-03-19 12:36:11 AUTO-INFO: *******list of softwares Installed ********
Name           : BigFix Client
Version        : 10.0.7.52
PSComputerName : W5DSECP002
RunspaceId     : 62e223c7-b496-4c6b-9d57-f801ea23b0db
Name           : VMware Tools
Version        : 12.4.5.23787635
PSComputerName : W5DSECP002
RunspaceId     : 62e223c7-b496-4c6b-9d57-f801ea23b0db
Name           : Symantec Endpoint Protection
Version        : 14.3.8289.5000
PSComputerName : W5DSECP002
RunspaceId     : 62e223c7-b496-4c6b-9d57-f801ea23b0db
Name           : Veritas NetBackup Client
Version        : 10.0.0.1
PSComputerName : W5DSECP002
RunspaceId     : 62e223c7-b496-4c6b-9d57-f801ea23b0db
Name           : Microsoft Monitoring Agent
Version        : 10.19.10014.0
PSComputerName : W5DSECP002
RunspaceId     : 62e223c7-b496-4c6b-9d57-f801ea23b0db
2025-03-19 12:36:11 AUTO-INFO: ********IP Details :********
Windows IP Configuration
   Host Name . . . . . . . . . . . . : W5DSECP002
   Primary Dns Suffix  . . . . . . . : myl.com
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : myl.com
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix  . :
Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
Physical Address. . . . . . . . . : 00-50-56-84-87-87
DHCP Enabled. . . . . . . . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . . . . . . . : 10.6.176.142(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.128
Default Gateway . . . . . . . . . : 10.6.176.129
DNS Servers . . . . . . . . . . . : 172.18.86.19
                                    10.250.31.41
NetBIOS over Tcpip. . . . . . . . : Enabled
2025-03-19 12:36:11 AUTO-INFO: *******Disk info :***********
C: - 119.363277435303 ,
D: - 99.9979858398438 ,
P: - 15.9979858398438 ,
R: - 0 ,
2025-03-19 12:36:15 AUTO-INFO: **********WindowsActivationStatus :************
@{Description=Windows(R) Operating System, VOLUME_KMSCLIENT channel;
Licensefamily=ServerStandard; LicenseStatus=5}

2025-03-19 12:36:15 AUTO-INFO: ************LocalUsers :***********
DefaultAccount noguestaccount WDAGUtilityAccount wintel

2025-03-19 12:36:15 AUTO-INFO: ***********Timezone : ***********
@{caption=(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague}

Name           : Microsoft Visual C++ 2022 X64 Additional Runtime - 14.36.32532
Version        : 14.36.32532
PSComputerName : W5DSECP002
RunspaceId     : 62e223c7-b496-4c6b-9d57-f801ea23b0db
Name           : Microsoft Edge
Version        : 128.0.2739.67
PSComputerName : W5DSECP002
RunspaceId     : 62e223c7-b496-4c6b-9d57-f801ea23b0db
Name           : BigFix Client
Version        : 10.0.7.52
PSComputerName : W5DSECP002
RunspaceId     : 62e223c7-b496-4c6b-9d57-f801ea23b0db
Name           : VMware Tools
Version        : 12.4.5.23787635
PSComputerName : W5DSECP002
RunspaceId     : 62e223c7-b496-4c6b-9d57-f801ea23b0db
Name           : Symantec Endpoint Protection
Version        : 14.3.8289.5000
PSComputerName : W5DSECP002
RunspaceId     : 62e223c7-b496-4c6b-9d57-f801ea23b0db
Name           : Veritas NetBackup Client
Version        : 10.0.0.1
PSComputerName : W5DSECP002
RunspaceId     : 62e223c7-b496-4c6b-9d57-f801ea23b0db
Name           : Microsoft Monitoring Agent
Version        : 10.19.10014.0
PSComputerName : W5DSECP002
```

