ESET Tech Center

Knowledgebase > Diagnostics > Create a full memory dump of a VMware virtual machine

Create a full memory dump of a VMware virtual machine

Steef | ESET Nederland - 2023-06-05 - Comments (0) - Diagnostics

Issue

- You are running an ESET product on a VMware virtual machine
- You need to create a memory dump of a VMware virtual machine for troubleshooting purposes
- I. Create and download a virtual machine snapshot
- II. Use the vmss2core tool to create a memory dump from the virtual machine snapshot

Solution

I. Create and download a virtual machine snapshot

- 1. In the VMware environment, select the virtual machine that has issues.
- 2. Replicate the issue on the virtual machine.
- 3. Right-click the virtual machine \rightarrow **Snapshots** \rightarrow **Take snapshot**.

vm vSphere Client Menu 🗸						
	Summany Mon	10 Virtual Machine	s Datastores Netwo	ACTIONS ~		
	Actions - Windows to Virtual Machine Power Guest OS Snapshots Popen Remote Console Migrate Clone	Guest OS: Compatibility: VMware Tools: Co Take Snapshot. Manage Snapshots Revert to Latest Snapshot Consolidate				CPU USAGE 62 MHz MEMORY USAGE 860 MB STORAGE USAGE 39.09 GB
		Delete All Snapshots		Notes Edit Notes		^
	Compatibility Export System Logs			Custom Attributes Attribute	Value	^
B Windows 10 Virtual Machine	Edit Settings Move to folder Rename Edit Notes	8				- 11
	Add Permission			< Edit	N	o items to display
	Alarms Remove from Inventory Delete from Disk	Category De	scription	vSphere HA Failure	Response	^
Recent Tasks Alarms		•		Host failure	 Restart VMs 	*

4. Type the name, select the check box next to Snapshot the Virtual Machine's memory and click OK.

Take Snapsho	Windows 10 Virtual Machine	×
Name	My Snapshot	
Description		
Snapshot the virtual r	machine's memory	8
Quiesce guest file sys	stem (Needs VMware Tools installed)	
	CANCEL	

5. Right-click the virtual machine and select **Edit Settings**.

vm vSphere Client Menu	Q Search in all environments	1		C	® ~
1 2 8 2	🖧 Windows 1	IO Virtual Mach	ine 🕨 🖷 😻 🕴	ACTIONS ~	
	Summany Monito	r Configure Per	missions Datastores	Networks	
	Power Guest OS Snapshots	Guest OS: Compatibility: VMware Tools DNS Name: IP Addresses:			CPU USAGE 62 MHz MEMORY USA 860 MB STORAGE USA
	Clone	Host:			U 39.09 GE
	Fault Tolerance			V Notes Edit Notes	,
	Compatibility			Custom Attributes Attribute	, Volue
R Windows 10 Virtual Machine	Bedit Settings	©			
	Rename Edit Notes Taqs & Custom Attributes	<u></u>			
	Add Permission			A Edit	No items to display
	Alarms	Category	Description	A VSphere HA	Response
cent Tasks Alarms	Delete from Disk Update Manager			Host failure	✓ Restart VMs

6. Select the virtual machine \rightarrow click **Datastores** and click the datastore name.

vm vSphere Client Menu Q Search in all environments			٢
Vindows 10 Virtual Machine Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all environments Image: Second in all enviro	C ② ~	v Capacity v Fitter v Capacity v Fitter 4 TB 556:05 G	~
Recent Tasks Alarms		🔓 Export	1 items

7. Select the virtual machine, select the .vmsn file (VMware Snapshot file), click **Download** and save the file locally.

	SAN	ACTIONS ~				
-	Summary Monitor Configure	Permissions Files Hosts VM	5			
B	Q Search					
_				_		
		New Folder Delete Inflate Delete Delete	Upload Folder 🔐 Register VM	vnload □ Copy to →	Move to 🔊 Rename to	
		Name	Y Size Y	Modified T	Туре т	Path
		Windows 10 Virtual Machine-Snaps		04/06/2021, 4:09:3	VM Snapshot	
and the second s						
		-				
	Contraction and the second second					
	> 🛄 Windows 10 Virtual Machine					
		-				
		<				•
		v				17 item

II. Use the vmss2core tool to create a memory dump from the virtual machine snapshot

- 1. Download Vmss2core.
- 2. Select the check box next to I have read and agree to the Technical Preview License I also understand that Flings are experimental and should not be run on production systems.
- 3. Select the file for your operating system from the drop-down menu (for example, if you want to run the tool on Windows, select vmss2core-sb-8456865.exe) and click **Download**.

vmware [®] Flings	Q All Flings Login >
Vmss2core version 1.0.1 – March 17, 2021 ANALYZE SYMBOLS CORE CRASH DUMP DEBUGGING FORENSICS VCENTER [™] VMSS VMSS2CORE ZERO CONFIGURATION	Release Date: March 06, 2014 Communities: 營 vCenter™ Share on: ♥ f in
	Cookie Settings

- 4. Place the <u>vmss2core tool</u> and the VMware snapshot file (downloaded in Step 7) into the same folder.
- 5. Run the vmss2core (vmss2core-sb-8456865.exe in this example) in the command line with the following parameters:
 - $\circ~$ Specify the guest operating system from which the snapshot was created:
 - -W8 —Windows 8 and later or Windows Server 2012 and later.
 - -W —Windows 7 and older or Windows Server 2008 and older.
 - Virtual machine snapshot filename (for example, virtual machine name.vmsn).



vmss2core-sb-8456865.exe -W8 "virtual_machine_name.vmsn"

6. When the vmss2core tool completes the operation, it creates a memory dump file named memory.dmp that can be used for additional troubleshooting.

Related Content

- How do I generate a memory dump manually?
- How to reate a Wireshark log
 Run the Info_get.command on a Linux machine and send the logs to ESET Technical Support
- <u>Using tcpdump on a MacOS</u>
- Using Process Monitor to create log files
 Using tcpdump on a Virtual Appliance
- How do I use ESET Log Collector?