CyberArk SYSLOG

Data Collection

Script

This script is based off of the PAS APM Dashboard Package for Splunk created by James Creamer III (jcreameriii). GitHub link: <https://github.com/jcreameriii/PAS-APM-Dashboard-Package-for-Splunk>

The scripts as provided had one dedicated to the Vault server and one dedicated to the other Component servers. You were expected to customize each script for the component to be targeted.

The script is written in PowerShell and is expected to be ran on Windows OS server with a minimum of PowerShell version 5.

The new script takes command line parameters to designate the “CollectionProfile”. This is a data collection profile. This command line parameter accepts an array so you can specify multiple collection profiles.

# Command Line Parameters

Here are the available command line parameters that can be passed to the script at run time.

## CollectionProfile options

Collection profile types:

1. All
   1. All collection profiles will be run.
2. LocalHostInfo
   1. This collects extensive information about the server.
3. LocalHostNetwork
   1. This collects information about all active network adapters.
4. LocalHostDrives
   1. This collects information about all drives connected to the server.
5. LocalHostFirewall
   1. This collects information about all enabled firewall rules. Inbound and Outbound rules will be provided on separate messages.
6. LocalUsers
   1. This collects information about all local OS users on the server.
7. LocalGroups
   1. This collects all of the members of all local groups on the OS.
8. LocalSoftwareAll
   1. This collects about all software installed on the host, that shows up in the Add/Remove programs page.
9. LocalSoftwareFilter
   1. This is the same as LocalSoftwareAll but applies a filter that is defined in the script. The variable name is “$COLLECTSOFTWAREINFOFILTER”.
10. Vault
    1. This is a CyberArk specific collection. It collects information related to the Secure Digital Vault, Disaster Recovery Service, and Remote-Control Agent.
11. PVWA
    1. This is a CyberArk specific collection. It collects information related to the PrivateArk Web Access server.
12. CPM
    1. This is a CyberArk specific collection. It collects information related to the CyberArk Central Policy Manager.
13. PSM
    1. This is a CyberArk specific collection. It collects information related to the CyberArk Privileged Session Manager.
14. CCP
    1. This is a CyberArk specific collection. It collects information related to the CyberArk Central Credential Provider.
15. CVCS
    1. This is a CyberArk specific collection. It collects information related to the CyberArk Conjur Vault synchronizer service.

## TextSeperator

The text separator can be changed from the default of Pipe “|”. This can cause issues with other nested data types because of how deep the nesting can go.

The table of separators and the order in which they are used is called “TEXTSEPARATORORDER”.

Text Separator Order

1. '|'
   1. Pipe
2. ';'
   1. Semi Colon
3. '~'
   1. Tilde
4. '+'
   1. Plus
5. '@'
   1. At
6. '\*'
   1. Star
7. '%'
   1. Percent
8. '^'
   1. Carrot / Top Hat
9. '`'
   1. Back Tick

## PVWALogonType

This specifies the CyberArk PasswordVault Web Access page to test for the synthetic transaction monitoring. The table name for the addresses is “PVWAENDPOINTSTOTEST”.

1. DefaultLogon
   1. "PasswordVault/v10/logon"
2. CyberArk
   1. "PasswordVault/v10/logon/cyberark"
3. LDAP
   1. "PasswordVault/v10/logon/LDAP"
4. RADIUS
   1. "PasswordVault/v10/logon/RADIUS"
5. SAML
   1. "PasswordVault/v10/logon/SAML"

## WriteLog

If this option is specified then a log of the data sent to the SYSLOG server will be created. This should be used for troubleshooting.

# Optional Script Modifications

There is an option to write the SYSLOG message to a log file. This parameter is “SYSLOGENABLEDATALOGGING” and is either True or False.

The parameter “SYSLOGDATALOGFILE” specifies the filename for the log file. This will be written to the working directory. The working directory can be the same as the folder where the PowerShell script is executed.

# Required Script Modifications

The variables listed below must be customized to your environment.

