A white text on a black background

AI-generated content may be incorrect.

**C&W MANAGED AZURE FAILOVER AND FAILBACK**

**ATTESTATION REPORT**

**Rubis Eastern Caribbean SRL**

**Date of report: September 3rd 2025**

&W MANAGED AZURE FAILOVER AND FAILBACK ATTESTATION

A person and person looking at a tablet

AI-generated content may be incorrect.

**Disclaimer**

© Copyright Liberty Business 2025. All rights reserved.

The information contained in this document is the property of Liberty Caribbean and its affiliates and subsidiary companies forming part of the Cable & Wireless Communications LLC group of companies (individually or collectively). No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means; electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Cable & Wireless. Legal action will be taken against any infringement.

**Submitted to**

**Valdez Lewis – IT Manager &**

**Anthony Harris – Business Infrastructure Administrator**

**Addres: One Rubis Plaza, Welches, St Thomas, Barbados**

**Phone: 1-246-231-8291 – Valdez Lewis**

**1-246-233-1172 – Anthony Harris**

## SUMMARY

1. Azure Site Recovery is procured by Rubis through C&W Business to replicate the VMs from Azure EastUS to Azure WestUS.
2. The failover was tested on August 22nd, 2025, between 12:00 PM and 4:00 PM August 23rd, 2025.

Below are the general steps followed through the window:

1. All VMs were configured with Site Recovery to replicate from EastUS to WestUS.
2. Before the failover, the Rubis Finance team checked the current state of the ERP application.
3. The failover to WestUS was executed twice. During the first attempt, an incorrect configuration on the protected subnet —introduced by the CSD—caused the failover to assigned wrong IP addressing, requiring the deletion of the failed-over VMs. After correcting the configuration, CSD re-protected all VMs and successfully completed the failover in the second attempt.
4. Due to the initial misconfiguration and the subsequent re-deployment made by the CSD, the Rubis Finance team had to adjust some IP addresses in the application. Once those changes were applied, Rubis Finance validated the access and the correct application state. Then, the Finance team generated a new application transaction that was keyed to the database successfully. For future failover activities, the CSD team will ensure the availability of the IP addresses expected by Rubis.
5. The VMs were re-protected to the EastUS site.
6. The failback process to EastUS was performed.
7. The Rubis Finance team verified the failed-back VMs, now operating in EastUS, did not include the transaction/s performed in WestUS for the SQL VM.

## ASR Resources and Settings

# Recovery Services Vaults

# 

# Virtual Machines:

# 

**BGIVMNAVAPP2**

Diagrama

El contenido generado por IA puede ser incorrecto.

**NAVWEBSVR**

Diagrama

El contenido generado por IA puede ser incorrecto.

**BGIVMNAVAPP1restore082424**

Diagrama

El contenido generado por IA puede ser incorrecto.

**BGIVMNAVSQL1**

Diagrama

El contenido generado por IA puede ser incorrecto.

# Networking

Una captura de pantalla de una computadora

El contenido generado por IA puede ser incorrecto.

Una captura de pantalla de una computadora

El contenido generado por IA puede ser incorrecto.

Captura de pantalla de computadora

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

# Replicated Items

# Tabla El contenido generado por IA puede ser incorrecto.

## Steps taken during the failover/failback window

| **Phase** | **Task** | **Responsible** | **Time** | **Start time** |
| --- | --- | --- | --- | --- |
| Before Failover | Check the current state of the application | Rubis Finance team | 10 min | 22/08 12:02 pm |
| Check that the VM is protected and healthy, before you run a failover | Liberty CSD | 10 min | 22/08  12:02 pm |
| Check there is an existing backup for each VM  Applies to all 4 machines  Backup must already be setup | Liberty CSD | 10 min | 22/08  12:10 pm |
| Failover | Start failover with the 'Shut down machine before beginning the failover' option enabled | Liberty CSD | 10 min | 22/08  12:15 pm |
| Commit the failover | Liberty CSD | 10 min | 22/08  12:20 pm |
| **Re-Protect VMs**: A Network Security Group appeared in the window that was not targeting the Protected Subnet. This caused a loss of access when the machines were moved to the West US zone. For this reason, the machines that had already synchronized were deleted and re-synchronized, which caused a delay in the failover window. | Liberty CSD | 7 hours | 22/08  Finish  7:34 pm |
| Rubis Technical team had to adjust some IP addresses in the application, because some of the expected addresses for the VMs were not available (other resources had taken those address from the protected subnet).  It is CSD’s responsibility to agree with Rubis in advance, on the IP addressing mappings and reserve those IPs in the replica settings, so this step be not necessary in future failover executions. | Rubis Technical team / Liberty CSD | 10 min | 23/08  9:20 am |
| Check the state of the application in the alternate location | Rubis Finance team | 10 min | 23/08  9:30 am |
| Create control point. Generate a new transaction in the application | Rubis Finance team | 45 min | 23/08  11:30 am |
| Failback | Re-Protect VMs | Liberty CSD | 3 hours | 23/08  Finish  1:45 pm |
| Start failover with the 'Shut down machine before beginning the failover' option enabled | Liberty CSD | 10 min | 23/08  1:45 pm |
| Commit the failover |  | 10 min | 23/08  1:55 pm |
| After Failback | Check the state of the application in the primary location | Rubis Finance team | 45 min | 24/08  10:45 am |
| Re-protect customer data from EastUS to WestUS | Liberty CSD | 10 hours | 24/08  Finish  5:54 am |
| Clean up resources | Liberty CSD | 10 min | 24/08  7:34 am |

**Note:** The above-described activity ‘**Re-Protect VMs**’, during the failover phase, was not a normal or required step at that moment of the window. This was an additional step the CSD had to apply in order to correct a replica setting misconfiguration regarding the networking assignment for the new VMs at the target location.

