|  |  |  |
| --- | --- | --- |
|  | Document Number | EDCS-xxxxx |
| Based on Template | EDCS-709651 |
| Created By | Silvija Dry |

vMS 2.2 OSS Assurance  
iWAN Service Blueprint

Purpose of this document

This document provides the service specific details on monitoring and assurance of iWAN service in alignment with assurance functions delivered by vMS OSS Assurance Platform which is described in vMS OSS Assurance Platform System Architecture Specification.

Modification History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision | Date | Originator | Comments |
| 1.0 | 11/09/2015 | Silvija Dry | Initial Draft |
| 2.0 | 11/12/2015 | Silvija Dry | Updates based on review comments |

Table of Contents

1 Introduction 3

2 CloudVPN Monitored Components 3

2.1 vMS 2.2 iWAN Assured Services 3

2.2 vMS 2.2 iWAN Monitored Components 3

2.3 Monitored System Overview 4

3 vMS 2.2 iWAN Service Health 5

3.1 Service Health 5

3.2 BR Status & Connectivity 8

3.1 MC Status 8

3.2 Branch Data Plane Performance – additional detail 9

4 vMS 2.2 Metric 10

4.1 Usage Metric 10

4.2 Performance & Availability Metric 10

5 vMS 2.2 CloudVPN Alarms & Events 11

5.1 ESC Alarms & Events 12

5.2 NSO Alarms & Events 12

6 iWAN Logs 13

7 iWAN Fault Analysis 13

7.1 Data Sources 13

7.2 Service Impact Enrichment 14

# Introduction

# CloudVPN Monitored Components

## vMS 2.2 iWAN Assured Services

Following table lists set of assured iWAN service types, i.e. vMS services that assurance system needs to assure. Assured services typically refer to end to end service that tenant or end user will be purchasing.

Table 1: iWAN Managed Services - vMS 2.2

| **Service ID** | **Priority** | **Service Description** |
| --- | --- | --- |
|  | Mandatory | IWAN vMS service offers CPE overlay transport for Internet and MPSL connections with intelligent path control, application optimization and highly secure connectivity. |

## vMS 2.2 iWAN Monitored Components

In this section we list all components that need to be managed and monitored. We are also including type of monitoring data that will be collected from each component.

Figure 2 Devices

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Managed Component | Status/Health | Metric | Events/Alarms | Logs | Netflow |
| ISR4k (BR/MC) | Yes | Yes | Yes (only TCAs) | Yes | Potentially |
| ISRG2 (BR/MC) | Yes | Yes | Yes (only TCAs) | Yes | Potentially |
| ASR1k (Border Router) | Yes | Yes | Yes (only TCAs) | Yes | Potentially |
| ASR1k (Master Controller) | Yes | Yes | Yes (only TCAs) | Yes | No |

NOTE: Netflow is not required to determine service status, however in order to get service performance metric (delay, jitter, packet loss) monitored by Performance Monitor Netflow will be needed. If Netflow export to SME can’t get accomplished in vMS 2.2 timeframe, engineering can explore any possible alternatives to export this data to SME.

## Monitored System Overview

In this section we provide brief overview of relevant aspects of vMS managed system which is delivering services listed in section 2.

It is not intent to provide detailed design of vMS architecture, but it can be found in vMS 2.2 Rally space – NEED LINK TO US.

iWAN Enterprise CVD:

<http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Jan2015/CVD-IWANDesignGuide-JAN15.pdf>

Diagram below illustrate components and their interconnections for iWAN service.



Here are some relevant highlights:

List of iWAN features included in vMS 2.2 are:

* + DMVPN Transport
  + HQoS
  + BGP overlay routing protocol
  + OSPF or EIGRP
  + Single CPE branch
  + PfRv3 with Transit Site support
  + PfRv3 with DSCP based policies

Here is list of features configured on ISR4k and ASR1k that need to be monitored and managed:

ISR4k/ISRG2 (MC/BR):

* TBD

ASR1k (MC):

* TBD

ASR1k (BR):

* TBD

Complete list of features is available in the config templates maintained at: https://cisco.app.box.com/s/6ovc7twfbdlmi0mgb3ozquybjqpfhnbr

# vMS 2.2 iWAN Service Health

## Service Health

NOTE: In vMS 2.2 assurance system will not have SH/IA app (which comes in 3.0) and we will use temporary solution where SME performs service status calculations. SME doesn’t have out of box capabilities to apply complex policies on number of data points needed to calculate overall service state. As such in vMS 2.2, we will try to simplify iWAN service status definition.