1. $SYSLOGSERVER = "192.168.184.134"
   1. This should be the fully qualified domain name or IP address of the SYSLOG server.
2. $SYSLOGPORT = 514
   1. This should be the port that the SYSLOG server is using.
3. $SYSLOGPROTOCOL = "UDP"
   1. This is the protocol that the SYSLOG server is using.
4. $PVWAURL = "192.168.184.134"
   1. This is the fully qualified domain name or IP address of the PVWA server. You can specify a VIP here. This will only be needed if the PVWA data collection profile is specified.
5. $PVWAIGNORESSL = $true
   1. If using the IP address or if the PVWA server does not have a valid X.509/SSL/TLS   
      certificate then this option should be set to True.

# Output data structures

This section will describe the output data structure of each collection profile.

The default SYSLOG format is defined by RFC 5424 and the break down is can be found in the following links.

<https://www.rfc-editor.org/rfc/rfc5424>

<https://www.rfc-editor.org/rfc/rfc3164.html>

<https://en.wikipedia.org/wiki/Syslog>

Typical Fields:

1. Priority
2. Version
3. Timestamp
4. Hostname
5. Application
6. Process ID
7. Message ID

Example:

<31>1 2023-01-11T22:14:15Z Hostname.Domain.com CyberArk 328 Message Data

This script does not fully comply with the RFC.

## Typical Separator Order

For all of the data structures this is the order of the separators.

Some of the fields support multiple entries and if only 1 entry is found then that separator will not be present. Though it does not hurt to split on the character. This ensures if some of the data in the future contains multiple entries it will be parsed correctly.

Here is the separator order. Start with number 1 and work your way down.

1. '|'
2. ';'
3. '~'
4. '+'
5. '@'
6. '\*'
7. '%'

## Common Output Data

All of the collection profiles begin with the below portion. The default separator is “|” Pipe. This can be changed but it would break any existing integrations.

2023-01-20T09:51:22Z CEF:0|CyberArk|ApplicationMonitor|1.0.0000|Hostname|Nested Data

When split with the “|” Pipe character you get these entries:

1. Time Stamp & Version
   1. This field can be further split using the “T” character.
   2. This creates these fields.
      1. Date
      2. Time & Format
         1. This field can be further split using the “Z” character.
         2. This creates these fields.
            1. Time
            2. Format & Version

This field can be further split using the “:” character.

This creates these fields.

Format

Version

1. Device Product
2. Device Version
3. Device ID
4. Nested Data

## Local Host Info

Data fields:

1. Host Name
2. Host Domain
3. Host DNS Name
4. Host Manufacturer
5. Host Model
6. Host RAM
7. Host Serial Number
8. Host CPU Cores
9. Host Sockets
10. Host Processor Name
11. Host Processor Caption/Description
12. Host OS Root
13. Host OS Version
14. Host OS Install Date
15. Host Local Tie
16. Host Time Zone
17. Host Last Boot Time
18. Host Domain Role
19. Host Fully Qualified Domain Name
20. Host Last Update date and time

## Local Host Network

Data fields:

1. Network Device ID
2. Network Index Number
3. Globally Unique Identifier (GUID)
4. Network Caption
5. Network Description
6. Adapter Type
7. Host MAC Address
8. Time of Last Reset
9. Speed
10. IP Configurations
    1. IP Adapter
       1. IP Index Number
       2. DHCP Enabled
       3. DNS Domain Suffix Search Order
          1. DNS Suffix
       4. DNS Host Name
       5. DNS Server Search Order
          1. DNS Server
       6. IP Addresses
          1. IP Address
       7. IP Subnets
          1. IP Subnet
       8. Default IP Gateway
          1. IP Address
       9. Interface Index Number
       10. MAC Address
       11. IP Filter Security Enabled

## Local Host Disks

Data fields:

1. Drive ID (DID)
2. Drive Name
3. Drive Caption
4. Drive Description
5. Interface Type
6. Drive Size
7. Partition Count
8. Partitions
   1. Partition (There can be multiple partitions on the same drive.
      1. Partition Index
      2. Partition Name
      3. Partition Caption
      4. Partition Description
      5. Type
      6. Partition Size
      7. Logical Disks
         1. Logical Disk (There can be multiple logical disks on a partition.)
            1. Logical Device ID
            2. Volume Serial Number
            3. Logical Disk Name
            4. Logical Disk Caption
            5. Logical Disk Description
            6. Drive Type
            7. File System
            8. Media Type
            9. Logical Disk Size
            10. Free Space

## Local Host Firewall

Data fields:

1. Firewall Rule
   1. ID
   2. Display Name
   3. Group
   4. Enabled
   5. Profile
   6. Direction
   7. Action
   8. Caption
   9. Description
   10. Display Group
   11. Rule Group

## Local Users

Data fields:

1. Users
   1. User Security Identifier (SID)
   2. Username
   3. User Caption
   4. User Description
   5. User Domain
   6. Account Disabled
   7. Account Locked
   8. Last Password Change

## Local Groups

Data fields:

1. Groups
   1. Group Security Identifier (SID)
   2. Group Name
   3. Group Caption
   4. Group Domain
   5. Group Description
   6. Members
      1. Member
         1. User Domain\Username
         2. Security Identifier (SID)

## Local Software (All/Filtered)

This collection profile is the same for All or Filtered. The only difference is the Filtered option will only return software listed in the variable “COLLECTSOFTWAREINFOFILTER”. Common PowerShell wildcard characters will work here.

Data fields:

1. Software Packages
   1. Software Package
      1. Publisher
      2. DisplayName
      3. Display Version
      4. Install Date
      5. Install Location

## Common Component Collection

This collection profile is always performed.

OS Performance

1. CPU
2. RAM
3. Total HDD Space
4. Total Free Space

OS Monitor

1. OS Name
2. OS Version
3. OS Service Pack
4. OS Architecture

## Vault

This collection profile collects the following information.

Windows Services

1. PrivateArk Server
2. PrivateArk Database
3. CyberArk Logic Container
4. PrivateArk Remote Control Agent
5. Cyber-Ark Event Notification Engine
6. CyberArk Vault Disaster Recovery

Last Administrator Logon

1. Local Administrator Name
2. Local Administrator Security Identifier (SID)
3. Last Logon Time stamp

## PVWA

This collection profile collects the following information.

Messages

Windows Services

1. W3SVC
2. CyberArk Scheduled Tasks

Synthetic Transaction Monitor

1. Target URL
2. HTTP Status Code
3. Response time in milliseconds
4. HTTP Server Info (If available)
5. HTTP Response Message/Description

## CPM

This collection profile collects the following information.

Windows Services

1. Cyberark Password Manager
2. Cyberark Central Policy Manager Scanner

## PSM

This collection profile collects the following information.

Windows Services

1. Cyber-Ark Privileged Session Manager
2. W3SVC
3. TermService

Session Count

1. Remote Desktop User Session Count

Shadow Users

1. All local users on the PSM server whose name starts with PSM-
   1. Local user’s full name."

## CCP

This collection profile collects the following information.

Windows Services

1. CyberArk Vault-Conjur Synchronizer

## CVCS

This collection profile collects the following information.

Windows Services

1. W3SVC
2. CyberArk Application Password Provider

## Windows Service

For each service listed the following information is collected and displayed.

Data fields:

1. Service Name
2. Service Status
3. Service Status in Numeric form
4. Software Name
5. Software Version

# Running The Collection Script

This section will describe how to manually run or schedule the script to be run.

