Migrazione da SNMP a telemetria su IOS XR

Sommario

Introduzione

Questo articolo introduce i componenti SNMP (Simple Network Management Protocol) e fornisce una correlazione tra le implementazioni correnti basate sul monitoraggio SNMP nell'approccio MDT (Model Driven Telemetry).

SNMP

SNMP è un protocollo a livello di applicazione che fornisce un formato di messaggio per la comunicazione tra i manager SNMP e gli agenti. L'SNMP fornisce un framework standardizzato e un linguaggio comune utilizzato per il monitoraggio e la gestione dei dispositivi in una rete

Componenti di SNMP

Il framework SNMP ha i seguenti componenti, descritti nelle sezioni seguenti:

- SNMP Manager
- Agente SNMP
- MIB SNMP

SNMP Manager

SNMP Manager è un sistema che controlla e controlla le attività degli host di rete che utilizzano SNMP. Il sistema di gestione più comune è il Network Management System (NMS). Il termine NMS può essere applicato a un dispositivo dedicato utilizzato per la gestione della rete o alle applicazioni utilizzate su tale dispositivo.

Agente SNMP

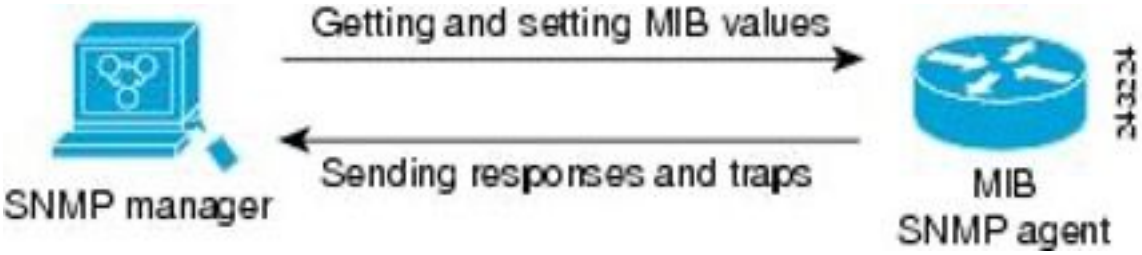
L'agente SNMP è il componente software all'interno di un dispositivo gestito che mantiene i dati per il dispositivo e li segnala, se necessario, alla gestione dei sistemi. L'agente risiede sul dispositivo di routing (router, server di accesso o switch).

MIB SNMP

Un agente SNMP contiene variabili MIB, i cui valori possono essere richiesti o modificati da SNMP Manager tramite le operazioni 'Get' o 'Set'. Un manager può ottenere un valore da un agente o memorizzarne uno in tale agente. L'agente raccoglie i dati dal MIB SNMP, il repository per

informazioni sui parametri dei dispositivi e i dati di rete. L'agente può inoltre rispondere alle richieste del manager di ottenere o impostare dati.

La figura seguente illustra le comunicazioni tra il manager SNMP e l'agente. Un manager invia una richiesta di agente per ottenere e impostare i valori MIB SNMP. L'agente risponde a queste richieste. Indipendentemente da questa interazione, l'agente può inviare al manager notifiche non richieste (trap o informazioni) per notificare al manager le condizioni della rete.



Operazioni SNMP

Le applicazioni SNMP eseguono le seguenti operazioni per recuperare i dati, modificare le variabili oggetto SNMP e inviare le notifiche:

- SNMP Get
- SET SNMP
- Notifiche SNMP

SNMP Get

L'operazione GET di SNMP viene eseguita da un NMS per recuperare le variabili oggetto SNMP. Esistono tre tipi di operazioni GET:

- GET - Recupera l'istanza di oggetto esatta dall'agente SNMP.
- GETNEXT - Recupera la variabile oggetto successiva, che rappresenta un successore lessicografico della variabile specificata.
- GETBULK - Recupera una grande quantità di dati di variabili oggetto, senza la necessità di eseguire ripetutamente operazioni GETNEXT.

SET SNMP

L'operazione SNMP SET viene eseguita da un NMS per modificare il valore di una variabile oggetto.

Notifiche SNMP

Una funzionalità chiave del protocollo SNMP è la capacità di generare notifiche non richieste da un agente SNMP.

Le notifiche non richieste (asincrone) possono essere generate come trap o richieste informate (informate). I trap sono messaggi che avvisano il gestore SNMP (Simple Network Management Protocol) di una condizione della rete. Le informazioni sono trap che includono una richiesta di conferma di ricezione da parte del manager SNMP. Le notifiche possono indicare un'autenticazione utente non corretta, riavvii, la chiusura di una connessione, la perdita di

connessione a un dispositivo adiacente o altri eventi significativi.

I trap sono meno affidabili di quelli informativi perché il ricevitore non invia una conferma quando riceve una trap. Il mittente non sa se la trap è stata ricevuta. Un manager SNMP che riceve un'informazione conferma il messaggio con una unità PDU (Protocol Data Unit) di risposta SNMP. Se il mittente non riceve mai una risposta, l'informazione può essere inviata di nuovo. È quindi più probabile che le informazioni raggiungano la destinazione prevista.

Le trap sono spesso preferite anche se sono meno affidabili perché le informazioni consumano più risorse nel dispositivo e nella rete. A differenza di una trap, che viene scartata non appena inviata, un informatore deve essere tenuto in memoria fino a quando non si riceve una risposta o la richiesta scade. Inoltre, le trap vengono inviate solo una volta, mentre un informatore può essere inviato più volte. I tentativi aumentano il traffico e contribuiscono a un maggiore sovraccarico sulla rete. L'uso di trappole e informazioni richiede un compromesso tra affidabilità e risorse.

MIB e RFC

I moduli MIB (Management Information Base) vengono in genere definiti nei documenti RFC (Request for Comments) inviati all'IETF (Internet Engineering Task Force), un organismo internazionale di normalizzazione. Le RFC sono scritte da singoli individui o gruppi e vengono prese in considerazione dalla Internet Society e dalla comunità Internet nel suo complesso, solitamente con l'intenzione di stabilire uno standard Internet consigliato. Prima di ottenere lo stato RFC, le raccomandazioni vengono pubblicate come documenti Internet Draft (I-D). Le RFC che sono diventate standard consigliati sono anche etichettate come documenti standard (STD). Per ulteriori informazioni sul processo di standardizzazione e sulle attività dell'IETF, visitare il sito Internet della società all'indirizzo http://www.isoc.org. Il testo completo di tutte le RFC, gli I-D e gli STD a cui si fa riferimento nella documentazione Cisco è disponibile sul sito Web dell'IETF all'indirizzo http://www.ietf.org.

L'implementazione Cisco di SNMP utilizza le definizioni delle variabili MIB II descritte nella RFC 1213 e le definizioni delle trap SNMP descritte nella RFC 1215.

Cisco fornisce le proprie estensioni MIB private con ogni sistema. I MIB aziendali Cisco sono conformi alle linee guida descritte nelle RFC pertinenti, a meno che non sia diversamente indicato nella documentazione. I file di definizione del modulo MIB e l'elenco dei MIB supportati su ciascuna piattaforma Cisco sono disponibili sul sito Web MIB di Cisco all'indirizzo Cisco.com.

Versioni di SNMP

Attualmente i dispositivi Cisco supportano le seguenti versioni di SNMP:

- SNMPv1—Simple Network Management Protocol: uno standard Internet completo, definito nella RFC 1157 (la RFC 1157 sostituisce le versioni precedenti pubblicate come RFC 1067 e RFC 1098). La sicurezza è basata sulle stringhe della community.
- SNMPv2c: il framework amministrativo basato su stringhe della community per SNMPv2. SNMPv2c (la "c" è per "community") è un protocollo Internet sperimentale definito nella RFC 1901, RFC 1905 e RFC 1906. SNMPv2c è un aggiornamento delle operazioni di protocollo e dei tipi di dati di SNMPv2p (SNMPv2 classico) e utilizza il modello di sicurezza basato sulla community di SNMPv1.
- SNMPv3—Versione 3 di SNMP. SNMPv3 è un protocollo interoperabile basato su standard definito nelle RFC da 3413 a 3415. L'SNMPv3 fornisce un accesso sicuro ai dispositivi tramite

l'autenticazione e la crittografia dei pacchetti sulla rete.

Le funzioni di sicurezza fornite in SNMPv3 sono le seguenti:

- Integrità dei messaggi: verifica che un pacchetto non sia stato manomesso durante il trasferimento.
- Autenticazione (Authentication) - Determina se il messaggio proviene da un'origine valida.
- Crittografia - Scrambling del contenuto di un pacchetto per impedire che venga appreso da una fonte non autorizzata.

Sia SNMPv1 che SNMPv2c utilizzano una forma di sicurezza basata su community. La comunità dei manager SNMP è in grado di accedere al MIB dell'agente definito da una stringa della community.

Il supporto di SNMPv2c include un meccanismo di recupero in blocco e la segnalazione dettagliata dei messaggi di errore alle stazioni di gestione. Il meccanismo di recupero in blocco supporta il recupero di tabelle e di grandi quantità di informazioni, riducendo al minimo il numero di round trip necessari. Il supporto migliorato della gestione degli errori di SNMPv2c include codici di errore estesi che distinguono i diversi tipi di errore; queste condizioni vengono segnalate tramite un singolo codice di errore in SNMPv1. Sono inoltre riportati i tre tipi di eccezioni seguenti: nessun oggetto, nessuna istanza e fine della visualizzazione MIB.

SNMPv3 è un modello di protezione in cui viene impostata una strategia di autenticazione per un utente e il gruppo in cui risiede l'utente. Un livello di protezione è il livello di protezione consentito all'interno di un modello di protezione. La combinazione di un modello di sicurezza e di un livello di sicurezza determina il meccanismo di sicurezza utilizzato quando si gestisce un pacchetto SNMP.

Sono disponibili tre modelli di sicurezza: SNMPv1, SNMPv2c e SNMPv3. La tabella seguente elenca le combinazioni di modelli e livelli di sicurezza e il relativo significato.

Modello	Livello	Autenticazione	Crittografia	Cosa succede
v1	noAuthNoPriv	Stringa della community	No	Utilizza una stringa della community per l'autenticazione.
v2c	noAuthNoPriv	Stringa della community	No	Utilizza una stringa della community per l'autenticazione.
v3	noAuthNoPriv	Username	No	Utilizza un nome utente corrispondente per l'autenticazione.
v3	authNoPriv	MD5 (Message Digest 5) o SHA (Secure Hash Algorithm)	No	Fornisce l'autenticazione basata sugli algoritmi HM MD5 o HMAC-SHA.
v3	authPriv	MD5 o SHA	DES (Data Encryption Standard)	Fornisce l'autenticazione basata sugli algoritmi HM MD5 o HMAC-SHA. Crittografia DES a 56 bit oltre all'autenticazione basata sullo standard CBC-DES (DES-56).

Ènecessario implementare un agente SNMP per utilizzare la versione di SNMP supportata dalla stazione di gestione. Un agente può comunicare con più manager.

L'SNMPv3 supporta le RFC da 1901 a 1908, 2104, 2206, 2213, 2214 e da 2271 a 2275. Per ulteriori informazioni su SNMPv3, vedere la RFC 2570, Introduction to Version 3 of the Internet-standard Network Management Framework (questo non è un documento sugli standard).

Modelli Yang

I modelli Yang rappresentano un'astrazione ad albero di una specifica funzionalità o caratteristiche hardware di un sistema. Negli elementi di rete, un modello Yang potrebbe rappresentare un protocollo di routing, array interni di sensori fisici. La lingua e la terminologia YANG sono descritte nella RFC 6020 e successivamente aggiornate nella RFC 7950. In un modello di alto livello, i dati che rappresentano la struttura principale vengono organizzati in sottomoduli e contenitori correlati a un elenco di sottonodi. Di seguito vengono illustrati vari tipi di nodi.

Un nodo foglia contiene dati semplici come un numero intero o una stringa. Ha esattamente un valore di un particolare tipo e nessun nodo figlio.

```
leaf nome-host {
        tipo string;
        descrizione "Hostname for this system";
      }
```

Un elenco foglia è una sequenza di nodi foglia con esattamente un valore di un determinato tipo per ogni foglia.

```
leaf-list domain-search {
       tipo string;
       descrizione "Elenco dei nomi di dominio da cercare";
    }
```

Un nodo contenitore viene utilizzato per raggruppare nodi correlati in una sottostruttura. Un contenitore ha solo nodi figlio e nessun valore. Un contenitore può contenere un numero qualsiasi di nodi figlio di qualsiasi tipo (inclusi fogli, elenchi, contenitori ed elenchi foglia).

```
sistema contenitore {
       login contenitore {
          messaggio foglia {
             tipo string;
             descrizione
                "Messaggio inviato all'inizio della sessione di accesso";
          }
       }
   }
```

Un elenco definisce una sequenza di voci. Ogni voce è simile a una struttura o a un'istanza di record ed è identificata in modo univoco dai valori dei relativi fogli chiave. Un elenco può definire più fogli di chiave e può contenere un numero qualsiasi di nodi figlio di qualsiasi tipo (inclusi fogli, elenchi, contenitori e così via).

Infine, un modello di esempio che associa tutti questi tipi di nota avrà l'aspetto illustrato nell'esempio seguente:

```
## Contents of "example-system.yang" module example-system { yang-version 1.1; namespace
"urn:example:system"; prefix "sys"; organization "Example Inc."; contact "joe@example.com";
description "The module for entities implementing the Example system."; revision 2007-06-09 {
description "Initial revision."; } container system { leaf host-name { type string; description
"Hostname for this system."; } leaf-list domain-search { type string; description "List of
```

```
domain names to search."; } container login { leaf message { type string; description "Message
given at start of login session."; } list user { key "name"; leaf name { type string; } leaf
full-name { type string; } leaf class { type string; } } } } }
```

Tuttavia, la lingua Yang utilizzata nei modelli Yang non indica l'organizzazione dei dati in contenitori/elenchi/fogli. Per questo motivo una determinata funzione di un elemento di rete potrebbe essere rappresentata con diversi modelli Yang. Questa sfida è stata affrontata con i seguenti tipi di modelli Yang:

- Modelli OpenConfig
- Modelli nativi

Modelli OpenConfig

I modelli OpenConfig sono stati sviluppati utilizzando un'organizzazione di fornitori agnostici per il modello che rappresenta una funzionalità specifica, il vantaggio di questo approccio è che un NMS potrebbe utilizzare questi modelli per interagire con gli elementi di rete in ambienti multi-vendor o anche multipiattaforma.

Come afferma il nome, questi modelli sono aperti e sono disponibili al pubblico per l'ispezione su repository come github su questo link:

https://github.com/openconfig/public/tree/master/release/models

Ad esempio, è possibile trovare un modello openconfig per Border Gateway Protocol (BGP), un altro per Link Aggregation Control Protocol (LACP) e un altro per ISIS, con un modello specifico diverso. Nel caso di BGP è possibile trovare un modello per gli errori BGP, un altro per le policy BGP e così via. I modelli possono essere correlati, e alcuni modelli possono chiamare un altro pacchetto yang. Ad esempio, openconfig-bgp-neighbor.yang appartiene a openconfig-bgp.yang:

```
module openconfig-bgp { yang-version "1"; ## namespace namespace
"http://openconfig.net/yang/bgp"; prefix "oc-bgp"; ## import some basic inet types import
openconfig-extensions { prefix oc-ext; } import openconfig-rib-bgp { prefix oc-bgprib; } ##
Include the OpenConfig BGP submodules ## Common: defines the groupings that are common across
more than ## one context (where contexts are neighbor, group, global) include openconfig-bgp-
common; ## Multiprotocol: defines the groupings that are common across more ## than one context,
and relate to Multiprotocol include openconfig-bgp-common-multiprotocol; ## Structure: defines
groupings that are shared but are solely used for ## structural reasons. include openconfig-bgp-
common-structure; ## Include peer-group/neighbor/global - these define the groupings ## that are
specific to one context include openconfig-bgp-peer-group; include openconfig-bgp-neighbor;
include openconfig-bgp-global;
```

In sintesi, i modelli OpenConfig sono orientati ai protocolli comuni a tutte le piattaforme, come le funzionalità standardizzate IETF o RFC.