Section below gives one proposal but after engineering analysis is done change may be made to reduce amount of throw away work on SME.

Definition of Service Health Status:

|  |  |  |
| --- | --- | --- |
| **Type of Status/State** | **Status/State** | **Description** |
| Operational Status | Up | Service and all of its functions are up for all sites. |
| Operational Status | Partially Up | Service is up for some sites but Down for at least one site. |
| Operational Status | Degraded | Service is up for all of sites but there is performance degradation of service for at least one site or there is performance degradation of any of Hub services or components. |
| Operational Status | At Risk | Redundant service or service function is UP but had lost its redundant components, so next failure may result in loss of service.  Data plane is up, but control plane is down (e.g. all BRs and paths between them is up, but MC is down), thus services are currently UP but if one of the paths gets degraded or down, traffic will not be switched to alternative path. |
| Operational Status | Down | Service is not operational for all of its sites. |

NOTE: iWAN has redundancy built in on multiple levels – due to temporary use of SME for service health proposal is not to explicitly account for redundancy in vMS 2.2 (which means there would be no At Risk state) – unless engineering finds it simple to implement.



For iWAN in vMS 2.2 we will look at two key functions to determine service health of overall service:

* Hub Status:
  + Hub Master Controllers Status:
    - Status of Hub Master Controllers (**show domain iwan master status, ICMP Device Availability Test)**
  + Hub BR Status (**show domain iwan border status, ICMP Device Availability Test)**
* Branches Status:
  + Service Health of each branch will be calculated first. Once service health for each branch is determined we will apply policy that will ‘roll-up’ status of individual branches to overall service status.
  + Status of each branch will be determined by two components:
    - Control Plane:
      * Constitutes of status of following components:
        + Status of Branch MC (**show domain iwan master status, ICMP Device Availability Test)**
        + Status of Connectivity between branch BR and MC (**show domain iwan border status)**
    - Data Plane:
      * Constitutes of status of following components:
        + Status of Branch BR (**show domain iwan border status, ICMP Device Availability Test)**
        + Health of branch data plane: will be determined by looking at per DSCP performance aggregate for each Branch (measured using Performance Monitor for purposes of PfR). Performance metric includes delay, jitter and loss and is defined per DSCP in the templates configured for PfR domain in HMC. Furthermore templates define thresholds utilized to determine when PfR will switch to different path. The same thresholds will be used for purposes of service health

iWAN Service Health can be calculated as follows in vMS 2.2:

* Hub Function Status:
  + UP if all Hub MCs and all Hub BRs are UP
  + DEGRADED if there is performance degradation of any thresholded performance metric for any of Hub MCs or any of Hub BRs
  + Partially UP if one but not all MCs are DOWN or if one but not all BRs are DOWN
  + DOWN if all MCs are DOWN or if all BRs are down.
  + At Risk if all MCs are DOWN but BRs are up (i.e. loss of control plane but data plane is UP)
* Branches Function Status:
  + UP if status of all Branches is UP
  + DOWN if status of all Branches is DOWN
  + Partially UP if status of at least one of the branches is DOWN
  + DEGRADED if status of any of branches is DEGRADED
* Status of individual Branch:
  + UP if both Control and Data functions are UP
  + DEGRADED if there either Control or Data functions are DEGRADED
  + Partially UP if Data function is Partially UP
  + DOWN if Data function is DOWN.
  + At Risk if all Control function is DOWN and Data function is up
* Status of individual Branch Data function:
  + UP if all branch BRs are UP
  + DOWN if all branch BRs are DOWN
  + Partially UP if one branch BR is up and other DOWN
  + DEGRADED if Performance Monitor for any of DSCPs is out of policy as determined by MC
* Status of individual Branch Control function:
  + UP if all connections between branch BR and Hub MCs are UP, and status of all Branch MCs is UP
  + Partially UP if either status of one of Hub MCs is DOWN or status of at least one of connections between branch BR and Hub MC is DOWN (but there is at least one connection that is UP)
  + DOWN if all connections between branch BR and Hub MCs are DOWN and Branch MC is down
  + DEGRADED if there is performance degradation of any thresholded performance metric for any of Branch MCs

## BR Status & Connectivity

The status of BR, status of its connection to MC and status of its two data path tunnel interfaces (via INET and MPLS) can be viewed using following show commands – examples included below – engineering to investigate the best way to extract that data (SNMP, netconf, CLI, etc.).

