Event Management for VNS/SD-WAN

January 2024

Document ID: VZK52766

verizon✓

Content

- Introduction
- What is Event Management?
- Versa/Viptela Monitoring
- SilverPeak Monitoring
- Fortinet Monitoring
- Alarm Creation
- From Event to Incident Ticket
- Alarm List
- Ticket Priority Definitions
- ServiceImpact
- Alarm Correlation

Introduction

The purpose of this presentation is to provide a high level overview of the process where an event triggers the creation of a proactive incident ticket.

It is a generic overview and therefore exceptions as well as custom arrangements are not being covered.

Please refer to the appendix at the end of the presentation for an explanation of terms.

What is Event Management

Event Management Definition

An event can be defined as any detectable occurrence that has significance for the delivery of IT services. Events are typically notifications created by an IT service, Configuration Item (CI) or monitoring tool.

Event Management by Verizon

Verizon is using Assure1 as the event monitoring tool for VNS/SD-WAN services which is using different methods to detect service interruptions:

1. Pollers are configured to poll (SNMP & ICMP walk) provisioned devices every 2 to 5 minutes.
2. Assure1 is polling the API's from the vendor management systems approximately every 5-6 minutes.
3. Via the Assure1 WebSocket/Webhooks collector.

Alerts are delivered through the Assure1 element manager and forwarded up through to IMPACT for standard automation.

Versa/Viptela Monitoring

Viptela

Viptela vManage provides a central management function to the Viptela SD-WAN Secure Extensible Network (SEN). vManage works in conjunction with Viptela vSmart an vBond servers as the SD-WAN controller for individual customer deployments. Verizon is using the Viptela vManage RESTful API to perform performance and fault monitoring, configuration, policy management and control of the SD-WAN network.

Versa

Versa Director provides a central management function to the Versa SD-WAN network. Director works in conjunction with Versa SD-WAN Controller as the SD-WAN control for individual customer deployments. Versa also employs an analytic platform named Versa Analytics. Versa Analytics acts as a centralized reporting function to provide reporting and alerting on various elements and functions within the Versa deployment. Verizon is using the API capabilities of Director and Analytics to perform performance and fault monitoring, configuration, policy management and control of the SD-WAN network.

SilverPeak Monitoring

Silver Peak

The Silver Peak SD-WAN does not work with a centralized control plane, i.e. each network node is aware of the status of the network and computes the reachability information autonomously. The orchestrator is the central configuration interface, but in the absence of a central controller instance, the Silver Peak orchestrator also acts as a centralized provider and collection point for management information. The Silver Peak orchestrator is multi-tenant and resides in the public cloud.

Verizon will use API to discover the Silver Peak Edge Connect routers, and to establish a Web Socket connection to the Silver Peak Tenant Orchestrator to allow streaming of alarms from Silver Peak to Assure1. In the event of an outage to the WebSocket connection, Assure1 will use REST API to poll for any alarms that may not have been received.

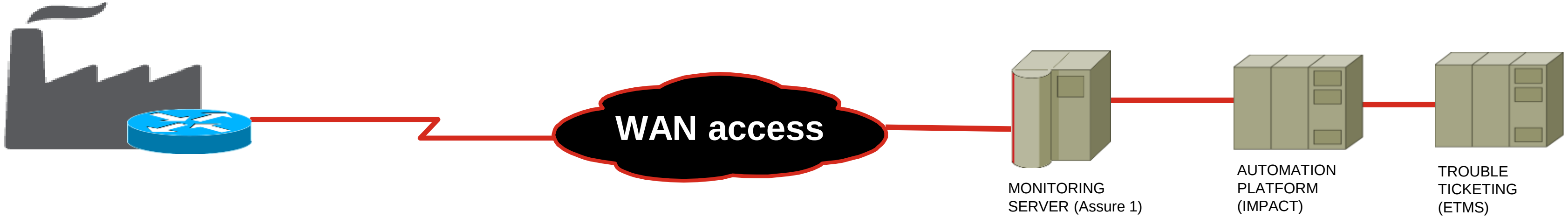
Fortinet Monitoring

Fortinet

Fortinet SDWAN branch/customer devices will be managed via Assure1 for fault management. The Assure1 platform will poll the Fortigates directly and generate alarms based on this.

The Hosted Head end FortiGates (Fortinet SDWAN Gateway) and the FortiManagers will be monitored via SNMP polling via the SmartsAssure1 platform.

Alarm Creation

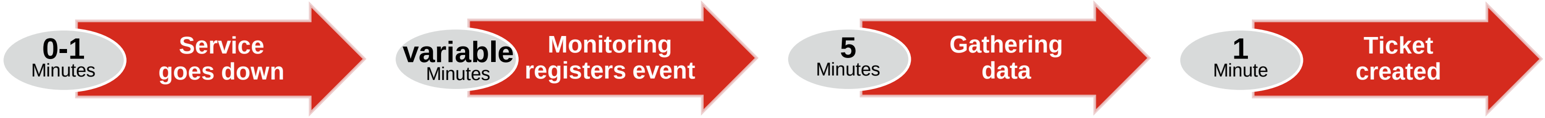


Fault detection: When Assure1 receives a new fault event via an API or the Websocket collector an event in Assure1 is created.

Event sent to Automation (IMPACT): Assure1 forwards the event to IMPACT based on messaging policy after a set hold timer which depends on the technology being used.

IMPACT: Upon receiving an event from Assure1 IMPACT queries ESP (Managed Device Inventory Database) against the entity name to retrieve information such as: Circuit ID, Customer name, Product, Service desk, NOC, etc. This information is used to populate the alarm and to create the ticket within Verizon's Enterprise Ticket Management System (ETMS).

