



cDOT Anti Virus

Synopsis: This document details the cDOT AV Standard for Deployment in TR.

Segment: Unified Storage Engineering

Authors: Ian Daniel

Contributors: Ken Zola, Haris Kazazic, Brett Truhler

Document Version: V1.1

Date: 21st July 2015

Document Status: Release

CONFIDENTIAL INFORMATION

This document contains information proprietary to Thomson Reuters and may not be reproduced, disclosed or used in whole or part without express permission of Thomson Reuters.

© Thomson Reuters 2015



1 Contents

Table of Contents

1	Contents.....	2
1.1	Introduction.....	4
1.2	Document Scope	4
1.3	References	4
1.4	Change History	4
1.5	Distribution List.....	4
1.6	Glossary.....	4
2	AV Overview.....	5
3	TR AV Architecture	6
3.1	Servers.....	6
3.1.1	Overview	6
3.1.2	Server Requirements	6
3.1.3	AV Server Architecture.....	6
3.1.4	AV Scanner Domain Accounts.....	6
3.1.5	NetApp AV Connector Accounts on Vservers	7
3.1.5.1	Create a Read Only Role.....	7
3.1.5.2	Create the AV Login	7
3.1.5.3	Add a Domain Tunnel.....	7
4	NetApp AV Cluster Configuration	8
4.1	Overview	8
4.1.1	NetApp Cluster AV Configuration	8
4.1.1.1	Create a Scanner Pool On the Cluster	8
4.1.1.2	Associate a Scanner Pool with a Vserver	8
4.1.1.3	Create an On Access Policy (There is a default_CIFS policy you would normally use)	8
4.1.1.4	Disable Mandatory Scanning (Run on cluster vserver)	8
4.1.1.5	Enable Vserver On Access Policy (If Not Using The Default)	9
4.1.1.6	Enable Vserver Virus Scanning.....	9
5	AV Software Testing	10
5.1	Overview	10
5.1.1	Initial Vserver Configuration	10
5.1.1.1	vserver.....	10
5.1.1.2	LIF	10
5.1.1.3	Shares.....	10
5.2	Vserver AV Configuration	11
5.2.1.1	Apply the scanner pool to the vserver	11
5.2.1.2	Enable Scanning	11
5.2.1.3	Show Status.....	11
5.2.1.4	Check Log Entries For VSCAN Information	11
5.3	Virus Test File.....	12
6	cDOT AV Test Plan	13
6.1	CIFS Test Shares	13

6.2 CIFS Test Clients13

6.3 SI Functional Tests.....14

6.3.1 Single AV Server 14

6.3.2 Active/Passive AV Servers..... 16

6.3.3 Active/Active AV Servers..... 21

6.4 SI Performance Tests24

6.5 SI Summary.....24

1.1 Introduction

This document provides details of the current cDOT AV standard and deployment guidelines. This is for cDOT 8.2.1 and higher.

1.2 Document Scope

Scope of the document is cDOT AV for CIFS only. It does not provide installation instructions for the Trend AV products in a production environment. It will detail the installation in a test environment to show how it was installed for test purposes in the SI lab.

1.3 References

	Document	Version	Date	Author
1.	ServerProtect Getting Started Guide http://www.trendmicro.com/ftp/documentation/guides/GSG_SPNAF58.pdf	SP1	January-2014	Trend Micro
2.				

1.4 Change History

Ver	Date	Author	Key Changes
0.1	7-May-2015	Ian Daniel	Initial version
0.2	25-June-2015	Ian Daniel	Updated
0.3	26-June-2015	Ian Daniel	Updated to include service pack
0.4	27-June-2015	Ian Daniel	Updated images and pre-requisites.
0.5	31-June-2015	Ian Daniel	Fixed error in examples. Clarified AD account requirements. Added logfile check for vscan information. Added test plan.
0.6	15-July-2015	Ian Daniel	Added test cases. Updated wording to cater for multiple configs.
0.7	17-July-2015	Ian Daniel	Added example commands and completed the cDOT configuration tests.
0.8	20-July-2015	Ian Daniel	Updated tests. Updated Read Only Account.
0.9	20-July-2015	Ian Daniel	Updated Read Only Account.
1.0	20-July-2015	Ian Daniel	Updated with test results
1.1	20-July-2015	Ian Daniel	Removed Installation Instructions and non-storage related tasks

1.5 Distribution List

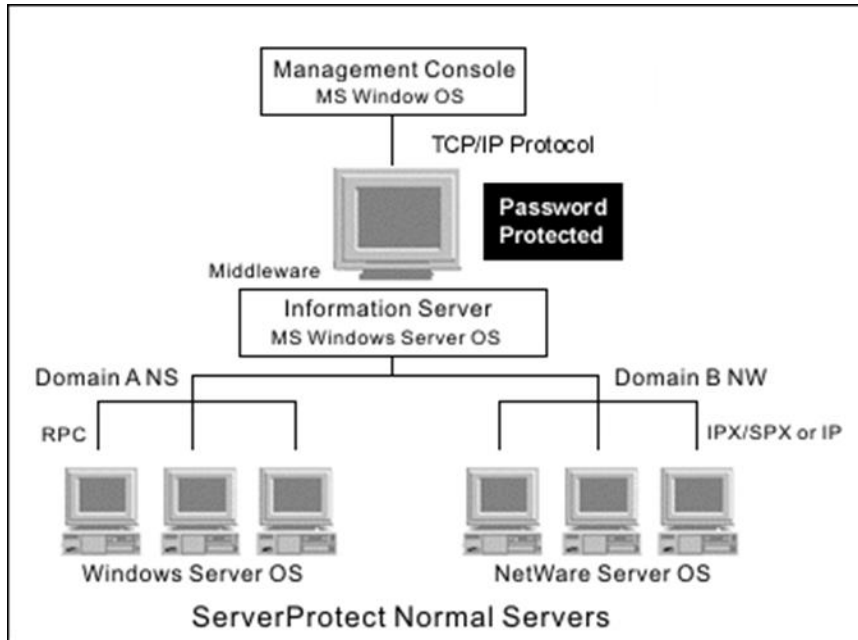
Name	Role
Sridhar Chevendra	Reviewer
Kevin Atkin	Customer

