TapCon: Practical Third-Party Attestation for the Cloud

Yan Zhai*
University of Wisconsin Madison

Qiang Cao
Duke University

Jeffrey Chase
Duke University

Michael Swift
University of Wisconsin Madison

Why Should We Trust a Remote Service?

Why Should We Trust a Remote Service?

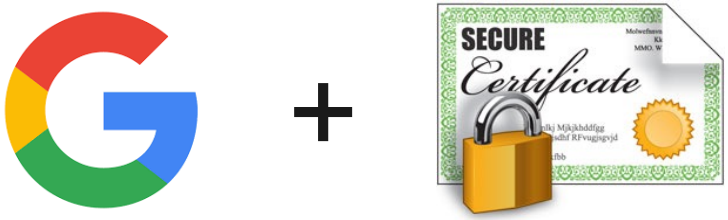


Why Should We Trust a Remote Service?

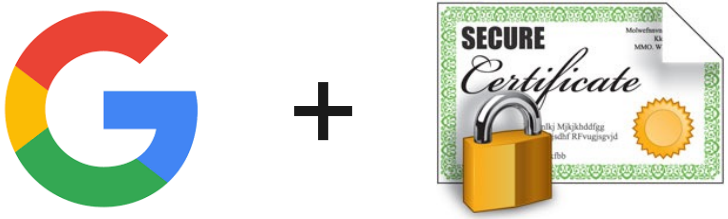


+

Why Should We Trust a Remote Service?



Why Should We Trust a Remote Service?



social trust?

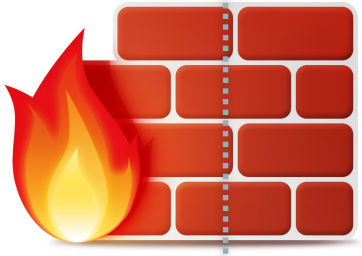
Why Should We Trust a Remote Service?



+



social trust?



#	Policy	Protocol	Destination	Port	Comment	Actions
1	Deny	TCP	Any	25	Block SMTP	
2	Deny	TCP	Any	6881	Block BitTorrent	
3	Allow	TCP	192.168.1.37/32	Any	Access to student printer	
	Deny	Any	Local LAN	Any	Wireless clients accessing LAN	
	Allow	Any	Any	Any	Default rule	

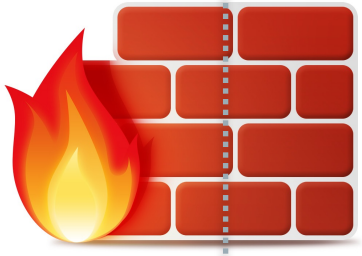
Why Should We Trust a Remote Service?



+



social trust?





#	Policy	Protocol	Destination	Port	Comment	Actions
1	Deny	TCP	Any	25	Block SMTP	
2	Deny	TCP	Any	6881	Block BitTorrent	
3	Allow	TCP	192.168.1.37/32	Any	Access to student printer	
	Deny	Any	Local LAN	Any	Wireless clients accessing LAN	
	Allow	Any	Any	Any	Default rule	

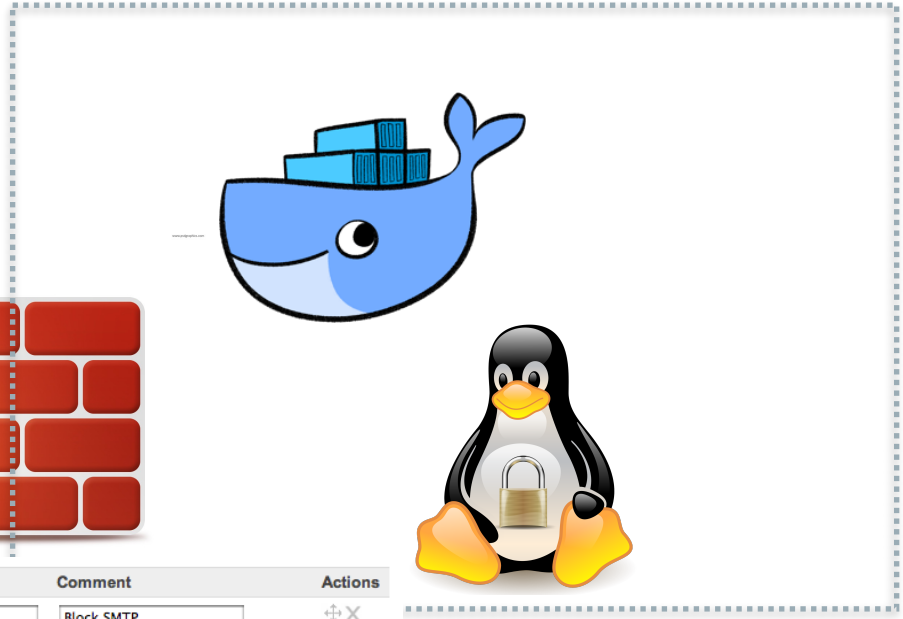
Why Should We Trust a Remote Service?



+



social trust?



#	Policy	Protocol	Destination	Port	Comment	Actions
1	Deny	TCP	Any	25	Block SMTP	
2	Deny	TCP	Any	6881	Block BitTorrent	
3	Allow	TCP	192.168.1.37/32	Any	Access to student printer	
	Deny	Any	Local LAN	Any	Wireless clients accessing LAN	
	Allow	Any	Any	Any	Default rule	

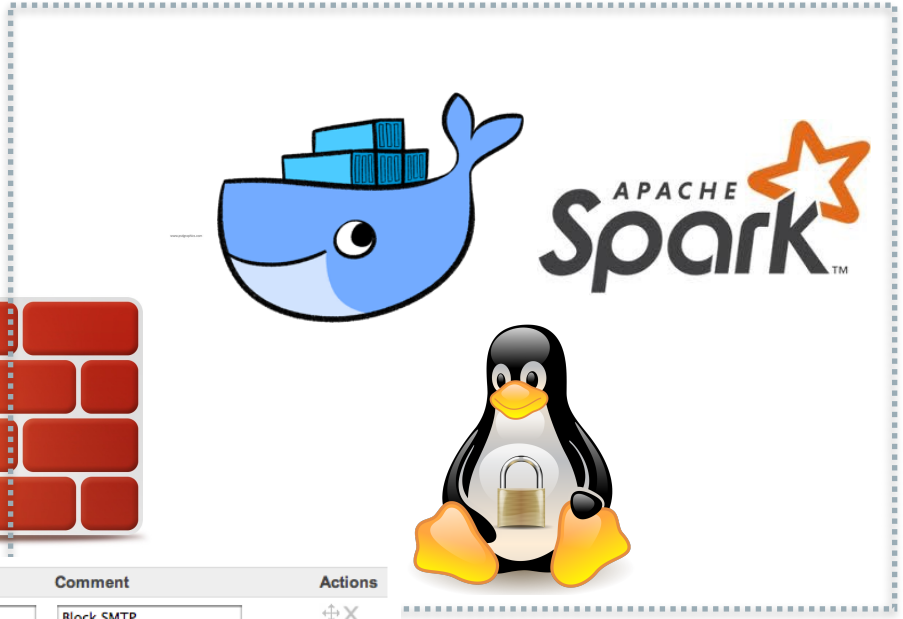
Why Should We Trust a Remote Service?



+

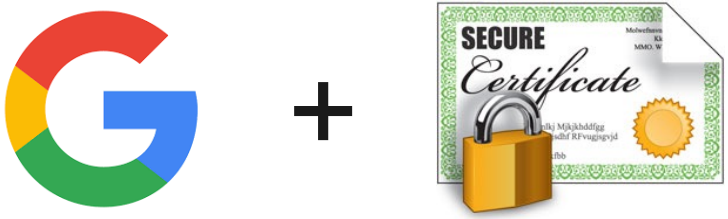


social trust?



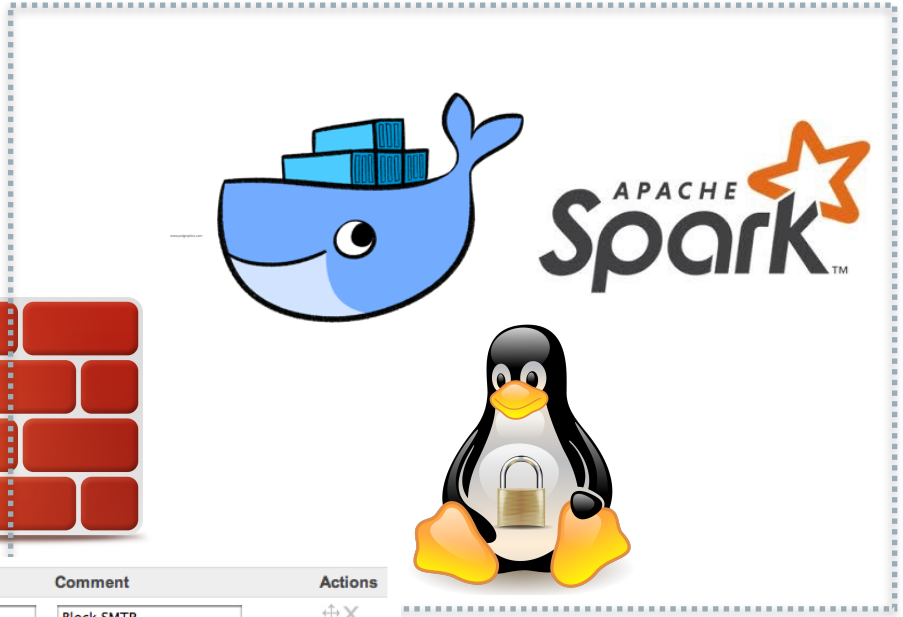
#	Policy	Protocol	Destination	Port	Comment	Actions
1	Deny	TCP	Any	25	Block SMTP	
2	Deny	TCP	Any	6881	Block BitTorrent	
3	Allow	TCP	192.168.1.37/32	Any	Access to student printer	
	Deny	Any	Local LAN	Any	Wireless clients accessing LAN	
	Allow	Any	Any	Any	Default rule	

Why Should We Trust a Remote Service?



social trust?

Check Code identity and Configuration?



#	Policy	Protocol	Destination	Port	Comment	Actions
1	Deny	TCP	Any	25	Block SMTP	
2	Deny	TCP	Any	6881	Block BitTorrent	
3	Allow	TCP	192.168.1.37/32	Any	Access to student printer	
	Deny	Any	Local LAN	Any	Wireless clients accessing LAN	
	Allow	Any	Any	Any	Default rule	

Cloud Enables It…

Cloud Enables It…

- **Trusted:** cloud provider has very good reputation

Cloud Enables It…

- **Trusted:** cloud provider has very good reputation
- **Unspoofable**: tightly controlled network

Cloud Enables It…

- **Trusted:** cloud provider has very good reputation
- **Unspoofable**: tightly controlled network
- **Knowledgeable**: aware of VM identity and configuration

Cloud Enables It…

- **Trusted:** cloud provider has very good reputation
- **Unspoofable**: tightly controlled network
- **Knowledgeable**: aware of VM identity and configuration
- **Motivated**: helpful to tenants in security

Cloud Enables It…

- **Trusted:** cloud provider has very good reputation
- **Unspoofable**: tightly controlled network
- **Knowledgeable**: aware of VM identity and configuration
- **Motivated**: helpful to tenants in security



Alice



192.168.0.1

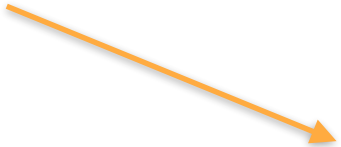
amazon web services

Cloud Enables It…

- **Trusted:** cloud provider has very good reputation
- **Unspoofable**: tightly controlled network
- **Knowledgeable**: aware of VM identity and configuration
- **Motivated**: helpful to tenants in security



Alice



(1) what's running on 192.168.0.1?



192.168.0.1

amazon web services

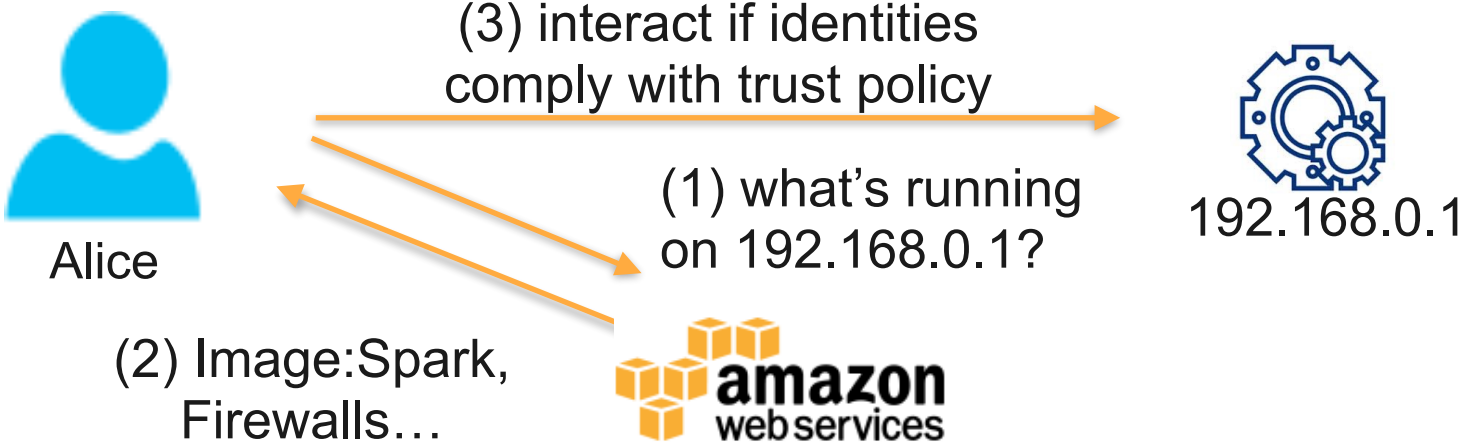
Cloud Enables It…

- **Trusted:** cloud provider has very good reputation
- **Unspoofable**: tightly controlled network
- **Knowledgeable**: aware of VM identity and configuration
- **Motivated**: helpful to tenants in security



Cloud Enables It…

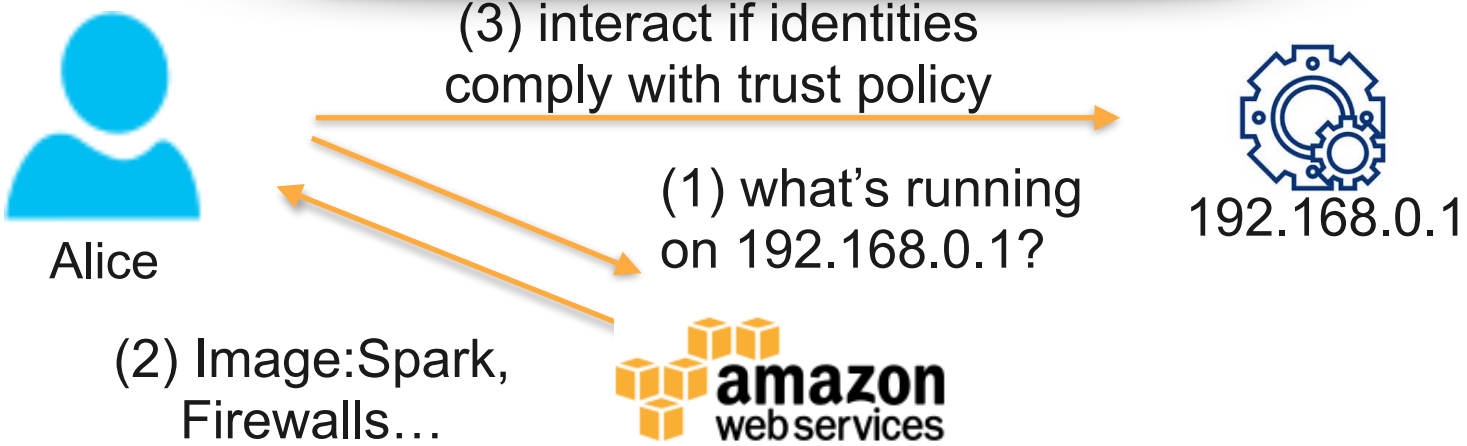
- **Trusted:** cloud provider has very good reputation
- **Unspoofable**: tightly controlled network
- **Knowledgeable**: aware of VM identity and configuration
- **Motivated**: helpful to tenants in security



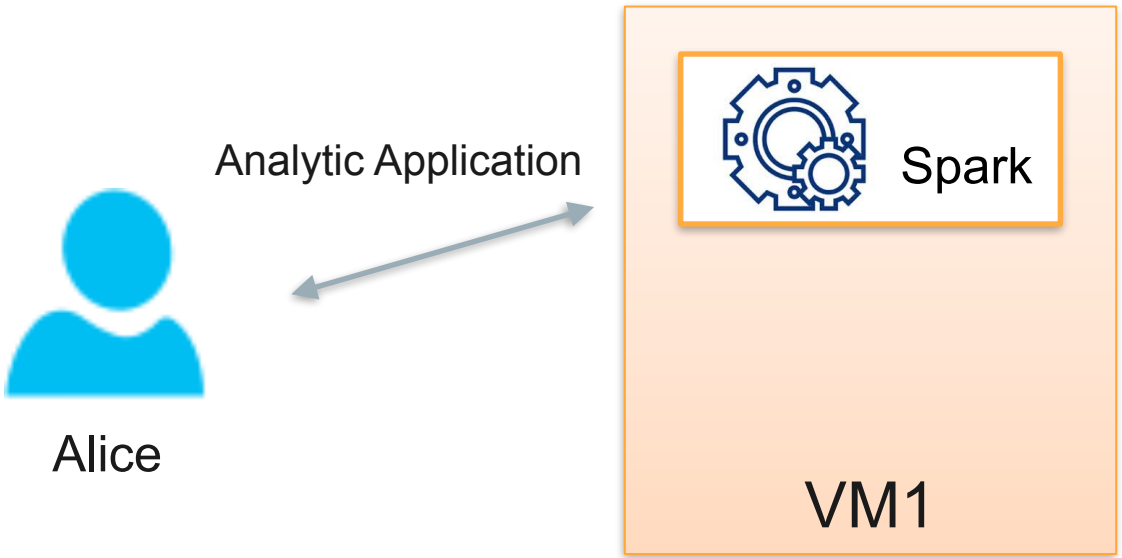
Cloud Enables It…

- **Trusted:** cloud provider has very good reputation
- **Unspoofable**: tightly controlled network
- **Knowledge** [illegible] **onfiguration**
- **Motivated**:

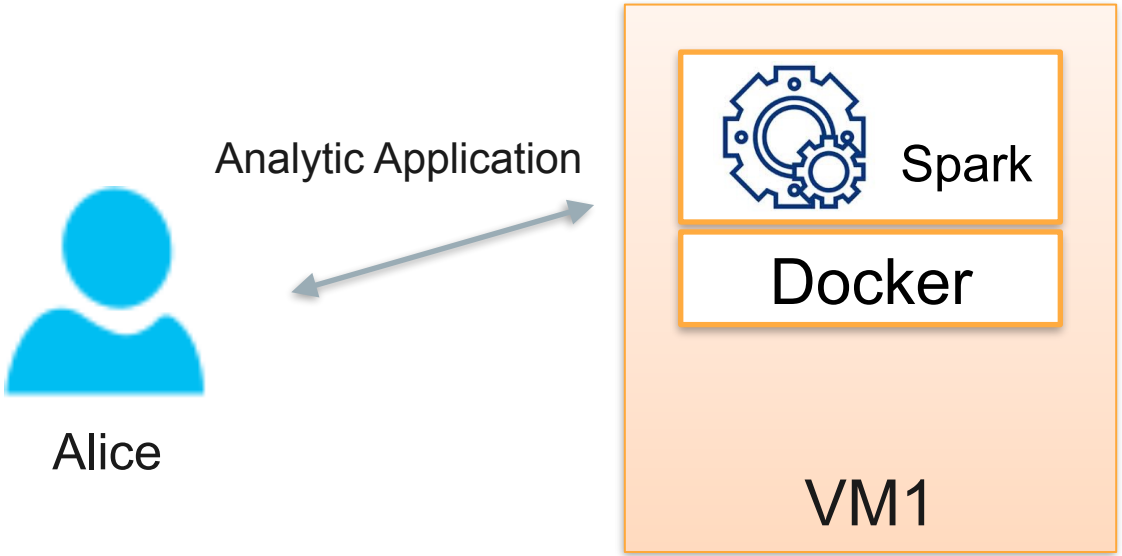
This is not enough…



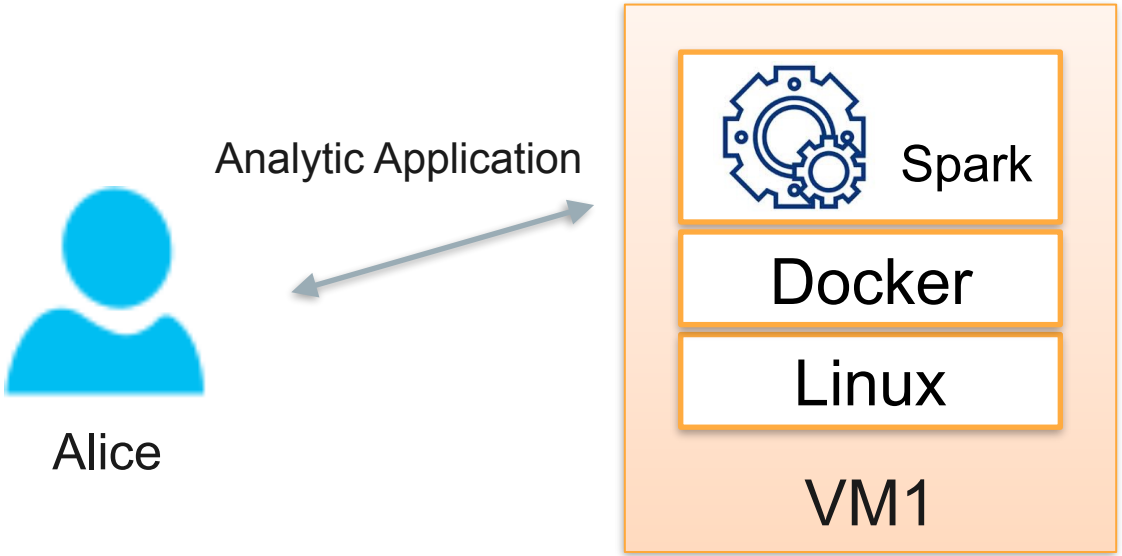
Applications are Complicated



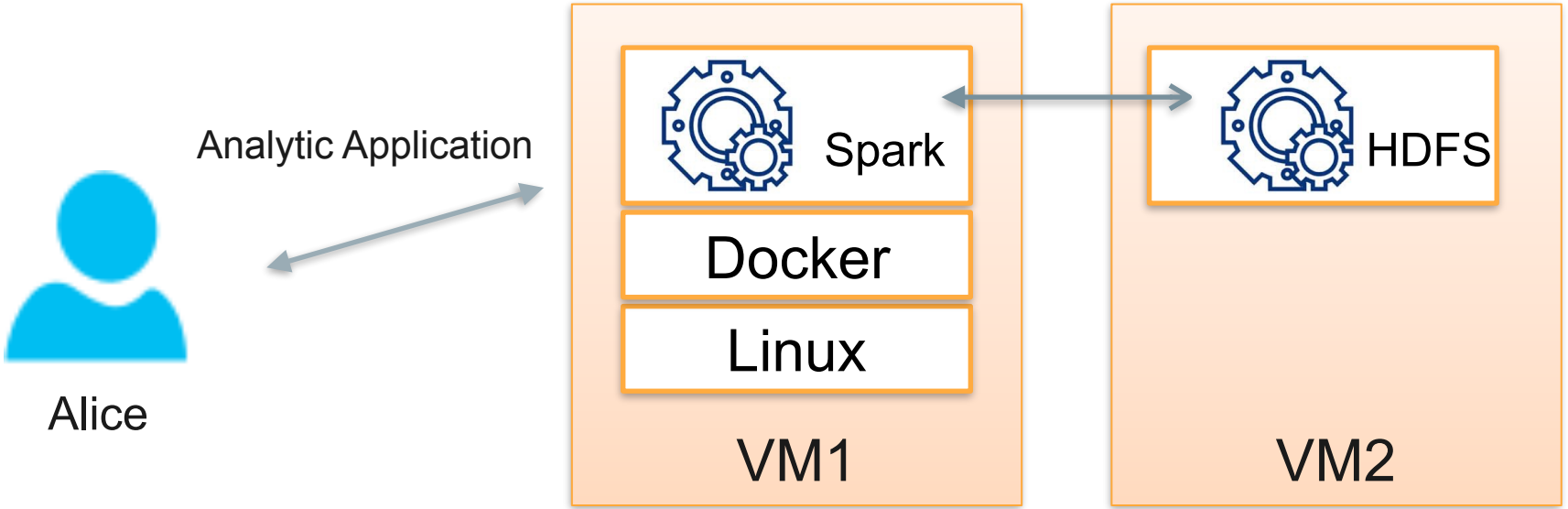
Applications are Complicated



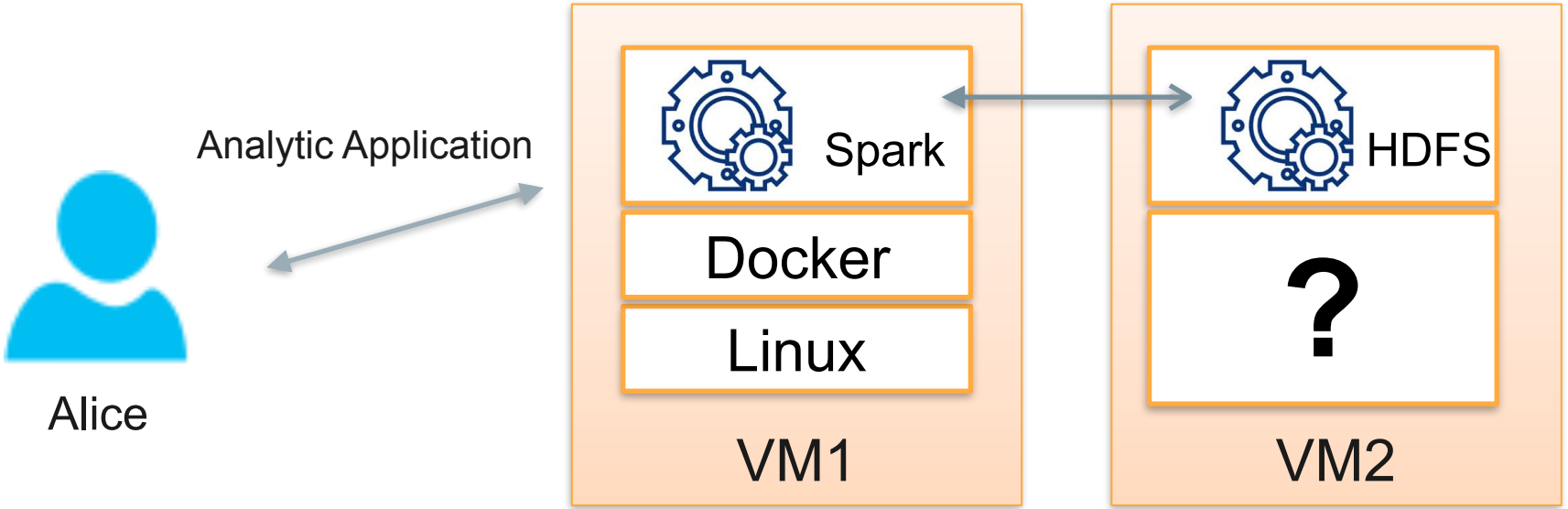
Applications are Complicated



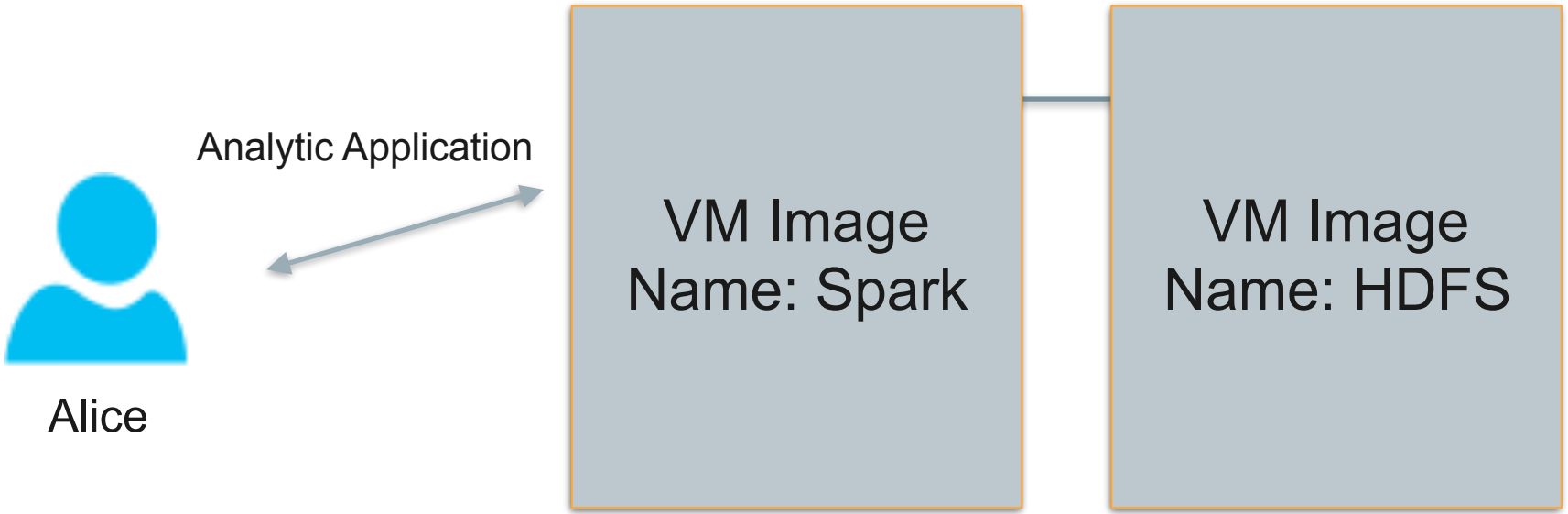
Applications are Complicated



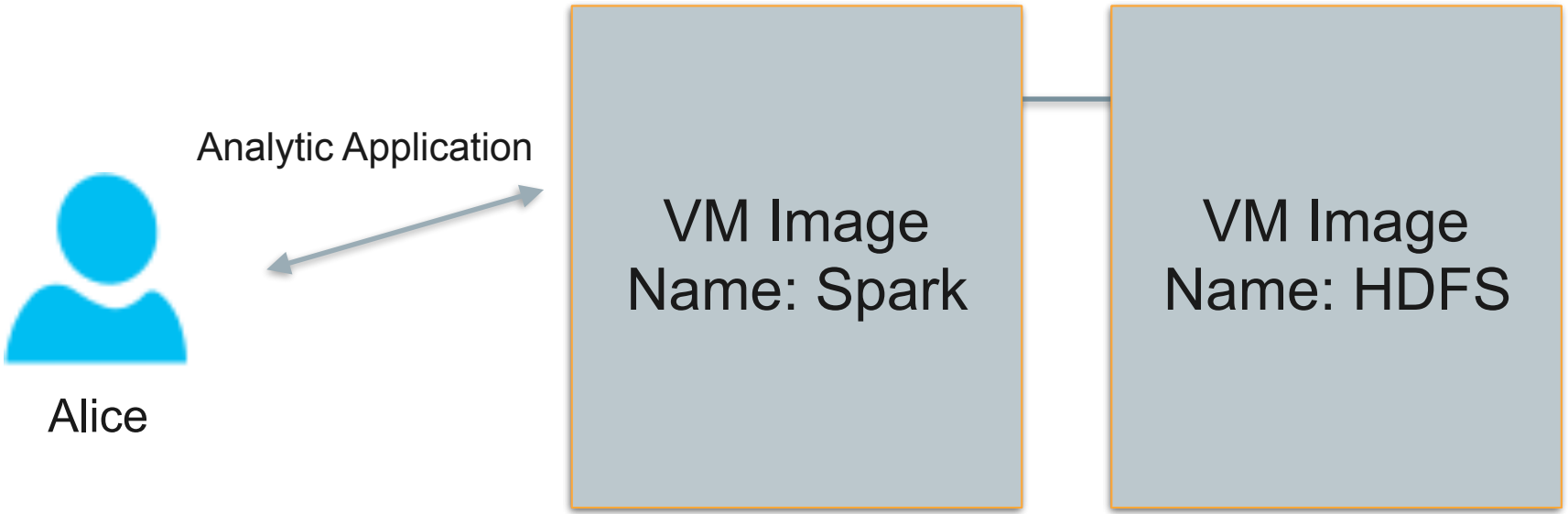
Applications are Complicated



Applications are Complicated



Applications are Complicated



Hash does not make much sense to third parties!

TapCon: Attestation Platform for Containers

TapCon: Attestation Platform for Containers

An IaaS service composed by locked down VMs and authenticated storage for information about containers and images

TapCon: Attestation Platform for Containers

An IaaS service composed by locked down VMs and authenticated storage for information about containers and images

- Attest containers to its source manifest

TapCon: Attestation Platform for Containers

An IaaS service composed by locked down VMs and authenticated storage for information about containers and images

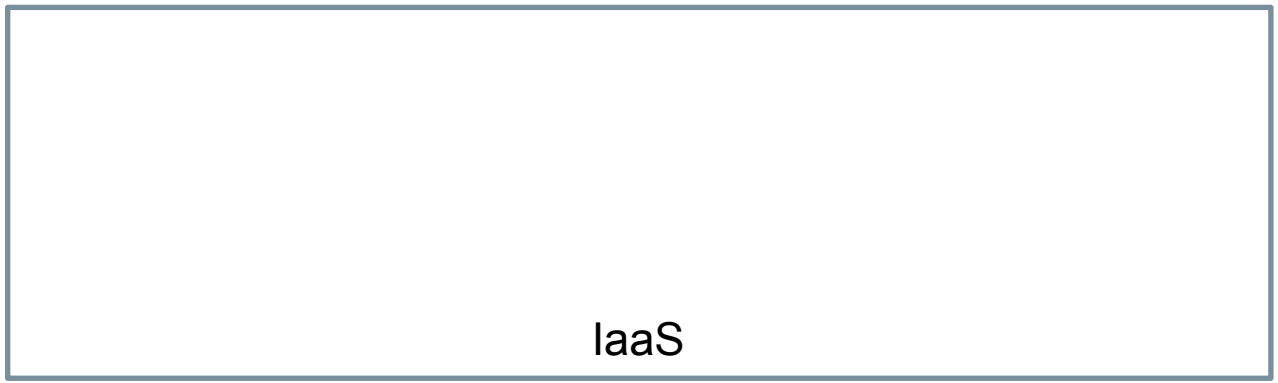
- Attest containers to its source manifest
- Compatible with existing applications

TapCon: Attestation Platform for Containers

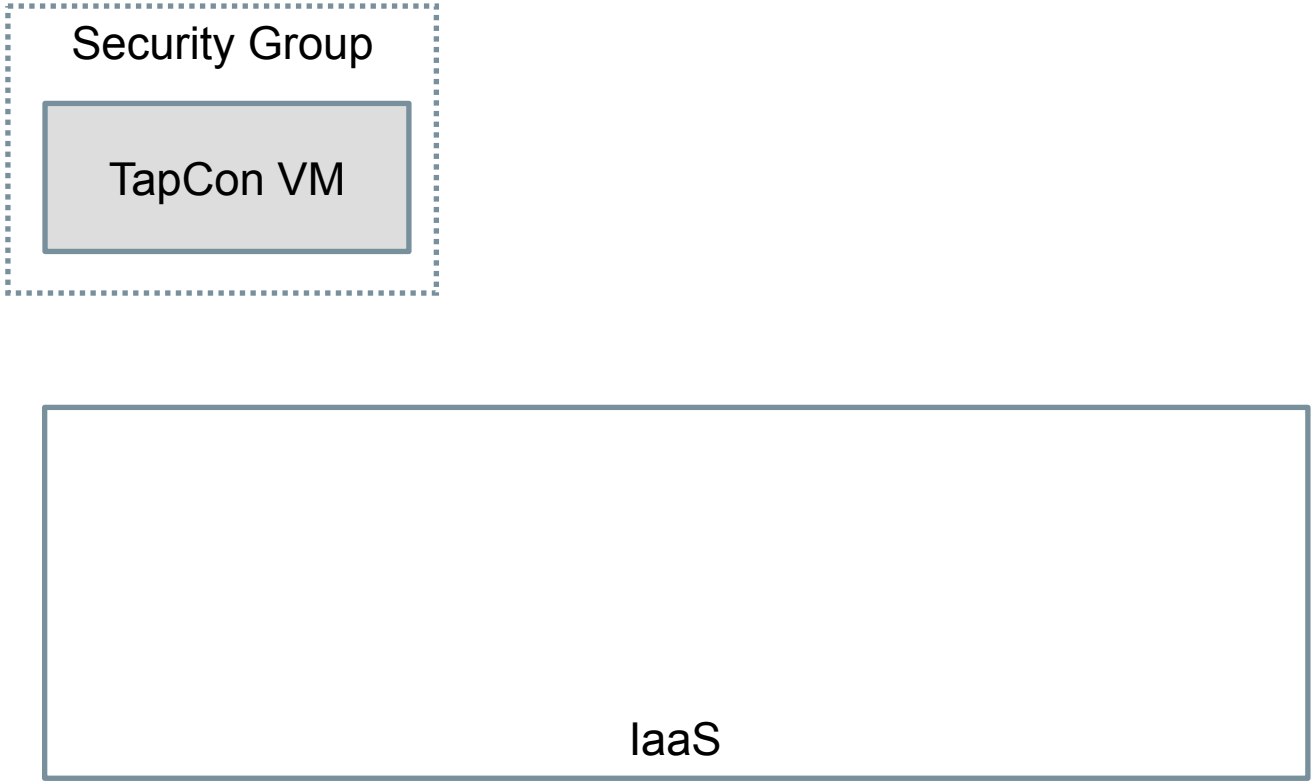
An IaaS service composed by locked down VMs and authenticated storage for information about containers and images

- Attest containers to its source manifest
- Compatible with existing applications
- Rich policy for what should be trusted