## Manual

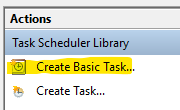
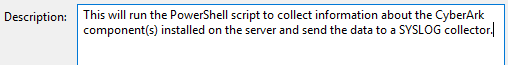
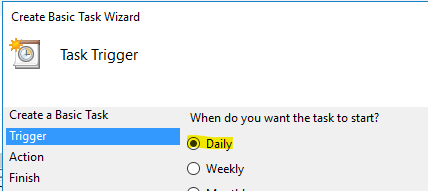
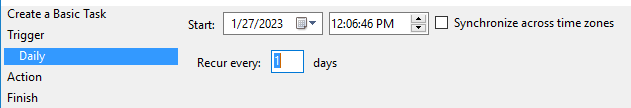
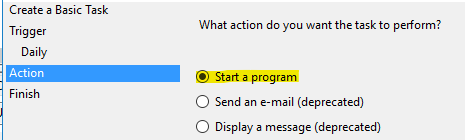
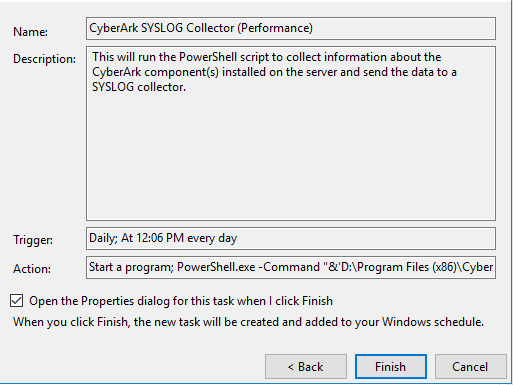
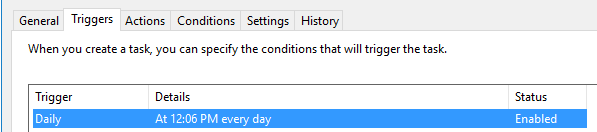
Examples:

1. This will use the “All” Collection Profile
   1. .\PAS-APM-Components-01.ps1
2. This will use the “LocalHostInfo” Collection Profile
   1. .\PAS-APM-Components-01.ps1 -CollectionProfile LocalHostInfo
3. This will use the “LocalHostInfo” and “LocalGroups” Collection Profiles
   1. .\PAS-APM-Components-01.ps1 -CollectionProfile LocalHostInfo,LocalGroups
4. This will use the “LocalHostInfo” and “LocalGroups” Collection Profiles and write the SYSLOG output to a log file. The default log file is named like this: 2023-01-26\_SYSLOG\_Data\_Sent.log
   1. .\PAS-APM-Components-01.ps1 -CollectionProfile LocalHostInfo,LocalGroups -WriteLog

## Schedule Performance

This uses the Windows Task Scheduler.

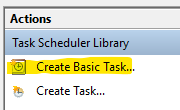
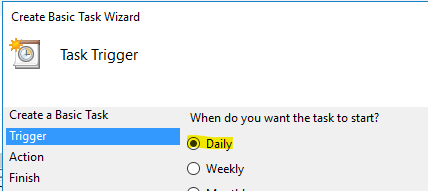
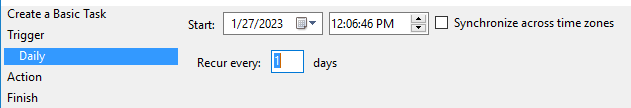
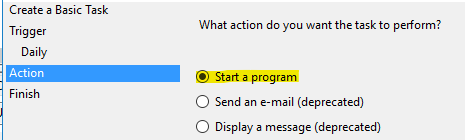
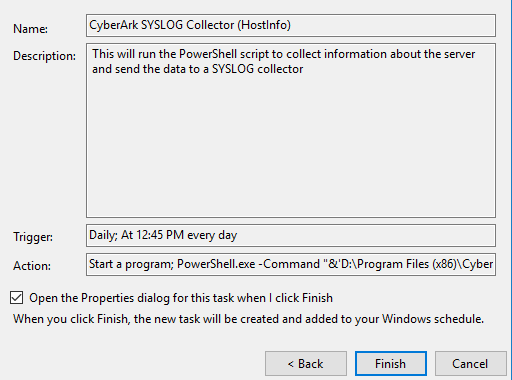
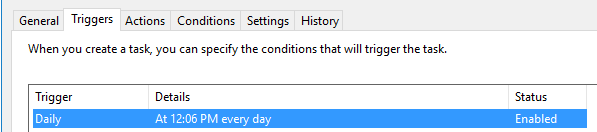
Steps:

1. Click on “Create Basic Task”  
   
2. Click on “Name” and enter: CyberArk SYSLOG Collector (Performance)  
   
3. Click on “Description” and enter: This will run the PowerShell script to collect information about the CyberArk component(s) installed on the server and send the data to a SYSLOG collector.  
   
