Configuration and Deployment

Dell EMC ECS: Using Veritas Enterprise Vault

Abstract

This document explains how to use Dell EMC™ ECS™ object storage as Primary Storage for Veritas™ Enterprise Vault™.

April 2020

H15309

Revisions

Date	Description
October 2018	Release 8
December 2018	Release 9
January 2019	Release 10
April 2019	Release 11
January 2020	Release 12
April 2020	Release 13

Acknowledgements

Author: Paul McKeown

Table of contents

Executive summary

To support Dell EMC™ ECS™ object storage with Veritas™ Enterprise Vault™, the Dell EMC ECS Streamer driver is used to translate the Veritas Streamer API to the ECS S3 API. This allows content to be archived from Enterprise Vault servers to ECS, as well as queried, restored, and deleted. The ECS Streamer driver leverages the ECS S3 API extensions for retention support and for replication status checking required by Enterprise Vault.

This document discusses how to configure Enterprise Vault to use ECS as an archive target.

Audience

This document is intended for storage administrators and Dell EMC professional services personnel who wish to learn how to deploy and configure Dell EMC ECS object storage with Veritas Enterprise Vault.

Terminology

EV: Veritas Enterprise Vault

S3: Simple Storage Service (API)

LB: IP Network Load Balancer

VDC: ECS Virtual Data Center

Bucket: Logical unit of storage on an ECS system in which objects (including their metadata) are stored

1 Solution overview

This section provides an overview of the integration of ECS with Veritas Enterprise Vault and the key technologies used.

1.1 ECS Streamer overview

Veritas has developed a Storage Streamer API for Enterprise Vault (EV) which archive storage vendors must integrate with to allow Enterprise Vault to archive files, email, and other items to their storage systems. Dell EMC has developed the ECS Storage Streamer driver to allow Veritas Enterprise Vault to archive to ECS. The ECS Streamer driver translates the Streamer API calls to the ECS S3 API.

Customers can now create Vault Store partitions of type Dell EMC ECS within the Veritas Enterprise Vault VAC. These Vault Store partitions are associated with S3 buckets on the ECS cluster where savesets archived to the Vault Store will reside.

ECS buckets reside within ECS namespaces that may be compliant or non-compliant. Both compliant and non-compliant namespaces allow retention to be propagated from Enterprise Vault to the ECS cluster, however compliant namespaces store archive data in tamper-resistant storage which meets strict SEC 17a-4(f) rules for electronic record-keeping.

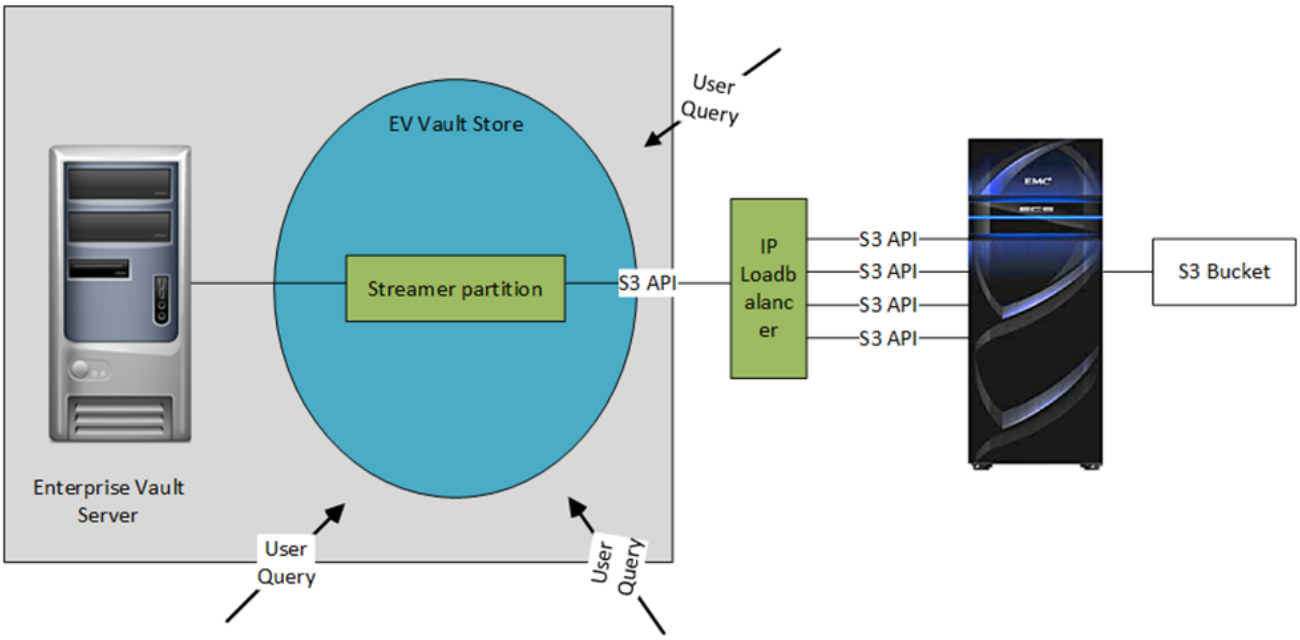

Figure 1 Example of an ECS-based storage solution for Veritas Enterprise Vault

The Veritas Enterprise Vault system has archive policies that archive files to a Vault Store in which an ECS based partition has been defined. The ECS Streamer driver uses the ECS S3 API to store/access objects in the S3 bucket on the ECS cluster.

ECS systems are clusters of 4 or more individual ECS nodes. Customers can use the ECS Streamer built in load balancer (from revision 2.0) to distribute I/O across all nodes in the ECS cluster or deploy an IP Load Balancer to distribute I/O.

1.2 ECS: multi-protocol, API-accessible storage

ECS is a massively scalable, software-defined object storage platform that enables any organization to store, access and manipulate unstructured data as objects. ECS provides support for industry standard APIs such as Amazon S3. In addition, ECS extends the Amazon S3 API with support for retention, byte range updates and atomic appends.

1.2.1 Simple multi-tenancy

ECS delivers a flat software architecture ideal for multi-tenant environments. Configuring, provisioning, creating a namespace and managing a multitenant platform has never been easier. Key metrics and reporting are provided for capacity, object count, objects created, objects deleted and inbound/outbound bandwidth. These activities are all visible via the ECS GUI and through the REST API.

1.2.2 Multi-site, active-active architecture and access

ECS features a truly geo-efficient architecture that stores, distributes and protects data both locally and geographically. This eliminates any single point of failure and provides seamless failover from site to site with no impact to the business. ECS automatically maximizes throughout, maintains high availability and data durability, and increases capacity and the reliability of applications. In terms of geographic limitations – there are none – providing users with a single global namespace with anywhere access to content

Today's modern applications demand a different architecture. Managing both cost and accessibility as storage environments grow and become more complex is one of the biggest challenge's organizations face today. Developers are finding it easier to go to public cloud alternatives putting data at risk and increasing management costs. ECS provides a cloud-scale storage architecture that is specifically designed to support modern applications with unparalleled availability, protection, simplicity and scale.

2 ECS configuration details

How the ECS is configured (for example, the number of ECS nodes, number of VDCs, GEO protection, and application location access) is decided by the solution architect designing the ECS configuration, and for the most part, Veritas Enterprise Vault is unaware of the design. However, the solution architect should consider the compliance requirements of the customer's Enterprise Vault solution.

2.1 Namespace compliance

If the customer wishes to have an SEC-compliant solution, the namespace that the buckets (that all Enterprise Vault partitions will use) should be configured as compliant.

When creating the namespace in the ECS Management GUI, ensure the Compliance option is selected.

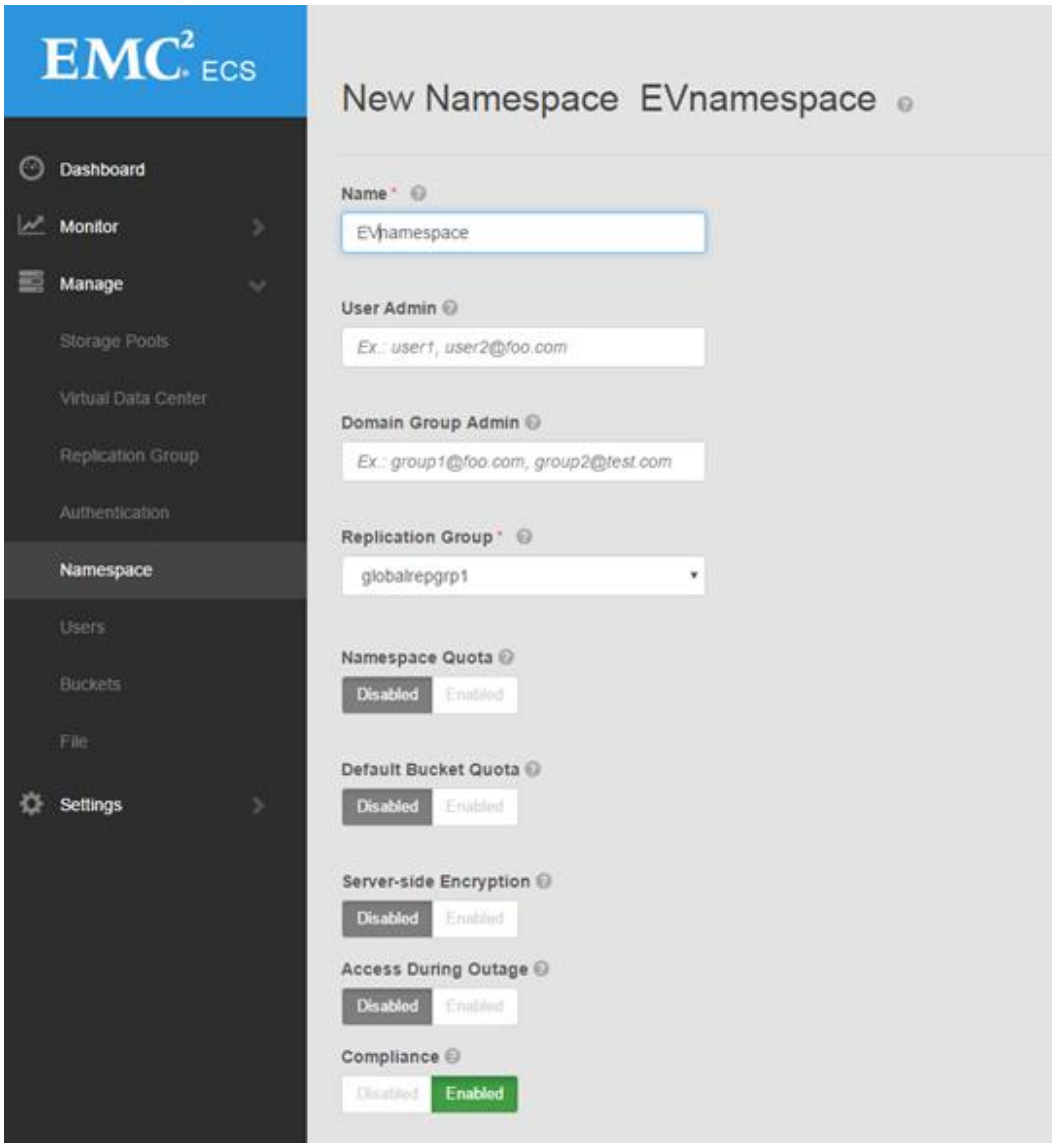

Figure 2 Namespace creation

When using ECS buckets in a compliant ECS namespace to meet SEC 17-A4 requirements, be aware of the following potential issues when choosing between WORM and NON-WORM partition types

NON-WORM mode EV partitions

If you are setting an ECS Streamer partition to NON-WORM mode, EV will write objects with no retention period even if you are setting a retention period in the EV Retention Category. If you are using NON-WORM partitions, it is likely that you should not be using a compliant ECS namespace.

WORM mode

If you are using a compliant namespace, you must give a minimum of a one-second retention to the bucket retention value. This means you must set the following option after the Host IP address when creating the ECS Streamer Partition:

```
DISABLE_WRITE_TEST
```

If you do not set this option, the ECS Streamer will fail connectivity checking because it will create an object and then delete it as part of its checks. This create/delete will occur within one second and will fail and cause the connectivity check fail.