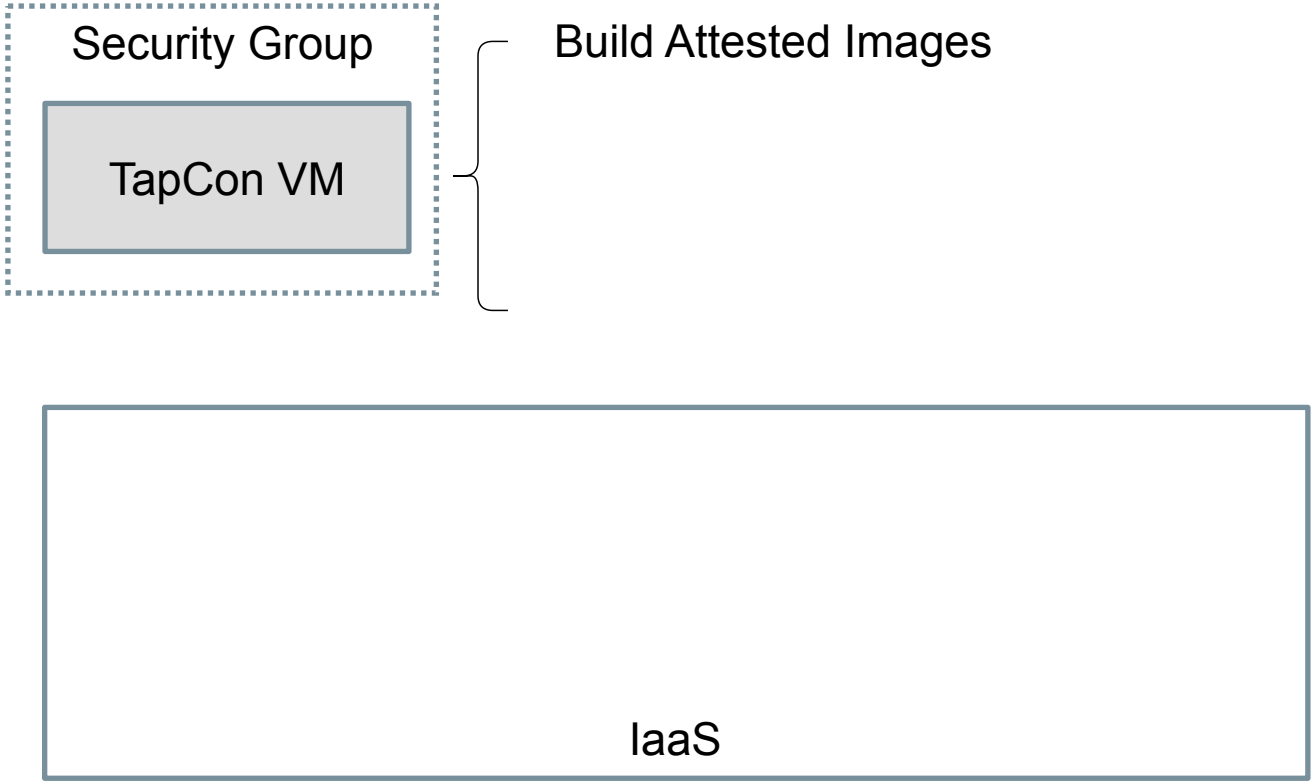
Overview of TapCon



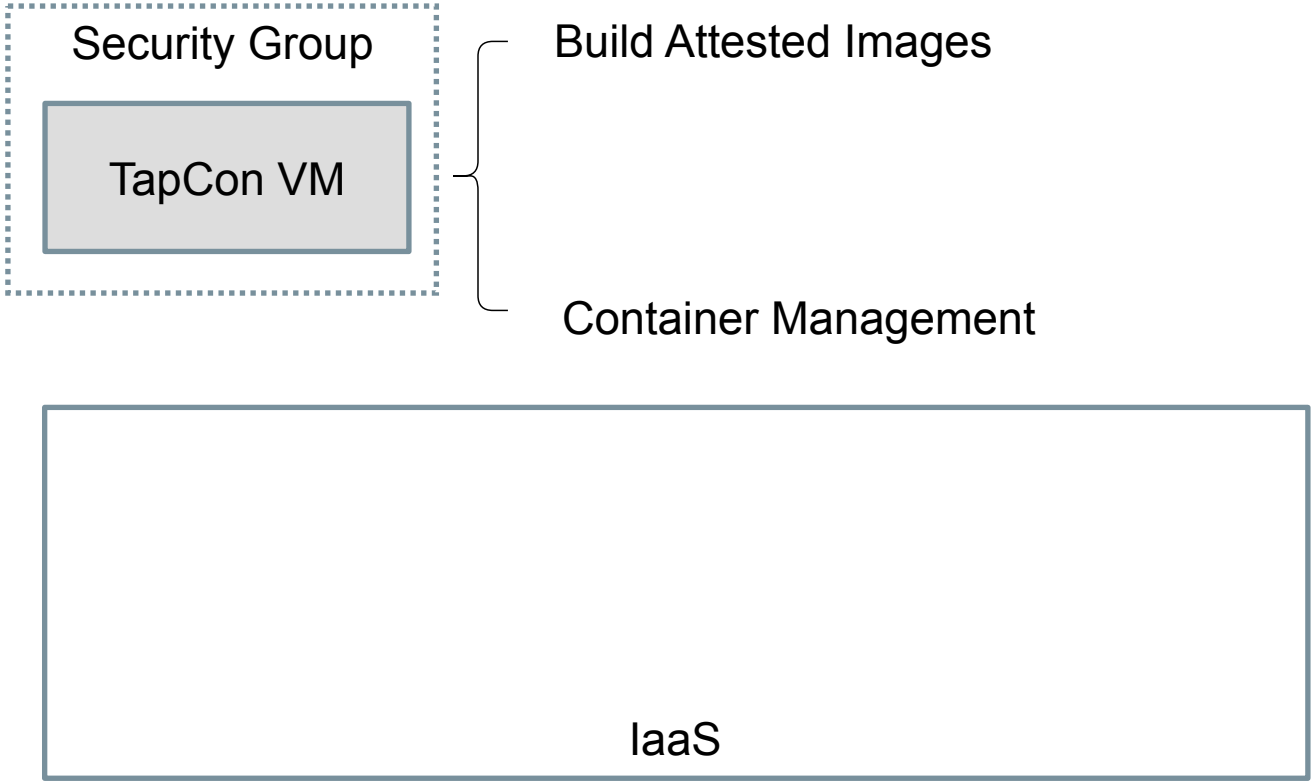
Overview of TapCon



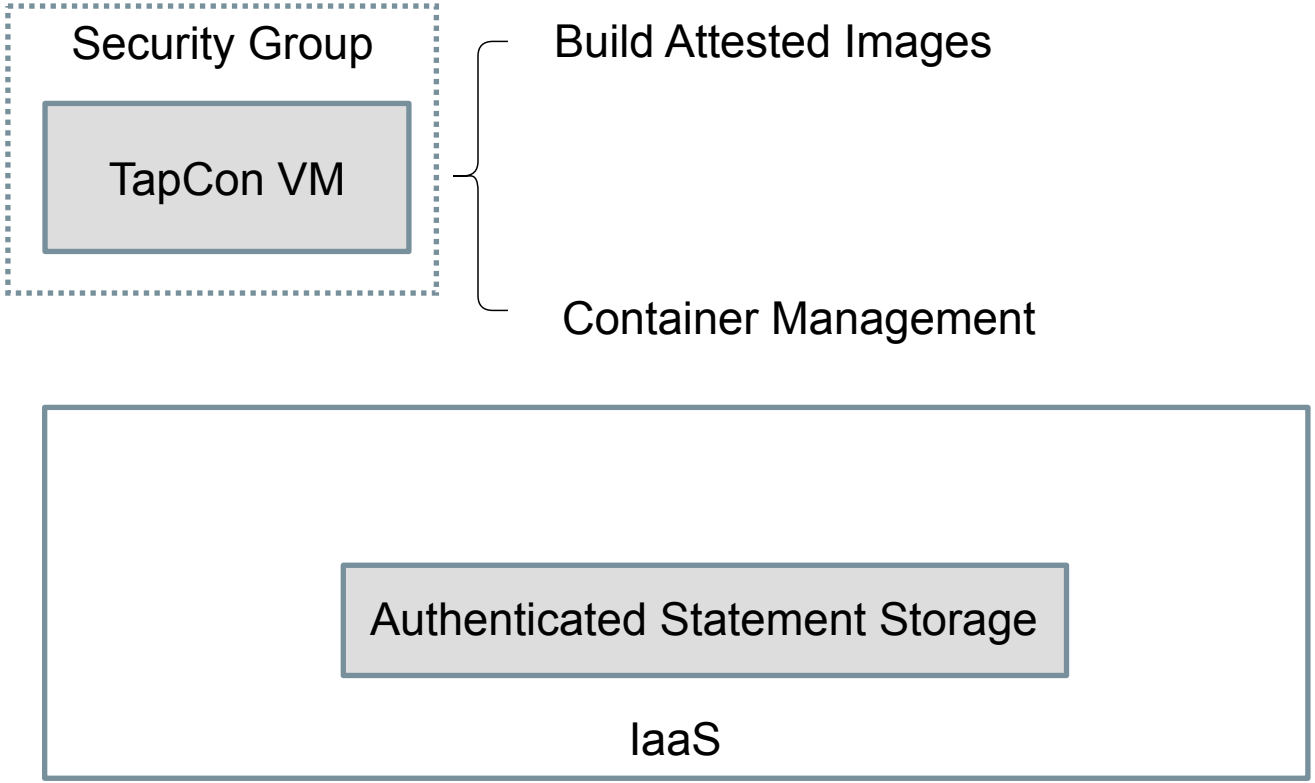
Overview of TapCon



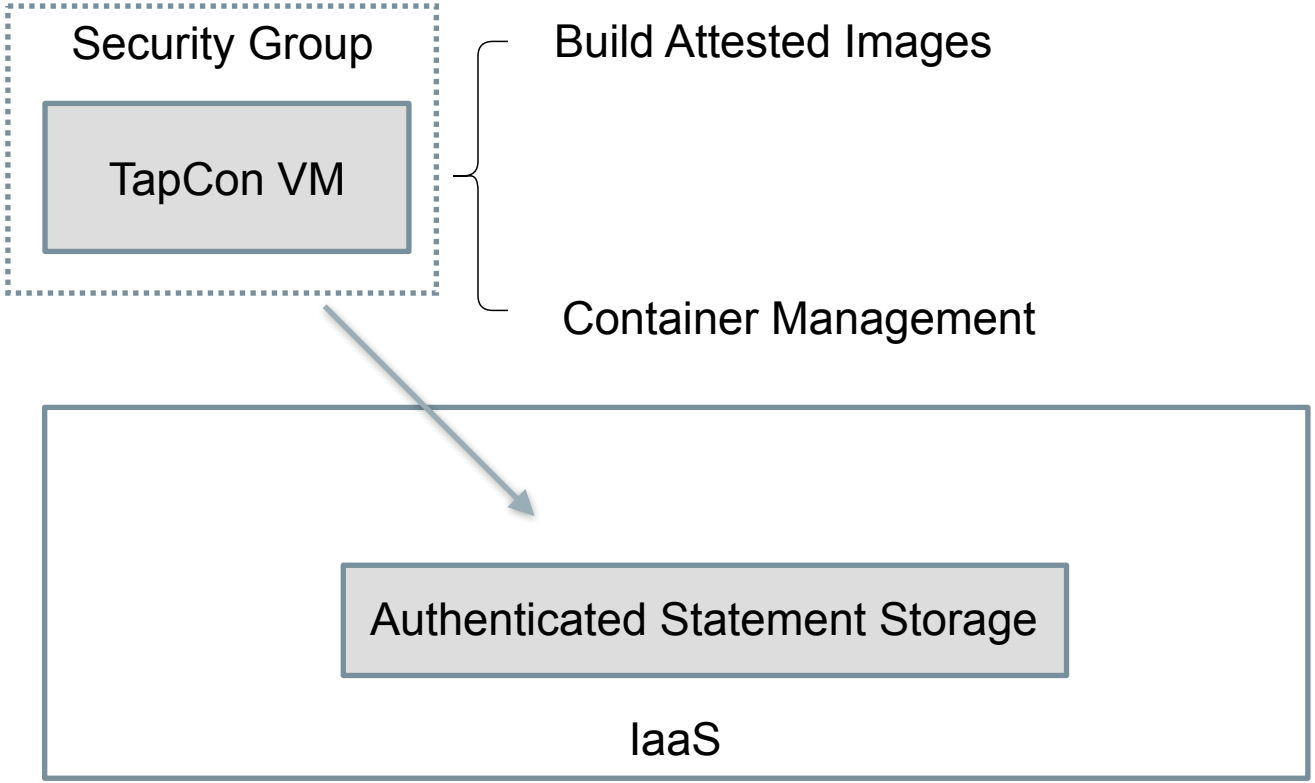
Overview of TapCon



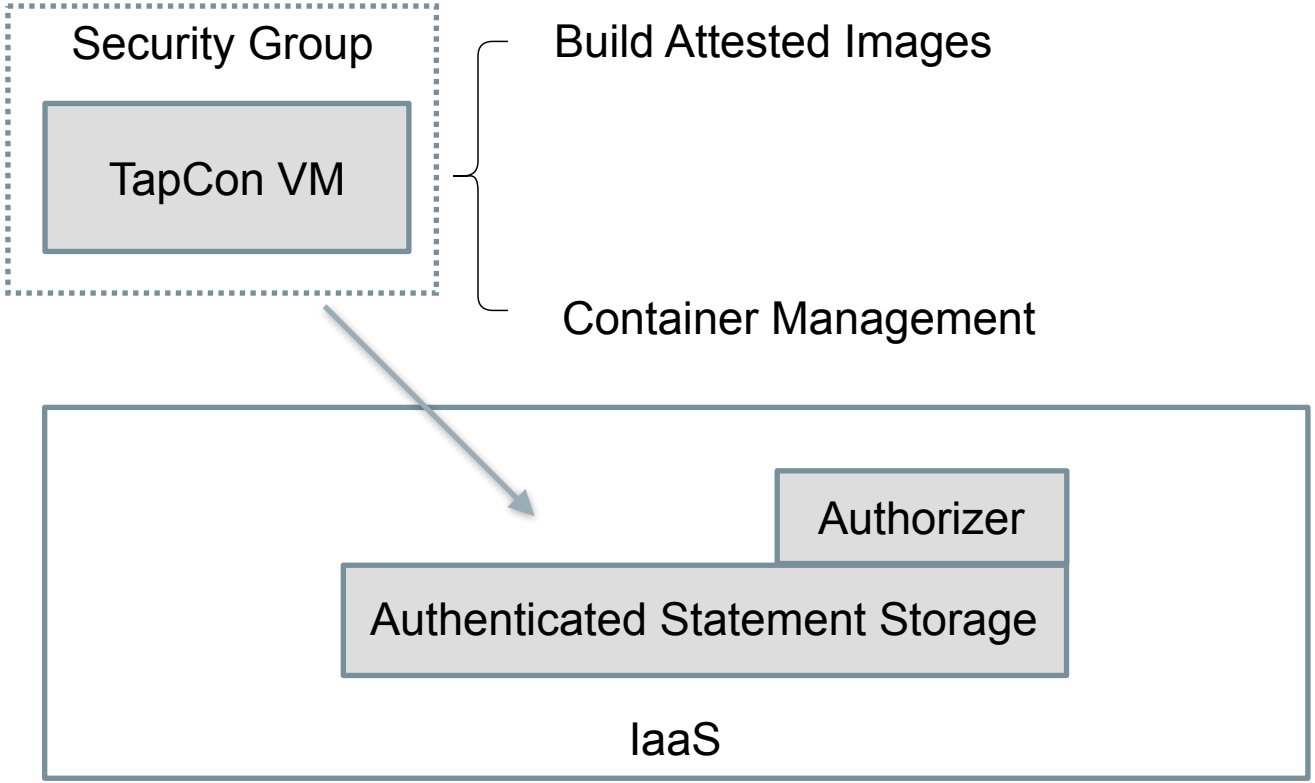
Overview of TapCon



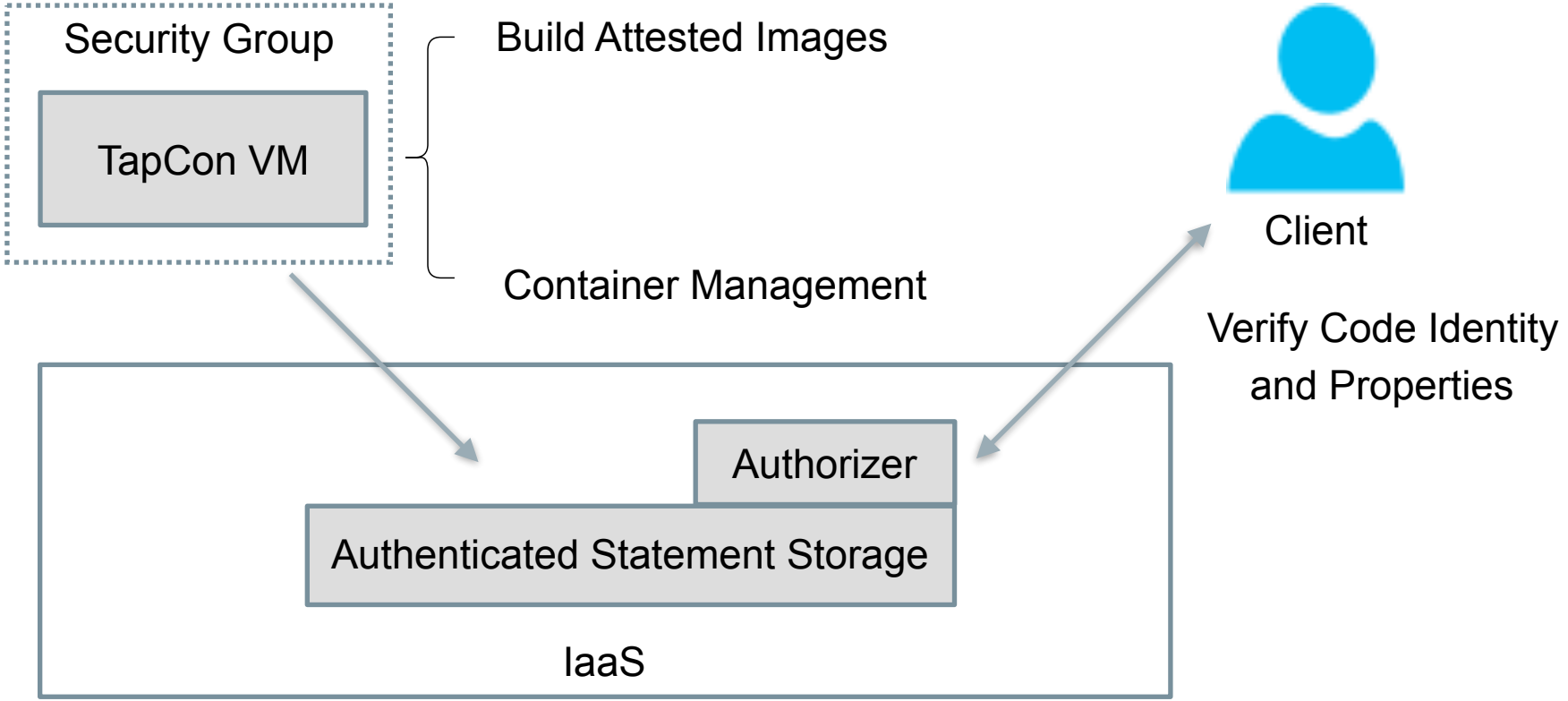
Overview of TapCon



Overview of TapCon



Overview of TapCon



Build Attested Images

Build Attested Images


TapCon Container Manager

Question: How do we connect source to images?

TapCon Container Manager

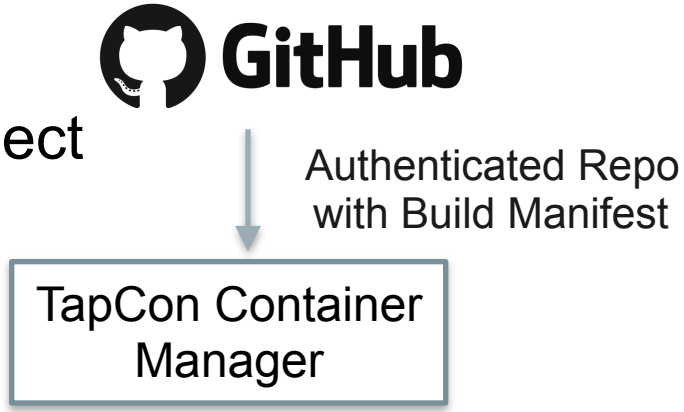
Question: How do we connect source to images?

- Identify Repository

TapCon Container Manager

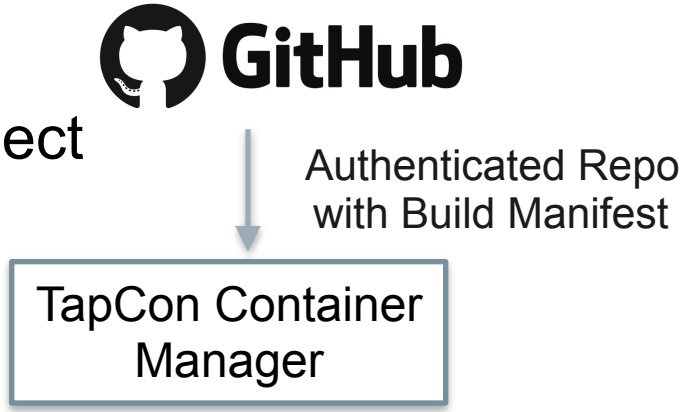
Question: How do we connect source to images?

- Identify Repository



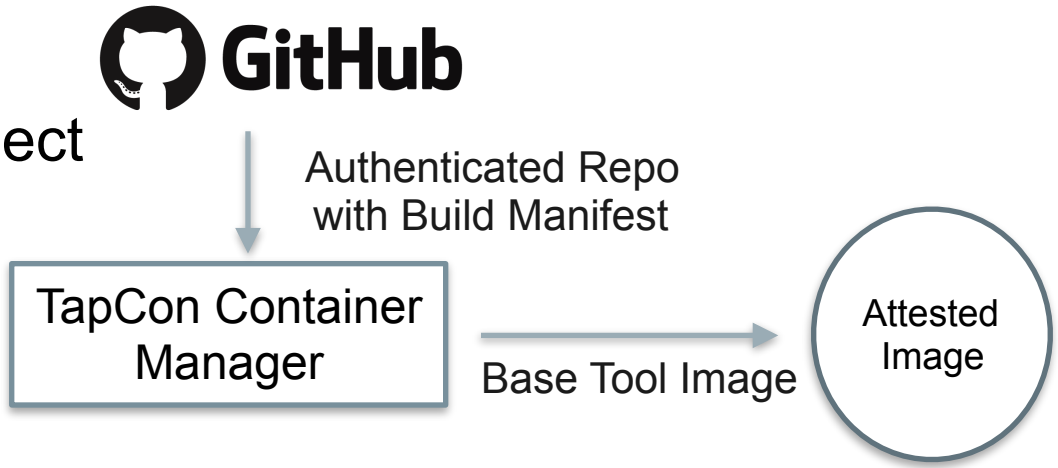
Question: How do we connect source to images?

