

Script Horizon Forensics Doc

How Forensics works :

<https://docs.vmware.com/en/VMware-Horizon/2309/virtual-desktops/GUID-9B386F81-AA24-43EA-919C-A0C391AC8499.html>

Forensic is enabled per user (or users groups).

When enabled for a given user, the ICs for this user are not refreshed or deleted, and they can therefore be accessed for troubleshooting or archiving

This script runs the REST API queries to manage the Forensic feature – as described in the Horizon documentation.

The script format makes it customizable.

How to proceed

The first step is to create a **Forensic Admin role** (needs to be done once)

Only an administrator with this role can enable / disable forensics for a user

The powershell script allows to check if this role was already created. And proceed with the role creation if not.

The script then allows to set / unset / list forensics for Horizon users

Prerequisites :

set-ExecutionPolicy -executionPolicy Unrestricted

```
PS C:\Windows\system32> set-ExecutionPolicy -executionPolicy Unrestricted
```

```
PS C:\Windows\system32> |
```

Guide

Run script (no parameter for interactive mode)

```
PS C:\Windows\system32> C:\tmp\jpl\Horizon-Rest-HoldIC-v1.1.ps1  
cmdlet Horizon-Rest-HoldIC-v1.1.ps1 at command pipeline position 1  
Supply values for the following parameters:  
(Type !? for Help.)  
ConnectionServerURL: |
```

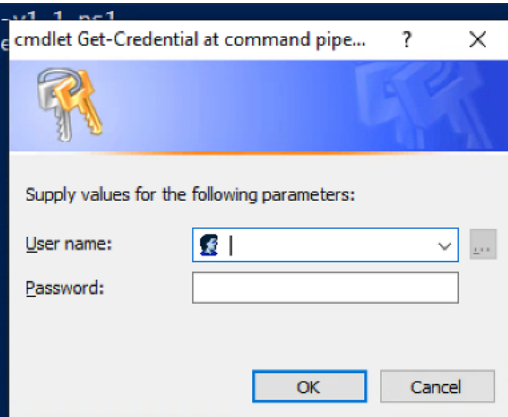
Input the connection server URL : `https://<HorizonServerURL>`
(ex: `https://myHorizonServer.net`)

```
PS C:\Windows\system32> C:\tmp\jpl\Horizon-Rest-HoldIC-v1.1.ps1  
cmdlet Horizon-Rest-HoldIC-v1.1.ps1 at command pipeline position 1  
Supply values for the following parameters:  
(Type !? for Help.)  
ConnectionServerURL: https://[REDACTED].local|
```

Prompt for user / login

This user will execute the REST API on the server

```
PS C:\Windows\system32> C:\tmp\jpl\Horizon-Rest-HoldIC-v1.1.ps1  
cmdlet Horizon-Rest-HoldIC-v1.1.ps1 at command pipeline position 1  
Supply values for the following parameters:  
(Type !? for Help.)  
ConnectionServerURL: https://[REDACTED].local  
cmdlet Get-Credential at command pipeline position 1  
Supply values for the following parameters:
```



The input format is : `<domain>\<user>`

You should get this menu.

```
A - Check Forensics Privileges
B - Set Forensic Privileges
C - List Users on hold
D - Put User on Hold
E - Release User from Hold

X - Exit

Type your choice and press Enter: |
```

A/B items are to check Forensic privileges - and should be run the first time only.

A : to check if a role with the Forensics Privileges exists

Only users with a role with this privilege can perform forensics operations

```
A - Check Forensics Privileges
B - Set Forensic Privileges
C - List Users on hold
D - Put User on Hold
E - Release User from Hold

X - Exit

Type your choice and press Enter: A

Checking Forensic Role ...
GroupID = 938dc845-a247-3def-99c0-638e3b19302a
Name = Forensic Admin
Privileges = MACHINE_MANAGEMENT;MACHINE_MAINTENANCE;GLOBAL_ADMIN_UI_INTERACTIVE;MACHINE_REBOOT;MACHINE_VIEW;POOL_VIEW;FORENSICS;UDD_VIEW;CVP_VIEW;MACHINE_
MANAGE_OFFLINE_SESSION;GLOBAL_ADMIN_SDK_INTERACTIVE;REMOTE_ASSISTANCE;MACHINE_MANAGE_VDI_SESSION;MANAGE_REMOTE_PROCESS;MACHINE_USER_MANAGEMENT
type a key:
```