Revision 2.0.1 of the ECS Streamer driver will check if there is a retention period set on the bucket and if so, it will not perform the write test.

Later revisions of the ECS Streamer driver reintroduced write check when there is bucket level retention but now retry to ensure the operation is performed over a 1 second timeframe.

ECS Bucket default retention setting

Create the bucket for the EV Vault Store in the compliant Namespace.

Ensure that the Bucket Retention is set to a value that does not conflict with any Enterprise Vault Retention Category, ideally just 1 second. This must be set, or an error will occur when you attempt to create the bucket.

Administrators should take care when setting the ECS bucket-level retention. Enterprise Vault will expect to be able to delete expired content and although EV will cleanly handle deletion errors on content that is still under ECS retention, it will post and error in the Microsoft® Windows® Event log.

If a customer is using a NON-WORM EV partition it is recommended that ECS bucket level retention is not applied as EV will expect all the savesets written to the partition to have no retention.

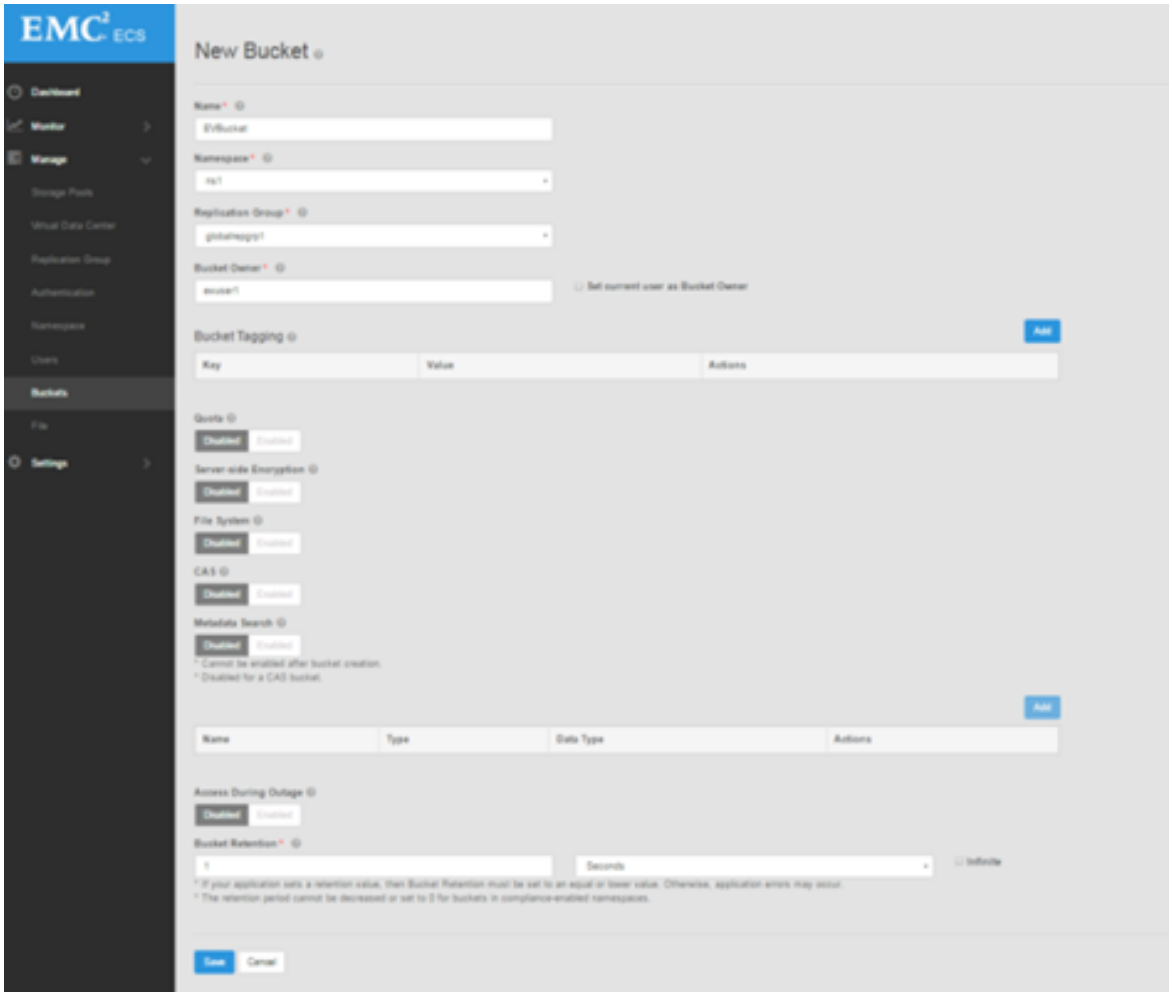

Figure 3 Bucket creation

Consideration should be given to the interaction between Enterprise Vault and bucket-level retention if more than one second is used for Enterprise Vault Partitions.

3 ECS Streamer installation

3.1 ECS Streamer driver install (simple)

You can use the following procedure to download the ECS Streamer driver and quickly perform a default installation of the driver on a Windows server

Go to www.dell.com/support to locate the ECS Streamer driver installer. Once you have download the ECS Streamer driver onto the Enterprise Vault server, double click the installation file and installation will start

Unless they have already been installed on this server you will be prompted to allow the installer to install the VC++ Redistributed file

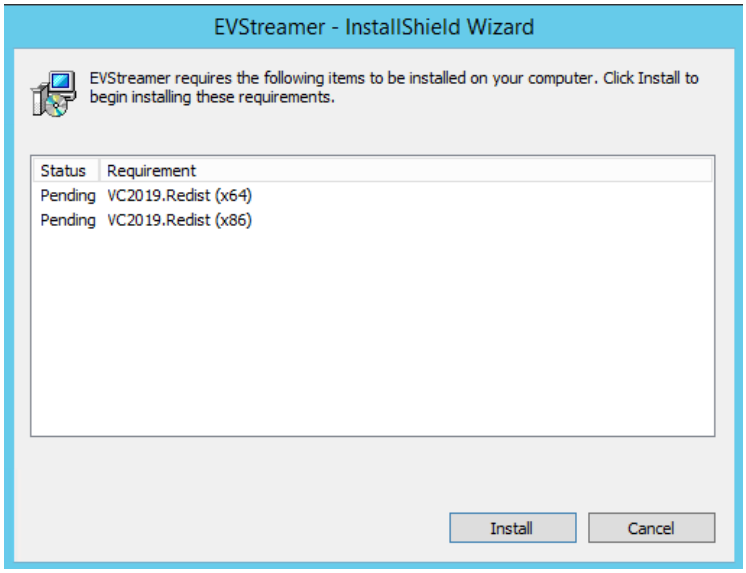

Figure 4 ECS Streamer driver install - 1

Click **Install** to install the Visual C++ redistributed packages. You will be asked to reboot the server

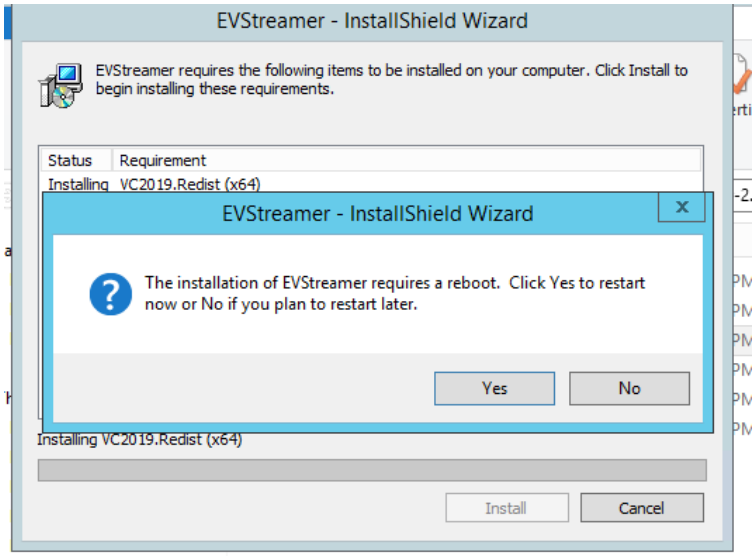

Figure 5 ECS Streamer driver install - Reboot

Click **Yes** to reboot the server.

When you log in after the restart you may be asked to install the VC++ 32bit version of the distribution, follow the instructions are reboot.

When you log in after the reboot the installer will automatically continue the installation

Click **Next** to install the ECS Streamer driver and click through the remaining screens to finish the installation.

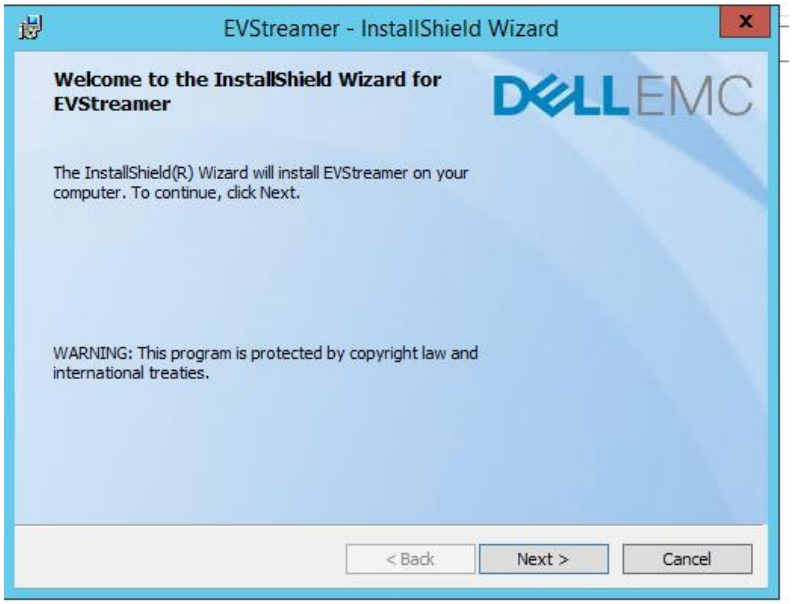

Figure 6 ECS Streamer installation

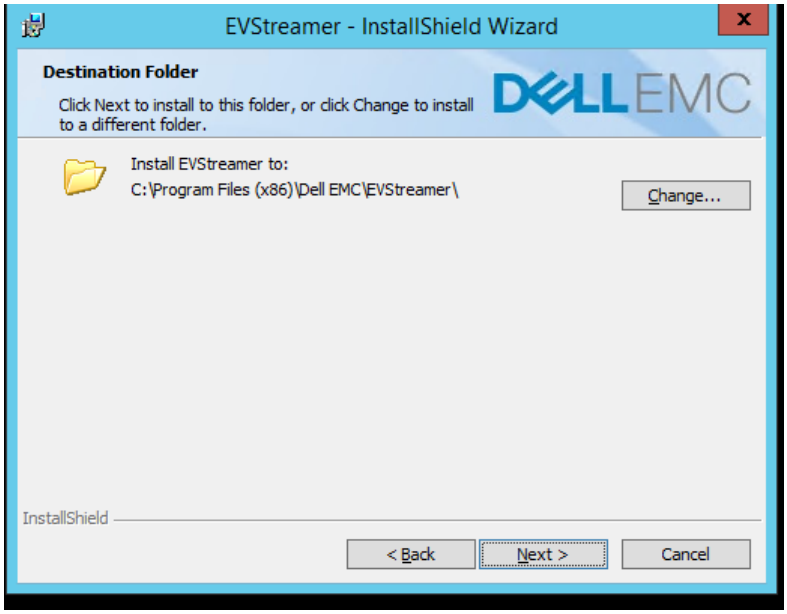

Figure 7 ECS Streamer installation – change installation folder

You can change the installation folder for the ECS Streamer driver at this screen if you wish, otherwise click through the remaining prompts.

The ECS Streamer driver should be installed on all Enterprise Vault servers.

Please refer to the ECS Streamer release notice for further details on installing the driver.

3.2 ECS Streamer driver install (manual)

Download the ECS Streamer driver as per the above section.