- Identify Repository
- Identify Environment



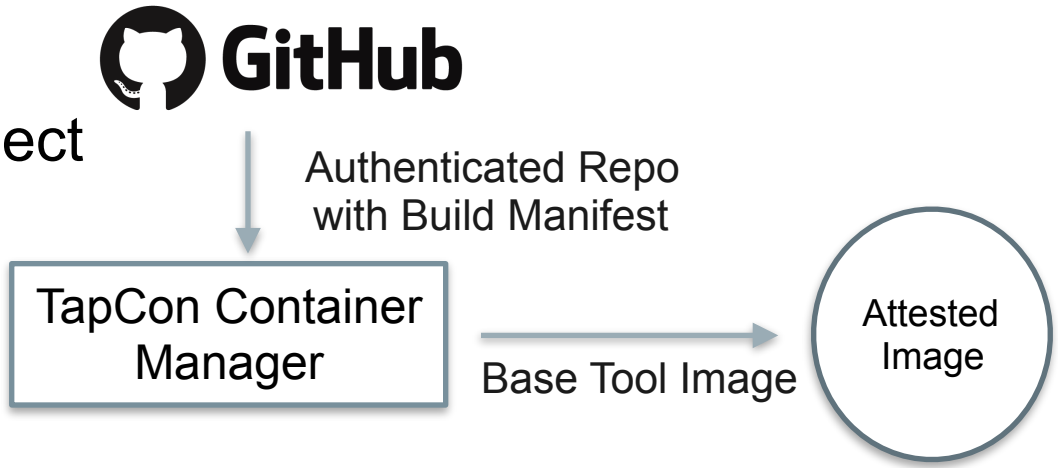
Question: How do we connect source to images?

- Identify Repository
- Identify Environment



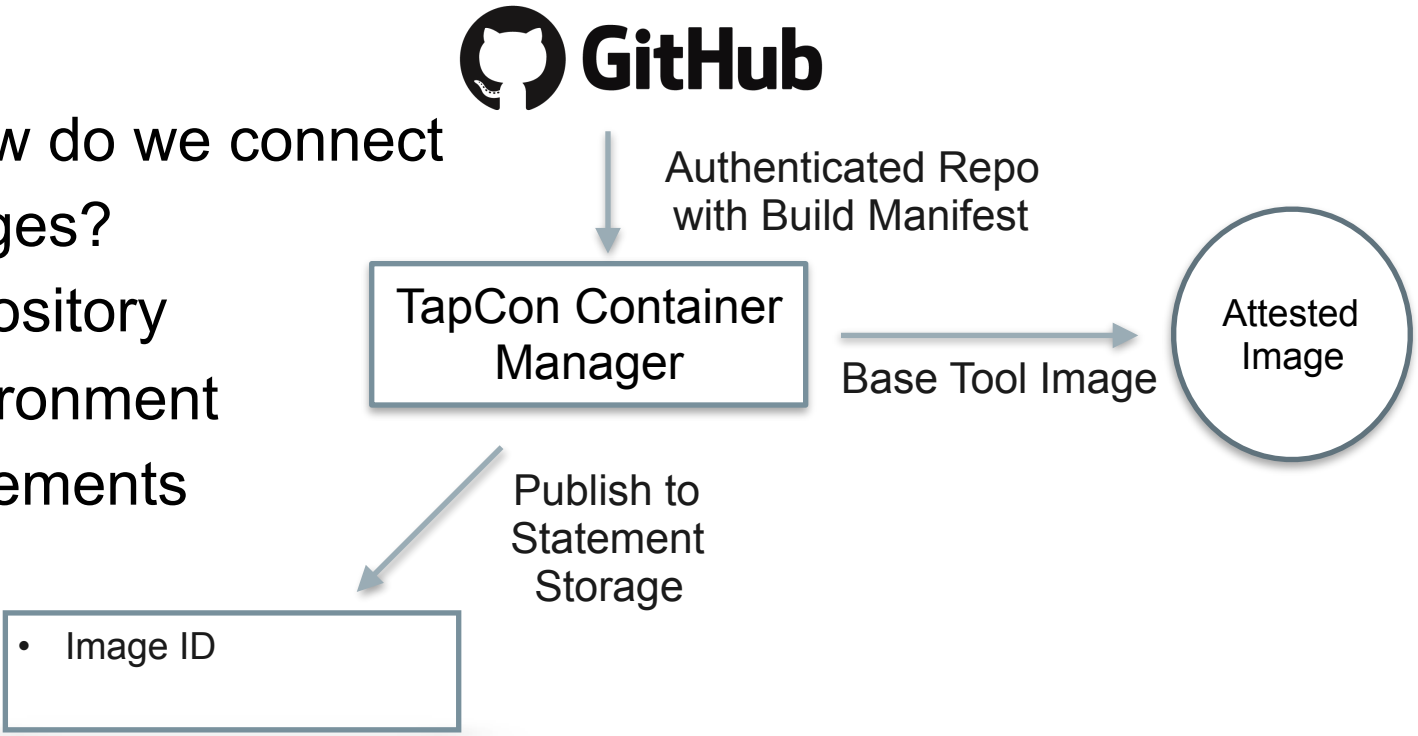
Question: How do we connect source to images?

- Identify Repository
- Identify Environment
- Publish Statements



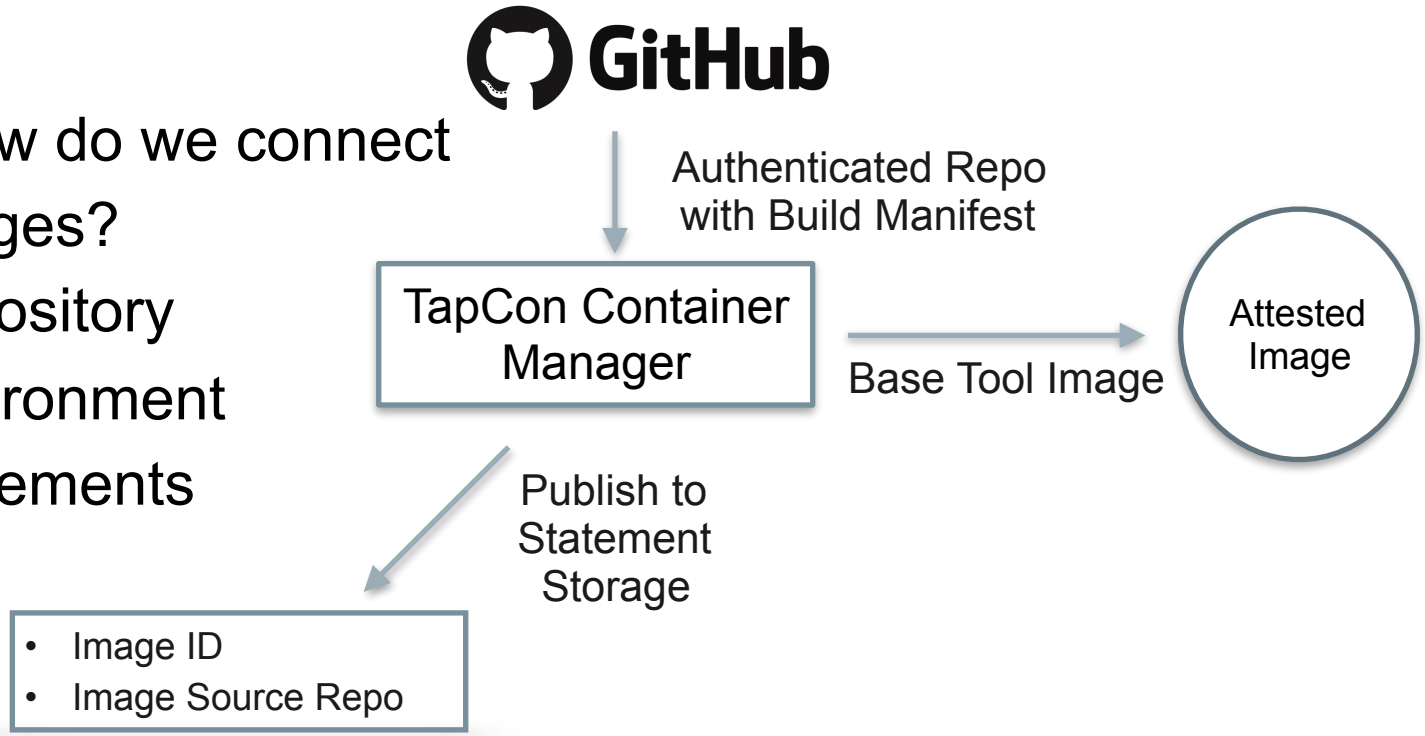
Question: How do we connect source to images?

- Identify Repository
- Identify Environment
- Publish Statements



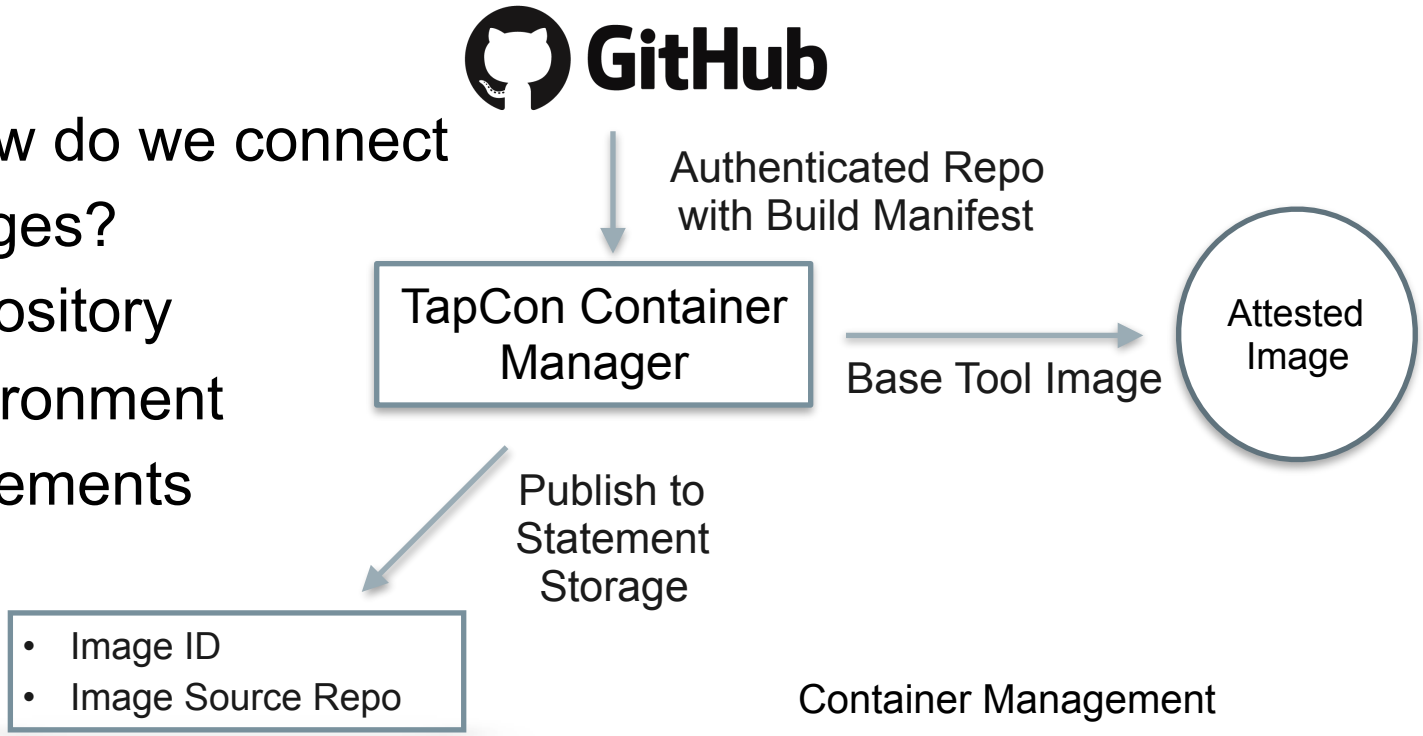
Question: How do we connect source to images?

- Identify Repository
- Identify Environment
- Publish Statements



Question: How do we connect source to images?

- Identify Repository
- Identify Environment
- Publish Statements



Container Management

Container Management


TapCon Container Manager

Question: How do we attest source of a container?

TapCon Container Manager

Question: How do we attest source of a container?

- Restrict Images

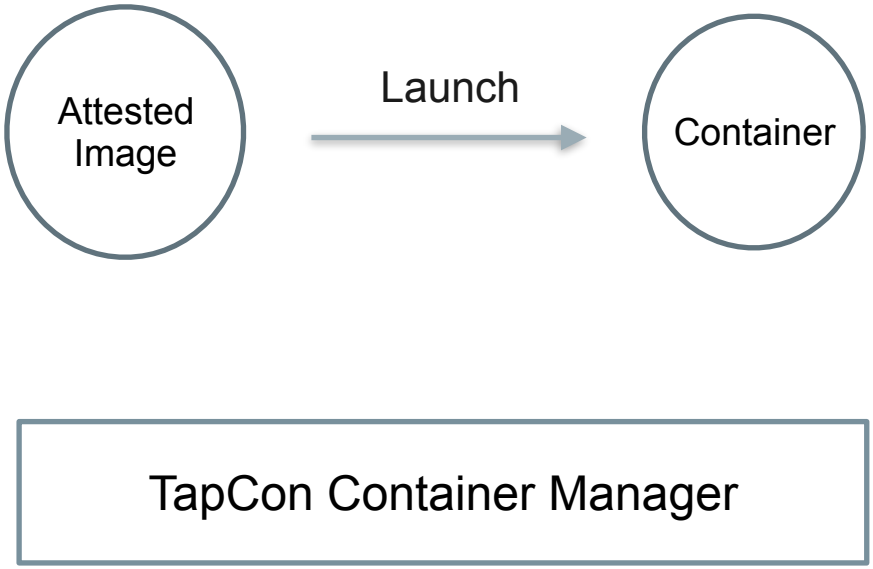


Question: How do we attest source of a container?

- Restrict Images

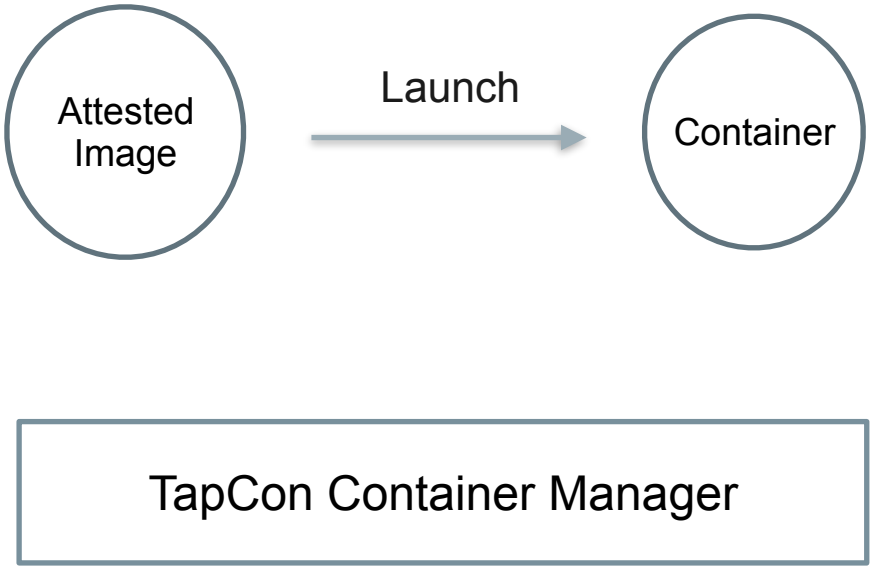


TapCon Container Manager



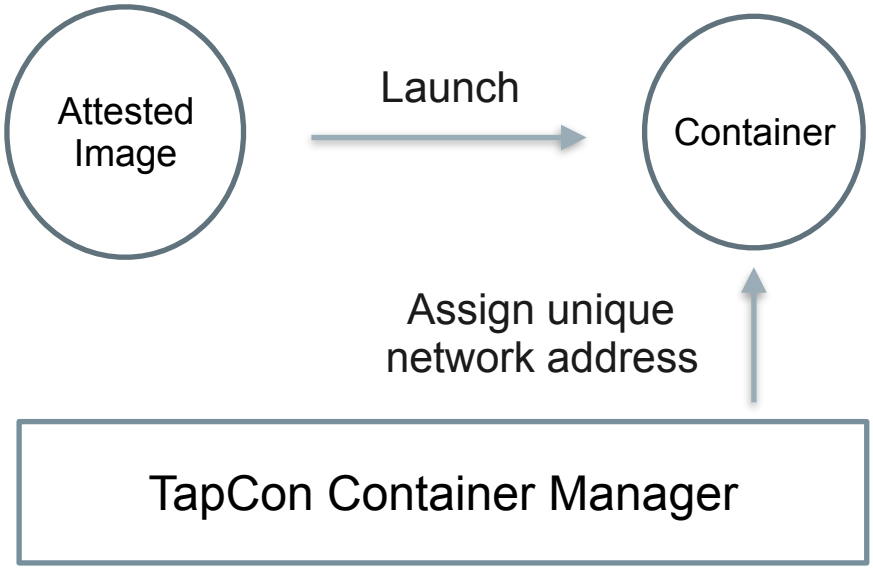
Question: How do we attest source of a container?

- Restrict Images



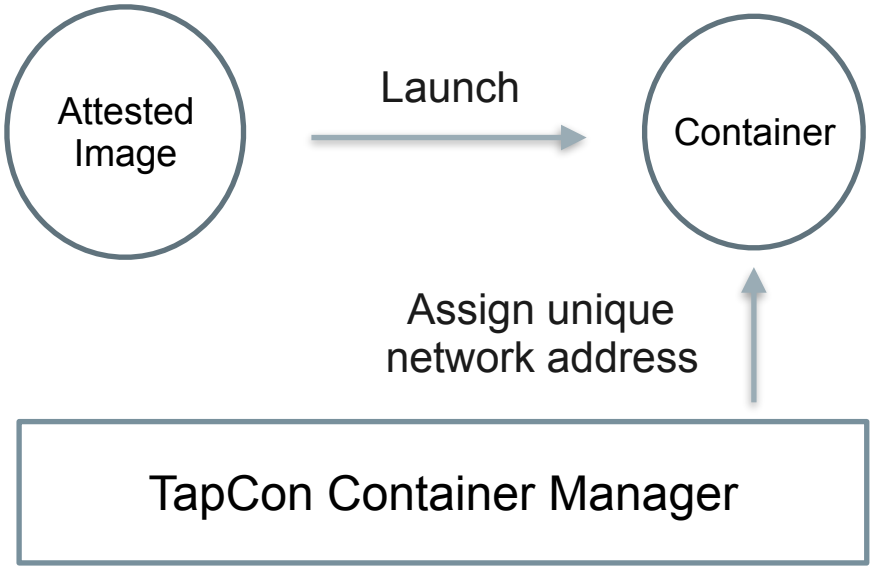
Question: How do we attest source of a container?

- Restrict Images
- Net Address as ID



Question: How do we attest source of a container?

- Restrict Images
- Net Address as ID

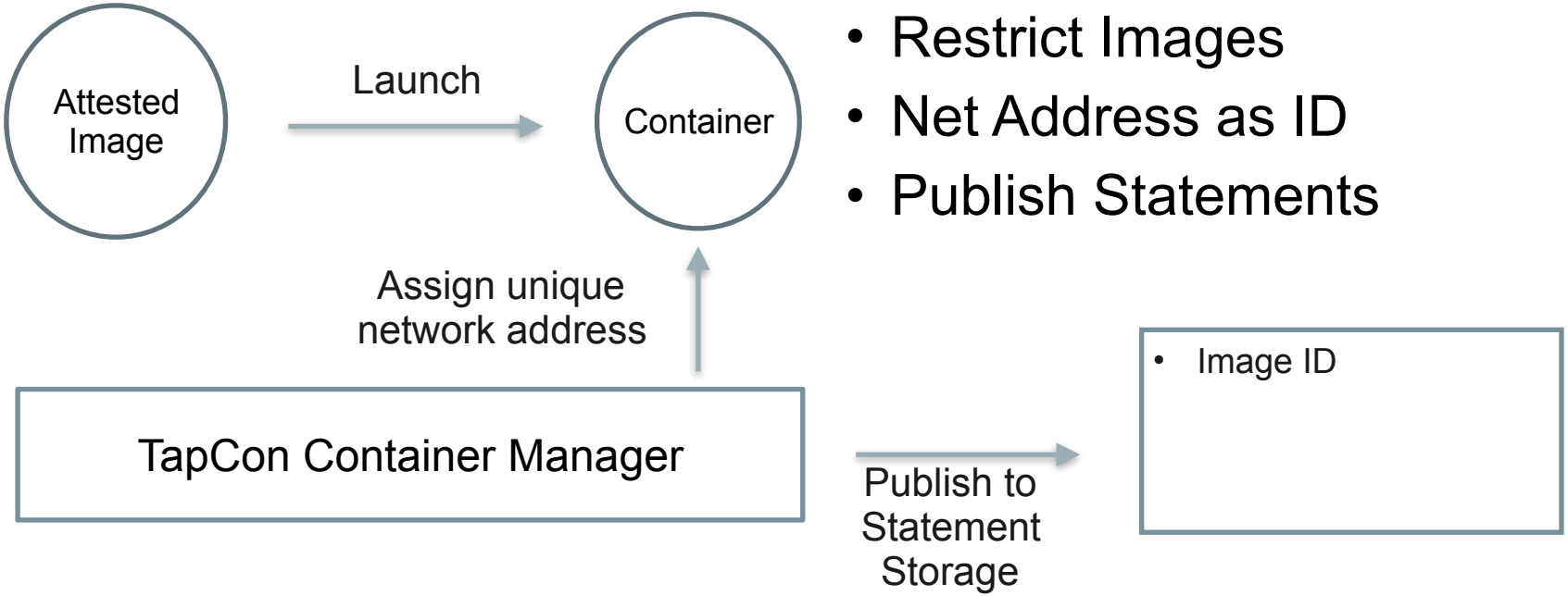


Question: How do we attest source of a container?

