# Introduction

## The use cases document goal is try and understand what is the required information for a root cause analysis (RCA) service to fully understand the origin of typical problems in a multi-layer, both physical and virtual network. This process would be followed by a gap analysis that will find out if this information exist in the network and if there are APIS to reveal it

## The use case table includes a variety of representative problems from both physical and virtual layer. Each failure appear twice, once in a HA environment and once in a non HA environment. High availability environment is an environment that exists in most network deployment in which no link is a single point of failure meaning most failures will not affect service. Non HA environment is an environment in which most if not all failures will affect service and will provide additional information regarding the failure

# Use cases (Non HA deployment) summary

|  |  |  |
| --- | --- | --- |
| **Root Cause ->** | **Symptoms** | **Required API** |
| 1. **Physical Switch down** | * Management port down * Neighbor switches port down * Neighbor hosts port down * VMs connectivity lost * Apps connectivity lost | * Get physical topology – Find out all existing switches in the domain, connectivity, connection to racks, connection to hosts * Get virtual topology * Get mappings: VMs to hosts, Hosts to racks, racks to switch ports, apps to VMs * SNMP Manager – Receive SNMP traps * Get switch status/ event * Get switch port status /event * Get NIC status /event * Get VMs status /Event * Activate link OAM tool |
| 1. **Switch port down** | * Switch port down * Neighbor switch/ host port down * VMs connectivity lost * Apps connectivity lost | * Get physical topology – Find out all existing switches in the domain, connectivity, connection to racks, connection to hosts * Get virtual topology * Get mappings: VMs to hosts, Hosts to racks, racks to switch ports, apps to VMs * SNMP Manager – Receive SNMP traps * Get switch port status /event * Get VMs status /Event * Activate link OAM tool |
| 1. **Host’s Nic Down** | * Switch port down * VMs connectivity lost * Apps connectivity lost | * Get mappings: VMs to hosts, Hosts to racks, racks to switch ports, apps to VMs * SNMP Manager – Receive SNMP traps * Get NIC status /event * Get VMs status /Event * Activate link OAM tool |
| 1. **Damaged host cable (Not disconnected)** | * Lost packets and CRC errors in one port of switch * Lost packets and CRC errors in and NIC of one host * Apps retransmissions may result in app performance degradation | * Get mappings: VMs to hosts, Hosts to racks, racks to switch ports, apps to VMs * Get switch’s port statistics * Get host’s NIC statistics * Get virtual topology * Activate link quality OAM tool – measure quality of link |
| 1. **OVS crash** | * Host connectivity lost * VMs connectivity lost * Apps connectivity lost | * Get mappings: VMs to hosts, apps to VMs * Get virtual topology * Get host process list and status * Get OVS switch status * Activate connection tool |
| 1. **L2 agent crash** | * OVS may be reconfigured * don’t know if effect traffic | * Get host process list and status * Get L2 agent status |
| 1. **OVS port down** | * No communication to a single VM * Apps connectivity lost | * Get mappings: VMs to hosts, apps to VMs * Get OVS/ SDN switch port status * Get OVS port down event |
| 1. **Hypervisor crash** | * No connectivity to VMs * Couldn’t access VMs via VNC proxy | * Get mappings: VMs to hosts, apps to VMs * Get Hypervisor status/ event * Check process up time |
| 1. **Host restarted** | * VMs connectivity lost * Apps connectivity lost | * Get virtual topology – mapping VMs to hosts * Get host restarted event * IPMI – sys up time |
| 1. **vNIC crash** | * No communication to a single VM * Apps on that VM, connectivity lost | * Same as OVS port down * Get vNIC status |
| 1. **MTU misconfigure** | * Host/ VM/ App Degraded communication | * Get mappings: VMs to hosts, Hosts to racks, racks to switch ports, apps to VMs * Get virtual topology * Get actual MTU from all devices * Get expected MTU of all devices |
| 1. **IP address misconfigure** | * No communication to Host/ VM/ App | * Get mappings: VMs to hosts, apps to VMs * Get virtual topology * Get actual IP address all hosts and VMs * Get expected IP address of all hosts and VM |

|  |  |  |
| --- | --- | --- |
|  | **No communication** |  |
|  | **Bandwidth degradation** |  |
|  | **Bandwidth quality degradation** |  |
|  | **QoS misbehavior** |  |
|  | **VM not responding** |  |
|  | **Host not responding** |  |
|  | **Tenant not responding** |  |
|  |  |  |