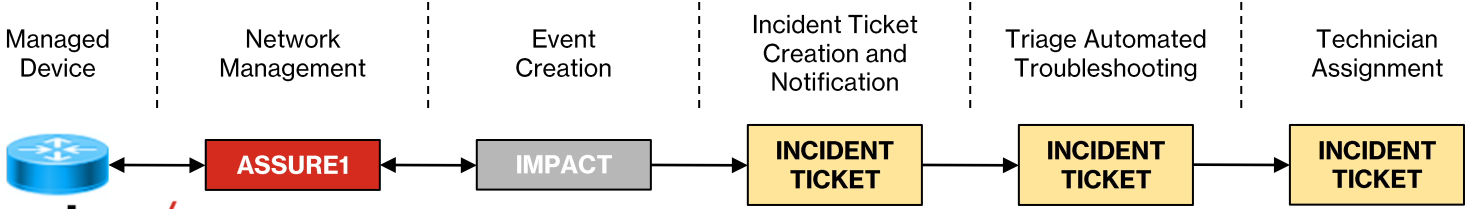
From Event to Incident Ticket



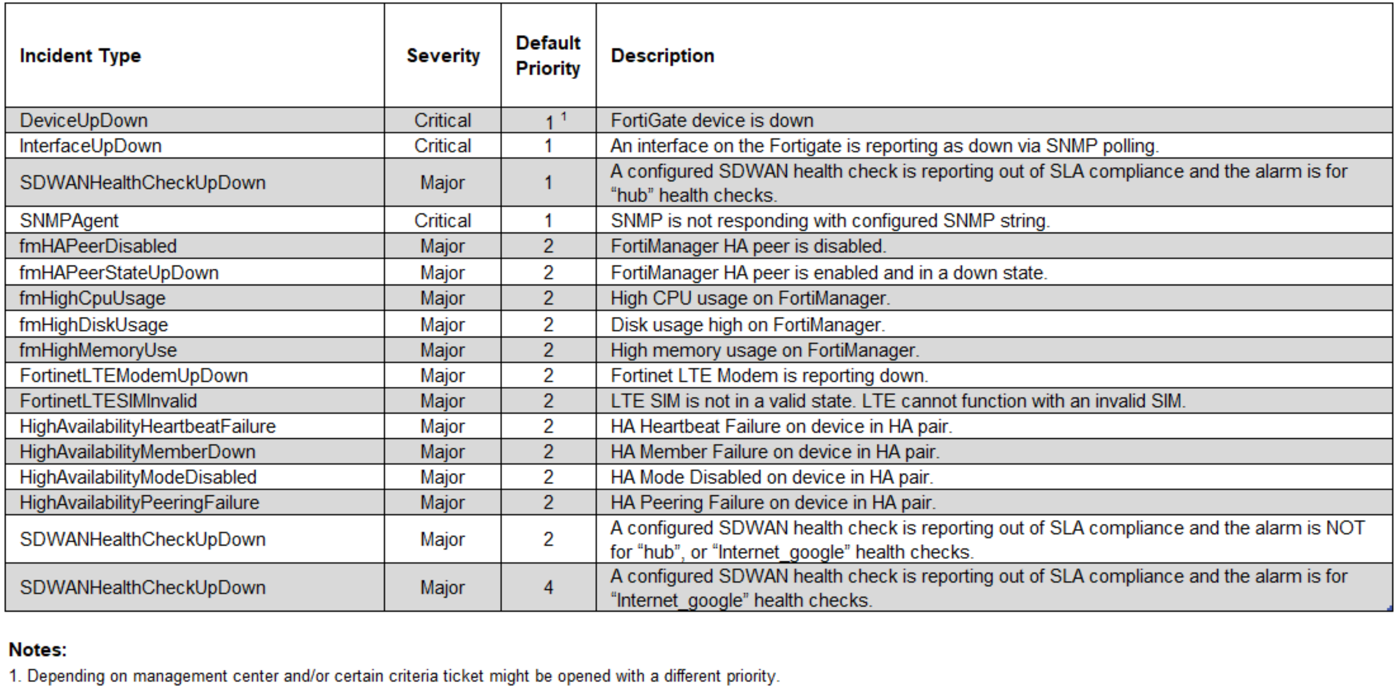
It depends on the type of event as to how quickly a ticket is created. For example, DeviceUpDown tickets are created within ~13 minutes after the initial network event whereas other types of event may take longer.

Automated troubleshooting commences immediately after the creation of the proactive incident ticket. This is the so called ‘triage‘ phase and is published on the VEC Portal and via eBonding.

Triage Automated troubleshooting enables faster resolution as ticket is automatically transferred to NOC if further diagnostics are required by technicians. The NOC technicians can also use the Triage output to diagnostic data.



