Anti-virus on VNX CIFS Servers

To scan viruses on your Windows File Servers using local or block (SAN) storage is easy – you just install an AV agent on the Windows Server and voila. But what if your Windows File Server is replaced by an emc VNX CIFS Server?

The VNX uses an optional agent called CAVA (Common Anti-virus Agent) that enables a filter driver on the CIFS Server that sends the file off to a third party AV server for scanning. If a virus signature is found, the VNX subsequently deletes the file.

Here's everything you need to set it up… (Note that versions described below may change over time).

emc CAVA for VNX Installation, Configuration and Administration

Create a Windows Server, preferably 2 or a couple of VMs and add to the domain.

Download VNX Common Event Enabler from here (291MB)…

You'll need to register an account on support.emc.com if you don't already have one (Powerlink account).

https://download.emc.com/downloads/DL48037_Common-Event-Enabler-6.3.1-for-Windows.iso

Install VNX Common Event Event Enabler 6.3.1 (includes CAVA) and a 3rd party AV product of your choice.
emc_VEE_Pack_x64_6.3.1.exe

You will also need to install <vnx nas version>_VNXFileCifsMgmt.exe which sadly is only available on CD2 of the Tools Pack that came with your VNX. If you've subsequently upgraded the NAS to a more recent version, you'll need to obtain the latest software from EMC. I was able to download the elusive software from a link sent to me by EMC support, even though I couldn't find it or search for it on Powerlink. The links below may work for you, it may not. Try it.

https://support.emc.com/search/?text="cifs%20tools"&facetResource=ST

or try this one…

https://support.emc.com/search/?text=Dl48750%20DL32448

Start, Administrative Tools, Celerra Management,
Expand Data Mover Management (you'll need to point it at the IP address of your CIFS interface)
Expand Anti-virus
Set file masks (don't use *.*), and exclude files that don't harbor viruses, configure CAVA CIFS Server name to exactly match that on the VNX CIFS Server name (may need to be in caps!), and IP addresses of CAVA AV Servers. Example viruschecker.conf shown below. How you get this into your viruschecker.conf is your problem. Personally, I'd take the easy option of using the gui, then manually edit the viruschecker.conf file using vi to fix any problems, remove square brackets and stuff. To edit the viruschecker.conf file manually on the datamover over ssh, log on as nasadmin, su to root and use these commands…

server_file server_2 -get viruschecker.conf viruschecker.conf

vi viruschecker.conf *(and tidy it up)*

server_file server_2 -put viruschecker.conf viruschecker.conf

> *CIFSserver=globalcifsserver -Note that this CIFS Server must reside on physical DM, not your CIFS Server on VDM*
> *Addr=<IP addresses of AV engines separated by semi colons> eg*

```
10.1.1.1:10.1.1.2
shutdown=viruschecking

excl=*.dwl:*.edb:*.fmb:*.fmt:*.fmx:*.frm:*.inp:*.ldb:*.ldf:*.
mad:*.maf:*.mam:*.maq:*.mar:*.mat:*.mda:*.mdb:*.mde:*.mdf:*.m
dn:*.mdw:*.mdz:*.ndf:*.ora:*.orc:*.ost:*.pst:*.sc:*.sqc:*.sql
:*.sqr:*.stm:*.tar:*.tmp:*.zip:????????:*RECYCLER*

masks=*.386:*.ace:*.acm:*.acv:*.acx:*.add:*.ade:*.adp:*.adt:*
.app:*.asd:*.asp:*.asx:*.avb:*.ax:*.ax?:*.bas:*.bat:*.bin:*.b
o?:*.btm:*.cbt:*.cdr:*.cer:*.cfm:*.chm:*.cla:*.class:*.cmd:*.
cnv:*.com:*.cpl:*.cpy:*.crt:*.csc:*.csh:*.css:*.dat:*.dbx:*.d
er:*.dev:*.dl?:*.dll:*.do?:*.do??:*.doc:*.docx:*.dot:*.drv:*.
dvb:*.dwg:*.eml:*.exe:*.fon:*.fxp:*.gadget:*.gms:*.gvb:*.hlp:
*.hta:*.htm:*.html:*.htt:*.htw:*.htx:*.im?:*.inf:*.ini:*.ins:
*.ins:*.isp:*.its:*.js:*.js?:*.jse:*.jtd:*.lgp:*.lib:*.lnk:*.
lnk:*.mad:*.maf:*.mag:*.mam:*.maq:*.mar:*.mas:*.mat:*.mau:*.m
av:*.maw:*.mb?:*.mda:*.mdb:*.mde:*.mdt:*.mdw:*.mdz:*.mht:*.mh
tm:*.mhtml:*.mod:*.mp?:*.mpd:*.mpp:*.mpt:*.mrc:*.ms?:*.msc:*.
msg:*.msh:*.msh1:*.ksh:*.msh1xml:*.msh2:*.msh2xml:*.mshxml:*.
msi:*.mso:*.msp:*.mst:*.nch:*.nws:*.obd:*.obj:*.obz:*.ocx:*.o
ft:*.olb:*.ole:*.ops:*.otm:*.ov?:*.pcd:*.pcd:*.pci:*.pdb:*.pd
f:*.pdr:*.php:*.pif:*.pl:*.plg:*.pm:*.pnf:*.pnp:*.pot:*.pot:*
.pp?:*.pp??:*.ppa:*.pps:*.pps:*.ppt:*.prc:*.prf:*.prg:*.ps1:*
.ps1xml:*.ps2:*.ps2xml:*.psc2:*.pwz:*.qlb:*.qpw:*.reg:*.rtf:*
.sbf:*.scf:*.sco:*.scr:*.sct:*.sh:*.shb:*.shs:*.sht:*.shtml:*
.shw:*.sis:*.smm:*.swf:*.sys:*.td0:*.tlb:*.tmp:*.tsk:*.tsp:*.
tt6:*.url:*.vb:*.vb?:*.vba:*.vbe:*.vbs:*.vbx:*.vom:*.vs?:*.vs
d:*.vsmacros:*.vss:*.vst:*.vsw:*.vwp:*.vxd:*.vxe:*.wbk:*.wbt:
*.wiz:*.wk?:*.wml:*.wms:*.wpc:*.wpd:*.ws:*.ws?:*.wsc:*.wsf:*.
wsh:*.xl?:*.xl??:*.xla:*.xls:*.xlt:*.xlw:*.xml:*.xnk:*.xtp
```