Admins can run the ECS Streamer installation from a CLI (DOS) shell and specify

- The log file pathname
- Set the installation directory by specifying a path for the INSTALLDIR property

For example:

➢ `ECSStreamer.2.0.5.7.exe /V"/log c:\setuplogs\install.log INSTALLDIR=f:\EVStreamer"`

Please refer to the ECS Streamer release notice for further details on installing the driver

3.3 ECS Streamer driver remote installation

A utility is now part of the distribution that aids in scripting remote installations.

EVRemoteInstall.exe is a stand-alone executable that can be used in a script. It takes as parameters the ECS Streamer setup file, along with a remote computer target. It also has extensive logging options.

This utility can be run in one of two ways:

- Install ECS Streamer on a remote system. This utility can be used in a script to install on any number of systems. Use the /r parameter to specify the remote server.

- Specify a file containing a list of remote systems and install/uninstall/get status on all the servers in the list. Use the /rf parameter to specify the list of remote servers.

Command line usage:

```
C:\>EVRemoteInstall.exe /?
Invalid Parameter: /?
Product: EVStreamer
Usage:
   EVRemoteInstall.exe <options> [<properties>]
   <options>:
      /i <path to setup file> - Install (UNC path or local path)
      /x                      - Uninstall
      /s                      - Check Install Status
      [/u <domain\user>]      - Connect with specified 'domain\user'
      [/a <password>]         - If /u specified, use password to connect
      [/r <remote server>]    - Remote server
      [/rf <file>]            - File contains one server per-line
      [/n <number>]           - Number of parallel installs (default = 4)
      [/p]                    - Display progress
      [/pv]                   - Verbose progress (list actions)
      [/b]                    - Reboot after install/uninstall

   Logging Options
      /l[i|w|e|a|r|u|c|m|o|p|v|x|+|!|*] <LogFile>
            i - Status messages
            w - Nonfatal warnings
            e - All error messages
            a - Start up of actions
            r - Action-specific records
            u - User requests
            c - Initial UI parameters
            m - Out-of-memory or fatal exit information
            o - Out-of-disk-space messages
            p - Terminal properties
            v - Verbose output
            x - Extra debugging information
            + - Append to existing log file
            ! - Flush each line to the log
            * - Log all information, except for v and x options

      /log <LogFile>
            Equivalent of /l* <LogFile>

   <properties> - any number of install properties of the format:

            PROPERTYNAME=<value>



   if /rf is specified, then /r, /p or /pv are ignored.
   if /rf is not specified, then /n is ignored.
```

Sample usage:

This command will install the EV streamer on "`remotecomputer`". It will set the install folder to `f:\EVStreamer` and save the installation log:

```
C:\>EVRemoteInstall.exe /i c:\setupfiles\ECSStreamer.2.0.5.7.exe /r remotecomputer /p
/log c:\setuplogs\ECSStreamer.remotecomputer.log INSTALLDIR=f:\EVStreamer
```

Requirements:

- EVRemoteInstall.exe does not require installation and can be run on any supported version of Windows Server. Windows Server 2008R2, 2012, 2012R2 and 2016.
- Client versions of Windows (7, 8, 8.1 and 10) are not supported, either for the system running EVRemoteInstall.exe, or the system where the streamer is being installed.
- All servers must have file sharing enabled.
    - File sharing is used to copy files to and from the target system, as well as install a remote service and access remote registry.
    - A named pipe connection is created at the local system to the target system.

Additional Information:

You will notice that no progress is displayed for the first stage of the install. This is because the Microsoft Redistributables are being installed during this time. After they are installed, you'll see progress indications for the install.

The /p option should not be used in a script. This option is good for showing progress when using this utility interactively. It will display a row of dots to show progress.

This command will set an exit code of zero if the installation was successful, or non-zero if it was not successful. You should capture any standard output, plus save a log file (/log option) to be able to analyze why the installation failed.

When specifying /rf <file> and a log file (/l) parameter, it will create one log file for the overall operation, plus one log file for each server in the file list. The server name is added to the log file name specified.

If the remote server is in a different domain, then you must specify credentials: "`/u <domain\user>`" and "`/a <password>`" on the command line.

When specifying `/rf <file>`, the file should contain a list of servers, one per line. The syntax of each line is:

```
[#]<server name/IP>[;<domain/user>;<password>]
```

Where:

- If the line starts with '#' the line is ignored
- Blank lines are ignored
- If ";<domain/user>;<password>" is included, those values override the same parameters specified on the command line, if any. This is useful if servers in the list are in different domains.

Please refer to the ECS Streamer release notice for further details on installing the driver

4 ECS Streamer configuration

4.1 Add ECS as a storage option in Enterprise Vault

Refer to the following procedure on the Veritas support web site:
https://www.veritas.com/support/en_US/article.000114337

This procedure is only required to be performed on one Enterprise Vault server instance (the primary EV server typically).

Note: With Enterprise Vault revision 12.3 and later, the ECS Streamer driver configuration files (not the ECS Streamer Driver itself) are already included in the EV distribution and this task does not need to be performed.

Always check with the Veritas document linked above in case Veritas have made any changes to this procedure.

4.2 Configuring an ECS Streamer-based Enterprise Vault Store partition

In the VAC, expand the Enterprise Vault Site and Vault Store Groups and right-click the Vault Store you wish to create a new Vault Store Partition for. Click **New** > **Partition** and click **Next**.

Choose an appropriate Name and Description and click **Next**.

Choose Dell EMC ECS from the Storage Type drop-down menu. Click **Next**.

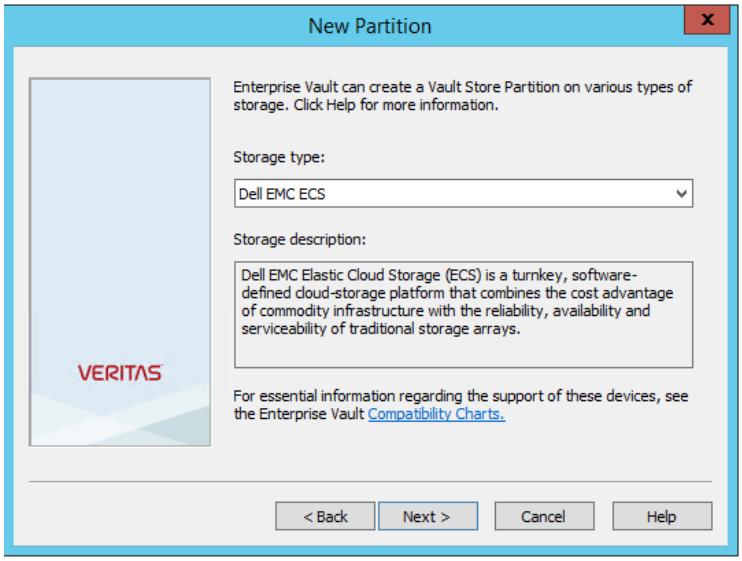

Figure 8 New Partition menu

Enter the connectivity details for the ECS cluster to be connected to and select **Test** to check the configuration details.

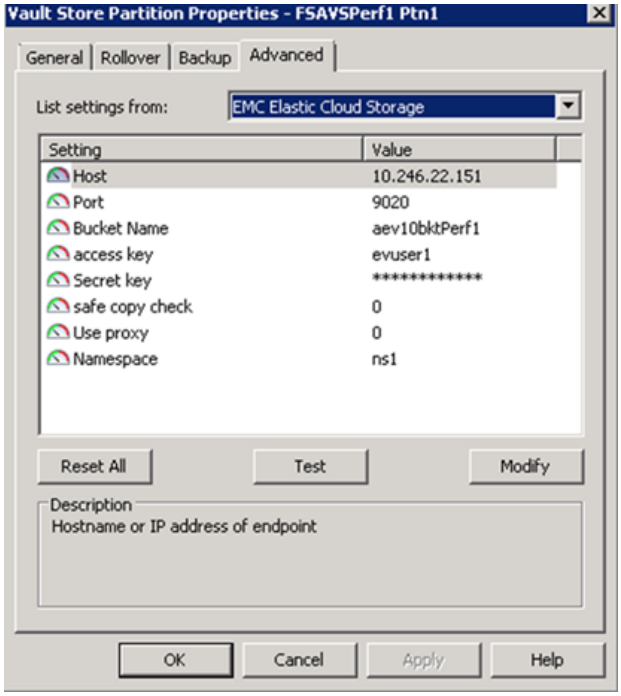

Figure 9 Partition definition

Table 1 Partition properties

Property	Description
HOST	Enter the IP address or FDQN of the LB service or ECS nodes. See section 4.2.1.
Port	Default 9020. Enter the port number being used for data connection to the ECS (or Load Balancer).
Bucket Name	Enter the name of the ECS bucket to be used. ECS buckets used by Enterprise Vault should not be file system enabled.
Access Key	Enter the ECS access key (object user) to be used.
Secret Key	Enter the Access key secret key.
Safe Copy Check	0, 1 or 2. See section 5.4.
Use proxy	Set to 0 if no proxy is being used or to the port the proxy is using.

Click the **Test** button to perform a check of the configuration settings. If you get an error, recheck the settings as entered. Also check what errors are being logged in the Windows Event Log.

Pre ECS 3.4 - the namespace property is only used in the dtquery request (used when safe copy check is 2, see the section below). The namespace property is irrelevant to the actual archiving process and it is not used in S3 object requests. The object user is globally unique and belongs to a namespace, therefore the namespace is implicitly identified.

ECS 3.4 – the ECS Streamer Driver can be configured to use an EMC ECS extension to the S3 API to discover the replication status of a saveset and this uses the same network port as normal S3 data access.

If the Test is successful, click **Next**.

In the next GUI form, select the appropriate WORM setting for the partition. The ECS Streamer driver has been validated for NON-WORM and well as WORM Enterprise Vault partitions, check or un-check this radio button appropriately.

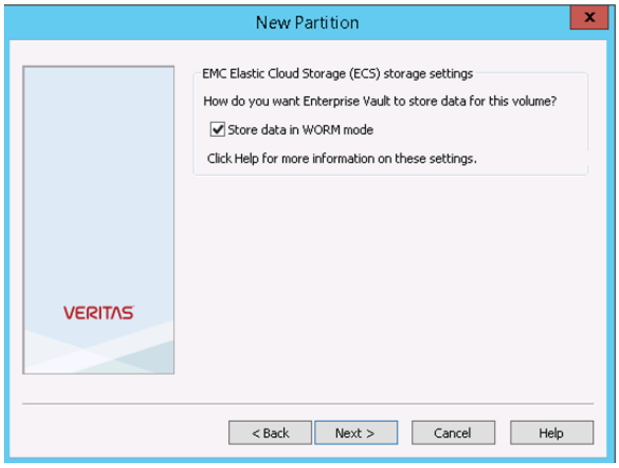

Figure 10 WORM or NON-WORM setting

Complete the forms that follow as required.

4.2.1 Host property

With revision 2.0.1.1, it is possible to specify a comma-separated list of ECS Node IP or FQDN addresses as the Host value in the Partition Configuration GUI. See the following examples:

```
U300-01.lab.emc.com,U300-02.lab.emc.com,U300-03.lab.emc.com,U300-04.lab.emc.com
```

```
10.0.0.1,10.0.0.2,10.0.0.3,10.0.0.4
```

You may also specify an IP address range, for example:

```
10.0.0.1-10.0.0.8
```

When specifying the host addresses or range, use of the ECS Streamer driver internal IP Load Balancer is enabled.

The ECS Streamer driver will not attempt to auto-discover any other ECS Node IPs when a list or range is specified.

If you do use the **;LB=true** option, the ECS streamer driver will auto-discover all Node IPs and ignore your list or range.

With version 1.0.10 of the Dell ECS Streamer driver, some additions were made to the syntax of the Host property to allow the administrator to set some internal settings of the Dell ECS Streamer driver. The options are as follows:

- MAX_TRIES
- DISABLE_WRITE_TEST
- MAX_CONNS
- DTHOST

- RDT
- SHOWCHUNKS
- LB=true
- DONT_TEST_STOPPING
- IGNORE_BAD_COMMON_NAME
- S3V4

To use the options, the Host IP (or name) must come first and the other options can be specified using a semicolon separator in <name>=<value> format, for example:

```
10.1.83.51;MAX_TRIES=2;MAX_CONNS=25;DISABLE_WRITE_TEST=1
```

With revision 2.0.2.1 of the ECS streamer driver, you may just specify the value to have it set to 1 (or true). The following example is the same as the prior example:

```
10.1.83.51;MAX_TRIES=2;MAX_CONNS=25;DISABLE_WRITE_TEST
```

4.2.1.1 MAX_TRIES

When any server failure response is received, the Streamer will attempt a total of 5 tries by default before returned bad status to Evault. There is a standard exponential back-off algorithm between retries. This value can be overridden by the MAX_TRIES option which must be greater than 0 and less than 5.

