The science behind the report:

Dell EMC Cyber Recovery protected our test data from a cyber attack

This document describes what we tested, how we tested, and what we found. To learn how these facts translate into real-world benefits, read the report Dell EMC Cyber Recovery protected our data from a cyber attack.

We concluded our hands-on testing on January 18, 2019. During testing, we determined the appropriate hardware and software configurations and applied updates as they became available. The results in this report reflect configurations that we finalized on November 16, 2018 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

System configuration information

The table below presents detailed information on the systems we tested.

Server configuration information	4 x Dell EMC VxRail V470F
BIOS name and version	Dell 2.8.0
Non-default BIOS settings	None
VxRail version	VxRail 4.5.218-9630256
Operating system name and version/build number	VMware ESXi, 6.5.0, 9298722
Date of last OS updates/patches applied	09/17/2018
Power management policy	Maximum Performance
Processor	
Number of processors	2
Vendor and model	Intel Xeon E5-2698 v4
Core count (per processor)	20
Core frequency (GHz)	2.20
Stepping	1

Server configuration information	4 x Dell EMC VxRail V470F
Memory module(s)	
Total memory in system (GB)	512
Number of memory modules	12
Vendor and model	Hynix HMA84GR7MFR4N-UH
Size (GB)	32
Type	DDR4-2400
Speed (MHz)	2,400
Speed running in the server (MHz)	2,400
Storage controller	
Vendor and model	Dell PERC H330 Mini
Cache size (GB)	N/A
Firmware version	15.17.09.06
Driver version	N/A
Storage	
Number of drives	9
Drive vendor and model	HGST SG0CW988HGS0071304PGA00
Drive size (GB)	1788.50
Drive information (speed, interface, type)	12Gbps, SAS, SSD
Network adapter	
Vendor and model	Intel Ethernet 82599 10G
Number and type of ports	2 x 10GbE
Driver version	18.5.17

Storage configuration information	2 x Data Domain servers
Model number	DD6300
Version	6.1.1.20-594920
Processor	Intel Xeon E5-2620 v3
Memory size (GB)	96
Number of shelves	1
Storage	
Number of drives	14
Drive vendor and model number	Seagate STMFSND2CLAR4000
Drive size	3.63TB
Drive information (speed, interface, type)	7.2K RPM SAS HDD

Storage configuration information	2 x Data Domain servers
Network	
Vendor and model	Broadcom BCM5727 1GbE
Number and type of ports	1GbE
Vendor and model	Quad Port 10GBase-T
Number and type of ports	4x 10GbE

Virtual machine configuration information	Cyber Recovery management	Index Engines host	NetWorker server	SQL server
VMware vSphere version	VMware ESXi, 6.5.0-9298722	VMware ESXi, 6.5.0-9298722	Vmware ESXi 6.5.0-9298722	VMware ESXi, 6.5.0-9298722
Software version	18.1.0-529	7.0.0-Build 1.1.0.2	9.1.0.2	SQL Server 2016
vCPU count	4	12	4	4
Memory size (GB)	10	256	8	8
Virtual disk	16GB	2TB	40GB	200GB
Virtual disk controller	VMware Paravirtual	VMware Paravirtual	VMware Paravirtual	VMware Paravirtual
Virtual NIC	VMXNET 3	VMXNET 3	VMXNET3	VMXNET 3
OS	CentOS 7	CentOS 7	Windows Server 2016	Windows Server 2016

How we tested

We installed and configured a four-node VxRail-V470 cluster. We deployed a SQL Server VM and a DVD Store 2 client driver VM together with infrastructure VMs on top of the cluster. We also deployed a Networker server and set up a backup policy to back up the SQL database to a storage pool managed by one of the two Data Domain appliances.

We deployed Cyber Recovery software and set up a replication relationship between the two Data Domain appliances. The first DD was used as a production backup appliance and the second DD was used as a Vault storage. We verified Cyber Recovery operations inside the vault. We also simulated a cyber attack by injecting virus to one of the point-in-time copies and used CyberSense to successfully detect the attack.