The script returns the role name and ID that has the Forensic privilege and details all the privileges

If no role is returned - go to B to create a role

In Horizon Console, check the permissions on the role that was return for the user(s) assigned to forensic operations

Global Administrators View

[Administrators and Groups](#) [Role Privileges](#) [Role Permissions](#) [Access Groups](#)

Add

Remove

☐

Horizon admins

☐

Administrator

☐

Role

Access Groups

☐

Administrators

Root(/)

☒

Forensic Admin

Root(/)

Here the AD 'Horizon Admins' group is allowed for forensic admins.

The user logged in with the script should be granted with the 'Forensic Admin' role

B- Role Creation

A role 'Forensic Admin' is created with Forensic privilege enabled

C-D-E- List / Add / Remove Users or group of users

For the users listed, their IC should not be refreshed / deleted after a session.

First specify a user or group. It is possible to select several users.

Ex:

name starting 'jplep' - 2 users listed - reselect only the first one

```
A - Check Forensics Privileges
B - Set Forensic Privileges
C - List Users on hold
D - Put User on Hold
E - Release User from Hold

X - Exit

Type your choice and press Enter: D

Putting User on Hold ...
Enter the first letters of a name (group or user):
jplep
Putting these users/groups on hold ?
1 : Jean-Philippe LEPAGE
2 : Jean-Philippe LEPAGE-USR
Confirm - enter index or A (All) - other key to quit: 1
Holding User Jean-Philippe LEPAGE
Server Response = 200
Server Error =
type a key: |
```

Check the users enabled for forensics (D)

```
A - Check Forensics Privileges
B - Set Forensic Privileges
C - List Users on hold
D - Put User on Hold
E - Release User from Hold

X - Exit

Type your choice and press Enter: C

List Users on hold...
Jean-Philippe LEPAGE
type a key: |
```

Remove the user of forensic - E

```
A - Check Forensics Privileges
B - Set Forensic Privileges
C - List Users on hold
D - Put User on Hold
E - Release User from Hold

X - Exit


Type your choice and press Enter: E

Release User on Hold ...
1 : Jean-Philippe LEPAGE
Enter number or A for All - other key to escape: 1
Releasing Clones for user/group : Jean-Philippe LEPAGE
Server Response = 200
Server Error =
type a key: |
```

Follow up on Horizon admin console

Example with a IC pool (non persistent)

No connection

<input type="checkbox"/>	Machine	Agent Version	Connected User	Assigned User	Machine Alias	Host	Datastore	Task	Status
<input type="checkbox"/>	 DEM-AV10	8.10.0-22012512		N/A	N/A	10.1.0.12	vsanDatastore	None	Available
<input type="checkbox"/>	 DEM-AV09	8.10.0-22012512		N/A	N/A	10.1.0.12	vsanDatastore	None	Available

connected - assigned user = N/A

User (listed in Forensics) is connected

<input type="checkbox"/>	Machine	Agent Version	Connected User	Assigned User	Machine Alias	Host	Datastore	Task	Status
<input type="checkbox"/>	 DEM-AV10	8.10.0-22012512		N/A	N/A	10.1.0.12	vsanDatastore	None	Available
<input type="checkbox"/>	 DEM-AV09	8.10.0-22012512	euc.local\jplepage	euc.local\jplepage	N/A	10.1.0.12	vsanDatastore	None	Connected

connected - assigned user = jplepage

User (listed in Forensics) logs out

<input type="checkbox"/>	Machine	Agent Version	Connected User	Assigned User	Machine Alias	Host	Datastore	Task	Status
<input type="checkbox"/>	 DEM-AV10	8.10.0-22012512		N/A	N/A	10.1.0.12	vsanDatastore	None	Available
<input type="checkbox"/>	 DEM-AV09	8.10.0-22012512		euc.local\jplepage	N/A	10.1.0.12	vsanDatastore	None	Available

Connected user = N/A - assigned user = jplepage

If removing the VM transits to maintenance to be refreshed

Note that it is also possible to follow the VM in Forensic mode in vCenter (a tag is assigned to the VM)