Alarm List – Fortinet

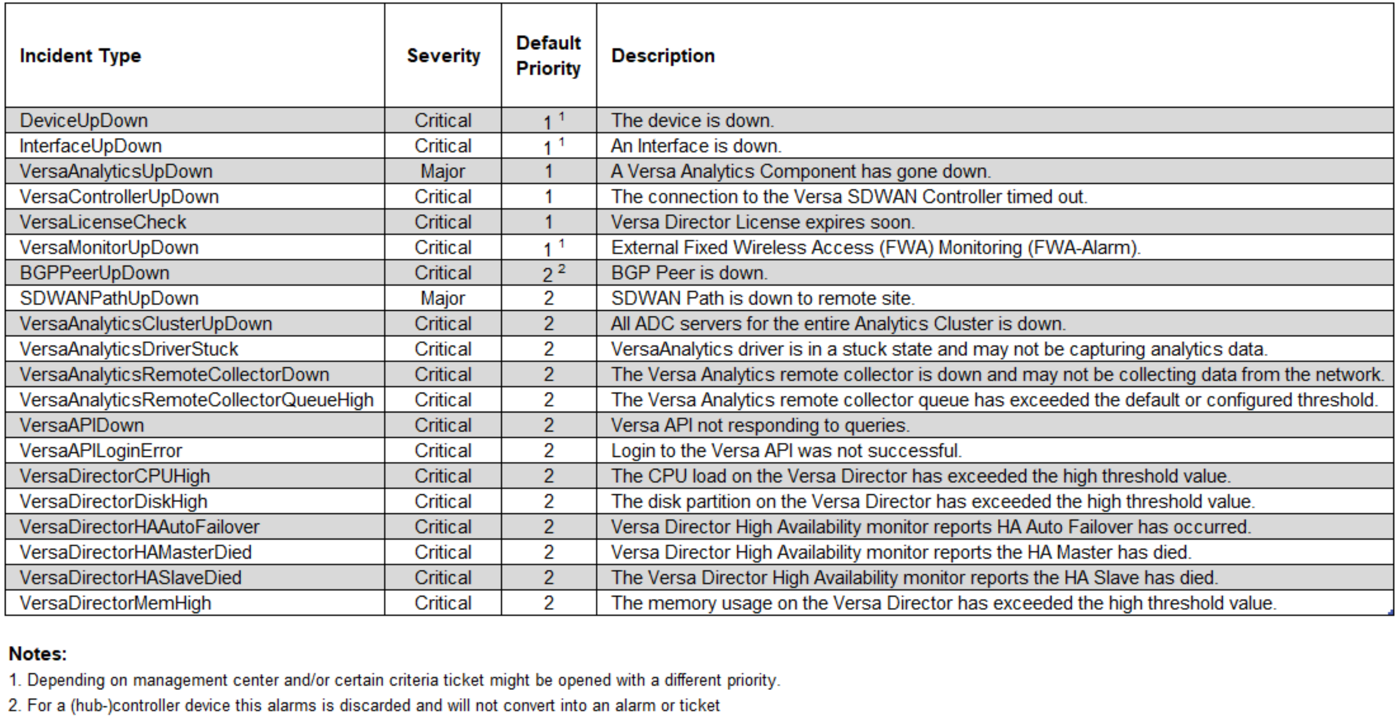


Incident Type	Severity	Default Priority	Description
DeviceUpDown	Critical	1[1]	FortiGate device is down
InterfaceUpDown	Critical	1	An interface on the Fortigate is reporting as down via SNMP polling.
SDWANHealthCheckUpDown	Major	1	A configured SDWAN health check is reporting out of SLA compliance and the alarm is for "hub" health checks.
SNMPAgent	Critical	1	SNMP is not responding with configured SNMP string.
fmHAPeerDisabled	Major	2	FortiManager HA peer is disabled.
fmHAPeerStateUpDown	Major	2	FortiManager HA peer is enabled and in a down state.
fmHighCpuUsage	Major	2	High CPU usage on FortiManager.
fmHighDiskUsage	Major	2	Disk usage high on FortiManager.
fmHighMemoryUse	Major	2	High memory usage on FortiManager.
FortinetLTEModemUpDown	Major	2	Fortinet LTE Modem is reporting down.
FortinetLTESIMInvalid	Major	2	LTE SIM is not in a valid state. LTE cannot function with an invalid SIM.
HighAvailabilityHeartbeatFailure	Major	2	HA Heartbeat Failure on device in HA pair.
HighAvailabilityMemberDown	Major	2	HA Member Failure on device in HA pair.
HighAvailabilityModeDisabled	Major	2	HA Mode Disabled on device in HA pair.
HighAvailabilityPeeringFailure	Major	2	HA Peering Failure on device in HA pair.
SDWANHealthCheckUpDown	Major	2	A configured SDWAN health check is reporting out of SLA compliance and the alarm is NOT for "hub", or "Internet_google" health checks.
SDWANHealthCheckUpDown	Major	4	A configured SDWAN health check is reporting out of SLA compliance and the alarm is for "Internet_google" health checks.

Notes:

1. Depending on management center and/or certain criteria ticket might be opened with a different priority.

Alarm List – Versa

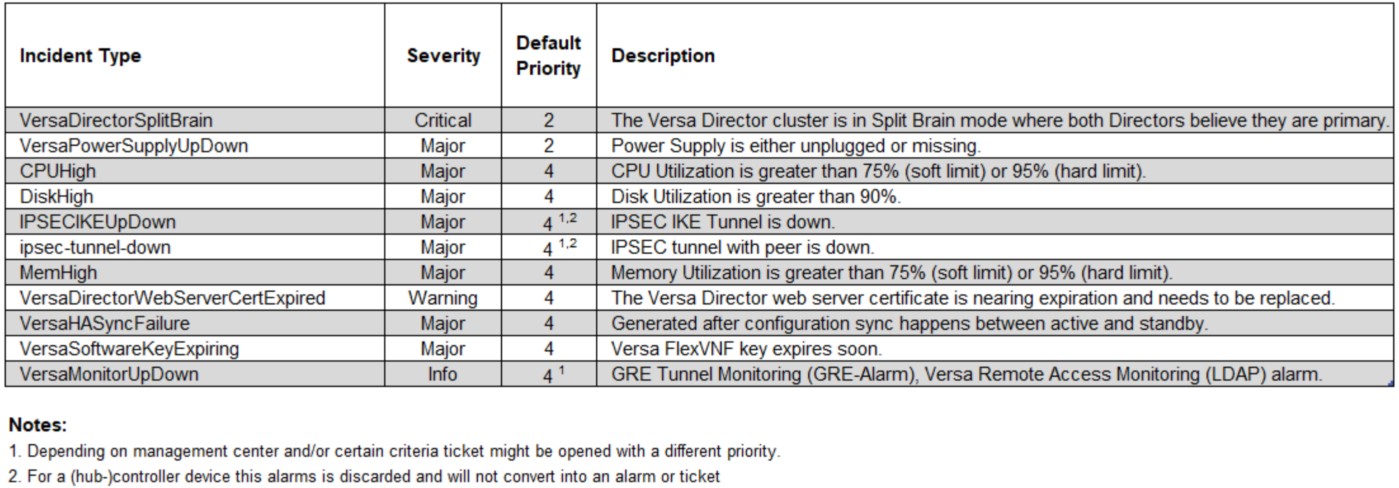


Incident Type	Severity	Default Priority	Description
DeviceUpDown	Critical	1[1]	The device is down.
InterfaceUpDown	Critical	1[1]	An Interface is down.
VersaAnalyticsUpDown	Major	1	A Versa Analytics Component has gone down.
VersaControllerUpDown	Critical	1	The connection to the Versa SDWAN Controller timed out.
VersaLicenseCheck	Critical	1	Versa Director License expires soon.
VersaMonitorUpDown	Critical	1[1]	External Fixed Wireless Access (FWA) Monitoring (FWA-Alarm).
BGPPeerUpDown	Critical	2[2]	BGP Peer is down.
SDWANPathUpDown	Major	2	SDWAN Path is down to remote site.
VersaAnalyticsClusterUpDown	Critical	2	All ADC servers for the entire Analytics Cluster is down.
VersaAnalyticsDriverStuck	Critical	2	VersaAnalytics driver is in a stuck state and may not be capturing analytics data.
VersaAnalyticsRemoteCollectorDown	Critical	2	The Versa Analytics remote collector is down and may not be collecting data from the network.
VersaAnalyticsRemoteCollectorQueueHigh	Critical	2	The Versa Analytics remote collector queue has exceeded the default or configured threshold.
VersaAPIDown	Critical	2	Versa API not responding to queries.
VersaAPILoginError	Critical	2	Login to the Versa API was not successful.
VersaDirectorCPUHigh	Critical	2	The CPU load on the Versa Director has exceeded the high threshold value.
VersaDirectorDiskHigh	Critical	2	The disk partition on the Versa Director has exceeded the high threshold value.
VersaDirectorHAAutoFailover	Critical	2	Versa Director High Availability monitor reports HA Auto Failover has occurred.
VersaDirectorHAMasterDied	Critical	2	Versa Director High Availability monitor reports the HA Master has died.
VersaDirectorHASlaveDied	Critical	2	The Versa Director High Availability monitor reports the HA Slave has died.
VersaDirectorMemHigh	Critical	2	The memory usage on the Versa Director has exceeded the high threshold value.

Notes:

1. Depending on management center and/or certain criteria ticket might be opened with a different priority.
2. For a (hub-)controller device this alarms is discarded and will not convert into an alarm or ticket

Alarm List – Versa (continued)

