# SCAP v2 Endpoint Data Collection

# Purpose and Scope

The purpose of this document is to describe the architectural components involved in implementing SCAPv2 endpoint data collection functions and their interactions with one-another.

# Overview of Architectural Components and Operations

**Endpoint:** The target of a posture assessment. It reports information to the *Posture Collection Service* based on change events and responds to direct queries from the *Posture Collection Service* about the endpoint’s configuration.

**Posture Collection Service:** Queries *Endpoints* to collect specific posture (configuration) data. These queries may contain SCAP Content retrieved from an *SCAP Content Repository*. It sanity checks the posture data it receives and stores it in the *Configuration Management Database* (*CMDB*) for later use. It also reports newly collected posture data to entities which have subscribed to receive it (i.e., a *Posture Evaluator*)..

# Components

The following subsections describe each component in the SCAP v2 conceptual architecture.

## Endpoint

The *Endpoint* is responsible for reporting posture data to the *Posture Collection Service* over Interface I1. To do this, an *Endpoint* is provisioned with a Posture Collection Engine capable of collecting posture data and reporting that data to the Posture Collection Manager on the *Posture Collection Service*. The reporting of posture data by a Posture Collection Engine may be driven by change events on the *Endpoint* or by direct queries from the Posture Collection Managerover Interface I1. This means that a Posture Collection Engine must be able to detect changes to monitored posture data and report them as soon as they are noticed. Prior to reporting posture data to the Posture Collection Manager, the Posture Collection Engine may process the data in some way to ensure that it is in a usable form. Processing might include structuring the information into a standard format, transforming it into an alternate representation, and/or performing pre-processing so that the Posture Collection Manager receives processing results rather than raw data. Lastly, a Posture Collection Engine must be able to establish a secure communication channel with the Posture Collection Manager in which to transmit and receive information. Posture Collection Engines on the *Endpoint* must be able to provide the following capabilities.

* **Deliver Requests:** Deliver collection requests to the appropriate collection mechanism on the *Endpoint*.
* **Deliver Posture Data:** Deliver posture data collected by collection mechanisms on the *Endpoint* to the Posture Collection Manager for validation and storage.
* **Discover Services:** Discover authorized Posture Collection Services from which it can receive collection requests and send collected posture data.
* **Establish Secure Connections:** Provide cryptographic protection for communications with the Posture Collection Manager.

## Posture Collection Service

The *Posture Collection Service* receives posture data from an *Endpoint* over Interface I1, performs basic sanity checking on received data, and stores the posture data in the *CMDB* leveraging Interface I3. The *Posture Collection Service* receives the posture data via a Posture Collection Manager. The Posture Collection Manager can obtain specific posture data from an *Endpoint*, by sending a query to the Posture Collection Engine over Interface I1. The query may include or otherwise use SCAP Content retrieved from the *SCAP Content Repository* using Interface I2. Lastly, the Posture Collection Manager must be able to manage secure communication channels with one or more *Endpoint*s. Posture Collection Managers on the *Posture Collection Service* must be able to provide the following capabilities.

* **Query Posture Data:** Send collection requests to Posture Collection Engine to retrieve current posture data.
* **Validate Posture Data:** Perform basic sanity checking on collected posture data. It may perform additional validation on the collected posture data.
* **Store Posture Data:** Store collected posture data in the *CMDB*.
* **Establish Secure Connections:** Provide cryptographic protection for communications with a Posture Collection Engine.
* **Manage Connections:** Manage communication channels with one or more Posture Collection Engines.

### Interface I1 – Endpoint Data Collection and Reporting



Figure 1: Interface for Endpoint Data Collection and Reporting.

Interface I1 represents the interface between an *Endpoint* and the *Posture Collection Service* which is responsible for reporting posture data from the *Endpoint* to the *Posture Collection Service* for storage in the *CMDB*. Implementations of Interface I1 should provide the following capabilities.