- Restrict Images
- Net Address as ID
- Publish Statements

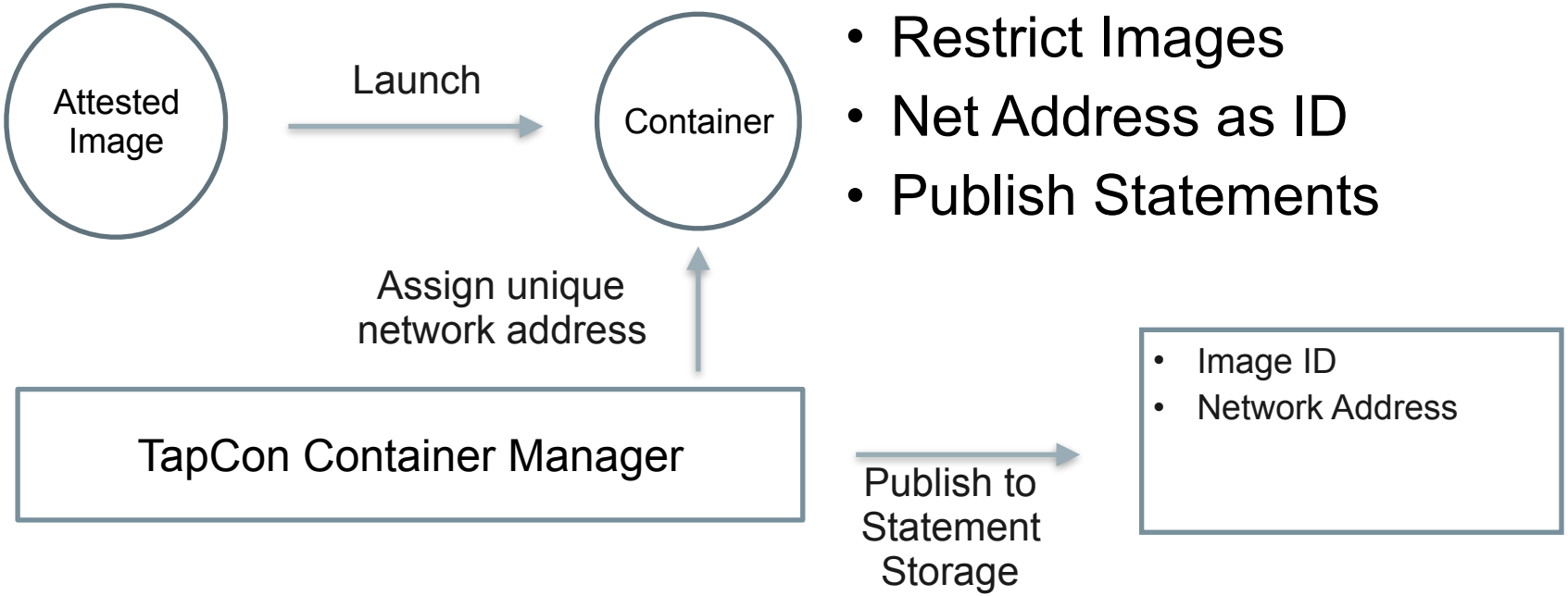
Question: How do we attest source of a container?

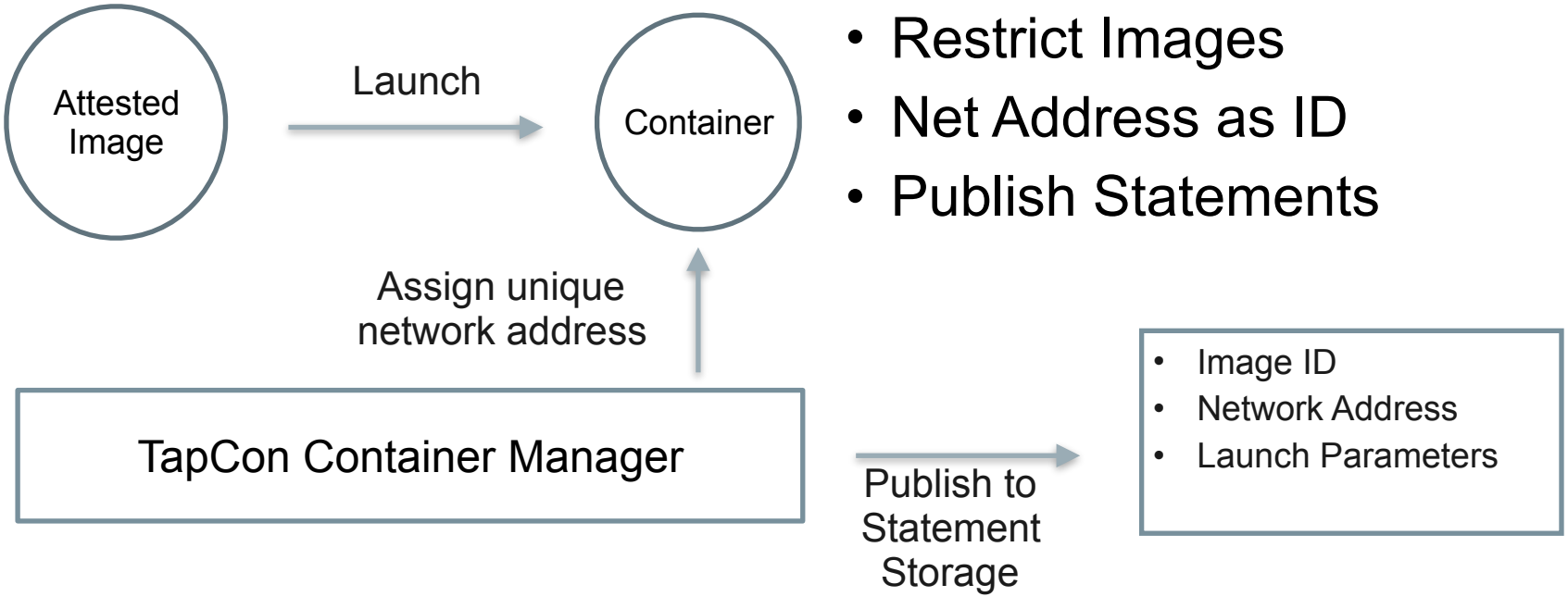
- Restrict Images
- Net Address as ID
- Publish Statements



Question: How do we attest source of a container?

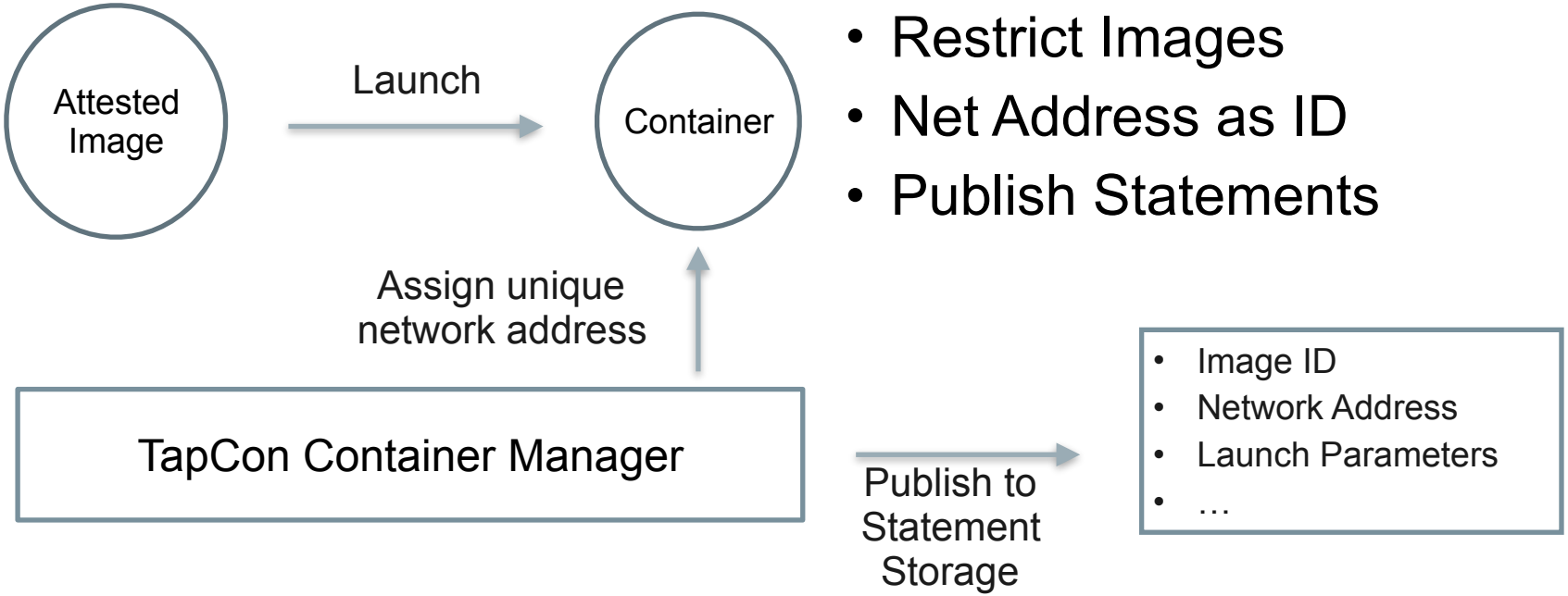
- Restrict Images
- Net Address as ID
- Publish Statements





Question: How do we attest source of a container?

- Restrict Images
- Net Address as ID
- Publish Statements



Question: How do we attest source of a container?

- Restrict Images
- Net Address as ID
- Publish Statements

- Image ID
- Network Address
- Launch Parameters
- …

- Image ID
- Network Address
- Launch Parameters
- …

- Image ID
- Network Address
- Launch Parameters
- …

Image Statement:
Image ID, source repo

- Image ID
- Network Address
- Launch Parameters
- …

Image Statement:
Image ID, source repo

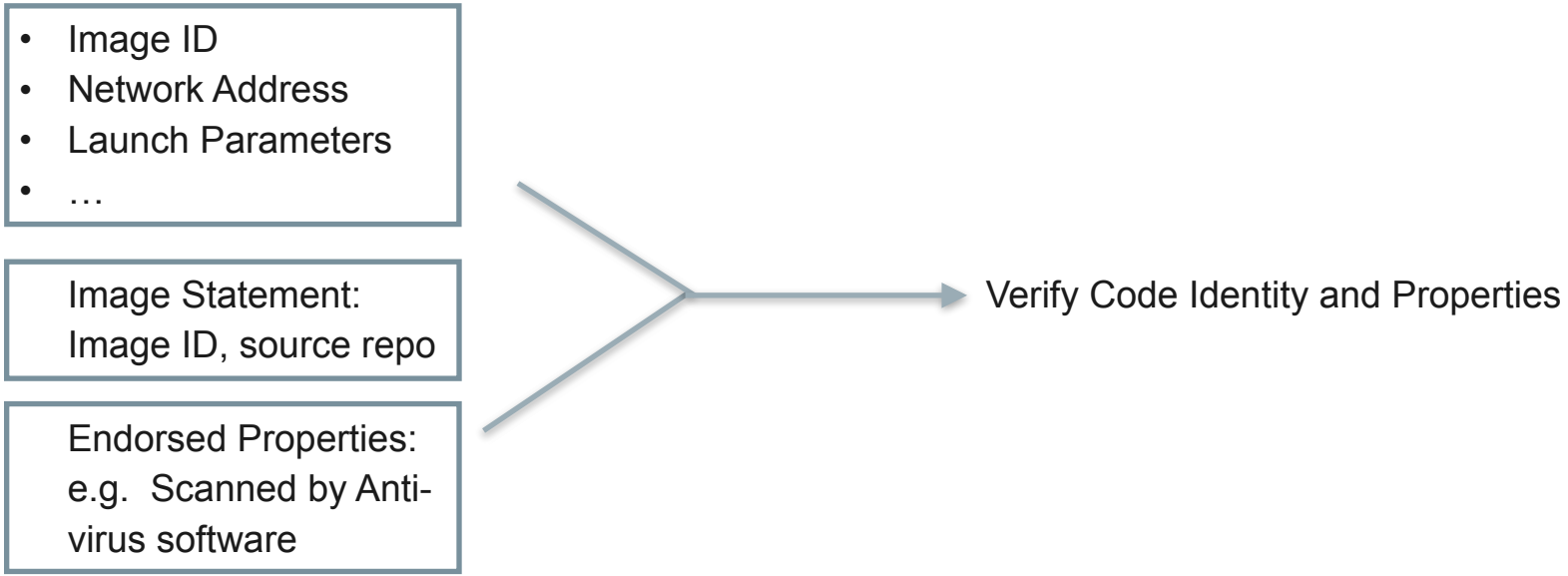
Clients may have own belief about code, or it can trust an experienced party to inspect the code and endorse it

- Image ID
- Network Address
- Launch Parameters
- …

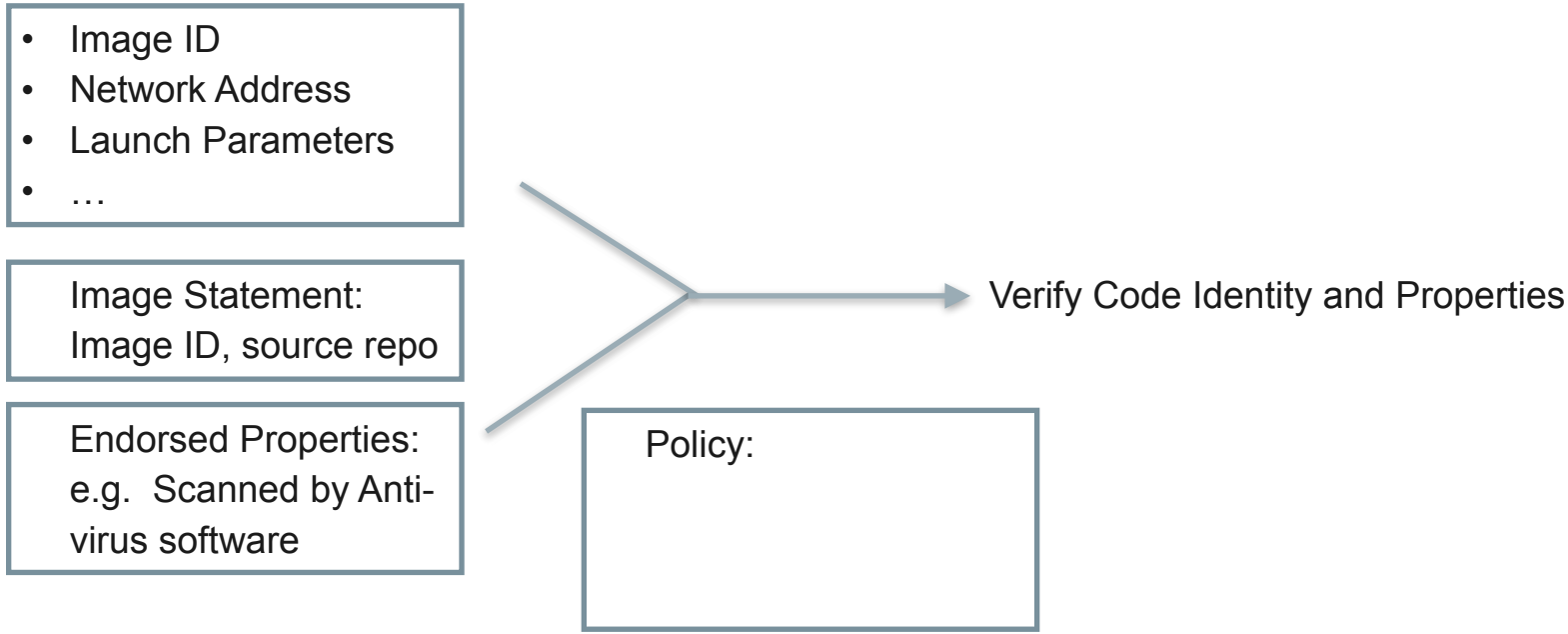
Image Statement:
Image ID, source repo

Endorsed Properties:
e.g. Scanned by Anti-virus software

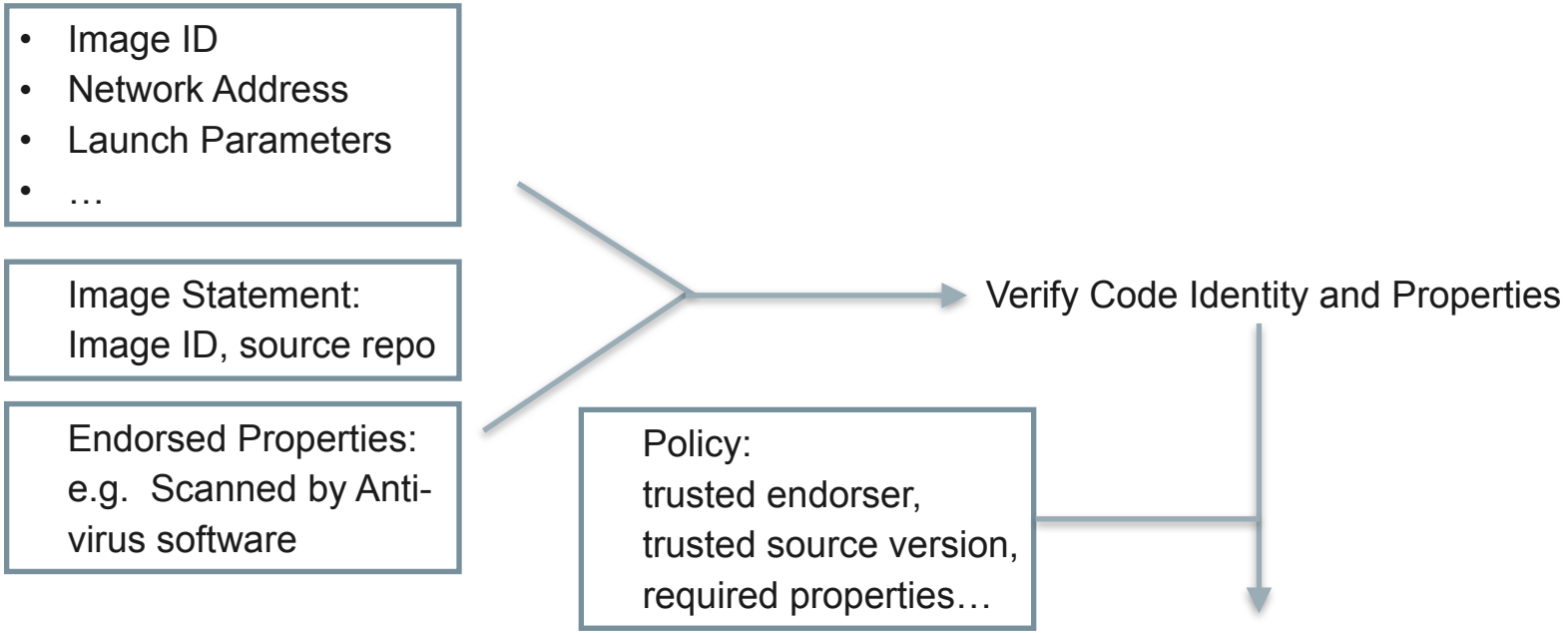
Clients may have own belief about code, or it can trust an experienced party to inspect the code and endorse it