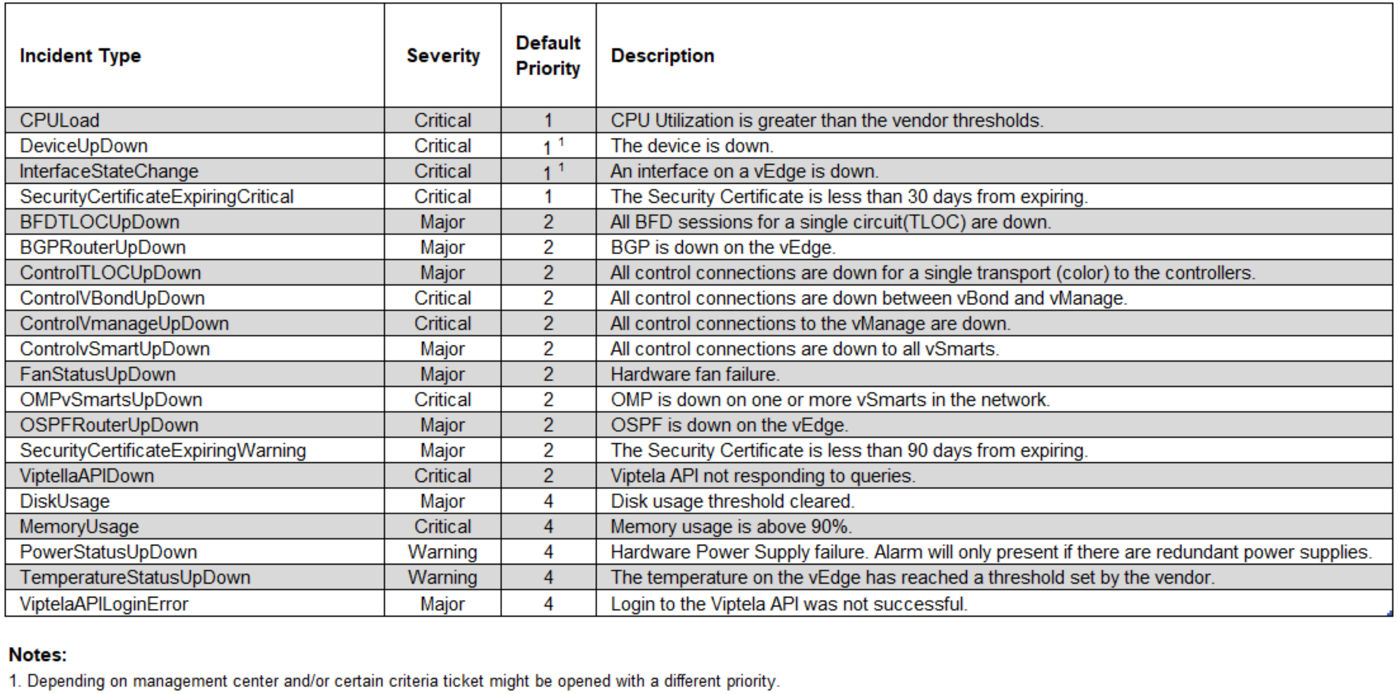


Incident Type	Severity	Default Priority	Description
VersaDirectorSplitBrain	Critical	2	The Versa Director cluster is in Split Brain mode where both Directors believe they are primary.
VersaPowerSupplyUpDown	Major	2	Power Supply is either unplugged or missing.
CPUHigh	Major	4	CPU Utilization is greater than 75% (soft limit) or 95% (hard limit).
DiskHigh	Major	4	Disk Utilization is greater than 90%.
IPSECIKEUpDown	Major	4 [1,2]	IPSEC IKE Tunnel is down.
ipsec-tunnel-down	Major	4 [1,2]	IPSEC tunnel with peer is down.
MemHigh	Major	4	Memory Utilization is greater than 75% (soft limit) or 95% (hard limit).
VersaDirectorWebServerCertExpired	Warning	4	The Versa Director web server certificate is nearing expiration and needs to be replaced.
VersaHASyncFailure	Major	4	Generated after configuration sync happens between active and standby.
VersaSoftwareKeyExpiring	Major	4	Versa FlexVNF key expires soon.
VersaMonitorUpDown	Info	4 [1]	GRE Tunnel Monitoring (GRE-Alarm), Versa Remote Access Monitoring (LDAP) alarm.

Notes:

1. Depending on management center and/or certain criteria ticket might be opened with a different priority.
2. For a (hub-)controller device this alarms is discarded and will not convert into an alarm or ticket