**Endpoint Health Request (Query-Response)**

The *Posture Collection Service* sends a query to the *Endpoint* identifying specific posture data that the *Endpoint* should collect and report back. Upon receipt of this query, the *Endpoint* collects the requested posture data and reports back to the *Posture Collection Service* for storage in the *CMDB*.

**Endpoint Subscription Request (Subscribe-Post)**

The *Posture Collection Service* sends a subscription request to the *Endpoint* that identifies the types of posture data that the *Endpoint* should monitor and report upon. The *Endpoint* saves this request and monitors the state of its posture data to detect changes that match the subscription parameters. When the *Endpoint* detects a change that matches the subscription parameters, it immediately reports the posture data to the *Posture Collection Service* for storage in the *CMDB*.

### Interface I3 – Posture Data Storage and Retrieval

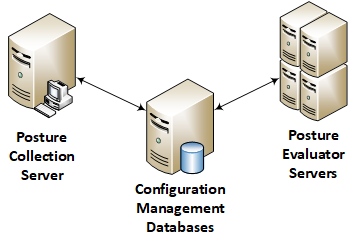


Figure 2: Interface for Posture Data Storage and Retrieval.

Interface I3 represents the interfaces between the *Posture Collection Service* and the *CMDB* to support the storage of collected posture data as well as the *Posture Evaluators* and the *CMDB* to support the query of posture data and the storage of assessment results. Protocols that implement Interface I3 should provide the following capabilities.

**Post Collected Posture Data (Data Push – Response)**

The *Posture Collection Service* receives posture data from target *Endpoints*, the posture data is pushed to the *CMDB* along with any relevant contextual metadata. The *CMDB* receives the posture data and metadata, stores it, and responds to the *Posture Collection Service* with pointers to information as stored in its tables.

**Query Posture Data for Evaluation (Query – Response)**

The *Posture Evaluator* requires posture data to perform an assessment of a target *Endpoint* and queries the *CMDB*. The *CMDB* receives the query and parameters, gathers the requested information, if present, and returns it to the *Posture Evaluator* along with relevant contextual metadata. If the *CMDB* does not have the requested information, it sends a response to the *Posture Evaluator* indicating that posture data matching the query could not be found.

**Post Evaluated Posture Data (Data Push – Response)**

After the assessment of posture data, the results are pushed to the *CMDB*. The *CMDB* responds to the *Posture Evaluator* with pointers to the results as stored within its tables.

### Interface I4 – Remote Data Collection for Evaluation

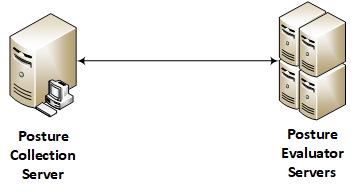


Figure 3: Interface for Remote Data Collection and Evaluation.

Interface I4 represents the interfaces between the *Posture Collection Service* and the *Posture Evaluator* to support the collection of posture data from target *Endpoints* when the posture data is not available in the *CMDB*. Protocols that implement Interface I4 should provide the following capabilities.

**Posture Collection Service Query (Query – Response)**

The *Posture Evaluator* queries the *Posture Collection Service* for posture data required in an assessment because that information was not available in the *CMDB*. The query may contain references to SCAP Content stored in an *SCAP Content Repository*. The *Posture Collection Service* receives the request and queries all targeted *Endpoints*. Target *Endpoints* collect the required posture data and report it to the *Posture Collection Service*. The *Posture Collection Service* posts the posture data to the *CMDB* which responds with pointers to the posture data as stored within its tables. The *Posture Collection Service* forwards pointers to the posture data to the *Posture Evaluator*. The *Posture Evaluator* queries the *CMDB* using the pointers to acquire the required posture data to perform the assessment.

**Posture Collection Service Subscription Request (Subscribe – Post)**

A *Posture Evaluator* may wish to perform certain assessments when new posture data is available. To do this, the *Posture Evaluator* requests a subscription from the *Posture Collection Service*. The request is parameterized and may reference SCAP Content from an *SCAP Repository* to identify the posture data the *Posture Evaluator* wants to be alerted about. In this subscription request, the *Posture Evaluator* may specify which *Endpoints* it wishes to receive updates from as well as the periodicity in which the *Posture Collection Service* should query the *Endpoints* for updates if it does not establish real-time subscriptions to the *Endpoints*.

When the *Posture Collection Service* receives new posture data (either due to a subscription fulfillment or due to a query) that matches the criteria given in a *Posture Evaluator* subscription request, it sends the posture data to the *CMDB* and forwards the pointers to the *Posture Evaluator*. The *Posture Evaluator* can then use those pointers to retrieve the posture data from the *CMDB*.

## SCAP v2 Workflows

The following subsections describe the possible workflows between components that occur in the SCAP v2 architecture.

### Posture Data Collection Workflow

The Posture Data Collection Workflow, shown in Figure 7, describes the interactions between components of the architecture in support of the collection of posture data. In this workflow, there are multiple starting points to accommodate query-based and event-based collection covering a range of possible scenarios. Examples include:

* Query-based collection of posture data with SCAP Content. This may be triggered by the *Posture Collection Service* or *Posture Evaluator* (from Workflow 2)
* Query-based collection of posture data without SCAP Content. This may be triggered by the *Posture Collection Service* or *Posture Evaluator* (from Workflow 2)
* Collection and reporting of posture data based on a change event
* Delivery of posture data based on a change event

Each of these collections terminate after the *Posture Collection Service* stores the newly collected posture data in the *CMDB* and recieves pointers to that posture data, which it can use to drive follow-up actions like triggering an evaluation.

This workflow also serves as a starting point for event-based evaluation when the *Posture Collection Service* receives posture data of interest to the *Posture Evaluator*. This terminates in the Posture Data Evaluation work flow shown in Figure 8 once the posture data is evaluated, the assessment results are stored, and the *Posture Evaluator* receives pointers to the assessment results in the *CMDB*.

****

Figure 4: Posture Data Collection Workflow.

### Posture Data Evaluation Workflow

Similarly, the Posture Data Evaluation Workflow, shown in Figure 8, describes the interactions between components of the architecture in support of the evaluation of posture data. As before, there are multiple possible starting points to accommodate different scenarios. Examples include:

* Evaluation of posture data using SCAP Content. This may be triggered by the *Posture Evaluator* or *Posture Collection Service* (from Workflow 1)
* Evaluation of posture data without SCAP Content. This may be triggered by the *Posture Evaluator* or *Posture Collection Service* (from Workflow 1)

These evaluations terminate after the *Posture Evaluator* evaluates the posture data, stores the assessment results in the *CMDB*, and receives pointers to those assessment results.

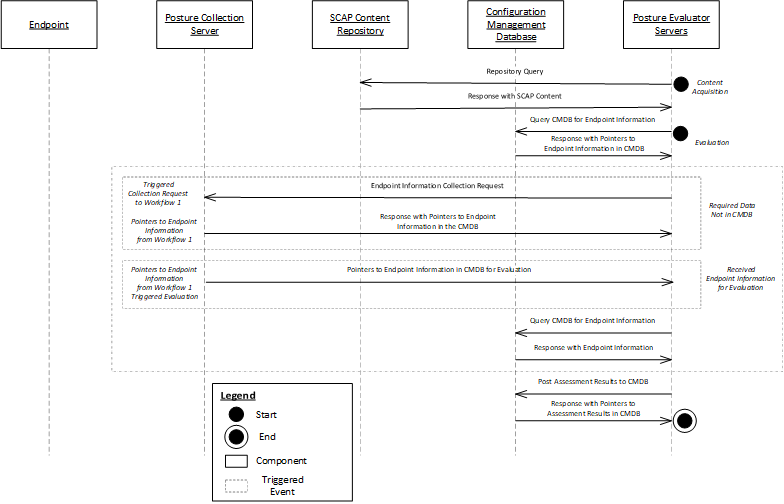


Figure 5: Posture Data Evaluation Workflow.