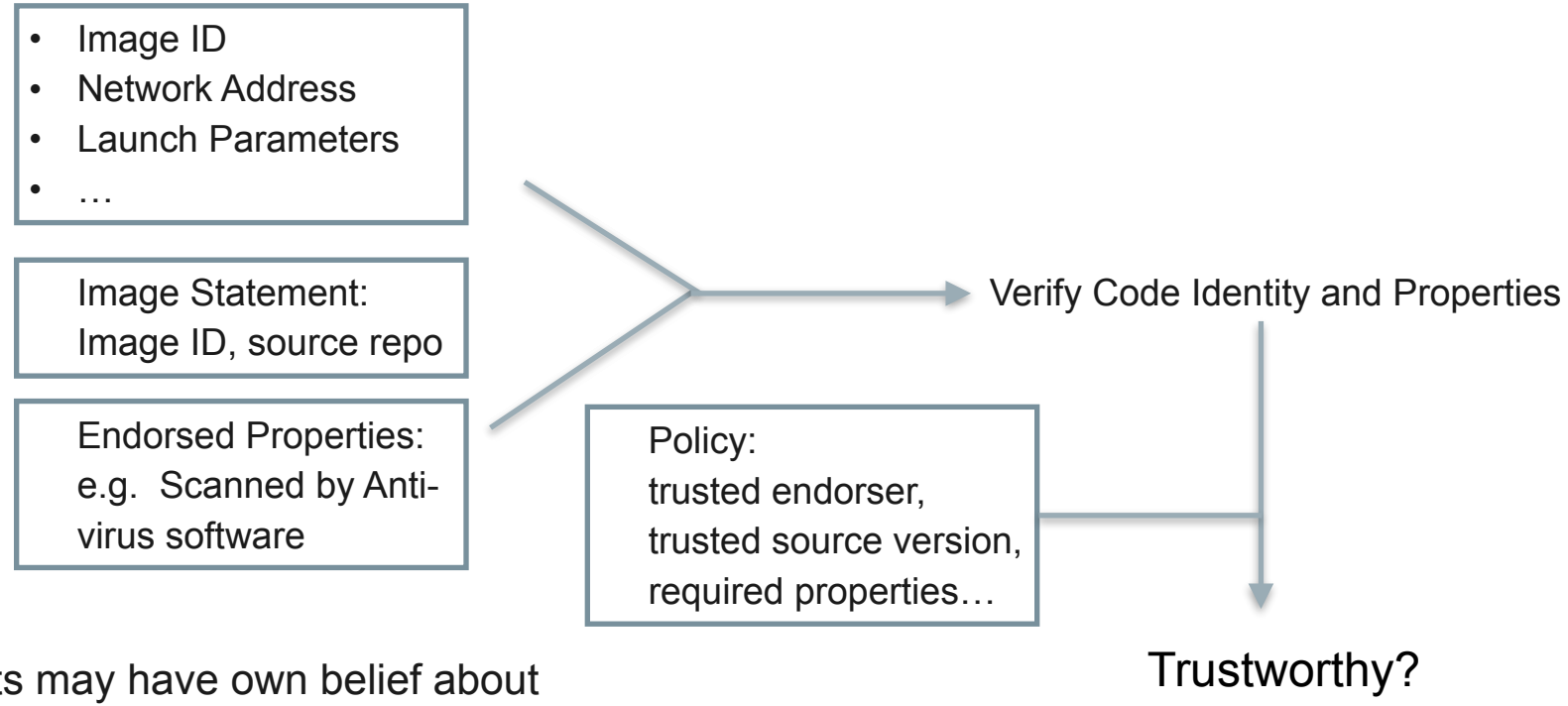
Clients may have own belief about code, or it can trust an experienced party to inspect the code and endorse it



Clients may have own belief about code, or it can trust an experienced party to inspect the code and endorse it



Clients may have own belief about code, or it can trust an experienced party to inspect the code and endorse it



Clients may have own belief about code, or it can trust an experienced party to inspect the code and endorse it