4.2.1.2 MAX_CONNS

This controls the maximum number of simultaneous safe copy checks that can occur at one time. The default is 65 as of revision 1.0.14 of the Streamer driver. Customers should not need to change this number but it may be set between 2 and 100.

Note: As of revision 2.0 of the Streamer driver, this setting is ignored if used.

4.2.1.3 DISABLE_WRITE_TEST

When creating a Vault Store Partition for the first time when there is a Temporary Site Outage (TSO), the tests performed when the user clicks on the Test button will fail because of the TSO. We recommend that you do not create Vault Store Partitions while a TSO is in effect, but if needed, set DISABLE_WRITE_TEST=1 to disable the test. With revision 2.0.2.1 of the Streamer driver, you need only specify DISABLE_WRITE_TEST to set the flag to 1.

Additionally, if you are using a compliance namespace, you should disable the write test. When the ECS Streamer checks connectivity, it writes a test object and deletes it to check connectivity. This will occur in less than one second which would cause even a one-second bucket-retention setting on a bucket to fail the deletion. The ECS Streamer would then report an error to Enterprise Vault.

With revision 2.0.1, the ECS Streamer driver will check if there is a retention period set on the bucket and if so it will not perform the write test.

4.2.1.4 DTHOST=<hostname> or <IP>

This allows the user to specify the endpoint for the DTQUERY geo replication checking to a different host than the one specified for the Vault Store partition. This should only be changed under the instruction of Dell EMC support personnel.

RDT=1

This will set **&random=<someUniqueGuid>** to the end of the DTQUERY URL to make sure the URL response is never cached. The <someUniqueGuid> is never reused to ensure the request URL is unique. Although additional flags are now used in the request constructor to prevent caching, but this variation is still available for use. This is added to revision 1.0.14 of the Streamer driver.

4.2.1.5 SHOWCHUNKS=1

This will include the chunkIDs and chunk ranges for files written in the DTRACE log, only if the files were archived to the bucket-owning site. Do not enable this unless told to by Dell EMC support personnel. If enabled, there will be an effect on performance. This is added to revision 1.0.14 of the Streamer driver.

4.2.1.6 LB=true

With revision 2.0.0, the ECS Streamer driver has a built-in load balancer which obviates the need to use an IP load balancer with the ECS Streamer driver to ensure that all nodes in an ECS VDC are used. To use the built-in LB, specify **;LB=true** after the IP Address prompt (and any other parameter being used).

10.1.83.51;LB=true

The IP address must be of an ECS node in the VDC, and the ECS Streamer will auto-discover the IP addresses of all the ECS nodes in the VDC. The IP address must **not** be an IP load balancer. Any firewall between the EV server and the ECS must open ports 9020/9021 and 9101 for HTTP, HTTPS and HTTP traffic, respectively.

If you are using IP addresses and SSL certificates with your ECS or IP load balancer, ensure that the ECS node IP addresses are include in the certificates SANs.

An example of a SAN in a certificate is as follows

```
IP Address=10.1.83.51
IP Address=10.1.83.52
IP Address=10.1.83.53
IP Address=10.1.83.54
DNS Name=*.company.com
DNS Name=*.*.company.com
```

On Windows 10 or Windows Server® 2016, using IP addresses for an SSL connection is acceptable.

If the system is Windows Server 2012 R2 or earlier, it will fail because it does not recognize that the IP address is in the certificate.

This means that for Windows Server 2016, it is possible to use the LB option:

```
Host property: 10.1.83.51;LB
```

For earlier versions of Windows, you will need to use the fully qualified DNS name, such as:

```
Host property:
ecsnd1.company.com,ecsnd2.company.com,ecsnd3.company.com,ecsnd4.company.com
```

With revision 2.0.2.1 of the ECS Streamer driver, you need only specify **;LB** to enable IP load balancing.

4.2.1.7 DONT_TEST_STOPPING

This will disable the streamer INIT check which tests if the EV Storage Service is up. Only set this is instructed by Dell EMC support.

4.2.1.8 IGNORE_BAD_COMMON_NAME

Normally when establishing an HTTPS connection, the connection will fail if the host name provided does not match the name in the certificate, for example, when using an IP address.

With Streamer revision 2.0.2.1, if you are using an older version of Windows Server, you can use the "IGNORE_BAD_COMMON_NAME" option in the host parameter to allow the connection to succeed.

```
10.1.83.51;LB;IGNORE_BAD_COMMON_NAME
```

4.2.1.9 Support for S3 V4 Authentication

V4 authentication can be enabled by adding "S3V4" to the host field

For example:

```
10.1.83.51;LB;S3V4
```

Will make the ECS Streamer driver use S3 V4 authentication

5 ECS Streamer driver details

5.1 Network ports

The following network ports are used to communicate between the Enterprise Vault Server and ECS.

Table 2 Network ports

Port number	Port detail
9101	Required to perform the Enterprise Vault “safe copy” check. TCP to the ECS. From ECS revision 3.4 this port does not have to be used if the safe copy option is set to 1 (see section 5.4)
9020 or 9021	Non-SSL or SSL data connection port

If the customer uses an IP Load Balancer they may choose to use different HTTP or HTTPS ports from the Enterprise Vault server to the IP Load Balancer. Ports used should be configured in any IP Load Balancer for TCP to the ECS nodes.

At the present, port 9101 cannot be mapped to another port by any Load Balancer being used. From ECS revision 3.4 this port is no required to does not need to be remapped by an IP Load Balancer

5.2 Retention

Enterprise Vault allows users to associate EV retention policies to archived objects, files, email, or other data. The ECS Streamer driver provides Enterprise Vault with the capability of associating these EV retention policies with the objects stored on the ECS. The ECS object store will enforce the objects retention and will not allow objects to be deleted until its retention has expired.

Objects archived to ECS cannot have their retention shortened or extended by Enterprise Vault.

Enterprise Vault will not any apply retention periods to objects stored in a Dell ECS Streamer Partition that is configured as NON-WORM.

5.2.1 Retention policies

The ECS Streamer driver does not support ECS retention policies.

5.3 WORM and NON-WORM support

Veritas defines WORM and NON-WORM as follows:

WORM: Enterprise Vault will set the retention period defined in an Enterprise Vault Retention Category to the objects written to an ECS Streamer Partition.

NON-WORM: Enterprise Vault will not set the retention period defined in an Enterprise Vault Retention Category to the objects written to an ECS Streamer Partition.

When a NON-WORM partition is created, this allows the following:

- Even if a Vault Store is using a Retention Category that has a retention period, users using the Enterprise Vault Search Browser can select a document(s) for deletion and as there is no-retention on the object(s) on the ECS, the ECS will allow the deletion to succeed. Administrators, for example, use this to set documents to be Retained Forever in Enterprise Vault so that the Enterprise Vault Expiration Task will not be run on the Partition but still allow users to delete individual documents.
- Enterprise Vault Administrators can change the retention period of a Retention Category and can shorten it. Subsequent runs of the Enterprise Vault Expiration Task will act on the newly shortened retention period and will attempt to delete the content which will succeed as there is no retention on the object on the ECS.

ECS 3.x is supported as a WORM or NON-WORM enabled Enterprise Vault archive device for EV11 and EV12. When any Veritas Vault Store Partition is created and uses the ECS Streamer driver, check the box shown in Figure 11 to enable WORM storage, or uncheck the box to use NON-WORM.

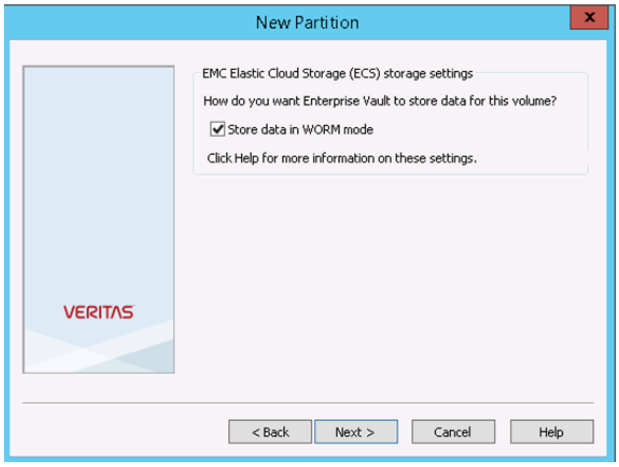

Figure 11 WORM or NON-WORM setting

This setting cannot be changed once the Partition has been created.

5.4 Safe Copy Check

Enterprise Vault has a **Safe Copy Check** feature which can be enabled by customers at the Vault Store level. This check is to ensure that content archived by Enterprise Vault is not replaced in its original location by an HTM link until it has been backed up to a second archive device via the device's replication functionality.

This approach is commonly used by customers who use archive devices with replication functionality that have an eventual consistency model. With Dell EMC Centera™, for example, it can be several minutes before replication has created the second copy of the archive content and the Safe Copy Check is commonly used.

ECS implements a strong consistency model and the latencies that exist in the Centera replication queues do not exist in ECS. Customer can be assured that an object that is written to one Virtual Data Centre in a Replication Group will also be available to all other Virtual Data Centers in that Replication Group. However, customer may regard even the smallest of delta-t window as being unacceptable and may wish to perform the safe-copy check.

The concept of a safe copy means that an archived object is geo replicated to a secondary VDC. However, within a VDC, archived files are always stored in a resilient manner (such as Erasure coding and a copy). Please read the ECS storage documentation for more information.

Prior to ECS revision 3.4, customers who wish to perform this check will need to specify option 2 described in Table 3. This will cause the ECS Streamer driver to use dtQuery to perform the check over port 9101.

If safe copy check is set to 2, the dtQuery request to validate a safe archive copy exists (such as Geo replication to a second VDC) will be sent.

The ECS streamer does not control the message in the failure alert window. ECS streamer will attempt to log a reason for the error in the Windows Event Log.

Should a customer wish to use the Enterprise Vault safe copy check, they can enable this as before on the Vault Store and then choose option 2 in the Vault Store Partition configuration GUI. This check uses port 9101 and this must be considered when planning Load Balancers and Firewalls. The port 9101 is fixed and cannot be mapped to another. This is set on the Partition setup management GUI.

The following table shows the three possible values for the Safe Copy Check parameter.

Table 3 Safe Copy Check property pre ECS 3.4

Value	Has the object been replicated
0	Always return TRUE
1	DO NOT USE. Reserved for future use.
2	Uses the ECS dtQuery check to determine replication status and returns TRUE or FALSE appropriately.

With ECS Revision 3.4 the ECS S3 API support has been extended to provide a call which can request the replication status of an object

```
Request:

GET /bucket/key?replicationInfo

Response:

<ObjectReplicationInfo xmlns="http://s3.amazonaws.com/doc/2006-03001/"
<IndexReplicated>false</IndexReplicated>
<ReplicatedDataPercentage>64.0</ReplicatedDataPercentage>
</ObjectReplicationInfo>
```

This call can now be used by customers to check the replication status of savesets. The ECS Streamer Driver when using this ECS S3 API call will not use port 9101, rather it will use the port used for S3 data.

Admins can still choose 1 or 2 for the safe check property

Table 4 Safe Copy Check property ECS 3.4

Value	Has the object been replicated
0	Always return TRUE
1	Will check replication status using ?dtquery and will use port 9101
2	Will check replication status EV Savesets via `GET /bucket/key?replicationInfo`

5.5 Support of large partition listings

When Enterprise Vault has asked for an enumeration of the objects in a partition, the previous 2.x versions of the streamer would collect the entire listing before returning to Enterprise Vault with the first object. This fails if there are a lot of objects to list. This version will gather objects in groups of 1,000. This means that the first object is returned much faster, but it insures that the request will not time out waiting for all the objects to be fetched.