Modelli nativi

Al contrario, i modelli nativi sono modelli orientati ai fornitori che coprono le strutture di profondità specifiche di una particolare piattaforma. Ad esempio, modelli che raggruppano i sensori dei valori fisici all'interno di un elemento di rete come tensioni, temperature, contatori ASIC, contatori Fabric e così via. Poiché dipendono dalla piattaforma, è comune trovare modelli specifici per NCS6K, ASR9K o Cisco 8000.

Come i modelli OpenConfig, anche i modelli nativi sono disponibili nel repository Github:

https://github.com/YangModels/yang/tree/master/vendor/cisco/xr

Poiché questi modelli tendono ad essere molto più specifici e completi rispetto ai modelli OpenConfig, sono legati a versioni software specifiche e soggetti a modifiche tra le versioni software.

Sono disponibili due categorie principali per i modelli nativi:

- Modelli "Oper", utilizzati per recuperare informazioni da un elemento.

Ad esempio, Cisco-IOS-XR-eigrp-oper.yang

- Modelli "Cfg", utilizzati per configurare un elemento di rete

Ad esempio, Cisco-IOS-XR-eigrp-cfg.yang

In termini generali, la telemetria guidata dal modello utilizza modelli "oper" per trasmettere i dati dall'infrastruttura e NMS come NSO utilizza modelli "cfg" per apportare modifiche alla configurazione sugli elementi di rete.

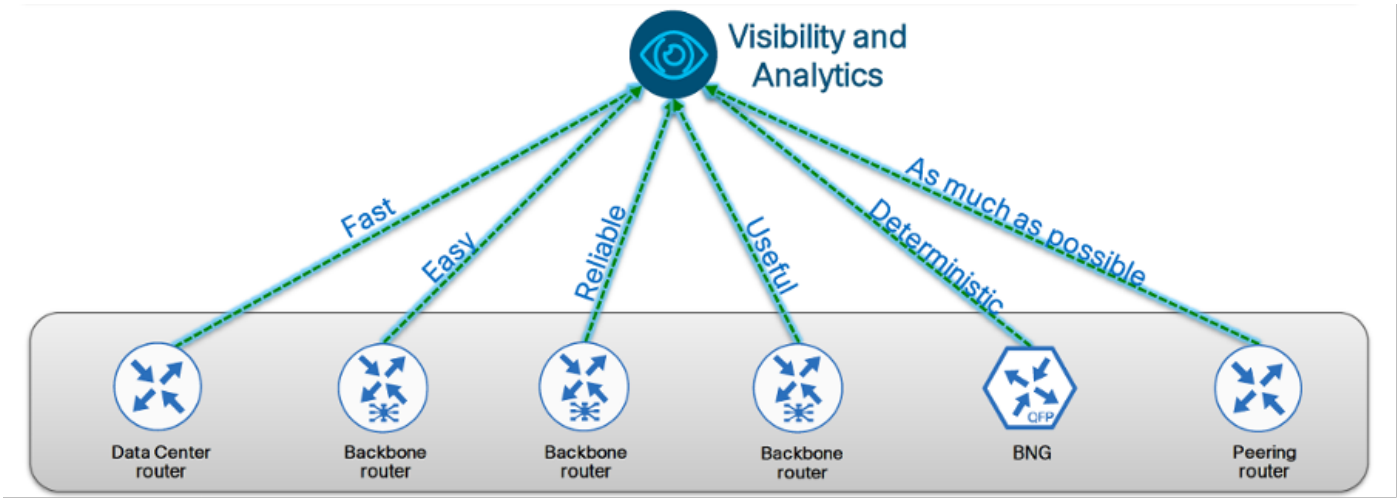
I modelli Yang nativi e OpenConfig sono presenti sul software XR nella cartella /pkg/yang e possono essere elencati per scoprire se un modello Yang è disponibile su una piattaforma. Questo esempio è per XRrv9k con cXR 6.4.2:

```
RP/0/RP0/CPU0:xrv9k1#run ls /pkg/yang | isis grep
mar 22 set 14:21:27.471 CLST
Cisco-IOS-XR-clns-isis-cfg.yang
Cisco-IOS-XR-clns-isis-datatypes.yang
Cisco-IOS-XR-clns-isis-oper-sub1.yang
Cisco-IOS-XR-clns-isis-oper-sub2.yang
Cisco-IOS-XR-clns-isis-oper-sub3.yang
Cisco-IOS-XR-clns-isis-oper.yang
Cisco-IOS-XR-isis-act.yang
openconfig-isis-lsdb-types.yang
openconfig-isis-lsp.yang
openconfig-isis-policy.yang
openconfig-isis-routing.yang
openconfig-isis-types.yang
openconfig-isis.yang
RP/0/RP0/CPU0:xrv9k1#
```

Telemetria

La telemetria è un processo che consente di raccogliere informazioni da diversi elementi remoti in una posizione centrale che aggrega la visibilità e il livello di analisi.

Negli ambienti di rete, i dati potrebbero essere prodotti da ogni elemento della rete, router, switch tra gli altri e le informazioni potrebbero essere relative a un set molto grande di protocolli specifici, contatori delle prestazioni o misure da sensori fisici.



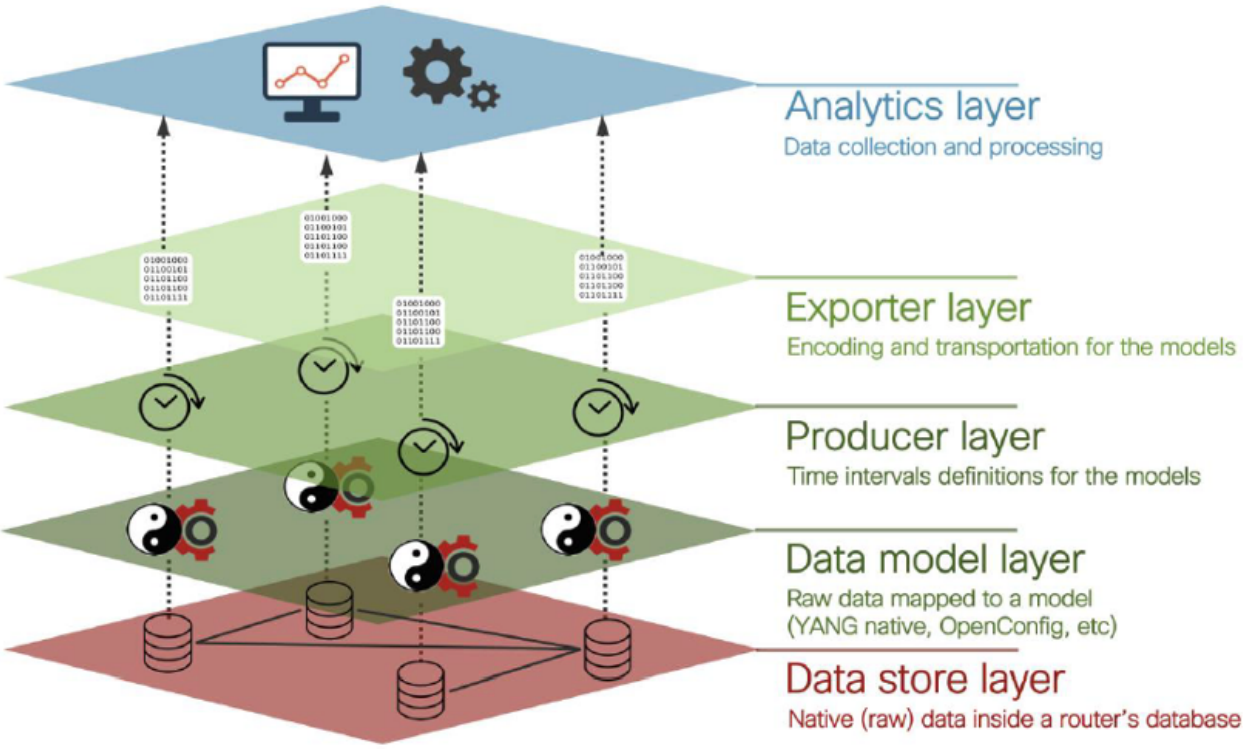
In generale, le funzioni Visibility and Analytics si trovano in punti centrali nelle reti, lo streaming delle informazioni telemetriche è fatto utilizzando meccanismi di trasporto di rete, quindi le informazioni telemetriche dovrebbero essere il più possibile veloci permettendo la scalabilità.

A differenza dei meccanismi legacy di SNMP, la telemetria utilizza un paradigma Push, in cui la rete deve disporre dello streaming dei propri dati senza essere sottoposta a polling a intervalli regolari, che è la caratteristica principale del monitoraggio basato su SNMP. Questa disposizione viene spesso definita sottoscrizione e si basa su un insieme di variabili da monitorare, l'intervallo regolare per l'intervallo di campionamento per la raccolta dei dati e il sistema remoto per l'invio di questi dati attraverso la rete.

Telemetria guidata dal modello

MDT è stato definito per la telemetria guidata da modello e, come dice il nome, è basato su modelli Yang. Ogni aspetto delle apparecchiature di rete potrebbe essere rappresentato con i modelli Yang, ad esempio tabella dei vicini OSPF, RIB o sensori di temperatura per ogni componente dei sistemi modulari.

Per quanto riguarda l'architettura MDT, può essere suddivisa nei seguenti livelli:



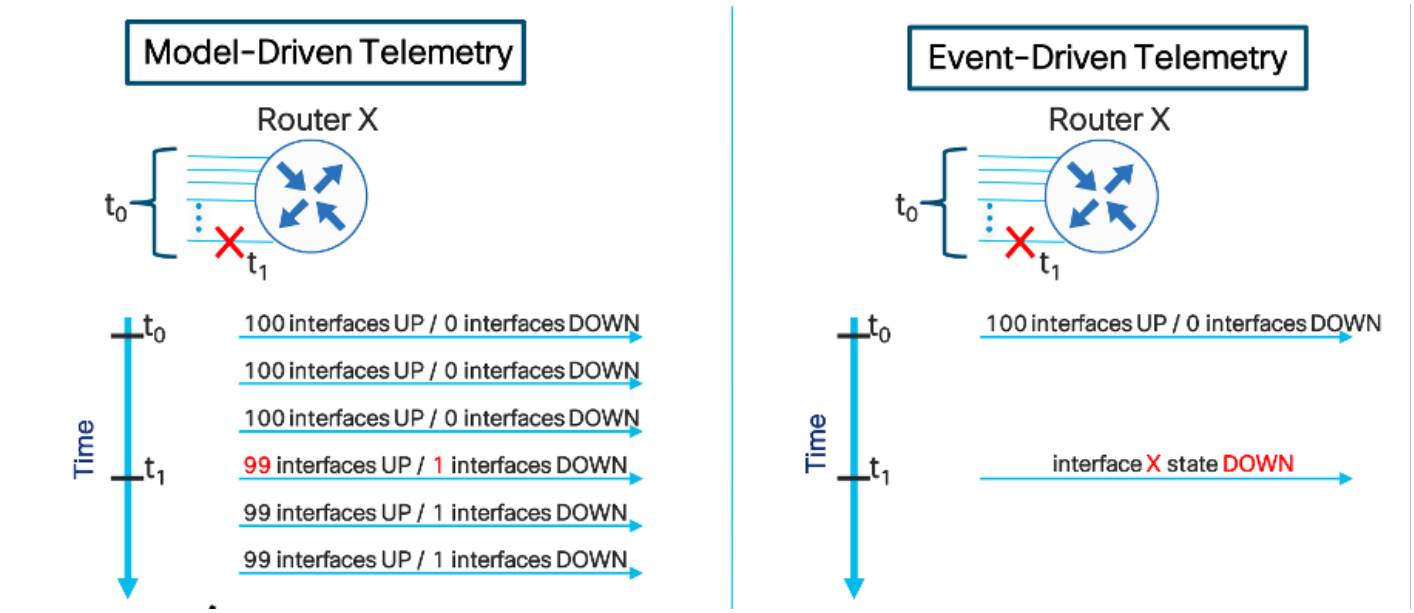
Nota: Per quanto riguarda il livello del produttore, nella telemetria guidata dal modello è presente una definizione dell'intervallo di campionamento che controlla la frequenza con cui il dispositivo consulta il database interno per i dati raw e organizza questi dati nel livello del modello dati.

La sottoscrizione di telemetria definisce anche quali modelli e con contenitori/percorso produrrebbero i dati da inviare in streaming nel livello di analisi. Questa definizione avrebbe un impatto sulle informazioni rilevanti per gli scopi aziendali. La definizione MDT di questo percorso-sensore sarebbe analogica per definire l'OID da recuperare tramite SNMP, poiché entrambe le tecnologie producono dati strutturati a una frequenza di campionamento definita.

Telemetria basata su eventi

EDT è l'acronimo di Event Driven Telemetry ed è anche basato sui modelli Yang per la struttura. La differenza principale consiste nel fatto che il trigger per la raccolta e il flusso di dati non è un intervallo regolare, ma un evento specifico, ad esempio lo scambio di soglie, gli eventi di collegamento, gli errori hardware e così via.

Di seguito viene illustrato un confronto tra un evento e la telemetria guidata dal modello e la telemetria guidata dagli eventi:



Suggerimento: Nella figura vengono illustrati i messaggi ridondanti che utilizzano MDT, ma solo i messaggi che rappresentano le modifiche mediante EDT.

Trasporto

La telemetria deve essere il più possibile affidabile, quindi ha senso utilizzare il trasporto basato su TCP (Transmission Control Protocol) per l'utilizzo di socket orientati alla sessione tra l'infrastruttura e il livello Analytics, che dovrebbe implementare i raccoglitori per la creazione della sessione.

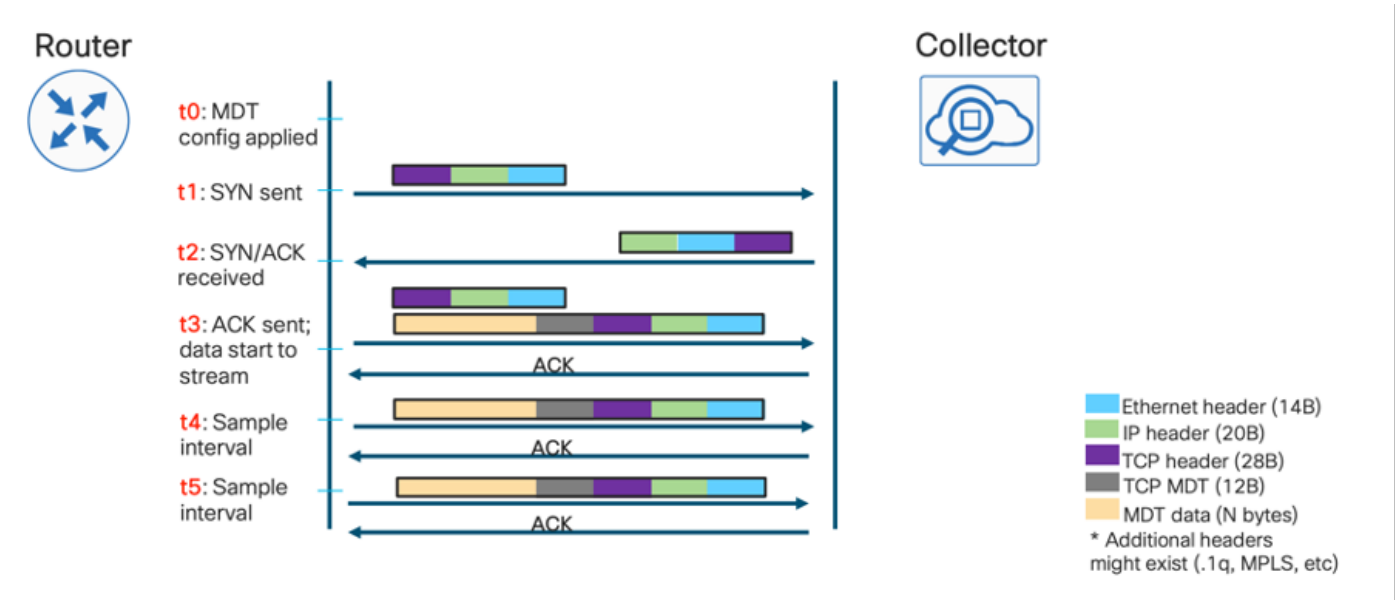
Esistono due approcci principali quando si utilizza la telemetria, che differiscono tra loro nel flusso iniziale di handshake a tre vie.