Verify Code Identity and Properties

Verify Code Identity and Properties

Verify Code Identity and Properties

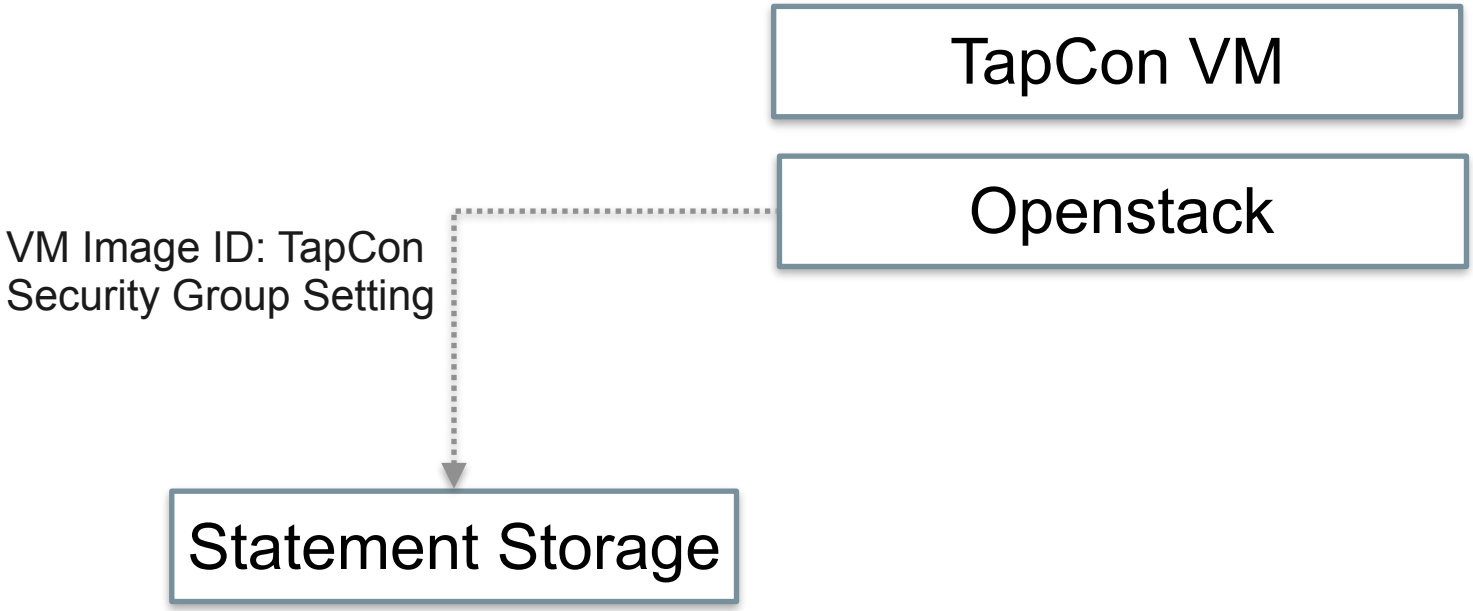
Openstack

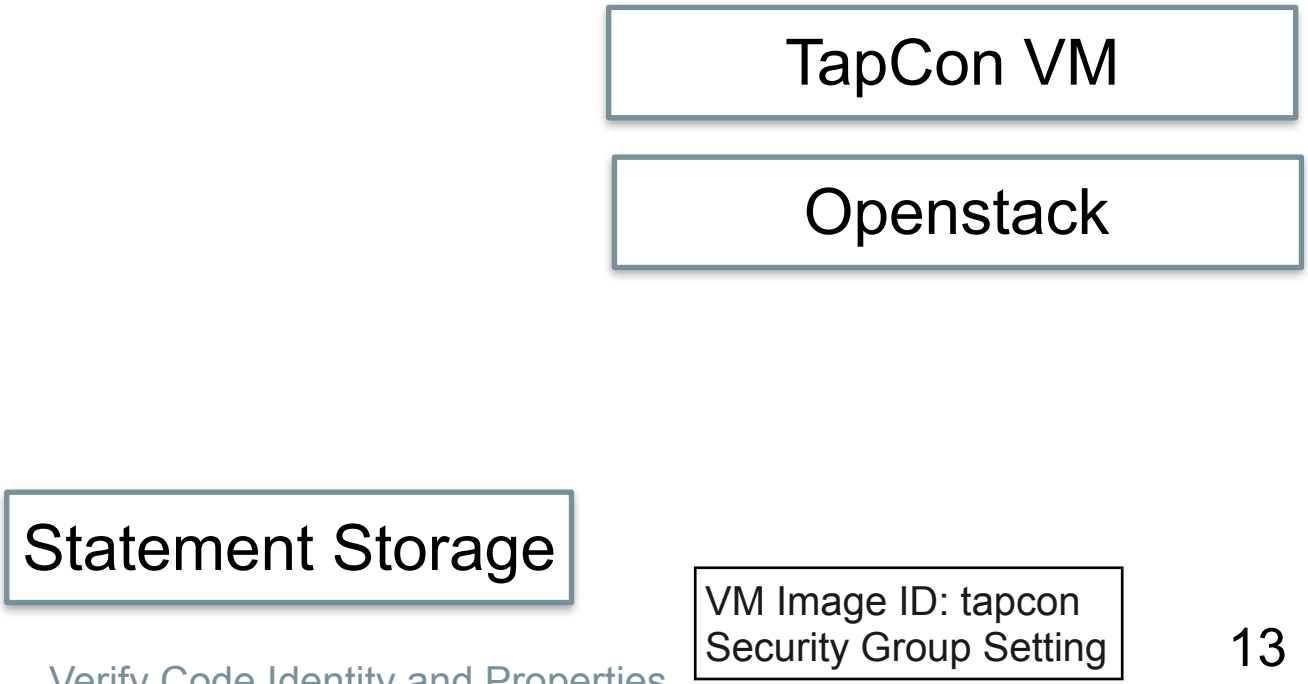
Statement Storage

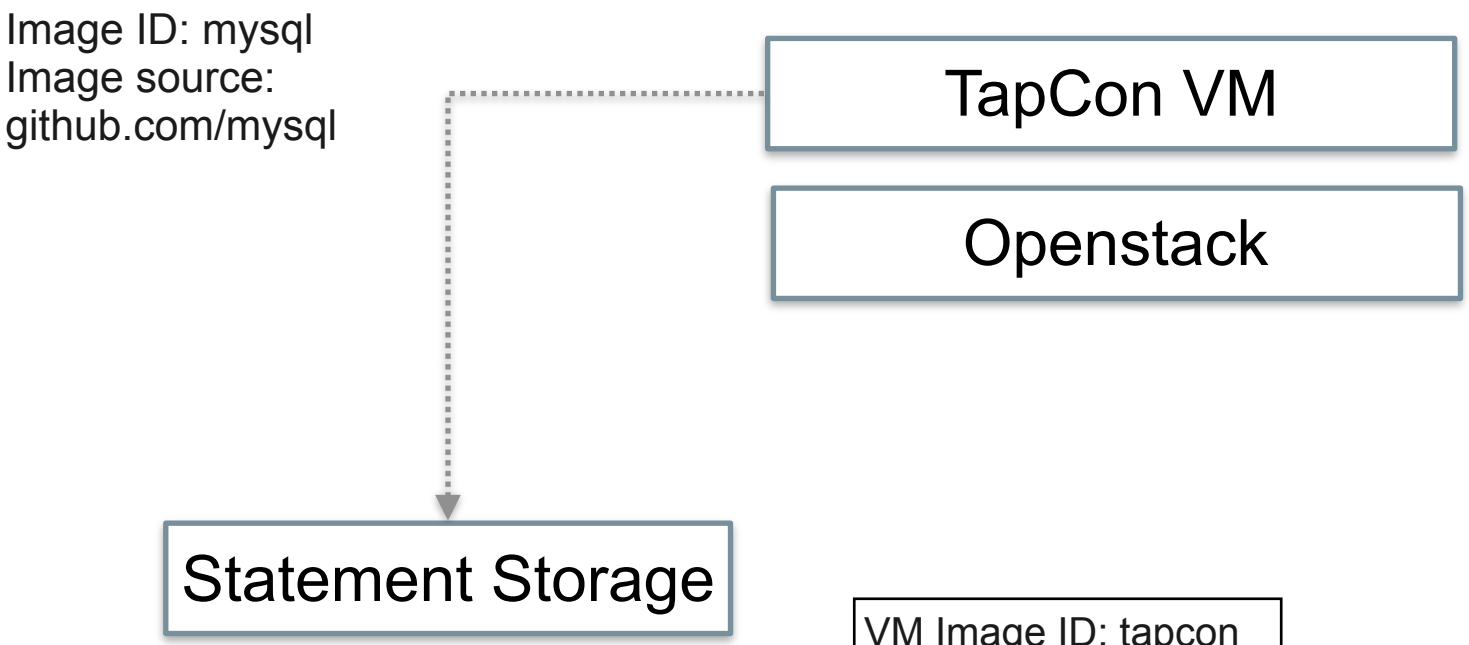
TapCon VM

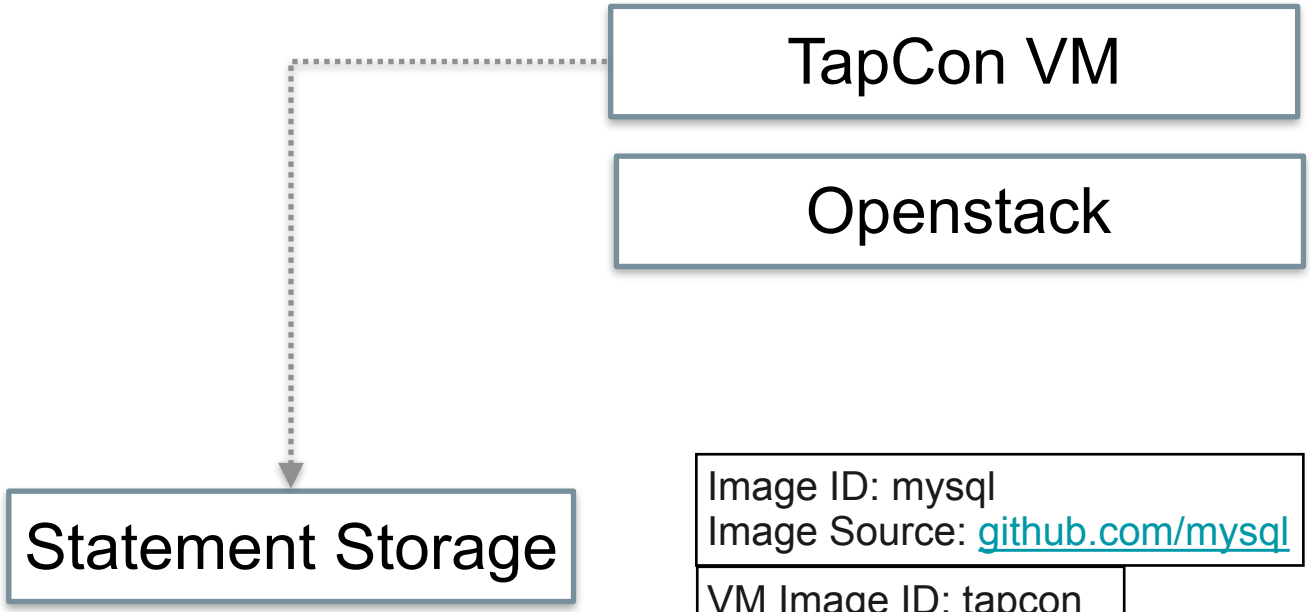
Openstack

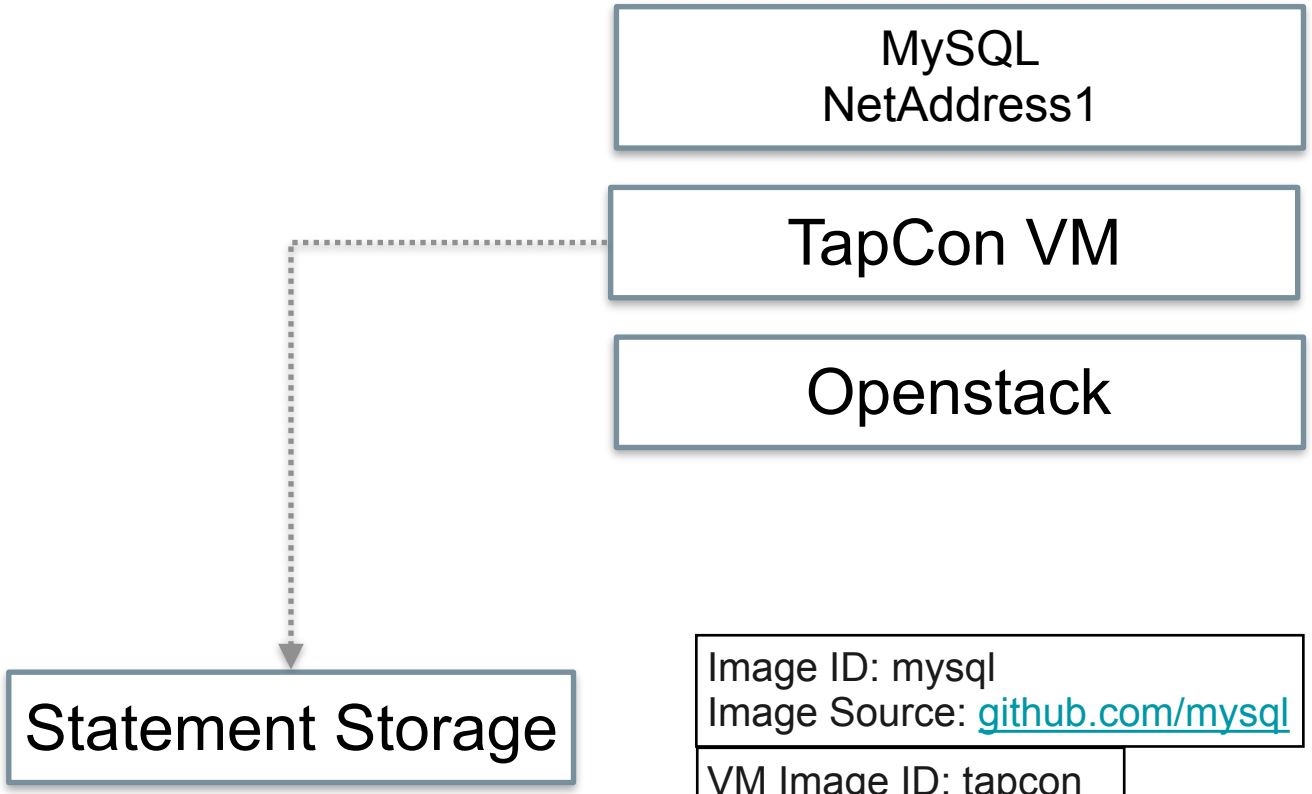
Statement Storage

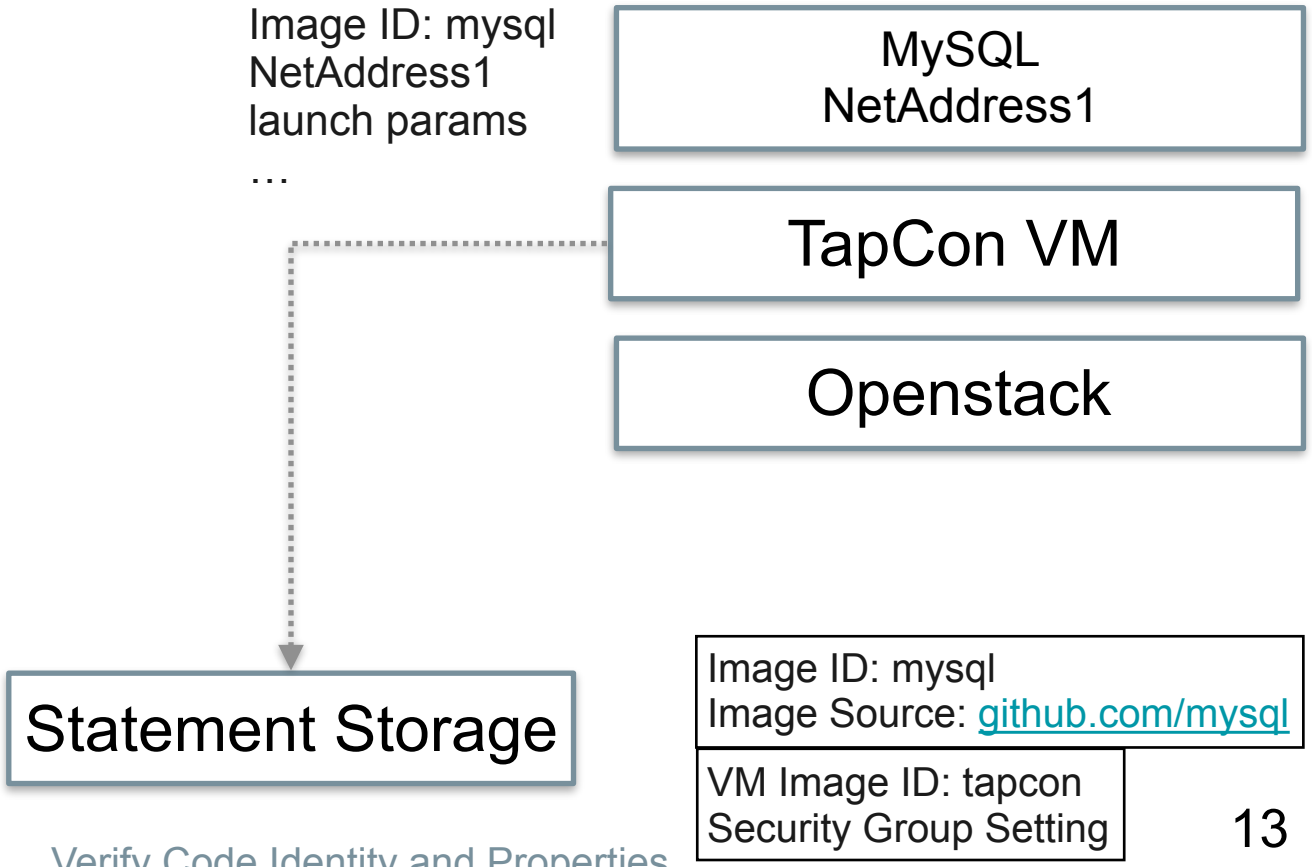

TapCon VM
Openstack
VM Image ID: TapCon
Security Group Setting
Statement Storage

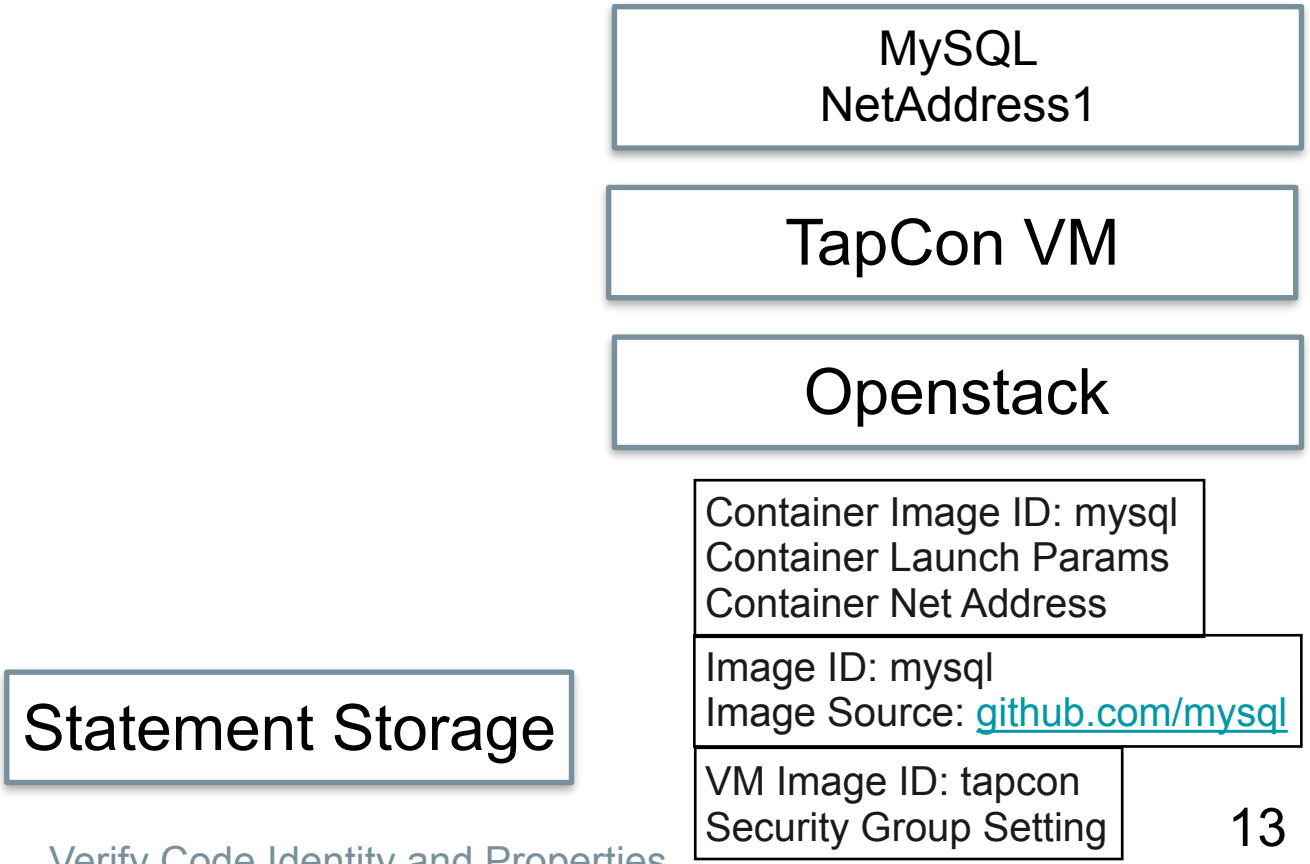

TapCon VM
Openstack
Statement Storage
VM Image ID: tapcon
Security Group Setting
Verify Code Identity and Properties


Image ID: mysql
Image source:
github.com/mysql
TapCon VM
Openstack
Statement Storage
VM Image ID: tapcon
Security Group Setting


TapCon VM
Openstack
Statement Storage
Image ID: mysql
Image Source: github.com/mysql
VM Image ID: tapcon
Security Group Setting


MySQL
NetAddress1
TapCon VM
Openstack
Statement Storage
Image ID: mysql
Image Source: github.com/mysql
VM Image ID: tapcon
Security Group Setting


Image ID: mysql
NetAddress1
launch params
…
MySQL
NetAddress1
TapCon VM
Openstack
Statement Storage
Image ID: mysql
Image Source: github.com/mysql
VM Image ID: tapcon
Security Group Setting


MySQL
NetAddress1
TapCon VM
Openstack
Container Image ID: mysql
Container Launch Params
Container Net Address
Image ID: mysql
Image Source: github.com/mysql
VM Image ID: tapcon
Security Group Setting
Statement Storage

MySQL
NetAddress1

Container Image ID: mysql
Container Launch Params
Container Net Address

Image ID: mysql
Image Source: github.com/mysql

VM Image ID: tapcon
Security Group Setting

Statement Storage

Verify Code Identity and Properties



MySQL
NetAddress1

Container Image ID: mysql
Container Launch Params
Container Net Address

Image ID: mysql
Image Source: github.com/mysql

VM Image ID: tapcon
Security Group Setting

Statement Storage

Verify Code Identity and Properties



InspectorA

source: github.com/mysql
endorse property: Inspected by SWAMP

MySQL
NetAddress1

Statement Storage

Container Image ID: mysql
Container Launch Params
Container Net Address

Image ID: mysql
Image Source: github.com/mysql

VM Image ID: tapcon
Security Group Setting

Verify Code Identity and Properties

MySQL
NetAddress1

Speaker: InspectorA
Source: github.com/mysql
Endorse: “Inspected by SWAMP”

Container Image ID: mysql
Container Launch Params
Container Net Address

Image ID: mysql
Image Source: github.com/mysql

VM Image ID: tapcon
Security Group Setting

Statement Storage

Verify Code Identity and Properties

MySQL
NetAddress1



Client

Speaker: InspectorA
Source: github.com/mysql
Endorse: “Inspected by SWAMP”

Container Image ID: mysql
Container Launch Params
Container Net Address

Image ID: mysql
Image Source: github.com/mysql

VM Image ID: tapcon
Security Group Setting

Statement Storage

MySQL
NetAddress1



Client

I trust InspectorA,
What's running on
NetAddress1?

Statement Storage

Speaker: InspectorA
Source: github.com/mysql
Endorse: "Inspected by SWAMP"

Container Image ID: mysql
Container Launch Params
Container Net Address

Image ID: mysql
Image Source: github.com/mysql

VM Image ID: tapcon
Security Group Setting

MySQL
NetAddress1



Client

I trust InspectorA,
What's running on
NetAddress1?

Source: github.com/mysql
Service has property
"Inspected by SWAMP"

Statement Storage

Speaker: InspectorA
Source: github.com/mysql
Endorse: "Inspected by SWAMP"

Container Image ID: mysql
Container Launch Params
Container Net Address

Image ID: mysql
Image Source: github.com/mysql

VM Image ID: tapcon
Security Group Setting

Verify Code Identity and Properties

How do we know know that:

Service at 192.168.0.1:5000
has property **“Inspected by SWAMP”**

Service at 192.168.0.1:5000
has property **“Inspected by SWAMP”**

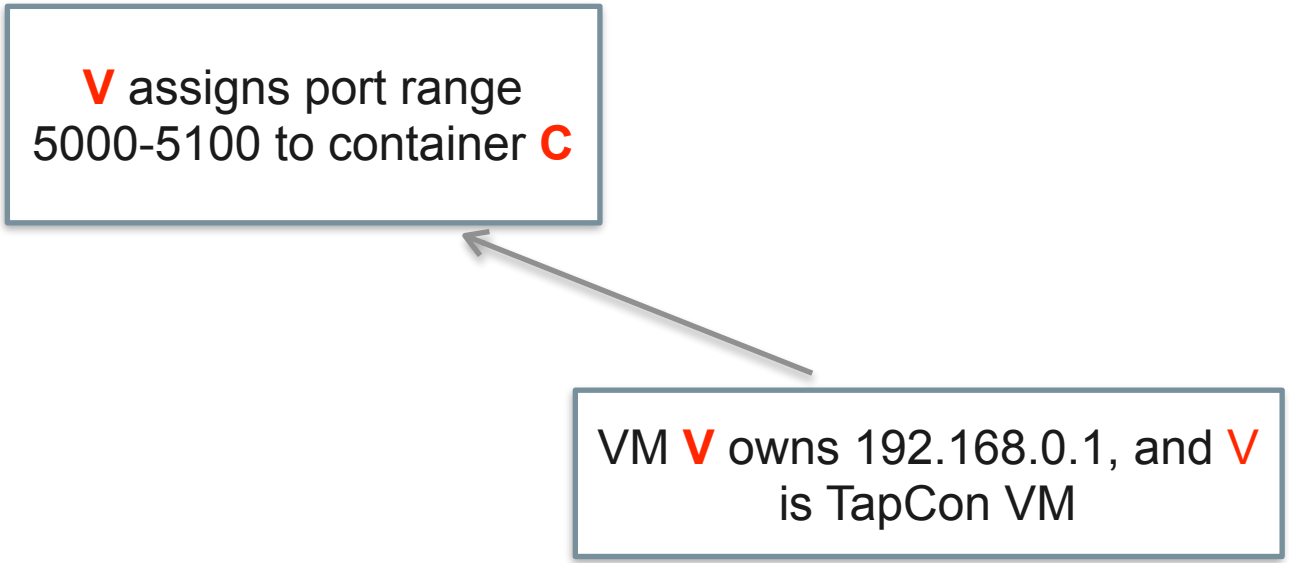
Service at 192.168.0.1:5000 has property **“Inspected by SWAMP”**

Service at 192.168.0.1:5000 has property **“Inspected by SWAMP”(P)**

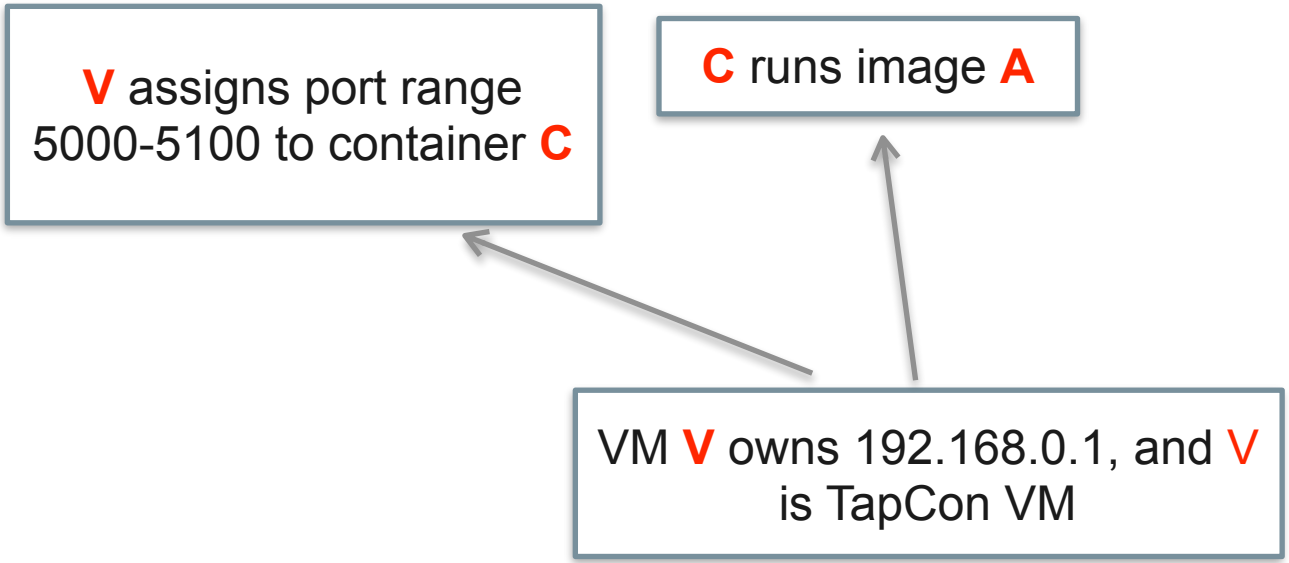
Service at 192.168.0.1:5000 has property **“Inspected by SWAMP”(P)**

VM **V** owns 192.168.0.1, and V is TapCon VM

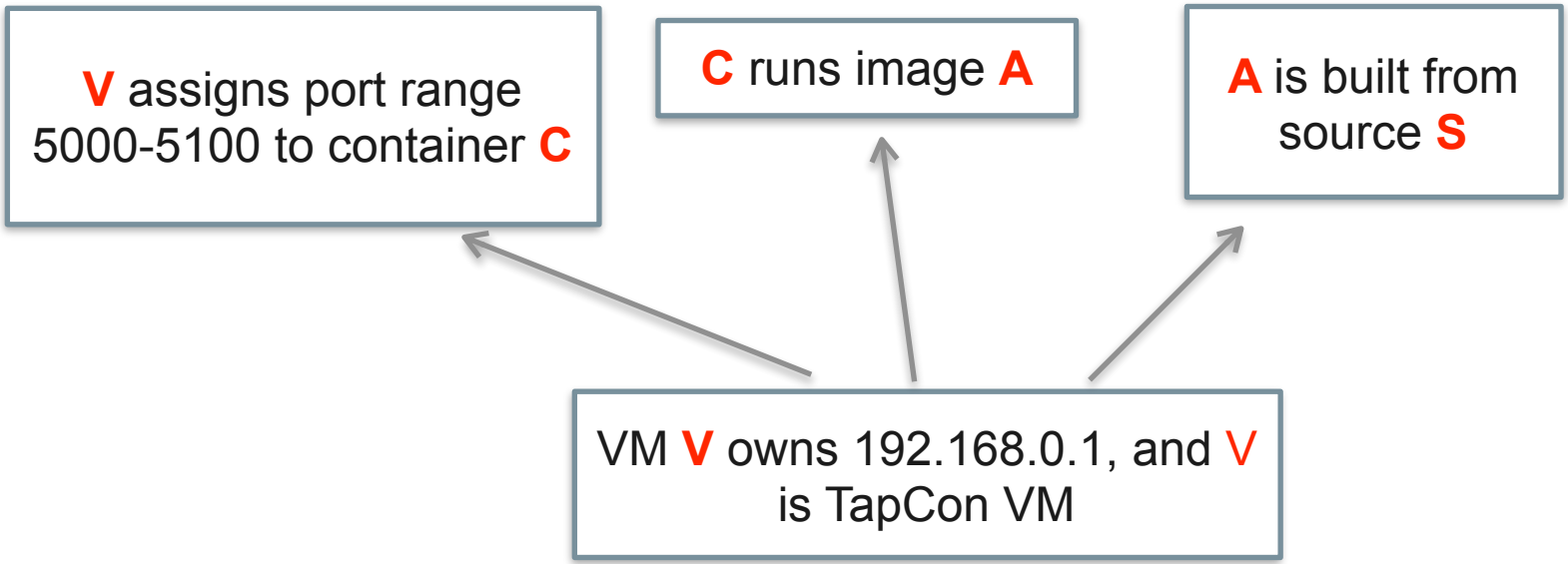
Service at 192.168.0.1:5000 has property **“Inspected by SWAMP”(P)**



Service at 192.168.0.1:5000 has property **“Inspected by SWAMP”(P)**

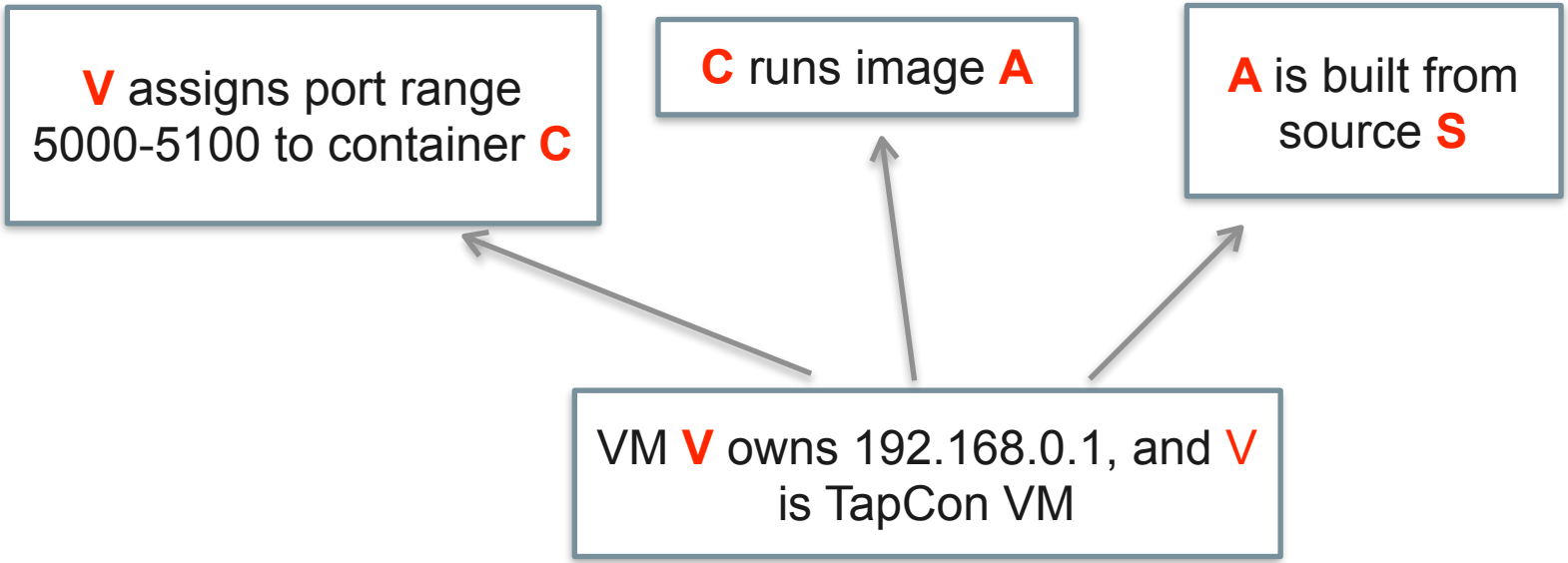


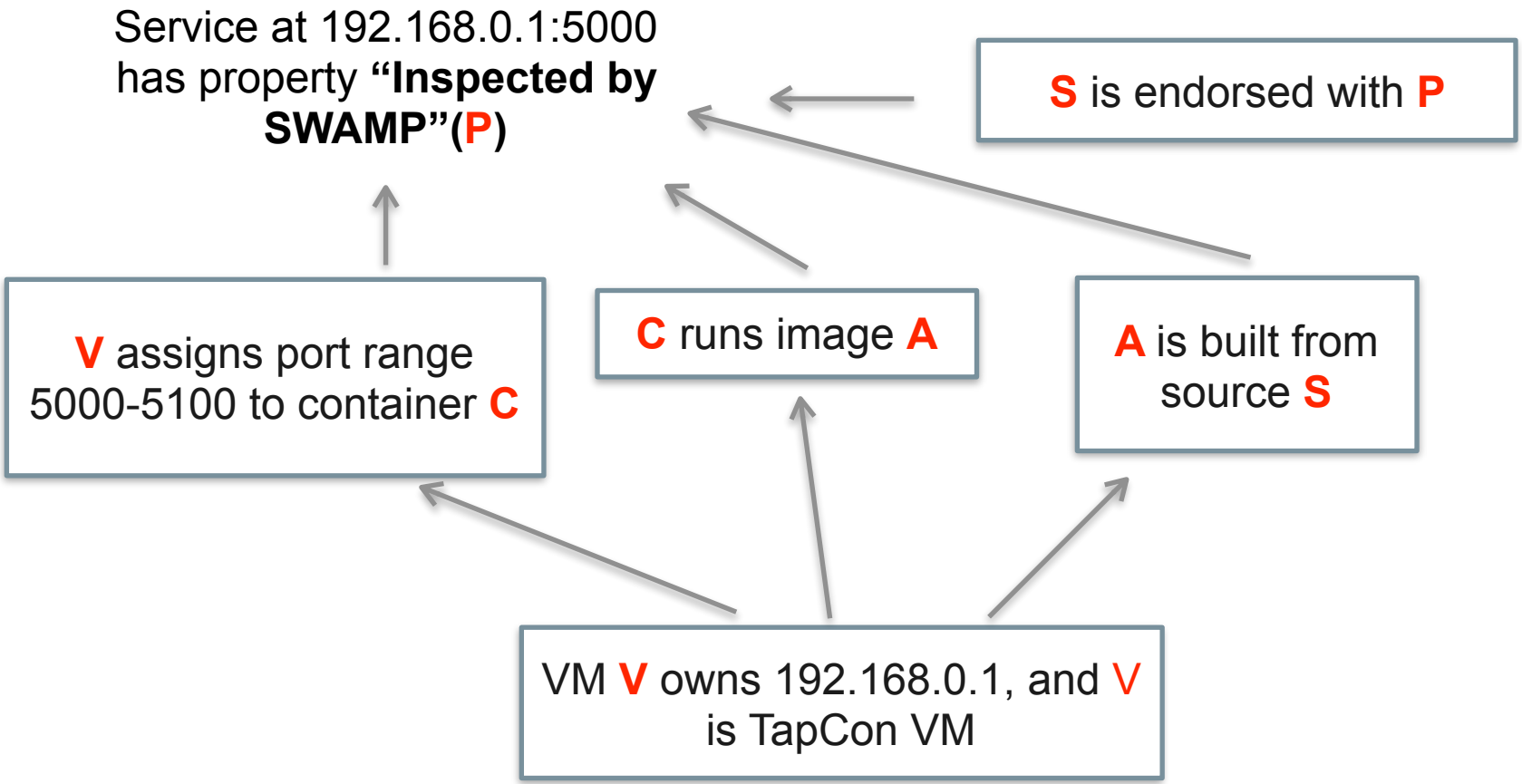
Service at 192.168.0.1:5000 has property **“Inspected by SWAMP”(P)**



