THOMSON REUTERS

# cDOT Anti Virus Delivery Deployment

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

**Segment:** Unified Storage Engineering

**Authors:** Ian Daniel

**Contributors:** Ken Zola, Haris Kazazic, Brett Truhler, Aaron Van De Hey

**Document Version:** V0.2
**Date:** 25th July 2015
**Document Status:** Draft

# 1 Contents

## Table of Contents

## 1.1 Introduction

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

## 1.2 Document Scope

Scope of the document is cDOT AV for CIFS only.

## 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 | 24-July-2015 | Ian Daniel | Initial version |
| 0.2 | 25-July-2015 | Ian Daniel | Updated to show behaviour when using trusted domain. |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## 1.5 Distribution List

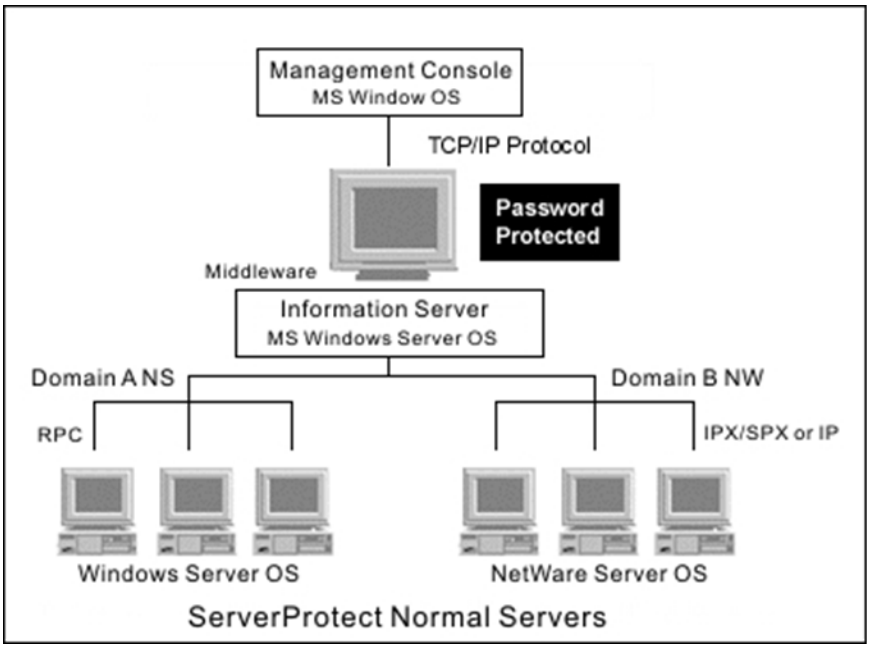
| Name | Role |
|---|---|
| Sridhar Chevendra | Reviewer |
| Aaron Van De Hey | Customer |

## 1.6 Glossary

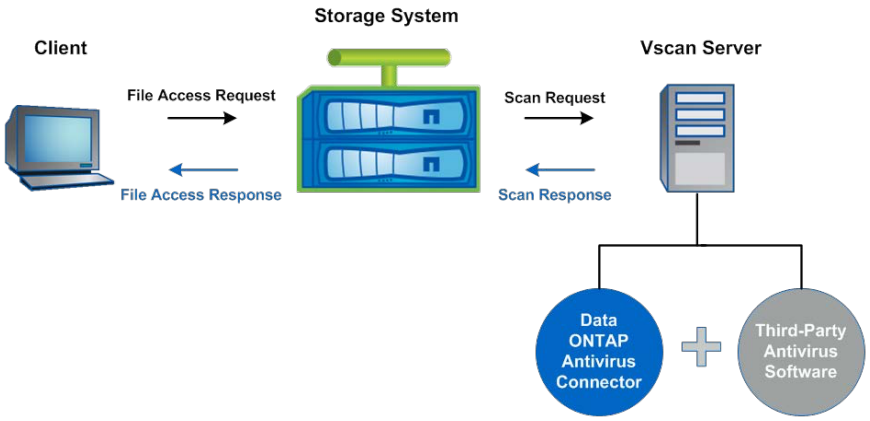
| Term | Definition |
|---|---|
| | |

# 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 NetApp AV Base Cluster Configuration

## 3.1 Overview

The base cDOT cluster is configured for AV as follows.

