Falkenberg 2025-10-28

INCIDENT REPORT REGARDING VMWARE PARTIAL OUTAGE IN FALKENBERG

Glesys has prepared the following Reason for Outage (RFO). This report summarizes the background, timeline, and conclusions for the partial outage in Falkenberg on 11 September 2025.

Glesys AB
Box 134, 311 22 Falkenberg
Sweden

Phone. +46 (0) 346 738800
Mail: info@glesys.se
Web https://glesys.com

Org.nr. 556647-9241
VAT No. SE556647924101
BIC NDEASESS
IBAN 300000003052170377

Background
In the early hours of 11 September, a small number of virtual machines (VMs) in our VMware environment became unavailable.

The issue was linked to a routine maintenance task performed the evening before, where old snapshot data was removed following standard procedures.

Due to an unexpected behavior in the vendor's storage software, parts of that cleanup affected data that was still in use, but nothing happened immediately since those files were locked. When the system later released those files during normal operations, a few VMs lost access to their disks.

All affected VMs were restored from the latest available backups, except one which did not have backup enabled.

The environment has remained stable since.

Sequence of events (CEST)

2025-09-10	
20:08	Routine maintenance: cleanup of old snapshot data.
2025-09-11	
04:03	First alert from a monitored VM: investigation began.
04:53	Recovery started from backups while continuing investigation.
06:10	Priority support case opened with vendor.
06:17	Incident published on Glesys status page.
06:32	Live troubleshooting session held with vendor.
09:20	Troubleshooting session ended. During the call we confirmed no additional VMs were at risk, and our vendor received environment-wide logs for further analysis.
13:16	Last affected VM confirmed operational: status page set to Monitoring
15:19	Status page set to Resolved.

Immediate actions

- Restored all VMs with backup enabled from the latest available restore point.
- Engaged vendor support to verify the environment and confirm no further impact.
- Updated internal procedures and added safeguards to prevent similar issues during maintenance.

Findings

Our investigation, together with the vendor's analysis, confirmed that the incident was caused by the storage software's current design, which in certain situations where manual tasks are included can remove active data links when old snapshot folders are deleted.

The maintenance itself followed standard practice and was performed correctly.

When the system later released file locks during normal overnight operations, the affected disks were removed by the software, resulting in loss of access for a small number of VMs.

Vendor status

The vendor has acknowledged that this behavior is functioning as designed but can lead to unintended consequences in maintenance scenarios where manual tasks are included.

They have provided updated procedures for safely performing this type of cleanup, which we have implemented internally.

In parallel, the vendor will continue to work on our request to develop product-level safeguards to prevent similar issues from occurring in the future – both for us and for other customers using their products.

Sincerely,
Stefan de Vries
Glesys