```
RunspaceId     : 62e223c7-b496-4c6b-9d57-f801ea23b0db
Name          : Microsoft Visual C++ 2022 X86 Additional Runtime - 14.36.32532
Version       : 14.36.32532
PSComputerName : W5DSECP002
RunspaceId     : 62e223c7-b496-4c6b-9d57-f801ea23b0db
Name          : Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.36.32532
Version       : 14.36.32532
PSComputerName : W5DSECP002
RunspaceId     : 62e223c7-b496-4c6b-9d57-f801ea23b0db
Name          : Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.36.32532
Version       : 14.36.32532
PSComputerName : W5DSECP002
RunspaceId     : 62e223c7-b496-4c6b-9d57-f801ea23b0db
2025-03-19 07:36:57 AUTO-INFO: *****************The OU Evidence Section Start *******************
2025-03-19 07:36:57 AUTO-INFO: The New VM W5DSECP002 is part of OU :
CN=W5DSECP002,OU=HUN,OU=Servers,DC=myl,DC=com
2025-03-19 07:36:57 AUTO-INFO: *****************The OU Evidence Section End*******************
***********************DNS Evidence Start****************
Server:  W0BVADC002.myl.com
Address:  172.20.24.19
Name:    W5DSECP002.myl.com
Address:  10.6.176.142
***********************DNS Evidence End****************
2025-03-19 07:37:17 AUTO-INFO: ******************************Scom Agent Status
Start************************
2025-03-19 07:38:37 AUTO-INFO: ******************************Scom Agent Status Ended
************************
**************************************VM Backup Evidence Start ***********************************
Backup Evidence Log Started
  Max Jobs This Client: Not Specified
 Client:            W5DSECP002
 Backup ID:           W5DSECP002_1742384404
 Policy:            VAPI-5D-MANUAL-BACKUP
 Policy Type:         VMware (40)
 Proxy Client:        (none specified)
 Creator:            root
 Name1:              (none specified)
 Sched Label:         monthly
 Schedule Type:        FULL (0)
 Retention Level:    1 week (0)
 Backup Time:         Wed 19 Mar 2025 12:40:04 PM CE (1742384404)
 Elapsed Time:       653 second(s)
 Expiration Time:    Wed 26 Mar 2025 12:40:04 PM CE (1742989204)
 Maximum Expiration Time:   Wed 26 Mar 2025 12:40:04 PM CE (1742989204)
 Compressed:          no
 Client Encrypted:  no
 Kilobytes:          29710021
 Number of Files:    364850
 Number of Copies:  1
 Files File Name:   VAPI-5D-MANUAL-BACKUP_1742384404_FULL.f
 Backup Status:      0
VM Backup Evidence End
2025-03-19 08:17:28 AUTO-INFO: *****************Windows Patch Update Evidence
```

```
Started********************
2025-03-19 13:17:35 AUTO-INFO: Hot Fix List Before Install
2025-03-19 13:17:35 AUTO-INFO:
\\W5DSECP002\root\cimv2:Win32_QuickFixEngineering.HotFixID="KB5039889",ServicePackInEffect=""
\\W5DSECP002\root\cimv2:Win32_QuickFixEngineering.HotFixID="KB5012170",ServicePackInEffect=""
\\W5DSECP002\root\cimv2:Win32_QuickFixEngineering.HotFixID="KB5042881",ServicePackInEffect=""
\\W5DSECP002\root\cimv2:Win32_QuickFixEngineering.HotFixID="KB5043167",ServicePackInEffect=""
2025-03-19 13:17:35 AUTO-INFO: Hot Fix List End
2025-03-19 09:09:10 AUTO-INFO: *****************Windows Patch Update Evidence End********************
2025-03-19 09:09:10 AUTO-INFO: *****************Windows Update Setttings Start:********************
@{ComputerName=W5DSECP002; NoAUShutdownOption=1; NoAUAsDefaultShutdownOption=1;
NoAutoRebootWithLoggedOnUsers=1; DetectionFrequencyEnabled=1; DetectionFrequency=6;
RebootRelaunchTimeoutEnabled=0; NoAutoUpdate=1}
2025-03-19 09:09:33 AUTO-INFO: *****************Windows Update Setttings End:********************
2025-03-19 14:09:34 AUTO-INFO: The VM Registry Changes after Patching Started
2025-03-19 14:09:37 AUTO-INFO: The Registry path was found
2025-03-19 14:09:37 AUTO-INFO: The Registry settings have applied after patch
2025-03-19 14:09:37 AUTO-INFO: The Registry Settings after patch completed Sucessfully , Going for
Restarting of the Server to make the Changes .......
2025-03-19 14:09:37 AUTO-INFO: The VM Registry Changes after Patching Completed-Sucessfully
2025-03-19 14:14:48 AUTO-INFO: **********LocalAdministrators:************
	MYL\AG-GBL-SECADMIN MYL\AG-GBL-SRVADMIN MYL\AG-W5DSECP002-Priv MYL\Domain Admins
MYL\MGW BO Group W5DSECP002\wintel