Nota: Nella modalità Dial-Out, la configurazione della sessione viene avviata sul lato infrastruttura, il che implica che i sensori di interesse devono essere configurati sugli elementi della rete. In modalità Constrast, l'approccio Dial-In consente una configurazione più leggera sugli elementi di rete, poiché il raccoglitore deve richiedere percorsi di sensore specifici in fase di configurazione.

TCP

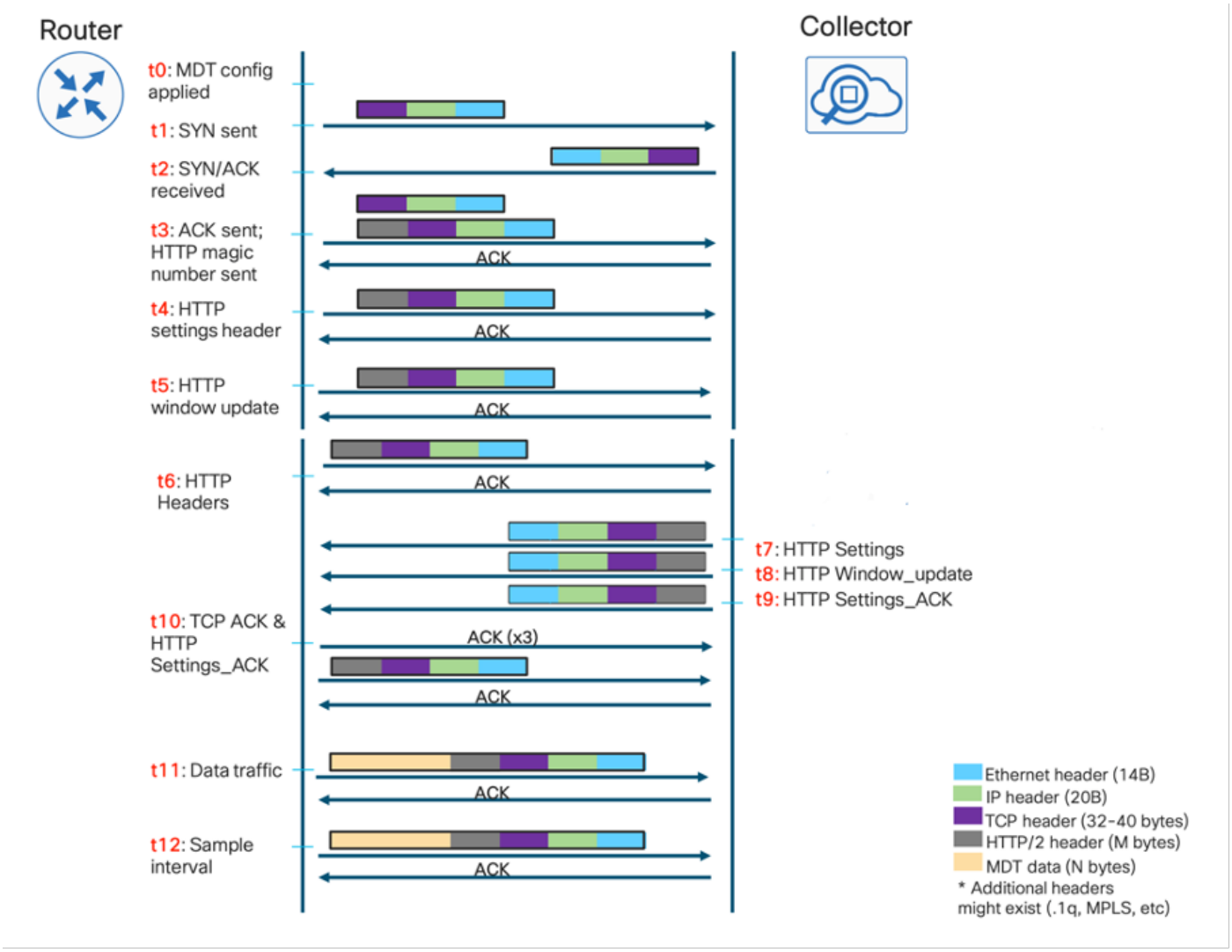
Il protocollo TCP è il modo più semplice per stabilire una sessione orientata alla connessione tra un elemento di rete e un collettore di telemetria e il flusso di dati inizia da un router all'altro, che a

sua volta restituisce il pacchetto al router per motivi di affidabilità:



RPC

Poiché Google Protocol RPC (gRPC) funziona su Hypertext Transfer Protocol/2 (HTTP/2), la sessione stessa dovrebbe formarsi al momento della configurazione e consentire il controllo della velocità dal lato dell'agente di raccolta in modo nativo:



gNMI/gNOI

gRPC Network Management Interface (gNMI) è il protocollo di gestione di rete gRPC sviluppato da Google. gNMI fornisce il meccanismo per installare, modificare ed eliminare la configurazione dei dispositivi di rete, nonché per visualizzare i dati operativi. Il contenuto fornito tramite gNMI può essere modellato utilizzando YANG.

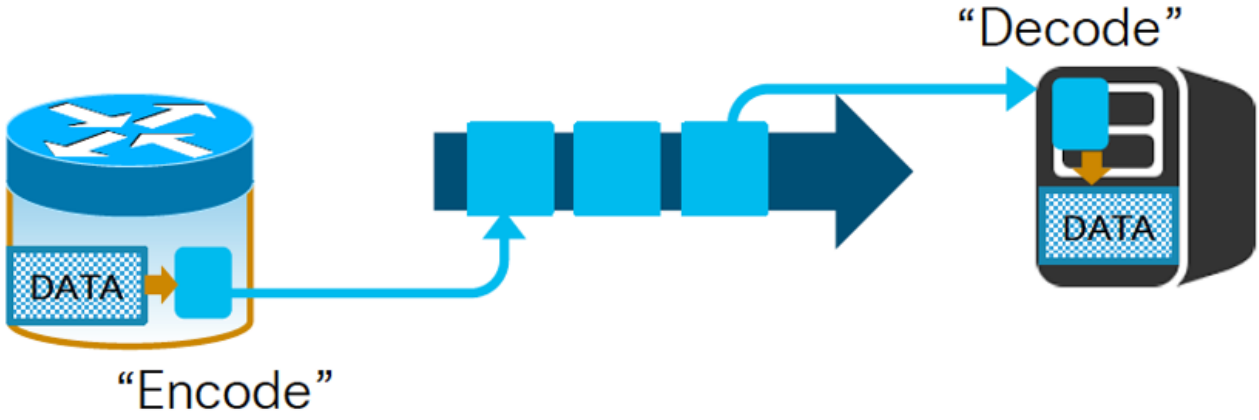
gNMI utilizza gRPC-HTTP/2 per configurare una connessione e fornisce un canale bidirezionale tra gli elementi di rete e un NMS che può anche essere un agente di raccolta di telemetria, ma fornisce anche un'interfaccia per gestire i dispositivi.

Tra le operazioni supportate da questo protocollo, è possibile trovare gNMI Get, gNMI Set che restituiscono le informazioni richieste, i messaggi di riuscita o di errore.

gRPC Network Operations Interface (gNOI) è una raccolta di microservizi che utilizza lo stesso canale di comunicazione di gNMI ma consente operazioni generiche non correlate alla configurazione stessa, ad esempio ping, riavvio, modifica dei certificati SSL, cancellazione e così via.

Codifica

I modelli Yang definiscono la struttura dei dati, la relativa gerarchia e il tipo di ogni nodo foglia in esso contenuto. Tuttavia, la modellazione non indica la modalità di serializzazione dei dati. Questo processo regola la conversione dai dati strutturati in un flusso di byte da inviare tramite la connessione TCP (TCP raw, gRPC, gNMI, ecc.).



Nota: Questo processo dovrebbe essere implementato con un meccanismo equivalente nell'elemento di rete che dovrebbe codificare i dati e l'agente di raccolta dovrebbe decodificare tali dati.

JSON

Il primo meccanismo di codifica è il formato JSON (JavaScript Object Notation) nativo, noto ma orientato all'uomo, in quanto ogni chiave è rappresentata come stringa, il che non è efficiente in termini di dimensioni del messaggio. Il vantaggio principale dell'utilizzo di JSON è la facilità di analisi e la possibilità di leggere il testo come nell'esempio seguente:

{ “node_id_str":"test-IOSXR ", "subscription_id_str":" if_rate", "encoding_path":"Cisco-IOS-XR-infra-statsdoper:infra-statistics/interfaces/interface/latest/datarate", "collection_id":49, "collection_start_time":1510716302467, "msg_timestamp":1510716302479, "data_json": [{ "timestamp":1510716282334, "keys":{ "interface-name":"Null0” }, "content":{ "input-data-rate":0, "input-packet-rate":0, "output-data-rate":0, "output-packet-rate":0, <> { "timestamp": 1510716282344, "keys":{ "interface-name":"GigabitEthernet0/0/0/0” }, "content":{ "input-data-rate":8, "input-packet-rate":1, "output-data-rate":2, "output-packet-rate":0, <> "collection_end_time":1510716302372 }

GPB-KV

Il formato di codifica Google Protocol Buffers-Key Value (GPB-KV) è anche chiamato GPB autodescrittivo perché fa uso di buffer di protocollo per fare uso di messaggi che puntano a elementi particolari sui modelli Yang. Ciò implica che è necessario un solo file .proto per codificare/decodificare gli scopi, e le chiavi stesse dai dati sono in stringhe autodescritte.

node_id_str: “test-IOSXR" subscription_id_str: ”if_rate" encoding_path: "Cisco-IOS-XR-infra-statsd-oper:infrastatistics/interfaces/interface/latest/data-rate" collection_id: 3 collection_start_time: 1485793813366 msg_timestamp: 1485793813366 data_gpbkv { timestamp: 1485793813374 fields { name: "keys" fields { name: "interface-name" string_value: "Null0" } } fields { name: "content" fields { name: "input-data-rate" 8: 0 } fields { name: "input-packet-rate" 8: 0 } fields { name: "output-data-rate" 8: 0 } fields { name: "output-packet-rate" 8: 0 } <> data_gpbkv { timestamp: 1485793813389 fields { name: "keys" fields { name: "interface-name" string_value: "GigabitEthernet0/0/0/0" } } fields { name: "content" fields { name: "input-data-rate" 8: 8 } fields { name: "input-packet-rate" 8: 1 } fields { name: "output-data-rate" 8: 2 } fields { name: "output-packet-rate" 8: 0 } <> } ... collection_end_time: 1485793813405

GPB

Infine, Google Protocol Buffers (GPB), chiamato anche compact GPB, porta questo approccio un passo avanti e richiede file .proto per mappare ogni chiave della struttura rendendola molto più efficiente in termini di dimensioni del messaggio poiché tutto è inviato come valori binari. Tuttavia, lo svantaggio è la necessità di compilare ogni file .proto associato a ogni modello Yang supportato da infrastruttura/collector.

node_id_str: ”test-IOSXR" subscription_id_str: ”if_rate" encoding_path: "Cisco-IOS-XR-infra-statsdoper:infrastatistics/interfaces/interface/latest/data-rate" collection_id: 5 collection_start_time: 1485794640452 msg_timestamp: 1485794640452 data_gpb { row { timestamp: 1485794640459 keys: "\n\005Null0" content: "\220\003\000\230\003\000\240\003\000\250\0 03\000\260\003\000\270\003\000\300\003\000\ 310\003\000\320\003\000\330\003\t\340\003\00 0\350\003\000\360\003\377\001" } row { timestamp: 1485794640469 keys: "\n\026GigabitEthernet0/0/0/0" content: "\220\003\010\230\003\001\240\003\002\250\0 03\000\260\003\000\270\003\000\300\003\000\ 310\003\000\320\003\300\204=\330\003\000\34 0\003\000\350\003\000\360\003\377\001" } collection_end_time: 1485794640480

Configurazione di MDT in IOS XR

I componenti principali utilizzati nello streaming dei dati di telemetria basati su modelli sono:

- Sessione
- Percorso sensore
- Abbonamento

- Trasporto e codifica

Le opzioni della sessione possono essere Dial-in o Dial-out, come descritto in precedenza. Per

compilare la configurazione in IOS XR.

Modalità Dial-Out

in modalità dial-out, il router avvia una sessione sulle destinazioni basate sulla sottoscrizione. il processo deve includere i passi riportati di seguito.

- Crea un gruppo di destinazione
- Crea un gruppo di sensori
- Crea sottoscrizione
- Convalida configurazione chiamate in uscita

Per creare un gruppo di destinazione, è necessario conoscere l'indirizzo IPv4 (Internet Protocol Version 4) / IPv6 (Internet Protocol Version 6) dell'agente di raccolta e la porta che servirebbe l'applicazione. Inoltre, è necessario specificare il protocollo e la codifica da concordare sul dispositivo di rete e sull'agente di raccolta.

Infine, potrebbe essere necessario specificare il VRF (Virtual Routing and Forwarding) utilizzato per comunicare all'indirizzo di rete dell'agente di raccolta.

Viene quindi presentato un esempio di configurazione Dial-Out:

```
basato su modelli di telemetria
 gruppo di destinazione DG1
  vrf MGMT
  porta 5432 della famiglia di indirizzi ipv4 192.168.122.20
   codifica gpb autodescrittivo
   protocol tcp
  !
 !
```

Le opzioni di codifica sono illustrate di seguito:

```
RP/0/RP0/CPU0:C8000-1(config-model-driven-dest-addr)#encoding ?
  codifica GPB gpb
  codifica JSON json
  autodescrittivo-gpb Codifica GPB autodescrittiva }Nota anche come GPB-KV
RP/0/RP0/CPU0:C8000-1(config-model-driven-dest-addr)#encoding
```

Le opzioni dei protocolli:

```
RP/0/RP0/CPU0:C8000-1(config-model-driven-dest-addr)#protocol ?
  grpc gRPC
  TCP tcp
  UDP udp
RP/0/RP0/CPU0:C800-1(config-model-driven-dest-addr)#protocol grpc ?
  compressione messaggi gzip gRPC gzip
  no-tls No TLS
  tls-hostname Nome host TLS
  <cr>
RP/0/RP0/CPU0:C800-1(config-model-driven-dest-addr)#protocol tcp ?
  <cr>
RP/0/RP0/CPU0:C8000-1(config-model-driven-dest-addr)#protocol udp ?
  packetsize Dimensione pacchetto UDP
  <cr>
RP/0/RP0/CPU0:C800-1(config-model-driven-dest-addr)#protocol udp
```

Il protocollo TCP è semplice e richiede solo le impostazioni della porta collegate all'indirizzo IPv4/IPv6. Il protocollo UDP (User Datagram Protocol), al contrario, è senza connessione, quindi lo stato del gruppo di destinazione è sempre attivo.