This data would be needed from all BRs to be used for service status calculations proposed in earlier section.

In addition to data illustrated in show command below, we can use ICMP Availability tests between Metric aggregator (SME) and BR device. This will detect when we lose connectivity with device and thus can not obtain data illustrated in show command below.

**Verify that the branch BR is operational by using the**

show domain [name] border status

command.

This example shows the branch BR operational in the IWAN Hybrid model and the external WAN interfaces are

up.

RS11-2921#

**show domain iwan border status**

Fri Dec 05 14:38:45.911

--------------------------------------------------------------------

\*\*\*\*Border Status\*\*\*\*

Instance Status:

UP

Present status last updated: 1w4d ago

Loopback:

Configured Loopback0 UP (10.255.241.11)

Master: 10.255.241.11

**Connection Status with Master:**

**UP**

MC connection info:

CONNECTION SUCCESSFUL

Connected for: 1w4d

Route-Control: Enabled

Minimum Mask length: 28

Sampling: off

Minimum Requirement: Met

**External Wan interfaces:**

**Name:**

**Tunnel10**

**Interface Index: 15 SNMP Index: 12 SP:**

**MPLS**

**Status:**

**UP**

**Name:**

**Tunnel11**

**Interface Index: 16 SNMP Index: 13 SP:**

**INET**

**Status:**

**UP**

Auto Tunnel information:

Name:Tunnel0 if\_index: 25

## MC Status

The status of MC can be viewed using following show commands – examples included below – engineering to investigate the best way to extract that data (SNMP, netconf, CLI, etc.).

This data would be needed from all MCs to be used for service status calculations proposed in earlier section.

In addition to data illustrated in show command below, we can use ICMP Availability tests between Metric aggregator (SME) and MC device. This will detect when we lose connectivity with device and thus can not obtain data illustrated in show command below.

Step 8:

Verify that the branch MC is operational by using the

show domain [name] master status

command.

This example shows the branch MC operational in the IWAN Hybrid design model. The borders are up with the

correct tunnel and service provider information.

RS11-2921#

**show domain iwan master status**

\*\*\* Domain MC Status \*\*\*

Master VRF:

Global

Instance Type:

Branch

Instance id: 0

**Operational status:**

**Up**

**Configured status:**

**Up**

Loopback IP Address:

10.255.241.11

Load Balancing:

Operational Status:

Up

Max Calculated Utilization Variance: 0%

Last load balance attempt: never

Last Reason: Variance less than 20%

Total unbalanced bandwidth:

External links: 0 Kbps Internet links: 0 Kpbs

Route Control: Enabled

Mitigation mode Aggressive: Disabled

Policy threshold variance: 20

Minimum Mask Length: 28

Sampling: off

Minimum Requirement: Met

**Borders:**

**IP address: 10.255.241.11**

**Connection status:**

**CONNECTED**

**(Last Updated 1w4d ago )**

**Interfaces configured:**

**Name:**

**Tunnel10**

**| type: external | Service Provider:**

**MPLS**

**| Status:**

**UP**

**Number of default Channels: 2**

**Name:**

**Tunnel11**

**| type: external | Service Provider:**

**INET**

**| Status:**

**UP**

Number of default Channels: 2

Tunnel if: Tunnel0

Procedure 3

Configure PfR in the

## Branch Data Plane Performance – additional detail

PfRv3 uses Unified Monitor (also called Performance Monitor) to monitor traffic going into WAN links and traffic

coming from the WAN links. It monitors performance metrics per differentiated service code point (DSCP) rather

than monitoring on per-flow or per-prefix basis. When application-based policies are used, the MC will use a

mapping table between the Application Name and the DSCP discovered. This reduces the number of records

significantly. PfRv3 relies on performance data measured on the existing data traffic on all paths whenever it can,

thereby reducing the need of synthetic traffic. Furthermore, the measurement data is not exported unless there

is a violation, which further reduces control traffic and processing of those records.

Performance status will be monitored per DSCP per branch (relevenat DSCPs are defined in PfR templaates). Since PfR already monitors and thresholds according to PfR policy we can leverage those results for purposes of service health. Following is show command that can give us current performance status per DSCP can be viewed using “show domain [name] master traffic-classes dscp” command. See example below showing current performance status = in-policy.

AI: engineering to investigate all possible states so they can be fed in appropriate service health states.

