Runbook: Handling Server Down Alerts

Objective:

The purpose of this document is to provide Sysops team with guidelines for accurately differentiating between false positive and valid alerts relating to server downtime events within the TPICAP system. By outlining techniques to identify and properly handle both false alarms and legitimate server outages, this guide will equip sysops to efficiently triage issues and take appropriate response actions. With consistent use of the protocols below, sysops will become proficient in analyzing alerts contextually to determine if legitimate troubleshooting is required or if the event can be disregarded as a false alarm. The ultimate goal is to optimize the alert triage process so that sysops can minimize disruption while still effectively detecting and addressing genuine server downtime incidents.

Audience:

\*Sysops Team

\*Wintel Team

Background:

Wintel Keeps the lights on, Sysops is the first line of defense in figuring out what is a actionable alarm that requires some work cycles from engineers or a situation where Checkmk or appd falsely monitored a server down. Our vision is to leverage sysops as gate keepers in a shared responsibility model where everyone has to be vigilant in ensuring we keep the lights on. The challenge we have is balancing these infinite alerts against our finite resources. As part of the solution