1.6 Glossary

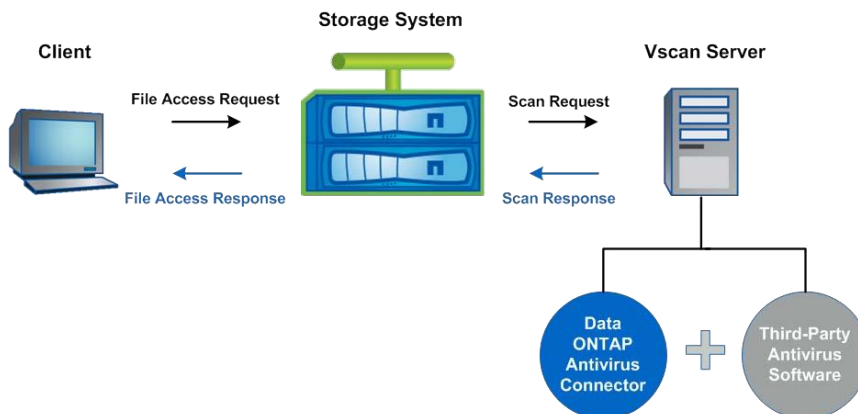
Term	Definition

2 AV Overview

This document is intended to provide a reference for AV deployments within TR for Clustered DataONTAP (cDOT). The AV solution is Trend ServerProtect and is a three tiered system as shown below.



The flow of data is shown in the diagram below. The vscan server is what Trend refer to as a normal server in the tiered architecture shown above.



On each vscan server there will be an AntiVirus connector installed which facilitates communication between the AV server software and the cDOT cluster.

Note: The AV solution is supported by Clustered DataONTAP 8.2.1 and later.

3 TR AV Architecture

3.1 Servers

3.1.1 Overview

The TR A/V server solution for cDOT is still under discussion so we are going to test 3 different configurations in order to ensure that whatever the final solution is we have covered it. The configurations we will test are:

- Single Server (**Current Solution**).
- Active/Passive Servers in a pool.
- Active/Active Servers in a pool.

We will also test with Mandatory scanning both enabled and disabled.

3.1.2 Server Requirements

The servers must run Windows Server (either 2008 or 2012), they will need .NET 3.0 or higher and will need to have SMB2.0 enabled on them.

The software is supported on virtual machines but careful assignment of workloads will need to be done in order to ensure the solution is performant.

3.1.3 AV Server Architecture

The approach we will be following is to use AV scanning configured on the cluster itself similar to how we currently configure it in 7-Mode. There are still vserver tasks to be completed but this approach reduces the overall complexity of the solution.

In order to ensure the solution is easy to manage it is proposed that we install all 3 software components on each VM used to scan a cluster.

Note: The current cDOT AV architecture for Trend servers is in review and the final configuration is not yet available. We are testing all permutations we can in these tests. The assumption is day one deployment will be a single AV server on the cluster as per 7-Mode with mandatory scanning disabled.

3.1.4 AV Scanner Domain Accounts

There needs to be a Domain account available to the scanner software and also the SVM in order to enable the AV to function correctly. Use of a single account for this is recommended as it reduces complexity and is easier to manage and maintain.

Accounts should have the following properties set:

- Password never expires
- User Can not change password

Note: We will use the account: TLR\svcavcdot for this work in SI but if there is already an account for virus scan usage please re-use it. The only requirement is that it is used consistently and that you have the password. The AD accounts in Production are secured via a password vault called CyberArk.

3.1.5 NetApp AV Connector Accounts on Vservers

There needs to be an account on the cluster or vserver that supports ontapi connections. To add this account do the following.

Note: we use the same Domain account used for the Trend A/V Software but with a read only role. We also need a domain tunnel to enable domain authentication.

Make sure the LIF firewall policy on the vserver LIF is set to mgmt..

3.1.5.1 [Create a Read Only Role](#)

```
eag-nasor-clus1-8040::> role create -role vscanro -cmddirname network -access  
readonly -query "" -vserver eag-nasor-clus1-8040  
(security login role create)
```

3.1.5.2 [Create the AV Login](#)

```
eag-nasor-clus1-8040::> security login create -username TLR\svcavcdot -  
application ontapi -authmethod domain -role vscanro -vserver eag-nasor-clus1-  
8040  
(security login create)
```

3.1.5.3 [Add a Domain Tunnel](#)

```
eag-nasor-clus1-8040::> domain-tunnel create -vserver silab-avcdot-01  
(security login domain-tunnel create)
```

```
eag-nasor-clus1-8040::> domain-tunnel show  
(security login domain-tunnel show)  
Tunnel Vserver: silab-avcdot-01
```



4 NetApp AV Cluster Configuration

4.1 Overview

The cDOT vservers are configured as follows.