La compressione in gRPC può essere ottenuta utilizzando la parola chiave ***gzip*** opzionale. Per impostazione predefinita, gRPC utilizza il protocollo TLS, quindi per questo utilizzo è necessario

installare un certificato localmente sul router. Questo comportamento può essere sostituito dalla configurazione della parola chiave ***no-tls***. Infine, è possibile specificare un nome host diverso ai fini del certificato utilizzando la parola chiave ***tls-hostname***.

In seguito, la sezione del gruppo di sensori dovrebbe essere aggiunto elencando i percorsi dei sensori del nostro interesse. Questa sezione è semplice, ma è importante sapere che il percorso del sensore stesso consente il filtraggio per ottimizzare diverse risorse come la CPU (Central Processing Unit) e la larghezza di banda.

```
basato su modelli di telemetria
 gruppo di sensori SG1
  percorso-sensore Cisco-IOS-XR-wdsysmon-fd-oper:monitoraggio-sistema/utilizzo-cpu
  sensor-path Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface[interface-name='Mgmt*']/data-rate
 !
!
```

Nota: Il formato necessario per un percorso del sensore è <nome-modello>:<percorso-contenitore>

Questo documento presenta la mappatura dal monitoraggio basato su SNMP utilizzando OID che rappresenta "foglie" in questo approccio legacy nei modelli YANG, rappresentati con XPATH che corrisponde alle stesse "foglie".

La fase di configurazione finale dovrebbe essere la configurazione di una sottoscrizione, che collega il gruppo di sensori con una cadenza per lo streaming telemetrico verso un gruppo di destinazione.

```
basato su modelli di telemetria
 sottoscrizione SU1
  sensor-group-id SG1 sample-interval 5000
  destination-id DG1
 !
!
```

In questo esempio viene utilizzato un intervallo di campionamento di 5000 millisecondi (5 secondi) relativo alla fine della raccolta precedente. Per modificare questo comportamento, è possibile modificare la parola chiave ***sample-interval*** con l'opzione ***strict-timer***.

Per la verifica, è possibile utilizzare il seguente comando relativo allo stato della sottoscrizione. Questo metodo permette di coprire anche le informazioni sui gruppi di sensori e sui gruppi di destinazione.

```
RP/0/RP0/CPU0:C8000-1#sh sottoscrizione su1 basata sul modello di telemetria
mercoledì 18 novembre 15:38:01.397 UTC
Sottoscrizione:  SU1
—
  State:       ATTIVA
  Gruppi di sensori:
  ID: SG1
    Intervallo di campionamento:      5000 ms
    Intervallo heartbeat:   N/D
    Percorso sensore:          Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface[interface-name='Mgmt*']/data-rate
    Stato percorso sensore:    Risolto
    Percorso sensore:          Cisco-IOS-XR-wdsysmon-fd-oper:monitoraggio del sistema/utilizzo della CPU
    Stato percorso sensore:    Risolto
  Gruppi di destinazione:
  ID gruppo: DG1
    IP di destinazione:       192.168.122.10
    Porta di destinazione:     5432
    Vrf Di Destinazione:      MGMT(0x60000001)
    Codifica:             gpb autodescrittivo
    Trasporto:            tcp
    State:                Active
    TLS:                  Falso
    Totale byte inviati:     636284346
```

```
  Totale pacchetti inviati:  4189
  Ora ultimo invio:      2020-11-18 15:37:58,1700077650 +0000
 Gruppi di raccolta:
 —
  ID: 9
  Intervallo di campionamento:     5000 ms
  Intervallo heartbeat:  N/D
  Heartbeat sempre:    Falso
  Codifica:            gpb autodescrittivo
  N. raccolta:   1407
  Ora raccolta:     Min:    4 ms max   13 ms
  Tempo totale:          Min:    8 ms medio:   10 ms max:   20 ms
  Totale rinviati:      0
  Totale errori di invio:   0
  Totale rilasci invio:    0
  Totale altri errori:  0
  Nessuna istanza di dati:   1407
  Inizio ultima raccolta:2020-11-18 15:37:57.1699545994 +0000
  Fine ultima raccolta:  2020-11-18 15:37:57,169955589 +0000
  Percorso sensore:         Cisco-IOS-XR-infra-statsd-oper:infra-statistiche/interfacce/interfaccia/velocità dei dati
  ID: 10
  Intervallo di campionamento:     5000 ms
  Intervallo heartbeat:  N/D
  Heartbeat sempre:    Falso
  Codifica:            gpb autodescrittivo
  N. raccolta:   1391
  Ora raccolta:     Min:  178 ms max:  473 ms
  Tempo totale:          Min:  247 ms medio:  283 ms max:  559 ms
  Totale rinviati:      0
  Totale errori di invio:   0
  Totale rilasci invio:    0
  Totale altri errori:  0
  Nessuna istanza di dati:   0
  Inizio ultima raccolta:2020-11-18 15:37:58.1699805906 +0000
  Fine ultima raccolta:  2020-11-18 15:37:58,1700078415 +0000
  Percorso sensore:         Cisco-IOS-XR-wdsysmon-fd-oper:monitoraggio del sistema/utilizzo della CPU
RP/0/RP0/CPU0:C8000-1#
```

Modalità chiamata in ingresso

In modalità Dial In, il raccoglitore avvia la connessione agli elementi di rete. L'agente di raccolta deve quindi indicare l'interesse a creare una sottoscrizione.

La configurazione prevede i passi riportati di seguito.

- Abilita servizio RPC
- Imposta gruppi di sensori
- Verifica

Per abilitare il servizio RPC, viene visualizzata la configurazione seguente:

```
!
grpc
 vrf MGMT
 porta 57400
 no-tls
 address-family dual
!
```

Le opzioni sono semplici, inclusi il VRF e la porta TCP. Per impostazione predefinita, gRPC utilizza TLS ma può essere disabilitato con la parola chiave ***no-tls***. Infine, l'opzione ***address-family dual*** consente la connessione tramite IPv4 e IPv6.

Successivamente, la connessione remota richiede la definizione di gruppi di sensori localmente, che verranno utilizzati dall'agente di raccolta in seguito per definire una sottoscrizione.

```
basato su modelli di telemetria
 gruppo di sensori SG3
  percorso-sensore Cisco-IOS-XR-wdsysmon-fd-oper:monitoraggio-sistema/utilizzo-cpu
  sensor-path Cisco-IOS-XR-fib-common-oper:fib-statistics/nodes/node/drops
 !
!
```

A questo punto, la configurazione per la modalità dial-in è completa e l'agente di raccolta dati stesso può effettuare una sottoscrizione al router utilizzando gRPC. Per la verifica, è possibile utilizzare lo stesso approccio utilizzato nella modalità dial-out:

```
RP/0/RP0/CPU0:C8000-1#sh sottoscrizione guidata dal modello di telemetria anx-1605878175837
Venerdì 20 nov. 13:58:37.894 UTC
Sottoscrizione:  anx-1605878175837
—
  State:       ATTIVA
  Gruppi di sensori:
  ID: SG3
    Intervallo di campionamento:      15000 ms
    Intervallo heartbeat:   N/D
    Percorso sensore:          Cisco-IOS-XR-wdsysmon-fd-oper:monitoraggio del sistema/utilizzo della CPU
    Stato percorso sensore:    Risolto
    Percorso sensore:          Cisco-IOS-XR-fib-common-oper:fib-statistics/nodes/node/drops
    Stato percorso sensore:    Risolto
  Gruppi di destinazione:
  ID gruppo: DialIn_1003
    IP di destinazione:       192.168.122.10
    Porta di destinazione:     46974
    Compressione:          gzip
    Codifica:             json
    Trasporto:             dialin
    State:                Active
    TLS:                  Falso
    Totale byte inviati:     71000035
    Totale pacchetti inviati:   509
    Ora ultimo invio:       2020-11-20 13:58:32,1030932699 +0000
  Gruppi di raccolta:
  —
    ID: 5
    Intervallo di campionamento:      15000 ms
    Intervallo heartbeat:   N/D
    Heartbeat sempre:     Falso
    Codifica:             json
    N. raccolta:    170
    Ora raccolta:      Min:   273 ms max:   640 ms
    Tempo totale:           Min:   276 ms medio:   390 ms max:   643 ms
    Totale rinviati:       0
    Totale errori di invio:    0
    Totale rilasci invio:     0
    Totale altri errori:   0
    Nessuna istanza di dati:    0
    Inizio ultima raccolta:2020-11-20 13:58:32.1030283276 +0000
    Fine ultima raccolta:  2020-11-20 13:58:32,1030910008 +0000
    Percorso sensore:          Cisco-IOS-XR-wdsysmon-fd-oper:monitoraggio del sistema/utilizzo della CPU
    ID: 6
    Intervallo di campionamento:      15000 ms
    Intervallo heartbeat:   N/D
    Heartbeat sempre:     Falso
    Codifica:             json
    N. raccolta:    169
    Ora raccolta:      Min:    Max 15 ms:    33 ms
    Tempo totale:           Min:    17 ms medio:    22 ms max    33 ms
    Totale rinviati:       0
    Totale errori di invio:    0
    Totale rilasci invio:     0
    Totale altri errori:   0
    Nessuna istanza di dati:    0
    Inizio ultima raccolta:2020-11-20 13:58:32.1030910330 +0000
    Fine ultima raccolta:  2020-11-20 13:58:32,1030932787 +0000
    Percorso sensore:          Cisco-IOS-XR-fib-common-oper:fib-statistics/nodes/node/drops
RP/0/RP0/CPU0:C8000-1#
```

Suggerimento: Notare che sul router per la modalità dial-in non sono presenti terminazioni, codifiche, indirizzi IP dell'agente di raccolta o trasporto.

Migrazione da SNMP a MDT

Per eseguire la migrazione dal protocollo SNMP tradizionale al modello di telemetria, è necessario considerare i seguenti aspetti:

- Migrazione MIB in XPATH

- Migrazione trap nella telemetria
- Considerazioni sulla sicurezza

Migrazione MIB in XPATH

A questo scopo, è possibile classificare MIB utilizzando una propria gerarchia che può essere mappata (almeno ad alto livello) a una particolare funzionalità.

MIB BGP4

La tabella seguente rappresenta il nome e il numero OID e l'XPATH corrispondente da configurare nei gruppi di sensori di telemetria basati su modelli correlati alle sessioni peer BGP.

Nome OID	Numero OID	Descrizione OID	XPATH
bgpPeerLastError	1.3.6.1.2.1.15.3.1.14	Ultimo codice di errore e sottocodice rilevato dal peer in questa connessione. Se non si è verificato alcun errore, questo campo è zero. In caso contrario, il primo byte di questa STRINGA a due byte contiene il codice di errore, mentre il secondo byte contiene il sottocodice.	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instan active/default-vrf/neighbo missing-eor-table/neighbor/last-notific error-code
bgpPeerOutUpdates	1.3.6.1.2.1.15.3.1.11	Numero di messaggi BGP UPDATE trasmessi su questa connessione.	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instan active/default-vrf/afs/af/neighbor-af-table/neighbor/update-messages-out
bgpPeerInUpdates	1.3.6.1.2.1.15.3.1.10	Numero di messaggi BGP UPDATE ricevuti su questa connessione.	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instan active/default-vrf/afs/af/neighbor-af-table/neighbor/update-messages-in
VersioneNegoziataPeerBGP	1.3.6.1.2.1.15.3.1.4	Versione negoziata di BGP in esecuzione tra i due peer. Questa voce DEVE essere zero (0) a meno che bgpPeerState non sia in stato openconfirm o stabilito. I valori validi per questo oggetto sono compresi tra 0 e 255.	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instan tance-active/default-vrf/afs/af/neighbor-af-table/neighbor/negotiatio protocol-version
bgpPeerState	1.3.6.1.2.1.15.3.1.2	Stato della connessione peer BGP.	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instan active/default-vrf/afs/af/neighbor-af-table/neighbor/connectio state

bgpPeerRemoteAddr	1.3.6.1.2.1.15.3.1.7	Indirizzo IP remoto del peer BGP della voce.	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance-active/default-vrf/afs/af/neighbor-af-table/neighbor/connection/remote-address
bgpPeerLocalAddr	1.3.6.1.2.1.15.3.1.5	Indirizzo IP locale della connessione BGP della voce.	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance-active/default-vrf/afs/af/neighbor-af-table/neighbor/connection/local-address
bgpPeerFsmEstablishedTime	1.3.6.1.2.1.15.3.1.16	Questo timer indica per quanto tempo (in secondi) il peer è rimasto nello stato stabilito o da quanto tempo il peer è rimasto nello stato stabilito. È impostato su zero quando si configura un nuovo peer o quando si avvia il router.	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance-active/default-vrf/afs/af/neighbor-af-table/neighbor/connection/formed-time
bgpPeerAdminStatus	1.3.6.1.2.1.15.3.1.3	Stato desiderato della connessione BGP. La transizione da 'stop' a 'start' genererà l'evento di avvio manuale BGP. Una transizione da 'start' a 'stop' causerà la generazione dell'evento di arresto manuale BGP. Questo parametro può essere utilizzato per riavviare le connessioni peer BGP. È consigliabile utilizzare l'operatore Care per consentire l'accesso in scrittura a questo oggetto senza un'autenticazione adeguata.	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance-active/default-vrf/afs/af/neighbor-af-table/neighbor/connection/admin-status

CISCO-BGP4-MIB

La tabella seguente rappresenta il nome e il numero OID e l'XPATH corrispondente da configurare nei gruppi di sensori di telemetria basati su modello relativi allo stato della sessione BGP e al prefisso interscambiato.

Nome OID	Numero OID	Descrizione OID	XPATH
cbgpPeer2RemoteAs	1.3.6.1.4.1.9.9.187.1.2.5.1.11	Numero di sistema autonomo remoto ricevuto nel messaggio BGP OPEN.	Cisco-IOS-XR-ipv4-bgp-oper:bgp/instance/instance-active/default-vrf/session/session/remote-as
cbgpPeer2PrevState	1.3.6.1.4.1.9.9.187.1.2.5.1.2	Stato precedente	Cisco-IOS-XR-ipv4-bgp

	9	della connessione peer BGP.	oper:bgp/instance/instan active/default-vrf/afs/af/neighbor-af-table/neighbor/PREVIO connection-state
cbgpPeer2State	1.3.6.1.4.1.9.9.187.1.2.5.1.3	Stato della connessione peer BGP.	Cisco-IOS-XR-ipv4-bgp oper:bgp/instance/instan active/default-vrf/afs/af/neighbor-af-table/neighbor/connecti state
cbgpPeer2LocalAddr	1.3.6.1.4.1.9.9.187.1.2.5.1.6	Indirizzo IP locale della connessione BGP della voce.	Cisco-IOS-XR-ipv4-bgp oper:bgp/instance/instan stance-active/default-vrf/afs/af/neighbor-af-table/neighbor/connecti local-address
cbgpPeer2AdvertisedPrefixes	1.3.6.1.4.1.9.9.187.1.2.8.1.6	Questo contatore viene incrementato quando un prefisso di route appartenente a una famiglia di indirizzi viene annunciato su questa connessione. Viene inizializzato su zero quando la connessione viene sottoposta a un reset a freddo.	Cisco-IOS-XR-ipv4-bgp oper:bgp/instance/instan active/default-vrf/afs/af/neighbor-af-table/neighbor/af-data/prefissi-annunciati
cbgpPeer2AcceptedPrefixes	1.3.6.1.4.1.9.9.187.1.2.8.1.1	Numero di prefissi di route accettati in questa connessione, appartenenti a una famiglia di indirizzi.	Cisco-IOS-XR-ipv4-bgp oper:bgp/instance/instan active/default-vrf/afs/af/neighbor-af-table/neighbor/af-data/prefissi-accept
cbgpPeerPrefixLimit	1.3.6.1.4.1.9.9.187.1.2.1.1.3	Numero massimo di prefissi di route accettati su questa connessione	Cisco-IOS-XR-ipv4-bgp oper:bgp/instance/instan active/default-vrf/afs/af/neighbor-af-table/neighbor/af-data/m prefix-limit
cbgpPeer2PrefixThreshold	1.3.6.1.4.1.9.9.187.1.2.8.1.4	Valore di soglia prefisso (%) per una famiglia di indirizzi su questa connessione in corrispondenza del quale viene generato un messaggio di avviso che indica il conteggio dei prefissi oltre la soglia o una notifica SNMP	Cisco-IOS-XR-ipv4-bgp oper:bgp/config-instance/config-instance default-vrf/entity-configuration/entity-configuration/af-depend config/max-prefix-warn-threshold

corrispondente.