5.6 Handling failed ECS nodes

If the Streamer driver detects that an ECS node has failed or become unavailable, the Streamer will mark the node as bad and will retry the I/O on another node.

The Streamer will retry the unavailable ECS node after 12 minutes with Streamer rev 2.0.3.1, and 2 hours with previous revisions.

5.7 Windows performance monitoring support

With ECS Streamer revision 2.0.5.1, support for Windows performance counters has been added.

There are three new Performance Monitor counter objects:

- Dell EMC EV Streamer: Global counters
- Dell EMC EV Streamer Instance: Only available if the streamer is currently active
- Dell EMC EV Streamer Process: Only available if the streamer is currently active

These counter objects allow the user to see the current activity going on with the streamer.

5.7.1 Global counter object

The global counters show the aggregation of all the streamer instances and connections.

Table 5 Global object counter

Name	Description
Bytes Received (bytes/sec)	The data rate (bytes/sec) received from ECS.
Bytes Sent (bytes/sec)	The data rate (bytes/sec) sent to ECS.
EV Request Rate	Request Rate (operations/second) from EVault. This is the aggregation of all requests coming from EVault.
Init Request Rate	Init Request Rate (operations/second) from EVault
Write Request Rate	Write Request Rate (operations/second) from EVault
Read Request Rate	Read Request Rate (operations/second) from EVault
Update Retention Request Rate	Update Retention Request Rate (operations/second) from EVault
Update Metadata Request Rate	Update Metadata Request Rate (operations/second) from EVault

Info Request Rate	Info Request Rate (operations/second) from EVault
Delete Request Rate	Delete Request Rate (operations/second) from EVault
Capacity Request Rate	Capacity Request Rate (operations/second) from EVault
Enum Start Request Rate	Enum Start Request Rate (operations/second) from EVault
Enum Next Request Rate	Enum Next Request Rate (operations/second) from EVault
Enum End Request Rate	Enum End Request Rate (operations/second) from EVault
Test Request Rate	Test Request Rate (operations/second) from EVault
Streamer Instances	Number of simultaneous Streamer Instances
Max Streamer Instances	Maximum number of simultaneous Streamer Instances
Current Requests	Number of simultaneous requests from EVault
Max Current Requests	Maximum number of simultaneous requests from EVault
Connection Cache Size	Number of connections in Connection Cache
Max Connection Cache Size	Maximum number of connections in Connection Cache
Max Configured Connections	This value reflects the configured number of MAX_CONNS.

5.7.2 Instance counter object

The Instance counters break that down into a list of streamer instances. The instances are named as follows:

<host>,<bucket>,<partition>

It may be possible for there to be more than one instance with the same ID. This can happen, for instance, if one of the other parameters have changed, such as one of the host options. If there is more than one instance with the same name, the subsequent instances will be named as follows:

<host>,<bucket>,<partition> (n)

In this example, **n** is a number. These counters are available in each connection instance:

Table 6 Instance counter object

Name	Description
Bytes Received (bytes/sec)	The data rate (bytes/sec) received from ECS
Bytes Sent (bytes/sec)	The data rate (bytes/sec) sent to ECS
EV Request Rate	Request Rate (operations/second) from EVault. This is the aggregation of all requests coming from EVault.
Write Request Rate	Write Request Rate (operations/second) from EVault
Read Request Rate	Read Request Rate (operations/second) from EVault
Update Retention Request Rate	Update Retention Request Rate (operations/second) from EVault

Update Metadata Request Rate	Update Metadata Request Rate (operations/second) from EVault
Info Request Rate	Info Request Rate (operations/second) from EVault
Delete Request Rate	Delete Request Rate (operations/second) from EVault
Capacity Request Rate	Capacity Request Rate (operations/second) from EVault
Enum Start Request Rate	Enum Start Request Rate (operations/second) from EVault
Enum Next Request Rate	Enum Next Request Rate (operations/second) from EVault
Enum End Request Rate	Enum End Request Rate (operations/second) from EVault
Test Request Rate	Test Request Rate (operations/second) from EVault
State List Size	State List Size. Each Connection can have many states which roughly relate to the number of different threads that are making requests through the streamer. This list is trimmed during garbage collection which occurs periodically.
Max State List Size	Maximum State List Size. Each Connection can have many states which roughly relate to the number of different threads that are making requests through the streamer. This is reset using EVResetPerf.exe.
Configured Enum Threads	This value reflects the configured number of threads that are spawned during an ENUM operation to speed up the gathering of the Metadata on each item.

5.7.3 Process counter object

The Process instance categorizes the instances by process. The Process instance is named as follows:

<processname> (<process id>)

The following counters are available in each process instance:

Table 7 Process counter object

Name	Description
Bytes Received (bytes/sec)	The data rate (bytes/sec) received from ECS.
Bytes Sent (bytes/sec)	The data rate (bytes/sec) sent to ECS.
EV Request Rate	Request Rate (operations/second) from EVault. This is the aggregation of all requests coming from EVault.
Write Request Rate	Write Request Rate (operations/second) from EVault
Read Request Rate	Read Request Rate (operations/second) from EVault
Update Retention Request Rate	Update Retention Request Rate (operations/second) from EVault
Update Metadata Request Rate	Update Metadata Request Rate (operations/second) from EVault
Info Request Rate	Info Request Rate (operations/second) from EVault
Delete Request Rate	Delete Request Rate (operations/second) from EVault
Capacity Request Rate	Capacity Request Rate (operations/second) from EVault
Enum Start Request Rate	Enum Start Request Rate (operations/second) from EVault
Enum Next Request Rate	Enum Next Request Rate (operations/second) from EVault
Enum End Request Rate	Enum End Request Rate (operations/second) from EVault
Test Request Rate	Test Request Rate (operations/second) from EVault

5.7.4 Reset performance monitor maximum counters: EVResetPerf.exe

Some of the counters show the highest values that have occurred since the last time they were reset. These include the following:

- Max Streamer Instances (global)
- Max Current Requests (global)
- Max Connection Cache Size (global)
- Max State List Size (instance)
- Max Streamer Instances (per-process)
- Max Current Requests (per-process)
- Max Connection Cache Size (per-process)

These counters can be reset using the CLI command: EVResetPerf.exe. This command takes no parameters and will reset the above counters to their current values (pre revision 2.0.6.12)

As of rev revision 2.0.6.12, EVRestPerf.exe now supports two parameters: /all and /schedule. If no parameters are supplied the “max” counters above are reset.

Usage; EVResetPerf [/all] [/schedule]

Parameter /all:

All counters are reset to zero. This removes all instances and process entries. The should be used onlu if there are no EVStreamer processes running. To reset all counters without worrying about running processes, use the /schedule option.

Parameter: /schedule

All counters will be rest to zero and all instances will be deleted at the next reboot.

5.7.5 Log-level registry value to troubleshoot performance monitor support

If Performance Monitor support is not working, the first thing to do is look in Event Viewer. Look for the following in the application log:

```
Source = DellEMCEVStreamer
```

The logging level can be changed by setting this registry value as follows:

```
Key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DellEMCEVStreamer\Parameter
s

Value: DWORD EventLogLevel
```

The registry can take the following values:

Value	Description
0	No event log messages ever.
1	Normal event logging. Errors only.
2	Minimum Debug logging.
3	Maximum Debug Logging.

6 Troubleshooting

6.1 Windows event log

Whenever you get an error or suspect an error is occurring, you should use the Windows Event Viewer to check the Windows Event Log for errors in the **Applications and Services Log section > Veritas Enterprise Vault.**

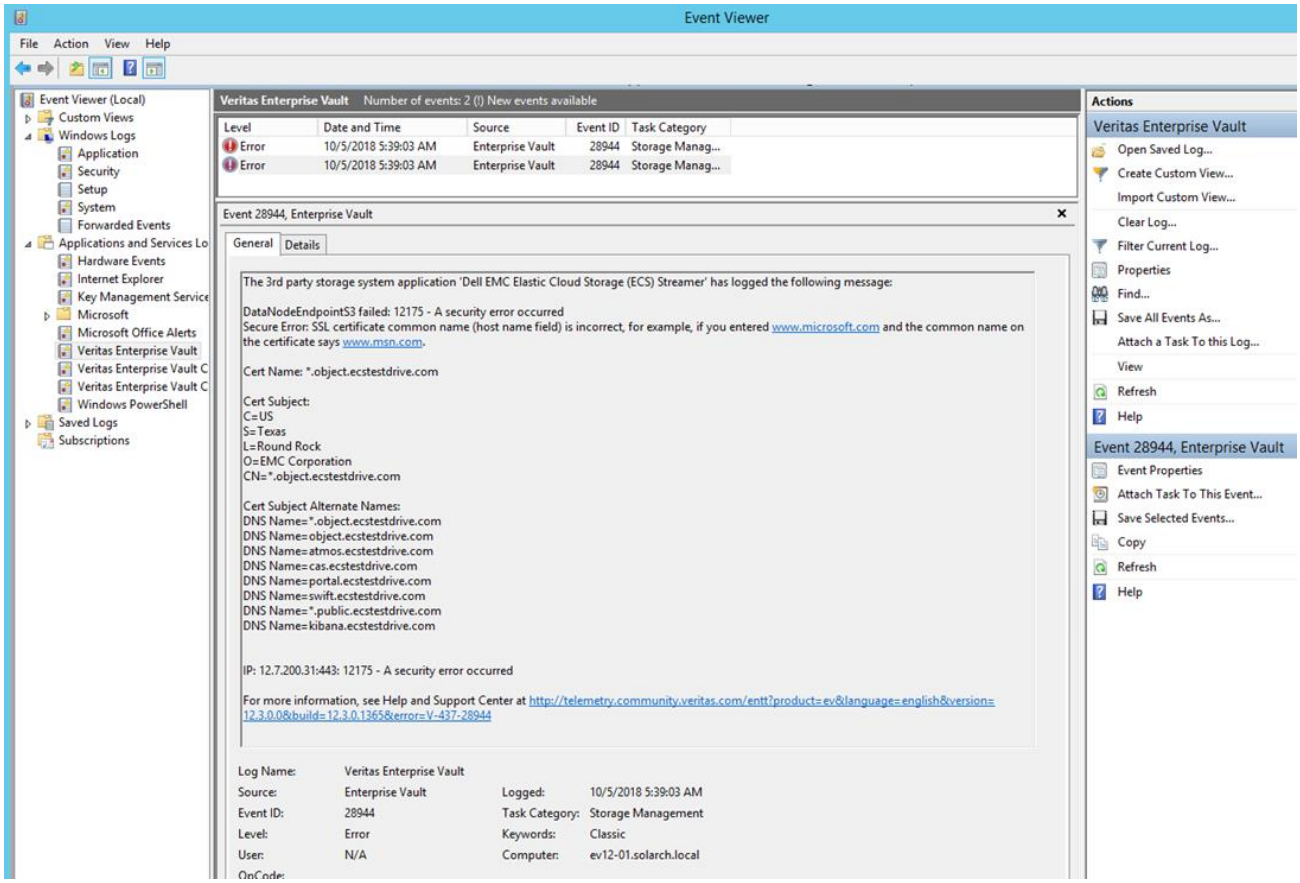

Figure 12 Windows event log

In this example, we see an error caused by using the IP address instead of the FQDN of the ECS portal. The ECS Portal SSL certificate is only valid when using the FQDN

This error was displayed by the EV Admin GUI when configuring the Vault Partition.