## 3.2 Configuration

### 3.2.1 Scanner Pools

This step can be carried out at any point during the build. It can be done during the intial build or when a vserver with CIFS is added.

#### 3.2.1.1 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
```

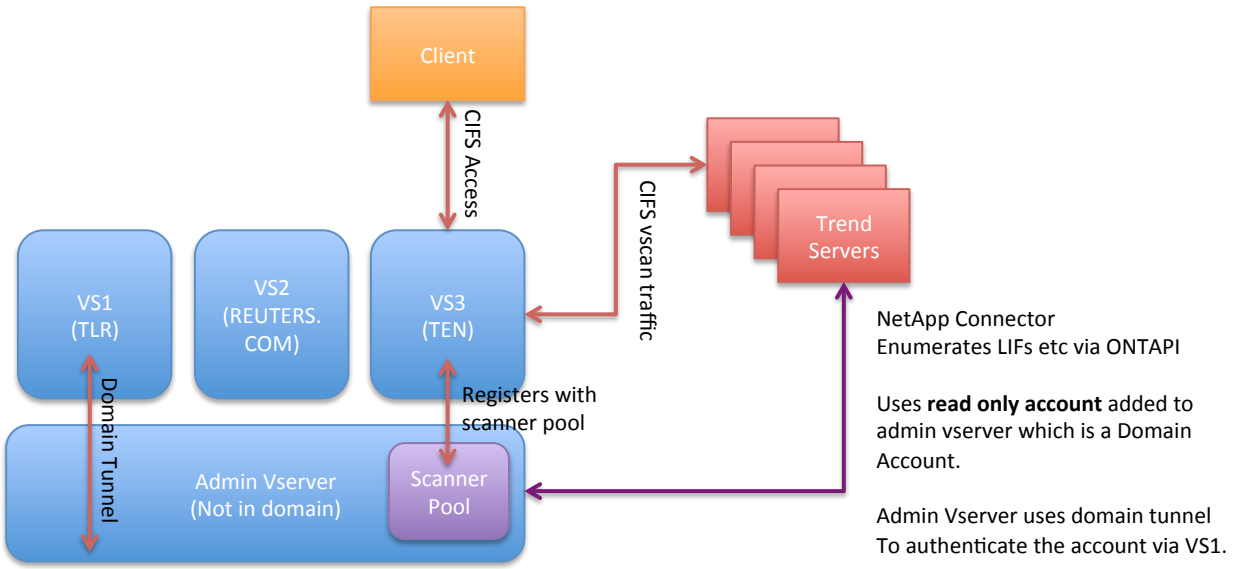
**Example**

```
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 NetApp AV Connector Deployment on the Cluster

## 4.1 Overview

The AV connector is installed onto  a Trend server and uses ONTAPI to communicate with the cDOT systems. We use the same account to facilitate this as we use for the privilidged account on the vscan configuration. This requires a domain tunnel for cDOT version below 8.3.x.



## 4.2 Configuration

The Trend Connector is configured n the server and so is outside of the scope of Storage Delivery deployments. The account and domain tunnel used to authenticate the account are required to be configured. Given the need for a domain tunnel you can only create the tunnel when you have a data vserver joined to the domain. The vserver needs to be in a domain to which the AV server and its accounts are also members.

### 4.2.1 Read Only Role Addition

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

  (security login role create)
```

### 4.2.2 Account Addition

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

  (security login create)
```

### 4.2.3 Domain Tunnel Addition

Requires a vserver in the domain that can be used

```
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
```

## 4.3 Trusted Domains

In the event you have a vserver used for the domain tunnel that has trusts with other domains and your read only account is in one of those domains authentication will work via that domain tunnel.

### 4.3.1 Displaying Trusts

With a domain tunnel in place you can display the trusts as follows.

```
eag-nasor-clus1-8040::vserver cifs domain trusts> show

   Node: eag-nasor-clus1-8040ht-01
Vserver: silab-avcdot-01

Home Domain                    Trusted Domains
------------------------------ ----------------------------------------------
--
TLR.THOMSON.COM                TEN.THOMSONREUTERS.COM, TAXPARTNERS.COM,
                               TFCORP.TFN.COM, EU.COMPUMARK.COM,
                               HUBBARDONE.NET, AMERS.IME.REUTERS.COM,
                               APAC.IME.REUTERS.COM, INT.CARSWELL.CA,
                               ELITECORP.COM, KARNOVGROUP.COM, PPCTX.COM,
                               ERF.THOMSON.COM, ERFQC.THOMSONQC.COM,
                               MASTERDATACENTER.COM, EMEA.IME.REUTERS.COM,
                               NA.THOMSONCORPORATE.COM, GLOBAL.INTERNAL.COM,
                               TLRROOT.THOMSON.COM, TLRQA.THOMSON.COM, TISA,
                               COMPLINET.LOCAL, CORP.OSITAX.COM,
                               TLR.THOMSON.COM
```