With traffic flowing over the WAN, verify that the PfR traffic classes are controlled in the outbound

direction on **one of the branch MC routers by using the**

**show domain [name] master traffic-classes dscp**

**command.**

This example shows a video call is taking place from remote site RS11 to the HQ location. The traffic class is

controlled, as signified by the Present State row. The INTERACTIVE-VIDEO, with a DSCP of AF41 (34), is in-policy

and using the MPLS path. The traffic class has a valid backup channel, which means the INET path is available if

the primary path falls out of policy.

RS11-2921#

**show domain iwan master traffic-classes dscp af41**

**Dst-Site-Prefix: 10.4.0.0/16 DSCP:**

**af41 [34]**

Traffic class id:304

TC Learned: 00:00:31 ago

Present State:

CONTROLLED

**Current Performance Status:**

**in-policy**

Current Service Provider:

MPLS

since 00:00:01 (hold until 88 sec)

Previous Service Provider: Unknown

BW Used: 416 Kbps

Present WAN interface:

Tunnel10 in Border 10.255.241.11

Present Channel (primary):

312

Backup Channel:

313

Destination Site ID: 10.6.32.251

Class-Sequence in use: 20

Class Name:

INTERACTIVE-VIDEO

using policy

real-time-video

BW Updated: 00:00:01 ago

Reason for Route Change: Uncontrolled to Controlled Transition

# vMS 2.2 Metric

## Usage Metric

Following metric will be monitored for purposes of reporting on usage:

* Aggregate usage per Branch:
  + At Branch BR monitor: input/output packets, bytes and rates for all WAN interfaces
* Per DSCP usage at each Branch BR:
  + For all DSCPs/QoS classes that are part of PfR template monitor per class packets, bytes and rates (this can be obtained from QoS related metric)

## Performance & Availability Metric

In vMS 2.2, in addition to usage metric we will start collecting and presenting additional performance and availability related metric for service and its components.

For some performance metric we will raise TCAs while for others we won’t but we will only present them.

Performance metric need to presented on UI in context of the service or service component that it relates to. Following tables list target performance & availability metric for various iWAN service components in vMS 2.2:

* Overall iWAN Service:
* Hub Service Function:
* Branches Service Function:
  + NONE (besides rolled up status)
  + Branch (metric in context of individual branch):
    - Loss (from Performance Monitoring)
    - Delay (from Performance Monitoring)
    - Jitter (from Performance Monitoring)
    - (part of UI drill down): QoS: Per QoS class number of packets, bytes, rates and queue drops
    - (part of UI drill down): DMVPN: up/down status, throughout
    - AI: engineering team to verify if above is all supported on SME and also provide to PLMs list of all metric supported on SME for other features configured for iWAN (listed in earlier section -.e.g DMVPN, PfR, BGP, etc). PLMs to decide which additional metric should be included as part of operator UI drilldown.
* ISR4k and ASR1k devices:
  + Metric & Threshold/TCA for:
    - CPU 5 Min Average Utilization - Device Average (PPM: Report>Resources>CPU)
    - Memory Pool Utilization - Device Average (PPM: Report>Resources>Memory)
    - Memory Pool Processor Utilization (PPM: Report>Resources>Memory)
    - Memory Pool I/O Utilization (PPM: Report>Resources>Memory)
    - Interface Utilization (PPM: Reports>Transport Statistics > Interface)
  + Metric only (without TCA) for:
    - System Uptime
    - Interface Availability (only data path interfaces)
    - Interface Error Percentage (only data path interfaces)
    - Interface Discards Percentage (only data path interfaces)
    - Interface Bytes (only data path interfaces)
    - Interface packets (only data path interfaces)

Potential other drill down metric that could be included – stretch:

IP Sec:

* + IP Sec tunnel In/Out drops (In/Out packet/octet should be already covered under Usage metric):
    - cipSecGlobalInOctets, cipSecGlobalHcInOctets, cipSecGlobalInOctWraps, cipSecGlobalInPkts, cipSecGlobalOutOctets, cipSecGlobalHcOutOctets, cipSecGlobalOutOctWraps, cipSecGlobalOutPkts, **cipSecGlobalInDrops, cipSecGlobalOutDrops**
    - **No TCAs**
  + Encrypt/Decrypt Stats & Failures: (AI: Review whether stats needed in UI – or just show %)
    - from cipSecGlobalInDecrypts, cipSecGlobalInDecryptFails, cipSecGlobalOutEncrypts, cipSecGlobalOutEncryptsFails)
    - No TCAs
  + Percentage of encrypt/decrypt failures:
    - Calculate from encrypt/decrypt failure metric
    - Include TCA
  + Authentication stats & failures : (AI: Review whether stats needed in UI – or just show %)
    - from cipSecGlobalInAuths, cipSecGlobalInAuthFails, cipSecGlobalOutAuths, cipSecGlobalOutAuthsFails)
    - No TCAs
  + Percentage of authentication failures:
    - Calculate from authentication failure metric
    - Include TCA
  + any other failure stats ??? ( cipSecGlobalProtocolUseFails, cipSecGlobalNoSaFails, cipSecGlobalSysCapFails)

# vMS 2.2 CloudVPN Alarms & Events

**Alarms/Events**

In vMS 2.0 assurance system will not be collecting alarms and events from managed devices.