CISCO-CLASS-BASED-QOS-MIB

La tabella seguente rappresenta il nome e il numero OID e l'XPATH corrispondente da impostare sui gruppi di sensori di telemetria basati su modelli correlati alle statistiche nelle classi/criteri QoS (Quality of Service).

Nome OID	Numero OID	Descrizione OID	XPATH
VelocitàBitCbQosCMDrop	1.3.6.1.4.1.9.9.166.1.15.1.1.18	Il bit rate delle gocce per classe come risultato di tutte le funzioni che possono produrre gocce (es., polizia, rilevamento casuale, ecc.).	Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/input/service-policy-names/service-policy-instance/statistics/class-stats/general-stats/total-rate Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/output/service-policy-names/service-policy-instance/statistics/class-stats/general-stats/total-rate
cbQosCMDropPkt64	1.3.6.1.4.1.9.9.166.1.15.1.1.14	Il contatore di 64 bit di perdita di pkt per classe come risultato di tutte le funzioni che possono produrre gocce (es., polizia, rilevamento casuale, ecc.).	Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/input/service-policy-names/service-policy-instance/statistics/class-stats/general-stats/total-packets Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/output/service-policy-names/service-policy-instance/statistics/class-stats/general-stats/total-packets
cbQosCMPrePolicyPkt64	1.3.6.1.4.1.9.9.166.1.15.1.1.3	I 64 bit contano i pacchetti in entrata prima di eseguire qualsiasi criterio QoS.	Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/input/service-policy-names/service-policy-instance/statistics/class-stats/general-stats/pre-policy-matched-packets Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/output/service-policy-names/service-policy-instance/statistics/class-stats/general-stats/pre-policy-matched-packets
cbNomeCMNQos	1.3.6.1.4.1.9.9.166.1.7.1.1.1	Nome della Classmap.	Cisco-IOS-XR-qos-ma-oper:qos/interface-

			table/interface/input/serv policy-names/service-po instance/statistics/class- stats/class-name
cbQosCMPostPolicyByte64	1.3.6.1.4.1.9.9.166.1.15.1.1.10	Conteggio a 64 bit degli ottetti in uscita dopo l'esecuzione dei criteri QoS.	Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/input/serv policy-names/service-po instance/statistics/class- stats/child-policy/class- stats/general- stats/transmission-bytes Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/output/se policy-names/service-po instance/statistics/class- stats/child-policy/class- stats/general- stats/transmission-bytes
cbQosIfIndex	1.3.6.1.4.1.9.9.166.1.1.1.1.4	ifIndex per l'interfaccia a cui è collegato il servizio. Questo campo ha senso solo se l'interfaccia logica ha un ifIndex snmp. Ad esempio, il valore di questo campo è privo di significato quando cbQosIfType è controlPlane.	Cisco-IOS-XR-infra-policymgr-oper:policy-manager/global/policy-map/policy-map-types/p map-type/policy-map-type/policy-maps
cbIndiceConfigurazioneQos	1.3.6.1.4.1.9.9.166.1.5.1.1.2	Un indice di configurazione arbitrario (assegnato dal sistema) (indipendente dall'istanza) per ciascun oggetto. Ogni oggetto con la stessa configurazione condivide lo stesso indice di configurazione.	Cisco-IOS-XR-infra-policymgr-oper:policy-manager/global/policy-map/policy-map-types/p map-type/policy-map-type/policy-maps
cbQosCMPrePolicyByte64	1.3.6.1.4.1.9.9.166.1.15.1.1.6	I 64 bit contano gli ottetti in entrata prima di eseguire qualsiasi criterio QoS.	Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/input/serv policy-names/service-po instance/statistics/class- stats/child-policy/class- stats/general-stats/pre-p

			matched-bytes Cisco-IOS-XR-qos-ma-oper:qos/interface-table/interface/output/se policy-names/service-po instance/statistics/class-stats/child-policy/class-stats/general-stats/pre-p matched-bytes

CISCO-ENHANCED-MEMPOOL-MIB

La tabella seguente rappresenta il nome e il numero OID e l'XPATH corrispondente da impostare sui gruppi di sensori di telemetria basati su modelli correlati all'utilizzo della memoria.

Nome OID	Numero OID	Descrizione OID	XPATH
cempMemPoolUsed	1.3.6.1.4.1.9.9.221.1.1.1.1.7	Indica il numero di byte del pool di memoria attualmente utilizzati dalle applicazioni nell'entità fisica.	Cisco-IOS-XR-nto-misc-oper:riepilogo memoria/nodi/nodo/riepilo
cempMemPoolHCUsed	1.3.6.1.4.1.9.9.221.1.1.1.1.18	Indica il numero di byte del pool di memoria attualmente utilizzati dalle applicazioni nell'entità fisica. Questo oggetto è una versione a 64 bit di cempMemPoolUsed.	Cisco-IOS-XR-nto-misc-oper:riepilogo della memoria/nodi/nodo/dettag tale-usato
cempMemPoolHCFree	1.3.6.1.4.1.9.9.221.1.1.1.1.20	Indica il numero di byte del pool di memoria attualmente inutilizzati nell'entità fisica. Questo oggetto è una versione a 64 bit di cempMemPoolFree.	Cisco-IOS-XR-nto-misc-oper:riepilogo della memoria/nodi/nodo/dettag emoria fisica libera

CISCO-ENTITY-FRU-CONTROL-MIB

La tabella seguente rappresenta il nome e il numero OID e l'XPATH corrispondente da impostare sui gruppi di sensori di telemetria basati su modelli correlati alle unità sostituibili sul campo nel sistema monitorato.

Nome OID	Numero OID	Descrizione OID	XPATH
cefcFRUPowerOperStatus	1.3.6.1.4.1.9.9.117.1.1.2.1.2	Stato di alimentazione operativo della FRU.	Cisco-IOS-XR-invmgr-oper:inventario/entità/e attributi/info-fru/alimentazione-stato

			operativo
cefcFRUPowerAdminStatus	1.3.6.1.4.1.9.9.117.1.1.2.1.1	Stato di alimentazione della FRU richiesto dall'amministratore.	Cisco-IOS-XR-invmgr-oper:inventario/entità/e attributi/info-fru/alimentazione-stato amministrativo
TempoUltimaModificaStatoModuloCefc	1.3.6.1.4.1.9.9.117.1.2.1.1.4	Il valore di sysUpTime nel momento in cui cefcModuleOperStatus viene modificato.	Cisco-IOS-XR-invmgr-oper:inventario/entità/a i/info-fru/ultima-modific stato-operativo
TempoAggiornamentoModulocefc	1.3.6.1.4.1.9.9.117.1.2.1.1.8	Questo oggetto fornisce il tempo di attività del modulo dall'ultima reinizializzazione. Questo oggetto non è persistente; se un modulo viene reimpostato, riavviato, spento, il tempo di attività inizia da zero.	Cisco-IOS-XR-invmgr-oper:inventario/entità/e attributi/info-fru/tempo-scheda
MotivoReimpostazioneModuloCefc	1.3.6.1.4.1.9.9.117.1.2.1.1.3	Questo oggetto identifica il motivo dell'ultima reimpostazione eseguita sul modulo.	Cisco-IOS-XR-invmgr-oper:inventario/entità/e attributi/info-fru/reimpostazione-cart motivo
cefcModuleOperStatus	1.3.6.1.4.1.9.9.117.1.2.1.1.2	Questo oggetto mostra lo stato operativo del modulo.	Cisco-IOS-XR-invmgr-oper:inventario/entità/e attributi/info-fru/stato-operativo-carta
cefcModuloStatoAmmin	1.3.6.1.4.1.9.9.117.1.2.1.1.1	Questo oggetto fornisce il controllo amministrativo del modulo.	Cisco-IOS-XR-invmgr-oper:inventario/entità/e attributi/info-fru/carta-s amministrativo

CISCO-ENTITY-SENSOR-MIB

La tabella seguente rappresenta il nome e il numero OID e l'XPATH corrispondente da impostare sui gruppi di sensori di telemetria guidati da modello correlati alle entità sensore sul nodo.

Nome OID	Numero OID	Descrizione OID	XPATH
ValoreSensoreInvio	1.3.6.1.4.1.9.9.91.1.1.1.1.4	Questa variabile indica la misurazione più recente rilevata dal sensore. Per visualizzare o interpretare correttamente il valore di questa variabile, è inoltre necessario conoscere entSensorType, entSensorScale e entSensorPrecision.	Cisco-IOS-XR-invmg oper:inventario/entità/attributi/buv-senso info/valore

ValutazioneSogliaSensoreInt	1.3.6.1.4.1.9.9.91.1.2.1.1.5	Tuttavia, è possibile confrontare entSensorValue con i valori di soglia specificati in entSensorThresholdTable senza alcuna conoscenza semantica. Questa variabile indica il risultato dell'ultima valutazione della soglia. Se la condizione di soglia è true, entSensorThresholdEvaluation è true(1). Se la condizione di soglia è false, entSensorThresholdEvaluation è false(2). Le soglie vengono valutate alla velocità indicata da entSensorValueUpdateRate.	Cisco-IOS-XR-invmgr-oper:inventario/entità/attributi/soglia

CISCO-FLASH-MIB

La tabella seguente rappresenta il nome e il numero OID e l'XPATH corrispondente da impostare sui gruppi di sensori di telemetria basati su modelli correlati alla memorizzazione flash sul sistema.

Nome OID	Numero OID	Descrizione OID	XPATH
NomePartizioneFlash	1.3.6.1.4.1.9.9.10.1.1.4.1.1.10	Nome della partizione Flash utilizzato dal sistema per fare riferimento a una partizione. Può essere una qualsiasi stringa di caratteri alfanumerici nel formato AAAAAAAAnn, dove A rappresenta un carattere alfanumerico facoltativo e n un carattere numerico. Qualsiasi carattere numerico deve sempre costituire la parte finale della stringa. Il sistema rimuove i caratteri alfa e utilizza la parte numerica per eseguire il mapping a un indice di partizione. Le operazioni Flash vengono indirizzate a una partizione di dispositivo basata su questo nome. Il sistema ha un concetto di partizione predefinita. Si tratta della prima partizione del dispositivo. Il sistema indirizza un'operazione alla	Cisco-IOS-XR-shellutil-filesyst oper:file-system/nodo/fil system/tipo

		partizione predefinita ogni volta che non viene specificato un nome di partizione. Il nome della partizione è pertanto obbligatorio tranne quando l'operazione viene eseguita sulla partizione predefinita o il dispositivo ha una sola partizione (non è partizionato).	
DimensionePartizioneFlashciscoEstesa	1.3.6.1.4.1.9.9.10.1.1.4.1.1.13	Dimensioni della partizione Flash. Deve essere un multiplo integrale di ciscoFlashDeviceMinPartitionSize. Se è presente una singola partizione, queste dimensioni saranno uguali a ciscoFlashDeviceSize. Questo oggetto è una versione a 64 bit di ciscoFlashPartitionSize	Cisco-IOS-XR-shellutil-filesyst oper:file-system/nodo/fil system/dimensi
ciscoFlashPartitionFreeSpaceExtended	1.3.6.1.4.1.9.9.10.1.1.4.1.1.14	Spazio libero in una partizione Flash. Si noti che le dimensioni effettive di un file in Flash includono un piccolo sovraccarico che rappresenta l'intestazione del file system. Alcuni file system possono inoltre avere un sovraccarico della partizione o dell'intestazione del dispositivo da prendere in considerazione quando si calcola lo spazio libero. Lo spazio disponibile verrà calcolato come la dimensione totale della partizione meno le dimensioni di tutti i file esistenti (file validi/non validi/eliminati e inclusa l'intestazione di ogni file), le dimensioni dell'intestazione della partizione meno le dimensioni dell'intestazione del file successivo in cui copiare. In breve, questo oggetto darà le dimensioni del file più grande che può essere copiato in. Non è previsto che l'entità di gestione conosca o utilizzi	Cisco-IOS-XR-shellutil-filesyst oper:file-system/nodo/fil system/free

		costi comuni quali la lunghezza delle intestazioni dei file e delle partizioni, in quanto tali costi possono variare da file system a file system. I file eliminati in Flash non liberano spazio. Potrebbe essere necessario cancellare una partizione per recuperare lo spazio occupato dai file. Questo oggetto è una versione a 64 bit di ciscoFlashPartitionFreeSpace	

CISCO-PROCESS-MIB

Nella tabella seguente vengono indicati il nome e il numero OID e l'XPATH corrispondente da impostare per i gruppi di sensori di telemetria basati su modelli relativi all'utilizzo della CPU e all'allocazione delle risorse per i processi.

Nome OID	Numero OID	Descrizione OID	XPATH
cpmCPUTotal1minRev	1.3.6.1.4.1.9.9.109.1.1.1.1.7	Percentuale complessiva di CPU occupata nell'ultimo periodo di 1 minuto. Questo oggetto deprecia l'oggetto cpmCPUTotal1min e aumenta l'intervallo di valori a (0..100).	Cisco-IOS-XR-wdsysmon-fd-oper:monitoraggio-sistema/utilizzo-cpu/totale-cpu-un m
cpmCPUTotal5minRev	1.3.6.1.4.1.9.9.109.1.1.1.1.8	Percentuale complessiva di CPU occupata negli ultimi 5 minuti. Questo oggetto deprecia l'oggetto cpmCPUTotal5min e aumenta l'intervallo di valori a (0..100).	Cisco-IOS-XR-wdsysmon-fd-oper:monitoraggio-sistema/utilizzo-cpu/totale-cpu-cinq minuti
cpmCPUTotal15minRev	1.3.6.1.4.1.9.9.109.1.1.1.1.31	Percentuale complessiva di CPU occupata negli ultimi 15 minuti. Questo oggetto deprecia l'oggetto cpmCPUTotal15min e aumenta l'intervallo di valori a (0..100).	Cisco-IOS-XR-wdsysmon-fd-oper:monitoraggio-sistema/utilizzo-cpu/totale-cpu-quin minuti
cpmNomeProcesso	1.3.6.1.4.1.9.9.109.1.2.1.1.2	Nome associato al processo. Se il nome è più lungo di 32 caratteri, verrà troncato ai primi 31 caratteri e verrà aggiunto un carattere `*' come ultimo carattere per indicare che si tratta di un nome di	Cisco-IOS-XR-wdsysmon-fd-oper:monitoraggio-sistema/utilizzo-cpu/nome-processo

		processo troncato.	
cpmElaboraDimensioneSegmentoTesto	1.3.6.1.4.1.9.9.109.1.2.3.1.15	Indica la memoria di testo di un processo e tutti i relativi oggetti condivisi.	Cisco-IOS-XR-proc oper:process-memory/nodes/nod cess-ids/process-id seg-size
cpmElaboraDimensioneMemoriaDinamica	1.3.6.1.4.1.9.9.109.1.2.3.1.18	Indica la quantità di memoria dinamica utilizzata dal processo.	Cisco-IOS-XR-proc oper:process-memory/nodes/nod cess-ids/process-id limit
cpmDimensioneSegmentoDatiProcesso	1.3.6.1.4.1.9.9.109.1.2.3.1.16	Indica il segmento di dati di un processo e tutti i relativi oggetti condivisi.	Cisco-IOS-XR-proc oper:processi-memoria/nodi/nodi/ processo/ID-processo/dimensio segmento-dati
cpmProcExtMemAllocatedRev	1.3.6.1.4.1.9.9.109.1.2.3.1.1	Somma di tutta la memoria allocata in modo dinamico che il processo ha ricevuto dal sistema. Ciò include la memoria che potrebbe essere stata restituita. La somma della memoria liberata è fornita da cpmProcExtMemFreedRev. Questo oggetto depreca cpmProcExtMemAllocated.	Cisco-IOS-XR-proc oper:processi-memoria/nodi/nodi/ processo/ID-proces
cpmProcExtMemFreedRev	1.3.6.1.4.1.9.9.109.1.2.3.1.2	Somma di tutta la memoria restituita dal processo al sistema. Questo oggetto depreca cpmProcExtMemFreed.	Cisco-IOS-XR-proc oper:processi-memoria/nodi/nodi/ processo/ID-proces

ENTITY-MIB

La tabella seguente rappresenta il nome e il numero OID e l'XPATH corrispondente da impostare sulle entità fisiche correlate ai gruppi di sensori di telemetria basati su modelli nel sistema.