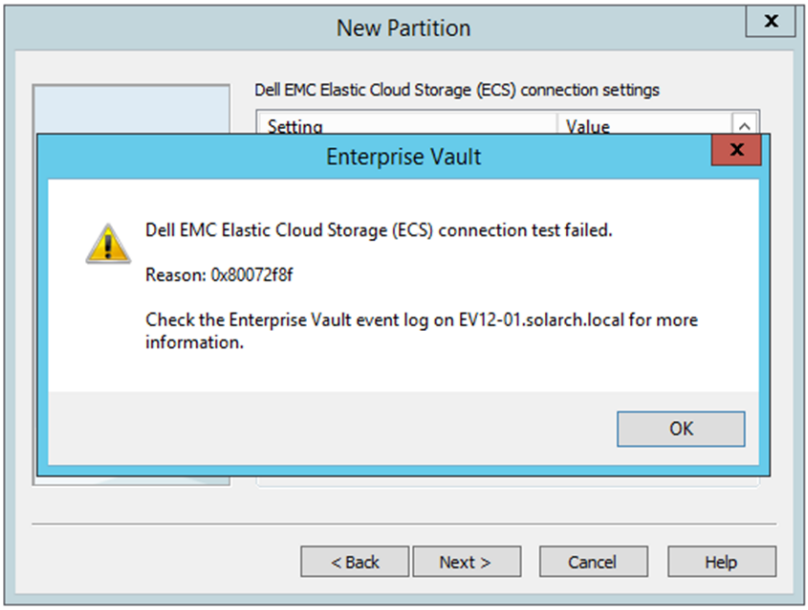

Figure 13 Partition configuration test error

As shown, there is more detailed logged by the ECS Streamer driver to the Windows event log.

6.2 Fiddler

Fiddler is a web debugging tool which will show the HTTP(S) traffic between the EV Server and the ECS system.

Download Fiddler from the following address: https://www.telerik.com/download/fiddler

After installation, change the EV Vault Store partition definition to use a Proxy on port 8888.

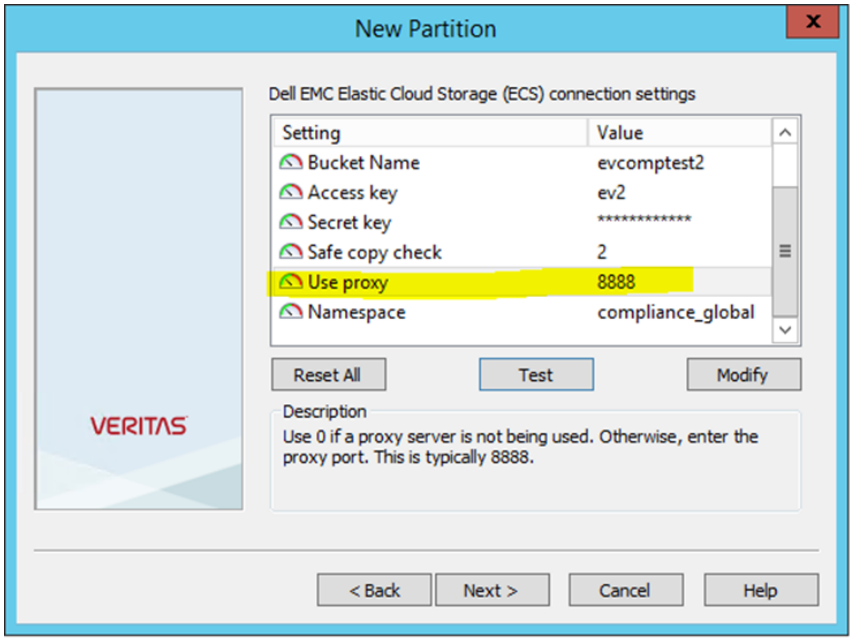

Figure 14 Fiddler change proxy port info

After updating the credentials, restart the EV Storage Service.

The following example shows the output in Fiddler from attempting to perform a Test of the Partition configuration when the partition has been configured to use the Dell EMC online ECS portal and when configuring the partition to use SafeCopy=2. Port 9101 is not open on the ECS portal load balancer and it will fail this check.

Incidentally, this is one of the more common issues encountered in new installations. The firewall and/or Load Balancers are not configured correctly for this port.

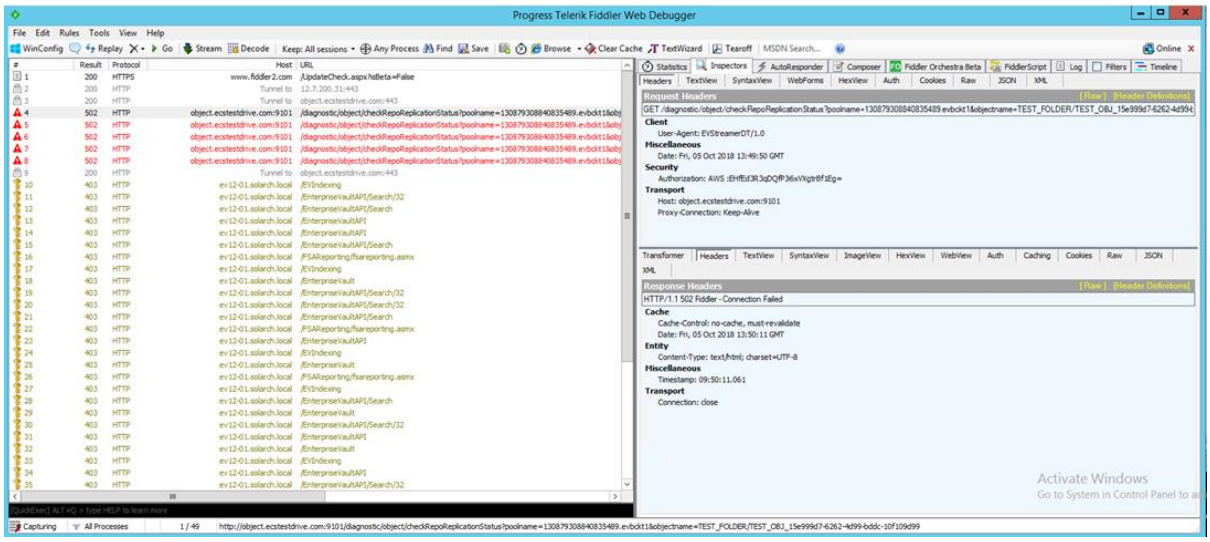

Figure 15 Fiddler output

You can see the attempts to connection to portal.ecstestdrive.com on port 9101 failing (the portal load balancer is not set up to pass 9101) on transactions 4 – 8.

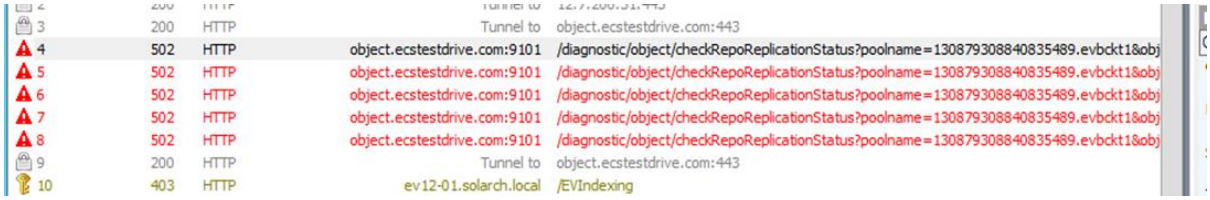

Figure 16 Fiddler output 2

The following screenshot shows the request and response headers.

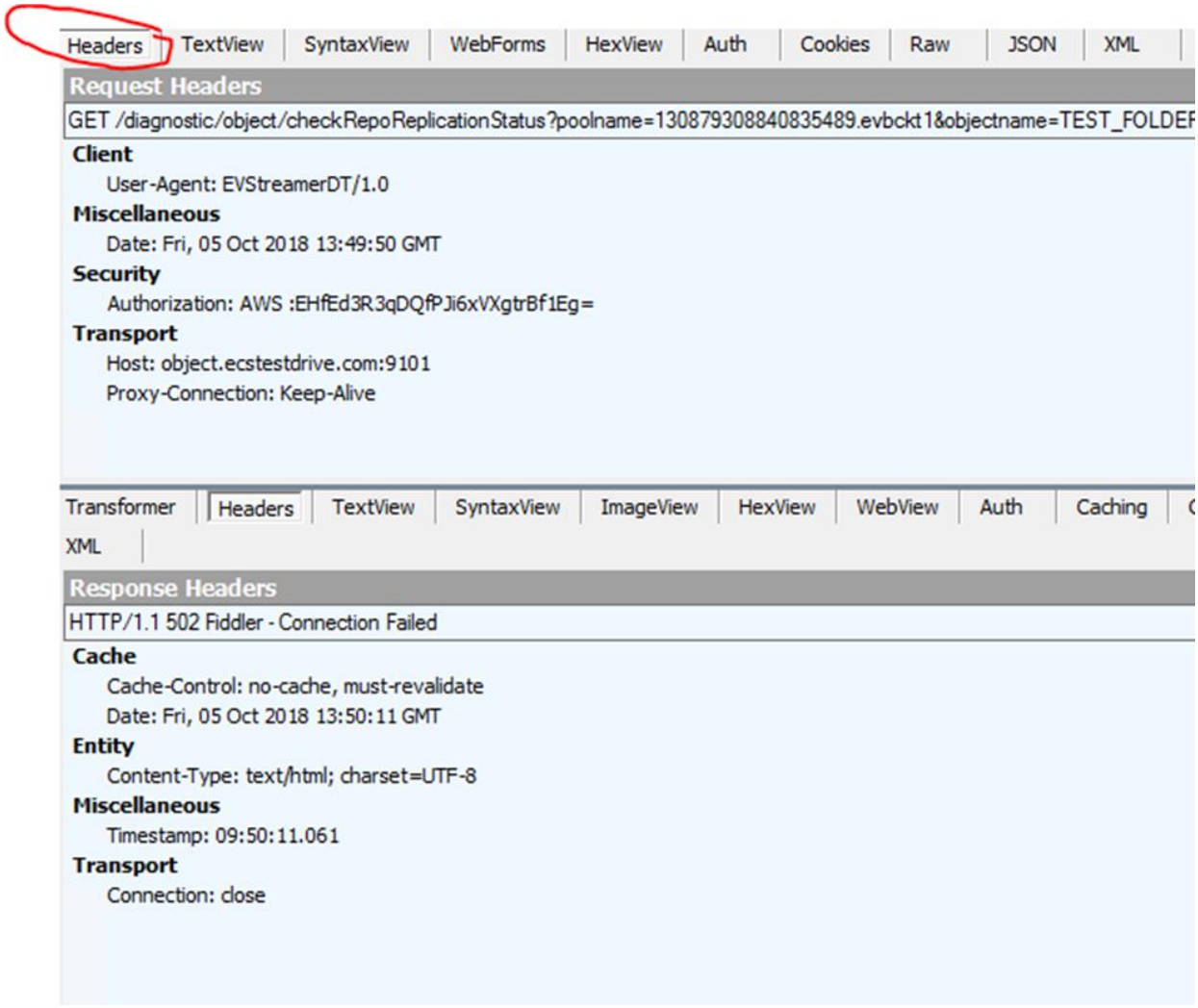

Figure 17 Fiddler header and response

The following shows the response as raw.

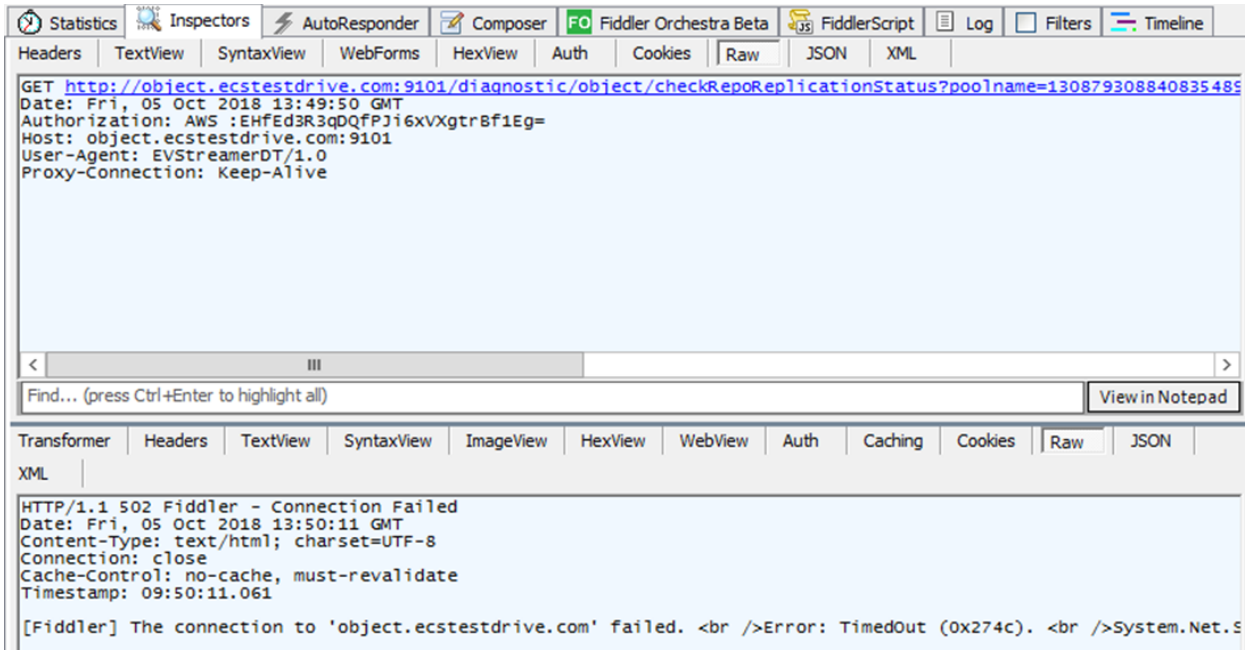

Figure 18 Fiddler: raw output

Fiddler is very useful for looking at the web traffic from the EV Server to ECS, and it may be simpler to use than a full network monitor.