# Use cases (HA deployment) summary

|  |  |  |
| --- | --- | --- |
| **Root Cause ->** | **Symptoms** | **Required API** |
| 1. **Physical Switch down** | * Management port down (logically) * Neighbor switches port down * Neighbor hosts port down * Damaged service – sometimes – If the service is damaged additional indications may pop | * Get physical topology – Find out all existing switches in the domain, connectivity, connection to racks, connection to hosts * Get mappings: VMs to hosts, Hosts to racks, racks to switch ports, apps to VMs – As this is HA scenario VMs and apps may be not that important * SNMP Manager – Receive SNMP traps * Get switch status/ event * Get switch up time * Get switch port status /event * Get NIC status /event * Get VMs status /Event ??? – through cloud infrastructure, meaning ceilometer * Activate link OAM tool – Perform binary fault detection on the connection |
| 1. **Switch port down** | * Switch port down * Neighbor switch/ host port down * Damaged service – sometimes – If the service is damaged additional indications may pop | * Get physical topology – Find out all existing switches in the domain, connectivity, connection to racks, connection to hosts * Get mappings: VMs to hosts, Hosts to racks, racks to switch ports, apps to VMs * SNMP Manager – Receive SNMP traps * OF-Config for SDN switches * Get switch port status /event * Get VMs status /Event ??? – through cloud infrastructure, meaning ceilometer * Activate link OAM tool – Perform binary fault detection on the connection |
| 1. **Host’s Nic Down** | * Switch port down * Host port down * Damaged service – sometimes – If the service is damaged additional indications may pop | * Get mappings: VMs to hosts, Hosts to racks, racks to switch ports, apps to VMs * SNMP Manager – Receive SNMP traps * Get NIC status /event * Get VMs status /Event ??? * Remote fault – find in the switch that the other side is down * Activate link OAM tool – Perform binary fault detection on the connection |
| 1. **Damaged host cable (Not disconnected)** | * Lost packets and CRC errors in one port of switch * Lost packets and CRC errors in and NIC of one host * Apps retransmissions may result in app performance degradation | * Get mappings: VMs to hosts, Hosts to racks, racks to switch ports, apps to VMs * Get switch’s port statistics * Get host’s NIC statistics * Get virtual topology * Activate link quality OAM tool – measure quality of link |
| 1. **OVS crash** | * VMs connectivity lost * Apps connectivity lost * Host connectivity lost | * Get mappings: VMs to hosts, apps to VMs * Get virtual topology * Get host process list and status * Get OVS switch status * Activate link OAM tool – Perform binary fault detection on the connection |
| 1. **L2 agent crash** | * OVS may be reconfigured * don’t know if effects traffic | * Get host process list and status * Get L2 agent status |
| 1. **OVS port down** | * No communication to a single VM * Apps connectivity lost | * Get mappings: VMs to hosts, apps to VMs * Get OVS/ SDN switch port status * Get OVS port down event |
| 1. **Hypervisor crash** | * No connectivity to VMs * Couldn’t access VMs via VNC proxy | * Get mappings: VMs to hosts, apps to VMs * Get Hypervisor status/ event * Check process up time |
| 1. **Host restarted** | * VMs connectivity lost * Apps connectivity lost | * Get virtual topology – mapping VMs to hosts * Get host restarted event * IPMI – sys up time |
| 1. **vNIC crash** | * No communication to a single VM * Apps on that VM, connectivity lost | * Same as OVS port down – only via vnc * Find out if the virtlib is checking VM status via vnc * Get vNIC status |
| 1. **MTU misconfigure** | * Host/ VM/ App Degraded communication | * Get mappings: VMs to hosts, Hosts to racks, racks to switch ports, apps to VMs * Get virtual topology * Get actual MTU from all devices * Get expected MTU of all devices |
| 1. **IP address misconfigure** | * No communication to Host/ VM/ App | * Get mappings: VMs to hosts, apps to VMs * Get virtual topology * Get actual IP address all hosts and VMs * Get expected IP address of all hosts and VM |

|  |  |  |
| --- | --- | --- |
|  | **No communication** |  |
|  | **Bandwidth degradation** |  |
|  | **Bandwidth quality degradation** |  |
|  | **QoS misbehavior** |  |
|  | **VM not responding** |  |
|  | **Host not responding** |  |
|  | **Tenant not responding** |  |