Service at 192.168.0.1:5000 has property **“Inspected by SWAMP”(P)**

S is endorsed with **P**




Service at 192.168.0.1:5000 has property "Inspected by SWAMP"(P)
S is endorsed with P
V assigns port range 5000-5100 to container C
C runs image A
A is built from source S
VM V owns 192.168.0.1, and V is TapCon VM

Measuring TapCon Overhead



Alice

TapCon VM

Authorizer

Measuring TapCon Overhead



Alice

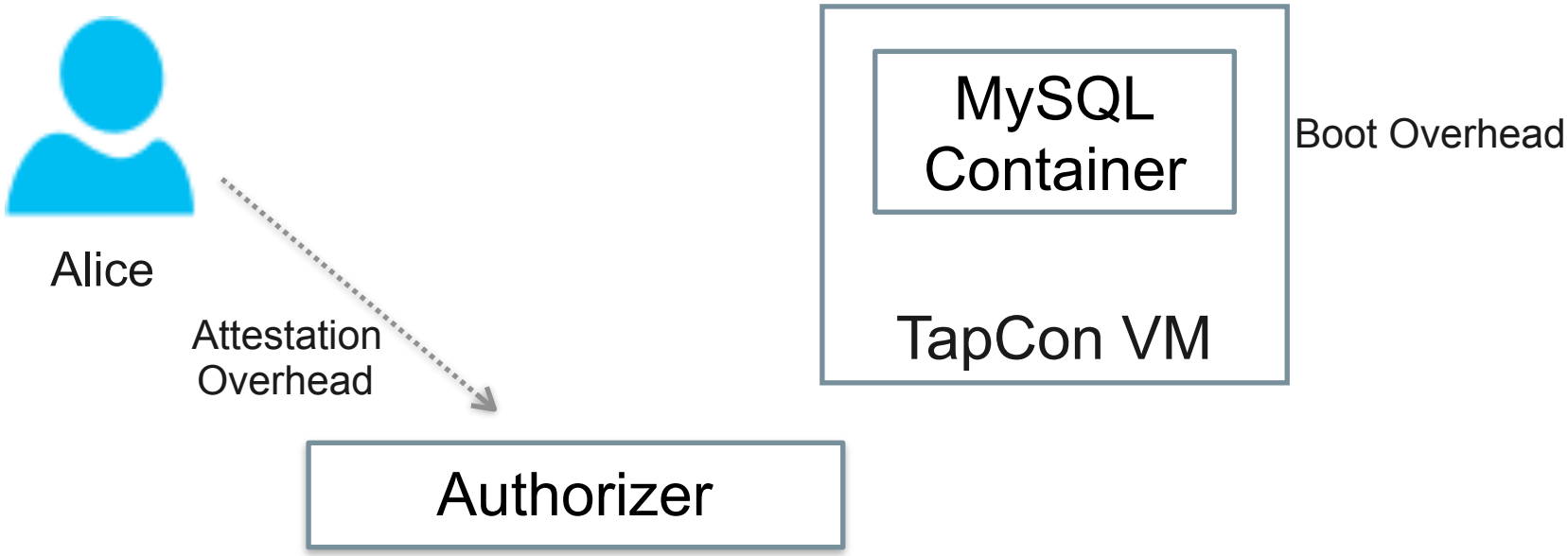
MySQL Container

TapCon VM

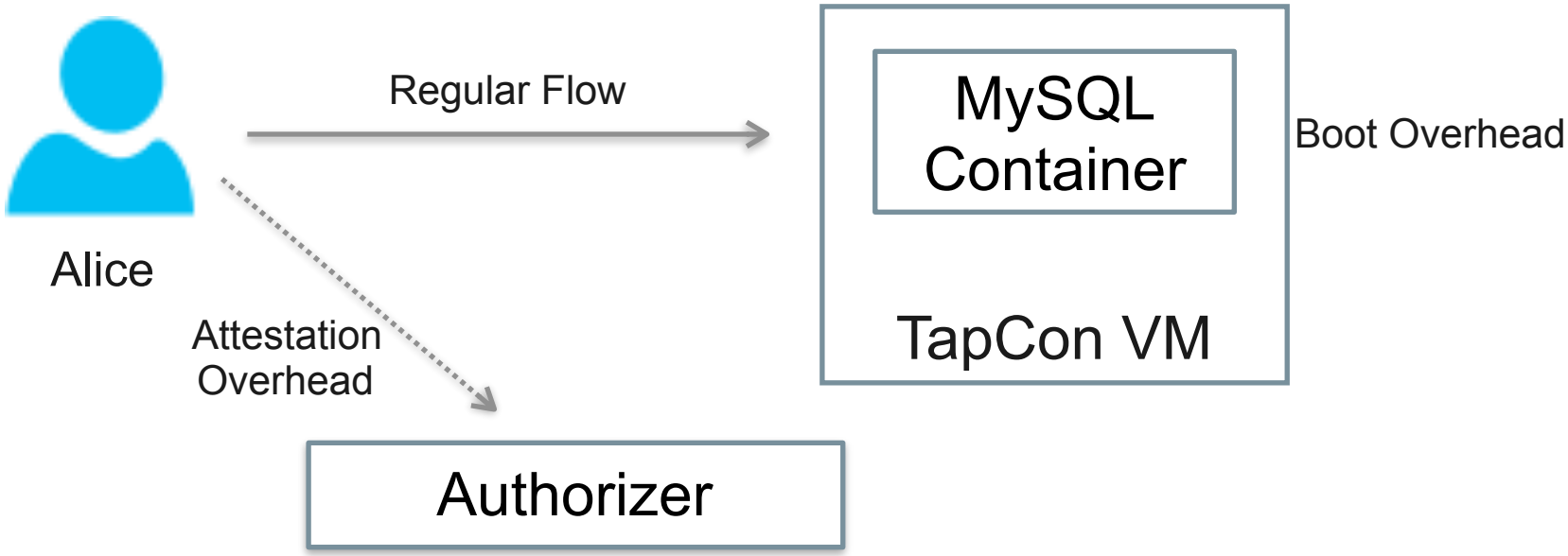
Boot Overhead

Authorizer

Measuring TapCon Overhead



Measuring TapCon Overhead



Performance Overhead

	Container Boot Time	First Query Time
Baseline	488ms (+-40ms)	9.6ms (+-0.3ms)
TapCon MySQL	497ms (+-49ms)	20.6ms (+-1.2ms)

IaaS: Openstack kilo+ Kvm
OS: Ubuntu 14.04
CPU: Intel E5-2630, 16 cores
Memory: 128GB
Network: 2x10GbE

Conclusion

Conclusion

- Social trust is not programmable

Conclusion

- Social trust is not programmable
- TapCon provides a trusted framework that connects source to containers, which gives clients more flexibility and possibilities in validating trustworthy of remote services

Future Work and Discussion

Future Work and Discussion

- TapCon binds containers to source

Future Work and Discussion

- TapCon binds containers to source
  - Finer grained attestation?

Future Work and Discussion

- TapCon binds containers to source
  - Finer grained attestation?
  - What specific source properties are useful?

Future Work and Discussion

- TapCon binds containers to source
  - Finer grained attestation?
  - What specific source properties are useful?
  - Are they available now? e.g. IBM vulnerability advisor

Future Work and Discussion

- TapCon binds containers to source
  - Finer grained attestation?
  - What specific source properties are useful?
  - Are they available now? e.g. IBM vulnerability advisor

- IaaS provider serves a unique role

Future Work and Discussion

- TapCon binds containers to source
  - Finer grained attestation?
  - What specific source properties are useful?
  - Are they available now? e.g. IBM vulnerability advisor

- IaaS provider serves a unique role
  - Attestation is only one example. What else can IaaS help to secure trust for a tenant service?

Future Work and Discussion

- TapCon binds containers to source
  - Finer grained attestation?
  - What specific source properties are useful?
  - Are they available now? e.g. IBM vulnerability advisor

- IaaS provider serves a unique role
  - Attestation is only one example. What else can IaaS help to secure trust for a tenant service?
  - Incorporate hardware trust (e.g. SGX)?

Future Work and Discussion

- TapCon binds containers to source
  - Finer grained attestation?
  - What specific source properties are useful?
  - Are they available now? e.g. IBM vulnerability advisor

- IaaS provider serves a unique role
  - Attestation is only one example. What else can IaaS help to secure trust for a tenant service?
  - Incorporate hardware trust (e.g. SGX)?

- Limitation of logic trust?

Future Work and Discussion

- TapCon binds containers to source
  - Finer grained attestation?
  - What specific source properties are useful?
  - Are they available now? e.g. IBM vulnerability advisor

- IaaS provider serves a unique role
  - Attestation is only one example. What else can IaaS help to secure trust for a tenant service?
  - Incorporate hardware trust (e.g. SGX)?

- Limitation of logic trust?

Thanks & Questions?

backup

Related Works

Related Works

- Cryptography: [Gentry’09], [Dijk’10], [Parno’13]

Related Works

- Cryptography: [Gentry’09], [Dijk’10], [Parno’13]
- Information Flow Control: [Andrew’97], [Zeldovich’06], [Maxwell’07]

Related Works

- Cryptography: [Gentry’09], [Dijk’10], [Parno’13]
- Information Flow Control: [Andrew’97], [Zeldovich’06], [Maxwell’07]
- Restricted Functionalities: [Miklas’09], [Roy’10]

Related Works

- Cryptography: [Gentry’09], [Dijk’10], [Parno’13]
- Information Flow Control: [Andrew’97], [Zeldovich’06], [Maxwell’07]
- Restricted Functionalities: [Miklas’09], [Roy’10]
- Attestation & Access Control: [Garfinkel’03], [Sirer’11], [Baumann’14],[Hunt’16]

Assign Network Address

Assign Network Address

- IPv4 + Ports

Assign Network Address

- IPv4 + Ports
- IPv6 (every container has an unique IP)

Assign Network Address

- IPv4 + Ports
- IPv6 (every container has an unique IP)
- Kubernete Trireme

Code Quality & Property

Code Quality & Property

- Scanned by security tools can enhance assurance of code

Threat Model

Threat Model

- IaaS provider is trusted

Threat Model

- IaaS provider is trusted
- Service owners are careless, or even malicious

Threat Model

- IaaS provider is trusted
- Service owners are careless, or even malicious
  - ✦ they may accidentally run code with known vulnerabilities

Threat Model

- IaaS provider is trusted
- Service owners are careless, or even malicious
  - ✦ they may accidentally run code with known vulnerabilities
  - ✦ they may change the security settings at any time

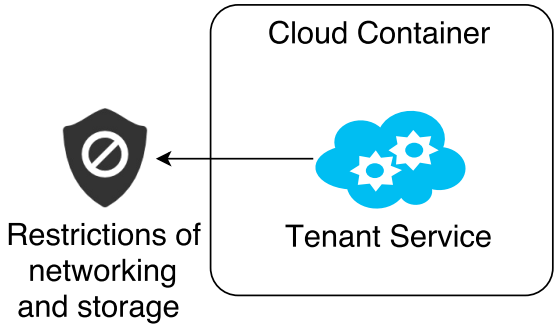
IaaS Support

IaaS Support

- A **metadata service** stores IaaS statement

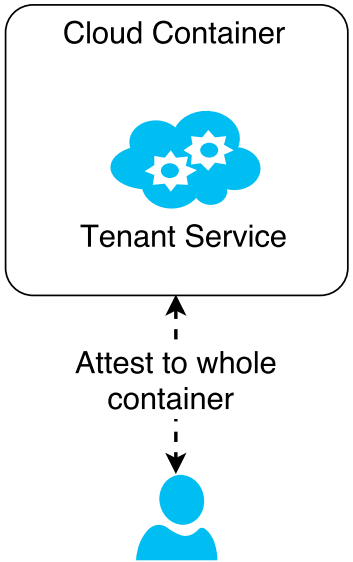
IaaS Support

- A **metadata service** stores IaaS statement
- **Attested VM**



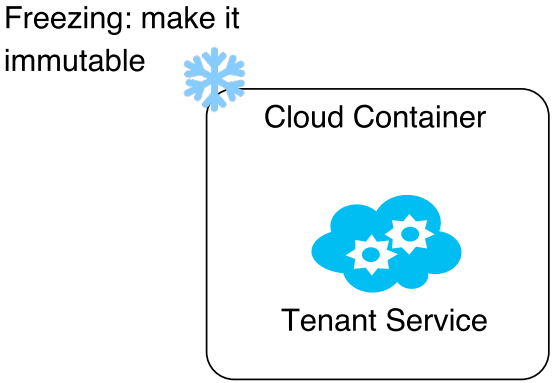
IaaS Support

- A **metadata service** stores IaaS statement
- **Attested VM**



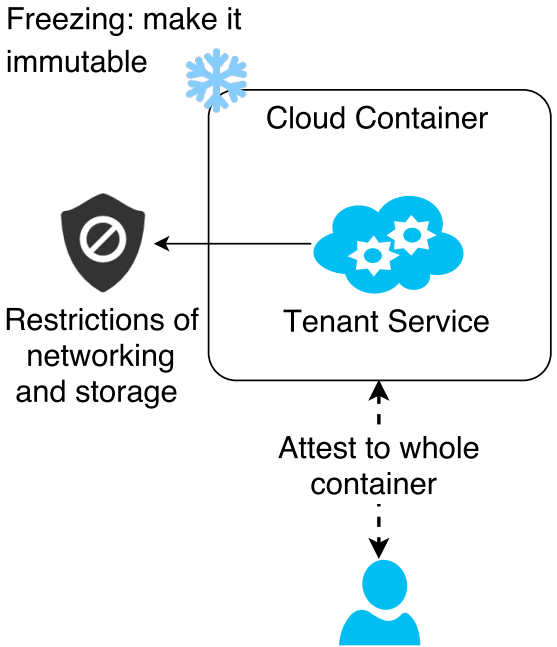
IaaS Support

- A **metadata service** stores IaaS statement
- **Attested VM**



IaaS Support

- A **metadata service** stores IaaS statement
- **Attested VM**



Cloud Assisted Attestation



Alice



192.168.0.1



Cloud Provider

Cloud Assisted Attestation



Alice

(1) what's running on 192.168.0.1?



192.168.0.1

amazon web services

Cloud Provider

Cloud Assisted Attestation



Alice

(1) what's running on 192.168.0.1?

(2) Image:Spark, Firewalls…

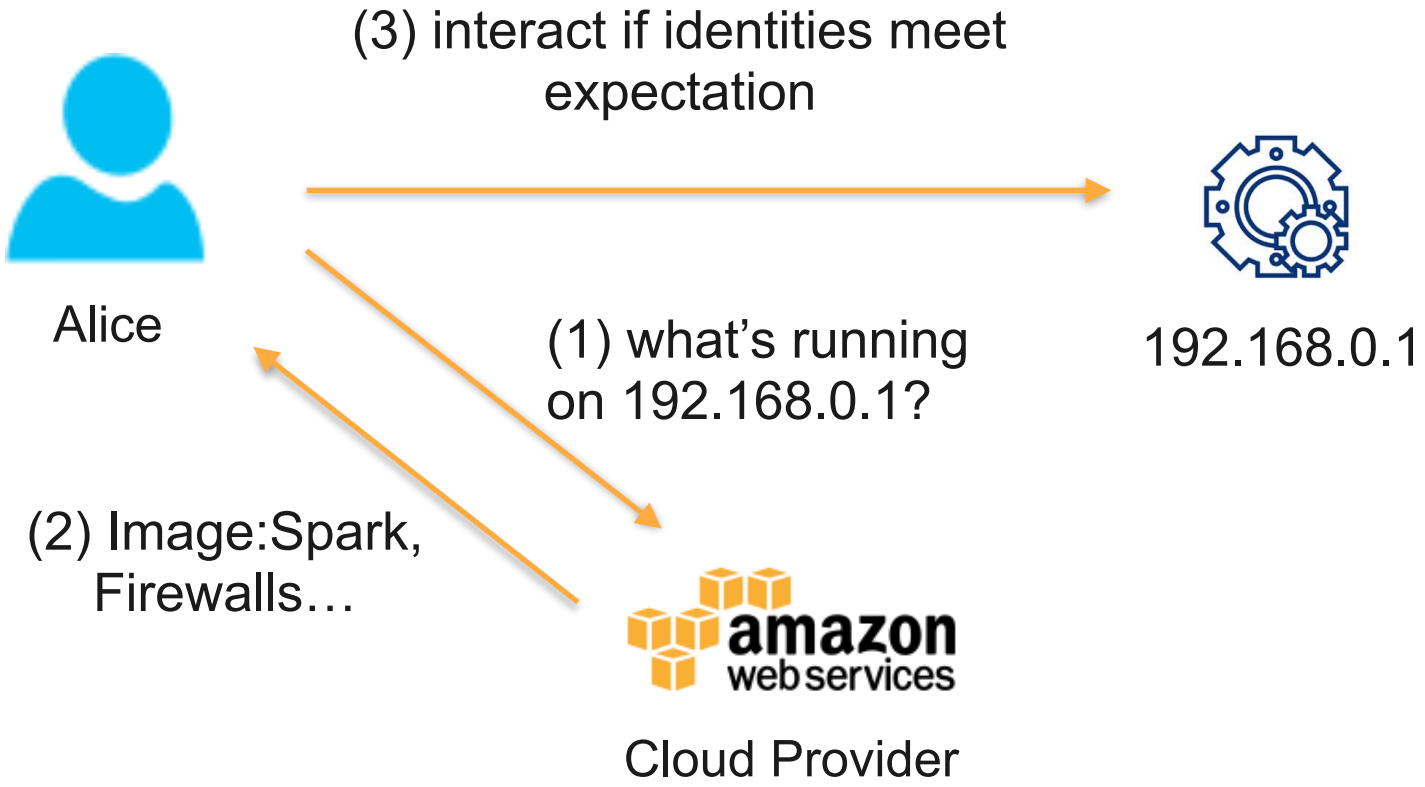


Cloud Provider



192.168.0.1

Cloud Assisted Attestation



Cloud Assisted Attestation

