Disaster Recovery Test Scenarios for CampusWatch

By Diya Neupane

CampusWatch utilizes many edge devices like Cameras and Sensors across the campus for monitoring. These devices are managed and configured using a backend. Disaster recovery testing ensures that if something goes wrong, the system can recover efficiently and without loss of data.

Some of the disasters that might be encountered by the CampusWatch system are:

- **Connection loss**
  Sometimes the connectivity between the edge devices and the backend might be lost due to various reasons such as disruption in physical connection mediums like cables or loss in internet connections(if required).
  This results in loss in communication between the devices and backend i.e data signals and commands cannot be exchanged which leaves the system highly vulnerable. This disaster has high likelihood of occurring.
  Therefore, the system should be thoroughly checked for the weak points in connections and effective techniques should be applied to take correct action as disaster in case the connection is lost.

- **Database failure**
  The database that stores data like video surveillance footage, users info or network settings might be unavailable temporarily.
  This causes the devices to lose their configuration settings , makes the system unavailable for endusers and data cannot be fetched or updated. While database failures are not as likely to occur, they can affect several services of the system. Therefore, effective mechanisms like backup, state preservation and graceful fallback methodsds (eg: read only mode) should be predefined to detect database failures and take necessary actions to prevent system from further crashing.

- **Primary Region Outrage**

  Primary region outrage occurs when the entire cloud region where backend services are located becomes inaccessible due to a catastrophic network or power outage.
  This leaves the entire system paralysed since this region supports all core backend activities, including device provisioning APIs and configuration update services.While the likelihood of a regional outage is not high, the impact is extreme.
  Therefore, an alternative cloud region needs to be predefined as a recovery technique where the system can run in case of this failure.

- **Cyber Attacks**

  An attacker with malicious intent might try to exploit the cloud, web or external devices in order to gain access to the system or damage it.
  The system is wide and has various endpoints that can be exploited, where each exploit can cause a separate kind of impact. Devices and IoT-level attacks like Firmware tampering may cause the device to be unavailable which results in loss of surveillance, while Network attacks, like man-in-the-middle or DDoS, might result in data privacy issues and system outages.
  This disaster has a medium likelihood of occurrence, while its impact can be catastrophic. Therefore, the system should be able to detect when these attacks occur, tests need to be performed to find any entry points for the attacker and a response team should always be ready.

- **Configuration Data Corruption**

  Configuration data corruption occurs when the configuration data being transferred within the system becomes damaged or altered during transmission. This can happen due to network problems, storage failures or software bugs while saving or retrieving configuration files.

When such corruption occurs, some devices may receive partial or corrupted configurations that make them fail or stop working altogether. This disrupts normal campus monitoring operations and introduces security blind spots. The likelihood of this issue is assessed as medium because data corruption can occasionally occur in complex distributed systems.

Therefore, the system must have the capability to validate the configuration files using checksums or hashes before applying them. The system should also versioned backup all of the device configurations and automatically roll back to the last known good version if a validation fails.

- **Natural Disasters**

  Events like earthquakes, flood, landslides, etc., can sometimes damage the data centers or the physical premises of the system like the Campus.

  This causes the system to crash with a catastrophic loss and many aspects or the system as a whole might be unavailable and may have a need to be rebuilt. While the natural disasters are less likely to occur , the impact is extreme . Therefore, backups should always be created to prepare for such situations.