4.1.1 NetApp Cluster AV Configuration

4.1.1.1 Create a Scanner Pool On the Cluster

The following command can be used to create a scanner pool

```
vserver vscan scanner-pool -vserver VSERVER_NAME -scanner-pool POOL_NAME -  
servers SERVER_IP_ADDRESSES -privileged-users AV_AD_ACCOUNT
```

Example

```
eag-nasor-clus1-8040::> vscan scanner-pool create -vserver eag-nasor-clus1-  
8040 -scanner-pool Active-Vscan-Pool -servers 10.220.177.203 -privileged-  
users TLR\svcavcdot  
(vserver vscan scanner-pool create)
```

4.1.1.2 Associate a Scanner Pool with a Vserver

The following command can be used to associate a scanner pool with a vserver

```
vserver vscan scanner-pool apply-policy -vserver VSERVER_NAME -scanner-pool  
POOL_NAME -scanner-policy primary
```


Example

```
eag-nasor-clus1-8040::> vscan scanner-pool apply-policy -vserver silab-avcdot-01 -  
scanner-pool Active-Vscan-Pool -scanner-policy primary  
(vserver vscan scanner-pool apply-policy)
```


4.1.1.3 Create an On Access Policy (There is a default_CIFS policy you would normally use)

The following command can be used to define an on-access policy for a vserver. Normally you would leave it using the default policy on the cluster.

```
vserver vscan on-access-policy create -vserver VSERVER_NAME -policy-name  
POLICY_NAME -filters  -maxfile-size 3GB -file-ext-to-exclude "mp3","txt"
```

Note: In order to turn off mandatory scanning you need to specify a  in the filters option when creating a policy.

Example

```
eag-nasor-clus1-8040::> vscan on-access-policy create -vserver eag-nasor-  
clus1-8040 -policy-name TR-AV -protocol CIFS -filters  -max-file-size 2GB
```

4.1.1.4 Disable Mandatory Scanning (Run on cluster vserver)

The following command disables mandatory scanning for the default vscan policy on a vserver.

Example

```
eag-nasor-clus1-8040::> vscan on-access-policy modify -vserver eag-nasor-  
clus1-8040 -policy-name default_CIFS -filters - -max-file-size 2GB  
(vserver vscan on-access-policy modify)
```



4.1.1.5 Enable Verserver On Access Policy (If Not Using The Default)

The following command can be used to enable the on-access policy for a vservers

```
vserver vscan on-access-policy enable -vserver VSERVER_NAME -policy-name POLICY_NAME
```

4.1.1.6 Enable Vserver Virus Scanning

Use the following command to enable AV on a vservers

```
vserver vscan enable -vserver VSERVER_NAME
```

Note: There is a default On-Access policy that is created and applied to all SVMs..."default_CIFS" Modify this policy as needed.

Note: Each CIFS share upon creation has the option of -vscan-fileop-profile. Use this option to remove a CIFS share from vscan.

5 AV Software Testing

5.1 Overview

The scanning will be configured on the cDOT cluster and enabled on a CIFS vserver. Mandatory scanning will be disabled on the vserver by modifying the default vsan policy. A virus file will be introduced to the CIFS share and results will be logged.

5.1.1 Initial Vserver Configuration

The vserver is detailed below with appropriate settings.

5.1.1.1 [vserver](#)

```
eag-nasor-clus1-8040::> vserver show -vserver silab-avcdot-01

Vserver: silab-avcdot-01
Vserver Type: data
Vserver UUID: 849241a1-1b32-11e5-9750-123478563412
Root Volume: silab_avcdot_01_rootvol
Aggregate: aggr1_data_sata2000_n03
Name Service Switch: file
Name Mapping Switch: file
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: C.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Allowed Protocols: cifs
Disallowed Protocols: nfs, fcp, iscsi, ndmp
Is Vserver with Infinite Volume: false
QoS Policy Group: -
```

5.1.1.2 [LIF](#)

```
eag-nasor-clus1-8040::> net int show -vserver silab-avcdot-01
(network interface show)

Vserver      Logical   Status   Network      Current   Current   Is
Interface    Admin/Oper Address/Mask Node       Port      Home
-----
silab-avcdot-01
  silab-avcdot-lif-01
    up/up      10.220.181.63/25  eag-nasor-clus1-8040lt-03
                                     a0a-2003
                                     true
```

5.1.1.3 [Shares](#)

```
eag-nasor-clus1-8040::> cifs share show -vserver silab-avcdot-01

Vserver      Share      Path      Properties Comment ACL
-----
silab-avcdot-01
  admin$      /          browsable -      -
silab-avcdot-01
  Control     c$         /          oplocks  -      BUILTIN\Administrators / Full
  ipc$       /          browsable -      -
  changenotify
  browsable
3 entries were displayed.
```

5.2 Vserver AV Configuration

This configures the vservers to use the cluster based scanner pool and enables scanning.

5.2.1.1 [Apply the scanner pool to the vservers](#)

```
eag-nasor-clus1-8040::> vscan scanner-pool apply-policy -vserver silab-avcdot-01 -
scanner-pool Active-Vscan-Pool -scanner-policy primary
(vserver vscan scanner-pool apply-policy)
```

5.2.1.2 [Enable Scanning](#)

```
eag-nasor-clus1-8040::> vscan enable -vserver silab-avcdot-01
(vserver vscan enable)
```

5.2.1.3 [Show Status](#)

```
eag-nasor-clus1-8040::> vscan show
(vserver vscan show)
```

Vserver	Vscan Status
TESTRESERVE-N03	
	off
cistest-e0010	off
cistest-e0013	off
orlab-cdot-fas8040-e0001	off
orlab-cdot-fas8040-e0002	off
orlab-cdot-fas8040-e0003	off
orlab-cdot-fas8040-e0004	off
orprod-e0001	off
reserve-n01-10001	off
reserve-n02-10001	off
reserve-n03-10001	off
reserve-n04-10001	off
	off
Vserver	Vscan Status
silab-avcdot-01	on
silab-e0002	off
silab-e0003	off

15 entries were displayed.