Alarm List – Viptela

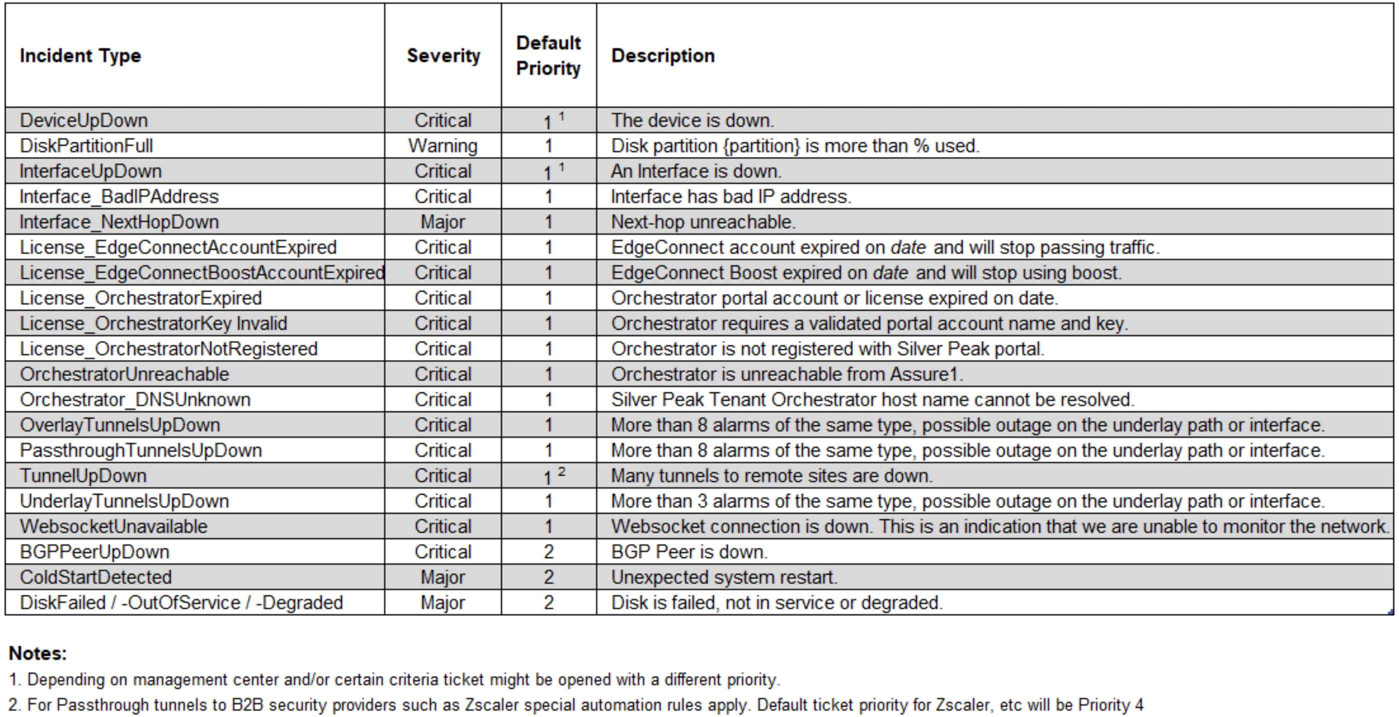


Incident Type	Severity	Default Priority	Description
CPULoad	Critical	1	CPU Utilization is greater than the vendor thresholds.
DeviceUpDown	Critical	1 [1]	The device is down.
InterfaceStateChange	Critical	1 [1]	An interface on a vEdge is down.
SecurityCertificateExpiringCritical	Critical	1	The Security Certificate is less than 30 days from expiring.
BFDTLOCUpDown	Major	2	All BFD sessions for a single circuit(TLOC) are down.
BGPRouterUpDown	Major	2	BGP is down on the vEdge.
ControlTLOCUpDown	Major	2	All control connections are down for a single transport (color) to the controllers.
ControlVBondUpDown	Critical	2	All control connections are down between vBond and vManage.
ControlVmanageUpDown	Critical	2	All control connections to the vManage are down.
ControlvSmartUpDown	Major	2	All control connections are down to all vSmarts.
FanStatusUpDown	Major	2	Hardware fan failure.
OMPvSmartsUpDown	Critical	2	OMP is down on one or more vSmarts in the network.
OSPFRouterUpDown	Major	2	OSPF is down on the vEdge.
SecurityCertificateExpiringWarning	Major	2	The Security Certificate is less than 90 days from expiring.
ViptellaAPIDown	Critical	2	Viptela API not responding to queries.
DiskUsage	Major	4	Disk usage threshold cleared.
MemoryUsage	Critical	4	Memory usage is above 90%.
PowerStatusUpDown	Warning	4	Hardware Power Supply failure. Alarm will only present if there are redundant power supplies.
TemperatureStatusUpDown	Warning	4	The temperature on the vEdge has reached a threshold set by the vendor.
ViptelaAPILoginError	Major	4	Login to the Viptela API was not successful.

Notes:

1. Depending on management center and/or certain criteria ticket might be opened with a different priority.

Alarm List – SilverPeak

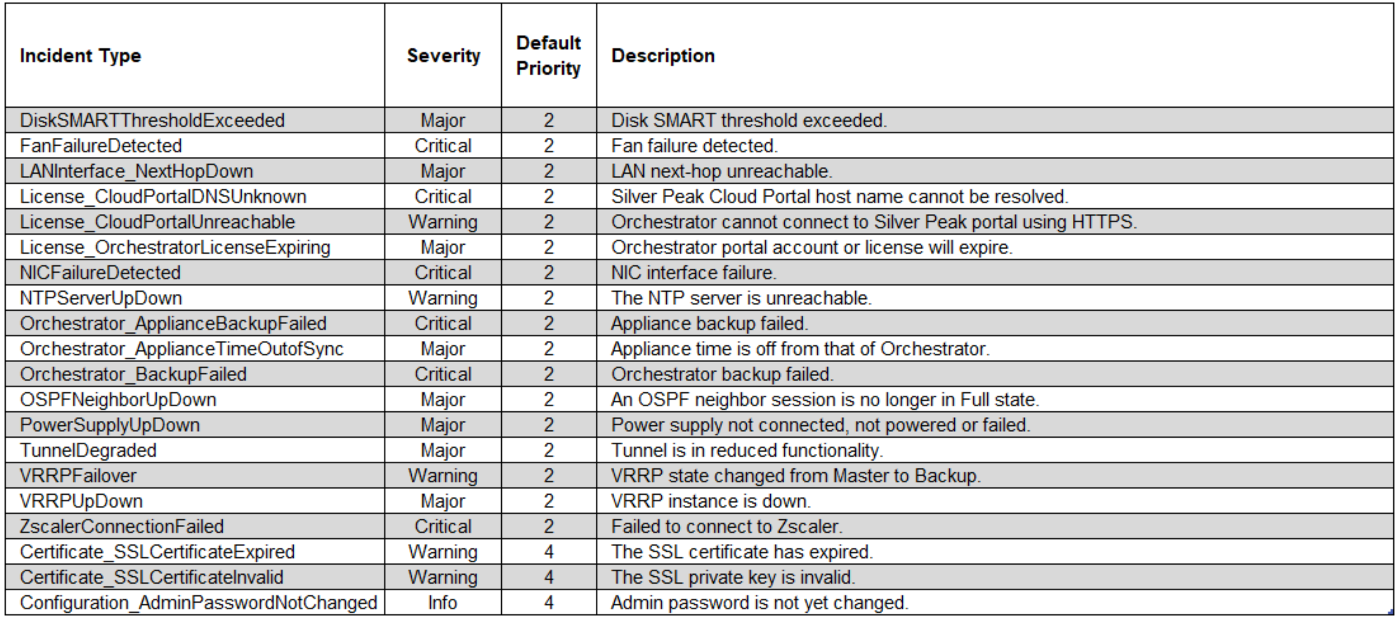


Incident Type	Severity	Default Priority	Description
DeviceUpDown	Critical	1 [1]	The device is down.
DiskPartitionFull	Warning	1	Disk partition {partition} is more than % used.
InterfaceUpDown	Critical	1 [1]	An Interface is down.
Interface_BadIPAddress	Critical	1	Interface has bad IP address.
Interface_NextHopDown	Major	1	Next-hop unreachable.
License_EdgeConnectAccountExpired	Critical	1	EdgeConnect account expired on *date* and will stop passing traffic.
License_EdgeConnectBoostAccountExpired	Critical	1	EdgeConnect Boost expired on *date* and will stop using boost.
License_OrchestratorExpired	Critical	1	Orchestrator portal account or license expired on date.
License_OrchestratorKey Invalid	Critical	1	Orchestrator requires a validated portal account name and key.
License_OrchestratorNotRegistered	Critical	1	Orchestrator is not registered with Silver Peak portal.
OrchestratorUnreachable	Critical	1	Orchestrator is unreachable from Assure1.
Orchestrator_DNSUnknown	Critical	1	Silver Peak Tenant Orchestrator host name cannot be resolved.
OverlayTunnelsUpDown	Critical	1	More than 8 alarms of the same type, possible outage on the underlay path or interface.
PassthroughTunnelsUpDown	Critical	1	More than 8 alarms of the same type, possible outage on the underlay path or interface.
TunnelUpDown	Critical	1 [2]	Many tunnels to remote sites are down.
UnderlayTunnelsUpDown	Critical	1	More than 3 alarms of the same type, possible outage on the underlay path or interface.
WebsocketUnavailable	Critical	1	Websocket connection is down. This is an indication that we are unable to monitor the network.
BGPPeerUpDown	Critical	2	BGP Peer is down.
ColdStartDetected	Major	2	Unexpected system restart.
DiskFailed / -OutOfService / -Degraded	Major	2	Disk is failed, not in service or degraded.

Notes:

1. Depending on management center and/or certain criteria ticket might be opened with a different priority.
2. For Passthrough tunnels to B2B security providers such as Zscaler special automation rules apply. Default ticket priority for Zscaler, etc will be Priority 4

Alarm List – SilverPeak (continued)

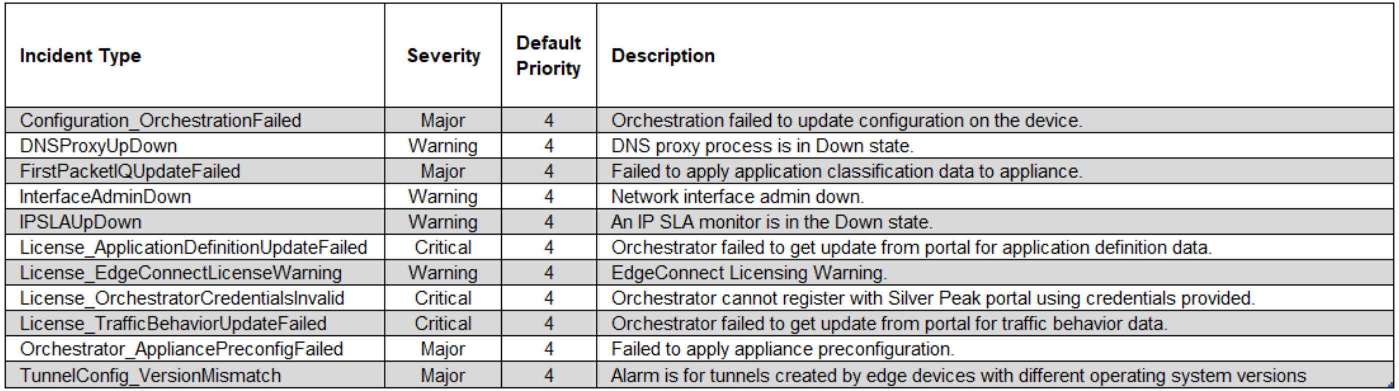


Incident Type	Severity	Default Priority	Description
DiskSMARTThresholdExceeded	Major	2	Disk SMART threshold exceeded.
FanFailureDetected	Critical	2	Fan failure detected.
LANInterface_NextHopDown	Major	2	LAN next-hop unreachable.
License_CloudPortalDNSUnknown	Critical	2	Silver Peak Cloud Portal host name cannot be resolved.
License_CloudPortalUnreachable	Warning	2	Orchestrator cannot connect to Silver Peak portal using HTTPS.
License_OrchestratorLicenseExpiring	Major	2	Orchestrator portal account or license will expire.
NICFailureDetected	Critical	2	NIC interface failure.
NTPServerUpDown	Warning	2	The NTP server is unreachable.
Orchestrator_ApplianceBackupFailed	Critical	2	Appliance backup failed.
Orchestrator_ApplianceTimeOutofSync	Major	2	Appliance time is off from that of Orchestrator.
Orchestrator_BackupFailed	Critical	2	Orchestrator backup failed.
OSPFNeighborUpDown	Major	2	An OSPF neighbor session is no longer in Full state.
PowerSupplyUpDown	Major	2	Power supply not connected, not powered or failed.
TunnelDegraded	Major	2	Tunnel is in reduced functionality.
VRRPFailover	Warning	2	VRRP state changed from Master to Backup.
VRRPUpDown	Major	2	VRRP instance is down.
ZscalerConnectionFailed	Critical	2	Failed to connect to Zscaler.
Certificate_SSLCertificateExpired	Warning	4	The SSL certificate has expired.
Certificate_SSLCertificateInvalid	Warning	4	The SSL private key is invalid.
Configuration_AdminPasswordNotChanged	Info	4	Admin password is not yet changed.