2025-03-19 14:17:07 AUTO-INFO: *******list of softwares Installed ********
Name           : CrowdStrike Device Control
Version        : 7.10.18083.0
PSComputerName : W5DSECP002
RunspaceId     : 75fb1191-ba24-4d18-9fe3-94d187aacce4
Name           : BigFix Client
Version        : 10.0.7.52
PSComputerName : W5DSECP002
RunspaceId     : 75fb1191-ba24-4d18-9fe3-94d187aacce4
Name           : VMware Tools
Version        : 12.4.5.23787635
PSComputerName : W5DSECP002
RunspaceId     : 75fb1191-ba24-4d18-9fe3-94d187aacce4
Name           : Symantec Endpoint Protection
Version        : 14.3.8289.5000
PSComputerName : W5DSECP002
RunspaceId     : 75fb1191-ba24-4d18-9fe3-94d187aacce4
Name           : Veritas NetBackup Client
Version        : 10.0.0.1
PSComputerName : W5DSECP002
RunspaceId     : 75fb1191-ba24-4d18-9fe3-94d187aacce4
Name           : Qualys Cloud Security Agent
Version        : 5.0.0.17
PSComputerName : W5DSECP002
RunspaceId     : 75fb1191-ba24-4d18-9fe3-94d187aacce4
Name           : CrowdStrike Sensor Platform
Version        : 7.16.18613.0
PSComputerName : W5DSECP002
RunspaceId     : 75fb1191-ba24-4d18-9fe3-94d187aacce4
```

```
Name           : Microsoft Monitoring Agent
Version        : 10.19.10014.0
PSComputerName : W5DSECP002
RunspaceId     : 75fb1191-ba24-4d18-9fe3-94d187aacce4
Name           : CrowdStrike Firmware Analysis
Version        : 7.14.18456.0
PSComputerName : W5DSECP002
RunspaceId     : 75fb1191-ba24-4d18-9fe3-94d187aacce4
Start Time: 2025-03-19T14:22:19Z
End Time: 2025-03-19T18:17:19Z
Appliance is up
https://0b-vnemgr1/rest/v1/appliance_pools/48
Scheduling scan
Received Response: <Response [201]>
Schedule ID: 3734
Validating scan completion.............................................................. Done.
Received audit ID: 202626
Waiting for audit status to be either Failed, Cancelled or Finished.. Done.
SecurityScanPassed with total score: 0
SMB Auth: False
WMI Auth: False
****************************Tripwire Evidence End****************************************
Name of the newly created server : w5dsecp002
Operating System                : Windows 2022 Standard
Status of the server            : In Development
Gxp sensitive                   : No
Environment                     : PROD
ITSM Applicability              : false
Short description               : Komarom Symantec server
Company                         :
Level 2 Support group           : Global-IT-INF-Windows
technical approval group        : GLOBAL-IT-INFRA-SERVER Technical Approvers
qa approval group               : Global Quality Assurance Approvers
Global CSV                      : CSV Approver Group
Business approver group         :
Governance approval group       :
Support Organization            : Viatris
CI Group                        :
CI Subgroup                     :
Class                           : Windows Server
Function                        :
Type                            :
Manufacturer                    : VMware, Inc.
Vendor                          :
Part number                     :
version                         :
Location                        : Komarom
Change Management group         :
Area                            :
CI owner                        : Sudhir Narang
CI disposition                  :
Model                           : VMware, Inc. VMware20,1
Serial Number                   : VMware-42 04 93 42 23 ca c6 8e-f2 6d 9b 19 e7 d5 77 ae
```

```
IP address                 : 10.6.176.142
Correlation id             :
**********Service CI relationship Evidence Start**********
Parent : Symantec Antivirus - PROD
Child: w5dsecp002
RelationType : Depends on::Used by
**********Service CI relationship Evidence End**********
Name of the newly created server : w5dsecp002
Operating System             : Windows 2022 Standard
Status of the server         : In Development
Gxp sensitive               : No
Environment                 : PROD
ITSM Applicability           : true
Short description           : Komarom Symantec server
Company                     :
Level 2 Support group         : Global-IT-INF-Windows
technical approval group      : GLOBAL-IT-INFRA-SERVER Technical Approvers
qa approval group            : Global Quality Assurance Approvers
Global CSV                  : CSV Approver Group
Business approver group        :
Governance approval group       :
Support Organization          : Viatris
CI Group                   :
CI Subgroup                 :
Class                     : Windows Server
Function                   :
Type                      :
Manufacturer                : VMware, Inc.
Vendor                     :
Part number                 :
version                    :
Location                   : Komarom
Change Management group         :
Area                      :
CI owner                   : Sudhir Narang
CI disposition              :
Model                      : VMware, Inc. VMware20,1
Serial Number               : VMware-42 04 93 42 23 ca c6 8e-f2 6d 9b 19 e7 d5 77 ae
IP address                 : 10.6.176.142
Correlation id             :
**********Service CI relationship Evidence Start**********
Parent : Symantec Antivirus - PROD
Child: w5dsecp002
RelationType : Depends on::Used by
**********Service CI relationship Evidence End**********
```