Nome OID	Numero OID	Descrizione OID	XPATH
NomeFisicoInvio	1.3.6.1.2.1.47.1.1.1.1.7	Nome testuale dell'entità fisica. Il valore di questo oggetto deve corrispondere al nome del componente assegnato dalla periferica locale e deve essere adatto all'utilizzo nei comandi immessi nella `console' della periferica. Può trattarsi di un nome di testo, ad esempio 'console' o di un semplice numero di componente (ad esempio, numero di porta o di	Cisco-IOS-XR-snmp-entitymib-oper:entità-indice-fisico

		modulo), ad esempio '1', a seconda della sintassi di denominazione dei componenti fisici del dispositivo. Se non esiste un nome locale o se l'oggetto non è applicabile, l'oggetto contiene una stringa di lunghezza zero. Notare che il valore di entPhysicalName per due entità fisiche sarà lo stesso nel caso in cui l'interfaccia della console non distingua tra loro, ad esempio, slot-1 e la scheda nello slot-1.	
DescrizioneLogicaInt	1.3.6.1.2.1.47.1.2.1.1.2	Descrizione testuale dell'entità logica. Questo oggetto deve contenere una stringa che identifica il nome del produttore per l'entità logica e deve essere impostato su un valore distinto per ogni versione dell'entità logica.	Cisco-IOS-XR-snmp-agent-oper:snmp/information-em-name/
DescrFisicoInt	1.3.6.1.2.1.47.1.1.1.1.2	Descrizione testuale dell'entità fisica. Questo oggetto deve contenere una stringa che identifica il nome del produttore per l'entità fisica e deve essere impostato su un valore distinto per ogni versione o modello dell'entità fisica.	Cisco-IOS-XR-snmp-agent-oper:snmp/Cisco-IOS-XR-snmp-entitym-oper:entity-mib/entity-physical-indexes/
InclusioneFisicaIn	1.3.6.1.2.1.47.1.1.1.1.4	Valore di entPhysicalIndex per l'entità fisica che 'contiene' questa entità fisica. Il valore zero indica che questa entità fisica non è contenuta in altre entità fisiche. Si noti che l'insieme di relazioni di contenimento definisce una gerarchia rigorosa; ovvero, ricorsione non consentita. Nel caso in cui un'entità fisica sia contenuta da più entità fisiche (ad esempio, moduli a doppio raggio), questo oggetto deve identificare l'entità contenitore con il valore più basso di entPhysicalIndex.	Cisco-IOS-XR-invmgr-oper:inventario/entità/-/attributi/inv-basic-bag/unique-id
ClasseFisicaRete	1.3.6.1.2.1.47.1.1.1.1.5	Indicazione del tipo di	Cisco-IOS-XR-invmgr

		hardware generale dell'entità fisica. Un agente deve impostare questo oggetto sul valore di enumerazione standard che indica con maggiore precisione la classe generale dell'entità fisica o la classe primaria se ne esiste più di una. Se non esiste un identificativo di registrazione standard appropriato per questa entità fisica, viene restituito il valore 'other(1)'. Se il valore è sconosciuto da questo agente, viene restituito il valore 'known(2)'.	oper:inventario/entità
InvPhysicalHardwareRev	1.3.6.1.2.1.47.1.1.1.1.8	Stringa di revisione hardware specifica del fornitore per l'entità fisica. Il valore preferito è l'identificatore di revisione hardware effettivamente stampato sul componente stesso (se presente). Se le informazioni di revisione vengono memorizzate internamente in un formato non stampabile (ad esempio binario), l'agente deve convertirle in un formato stampabile, in una modalità specifica dell'implementazione. Se al componente fisico non è associata alcuna stringa di revisione hardware specifica o se queste informazioni sono sconosciute all'agente, l'oggetto conterrà una stringa di lunghezza zero.	Cisco-IOS-XR-invmgr oper:inventario/entità/ /attributi/inv-basic-bag/revisione hardwa
InvPhysicalFirmwareRev	1.3.6.1.2.1.47.1.1.1.1.9	Stringa di revisione firmware specifica del fornitore per l'entità fisica. Se le informazioni di revisione vengono memorizzate internamente in un formato non stampabile (ad esempio binario), l'agente deve convertirle in un formato stampabile, in una modalità specifica dell'implementazione. Se al componente fisico non sono associati programmi specifici	Cisco-IOS-XR-invmgr oper:inventario/entità/ /attributi/inv-basic-bag/firmware-review

		del firmware o se queste informazioni sono sconosciute all'agente, questo oggetto conterrà una stringa di lunghezza zero.	
InvPhysicalSoftwareRev	1.3.6.1.2.1.47.1.1.1.1.10	Stringa di revisione software specifica del fornitore per l'entità fisica. Se le informazioni di revisione vengono memorizzate internamente in un formato non stampabile (ad esempio binario), l'agente deve convertirle in un formato stampabile, in una modalità specifica dell'implementazione. Se al componente fisico non sono associati programmi software specifici o se queste informazioni sono sconosciute all'agente, questo oggetto conterrà una stringa di lunghezza zero.	Cisco-IOS-XR-invmgr oper:inventario/entità/ /attributi/inv-basic-bag/software-revision
NumSerialeFisico	1.3.6.1.2.1.47.1.1.1.1.11	Stringa del numero di serie specifico del fornitore per l'entità fisica. Il valore preferito è la stringa del numero di serie effettivamente stampata sul componente stesso (se presente). Alla prima creazione di un'istanza di un'entità fisica, il valore di entPhysicalSerialNum associato a tale entità viene impostato sul numero di serie corretto assegnato dal fornitore, se queste informazioni sono disponibili per l'agente. Se un numero di serie è sconosciuto o inesistente, la costante netPhysicalSerialNum verrà impostata su una stringa di lunghezza zero. Si noti che le implementazioni in grado di identificare correttamente i numeri di serie di tutte le entità fisiche installate non devono fornire accesso in scrittura all'oggetto entPhysicalSerialNum. Gli	Cisco-IOS-XR-invmgr oper:inventario/entità/ /attributi/magazzino-b base/numero di serie

		agenti che non possono fornire una memoria non volatile per le stringhe entPhysicalSerialNum non sono necessari per implementare l'accesso in scrittura per questo oggetto. Non tutti i componenti fisici avranno un numero di serie o ne avranno bisogno. Le entità fisiche per le quali il valore associato dell'oggetto entPhysicalIsFRU è uguale a 'false(2)' (ad esempio, le porte del ripetitore all'interno di un modulo ripetitore), non hanno bisogno del proprio numero di serie univoco. Un agente non deve fornire accesso in scrittura per tali entità e può restituire una stringa di lunghezza zero. Se l'accesso in scrittura viene implementato per un'istanza di entPhysicalSerialNum e un valore viene scritto nell'istanza, l'agente deve mantenere il valore fornito nell'istanza di entPhysicalSerialNum associata alla stessa entità fisica per tutto il tempo in cui viene creata l'istanza di tale entità. Sono incluse le istanze di tutte le reinizializzazioni/riavvii del sistema di gestione di rete, incluse quelle che determinano una modifica del valore entPhysicalIndex dell'entità fisica.	
NomeMfgFisico	1.3.6.1.2.1.47.1.1.1.1.12	Nome del produttore del componente fisico. Il valore preferito è la stringa del nome del produttore effettivamente stampata sul componente stesso (se presente). Si noti che i confronti tra istanze degli oggetti entPhysicalModelName, entPhysicalFirmwareRev, entPhysicalSoftwareRev e entPhysicalSerialNum sono	Cisco-IOS-XR-invmgr oper:inventario/entità/ /attributi/magazzino-b base/nome-produttore

		significativi solo tra gli oggetti entPhysicalEntries con lo stesso valore di entPhysicalMfgName. Se la stringa del nome del produttore associata al componente fisico è sconosciuta all'agente, questo oggetto conterrà una stringa di lunghezza zero.	
NomeModelloFisicoInvio	1.3.6.1.2.1.47.1.1.1.1.13	Stringa dell'identificatore del nome del modello specifico del fornitore associata al componente fisico. Il valore preferito è il numero di parte visibile al cliente che può essere stampato sul componente stesso. Se la stringa del nome del modello associata al componente fisico è sconosciuta all'agente, questo oggetto conterrà una stringa di lunghezza zero.	Cisco-IOS-XR-invmgr oper:inventario/entità/ /attributi/inv-basic-bag/nome-modello

IF-MIB

Nella tabella seguente vengono indicati il nome e il numero OID e l'XPATH corrispondente da impostare nei gruppi di sensori di telemetria basati su modelli correlati alle caratteristiche e ai contatori dell'interfaccia.

Nome OID	Numero OID	Descrizione OID	XPATH
ifMtu	1.3.6.1.2.1.2.2.1.4	Dimensioni del pacchetto più grande che può essere inviato/ricevuto sull'interfaccia, specificate in ottetti. Per le interfacce utilizzate per la trasmissione di datagrammi di rete, si tratta delle dimensioni del datagramma di rete più grande che può essere inviato sull'interfaccia.	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interface/mtu
ifIndirizzoFisico	1.3.6.1.2.1.2.2.1.6	L'indirizzo dell'interfaccia al livello secondario del protocollo. Ad esempio, per un'interfaccia 802.x, questo oggetto normalmente contiene un indirizzo MAC. Il MIB specifico dell'interfaccia deve definire l'ordinamento di bit e byte e il formato del valore di questo oggetto. Per le interfacce che non dispongono	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interface/interface-ty information/bundle-information/member/m address

		di tale indirizzo (ad esempio, una linea seriale), questo oggetto deve contenere una stringa di ottetti di lunghezza zero.	
ifType	1.3.6.1.2.1.2.2.1.3	Tipo di interfaccia. I valori aggiuntivi per ifType vengono assegnati dalla IANA (Internet Assigned Numbers Authority) tramite l'aggiornamento della sintassi della convenzione testuale IANAifType.	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interfaccia/tipo-inter
IfOutUcastPkts	1.3.6.1.2.1.2.2.1.17	Numero totale di pacchetti di cui è stata richiesta la trasmissione tramite protocolli di livello superiore e che non sono stati indirizzati a un indirizzo multicast o broadcast di questo sottolivello, inclusi quelli scartati o non inviati. Le discontinuità nel valore di questo contatore possono verificarsi alla reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ifCounterDiscontinuityTime.	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interface/interface-statistics/full-interface-stats/packets-sent
IfHCOutUcastPkts	1.3.6.1.2.1.31.1.1.1.11	Numero totale di pacchetti di cui è stata richiesta la trasmissione tramite protocolli di livello superiore e che non sono stati indirizzati a un indirizzo multicast o broadcast di questo sottolivello, inclusi quelli scartati o non inviati. Questo oggetto è una versione a 64 bit di ifOutUcastPkts. Le discontinuità nel valore di questo contatore possono verificarsi alla reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ifCounterDiscontinuityTime.	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interface/interface-statistics/full-interface-stats/packets-sent
IfInUcastPkts	1.3.6.1.2.1.2.2.1.11	Il numero di pacchetti, recapitati da questo sottolivello a un sottolivello superiore, che non sono stati indirizzati a un indirizzo multicast o broadcast di questo sottolivello. Le discontinuità nel valore di questo contatore possono verificarsi alla	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interface/interface-statistics/full-interface-stats/packets-received

		reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ifCounterDiscontinuityTime.	
IfHCInUcastPkts	1.3.6.1.2.1.31.1.1.1.7	Il numero di pacchetti, recapitati da questo sottolivello a un sottolivello superiore, che non sono stati indirizzati a un indirizzo multicast o broadcast di questo sottolivello. Questo oggetto è una versione a 64 bit di ifInUcastPkts. Le discontinuità nel valore di questo contatore possono verificarsi alla reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ifCounterDiscontinuityTime.	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interface/interface-statistics/full-interface-stats/packets-received
IfOutErrors	1.3.6.1.2.1.2.2.1.20	Per le interfacce orientate ai pacchetti, il numero di pacchetti in uscita che non è stato possibile trasmettere a causa di errori. Per le interfacce orientate ai caratteri o a lunghezza fissa, il numero di unità di trasmissione in uscita che non è stato possibile trasmettere a causa di errori. Le discontinuità nel valore di questo contatore possono verificarsi alla reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ifCounterDiscontinuityTime.	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interface/interface-statistics/full-interface-stats/output-errors
IfOutDiscards	1.3.6.1.2.1.2.2.1.19	Il numero di pacchetti in uscita che sono stati scartati anche se non sono stati rilevati errori che ne impedissero la trasmissione. Uno dei possibili motivi per scartare un pacchetto di questo tipo potrebbe essere quello di liberare spazio nel buffer. Le discontinuità nel valore di questo contatore possono verificarsi alla reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ifCounterDiscontinuityTime.	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interface/interface-statistics/full-interface-stats/output-drops
IfOutMulticastPkts	1.3.6.1.2.1.31.1.1.1.4	Numero totale di pacchetti di	Cisco-IOS-XR-pfi-im-c

		cui è stata richiesta la trasmissione tramite protocolli di livello superiore e che sono stati indirizzati a un indirizzo multicast in questo sottolivello, inclusi quelli scartati o non inviati. Per un protocollo del livello MAC, sono inclusi sia gli indirizzi di gruppo che quelli funzionali. Le discontinuità nel valore di questo contatore possono verificarsi alla reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ifCounterDiscontinuityTime.	oper:interfacce/interfac xr/interface/interface-statistics/full-interface-stats/multicast-packets
IfHCOutMulticastPkts	1.3.6.1.2.1.31.1.1.1.12	Numero totale di pacchetti di cui è stata richiesta la trasmissione tramite protocolli di livello superiore e che sono stati indirizzati a un indirizzo multicast in questo sottolivello, inclusi quelli scartati o non inviati. Per un protocollo del livello MAC, sono inclusi sia gli indirizzi di gruppo che quelli funzionali. Questo oggetto è una versione a 64 bit di ifOutMulticastPkts. Le discontinuità nel valore di questo contatore possono verificarsi alla reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ifCounterDiscontinuityTime.	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interface/interface-statistics/full-interface-stats/multicast-packets
ifPacchettiMulticast	1.3.6.1.2.1.31.1.1.1.2	Il numero di pacchetti, recapitati da questo sottolivello a un sottolivello superiore, indirizzati a un indirizzo multicast di questo sottolivello. Per un protocollo del livello MAC, sono inclusi sia gli indirizzi di gruppo che quelli funzionali. Le discontinuità nel valore di questo contatore possono verificarsi alla reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ifCounterDiscontinuityTime.	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interface/interface-statistics/full-interface-stats/multicast-packets received
ifHCInMulticastPkts	1.3.6.1.2.1.31.1.1.1.8	Il numero di pacchetti, recapitati da questo sottolivello	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac

		a un sottolivello superiore, indirizzati a un indirizzo multicast di questo sottolivello. Per un protocollo del livello MAC, sono inclusi sia gli indirizzi di gruppo che quelli funzionali. Questo oggetto è una versione a 64 bit di ifInMulticastPkts. Le discontinuità nel valore di questo contatore possono verificarsi alla reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ifCounterDiscontinuityTime.	xr/interface/interface-statistics/full-interface-stats/multicast-packets received
IfInErrors	1.3.6.1.2.1.2.2.1.14	Per le interfacce orientate ai pacchetti, il numero di pacchetti in entrata che contenevano errori che ne impedivano il recapito a un protocollo di livello superiore. Per le interfacce orientate ai caratteri o a lunghezza fissa, il numero di unità di trasmissione in entrata che contenevano errori che ne impedivano il recapito a un protocollo di livello superiore. Le discontinuità nel valore di questo contatore possono verificarsi alla reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ifCounterDiscontinuityTime.	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interface/interface-statistics/full-interface-stats/input-errors
IfInDiscards	1.3.6.1.2.1.2.2.1.13	Il numero di pacchetti in entrata che sono stati scartati anche se non sono stati rilevati errori che ne impedissero il recapito a un protocollo di livello superiore. Uno dei possibili motivi per scartare un pacchetto di questo tipo potrebbe essere quello di liberare spazio nel buffer. Le discontinuità nel valore di questo contatore possono verificarsi alla reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ifCounterDiscontinuityTime.	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interface/interface-statistics/full-interface-stats/input-drops