Notes:

1. Depending on management center and/or certain criteria ticket might be opened with a different priority.
2. For Passthrough tunnels to B2B security providers such as Zscaler special automation rules apply. Default ticket priority for Zscaler, etc will be Priority 4

Alarm List – SilverPeak (continued)

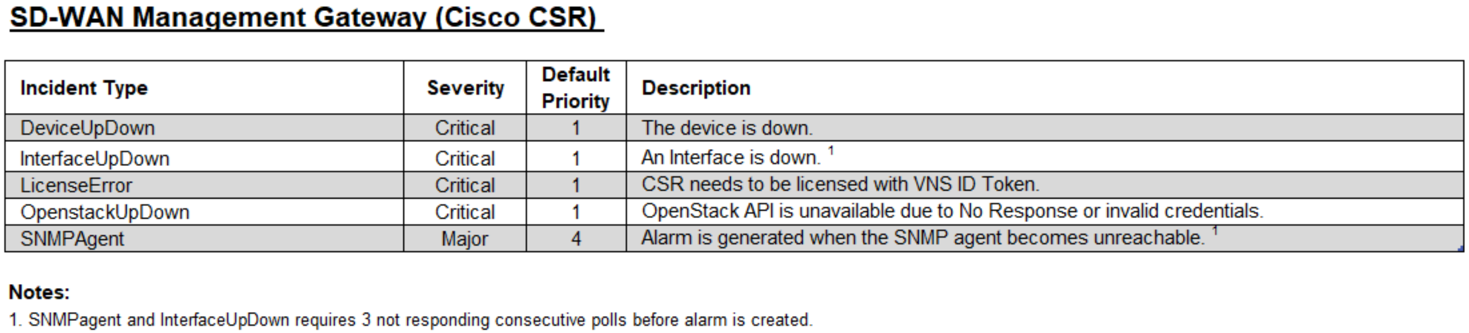


Incident Type	Severity	Default Priority	Description
Configuration_OrchestrationFailed	Major	4	Orchestration failed to update configuration on the device.
DNSProxyUpDown	Warning	4	DNS proxy process is in Down state.
FirstPacketIQUpdateFailed	Major	4	Failed to apply application classification data to appliance.
InterfaceAdminDown	Warning	4	Network interface admin down.
IPSLAUpDown	Warning	4	An IP SLA monitor is in the Down state.
License_ApplicationDefinitionUpdateFailed	Critical	4	Orchestrator failed to get update from portal for application definition data.
License_EdgeConnectLicenseWarning	Warning	4	EdgeConnect Licensing Warning.
License_OrchestratorCredentialsInvalid	Critical	4	Orchestrator cannot register with Silver Peak portal using credentials provided.
License_TrafficBehaviorUpdateFailed	Critical	4	Orchestrator failed to get update from portal for traffic behavior data.
Orchestrator_AppliancePreconfigFailed	Major	4	Failed to apply appliance preconfiguration.
TunnelConfig_VersionMismatch	Major	4	Alarm is for tunnels created by edge devices with different operating system versions

Notes:

1. Depending on management center and/or certain criteria ticket might be opened with a different priority.
2. For Passthrough tunnels to B2B security providers such as Zscaler special automation rules apply. Default ticket priority for Zscaler, etc will be Priority 4

Alarm List – Cisco CSR



SD-WAN Management Gateway (Cisco CSR)

Incident Type	Severity	Default Priority	Description
DeviceUpDown	Critical	1	The device is down.
InterfaceUpDown	Critical	1	An Interface is down. [1]
LicenseError	Critical	1	CSR needs to be licensed with VNS ID Token.
OpenstackUpDown	Critical	1	OpenStack API is unavailable due to No Response or invalid credentials.
SNMPAgent	Major	4	Alarm is generated when the SNMP agent becomes unreachable. [1]

Notes:

1. SNMPagent and InterfaceUpDown requires 3 not responding consecutive polls before alarm is created.

Ticket Priority Definitions

Ticket Type	Priority	Description
Outage	1	Service is unusable, complete loss of service. The service is released for testing without restriction.
Degraded	2	Service is experiencing intermittent issues or is degraded and is not released for testing without restriction.
Service Risk	3	Quality issues that threaten the performance of the service.
Assistance Request	4	Non-service impacting issues requiring investigation, resolution or other action.

These are the standard ticket priorities definitions used within Verizon.

ServiceImpact

For VNS - Premise and VNS - Hosted entities alarms are correlated in Assure1 to a Service Impact alert which is created against the VNS - Premise or VNS - Hosted entity. The ServiceImpact represents the product as a whole (1 or multiple VNFs in a service chain) and is only created when child alarms against the VNF(s) are created. The priority for the ticket will be set based on the highest ‘child’ alarm severity.

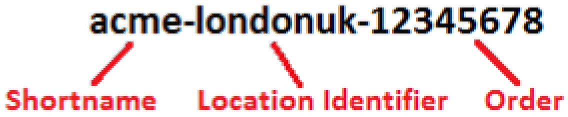
Service Impacts alerts will not be created against:

- Certificate alarms
- SNMPAgent alarms
- API alarms

Above mentioned alarms will be ticketed individually.

Alarm Correlation

For PNF’s, non VNS – Premise / Hosted entities the alarms are correlated by IMPACT. When alarms are presented to IMPACT, a correlation key is applied based on shortname and location identifier. Alarms with the same key and priority will be added to the same event and ticket. This key remains active for either 15 minutes for Hub locations or for 2 hours for remote locations.



acme-londonuk-12345678

Shortname Location Identifier Order

After the timer expires new alarms will create new events, perform all of the wait-time, backend queries, etc. and then a pre-existing ticket check will move the alarm to a previous event/ticket when an open event/ticket is found against the same shortname and location identifier.

Appendix

API
Application Programming Interface, a software intermediary that allows two applications to talk to each other.

Assure1
Assure1 is the standard management platform for VNS and SD-WAN services within Verizon and provides fault and performance alerting.

IMPACT
Integrated Management Platform for Advanced Communications Technologies is a application that provides surveillance, alarm topology augmentation, correlation, ticketing, and automation capabilities for the Verizon network.

NOC
Network Operation Center

PNF
Physical Network Function and refers to a purpose built hardware box that provides specific networking function.

SD-WAN
Software Defined Wide Area Network

VNF
Virtual Network Function refers to virtualization of a network function.

VNS
Virtual Network Services