Setting up the VxRail cluster

1. Rack and cable the VxRail V470F nodes.
2. Configure the network. We used a top-of-rack (ToR) switch for 1Gb management and iDRAC connectivity, and one Dell Networking Force10 S4810 switch, configured with ICMP snooping enabled, with an ISL configured for redundancy for VxRail networking. We connected 1-10G networking port to each of the S4810 switches.
3. Configure the iDRAC for each VxRail node with a static IP address.
4. Power on all nodes.
5. Connect a PC to the ToR switch. Configure the PC with an IP address of 192.168.10.100, and connect to the VxRail Appliance via SSH to 192.168.10.200.
6. Change to the root user account, and provide the root password for the VxRail Manager VM.
7. Reconfigure the VM to use a production network address. Enter `/opt/vmware/share/vami/vami_set_network eth0 STATICV4 <IP> <netmask> <gateway>`
8. Open a browser, and connect to `https://<new IP address of the VxRail manager>`.
9. Click Get Started.
10. At the VxRail EULA, click Accept.
11. When all nodes have appeared on the Expected Nodes page, click Next.
12. Populate the page with corresponding information for internal vCenter, PSC, and VxRail hosts.
13. Click Next to go through System, Networks, vSphere vMotion, vSAN, VMNetworks, Solutions setup.
14. To begin the validation process, click Validate.
15. Resolve any issues that the validation process finds. Download the JSON file, and save it for later reference. If the build passes the validation checks, click Build VxRail.
16. Click Start Configuration.
17. After approximately 25 minutes, the build will complete. To continue, click Manage VxRail.
18. Log into the VxRail Manager with `administrator@vsphere.local` and the appropriate password to verify the completion.
19. To download and upgrade to the latest VxRail version, click CONFIG, and click Internet Upgrade.
20. Open a browser tab, connect to `https://<vcenter_address>` and verify the information is correct.

Creating a Windows Server 2016 VM

1. Via the VMware web client, right-click the first VxRail server.
2. Select Create a new virtual machine, and click Next.
3. Assign a name to the VM, and click Next.
4. Select the VxRail server as the host, and click Next.
5. Select the appropriate storage, and click Next.
6. Choose ESXi 6.5 and later, and click Next.
7. Choose Windows, choose Microsoft Windows Server 2016 (64-bit), and click Next.
8. Select 4 CPUs, 4GB RAM and 400GB hard disk, and click Next.
9. Click Finish.
10. Right-click the VM, and choose Edit Settings.
11. Connect the VM virtual CD-ROM to the Microsoft Windows Server 2016 installation disk.
12. Start the VM.

Installing Microsoft Windows Server 2016

1. Open the VM console.
2. Leave the language, time/currency format, and input method as default, and click Next.
3. Click Install Now.

4. Choose Windows Server 2016 Datacenter Edition (Server with a GUI), and click Next.
5. Accept the license terms, and click Next.
6. Click Custom: Install Windows only (advanced).
7. Select Drive 0 Unallocated Space, and click Next, at which point Windows begins automatically and restarts automatically after completing.
8. Enter the administrator password twice, and click OK.
9. Install VMware Tools.
10. Reboot the server.
11. Connect the machine to the Internet and install all available Windows updates. Restart as necessary.
12. Enable remote desktop access.
13. Set up networking for the data network:
    a. Click Start, click Control Panel, right-click Network Connections, and choose Open.
    b. Right-click the VM traffic NIC, and choose Properties.
    c. Uncheck TCP/IP (v6).
    d. Select TCP/IP (v4), and choose Properties.
    e. Set the IP address, subnet, gateway, and DNS server.

Installing SQL Server 2016

1. Deploy a Windows Server 2016 VM named SQL1, and log in as administrator.
2. Mount the installation DVD for SQL Server 2016.
3. Click Run SETUP.EXE. If Autoplay does not begin the installation, navigate to the SQL Server 2016 DVD, and double-click it.
4. In the left pane, click Installation.
5. Click New SQL Server stand-alone installation or add features to an existing installation.
6. Select Enter the product key, and enter the product key. Click Next.
7. Click to accept the license terms, and click Next.
8. Click Use Microsoft Update to check for updates, and click Next.
9. Click Install to install the setup support files.
10. If there are no failures, click Next.
11. At the Setup Role screen, choose SQL Server Feature Installation, and click Next.
12. At the Feature Selection screen, select Database Engine Services, Full-Text and Semantic Extractions for Search, Client Tools Connectivity, Client Tools Backwards Compatibility, Management Tools – Basic, and Management Tools – Complete. Click Next.
13. At the Installation Rules screen, after the check completes, click Next.
14. At the Instance configuration screen, leave the default selection of default instance, and click Next.
15. At the Server Configuration screen, choose NT Service\SQLSERVERAGENT for SQL Server Agent, and choose NT Service\MSSQLSERVER for SQL Server Database Engine. Change the Startup Type to Automatic. Click Next.
16. At the Database Engine Configuration screen, select the authentication method you prefer. For our testing purposes, we selected Mixed Mode.
17. Enter a password for the system administrator account and confirm it.
18. Click Add Current user. This may take several seconds.
19. Click the Data Directories tab to relocate the system, user, and temp db files.
20. Change the location of the root directory to the D:\ volume.
21. Click Next.
22. At the Error and usage reporting screen, click Next.
23. At the Installation Configuration Rules screen, check that there are no failures or relevant warnings, and click Next.
24. At the Ready to Install screen, click Install.
25. After installation completes, click Close.

