Manual Recovery from Blue Screen on Windows Instances in GCP

Solution:

- Sensors - Windows OS Platforms
- Cloud Security Modules (CSPM & CWP)

Published Date: Jul 19, 2024

Objective

- Recover Windows instances from a blue screen state in Google Cloud Platform (GCP)
- Create snapshots, attach volumes to a new instance, modifying files, and restore the original instance

Applies To

- Tech Alert | Windows crashes related to Falcon Sensor | 2024-07-19
- Prerequisites:
    - **GCP Account:** Ensure you have administrative access to your GCP account.
    - **gcloud CLI:** Install and configure the gcloud command-line tool. Install gcloud CLI
    - **BitLocker Recovery Key:** Ensure you have access to BitLocker recovery keys if BitLocker is enabled

Procedure

1. Create a snapshot of the persistent disk of the affected Instance to ensure you have a backup

- Identify the disk

a.

```
BSOD_INSTANCE_NAME=affected_instance
BSOD_INSTANCE_ZONE=your instance zone
```

b.

```
BSOD_INSTANCE_DISK_NAME=$(gcloud compute instances describe
$BSOD_INSTANCE_NAME --zone=$BSOD_INSTANCE_ZONE
--format="get(disks[0].source.basename())")
```

c.

```
BSOD_INSTANCE_DEVICE_NAME=$(gcloud compute instances describe
$BSOD_INSTANCE_NAME --zone=$BSOD_INSTANCE_ZONE
--format="get(disks[0].deviceName)")
```

d.

```
BSOD_INSTANCE_PRE_RECOVERY_SNAPSHOT_NAME="$BSOD_INSTANCE_NAME-snapshot-$
(date +%Y%m%d%H%M%S)"
```

e.

```
gcloud compute snapshots create --source-disk-zone=$BSOD_INSTANCE_ZONE
--source-disk=$BSOD_INSTANCE_DISK_NAME --snapshot-type=STANDARD
$BSOD_INSTANCE_PRE_RECOVERY_SNAPSHOT_NAME
```

2. Create a New Persistent Disk from the Snapshot in the Same Zone

- Create New Disk:

a.

```
NEW_DISK_NAME="$BSOD_INSTANCE_DISK_NAME-recovery"
```

b.

```
gcloud compute disks create $NEW_DISK_NAME
--source-snapshot=$BSOD_INSTANCE_PRE_RECOVERY_SNAPSHOT_NAME
--zone=$BSOD_INSTANCE_ZONE --type=[disk-type, e.g. "pd-ssd"]
```

3. Launch a New Instance in That Zone Using a Different Version of Windows

- **Launch New Instance:**
  The new instance should be located in the same zone of the VM to recover.

a.

```
RECOVERY_INSTANCE_NAME="recovery-instance"
```

b.

```
RECOVERY_INSTANCE_ZONE=$BSOD_INSTANCE_ZONE
```

c.

```
RECOVERY_INSTANCE_IMAGE="your-instance-image"
```

d.

```
RECOVERY_INSTANCE_IMAGE_FAMILY="windows-2022"
```

e.

```
RECOVERY_INSTANCE_IMAGE_PROJECT="windows-cloud"
```

f.

```
RECOVERY_INSTANCE_MACHINE_TYPE="your-instance-machine-type"
```

g.

```
gcloud compute instances create RECOVERY_INSTANCE_NAME \
    --zone=RECOVERY_INSTANCE_ZONE \
    [--image=RECOVERY_INSTANCE_IMAGE |
--image-family=RECOVERY_INSTANCE_IMAGE_FAMILY] \
    --image-project=RECOVERY_INSTANCE_IMAGE_PROJECT \
    --machine-type=RECOVERY_INSTANCE_MACHINE_TYPE
```

- Find a detailed guide at [Create and manage Windows Server VMs | Compute Engine Documentation | Google Cloud]

4. Attach the Persistent Disk from Step 2 to the New Instance as a Data Volume

- Attach Disk:

a.

```
gcloud compute instances attach-disk $RECOVERY_INSTANCE_NAME
--disk=$NEW_DISK_NAME --zone=$BSOD_INSTANCE_ZONE --mode=rw
```

5. Connect to the Recovery Instance

- **(Optional) If Bitlocker encrypted drive:** make sure the recovery machine has bitlocker installed:

a.

```
Install-WindowsFeature -Name BitLocker -IncludeAllSubFeature
-IncludeManagementTools -Restart
```

6. Delete the Problematic File

- Run the following PowerShell Script as Administrator:

```
$diskNumber = 1

$disk = Get-Disk -Number $diskNumber

if ($disk.OperationalStatus -eq 'Offline') {
    Set-Disk -Number $diskNumber -IsOffline $false
    Set-Disk -Number $diskNumber -IsReadOnly $false
    Write-Host "Disk $diskNumber is now online."
} else {
    Write-Host "Disk $diskNumber is already online."
}

$partition = Get-Partition -DiskNumber $diskNumber | Where-Object {
$_.Type -eq 'Basic' }

if ($partition) {
    Write-Host "Drive letter D has been assigned to the partition on
disk $diskNumber."

    $filePath =
"D:\Windows\System32\drivers\CrowdStrike\C-00000291*.sys"
    $files = Get-ChildItem -Path $filePath -ErrorAction SilentlyContinue

    if ($files -eq $null) {
Write-Output "Failed to recover: the target files don't exist at the
path"
    }

    foreach ($file in $files) {
        try {
            Remove-Item -Path $file.FullName -Force
```

```
            Write-Output "Deleted: $($file.FullName)"
        } catch {
            Write-Output "Failed to delete: $($file.FullName)"
        }
    }

} else {
    Write-Host "No suitable partition found on disk $diskNumber."
}
```

- In the case your drive is locked with Bitlocker, you'll need to rerun the script after unlocking the mounted drive with the Bitlocker recovery key.

7. Detach the Persistent Disk from the New Instance

a. Detach Disk:

i.

```
gcloud compute instances detach-disk $RECOVERY_INSTANCE_NAME
--disk=$NEW_DISK_NAME --zone=$BSOD_INSTANCE_ZONE
```

ii.

```
gcloud compute instances stop $BSOD_INSTANCE_NAME
--zone=$BSOD_INSTANCE_ZONE
```

iii.

```
gcloud compute instances detach-disk $BSOD_INSTANCE_NAME
--disk=$BSOD_INSTANCE_DISK_NAME --zone=$BSOD_INSTANCE_ZONE
```

b. Attach to new disk to BSOD affected instance

i.

```
gcloud compute instances attach-disk $BSOD_INSTANCE_NAME
--disk=$NEW_DISK_NAME --zone=$BSOD_INSTANCE_ZONE --boot
--device-name=$BSOD_INSTANCE_DEVICE_NAME
```

c. Start the Instance:

i.

```
gcloud compute instances start $BSOD_INSTANCE_NAME
--zone=$BSOD_INSTANCE_ZONE
```

Additional Information

- **Monitoring and Validation:** Ensure the instances boot successfully into normal mode and the blue screen issue is resolved.
- **Backup:** Regularly create snapshots of your instance disks to avoid data loss.

Next Steps

- Automation being developed to allow deployment of the above workaround at scale.

See also

- Tech Alert | Windows crashes related to Falcon Sensor | 2024-07-19