Create a service account in the domain and check the user rights

Create a local group *viruscheckers* on the CIFS Server using the local users and groups snap-in, and add your service account in.

Make your service account a local admin on the CAVA Servers and double check that the debug programs right in group policy has local administrators in it (windows default setting) or put the cava service account in it. This is needed for the CAVA service to query the OS on the VM to determine the AV engine.

GPO_name\Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment ***Debug Programs***

Restart the EMC CAVA service on the CAVA Vm's using this service account – note: it'll get assigned Log On As A Service rights automatically.

If you need to re-add rights to the CAVA service account in group policy for any reason (they've been stripped out in an update), then you'll need to also **restart the CAVA Service** on the VM before the CAVA Agent on the Datamover will re-recognise the AV engine.

In the EMC Celerra Management snap-in

Expand User Rights Assignment
Expand EMC Virus Check
Add
Select the service account in the Domain to give virus checking right to, Add, OK, OK

PuTTY/SSH to VNX Control Station
Login as *nasadmin*
server_viruschk server_2
You should see ONLINE, plus details of file masks and AV server used.

> *If you get Unknown AV Engine or Third Party AV engine, even though you're using McAfee or Sophos or one of the other*

supported AV engines, then something is up – HP Protect Tools can get in the way of the DM authenticating to the CAVA VM's. I'm using McAfee and although mcshield.exe is a known av engine and its running, it didn't pick it up because the ***password was getting scrambled by ProtectTools****. Check your AV policy being applied to the AV engine includes Network Drives. It may not. Until you solve this problem, set shutdown=viruschecking in your viruschecker.conf to shutdown=no to prevent it from stopping all the time. Use the snap-in to adjust this setting. Also make sure your viruschecker.conf is pointing as a global cifs server permanently resident on the physical datamover and not your cifs server on a virtual data mover thats actually sharing your filesystems.*

server_viruschk server_2 -audit
Should see details of viruses caught. This can be tested using EICAR test virus and dropping the file into the CIFS Share on the CIFS Server.
The file should get automatically deleted by your anti-virus software.

Reboot everything once it's all set up (CAVA Vm's). A reboot can cure most problems.

Common Commands via the CLI

Replace server_x with the data mover you are accessing eg server_2

server_viruschk server_x Shows if virus checking is running and scanning rules
server_viruschk server_x -audit Shows CAVA scanning stats and scan queue. Very useful to see if the CAVA queue is blocked
server_log server_x To see if there are any errors on the data movers
server_setup server_x –P viruschk –o start=64 Start the virus checker service on the data mover

server_setup server_x –P viruschk –o stop Stop the virus checker service on the data mover
server_viruschk server_x –fsscan fs1 –create Starts a virus scanning job a on file system
server_viruschk server_x –fsscan fs1 –delete Stops a virus scanning job on a file system
server_viruschk server_x –fsscan fs1 –list Show the scanning status

Debugging CAVA

You can set debug logging on the data mover

.server_config server_2 “param viruschk Traces=0x00000004” #turns on debug for AV in the server_log
.server_config server_2 “param viruschk Traces=0x00000000” #turns off debug for AV in the server_log

server_log server_x To see if there are any errors logged on the data movers.

Donate