Installing the DVD Store2 client driver VM

1. Deploy a Windows Server 2016 VM in the VxRail Data Center, and log in as administrator.
2. Download and copy ds2sqlserverdriver.exe to C:\ on the VM.
3. Start the DVDStore2 workload:

```
C:\ds2sqlserverdriver.exe --target=<IP of the SQL Server> --ramp_rate=10 --run_time=10 --n_threads=32
-db_size=40GB -think_time=0 -warmup_time=5 -report_rate=1 -pct_newcustomers=40
```

Installing Microsoft Active Directory and DNS services

1. Deploy a Windows Server 2016 VM in the VxRail Data Center, and log in as administrator.
2. Launch Server Manager.
3. Click Manager, and click Add Roles and Features.
4. At the Before you begin screen, click Next.
5. At the Select Installation type screen, leave Role-based or feature-based installation selected, and click Next.
6. At the Server selection screen, select the server from the pool, and click Next. At the Select server roles screen, select Active Directory Domain services. Click Add Features, and click Next.
7. At the Select Features screen, click Next.
8. At the Active Directory Domain Services screen, click Next.
9. At the confirm installation selections screen, check Restart the destination server automatically if requested, and click install.
10. After the installation completes, a screen should pop up with configuration options. If not, click the task flag in the upper-right corner of Server Manager.
11. Click prompt this server to a Domain Controller.
12. At the deployment configuration screen, select Add a new forest. In the root domain name field, type `domain.local` and click Next.
13. At the domain controller option screen, leave the default values, and enter a password twice.
14. Click Next four times to accept default settings for DNS, NetBIOS, and directory paths.
15. At the Review Options screen, click Next.
16. At the Prerequisites Check dialog, allow the check to complete. If there are no relevant errors, check Restart the destination server automatically if required, and click Install.
17. When the server restarts, log on using test\Administrator and the specified password.
18. In the DNS manager, click Forward Lookup Zones, and click domain.local.
19. Right-click on the right panel, select New Host (A or AAAA), and specify the Host name and IP address for one of the VxRail servers. Check Create associated point (PTR) record, and click Add Host.
20. Repeat step 20 to add a DNS entry for all the VxRail servers, the Networker server, CR management host, SQL server, Data Domain servers, and Index Engines Server.

Setting up Data Domain hosts

1. Unpack and rack the Data Domain servers.
2. Cable and power on the Data Domain servers.
3. Connect an administrative console to the serial port on the back panel of the system, using 115200 baud rate.
4. To activate the console, press Enter.
5. The initial username is sysadmin and the initial password is the system serial number.
6. Accept the end user license agreement
7. Type `config setup` and follow the steps to set up the network.
8. Enable DDBoost:

```
sysadmin@DD2#ddboost enable
```

9. Create a new user account, and assign it to DDBoost:

```
sysadmin@DD# user add cradmin
sysadmin@DD# ddboost user assign cradmin
```

10. Open a browser, and connect to the management GUI of the first Data Domain: `https://<ip address of the management port>`
11. On the left pannel, click Replication.
12. On the top of the screen, click Create Pair.
13. Enter the FQDN of the second Data Domain as Destination System, and the path to source and destination mtrees. To complete the replication setup, click OK.

Setting up NetWorker

1. Deploy a Windows Server2016 VM in the VxRail Data Center.
2. Log into the VM with a user that has administrator privileges.
3. Disable firewall and automatic update on this Windows server.
4. Download the NetWorker software package from the EMC Online Support website to a temporary location. The package name is nw91_win_x64.zip.
5. Extract the NetWorker packages.
6. In the directory that contains the extracted NetWorker software, run NetWorker-9.1.0.0.exe.

7. In the Wizard Welcome page, select I agree to the license terms and agreements, and click Next.
8. In the Configure Windows Firewall page, select Do not configure the Windows Firewall, and click Next.
9. In the Wizard Options page, select Server and Client, and check the Networker Management Console option
10. To install the License manager server software, select NetWorker License Manager. The EMC NetWorker License Manager Installation and Administration Guide describes how to install and configure the NetWorker License Manager software.
11. Accept the default installation location, and click Next.
12. Click Install. When the installation completes, the Complete the Setup page provides the status of the installation and a link to the master setup log file. To complete the installation process, click Finish.
13. Launch the NetWorker application, and log in as administrator.
14. In the left menu, click localhost.
15. Click Launch Networker Administration, and log in as administrator.
16. From the left-hand menu, right-click Clients, and click New Client Wizard.
17. Enter the SQL server name as Client Name, and click Next.
18. Select Filesystem, and click Next.
19. Accept all default settings, and click Next.
20. Select the directory to be backed up, and click Next.
21. To create a new client, click Create.
22. In the pop-up window, click Devices.
23. Right-click Devices, and select New Device Wizard
24. Select Data Domain, and click Next.
25. In the Data Domain Configuration Checklist page, click Next.
26. Enter the FQDN of the first Data Domain server as a new DD system.
27. Enter the DDBoost user name and password created in the DD earlier.
28. Accept all other default settings, and click Next.
29. At the Select Folders for Devices screen, check the Backup box under the DD name, and provide a Networker Device Name for this mtree. Click Next.
30. In the Select Storage Nodes page, select an existing storage node from the drop-down menu, and click Next.
31. In the SNMP Monitoring Options page, accept all default options, and click Next.
32. Review the configuration settings, and complete the addition of DD to Networker.
33. At the top menu of the Management Console, click Protection.
34. Right-click Groups, and click New.
35. Select the SQL server from the list, and click OK to create a new group.
36. Right-click Platinum Policy, and click New.
37. Enter the name of the new workflow, and click OK.
38. In the right-hand pannel, right-click the newly created workflow, and click Properties.
39. Click the addition sign on the pop-up screen, and select the newly created group. Click OK.
40. To finish the configuration of the new backup workflow, click OK.

