Scan Tool (EV-6157) for Director 8.00 Vaults Instructions

EVault®
from Carbonite

The EVault Software Agent, EVault Software CentralControl, and EVault Software Director applications have the encryption option of AES (Advanced Encryption Standard). Advanced Encryption Standard algorithm (named Rijndael, pronounced "Rain Doll") was developed by cryptographers Dr. Joan Daemen and Dr. Vincent Rijmen. This algorithm was chosen by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce to be the new Federal Information Processing Standard (FIPS).

The EVault Software Agents and EVault Software Director applications also have the added security feature of an over the wire encryption method.

Introduction

This document describes how to run the scan tool provided for Director 8.00 vaults for detecting potential problems with deferred backups (issue EV-6157).

Issue description

In rare cases, problems can occur when maintenance processes run on deferred backups from a small subset of Agent versions. To prevent problems from occurring, upgrade Director to version 8.00h.

After upgrading Director to version 8.00h, run the scan tool provided. The scan tool identifies tasks that might have problems with deferred backups, and prevents subsequent maintenance processes from running on the tasks.

Note: The scan tool does not change pool files. A method will be provided in the near future to resolve any problems associated with this issue.

Scan tool description

The scan tool is provided in a .zip file named ScanTool_EV-6157_8.00h.zip. This .zip file contains a ScanTool folder that includes:

- the scan tool executable file: ScanTool-EV-6157.exe

- .dll files required by the scan tool

When you run the scan tool on a vault, the tool creates the following files in the folder where the scan tool is running:

- Output.csv – This file shows the total number of tasks in the vault and indicates whether each task is "safe", or at risk of problems with deferred backups.

  The first line of the Output.csv file shows the total number of tasks in the vault and the date and time when the scan tool ran. This summary line has the following format:

  "v*aultIdentifier(GUID)*","*vaultSystemName*","`__NumberOfTasksInVault`","*numberOfTasksInVault*" ,"*mmm-dd-yyyy-hh-mm-ss*"

  Note: If you run the scan tool more than once on a vault, the summary line could appear more than once in the Output.csv file. For more information, see the [UnknownTasks](#).txt file description.

  The remaining lines in the Output.csv file list each task in the vault, and indicate whether the task is safe or at risk of problems with deferred backups. Each line has the following format:

  "v*aultIdentifier(GUID)*","*vaultSystemName*","*customerName*","*location*","*computerName*, "*taskName*",`["Safe"|"AtRisk"][,"OfflineDataDetected"]`

  If "OfflineDataDetected" appears at the end of a line, some safesets for the task were offline and could not be scanned (e.g., archived or in detached secondary storage). To check these safesets, you can run the ssiverall subcommand on the safesets or try to restore the data. For more

information, see the *Director User Guide.* If "OfflineDataDetected" does not appear at the end of a line, all safesets for the task were online and could be scanned.

- UnknownTasks.txt – This file lists tasks that the scan tool has not completely scanned yet. A task might not be completely scanned if it is locked (e.g., if a backup is running) when the scan tool runs.

  When the scan tool runs, it first checks whether an Unknown.txt file exists. If an Unknown.txt file exists and includes task names, the scan tool only scans the tasks listed in the Unknown.txt file (i.e., tasks that were locked when the scan tool previously ran). The scan tool then appends another summary line to the Output.csv file that shows the total number of tasks in the vault and the date and time when the scan tool ran. The scan tool also appends a line in the Output.csv file for each task that it scans, and indicates whether the task is safe or at risk of problems with deferred backups.

- ScanTool-*xxxxxxxx-xxxx-xxxx*.log – This scanning process log indicates each task that was checked, and whether each task is safe or at risk of problems with deferred backups. *xxxxxxxxxxxx-xxxx* is a random GUID, and does not represent the vault GUID.

For each task that is identified as "at risk", the scan tool creates a blank vvmigrat.exe.config file and migratesecondary.exe.config file in the task folder. These blank config files prevent subsequent maintenance processes from running on the task, and possibly causing problems.

Run the scan tool

Before running the scan tool, upgrade Director to version 8.00h.

To run the scan tool:

1. Disable maintenance processes on the vault by doing the following:
   a. Select the vault in the left pane of Director Management Console.
   b. From the **Vault Maintenance** menu, choose **Vault Settings**.
   c. On the **Maintenance** tab, clear **Enable maintenance host on**

      '*vaultName'*. d. Click **OK**.

2. Extract the ScanTool_EV-6157_8.00h.zip file in a directory on the machine where Director 8.00h is installed.

   IMPORTANT: Do not extract files from the ScanTool_EV-6157_8.00h.zip file so that they overwrite files in the \Director\prog folder.

3. Right-click the scan-tool executable file (ScanTool-EV-6157.exe), and choose **Run as administrator**.

   When the scan is finished, output files (i.e., Output.csv, Unknown.txt, etc.) are available in the folder where you extracted the ScanTool_EV-6157_8.00h.zip file and ran the scan tool.

   Note: If any tasks are listed in the Unknown.txt file, these files have not been completely scanned yet. Run the scan tool again to scan these files. If the Unknown.txt file exists in the

directory where the scan tool runs and includes task names, the tool only scans the tasks listed in the Unknown.txt file.

4. Re-enable maintenance processes on the vault by doing the following:

   a. Select the vault in the left pane of Director Management Console.

   b. From the **Vault Maintenance** menu, choose **Vault Settings**.

   c. On the **Maintenance** tab, select **Enable maintenance host on '*vaultName'*.**

   d. Click **OK**.