RFO: Network and VMware incident in Falkenberg

2025-11-29

This document shares the details of the incident that took place in Falkenberg over the weekend of November 29th, 2025. We aim to provide a clear and transparent record of what happened, including the root cause, the steps we took to address it, and the improvements we are working on as a result.

Summary

An incorrectly configured customer interface accepted a large volume of traffic, resulting in resource exhaustion on our VMware platform in Falkenberg.

Timeline

Saturday, November 29th, CET:

- 12:25: First alerts received.
- 12:34: Root cause was mitigated.
- 13:01: Network team confirmed the root cause on the customer interface.
- 13:16: Incident status changed to monitoring.
- 13:17: Confirmation that there was a loop that started around 12:25.
- 18:14: Incident status changed to resolved.

Root cause

A misconfigured customer trunk caused a Layer-2 loop across VLANs that are also connected to our VMware platform in Falkenberg. This caused continuous BUM traffic to circulate, leading to MAC instability and EVPN duplicate-host events in the VMware-related VNIs.

The flooded traffic also entered the VMware environment, consuming a significant amount of the hosts' resources. As a result, several workloads on those hosts saw degraded performance and intermittent issues until the loop was isolated, and resource utilization stabilized.

Corrective actions

Following this incident, we have initiated a broader internal improvement program involving the network, virtualization/platform, and monitoring/operations teams. The goal is to enhance both preventive controls and resilience in environments where customer and platform networking meet.

Near-term measures aim to reduce the effects of abnormal traffic, including storm control and loop containment mechanisms, and tightening validation of customer trunk configurations.

Long-term, we are developing a network architecture that places customer networks into individual Layer-3 domains and further minimizes shared failure points through platform VNIs.

We apologize for any inconvenience caused by this disruption. If you have any questions or comments about this incident, please feel free to contact us at support@glesys.com.

Sincerely,

Christoffer Andersson
CTO, Glesys