Setting up the Index Engines host

1. Deploy a new Linux VM with CentOS 7.
2. Download the installation binary from client FTP site, and copy it to the Linux VM.
3. Log into the VM as root user.
4. Disable the firewall:

```
> systemctl disable firewalld
```

5. Install Index Engines software:

```
>mv install-indexengines-6.7.8-1.5-el7.x86_64.bin /tmp
> cd /tmp
>python install-indexengines-6.7.8-1.5-el7.x86_64.bin --force
>dservice status all
>dservice restart all
```

6. Once the installation is completed and services started, open a browser and connect to the IP address of the Index Engines host
7. Log in as user admin with default password admin.
8. Click Administration->System->License to add a license file to the server.
9. Click Administration->Home->Index Manager->Add Index to add a new index `PT CyberSense`
10. Click Administration->Home->Index Service, and enable the CyberSense Data Collection option. Click Submit.
11. The Index Engines host is now ready to be added to the Cyber Recover Vault as an application host.

Setting up Cyber Recovery Management

1. Log into a Linux VM and disable the firewall:

```
>systemctl is-enabled firewalld
>systemctl stop firewalld
>systemctl disable firewalld
```

2. Disable SELinux by editing `/etc/selinux/config`
3. Reboot the host and verify SELinux and firewall are disabled:

```
>sestatus
>systemctl status firewalld
```

4. Install docker and docker composer:

```
>yum install -y docker-ce
>systemctl enable docker
>systemctl start docker
>docker version
>sudo curl -L https://github.com/docker/compose/releases/download/1.21.0/docker-compose-
$(uname -s)-$(uname -m) -o /usr/local/bin/docker-compose
>sudo chmod +x /usr/local/bin/docker-compose
>docker-compose version
```

5. Download the CR installation tarball, and unzip it.
6. Install Cyber Recovery software:

```
>cd staging
>run ./crsetup.sh and follow the steps to complete the installation
```

7. Once installation is completed, open a browser and connect to `https://<IP address of the CR management host>:14777`
8. Log in as user `crso` and provide the password configured during installation process.
9. Follow the initialization process to create a new user account, and create a new vault storage (in this case, the second Data Domain server=).
10. In the upper-right corner, click System Settings, and click License.
11. Choose the license file you received from Dell EMC, and click Add to license the CR appliance.
12. Set up a new policy by specifying the vault storage and mtree path.
13. Click the Policies tab, and select the newly created policy. Click Actions.
14. From the drop-down menu, select Sync Copy. A new job will be created by synchronizing the two Data Domains and creating a new point-in-time copy inside the vault.
15. To verify the job is completed successfully and a new copy is created, click the Policies tab, and click Copies).
16. Click Assets, and click Applications.
17. Click the Add button to add the Index Engines host to the vault by providing the host name, root user account, and password.
18. Once the application host is added, go to Policies and Copies.
19. Select the copy you want to analyze, and click Analyze.
20. Select the Index Engines host just added, and from the drop-down menu, select Other for the data type.
21. To start a CyberSense analyze job, click Apply.
22. To simulate a cyber attack, introduce some compromised data to the production Data Domain. In our test, we used two infected files provided by Index Engines.
23. Repeat steps 13 through 15 to sync and create a new copy inside the vault with the two infected files included.
24. Select the newly created copy you want to analyze, and click Analyze.
25. Select the Index Engines host, and from the Data type drop-down menu, select Other.
26. To start a CyberSense analyze job, click Apply.
27. Once the analyze job is completed, click the Alerts and Events tab on the left menu of Cyber Recovery.
28. Verify that Cyber Recovery received an alert message "Suspicious point-in-time copy" from Index Engines.

Read the report at http://facts.pt/rkew01n ▶

This project was commissioned by Dell EMC.

Principled Technologies®

Facts matter.®