6.3 DebugView

The ECS Streamer driver publishes debug information which normally is not viewable. The DebugView utility from Microsoft allows admins to view and log debug information that all applications write.

Download DebugView from the following address: https://docs.microsoft.com/en-us/sysinternals/downloads/debugview

Make sure to run DebugView as administrator.

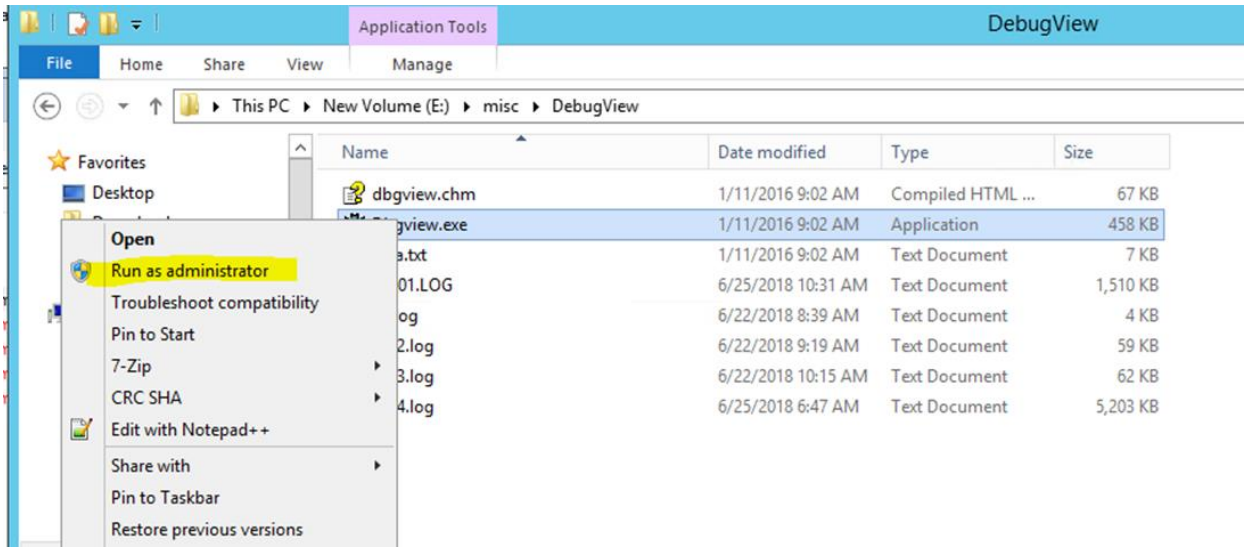

Figure 19 Running DebugView

When running DebugView, ensure that Capture Win32 and Capture Global Win32 are set .

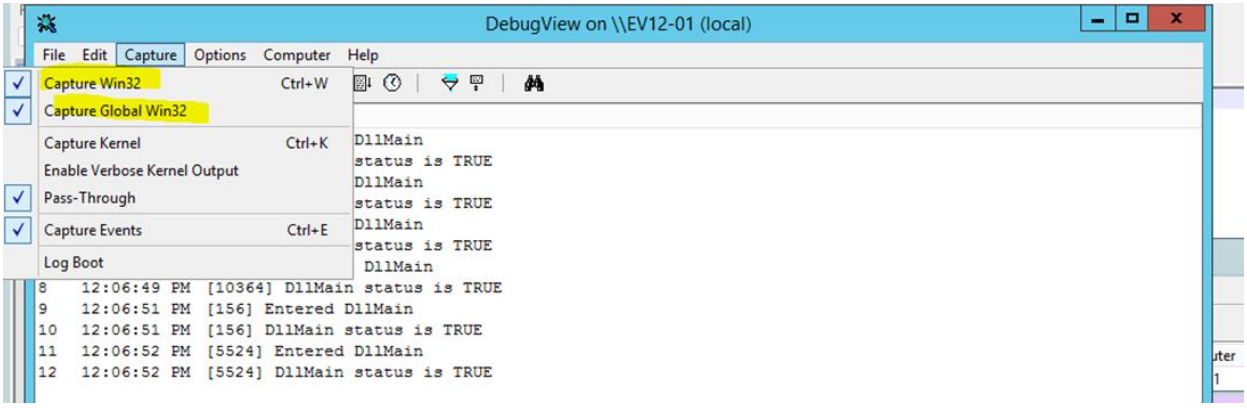

Figure 20 DebugView settings

If repeating a Partition Properties Test where specifying ;LB=true, the debugview window will show the following:

```
00140407 10:34:52 AM [9392] IP list coming in Init...prior to any possible
client side load balancing

00140408 10:34:52 AM [9392] 10.246.22.187
```

Enable more debugging output by running the EV dtrace.exe utility from the EV product installation directory and entering the following command:

```
set StorageManagement v y
```

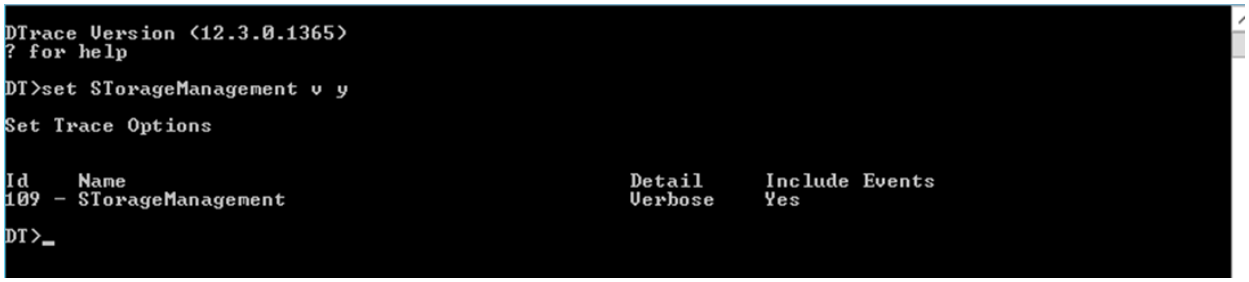

Figure 21 Running EV DTrace

If you repeat the same Test on the ECS Partition you will get a more-detailed debug output.

```
00140427   10:35:31 AM    [9392] IP list coming in Init...prior to any possible client side load
balancing

00140428   10:35:31 AM    [9392] 10.246.22.187

00140429   10:35:31 AM    [9392] [TID:9412] EVStreamer: DataNodeEndpointS3 for evtestbckt1 success

00140430   10:35:31 AM    [9392] [TID:9412] EVStreamer: setting endpoints for client side load
balancing

00140431   10:35:31 AM    [9392] [TID:9412] EVStreamer: client side load balancing: set address =
10.246.22.191

00140432   10:35:31 AM    [9392] [TID:9412] EVStreamer: client side load balancing: set address =
10.246.22.190

00140433   10:35:31 AM    [9392] [TID:9412] EVStreamer: client side load balancing: set address =
10.246.22.194

00140434   10:35:31 AM    [9392] [TID:9412] EVStreamer: client side load balancing: set address =
10.246.22.189

00140435   10:35:31 AM    [9392] [TID:9412] EVStreamer: client side load balancing: set address =
10.246.22.192

00140436   10:35:31 AM    [9392] [TID:9412] EVStreamer: client side load balancing: set address =
10.246.22.188

00140437   10:35:31 AM    [9392] [TID:9412] EVStreamer: client side load balancing: set address =
10.246.22.193

00140438   10:35:31 AM    [9392] [TID:9412] EVStreamer: client side load balancing: set address =
10.246.22.187

00140439   10:35:31 AM    [9392] [TID:9412] EVStreamer: CStreamerObject::Init checking if the bucket
has search metadata fields enabled

00140440   10:35:31 AM    [9392] [TID:9412] EVStreamer: CStreamerObject::Init does not seem to be
search meta but no error

00140441   10:35:31 AM    [9392] [TID:9412] EVStreamer: CStreamerObject::Init Exiting with HRESULT
0x0

00140442   10:35:31 AM    [9392] [TID:9412] EVStreamer: CStreamerObject::Test Entry
```

```
00140443    10:35:31 AM    [9392] [TID:9412] EVStreamer: ReadProperties for evtestbckt1 success

00140444    10:35:31 AM    [9392] [TID:9412] EVStreamer: property:sOwnerDisplayName

00140445    10:35:31 AM    [9392] [TID:9412] EVStreamer: property:sOwnerID

00140446    10:35:31 AM    [9392] [TID:9412] EVStreamer: property:sETag

00140447    10:35:31 AM    [9392] [TID:9412] EVStreamer: ReadProperties have been logged

00140448    10:35:31 AM    [9392] [TID:9412] EVStreamer: CStreamerObject::Test Connectivity check is
going to write a test object since replication check 2 is being used

00140449    10:35:31 AM    [9392] [TID:9412] EVStreamer: Create object for evtestbckt1 success

00140450    10:35:31 AM    [9392] [TID:9412] EVStreamer: CStreamerObject::Test ConnectivityCheckWrite
succeeded. About to try dtquery and delete it

00140451    10:35:31 AM    [9392] [TID:9412] EVStreamer: dtquery returning false

00140452    10:35:31 AM    [9392] [TID:9412] EVStreamer: CStreamerObject::Test Exiting with HRESULT
0x0
```

The output is displaying the ECS node IP addresses that it will use, and it will read the properties for the ECS bucket being used. It created and deleted a test object and checked the replication status of the test object. Also, 9392 is the PID of the StorageManagement.exe process.

6.4 ECSCHECK.EXE

With ECS Streamer driver revision 2.0.1.5, the driver ships with a diagnostic utility to help you check the connection to the ECS from your EV server.