5.2.1.4 [Check Log Entries For VSCAN Information](#)

```
eag-nasor-clus1-8040::> log show -severity INFORMATIONAL -event vscan*
(event log show)
```

Time	Node	Severity	Event
6/30/2015 23:23:17	eag-nasor-clus1-8040ht-01	INFORMATIONAL	vscan.enabled: Vscan is enabled on Vserver 'silab-avcdot-01'.
6/30/2015 23:23:08	eag-nasor-clus1-8040ht-01	INFORMATIONAL	vscan.disabled: Vscan is disabled on Vserver 'silab-avcdot-01'.
6/30/2015 00:00:36	eag-nasor-clus1-8040ht-01	INFORMATIONAL	vscan.newVersion.allocated: Vscan



version mechanism added new version-ID for Vserver 'silab-avcdot-02' corresponding to vendor 'trendmicro', version '757.759'.

6/30/2015 00:00:36 eag-nasor-clus1-8040ht-02

INFORMATIONAL vscan.newVersion.allocated: Vscan
version mechanism added new version-ID for Vserver 'silab-avcdot-01' corresponding to vendor 'trendmicro', version '757.759'.

4 entries were displayed.

5.3 Virus Test File

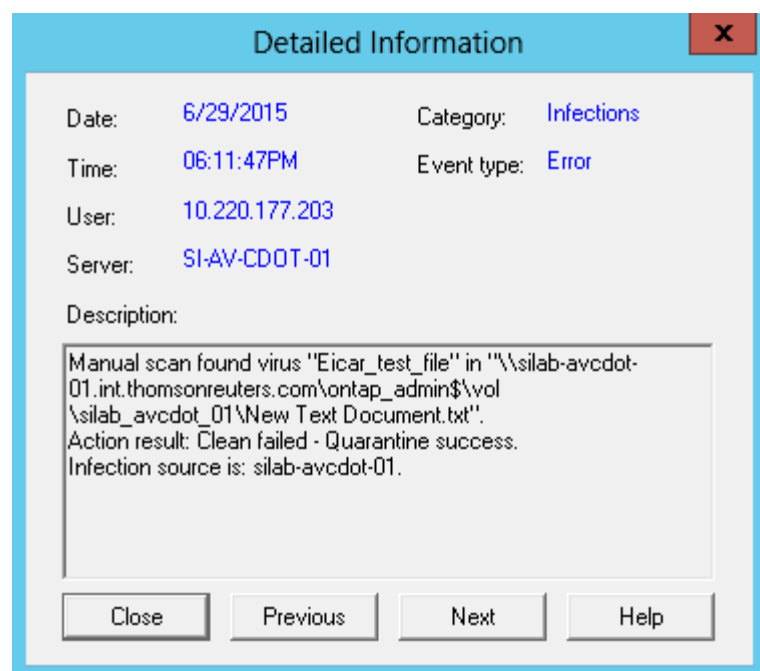
When you are ready to test mount the share you created on a workstation. Create a new file and edit it. Insert the virus string obtainable from this page into the file and save it.

The string looks like this.

X5OIP%@AP[4\PZX54(P^)7CC)7]\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*

<http://www.eicar.org/86-0-Intended-use.html>

The AV software should detect this string when you save the file and delete the file immediately. There will be a message logged in the management console as well as shown below.



6 cDOT AV Test Plan

The following test plan is to be used for testing cDOT AV in the SI environment. The test environment will use multiple shares configured with different access levels as follows.

6.1 CIFS Test Shares

We will create 4 test shares on the vserver being used to run AV tests. These will have the following permissions:

TLR\P-WEST-SI.C / Read
TLR\P-WEST-SI.C / Change
TLR\P-WEST-SI.C / Full Control
TLR\P-WEST-SI.C / No Access

Example

```
eag-nasor-clus1-8040::> cifs share access-control sho -vserver silab-avcdot-01
```

Vserver	Share Name	User/Group Name	Access Permission
silab-avcdot-01	avtest-chg	TLR\P-WEST-SI.C	Change
silab-avcdot-01	avtest-na	TLR\P-WEST-SI.C	No_access
silab-avcdot-01	avtest-ro	TLR\P-WEST-SI.C	Read
silab-avcdot-01	avtest-rw	TLR\P-WEST-SI.C	Full_Control

Test files will be created in each share using the test virus header shown earlier in the document.

6.2 CIFS Test Clients

The following VMs have been created for AV testing.

Server Name	OS Version	IP Address
SI-AV-CDOT-03	2012	10.220.177.81
SI-AV-CDOT-04	2012R2	10.220.177.104
SI-AV-CDOT-05	2008R2 SP1 Stnd	10.220.177.115
SI-AV-CDOT-06	2008R2SP1 Ent	10.220.177.157
SI-AV-CDOT-07	2008 SP2 x64	10.220.177.251

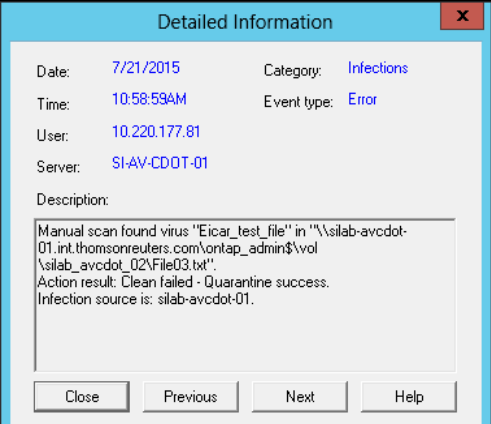
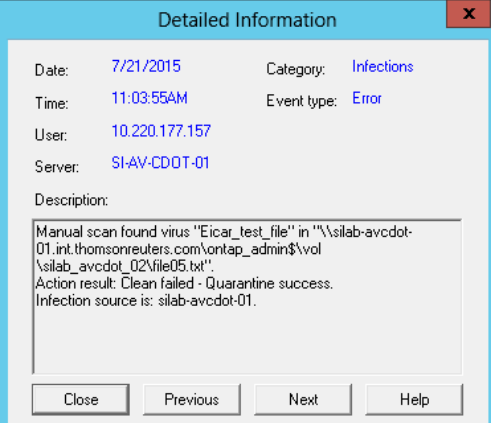
6.3 SI Functional Tests

The following tests are designed to cater for any eventual configuration we would have for cDOT A/V Servers.