4. Click on “Next”  
   
5. Choose “Daily”  
   
6. Click on “Next”  
   
7. Leave the default settings.  
   
8. Click on “Next”  
   
9. For Action, click on “Start a program”  
   
10. Click on “Next”  
    
11. For Program/script enter in: PowerShell.exe   
    
12. For Add arguments: -Command “&’full path\PAS-APM-Components-01.ps1’ -CollectionProfile PVWA,CPM,PSM,CCP”  
    
    1. Specify the component data to retrieve.
13. For Start in: The full path to the PowerShell script.  
    
    1. Notice there is no Quotes “ or trailing slash /
14. Click on “Next”  
    
15. Check the box “Open the Properties dialog for this task when I click Finish”  
    
16. Click on “Finish”  
    
17. Click on “Change User or Group”  
    
18. In “Enter the object name to select” enter: System  
    
19. Click on “Check Names”  
    
20. The name should change.  
    
21. Click on “Ok”  
    
22. Check “Run with highest privileges”  
    
23. Click on “Triggers”, then click on the listed trigger.  
    
24. Click on “Edit”  
    
25. Check “Repeat task every”.  
    
26. Set the interval to 1 minutes  
    
27. Check “Stop task if it runs longer than”  
    
28. Set the interval to 5 minutes  
    
29. Click on “Ok”  
    
30. Click on “Ok”  
    
31. The task is now ready.  
    

## Schedule Host Information

This uses the Windows Task Scheduler.

Steps:

1. Click on “Create Basic Task”  
   
2. Click on “Name” and enter: CyberArk SYSLOG Collector (HostInfo)  
   
3. Click on “Description” and enter: This will run the PowerShell script to collect information about the server and send the data to a SYSLOG collector.  
   
4. Click on “Next”  
   
5. Choose “Daily”  
   
6. Click on “Next”  
   
7. Leave the default settings.  
   
8. Click on “Next”  
   
9. For Action, click on “Start a program”  
   
10. Click on “Next”  
    
11. For Program/script enter in: PowerShell.exe   
    
12. For Add arguments: -Command “&’full path\PAS-APM-Components-01.ps1’ -CollectionProfile LocalHostInfo,LocalHostNetwork,LocalHostDrives,LocalHostFirewall,LocalUsers,LocalGroups,LocalSoftwareFilter”  
    
13. For Start in: The full path to the PowerShell script.  
    
    1. Notice there is no Quotes “ or trailing slash /
14. Click on “Next”  
    
15. Check the box “Open the Properties dialog for this task when I click Finish”  
    
16. Click on “Finish”  
    
17. Click on “Change User or Group”  
    
18. In “Enter the object name to select” enter: System  
    
19. Click on “Check Names”  
    
20. The name should change.  
    
21. Click on “Ok”  
    
22. Check “Run with highest privileges”  
    
23. Click on “Triggers”, then click on the listed trigger.  
    
24. Click on “Edit”  
    
25. Check “Repeat task every”.  
    
26. Set the interval to 1 minutes  
    
27. Check “Stop task if it runs longer than”  
    
28. Set the interval to 5 minutes  
    
29. Click on “Ok”  
    
30. Click on “Ok”  
    
31. The task is now ready.  
    

SIEM Field Name Update

This section will describe field names. Each SIEM is different so the steps will be different.

Extract new fields and use Pipe “|” as the separator.

1. Format
2. Vendor
3. Product
4. Version
5. Info1
6. Info2
7. Info3
8. Info4
9. Info5
10. Info6
11. Info7
12. Info8
13. Info9
14. Info10
15. Info11
16. Info12
17. Info13
18. Info14
19. Info15
20. Info16
21. Info17
22. Info18
23. Info19
24. Info20

These field names are used by the dashboards.