### 4.3.2 Show Domain Tunnel Details

The following command shows the details of the domain tunnel in place.

```
eag-nasor-clus1-8040::> domain-tunnel show (security login domain-tunnel
show)

Tunnel Vserver: silab-avcdot-01
```

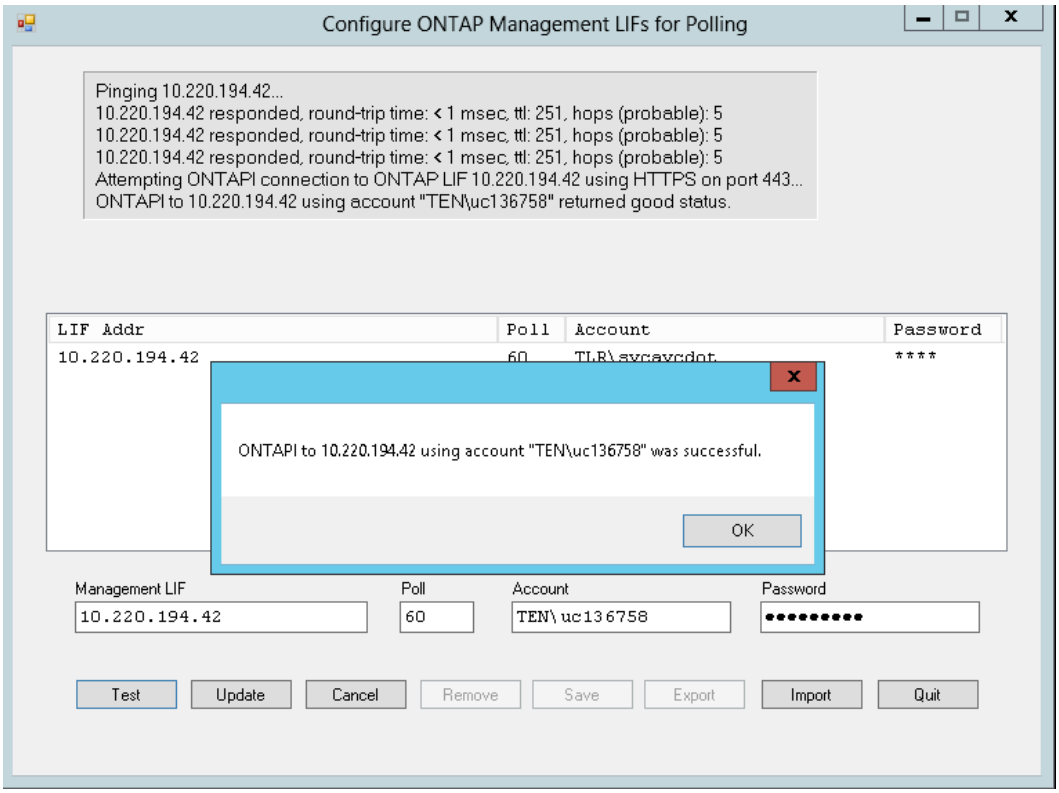
### 4.3.3 Account Addition

The following command adds a TEN domain account to the admin vserver for testing using the read only role previously created. The domain tunnel is left as is pointing to the same vserver as before.

```
eag-nasor-clus1-8040::> sec login create -username TEN\uc136758 -application
ontapi -authmethod domain -role vscanro -vserver eag-nasor-clus1-8040
```

### 4.3.4 Account Test

The following image shows a test of the AV connector to the cluster using the TEN account instead of the previously configured TLR account.




As you can see authentication is successful and the connector will work using an account via a trusted domain provided the domain tunnel is using a vserver that is joined to a domain with the relevant trusts in place.