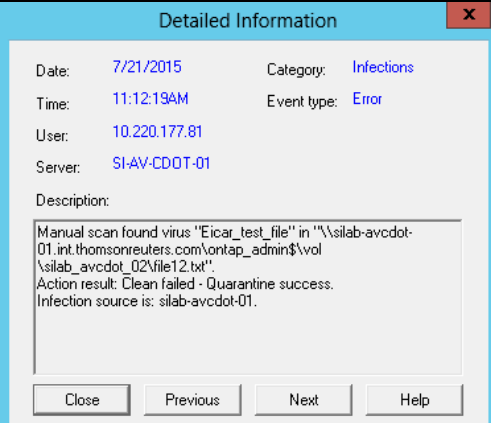
6.3.1 Single AV Server

Test ID	Test	Success Criteria	Notes/Results	Pass/Fail
6.3.1.1	<p>Create a cDOT A/V pool using a single server</p> <p>Example eag-nasor-clus1-8040::> vscan scanner-pool create -scanner-pool SS-Vscan-Pool -vserver eag-nasor-clus1-8040 -servers 10.220.177.203 -privileged-users TLR\svcavcdot</p> <p>Show Status eag-nasor-clus1-8040::> vscan scanner-pool show -vserver eag-nasor-clus1-8040</p>	Pool Created	<pre>eag-nasor-clus1-8040::> vscan scanner-pool show -vserver eag-nasor-clus1-8040 (vserver vscan scanner-pool show) Privileged Scanner Pool Vserver Pool Owner Servers Users Policy ----- -- eag-nasor-clus1-8040 cluster 10.220.177.203 TLR\svcavcdot idle SS-Vscan-Pool</pre>	PASS
6.3.1.2	<p>Ensure pool is set to primary on the vserver</p> <p>Example eag-nasor-clus1-8040::> vscan scanner-pool apply-policy -vserver silab-avcdot-01 -scanner-pool SS-Vscan-Pool -scanner-policy primary</p> <p>Show Status eag-nasor-clus1-8040::> vscan scanner-pool show-active -vserver silab-avcdot-01</p>	Vserver scanning options modified.	<pre>eag-nasor-clus1-8040::> vscan scanner-pool show-active -vserver silab-avcdot-01 (vserver vscan scanner-pool show-active) Vserver: silab-avcdot-01 List of Enabled Scanner Pools: SS-Vscan-Pool Merged List of IPs of Allowed Vscan Servers: 10.220.177.203 Merged List of Privileged Users: TLR\svcavcdot</pre>	PASS
6.3.1.3	<p>Set Mandatory scanning on</p> <p>Example eag-nasor-clus1-8040::> vscan on-access-policy modify -vserver eag-nasor-clus1-8040 -policy-name default_CIFS -filters scan-mandatory -max-file-size 2GB</p>	Setting changed	<pre>eag-nasor-clus1-8040::> vscan on-access-policy show -vserver silab-avcdot-01 -fields filters (vserver vscan on-access-policy show) vserver policy-name filters ----- silab-avcdot-01 default_CIFS scan-mandatory</pre>	PASS



	Show Status eag-nasor-clus1-8040::> vscan on-access-policy show -vserver silab-avcdot-01 -fields filters			
6.3.1.4	Create test virus file in share with Read Access. Repeat for all OS versions (all VMs).	File cannot be created	File not created	PASS
6.3.1.5	Create test virus file in share with Change Access. Repeat for all OS versions (all VMs).	File cleaned by A/V server. Event generated on server.		PASS
6.3.1.6	Create test virus file in share with Full Access. Repeat for all OS versions (all VMs).	File cleaned by A/V server. Event generated on server.		PASS
6.3.1.7	Create test virus file in share with No Access. Repeat for all OS versions (all VMs).	File cannot be created	File not created	PASS
6.3.1.8	Stop services on configured A/V server	Services Stopped	Service stopped	PASS
6.3.1.9	Attempt to copy/access/write file on CIFS share. Repeat for all OS versions (all VMs).	Access is blocked as mandatory scanning is enabled.	Access Denied	PASS
6.3.1.10	Set Mandatory scanning off Example	Setting changed	eag-nasor-clus1-8040::> vscan on-access-policy show -vserver silab-avcdot-01 -fields filters (vserver vscan on-access-policy show)	PASS



	<pre>eag-nasor-clus1-8040:> vscan on-access-policy modify -vserver eag-nasor-clus1-8040 -policy-name default_CIFS -filters - -max-file-size 2GB</pre> <p>Show Status</p> <pre>eag-nasor-clus1-8040:> vscan on-access-policy show -vserver silab-avcdot-01 -fields filters</pre>		<pre>vserver policy-name filters ----- silab-avcdot-01 default_CIFS -</pre>	
6.3.1.11	Attempt to copy/access/write file on CIFS share. Repeat for all OS versions (all VMs).	<p>Access is allowed as mandatory scanning is disabled.</p> <p>Infected files can be written to the share.</p>	Shares are accessible and can be written to when permissions allow it. File with virus can be written and is not quarantined.	PASS
6.3.1.12	Restart services	Trend services are started	Service started	PASS
6.3.1.13	Attempt to access all files that were written with a virus header.	File is detected and cleaned		PASS