IfOutOctets	1.3.6.1.2.1.2.2.1.16	Il numero totale di ottetti trasmessi dall'interfaccia, inclusi i caratteri di framing. Le discontinuità nel valore di questo contatore possono verificarsi alla reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ifCounterDiscontinuityTime.	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interface/interface- statistics/full-interface- stats/bytes-sent
IfHCOutOctets	1.3.6.1.2.1.31.1.1.1.10	Il numero totale di ottetti trasmessi dall'interfaccia, inclusi i caratteri di framing. Questo oggetto è una versione a 64 bit di ifOutOctets. Le discontinuità nel valore di questo contatore possono verificarsi alla reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ifCounterDiscontinuityTime.	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interface/interface- statistics/full-interface- stats/bytes-sent
ifInOttetti	1.3.6.1.2.1.2.2.1.10	Il numero totale di ottetti ricevuti sull'interfaccia, inclusi i caratteri di framing. Le discontinuità nel valore di questo contatore possono verificarsi alla reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ifCounterDiscontinuityTime.	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interface/interface- statistics/full-interface- stats/bytes-received
ifHCInOttetti	1.3.6.1.2.1.31.1.1.1.6	Il numero totale di ottetti ricevuti sull'interfaccia, inclusi i caratteri di framing. Questo oggetto è una versione a 64 bit di ifInOctets. Le discontinuità nel valore di questo contatore possono verificarsi alla reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ifCounterDiscontinuityTime.	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interface/interface- statistics/full-interface- stats/bytes-received
ifOutBroadcastPkts	1.3.6.1.2.1.31.1.1.1.5	Numero totale di pacchetti che sono stati richiesti per la trasmissione da protocolli di livello superiore e che sono stati indirizzati a un indirizzo di broadcast in questo sottolivello, inclusi quelli scartati o non inviati. Le discontinuità nel valore di questo contatore possono	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interface/interface- statistics/full-interface- stats/broadcast-packet sent

		verificarsi alla reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ifCounterDiscontinuityTime.	
ifHCOutBroadcastPkts	1.3.6.1.2.1.31.1.1.1.13	Numero totale di pacchetti che sono stati richiesti per la trasmissione da protocolli di livello superiore e che sono stati indirizzati a un indirizzo di broadcast in questo sottolivello, inclusi quelli scartati o non inviati. Questo oggetto è una versione a 64 bit di ifOutBroadcastPkts. Le discontinuità nel valore di questo contatore possono verificarsi alla reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ifCounterDiscontinuityTime.	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interface/interface-statistics/full-interface-stats/broadcast-packet sent
ifInPacchettiTrasmissione	1.3.6.1.2.1.31.1.1.1.3	Il numero di pacchetti, recapitati da questo sottolivello a un sottolivello superiore, indirizzati a un indirizzo di broadcast di questo sottolivello. Le discontinuità nel valore di questo contatore possono verificarsi alla reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ifCounterDiscontinuityTime.	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interface/interface-statistics/full-interface-stats/broadcast-packet received
ifHCInPacchettiTrasmissione	1.3.6.1.2.1.31.1.1.1.9	Il numero di pacchetti, recapitati da questo sottolivello a un sottolivello superiore, indirizzati a un indirizzo di broadcast di questo sottolivello. Questo oggetto è una versione a 64 bit di ifInBroadcastPkts. Le discontinuità nel valore di questo contatore possono verificarsi alla reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ifCounterDiscontinuityTime.	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interface/interface-statistics/full-interface-stats/broadcast-packet received
IfIndex	1.3.6.1.2.1.2.2.1.1	Un valore univoco, maggiore di zero, per ogni interfaccia. Si consiglia di assegnare i valori in modo contiguo a partire da	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interface/if-index

		1. Il valore di ciascun sottolivello di interfaccia deve rimanere costante almeno da una reinizializzazione del sistema di gestione di rete dell'entità alla successiva reinizializzazione.	
ifDescr	1.3.6.1.2.1.2.2.1.2	Stringa di testo contenente informazioni sull'interfaccia. Questa stringa deve includere il nome del produttore, il nome del prodotto e la versione dell'interfaccia hardware/software.	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interface/description
ifSpeed	1.3.6.1.2.1.2.2.1.5	Stima della larghezza di banda corrente dell'interfaccia in bit al secondo. Per le interfacce che non variano in larghezza di banda o per quelle in cui non è possibile effettuare una stima accurata, questo oggetto deve contenere la larghezza di banda nominale. Se la larghezza di banda dell'interfaccia è maggiore del valore massimo segnalabile da questo oggetto, l'oggetto deve restituire il valore massimo (4.294.967.295) e se è necessario utilizzare HighSpeed per segnalare la velocità dell'interfaccia. Per un sottolivello che non ha alcun concetto di larghezza di banda, questo oggetto dovrebbe essere zero.	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac xr/interfaccia/larghezza banda
.StatoOper	1.3.6.1.2.1.2.2.1.8	Stato operativo corrente dell'interfaccia. Lo stato testing(3) indica che non è possibile passare pacchetti operativi. Se ifAdminStatus è inattivo(2), ifOperStatus deve essere inattivo(2). Se ifAdminStatus è impostato su up(1), ifOperStatus deve essere impostato su up(1) se l'interfaccia è pronta a trasmettere e ricevere traffico di rete; deve diventare inattivo(5) se l'interfaccia è in attesa di azioni esterne (come una linea seriale in attesa di una connessione in entrata);	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac non-dinamica/interfacc non-dinamica/stato-op

		deve rimanere nello stato non attivo(2) se e solo se vi è un guasto che impedisce che si passi allo stato attivo(1); deve rimanere nello stato notPresent(6) se l'interfaccia ha componenti (generalmente hardware) mancanti.	
ifStatoAmmin	1.3.6.1.2.1.2.2.1.7	Stato desiderato dell'interfaccia. Lo stato testing(3) indica che non è possibile passare pacchetti operativi. Quando un sistema gestito viene inizializzato, tutte le interfacce iniziano con ifAdminStatus nello stato non attivo (2). A seguito di un'azione di gestione esplicita o di informazioni di configurazione conservate dal sistema gestito, seAdminStatus viene modificato in stato attivo(1) o test(3) (o rimane in stato inattivo(2)).	Cisco-IOS-XR-pfi-im-c oper:interfacce/interfac non-dinamica/interfacc non-dinamica/stato- amministratore
ifName	1.3.6.1.2.1.31.1.1.1.1	Nome testuale dell'interfaccia. Il valore di questo oggetto deve corrispondere al nome dell'interfaccia assegnata dalla periferica locale e deve essere adatto all'utilizzo nei comandi immessi nella `console' della periferica. Potrebbe trattarsi di un nome di testo, ad esempio `le0' o di un semplice numero di porta, ad esempio `1', a seconda della sintassi di denominazione dell'interfaccia del dispositivo. Se più voci nell'ifTable rappresentano insieme una singola interfaccia denominata dal dispositivo, ognuna avrà lo stesso valore di ifName. Si noti che per un agente che risponde a query SNMP relative a un'interfaccia su un altro dispositivo (proxy), il valore di ifName per tale interfaccia corrisponde al nome locale del dispositivo proxy per tale interfaccia. Se non esiste un nome locale o se l'oggetto non è applicabile,	Cisco-IOS-XR-pfi-im-c oper:interfacce/descriz interfaccia/descrizione interfaccia/nome-interf

ifAltaVelocità	1.3.6.1.2.1.31.1.1.1.15	l'oggetto contiene una stringa di lunghezza zero. Stima della larghezza di banda corrente dell'interfaccia in unità di 1.000.000 di bit al secondo. Se questo oggetto indica un valore di `n', la velocità dell'interfaccia è compresa tra `n-500.000' e `n+499.999'. Per le interfacce che non variano in larghezza di banda o per quelle in cui non è possibile effettuare una stima accurata, questo oggetto deve contenere la larghezza di banda nominale. Per un sottolivello che non ha alcun concetto di larghezza di banda, questo oggetto dovrebbe essere zero.	Cisco-IOS-XR-pfi-im-c oper:interfacce/descriz interfacce/descrizione- interfaccia/larghezza d banda64 bit

MIB IP

La tabella seguente rappresenta il nome e il numero OID e il corrispondente XPATH da impostare sui gruppi di sensori di telemetria basati su modelli correlati alle statistiche e ai valori operativi del protocollo Internet (IP).

Nome OID	Numero OID	Descrizione OID	XPATH
icmpInDestNonRaggiunge	1.3.6.1.2.1.5.3	Numero di messaggi ICMP "destinazione irraggiungibile" ricevuti.	Cisco-IOS-XR-ipv4-io- oper:rete/nodi/nodi/stat e/traffico/icmp-status ip
ProbParmInICMP	1.3.6.1.2.1.5.5	Numero di messaggi ICMP Parameter Problem ricevuti.	Cisco-IOS-XR-ipv4-io- oper:rete/nodi/nodi/stat e/traffico/icmp-status ip
icmpInSrcQuench	1.3.6.1.2.1.5.6	Numero di messaggi ICMP Source Quench ricevuti.	Cisco-IOS-XR-ipv4-io- oper:rete/nodi/nodi/stat e/traffico/icmp-status ip
icmpInEco	1.3.6.1.2.1.5.8	Numero di messaggi ICMP Echo (richiesta) ricevuti.	Cisco-IOS-XR-ipv4-io- oper:rete/nodi/nodi/stat e/traffico/icmp-status ip
icmpInEcoRappresentazioni	1.3.6.1.2.1.5.9	Numero di messaggi ICMP Echo Reply ricevuti.	Cisco-IOS-XR-ipv4-io- oper:rete/nodi/nodi/stat e/traffico/icmp-status ip
icmpIndicatoriOrariIn	1.3.6.1.2.1.5.10	Numero di messaggi ICMP Timestamp (richiesta) ricevuti.	Cisco-IOS-XR-ipv4-io- oper:rete/nodi/nodi/stat e/traffico/icmp-status ip
icmpIndMaschere	1.3.6.1.2.1.5.12	Numero di messaggi ICMP Richiesta maschera d'indirizzo ricevuti.	Cisco-IOS-XR-ipv4-io- oper:rete/nodi/nodi/stat e/traffico/icmp-status ip
rappresentazioniMascheraIndICMP	1.3.6.1.2.1.5.13	Numero di messaggi ICMP Address Mask Reply ricevuti.	Cisco-IOS-XR-ipv4-io- oper:rete/nodi/nodi/stat e/traffico/icmp-status ip
MessaggioFuoriICMP	1.3.6.1.2.1.5.14	Numero totale di messaggi ICMP che l'entità ha tentato di	Cisco-IOS-XR-ipv4-io- oper:rete/nodi/nodi/stat

		inviare. Notare che questo contatore include tutti quelli conteggiati da icmpOutErrors.	e/traffico/icmp-status ip
icmpOutDestUnreachs	1.3.6.1.2.1.5.16	Numero di messaggi ICMP "destinazione irraggiungibile" inviati.	Cisco-IOS-XR-ipv4-io-oper:rete/nodi/nodi/stat e/traffico/icmp-status ip
EccezioniTempoOutICMP	1.3.6.1.2.1.5.17	Numero di messaggi ICMP "tempo scaduto" inviati.	Cisco-IOS-XR-ipv4-io-oper:rete/nodi/nodi/stat e/traffico/icmp-status ip
ProbParmOutICMP	1.3.6.1.2.1.5.18	Numero di messaggi ICMP Parameter Problem inviati.	Cisco-IOS-XR-ipv4-io-oper:rete/nodi/nodi/stat e/traffico/icmp-status ip
icmpOutSrcQuench	1.3.6.1.2.1.5.19	Numero di messaggi ICMP Source Quench inviati.	Cisco-IOS-XR-ipv4-io-oper:rete/nodi/nodi/stat e/traffico/icmp-status ip
icmpOutRedirects	1.3.6.1.2.1.5.20	Numero di messaggi di reindirizzamento ICMP inviati. Per un host, questo oggetto sarà sempre zero, poiché gli host non inviano reindirizzamenti.	Cisco-IOS-XR-ipv4-io-oper:rete/nodi/nodi/stat e/traffico/icmp-status ip
icmpEchoOut	1.3.6.1.2.1.5.21	Numero di messaggi ICMP Echo (richiesta) inviati.	Cisco-IOS-XR-ipv4-io-oper:rete/nodi/nodi/stat e/traffico/icmp-status ip
icmpEcoRappresentazioni	1.3.6.1.2.1.5.22	Numero di messaggi ICMP Echo Reply inviati.	Cisco-IOS-XR-ipv4-io-oper:rete/nodi/nodi/stat e/traffico/icmp-status ip
icmpTimestamp	1.3.6.1.2.1.5.23	Numero di messaggi ICMP Timestamp (richiesta) inviati.	Cisco-IOS-XR-ipv4-io-oper:rete/nodi/nodi/stat e/traffico/icmp-status ip
icmpOutAddrMask	1.3.6.1.2.1.5.25	Numero di messaggi ICMP Richiesta maschera d'indirizzo inviati.	Cisco-IOS-XR-ipv4-io-oper:rete/nodi/nodi/stat e/traffico/icmp-status ip
icmpIndMaskRappresentazioni	1.3.6.1.2.1.5.26	Numero di messaggi ICMP Address Mask Reply inviati.	Cisco-IOS-XR-ipv4-io-oper:rete/nodi/nodi/stat e/traffico/icmp-status ip
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2	Valore di indice che identifica in modo univoco l'interfaccia a cui è applicabile questa voce. L'interfaccia identificata da un particolare valore di questo indice è la stessa interfaccia identificata dallo stesso valore di ifIndex della RFC 1573.	Cisco-IOS-XR-ipv4-io-oper:rete/nodi/nodo ipv
ipAdIntAddr	1.3.6.1.2.1.4.20.1.1	L'indirizzo IP a cui si riferiscono le informazioni di indirizzamento di questa voce.	Cisco-IOS-XR-ipv4-io-oper:rete/interfacce/inte ia/vrfs/vrf/detail/primary address
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3	Subnet mask associata all'indirizzo IP della voce. Il valore della maschera è un indirizzo IP con tutti i bit di rete impostati su 1 e tutti i bit	Cisco-IOS-XR-ipv4-io-oper:rete/interfacce/inte ia/vrfs/vrf/detail/prefix-l

ipAdEntBcastAddr	1.3.6.1.2.1.4.20.1.4	dell'host impostati su 0. Il valore del bit meno significativo nell'indirizzo di broadcast IP utilizzato per inviare datagrammi sull'interfaccia (logica) associata all'indirizzo IP di questa voce. Ad esempio, quando si utilizza l'indirizzo di broadcast standard Internet all-one, il valore sarà 1. Questo valore si applica sia agli indirizzi di broadcast di subnet che di rete utilizzati dall'entità in questa interfaccia (logica).	Cisco-IOS-XR-ipv4-io-oper:rete/interfacce/inte ia/vrfs/vrf/detail/direct-broadcast
IndirizzoFisicoMultimedialeIP	1.3.6.1.2.1.4.22.1.2	Indirizzo fisico dipendente dal supporto.	Cisco-IOS-XR-ipv4-arp oper:arp/nodes/node/e /entry/hardware-addres

IPMIB-COMMON

La tabella seguente rappresenta il nome e il numero OID e l'XPATH corrispondente da impostare sui gruppi di sensori di telemetria basati su modelli correlati alle statistiche IP.

Nome OID	Numero OID	Descrizione OID	XPATH
ipIfStatsHCOutTransmits	1.3.6.1.2.1.4.31.3.1.31	Il numero totale di datagrammi IP forniti da questa entità ai livelli inferiori per la trasmissione. Questo oggetto conta gli stessi datagrammi di ipIfStatsOutTransmits, ma consente valori maggiori. Le discontinuità nel valore di questo contatore possono verificarsi alla reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ipIfStatsDiscontinuityTime.	Cisco-IOS-XR-ipv4-io-oper:rete/nodi/nodo/st he/traffico/stati ipv4/pacchetti-inoltrati
ipIfStatsInReceives	1.3.6.1.2.1.4.31.3.1.3	Il numero totale di datagrammi IP di input ricevuti, inclusi quelli ricevuti per errore. Le discontinuità nel valore di questo contatore possono verificarsi alla reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ipIfStatsDiscontinuityTime.	Cisco-IOS-XR-ipv4-io-oper:rete/nodi/nodo/st he/traffico/stati ipv4/pacchetti di input
ipIfStatsHCInReceives	1.3.6.1.2.1.4.31.3.1.4	Il numero totale di datagrammi IP di input ricevuti, inclusi quelli ricevuti per errore. Questo oggetto conta gli	Cisco-IOS-XR-ipv4-io-oper:rete/nodi/nodo/st he/traffico/stati ipv4/pacchetti di input

		stessi datagrammi di ipIfStatsInReceives, ma consente valori più grandi. Le discontinuità nel valore di questo contatore possono verificarsi alla reinizializzazione del sistema di gestione e in altri momenti come indicato dal valore di ipIfStatsDiscontinuityTime.	

LLDP-MIB

La tabella seguente rappresenta il nome e il numero OID e l'XPATH corrispondente da impostare sui gruppi di sensori di telemetria basati su modelli correlati ai dati operativi LLDP (Link Layer Discovery Protocol) nel nodo monitorato.

Nome OID	Numero OID	Descrizione OID	XPATH
IDPorcaLocale	1.0.8802.1.1.2.1.3.7.1.3	Valore string utilizzato per identificare il componente porta associato a una determinata porta nel sistema locale.	Cisco-IOS-XR-etherne lldp-oper:lldp/nodes/node/ bors/devices/device/ll neighbor/port-id-detail
Sottotipo lldpLocPortId	1.0.8802.1.1.2.1.3.7.1.2	Tipo di codifica dell'identificatore di porta utilizzato nell'oggetto 'lldpLocPortId' associato.	Cisco-IOS-XR-etherne lldp-oper:lldp/nodes/node/ bors/devices/device/ll neighbor/mib/port-id-s type
Sottotipo lldpLocChassisId	1.0.8802.1.1.2.1.3.1	Tipo di codifica utilizzato per identificare lo chassis associato al sistema locale.	Cisco-IOS-XR-etherne lldp-oper:lldp/nodes/node/ bors/devices/device/ll neighbor/mib/chassis-sub-type
lldpLocSysName	1.0.8802.1.1.2.1.3.3	Valore stringa utilizzato per identificare il nome di sistema del sistema locale. Se l'agente locale supporta IETF RFC 3418, l'oggetto lldpLocSysName deve avere lo stesso valore dell'oggetto sysName.	Cisco-IOS-XR-etherne lldp-oper:lldp/nodes/node/ bors/devices/device/ll neighbor/detail/system name
lldpRemSysName	1.0.8802.1.1.2.1.4.1.1.9	Valore stringa utilizzato per identificare il nome di sistema del sistema remoto.	Cisco-IOS-XR-etherne lldp-oper:lldp/nodes/node/ bors/devices/device/ll neighbor/detail/system name
ID chassis lldpRem	1.0.8802.1.1.2.1.4.1.1.5	Valore stringa utilizzato per identificare il componente dello chassis associato al sistema remoto.	Cisco-IOS-XR-etherne lldp-oper:lldp/nodes/node/ bors/devices/device/ll

			neighbor/chassis-id
LldpRemChassisIdSubtype	1.0.8802.1.1.2.1.4.1.1.4	Tipo di codifica utilizzato per identificare lo chassis associato al sistema remoto.	Cisco-IOS-XR-ethern lldp-oper:lldp/nodes/node/ bors/devices/device/ll neighbor
Sottotipo lldpRemPortId	1.0.8802.1.1.2.1.4.1.1.6	Tipo di codifica dell'identificatore di porta utilizzato nell'oggetto 'lldpRemPortId' associato.	Cisco-IOS-XR-ethern lldp-oper:lldp/nodes/node/ bors/devices/device/ll neighbor
ID porta lldpRem	1.0.8802.1.1.2.1.4.1.1.7	Valore string utilizzato per identificare il componente porta associato al sistema remoto.	Cisco-IOS-XR-ethern lldp-oper:lldp/nodes/node/ bors/devices/device/ll neighbor
ID chassisLocLldp	1.0.8802.1.1.2.1.3.2	Valore string utilizzato per identificare il componente dello chassis associato al sistema locale.	Cisco-IOS-XR-ethern lldp-oper:lldp/nodes/node/ bors/details/detail/lldp- neighbor/chassis-id

MPLS-TE-STD-MIB

La tabella seguente rappresenta il nome e il numero OID e l'XPATH corrispondente da impostare sui gruppi di sensori di telemetria basati su modelli correlati ai valori operativi di Multiprotocol Label Switching (MPLS) Traffic Engineering sul dispositivo gestito.

Nome OID	Numero OID	Descrizione OID	XPATH
mplsNomeTunnel	1.3.6.1.2.1.10.166.3.2.2.1.5	Nome canonico assegnato al tunnel. Questo nome può essere usato per fare riferimento al tunnel sulla porta console dell'LSR. Se mplsTunnelIsIf è impostato su true, il valore di ifName dell'interfaccia corrispondente al tunnel deve essere uguale a mplsTunnelName. Vedere anche la descrizione di ifName nella RFC 2863.	Cisco-IOS-XR-mpls-t oper:mpls-te/p2p-p2r tunnel/tunnel-head/tu name
mplsTunnelDescr	1.3.6.1.2.1.10.166.3.2.2.1.6	Stringa di testo contenente informazioni sul tunnel. Se non è presente alcuna descrizione, l'oggetto contiene una stringa di lunghezza zero. Questo oggetto potrebbe non essere segnalato dai protocolli di segnalazione MPLS, di conseguenza il valore di questo oggetto in transito e	openconfig-network-instance:network-instance/network-instance/mpls/lsps/co ned-path/tunnels/tunnel/s escrizione

		gli LSR in uscita POTREBBERO essere generati automaticamente o assenti.	
mplsTunnelPerfHCPackets	1.3.6.1.2.1.10.166.3.2.9.1.2	Contatore ad alta capacità per il numero di pacchetti inoltrati dal tunnel.	openconfig-network-instance:network-instance/network-instance/mpls/lsps/co ned-path/tunnels/tunnel/s ontatori/pacchetti
mplsTunnelPerfHCBytes	1.3.6.1.2.1.10.166.3.2.9.1.5	Contatore ad alta capacità per il numero di byte inoltrati dal tunnel.	openconfig-network-instance:network-instance/network-instance/mpls/lsps/co ned-path/tunnels/tunnel/s ontatori/byte
mplsTunnelHopIpAddr	1.3.6.1.2.1.10.166.3.2.4.1.5	Indirizzo dell'hop del tunnel per questo hop del tunnel. Il tipo di questo indirizzo è determinato dal valore del corrispondente mplsTunnelHopAddrType. Il valore di questo oggetto non può essere modificato se il valore dell'oggetto mplsTunnelHopRowStatus corrispondente è 'active'.	Cisco-IOS-XR-mpls-t oper:mpls-te/p2p-p2r tunnel/tunnel-head/tu head/destinazione/in o-destinazione

RFC 2465-MIB

Nella tabella seguente vengono indicati il nome e il numero OID e l'XPATH corrispondente da impostare nei gruppi di sensori di telemetria basati su modelli correlati ai valori globali IPv6.

Nome OID	Numero OID	Descrizione OID	XPATH
ipv6AddrPfxLength	1.3.6.1.2.1.55.1.8.1.2	Lunghezza (in bit) del prefisso associato all'indirizzo IPv6 della voce.	Cisco-IOS-XR-ipv6-ma-oper:rete/nodi/nodo/inte a-dati/vrfs/vrf/brief/brief/in o/prefisso-lunghezza
ipv6AddrFlagAnycast	1.3.6.1.2.1.55.1.8.1.4	Questo oggetto ha il valore 'true(1)', se l'indirizzo è un indirizzo anycast e il valore 'false(2)' in caso contrario.	Cisco-IOS-XR-ipv6-ma-oper:rete/nodi/nodo/inte a-dati/vrfs/vrf/brief/brief/ad s/is-anycast

SNMP-MIB

La tabella seguente rappresenta il nome e il numero OID e l'XPATH corrispondente da impostare sui gruppi di sensori di telemetria basati su modello correlati all'agente SNMP stesso, se disponibile.

Nome OID	Numero OID	Descrizione OID	XPATH
TempoSuSistema	1.3.6.1.2.1.1.3	Stringa che rappresenta il tempo di attività del sistema	Cisco-IOS-XR-snmp-age oper:snmp/information/s -up-time/
IDEggetto	1.1.3.6.1.2.1.1.2.0	Stringa che rappresenta l'OID di sistema	Cisco-IOS-XR-snmp-age oper:snmp/information/s -oid/
sysDescr	1.3.6.1.2.1.1.1	Stringa che rappresenta la descrizione del sistema	Cisco-IOS-XR-snmp-age oper:snmp/information/s -descr

TCP-MIB

Nella tabella seguente vengono indicati il nome e il numero OID e l'XPATH corrispondente da configurare nei gruppi di sensori di telemetria basati su modelli correlati ai contatori specifici TCP.

Nome OID	Numero OID	Descrizione OID	XPATH
ErroriInTCP	1.3.6.1.2.1.6.14	Il numero totale di segmenti ricevuti per errore (ad esempio, checksum TCP errati).	Cisco-IOS-XR-ip-tcp-oper:tcp/nodes/node/sta /ipv4-traffic/tcp-checksur error-packets
InSegmentiTCP	1.3.6.1.2.1.6.10	Numero totale di segmenti ricevuti, inclusi quelli ricevuti per errore. Il conteggio include i segmenti ricevuti sulle connessioni attualmente stabilite.	Cisco-IOS-XR-ip-tcp-oper:tcp/nodes/node/sta /ipv4-traffic/tcp-input-pac
SegmentiTCP	1.3.6.1.2.1.6.11	Il numero totale di segmenti inviati, inclusi quelli sulle connessioni correnti ma esclusi quelli che contengono solo ottetti ritrasmessi.	Cisco-IOS-XR-ip-tcp-oper:tcp/nodes/node/sta /ipv4-traffic/tcp-output-pa

UDP-MIB

La tabella seguente rappresenta il nome e il numero OID e l'XPATH corrispondente da configurare nei gruppi di sensori di telemetria basati su modello correlati ai contatori UDP specifici.

Nome OID	Numero OID	Descrizione OID	XPATH
DatagrammiUDPut	1.3.6.1.2.1.7.4	Numero totale di datagrammi UDP inviati da questa entità.	Cisco-IOS-XR-ip-udp-oper:/udp/nodes/node/st s/ipv4-traffic/udp-output- packets Cisco-IOS-XR-ip-udp-oper:/udp/nodes/node/st s/ipv6-traffic/udp-output- packets
udpNoPorts	1.3.6.1.2.1.7.2	Totale dei datagrammi UDP ricevuti per i quali non era presente alcuna applicazione alla porta di destinazione.	Cisco-IOS-XR-ip-udp-oper:/udp/nodes/node/st s/ipv4-traffic/udp-no-port packets Cisco-IOS-XR-ip-udp-

ErroriInUDP	1.3.6.1.2.1.7.3	Numero di datagrammi UDP ricevuti che non è stato possibile recapitare per motivi diversi dalla mancanza di un'applicazione alla porta di destinazione.	oper:/udp/nodes/node/st s/ipv6-traffic/udp-no-port packets Cisco-IOS-XR-ip-udp- oper:/udp/nodes/node/st s/ipv4-traffic/udp-checks error-packets Cisco-IOS-XR-ip-udp- oper:/udp/nodes/node/st s/ipv6-traffic/udp-checks error-packets
datagrammiUDP	1.3.6.1.2.1.7.1	Numero totale di datagrammi UDP forniti agli utenti UDP.	Cisco-IOS-XR-ip-udp- oper:/udp/nodes/node/st s/ipv4-traffic/udp-input- packets Cisco-IOS-XR-ip-udp- oper:/udp/nodes/node/st s/ipv6-traffic/udp-input- packets

Migrazione trap SNMP

Le trap SNMP sono messaggi attivati da eventi dinamici sul dispositivo gestito. Questi messaggi si comportano in modo analogo al concetto di EDT descritto in precedenza.

Sul lato configurazione, MDT permette la stessa struttura per l'EDT, che dipende dall'implementazione sul collettore di telemetria in termini di scelta o capacità di chiamata in ingresso o in uscita.

Considerazioni sulla sicurezza

SNMPv2 utilizza solo la community come meccanismo di autenticazione/autorizzazione. Tuttavia, come descritto in precedenza nella sezione SNMP, È possibile utilizzare le credenziali per l'autenticazione e il modello di crittografia AES per la protezione delle informazioni.

Nell'approccio telemetrico, IOS XR consente l'utilizzo di tecniche gRPC/TLS basate sui certificati per eseguire l'autenticazione. Questi certificati possono essere utilizzati con un punto di attendibilità centrale, ad esempio un server CA. Dopo il processo di creazione di una relazione di trust, tutti i messaggi di telemetria vengono inviati all'interno di una sessione RPC crittografata con TLS che offre gli stessi vantaggi di SNMPv3.