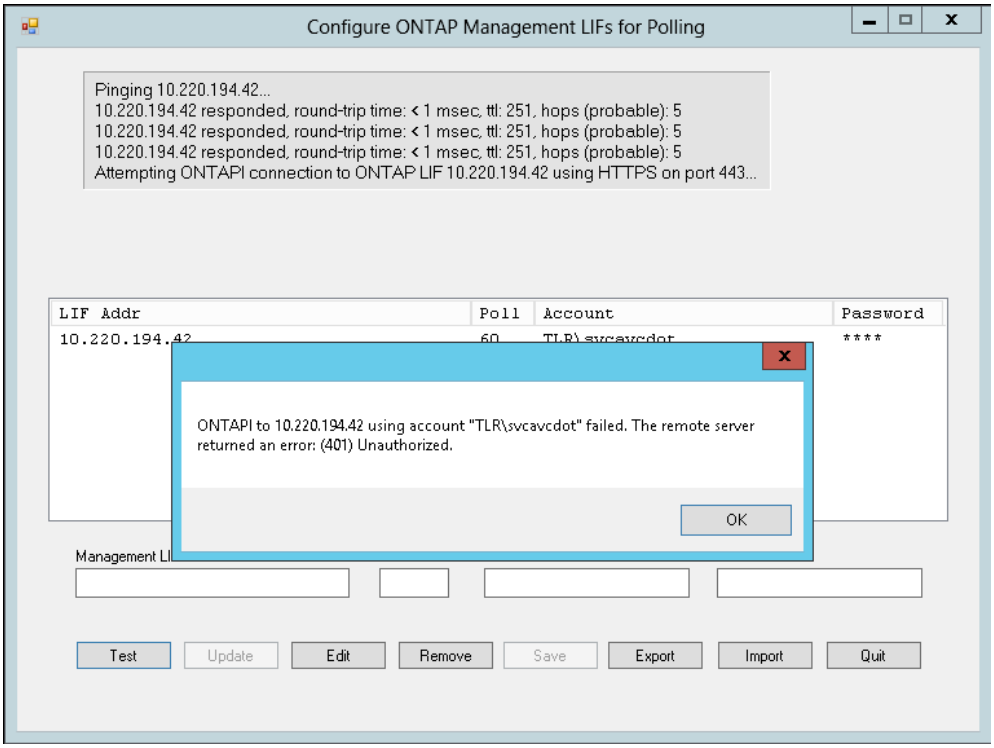
Note: It may be worth creating a vserver to use with a domain tunnel that is joined to a domain with the required trusts in place  at build time.

### 4.3.5 Account Behaviour With No Domain Tunnel In Place

If you remove the domain tunnel as shown the account will fail to authenticate.

```
eag-nasor-clus1-8040::> domain-tunnel delete
  (security login domain-tunnel delete)

eag-nasor-clus1-8040::> domain-tunnel show
  (security login domain-tunnel show)
This table is currently empty.
```




Simply adding the domain tunnel back in will fix this.

# 5 NetApp AV Vserver Configuration

## 5.1 Overview

These steps are carried out once a vserver using CIFS is added to the cluster.

## 5.2 Configuration

### 5.2.1 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)
```

### 5.2.2 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)
```

### 5.2.3 Enable Vserver Virus Scanning

Use the following command to enable AV on a vserver

```
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 if required.

# 6 Automation

## 6.1 Overview

The following is a suggestion on how automation might work.

### 6.1.1 Initial Steps

These steps might be called separately as they would generally be done once.

#### 6.1.1.1 Create a Scanner Pool On the Cluster

```
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)
```

#### 6.1.1.2 Read Only Role Addition

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

#### 6.1.1.3 Account Addition

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

#### 6.1.1.4 Domain Tunnel Addition (Requires a vserver in the domain that can be used)

```
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
```

Note: It may be worth creating a vserver to use with a domain tunnel that is joined to a domain with the required trusts in place at build time. That would then mean all vscan functionality is in place ready to go and it may make automation simpler.

### 6.1.2 CIFS Vserver Steps

These steps would be called on each addition as they would generally be done per vserver.

#### 6.1.2.1 Apply the scanner pool to the vserver

```
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)
```

#### 6.1.2.2 Enable Scanning

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

#### 6.1.2.3 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-l0001
                 off
reserve-n02-l0001
                 off
reserve-n03-l0001
                 off
reserve-n04-l0001
                 off

Vserver          Vscan Status
---------------  ------------
silab-avcdot-01
                 on
silab-e0002      off
silab-e0003      off
15 entries were displayed.
```