6.3.2 Active/Passive AV Servers

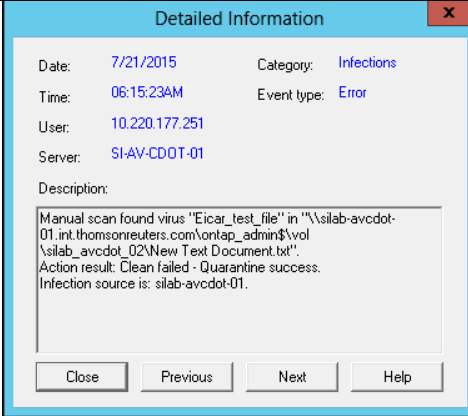
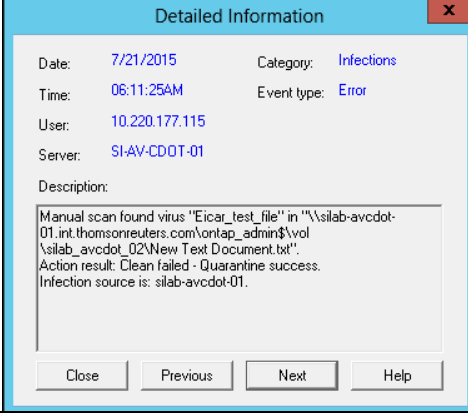
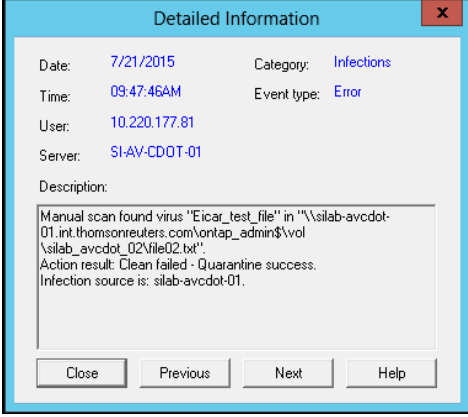
Test ID	Test	Success Criteria	Notes/Results	Pass/Fail
6.3.2.1	<p>Create a cDOT A/V pool to use a single server or re-use one already created.</p> <p>Example</p> <pre>eag-nasor-clus1-8040:> vscan scanner-pool create -scanner-pool</pre>	Pool modified or exists already	<pre>eag-nasor-clus1-8040:> vscan scanner-pool show -vserver eag-nasor-clus1-8040 (vserver vscan scanner-pool show) Scanner Pool Privileged Scanner Vserver Pool Owner Servers Users Policy ----- eag-nasor-clus1-8040 cluster 10.220.177.203 TLR\svcavcdot idle</pre>	PASS

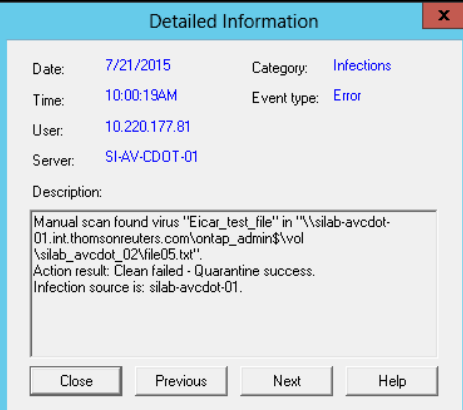


	SS-Vscan-Pool - vserver eag- nator-clus1- 8040 -servers 10.220.177.203 -privileged- users TLR\svcavcdot Show Status eag-nator- clus1-8040::> vscan scanner- pool show - vserver eag- nator-clus1- 8040		SS-Vscan- Pool	
6.3.2.2	Create second cDOT pool and add a single server Example eag-nator- clus1-8040::> vscan scanner- pool create - scanner-pool PS-Vscan-Pool - vserver eag- nator-clus1- 8040 -servers 10.220.177.222 -privileged- users TLR\svcavcdot Show Status eag-nator- clus1-8040::> vscan scanner- pool show - vserver eag- nator-clus1- 8040	Pool created	eag-nator-clus1-8040::> vscan scanner-pool show -vserver eag-nator- clus1-8040 (vserver vscan scanner-pool show) Scanner Pool Privileged Scanner Vserver Pool Owner Servers Users Policy ----- ----- ---- eag-nator-clus1-8040 cluster 10.220.177.222 TLR\svcavcdot idle PS-Vscan- Pool	PASS
6.3.2.3	Ensure one pool is set to primary and the other to secondary on the vserver Example eag-nator- clus1-8040::> vscan scanner- pool apply- policy -vserver silab-avcdot-01 -scanner-pool SS-Vscan-Pool - scanner-policy primary	Vserver scanning options modified.	eag-nator-clus1-8040::> vscan scanner-pool show -vserver silab- avcdot-01 (vserver vscan scanner-pool show) Scanner Pool Privileged Scanner Vserver Pool Owner Servers Users Policy ----- ----- ---- silab-avcdot-01 cluster 10.220.177.203, TLR\svcavcdot idle AA-Vscan- 10.220.177.222 Pool silab-avcdot-01 cluster 10.220.177.203, TLR\svcavcdot idle	PASS