Ecscheck.exe is installed into the same directory as the ECS Streamer, normally as in the following case.

```
C:\Program Files (x86)\Dell EMC\EVStreamer
```

Start a CMD.EXE window and change to that directory. The following shows ecscheck commands:

```
C:\Program Files (x86)\Dell EMC\EVStreamer>ecscheck.exe /?
Usage:

   /http                                  Don't use SSL
   /https                                 Use SSL (default)
   /endpoint <IP or hostname>             S3/ECS Server
   /port <port number>                    Rest API Port
   /user <user ID>                        ECS object user
   /secret <secret>                       ECS object secret
   /list <path, starting with bucket>     Object listing
   /create <localfile> <ECSpath>          Create ECS object and initialize with file
   /delete <ECSpath>                      Delete ECS object
   /read <localfile> <ECSpath>            Read ECS object into file
   /write <localfile> <ECSpath>           Write ECS object from file
   /readmeta <ECSpath>                    Read all metadata from object
   /cert                                  Display certificate even if connect successful
   /setcert                               Prompt user to install certificate
   /dtquery <namespace> <bucket> <object> DT Query for object
   /createbucket <bucket>                 Create ECS bucket
   /retention <seconds>                   Used with /createbucket to set bucket-level retention

Press ENTER to continue...
```

Figure 22 Getting help from ecscheck.exe

The following lists the details of the endpoint:

```
C:\Program Files (x86)\Dell EMC\EUStreamer>ecscheck.exe /http /endpoint 10.246.22.187 /port 9020 /user ev1 /secret OI+J8UxFscxEeFGMftHA3vsJazulFPUmsP6ZUIAx /listbuckets
OwnerID: ev1, Name: ev1
  Bucket: ev10bckt1: 8/4/2018 12:51:19 PM
  Bucket: ev10bckt2: 8/6/2018 6:59:58 AM
  Bucket: ev11bckt1: 6/27/2018 11:36:00 AM
  Bucket: ev12bckt1: 8/8/2018 11:13:37 AM
  Bucket: evbckt1: 5/23/2018 11:17:11 AM
  Bucket: evnwbckt1: 7/11/2018 1:34:24 PM
  Bucket: evnwperf1: 7/9/2018 4:12:37 PM
  Bucket: evperfbckt: 7/1/2018 10:14:44 AM
  Bucket: evperfbckt2: 7/2/2018 12:40:05 PM
  Bucket: evperfbckt3: 7/3/2018 8:29:37 AM
  Bucket: evperfbckt4: 7/3/2018 11:49:20 AM
  Bucket: evperfbckt5: 7/4/2018 10:59:10 AM
  Bucket: evtestbckt1: 10/1/2018 2:44:19 PM
  Bucket: test1: 10/16/2018 7:55:58 AM
Version: 3.2.1.0.102266.5bd8357.4
  Endpoint: 10.246.22.191
  Endpoint: 10.246.22.190
  Endpoint: 10.246.22.194
  Endpoint: 10.246.22.189
  Endpoint: 10.246.22.192
  Endpoint: 10.246.22.188
  Endpoint: 10.246.22.193
  Endpoint: 10.246.22.187

C:\Program Files (x86)\Dell EMC\EUStreamer>
```

Figure 23 Listing buckets and details

The /list command on its own will show the buckets available to the user and the IP addresses of all ECS Nodes in the cluster. The following shows obtaining the ECS installed certificate:

```
C:\Program Files (x86)\Dell EMC\EUStreamer>ecscheck.exe /https /endpoint 10.246.22.187 /port 9021 /user ev1 /secret OI+J8UxFscxEeFGMftHA3vsJazulFPUmsP6ZUIAx /cert
S3ServiceInformation error: 12175 - A security error occurred
Secure Error: The function is unfamiliar with the Certificate Authority that generated the server's certificate.
SSL certificate common name (host name field) is incorrect, for example, if you entered www.microsoft.com and the common name on the certificate says www.msn.com.

Cert Name: DataService

Cert Subject:
CN=DataService

Cert Subject Alternate Names:


IP: 10.246.22.187:9021
Cert Name: DataService

Cert Subject:
CN=DataService

Cert Subject Alternate Names:

Install Certificate?
n
Press ENTER to continue...
```

Figure 24 Obtain the installed certificate

This use of the /cert command shows you the installed certificate on the ECS. In this example, there is no certificate installed, and the utility does prompt to allow you to install one.

The following shows a self-signed certificate example:

```
C:\Program Files (x86)\Dell EMC\EUStreamer>ecscheck.exe /https /endpoint hop-paul-lb.solarch.lab.emc.com  /port 443 /user ev1 /secret OI+J8UxFscxEeFGMftHA3vsJazulFPUmsP6ZUIAx /cert
S3ServiceInformation error: 12175 - A security error occurred
Secure Error: The function is unfamiliar with the Certificate Authority that generated the server's certificate.

Cert Name: paul

Cert Subject:
C=MA
S=Massaschusettes
L=Hopkinton
O=DellEMC
OU=UDS
CN=paul
E=paul.mckeown@dell.com

Cert Subject Alternate Names:
DNS Name=hop-paul-lb.solarch.lab.emc.com
DNS Name=swift.hop-paul-lb.solarch.lab.emc.com
IP Address=10.246.27.211


IP: hop-paul-lb.solarch.lab.emc.com:443
Cert Name: paul

Cert Subject:
C=MA
S=Massaschusettes
L=Hopkinton
O=DellEMC
OU=UDS
CN=paul
E=paul.mckeown@dell.com

Cert Subject Alternate Names:
DNS Name=hop-paul-lb.solarch.lab.emc.com
DNS Name=swift.hop-paul-lb.solarch.lab.emc.com
IP Address=10.246.27.211

Install Certificate?
```

Figure 25 Obtain the installed certificate: self-signed certificate example

The following shows obtaining the installed certificate from portal.ecstestdrive.com. This screenshot shows the same command used against the ECS portal system which does have a certificate installed.

Figure 26 Obtain the installed certificate from portal.ecstestdrive.com

6.4.1 Test dtquery

To check that dtquery will work, create a new bucket, write a file, and do the dtrace check with the following commands:

```
ecscheck.exe /http /endpoint 10.x.x.x /port 9020 /user ev1 /secret OT+<snip> /createbucket test1

ecscheck.exe /http /endpoint 10.x.x.x /port 9020 /user ev1 /secret OT+<snip> /write localfile
/test1/object1

ecscheck.exe /http /endpoint 10.x.x.x /port 9020 /user ev1 /secret OT+<snip> /dtquery veritas_c test1
object1
```

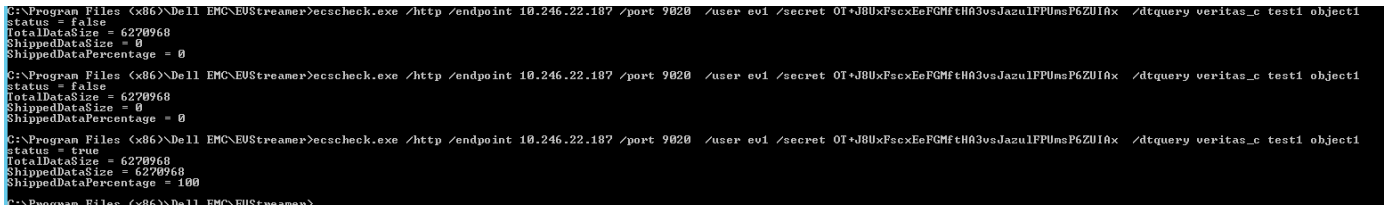

Figure 27 dtquery check

The dtquery check figure shows the check on the object showing that 0% of it has been replicated to ECS VDC2, but the second check shows that 100% of the object has been replicated.

7 Supported environments

7.1 Veritas Enterprise Vault

Veritas has a detailed support matrix for all Enterprise Vault including third-party software and hardware components at the following address: https://www.veritas.com/support/en_US/doc/128058600-128865835-0/index

7.2 Dell EMC ECS

As of ECS revision 3.4 customers should use revision 2.0.6.x of the ECS Streamer Driver. This is due to ECS hardening the port 9101.

If a customer is already using ECS Streamer Driver 2.0.6.x and they upgrade to ECS 3.4, they do not need to change how they have configured their Vault Store Partitions Safe Copy from 2 to 1, the driver will automatically use the correct Geo Replication checking mechanism.

8 Streamer release information

Table 8 Streamer release information

Release #	Description
2.0.6.18	Fix for: SDK-532: EV Streamer: May log: Severe Error! Dump file created here: <path> SDK-533: EV Streamer: dump files generated similar to: StorageManagement.exe_translate_exceptions_GUID.dmp
2.0.6.16	Fix for: SDK-530: EV Streamer: Allow DTQuery to be used for replication check if using ECS 3.4 SDK-528: EV Streamer: if safe-copy = 0 it doesn't comply with Veritas API spec: remotecopies = 0
2.0.6.13	Update of the Microsoft Visual C++ redistributables SDK-514: EV Streamer: Error log shows: Unexpected retentionType found: 0 SDK-517: EV Streamer setup doesn't always upgrade the VC++ redistributable to the required level SDK-518: EV Streamer: EnumNext returns StoredDate against local time instead of UTC SDK-519: EV Streamer: EnumNext: if time range is specified, it may not return the entries at start and end of range
2.0.6.2	Faster, more efficient method used to test for bucket level retention. Better testing of writes when there is bucket level retention of 1 second. Support for S3 V4 authentication. Performance monitor stats can be reset. Admin can specify an install path for the ECS Streamer driver on installation. Remote installation utility provided.
2.0.5.6	The Test() method no longer tests for bucket level retention. The admin must set the option DISABLE_WRITE_TEST or Test() will fail. Metadata search info call removed from initialisation.
2.0.5.4	Windows Performance Monitor counter objects added.

Release #	Description
	The ECS Streamer install directory is added to the Windows PATH environment variable. This allows users to run ECSCheck.exe or EVResetPerf.exe from any directory.
2.0.4.1	Throttle Streamer Instances – the number of outstanding EVStreamer requests by default limited to 65. Faster enumeration of objects in a vault store. Improved management of the connection object.
2.0.3.2	Corrections made to the error codes returned when some errors are encountered.
2.0.3.1	Corrections to error returns from the ECS Streamer to Enterprise Vault. Added DONT_TEST_STOPPING switch on HOST – Dell EMC Support use only Changed the time that the streamer will wait before retrying an ECS node marked as offline to 12 minutes from 2 hours.
2.0.2.3	Improved handling of Partition listings **Installation** Install file is a .MSI instead of a .EXE **Cached Connections** S3 connections are cached to greatly reduce the overhead involved with establishing connections. Currently the streamer will frequently execute the “Init()” entry which will do the following ECS requests: • Get endpoint list • Test if search metadata can be used. With the new version, that initialization only occurs the first time the connection is requested. It will only redo it if any of the parameters change, or if the S3 request fails. **Allow HTTPS connections to Ignore Bad CN Error** When establishing an HTTPS connection, normally the connection will fail if the host name provided does not match the name in the certificate. For example, using an IP address. The user can use the IGNORE_BAD_COMMON_NAME option in host parameter to allow the connection to succeed. **Relax Syntax for Host Name Options** The current syntax for each host name option is "<option>=<value>". The “=<value>” is now optional if <value> would be 1. This means that the following is now accepted: 10.1.2.3;LB;DISABLE_WRITE_TEST

Release #	Description
2.0.1.5	Improved error log messaging Additional IP range specification Writes of old files have their retention handled properly, previously an error would be generated. ecscheck utility.
2.0.0.7	Better error log messages and diagnostics Multi-Part uploads are multithreaded and will perform better Better overall performance Improved Stability Built in IP Load Balancer across ECS Nodes in the VDC being used.
1.0.16	Fix to partial file read requests which where erroneously on occasion performing full file reads unnecessarily.
1.0.14	Default MAX_CONNS changed to 65 Added optional SHOWCHUNKS configuration parameter to assist debugging Added optional RDT parameter to ensure requests are not cached Added option DTHOSTS parameter to assist with debugging Issue caused by caching in the Windows HTTP library resolved.
1.0.12	Modified the Test() function. Since Evault itself also calls the Test functionality, it is not reasonable to fail the test if the dtquery call fails. This information is logged but does not fail the connectivity test. This portion of the test is only done when safecopy==2. Unfortunately, dtquery has problems during TSO. So any call to the Test functionality by Evault when safecopy==2 during TSO, would cause archiving to stop. During archiving any failure in dtquery simply sets the safe copy boolean to false and archiving continues.
1.0.11	Added a fix for a potential Read() problem where Windows may require a larger buffer

9 Performance information

At the present, no performance testing has been performed. However, as part of the Veritas Enterprise Vault Self Certification testing performed by Dell EMC, some basic throughput measurements were taken.

9.1 Testing configuration

The following system configurations were used for testing with Enterprise Vault revisions tested.

Table 9 Testing configuration

Server	Configuration
SQL Server DB	8 x vCPU, 32Gb RAM 3 x 100GB SAN Disk 10GbE NIC Windows 2012R2 STD SQL Server 2014
EVServer 1	8 x vCPU, 32Gb RAM 3 x 100GB SAN Disk 10GbE NIC Windows 2012R2 STD
EVServer 2	8 x vCPU, 32Gb RAM 3 x 100GB SAN Disk 10GbE NIC Windows 2012R2 STD

9.2 Results

Table 10 Performance results

Item	EV12	
Ingest – File/Hour	136,000	
Ingest – Mbytes/hour	6,485	
Read Test – Files/Hour	1,285,550	
Expiration Test – Files/hour	34,600	

A Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

Storage technical documents and videos provide expertise that helps to ensure customer success on Dell EMC storage platforms.