This misconfiguration setting (done by the CSD previous to the window) was noted by  the CSD team after the activity had begun and the failover to West was committed, so it was necessary to start a new **Protect** run, this time with the correct networking settings. This effort in correcting the window course took around 7 hours.

## Microsoft investigation and conclusions of the failover/failback event

## After the failback activity from WestUS to EastUS was finished, the Rubis Finance team reported their latest application update committed in the WestUS was not replicated back to EastUS.

This prompted the CSD team to raise a support case with Microsoft - Ticket 2508250040012693, with the following comments after the Microsoft ASR specialist’s revision:

**Network Traffic Analysis During Replication**

1. Microsoft identified elevated data traffic during the window, particularly on the disks of VM BGIVMNAVSQL1, which approached the ASR bandwidth limit of 100 Mbps per VM.
2. This high traffic was generated during the four virtual machines re-protection. This process involves a full re-upload of data, equivalent to restarting replication from scratch.

A screenshot of a computer

AI-generated content may be incorrect.

[Azure Virtual Machines disaster recovery - High Churn support - Azure Site Recovery | Microsoft Learn](https://learn.microsoft.com/en-us/azure/site-recovery/concepts-azure-to-azure-high-churn-support#data-change-limits)

1. Although the traffic was high, Microsoft did not find conclusive evidence that bandwidth exhaustion directly caused replication failures. However, they acknowledged that such traffic levels are typical during re-protection and should be monitored closely.

Bandwidth Constraints:

Microsoft confirmed that the 100 Mbps per VM bandwidth limit is a predefined constraint across all Azure regions and cannot be increased under the current ASR available settings.

Current Status:

So far, network traffic has remained stable and healthy, indicating no immediate concerns. However, it is still recommended to monitor closely during re-protection and replication processes.

**Recovery Point Lifecycle Analysis - Failback**

Once the customer RUBIS finished the application update (new ERP transaction) in West US:

1. The re-protect process was triggered and took approximately 3 hours to complete.
2. Once re-protect finished, snapshots began to be taken every 5 minutes and stored in the **cache storage account**. These snapshots are not immediately usable as recovery points until they are processed and moved to the Vault.
3. The failback to East US was initiated just 15 minutes after re-protect completion. At that time, the only available recovery point was **Latest Processed**, which prioritizes low RTO but may not include the most recent data changes (higher RPO).
4. As a result, the recovery point used during failback **did not contain the latest application updates**, which most probably were still in the cache and not yet processed into the Vault.
5. After failback, a new re-protect was triggered in East US. This process initially failed a couple times due to incorrect VM states but eventually succeeded after VM state remediation.
6. The replication resumed and took approximately 3 hours to complete, after which snapshots began again and were processed into the Vault (current state).

**Final conclusions from Microsoft Support**

Case Summary:

Customer (Liberty CSD) started failover action, it completed. After committing and re-protecting, the failback procedure was initiated. When selecting the Recovery Point customer found only the option shown below:



The failback to the original region was completed; however, the new data taken by the customer while working in West was not present.

Site Recovery Job explanation:

1. Fail over initiated from East to West region. Completed
2. Commit in Target West region was done.
3. Customer triggered re-protect.
4. Re protect finish – took near 4.5 hours. It is at this moment when the snapshots start to be taken every 5 minutes (this is the **cache storage account**). A backend stage will process and send the data to Vault, to finally be available as recovery point. Snapshots/Data in the cache storage account are not considered during the failover recovery point selection, just the ones in the Vault.
5. Failover (failback) was initiated from West to East, just 15 minutes after reprotection got completed. Microsoft’s presumption here is that no RP was in the Vault yet, it was in the cache storage account and still not processed.
6. Commit in East region was done.
7. Now back in the East region, the customer triggered a new re-protect, that failed a couple times due to the VM was not in the correct state. A proper synchronization started after CSD took some action to solve the issue (by means of detach/re-attach actions on the VM network card).
8. Re-protect was finally completed in East and replication is back in place, taking around 3 hours. From this moment, snapshots started to be taken and processed to the Vault.

Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.

Conclusions:

* While Microsoft confirmed that the ASR platform executed the failover and failback operations as designed, the timing of operational steps—specifically the short interval between re-protect completion and failback initiation—resulted in the use of a recovery point that did not include the latest data.

An additional step during the window to wait for snapshots to be processed as valid Recovery Points in the Vault is required.