	eag-nasor-clus1-8040::> vscan scanner-pool apply-policy -vserver silab-avcdot-01 -scanner-pool PS-Vscan-Pool -scanner-policy secondary Show Status eag-nasor-clus1-8040::> vscan scanner-pool show -vserver silab-avcdot-01		Active-10.220.177.222 Vscan-Pool silab-avcdot-01 cluster 10.220.177.222 TLR\svcavcdot secondary PS-Vscan-Pool silab-avcdot-01 cluster 10.220.177.203 TLR\svcavcdot primary SS-Vscan-Pool 4 entries were displayed. eag-nasor-clus1-8040::> vscan scanner-pool show-active -vserver silab-avcdot-01 (vserver vscan scanner-pool show-active) Vserver: silab-avcdot-01 List of Enabled Scanner Pools: PS-Vscan-Pool, SS-Vscan-Pool Merged List of IPs of Allowed Vscan Servers: 10.220.177.203, 10.220.177.222 Merged List of Privileged Users: TLR\svcavcdot	
6.3.2.4	Set Mandatory scanning on Example eag-nasor-clus1-8040::> vscan on-access-policy modify -vserver eag-nasor-clus1-8040 -policy-name default_CIFS -filters scan-mandatory -max-file-size 2GB Show Status eag-nasor-clus1-8040::> vscan on-access-policy show -vserver silab-avcdot-01 -fields filters	Setting changed	eag-nasor-clus1-8040::> vscan on-access-policy show -vserver silab-avcdot-01 -fields filters (vserver vscan on-access-policy show) vserver policy-name filters ----- ----- silab-avcdot-01 default_CIFS scan-mandatory	PASS
6.3.2.5	Create test virus file in share with Read Access. Repeat for all OS versions (all VMs).	File cannot be created	File not created	PASS

6.3.2.6	Create test virus file in share with Change Access. Repeat for all OS versions (all VMs).	File cleaned by A/V server. Event generated on server.		PASS
6.3.2.7	Create test virus file in share with Full Access. Repeat for all OS versions (all VMs).	File cleaned by A/V server. Event generated on server.		PASS
6.3.2.8	Create test virus file in share with No Access. Repeat for all OS versions (all VMs).	File cannot be created	File not created	PASS
6.3.2.9	Stop services on active A/V server	Services Stopped	Service Stopped Note: Need to stop ONTAP AV Connector service to simulate host down. If Trend stops and this service is running access can fail with Mandatory Scanning enabled.	PASS
6.3.2.10	Attempt to copy/access/write file on CIFS share. Repeat for all OS versions (all VMs).	Access is allowed as passive server takes over. File is cleaned.		PASS
6.3.2.11	Stop services on	Services Stopped	Note: Slight delay in file access Stopped Trend ServProtect service	PASS

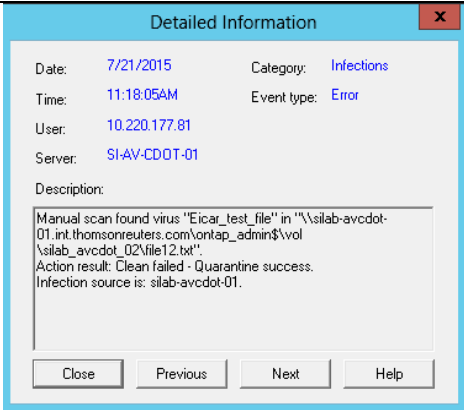
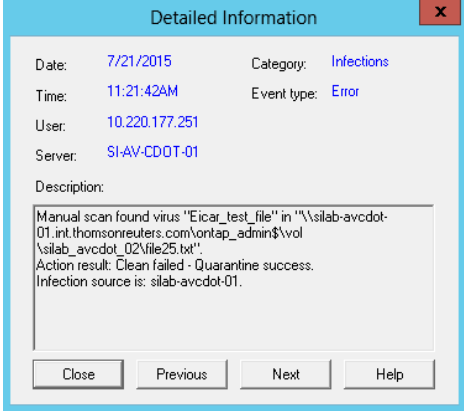
	passive A/V server			
6.3.2.12	Attempt to copy/access/write file on CIFS share. Repeat for all OS versions (all VMs).	Access is blocked as mandatory scanning is enabled.	Access to files is blocked	PASS
6.3.2.13	Set Mandatory scanning off Example eag-nasor-clus1-8040::> vscan on-access-policy modify -vserver eag-nasor-clus1-8040 - policy-name default_CIFS - filters - -max- file-size 2GB Show Status eag-nasor-clus1-8040::> vscan on-access-policy show -vserver silab-avcdot-01 -fields filters	Setting changed	eag-nasor-clus1-8040::> vscan on-access-policy show -vserver silab-avcdot-01 -fields filters (vserver vscan on-access-policy show) vserver policy-name filters ----- silab-avcdot-01 default_CIFS -	PASS
6.3.2.14	Attempt to copy/access/write file on CIFS share. Repeat for all OS versions (all VMs).	Access is allowed as mandatory scanning is disabled. Infected files can be written to the share.	Shares are accessible and can be written to when permissions allow it. File with virus can be written and is not quarantined.	PASS
6.3.2.15	Restart services	Trend services are started	Services restarted ok.	PASS
6.3.2.16	Attempt to access all files that were written with a virus header.	File is detected and cleaned		PASS