However, assurance system will be collecting alarms and events from:

* NSO Netconf notifications:
* SME:
  + Service Status Events (these would be alarms generated for service status/health change):
    - Need to be generated for changes in CVPN E2E service as well as sub-services defined in section 3.1.
  + Note that in vMS 2.0 there will be no TCAs for metric since type of metric collected in vMS 2.0 doesn’t require warning an operator upon crossing certain values and doesn’t necessarily indicate the failure

## NSO Alarms & Events

# iWAN Logs

In vMS 2.0 assurance system will be collecting logs and syslogs from all managed devices listed in section 2. In addition logs from following management and underlay components should be collected as well:

* NSO
* ISR4k
* ASR1k – BR
* ASR1k - MC

All collected logs are aggregated and used for fault analysis.

AI: Engineering to investigate set of relevant syslogs and SNMP traps for Target iWAN features. Include investigation on available data for PfR Controllers.

# iWAN Fault Analysis

## Data Sources

CVPN data sources used for fault analysis for CloudVPN service includes following:

* Logs/Syslogs from:
  + ISR4k
  + ASR1k – BR
  + ASR1k - MC
  + NSO
  + ESC
* Events & Alarms from:
  + SME TCAs for service status, device availability and metric TCAs.
  + NSO Netconf notifications
  + ISR4k - if equivalent data not already part of syslog
  + ASR1k - BR - if equivalent data not already part of syslog
  + ASR1k - MC - if equivalent data not already part of syslog

AI: Engineering to investigate set of relevant syslogs and SNMP traps for Target iWAN features. Include investigation on available data for PfR Controllers.

Path through architecture between these source and fault analysis component is described in vMS 2.0 Service Assurance Platform Architecture Spec.

## Service Impact Enrichment

Incident.Moog does not perform service impact analysis, however it can enrich alarms that are generated by tenant dedicated components with service impact information such as impacted tenant and service. It can also enrich situations that are created from such alarms. It does so by leveraging mapping between tenants, services and tenant dedicated resources. This mapping is obtained from the configuration databases/inventory in our case from NSO. Integration with inventory systems for our solution is documented in vMS 2.0 Service Assurance Platform Architecture.

In Incident.Moog there are two fields within situation and alarm that will provide service and tenant impact information. Following is proposal on what content to place within each for CVPN service:

* **Process Impacted** (intent is to indicate technical impact, i.e. information useful for technical personnel):
  + Populate with:
    - For Situation: Superset list of all Component Types from Process Impacted fields of individual alarms that are included in situation.
    - For Individual Alarm: **Component type and their roles (MC vs BR)** for alarms raised on components associated with iWAN service. Component types in this context can be:
      * Control (MC-ASR1k)
        + Optionally sub-component should be included where applicable: e.g. if we have failure of CSR’s interface one would populate this field with CSR ID/name and failed interfaced ID/name, if we have failure of CSR’s VM we would populate with CSR ID/name and failed CSR VM, etc.).
      * Data path (BR-ASR1k, BR-ISR4k)
      * Alarms from SME (TCAs) : enrich with keyword “TCA-devicetype” (e.g. TCA-BR-ISR4k, TCA-BR-ASR1k, TCA-MC-ASR1k, etc.)
* **Service Impacted** (intent is to indicate business impact, i.e. information useful for customer relationship and business personnel):
  + Populate with:
    - For Situation:
      * Superset list of all Service Impacted (or Tenant) fields of individual alarms that are included in situation.
      * If situation includes alarms from multiple tenants include list of all affected tenants
    - For Individual Alarms:
      * Populate with: Tenant and Service Type (e.g. iWAN) & service ID
      * If alarms from components shared by multiple tenants are included enrich with keyword ‘Shared Infrastructure” or “Shared”

Following figures illustrates examples from vMS 1.0 POC with Service Impacted and Process Impacted fields:



