Security Automation and Continuous Monitoring (SACM)

An IETF Working Group

Lisa Lorenzin

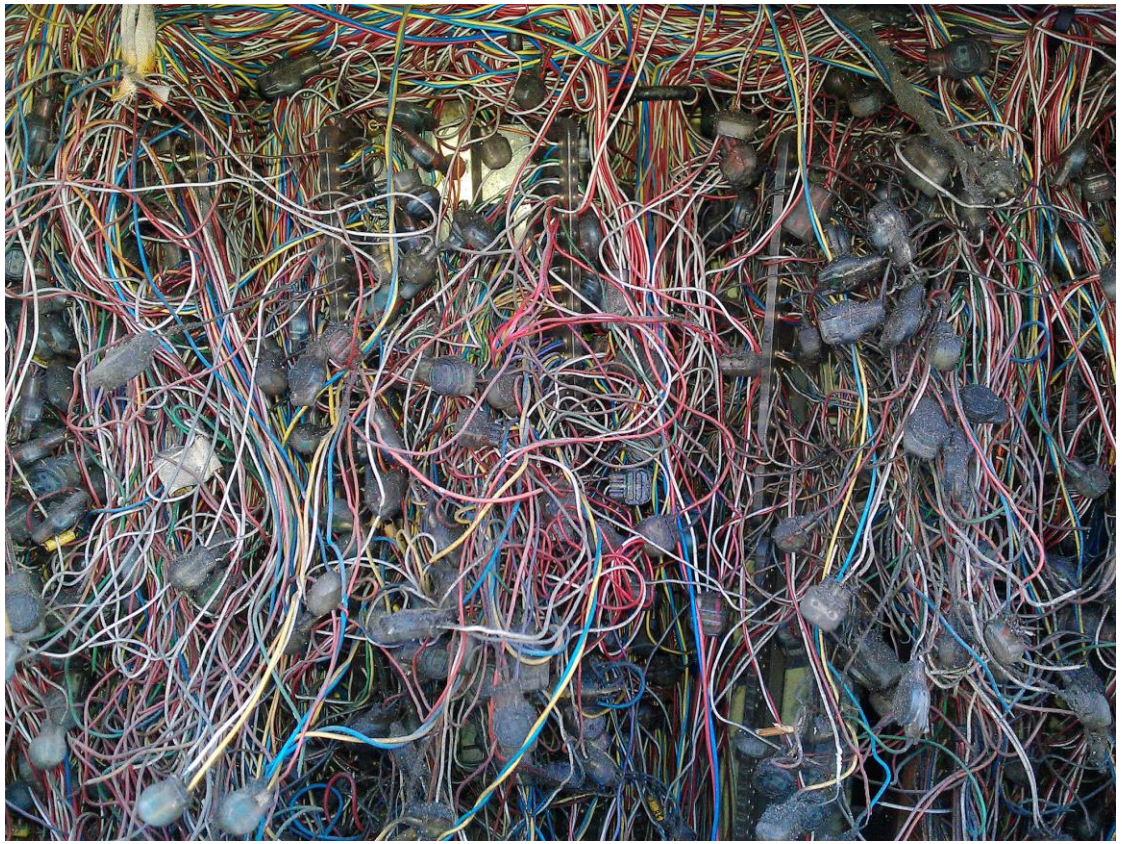
9/10/2015

A Preface

THREE TRUTHS

1. Threat Agents Continue To Surprise

2. Complexity Continues To Increase



3. Our Resources Become Scarcer

The Basics (still) Need To Be Automated

- Configuration Management
- Vulnerability Management
- Inventory Management

An IETF Working Group

SACM INTRODUCTION

The Gist

Enterprise assessment of endpoint posture

1. Identify endpoints
2. Determine specific endpoint elements to assess
3. Collect actual value of elements
4. Compare actual to expected values
5. Report

(By the way: Be enterprise-wide and interoperable)

(In effect: Define an ecosystem)

Endpoint Posture

What does “endpoint posture” include?

- Configuration
- Vulnerability
- Inventory

SACM Deliverables

- Information Model
- Supporting Data Model and Operations
- Architecture and Protocols

WHAT WE’RE DOING NOW

Done or In-progress Drafts

- Use Cases with usage scenarios (RFC 7632)
- Requirements (in progress)
- Architecture (in progress)
- Information Model (in progress)
- Terminology (in progress)

Use Cases

- Define, publish, query and retrieve security automation data
- Endpoint identification and assessment planning
- Endpoint posture attribute value collection
- Posture attribute evaluation

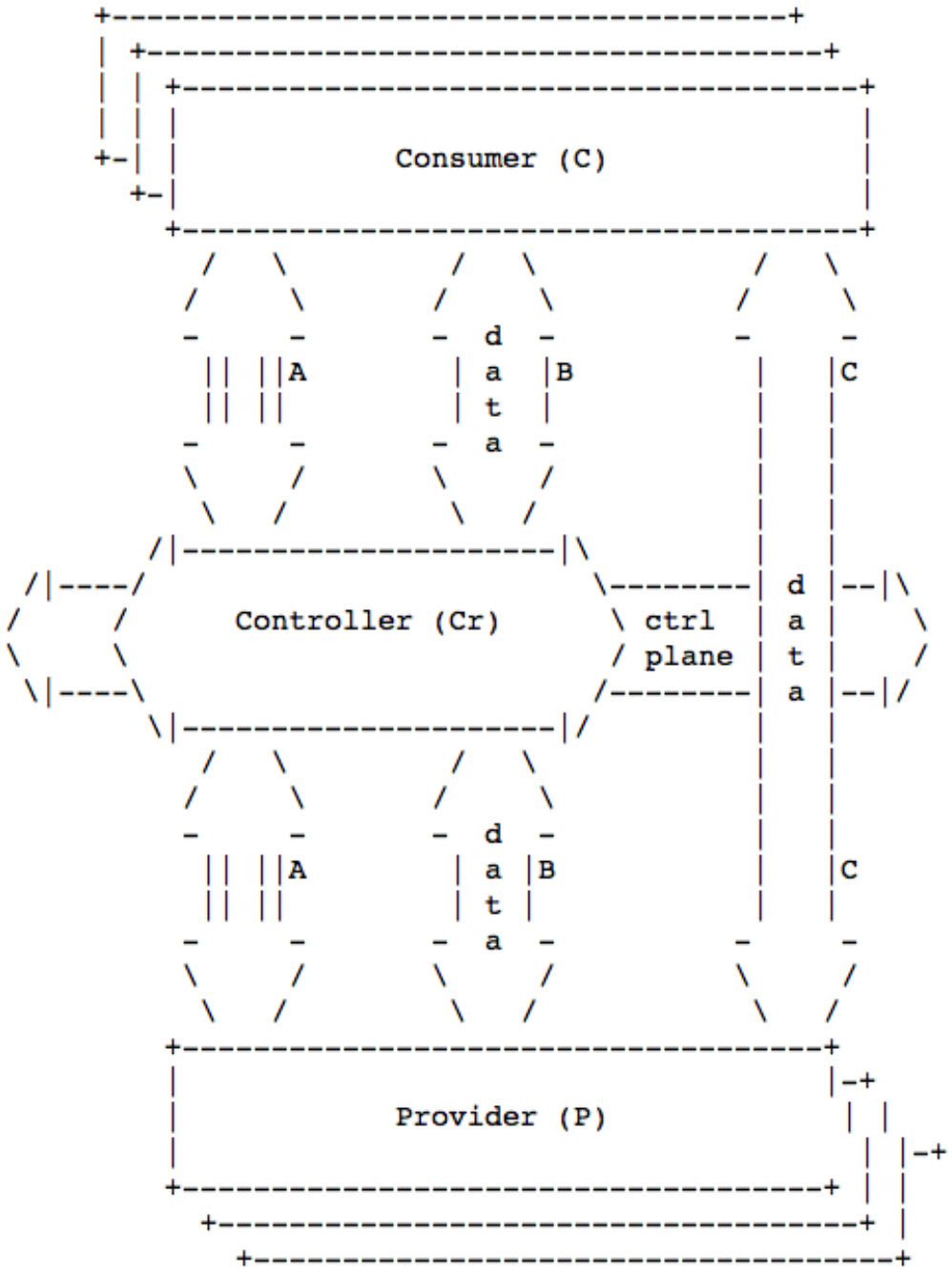
Usage Scenarios

- Definition and publication of automatable configuration checklists
- Automated checklist verification
- Detection of posture deviations
- Endpoint information analysis and reporting
- Asynchronous compliance/vulnerability assessment at Ice Station Zebra
- Identification and retrieval of guidance
- Guidance change detection

SACM Requirements

- General requirements (ecosystem-wide)
- Architecture
- Information Model
- Data Model
- Data Model Operations
- Transport Protocols

SACM Architecture



SACM Architecture

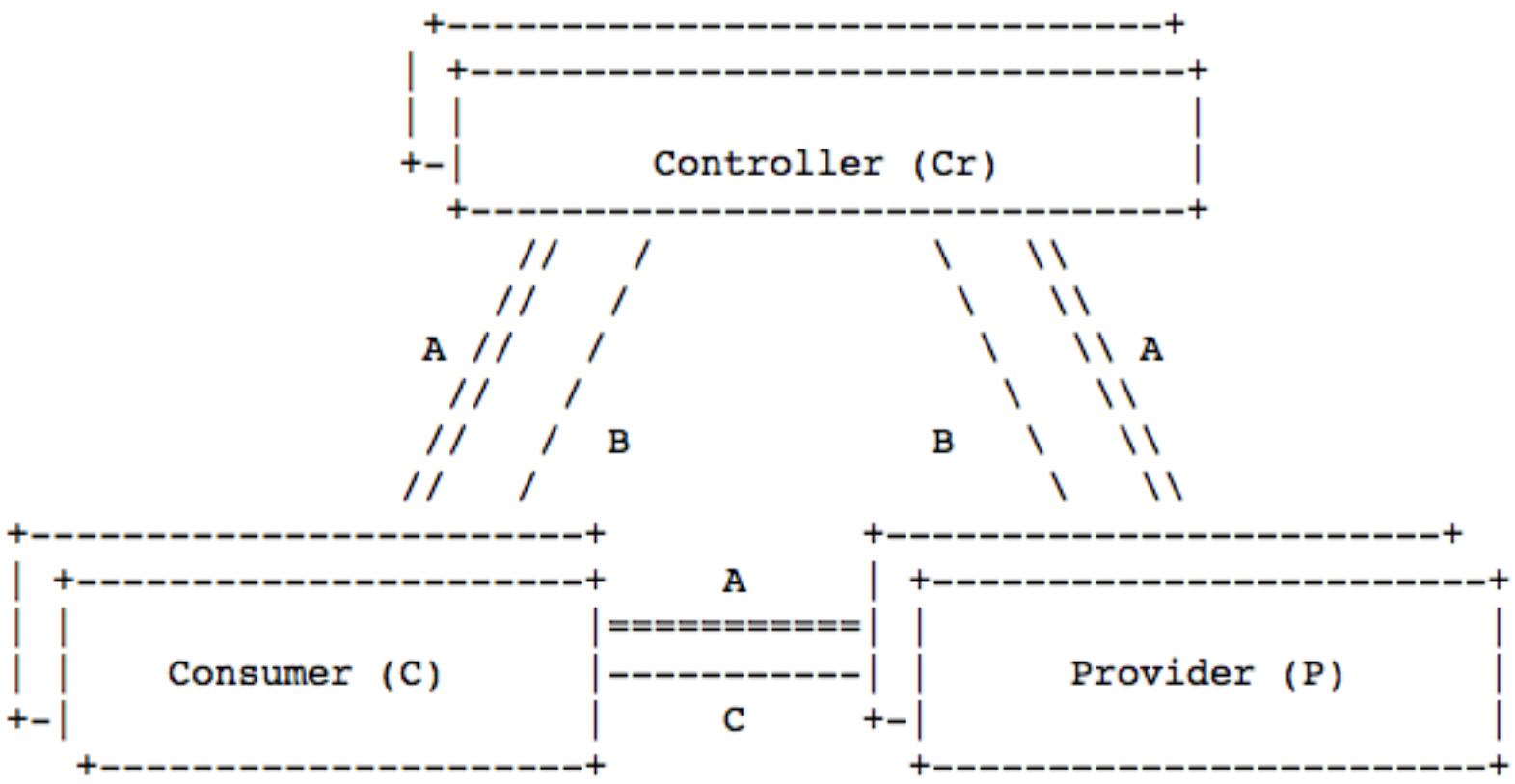


Figure 2: Communications Model

SACM Information Model

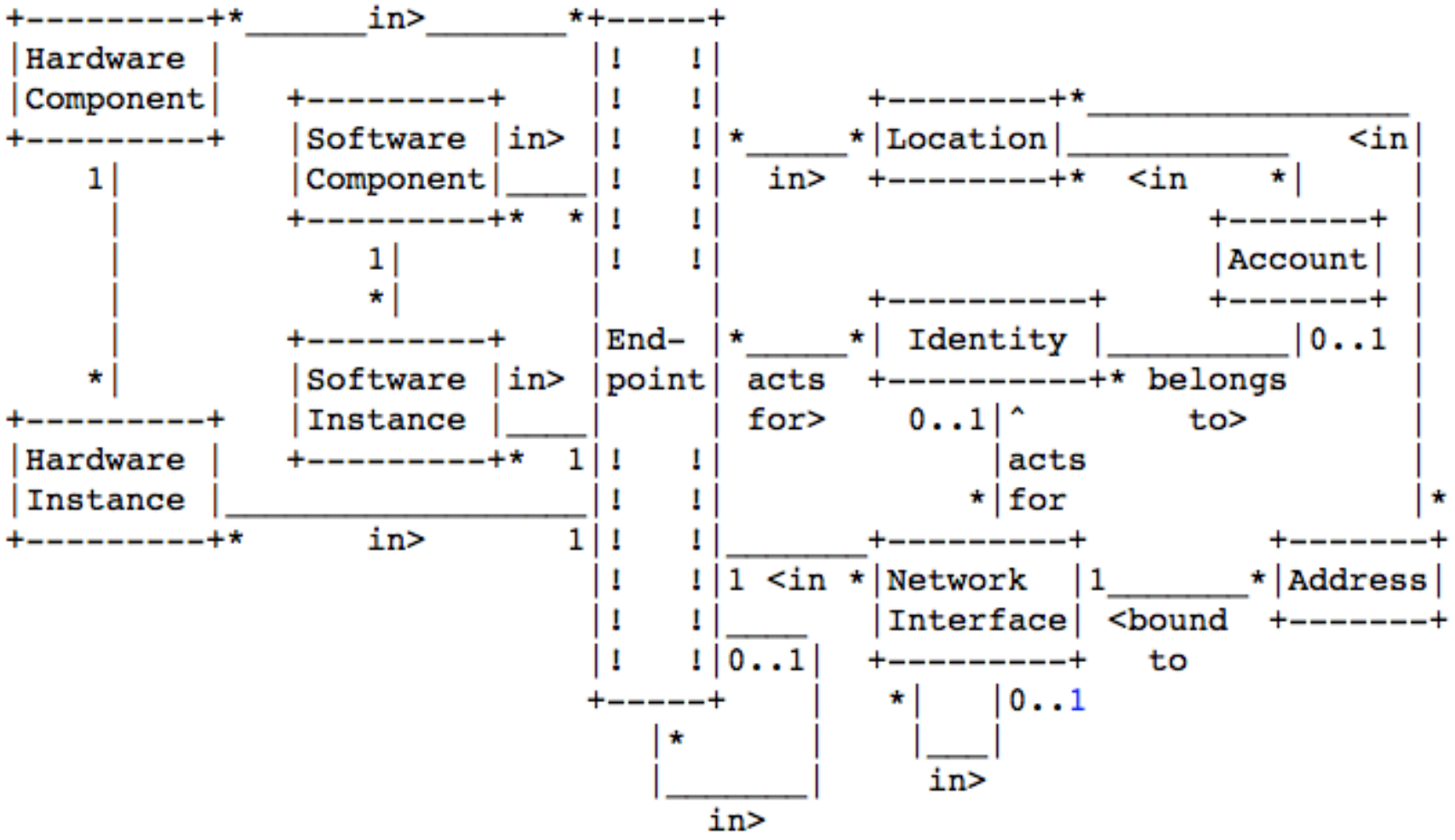


Figure 1: Model of an Endpoint

SACM Information Model

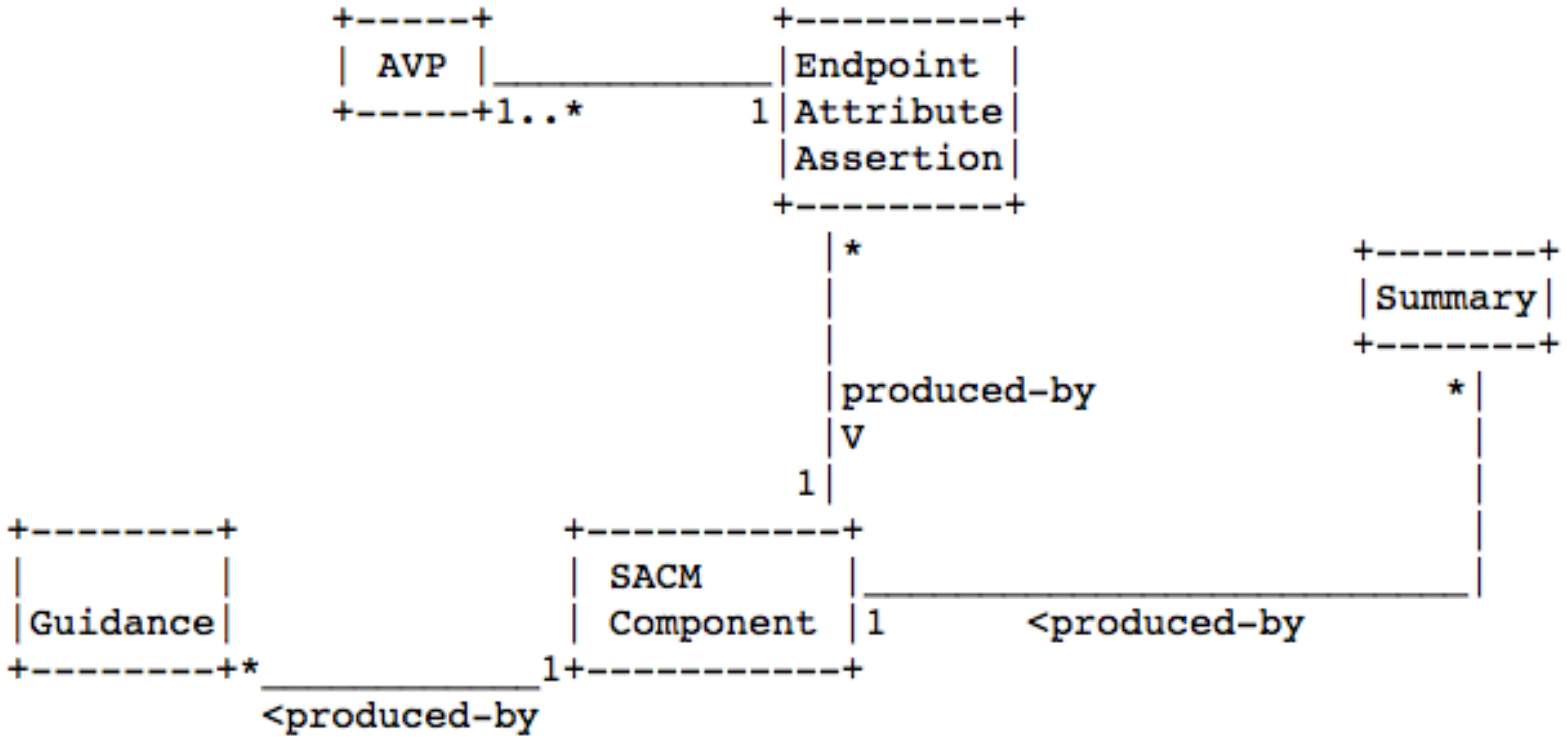


Figure 2: Information Elements

SACM Terminology

A living document; source of record for:

- SACM-specific terminology
- Terms leveraged by SACM but defined elsewhere

Strives to be semantically accurate.

EXAMPLE APPLICATIONS OF ARCHITECTURE TO USAGE SCENARIOS

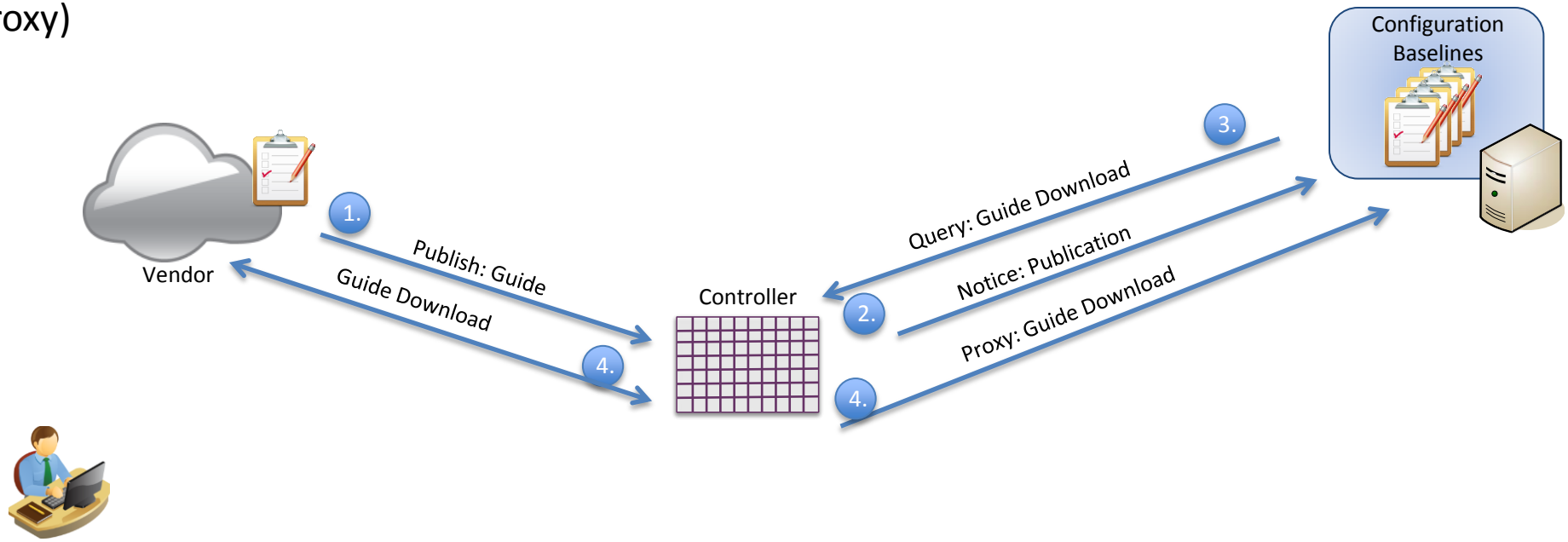
Three Modes for Controller

- Broker: Controller brokers the authorization and redirects consumers to producers
- Repository: Controller stores data from producers and provides data in response to consumer requests
- Proxy: Controller acts as proxy, collecting the data from the producers and presenting it to consumers

2.2.1 – DEFINITION AND PUBLICATION OF AUTOMATABLE CONFIGURATION GUIDES

2.2.1 – Define and Publish Automatable Configuration Guides

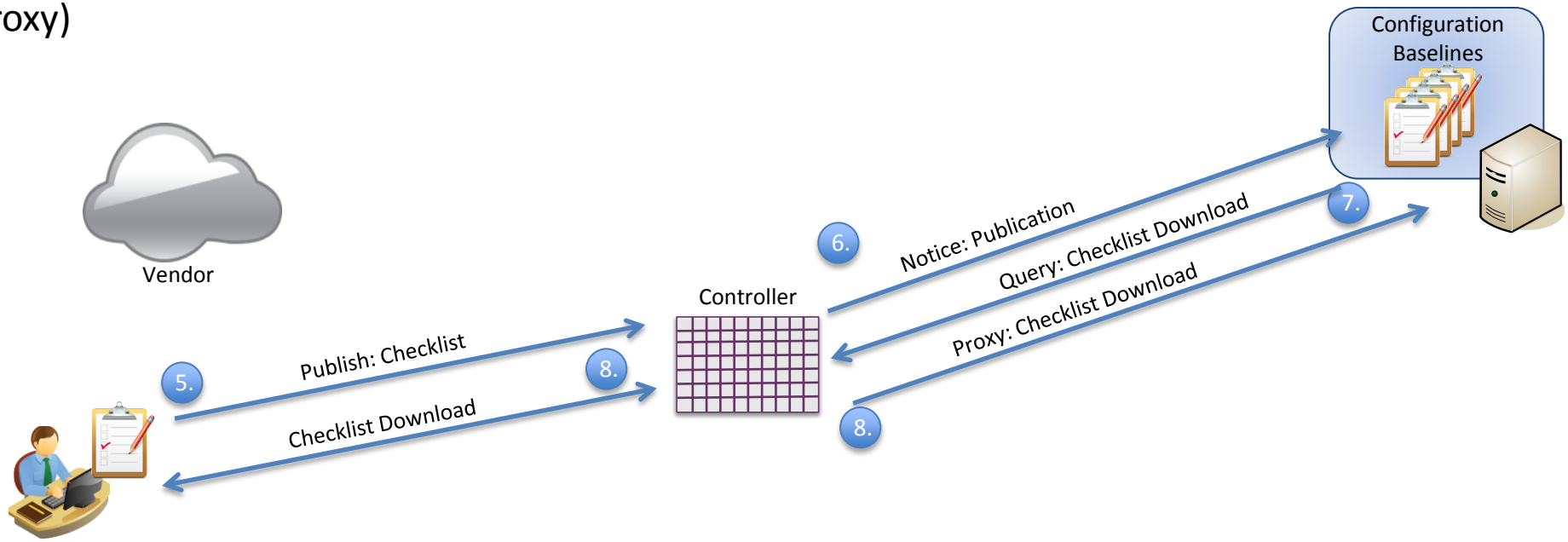
(Proxy)



1. Vendor publishes guide information to Controller
2. Controller notifies Consumer: Configuration Service
3. Configuration Service requests guide from Controller
4. Controller proxies the retrieval of guides

2.2.1 – Define and Publish Automatable Configuration Guides

(Proxy)

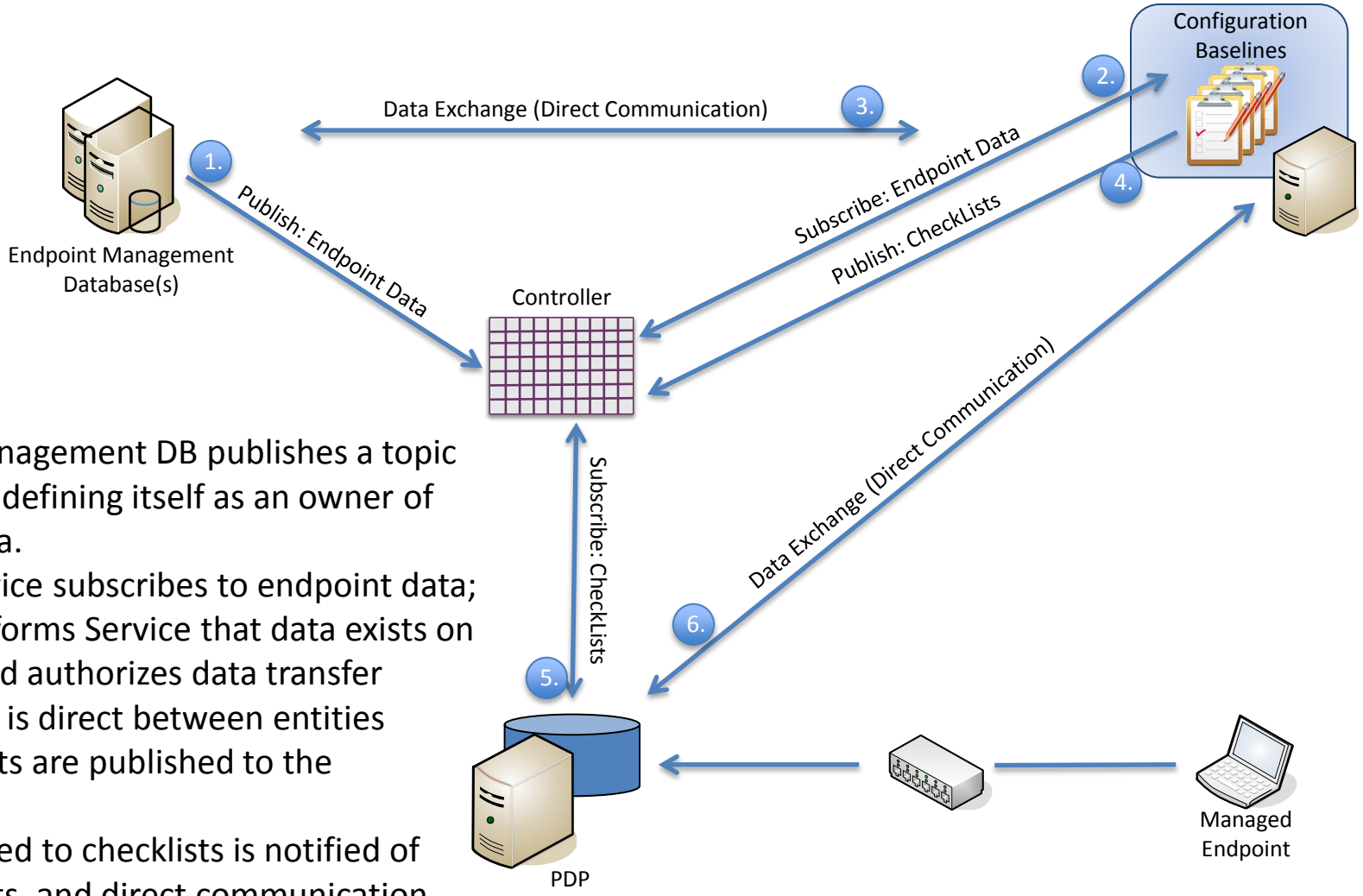


1. Vendor publishes guide information to Controller
2. Controller notifies Consumer: Configuration Service
3. Configuration Service requests guide from Controller
4. Controller proxies the retrieval of guides
5. Admin publishes custom checklists to Controller
6. Controller notifies Consumer: Configuration Service
7. Configuration Service requests checklists from Controller
8. Controller proxies the retrieval of checklists

2.2.2 – AUTOMATED CHECKLIST VERIFICATION

2.2.2 – Automated Checklist Verification

(Broker)

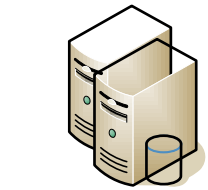


1. Endpoint Management DB publishes a topic to Controller defining itself as an owner of endpoint data.
2. Baseline Service subscribes to endpoint data; Controller informs Service that data exists on the EMDB and authorizes data transfer
3. Data transfer is direct between entities
4. New checklists are published to the Controller.
5. PDP subscribed to checklists is notified of new checklists, and direct communication is authorized
6. PDP downloads checklists from Baseline Service directly

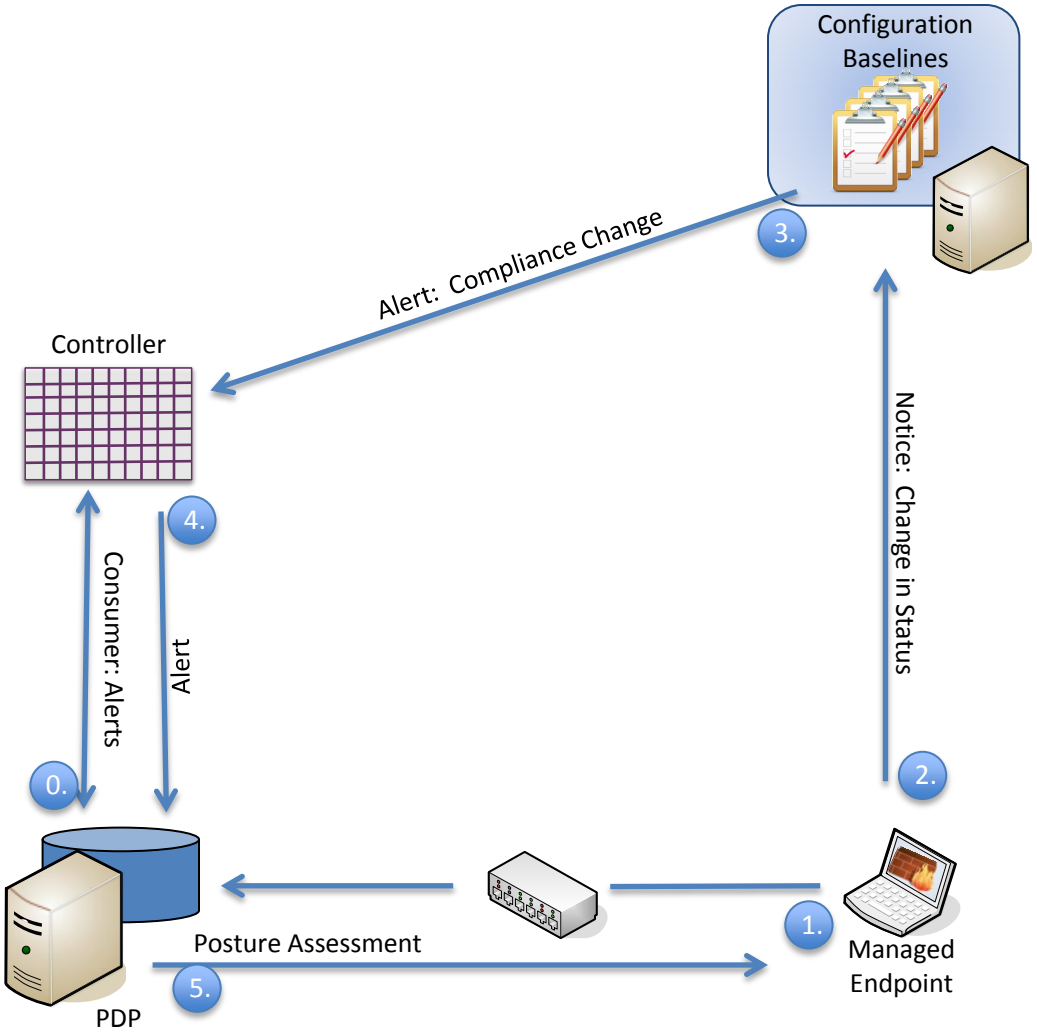
2.2.3 – DETECTION OF POSTURE DEVIATIONS

2.2.3 – Detection of Posture Deviations

(Repository)



Endpoint Management Database(s)

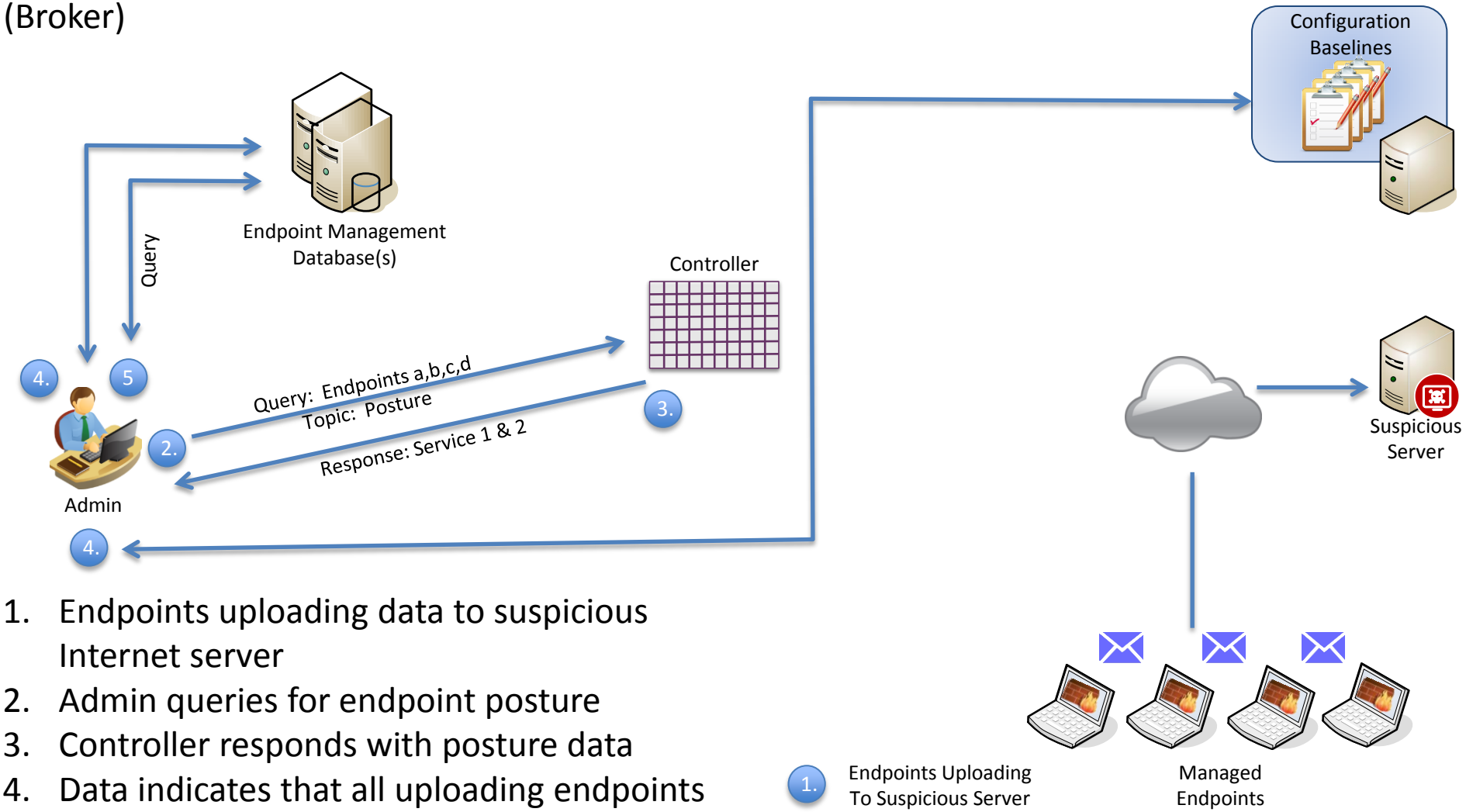


1. Endpoint user disables firewall
2. Endpoint client sends notice to Compliance Service
3. Compliance Service publishes alert
4. Assessment Service is notified
5. Endpoint is assessed

2.2.4 – ENDPOINT INFORMATION ANALYSIS AND REPORTING

2.2.4 – Endpoint Information Analysis and Reporting

(Broker)

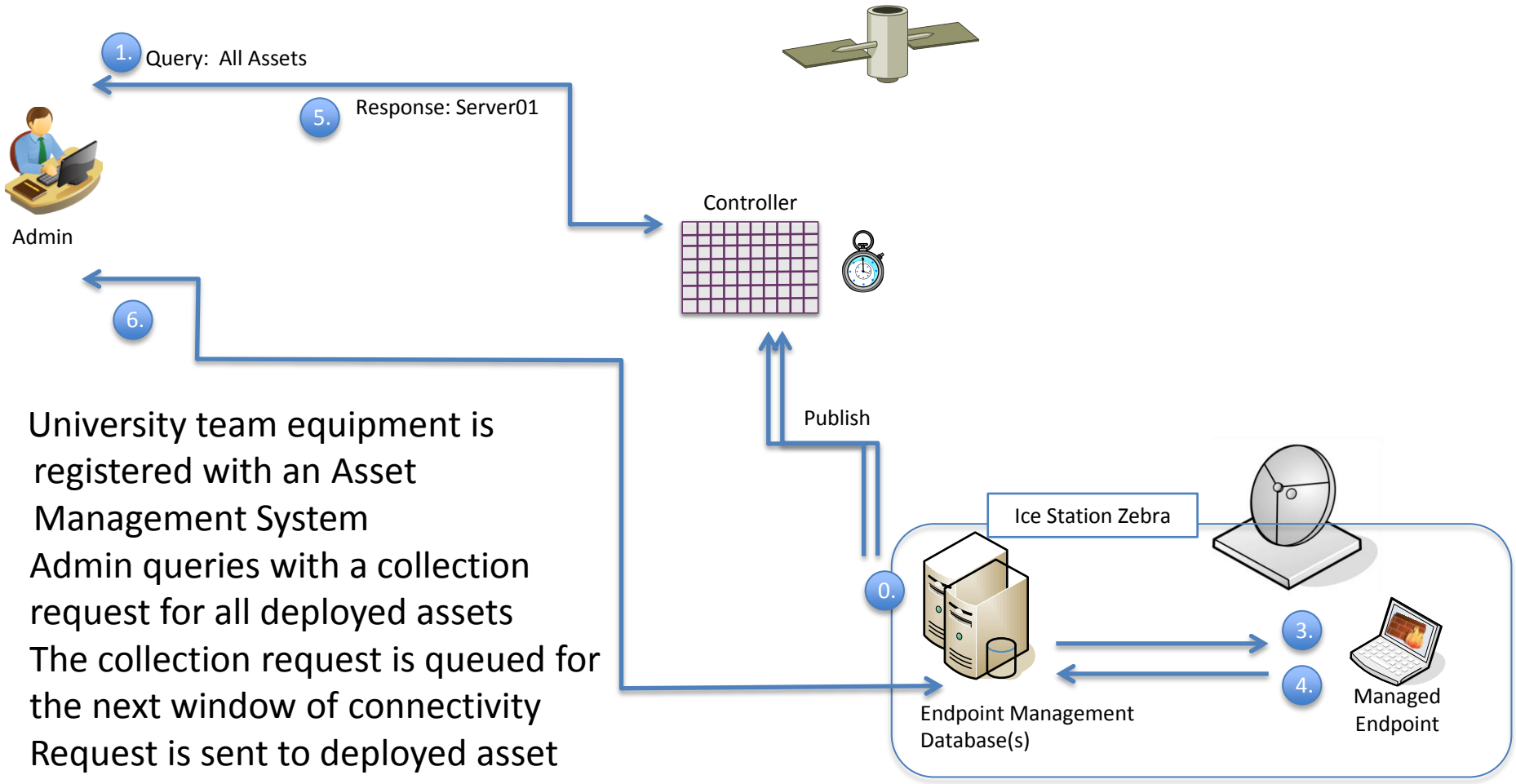


1. Endpoints uploading data to suspicious Internet server
2. Admin queries for endpoint posture
3. Controller responds with posture data
4. Data indicates that all uploading endpoints have a particular app Installed
5. Admin queries to see which other endpoints have the same app installed

2.2.5 – ASYNCHRONOUS COMPLIANCE / VULNERABILITY ASSESSMENT AT ICE STATION ZEBRA

2.2.5 – Async Compliance/Vulnerability Assessment at Ice Station Zebra

(Repository)

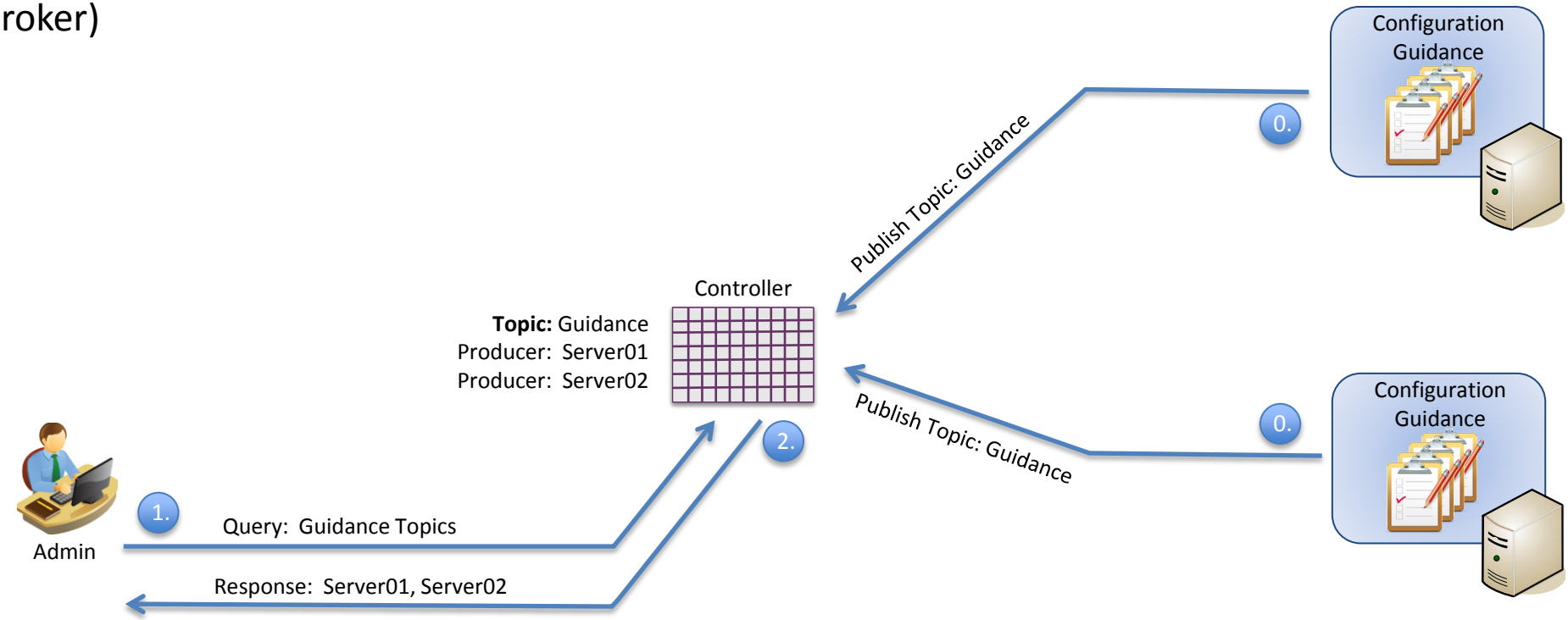


0. University team equipment is registered with an Asset Management System
1. Admin queries with a collection request for all deployed assets
2. The collection request is queued for the next window of connectivity
3. Request is sent to deployed asset
4. Asset fulfills the request and queues the results for the next return opportunity
5. Results are sent back to the admin
6. Admin compares results against Asset Management System data

2.2.6 – IDENTIFICATION AND RETRIEVAL OF GUIDANCE

2.2.6 – Identification and Retrieval of Guidance

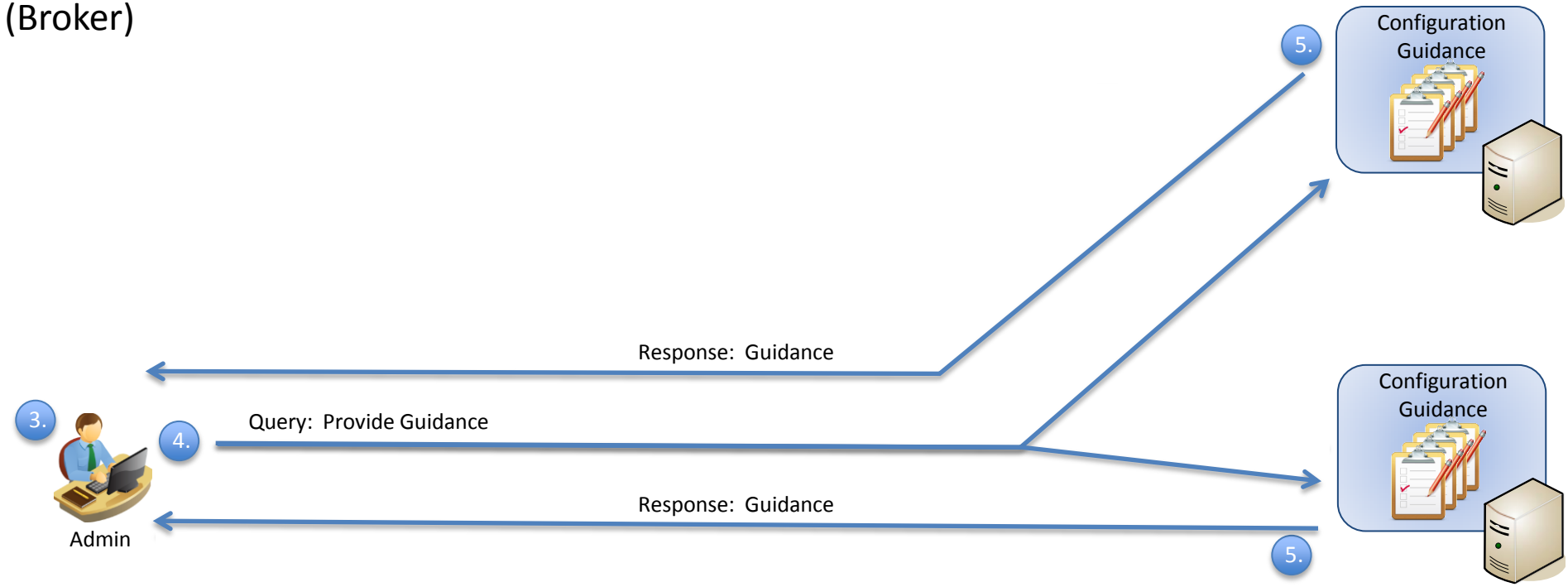
(Broker)



0. Data stores publish lists of the guidance they contain
1. Admin queries the Controller to find out which data stores contain what content
2. Controller replies with list of data stores

2.2.6 – Identification and Retrieval of Guidance

(Broker)

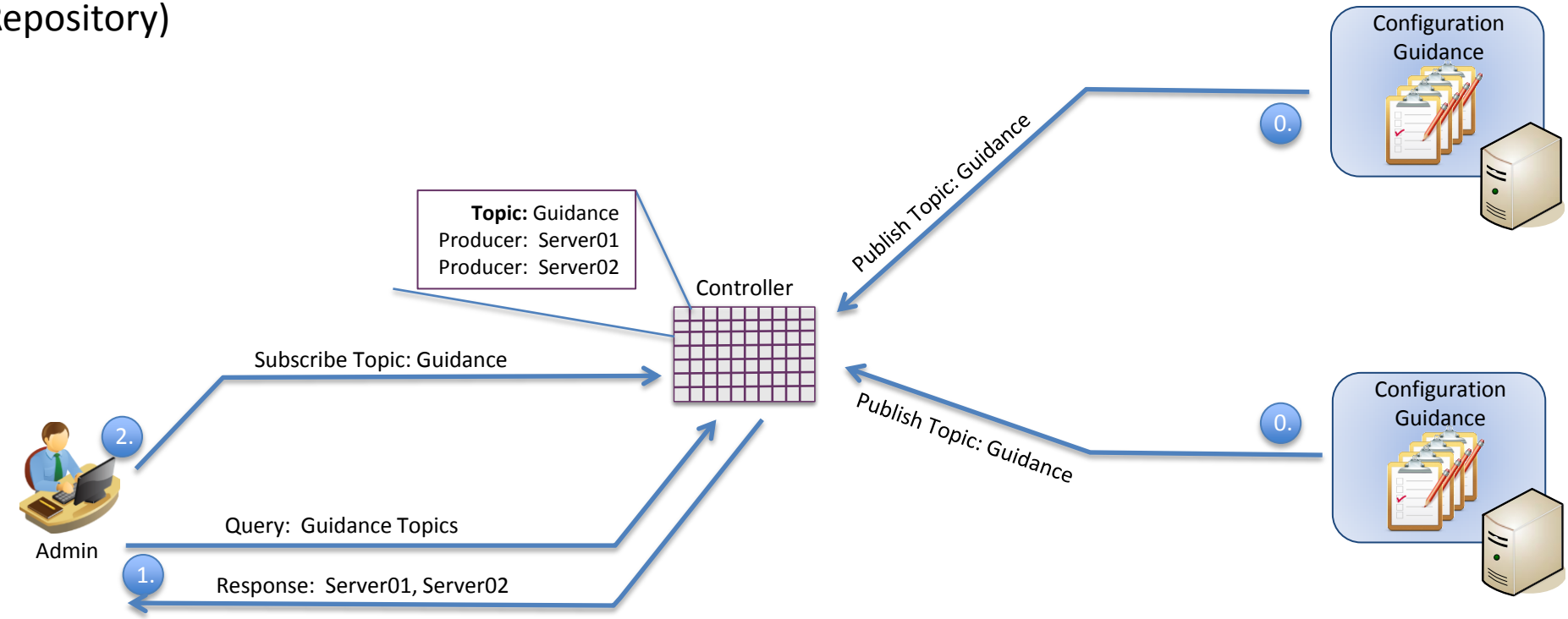


0. Data stores publish lists of the guidance they contain
1. Admin queries the Controller to find out which data stores contain what content
2. Controller replies with list of data stores
3. Admin defines search criteria
4. Admin queries data stores for that content
5. Content is returned to the operator

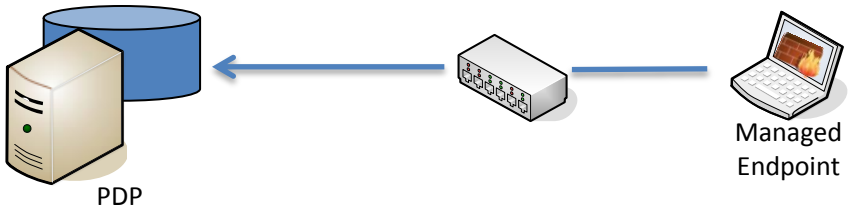
2.2.7 – GUIDANCE CHANGE DETECTION

2.2.7 – Guidance Change Detection

(Repository)

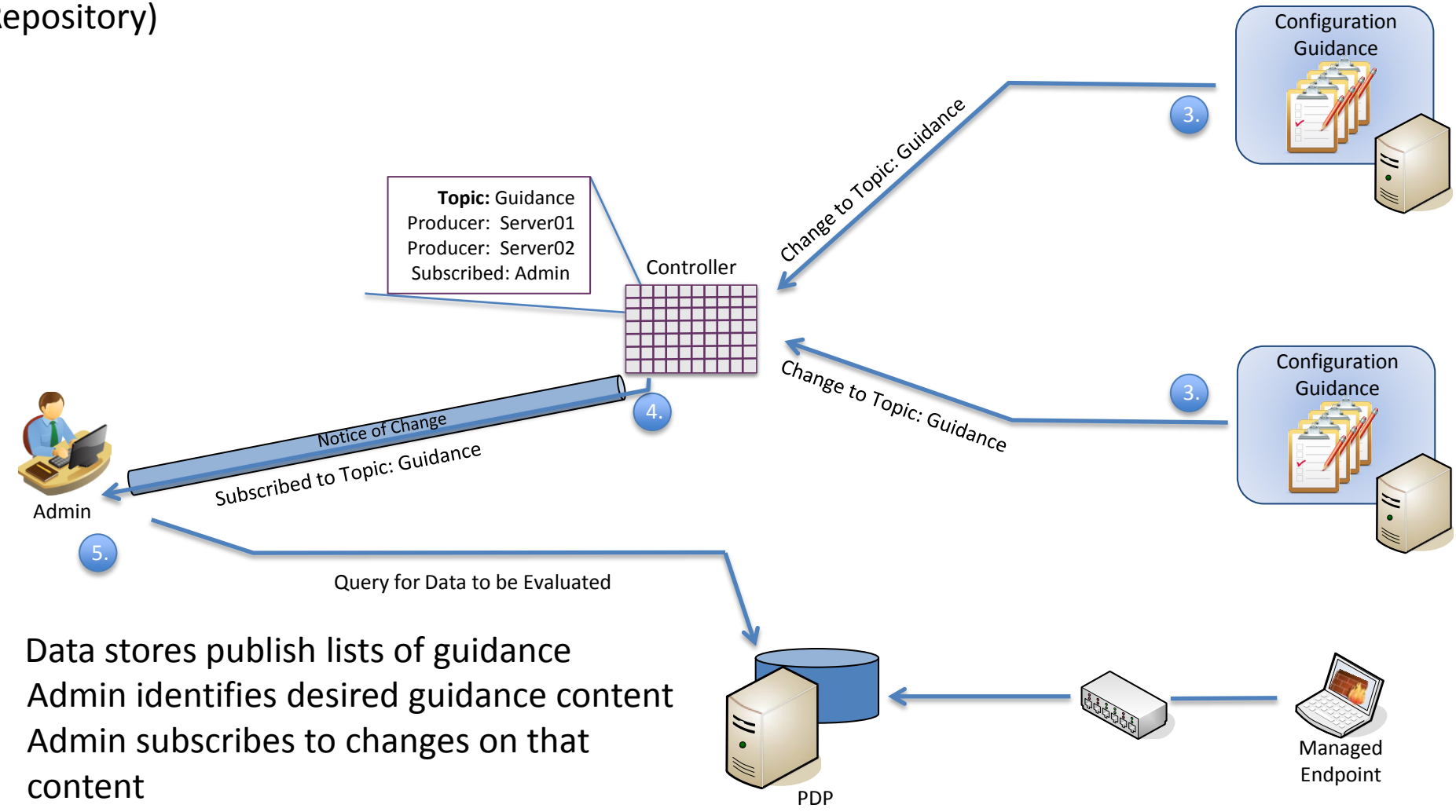


0. Data stores publish lists of guidance
1. Admin identifies desired guidance content
2. Admin subscribes to changes on that content



2.2.7 – Guidance Change Detection

(Repository)



0. Data stores publish lists of guidance
1. Admin identifies desired guidance content
2. Admin subscribes to changes on that content
3. Changes occur to that content
4. Admin is notified or sent a query response
5. New guidance data triggers new data collection / evaluation activities

Are we attempting too much?

Our Ask

ADDITIONAL PARTICIPANTS NEEDED

Asks

- Opine on scope – should we find one slice of one use case (or one slice that fits several use cases) and solve that problem first, then iterate? Or focus on fully understanding architecture and requirements first?
- Review and comment on drafts
- Volunteer to author or contribute text to drafts
- Travel is NOT necessary!

Where to go

https://datatracker.ietf.org/wg/sacm/charter/

https://github.com/sacmwg

https://www.ietf.org/mailman/listinfo/sacm

Thank you for your time…

QUESTIONS?