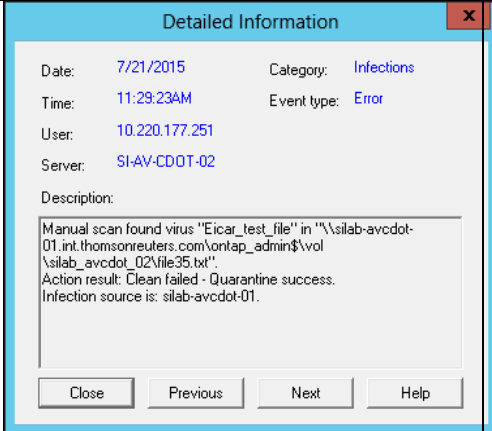
6.3.3 Active/Active AV Servers

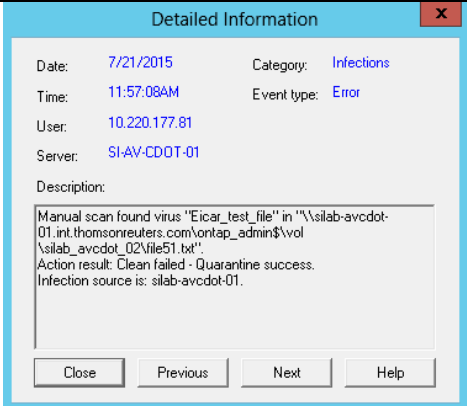
Test ID	Test	Success Criteria	Notes/Results	Pass/Fail
6.3.3.1	<p>Create cDOT A/V pool that uses two servers</p> <p>Example</p> <pre>vscan scanner-pool create -scanner- pool AA-Vscan-Pool- vserver eag-nasor- clus1-8040 -servers 10.220.177.203, 10.220.177.222 - privileged-users TLR\svcavcdot</pre> <p>Show Status</p> <pre>eag-nasor-clus1- 8040::> vscan scanner-pool show - vserver eag-nasor- clus1-8040</pre>	Pool created and contains 2 servers.	<pre>eag-nasor-clus1-8040::> vscan scanner-pool show -vserver eag- nasor-clus1-8040 (vserver vscan scanner-pool show) Scanner Pool Privileged Scanner Vserver Pool Owner Servers Users Policy ----- eag-nasor-clus1-8040 cluster 10.220.177.203, TLR\svcavcdot idle AA-Vscan- 10.220.177.222 Pool</pre>	PASS
6.3.3.2	<p>Ensure pool is set to active on the vserver</p> <p>Example</p> <pre>eag-nasor-clus1- 8040::> vscan scanner-pool apply- policy -vserver silab-avcdot-01 - scanner-pool AA- Vscan-Pool - scanner-policy primary</pre> <p>Show Status</p> <pre>eag-nasor-clus1- 8040::> vscan scanner-pool show- active -vserver silab-avcdot-01</pre>	Vserver scanning options modified.	<pre>eag-nasor-clus1-8040::> vscan scanner-pool show-active -vserver silab-avcdot-01 (vserver vscan scanner-pool show- active) Vserver: silab-avcdot-01 List of Enabled Scanner Pools: AA-Vscan-Pool Merged List of IPs of Allowed Vscan Servers: 10.220.177.203, 10.220.177.222 Merged List of Privileged Users: TLR\svcavcdot</pre>	PASS
6.3.3.3	<p>Set Mandatory scanning on</p> <p>Example</p> <pre>eag-nasor-clus1- 8040::> vscan on- access-policy modify -vserver eag-nasor-clus1- 8040 -policy-name default_CIFS - filters scan- mandatory -max- file-size 2GB</pre> <p>Show Status</p> <pre>eag-nasor-clus1- 8040::> vscan on- access-policy show -vserver silab-</pre>	Setting changed	<pre>eag-nasor-clus1-8040::> vscan on- access-policy show -vserver silab- avcdot-01 -fields filters (vserver vscan on-access-policy show) vserver policy-name filters ----- silab-avcdot-01 default_CIFS scan- mandatory</pre>	PASS



	avcdot-01 -fields filters			
6.3.3.4	Create test virus file in share with Read Access. Repeat for all OS versions (all VMs).	File cannot be created	File not created	PASS
6.3.3.5	Create test virus file in share with Change Access Repeat for all OS versions (all VMs).	File cleaned by A/V server. Event generated on server.		PASS
6.3.3.6	Create test virus file in share with Full Access. Repeat for all OS versions (all VMs).	File cleaned by A/V server. Event generated on server.		PASS
6.3.3.7	Create test virus file in share with No Access. Repeat for all OS versions (all VMs).	File cannot be created	File not created	PASS
6.3.3.8	Stop services on first A/V server.	Services Stopped	Service Stopped Note: Need to stop ONTAP AV Connector service to simulate host down. If Trend stops and this service is running access can fail with Mandatory Scanning enabled.	PASS



6.3.3.9	Attempt to copy/access/write file on CIFS share. Repeat for all OS versions (all VMs).	Access is allowed as second server takes over.		PASS
6.3.3.10	Stop services on second A/V server	Services Stopped	Service Stopped	PASS
6.3.3.11	Attempt to copy/access/write file on CIFS share. Repeat for all OS versions (all VMs).	Access is blocked as mandatory scanning is enabled.	Access failed.	PASS
6.3.3.12	Set Mandatory scanning off Example eag-nasor-clus1-8040::> vscan on-access-policy modify -vserver eag-nasor-clus1-8040 -policy-name default_CIFS -filters - -max-file-size 2GB Show Status eag-nasor-clus1-8040::> vscan on-access-policy show -vserver silab-avcdot-01 -fields filters	Setting changed	eag-nasor-clus1-8040::> vscan on-access-policy show -vserver silab-avcdot-01 -fields filters (vserver vscan on-access-policy show) vserver policy-name filters ----- silab-avcdot-01 default_CIFS -	PASS
6.3.3.13	Attempt to copy/access/write file on CIFS share. Repeat for all OS versions (all VMs).	Access is allowed as mandatory scanning is disabled.	Shares are accessible and can be written to when permissions allow it. File with virus can be written and is not quarantined	PASS
6.3.3.14	Restart services	Trend services are started	Services restarted ok.	PASS

6.3.3.15	Attempt to access all files that were written with a virus header.	File is detected and cleaned		PASS
----------	--	------------------------------	--	------

6.4 SI Performance Tests

Performance testing is outside the scope of this functional SI test.

6.5 SI Summary

All configurations of the Trend AV scanning option work. Of the three a single active pool would seem to yield the best overall service as it will load balance and also provide resilience. It was noted during testing that sometimes just stopping the Trend service would not cause another server to be used, you had to also stop the NetApp service as well (ONTAP AV Connector). In the event a server has failed this is not an issue. In the event Trend services fail for some reason this could cause problems. Leaving Mandatory scanning disabled will fix any such issues with odd failure conditions.