* Even though there were traffic peaks during the VMs replication during the re-protect stages, this is not the cause of the issue of not having the latest Recovery Points available in the Vault.
* The max amount of allocated bandwidth per VM for high churn, which is 100Mbps, cannot be increased. But strategies as upgrading the level of disks throughput, or splitting the high volumes disks into smaller ones on the VM, have beneficial effects in the whole replication process.

Recommendations:

* Perform a new test and allow some time after the re-protect is finished. Before initiating failback, allow sufficient time for recovery points to be processed and moved to the Vault.
* **Platform Optimization.** For critical workloads, such as databases, Microsoft recommends using disks with higher levels of Provisioned IOPS and throughput to increase replication performance. The SQL VM is currently configured with P30 tier disk, and Microsoft has recommended reconfiguring them to P40 improving the throughput to 250 Mbps Base Provisioned Throughput per disk.

[Select a disk type for Azure IaaS VMs - managed disks - Azure Virtual Machines | Microsoft Learn](https://learn.microsoft.com/en-us/azure/virtual-machines/disks-types#premium-ssd-size)

## Improvement actions for future executions

* To achieve a next successful failover/failback execution, a Microsoft Support agent will be included in the call to follow up and provide their insights on the whole recovery process. This support will be available 24/7 when the customer decides to execute the failover/failback window.

However, if the customer decides to execute the failover window during business hours, the specialist in charge of the raised ticket 2508250040012693, who already knows the customer specific situation, will be the one assigned. The Microsoft Support ticket will remain open until the successful execution of the customer activity.

* To further strengthen visibility and responsiveness during the next failover windows, CSD reassures its commitment in enhancing the activity tracking (precise timestamps, evidence, follow up) and real-time monitoring of each step, so a successful Disaster Recovery execution be guaranteed.

## Next failover execution planning

For the next window, two additional phases were added to ensure actions and recommendations are updated fully which includes Microsoft Support direct assistance during the window execution.

| **Phase** | **Task** | **Responsible** | **Date** | **Time** |
| --- | --- | --- | --- | --- |
| Platform optimization (database server) | Schedule a maintenance window to perform the database server disks type upgrade | Liberty CSD - Rubis | To be agreed | NA |
| Execute the disks update: Install Azure CLI, detach the data disk from the database server, change its performance tier and attach the data disk back to the VM. This activity must be executed in both regions (East-West).  For each disk, the upgrade implies additional charges of $125 a month. Three disks in total. | Liberty CSD - Rubis | To be agreed | 1 hour |
| Set the monitoring strategy for ASR | Liberty CSD | 29/08/2025 | 1 hour |
| Failover-Failback window preparation | Coordinate with the customer a new failover/failback window for the ERP application | Liberty CSD - Rubis | To be agreed | 2 hours |
| Schedule the Microsoft ASR specialist to the failover windows | Liberty CSD | To be agreed | 2 hours |
| Before Failover | Check the current state of the application | Rubis Finance team | To be agreed | 10 min |
| Ensure VMs Backup | Liberty CSD | To be agreed | 10 min |
| Failover | Start failover with the 'Shut down machine before beginning the failover' option enabled | Liberty CSD | To be agreed | 10 min |
| Commit the failover | Liberty CSD | To be agreed | 10 min |
| Re-Protect VMs | Liberty CSD | To be agreed | 4 hours |
| Check IP addresses assigned  (CSD must ensure the agreed IPs with Rubis are reserved) | Rubis Technical team / Liberty CSD | To be agreed | 10 min |
| Check the state of the application in the alternate location | Rubis Finance team | To be agreed | 10 min |
| Create control point. Generate a new transaction in the application | Rubis Finance team | To be agreed | 45 min |
|  | Wait for appropriate Recovery Point (low RPO) to be available in the Vault. | Liberty CSD | To be agreed | 30 min |
| Failback | Start failover with the 'Shut down machine before beginning the failover' option enabled | Liberty CSD | To be agreed | 10 min |
| Commit the failover | Liberty CSD | To be agreed | 10 min |
| Re-Protect VMs | Liberty CSD | To be agreed | 6 hours |
| Wait for the snapshots in the cache storage account to be processed to the Vault as valid Recovery Points. | Liberty CSD | To be agreed | 1 hour |
| After Failback | Check the state of the application in the primary location | Rubis Finance team | To be agreed | 45 min |
| Clean up resources | Liberty CSD | To be agreed | 10 min |
| Re-synchorize customer data from EastUS to WestUS | Liberty CSD | To be agreed | 4 hours |

During the Failover, when the VMs start operating in the WestUS region, the following IP address will be assigned mirroring the original assignment in EastUS:

|  |  |  |  |
| --- | --- | --- | --- |
| **NAME** | **LOCATION** | **IP ADDRESS EAST** | **IP ADDRESS WEST** |
| BGIVMNAVAPP1restore082424 | East US | 10.100.2.10 | 172.16.2.10 |
| BGIVMNAVAPP2 | East US | 10.100.2.7 | 172.16.2.7 |
| BGIVMNAVSQL1 | East US | 10.100.2.4 | 172.16.2.4 |
| NAVWEBSVR | East US | 10.100.2.8 | 172.16.2.8 |