Trestle: Compliance-as-Code Orchestrator and Automation Workflows

Anca Sailer, Lou Degenaro, Vikas Agarwal
IBM Research
Persona’s use of Compliance Artifacts

**Compliance as Code vs. Policy as Code**

### Controls
- **SC-7(4)**: Boundary protection “Implement a managed interface for each external telecommunication service”

### Rules
- **301**: “Ensure Kubernetes ingress is enabled through Cloud Internet Service”
- **302**: “Flow Logs must be enabled for param VPCs”

### Rules tests: Checks
- **ID C1**: Javascript check
- **ID C2**: Python check
- **ID C3**: OPA Rego check

### Assessment Results
- **Check Observation**: Result Pass/Fail
- **Check Risk**: Name – Value
- **Control Finding**: Name – Value
- **Aggregate results into controls posture**

### Tasks
- **Set Kubernetes ingress through Cloud Internet Service**
- **Associate with the mitigation, deviation, or remediation task**
NIST’s OSCAL language provides a standardized set of artifacts for compliance that can interoperate with operational systems.
DevSecOps provides a pattern for minimizing ‘waterfall’ roadblocks which can be leveraged for compliance.

Everything as code providing cross team visibility

Automated testing & verification

Systematic logging and monitoring of systems

_Trestle leverages this pattern for building compliance artifacts as code._
Conceptual Architecture

Applications

- Governed regulatory control content authoring and approval workflows
- Specialized Cloud / FedRAMP SSP Workflows
- Format conversions to/from OSCAL (e.g., spreadsheet, word doc, native artifacts)

Editing / authoring / transformation APIs and CLIs

- Tasks and Transformers
- Repository API
- CLI
- Markdown CLI
- Core OSCAL models

Trestle Base

- OSCAL adapter
- Core OSCAL models

Plugins (trestle-fedramp)
Trestle CLI

Requirement: As a new user to OSCAL the objects are extremely complex, I want tooling to help manage and create OSCAL files.

- Trestle provides functionality to manage large OSCAL files as fragments in a directory tree
- Utilities include generating object skeletons, import validation and release management on git based platforms
- Example below – use trestle to breakdown large OSCAL files to ease viewing / manipulation

```bash
(base) chris@jettopper nist-800-53 % ls
catalog.json
(base) chris@jettopper nist-800-53 % less catalog.json
78958 catalog.json
(base) chris@jettopper nist-800-53 % wc -l catalog.json
(base) chris@jettopper nist-800-53 % trestle split -f catalog.json -e 'catalog.groups.*'
(base) chris@jettopper nist-800-53 % cd ./catalog/groups
(base) chris@jettopper nist-800-53 % ls
0000_group.json 00003_group.json 00006_group.json 00009_group.json 00012_grc
0001_group.json 00004_group.json 00007_group.json 00010_group.json 00013_grc
0002_group.json 00005_group.json 00008_group.json 00011_group.json 00014_grc
```

Trestle used to break down an OSCAL catalog

Trestle merging and validating content meets schema / extended requirements
Trestle SDK: Tasks and Transformers

Requirement: Using trestle as an SDK to safely and automatically create OSCAL artifacts (Transitioning from 3rd party content to OSCAL)

• In order for OSCAL to provide value a set of converters are required from various formats.

• Trestle contains transformers which can be used both as an SDK and a CLI (e.g.: https://ibm.github.io/compliance-trestle/tutorials/task.tanuim-to-oscal/transformation/)

• Trestle conversion SDK is the basis for 3rd party conversions into IBM ‘Security and Compliance Centre’

• Trestle OSCAL object model can easily be used to convert content:
  - Excel files
  - XML content

• Demos https://github.com/IBM/compliance-trestle-demos/
Requirement: As a service team I would like to provide documentary artifacts to architecture/compliance/security only once.

- Based on an internal use case: Service teams are burdened by operational requirements
  - Particularly when multiple audits/reviews need to be conducted in parallel

- trestle author, combined with tests of OSCAL content, are used to enforce service teams follow templating.
  - Templates distributed by using `git submodules` for global consistency

- This allows CISO (as an example) teams to pull information from service teams confidently for reviews/audits/external documents.

- Allows service teams to manage all required artifacts in their VCS system and only have one system for approvals.

- Simplified demonstration using arc42 architecture templates.
  - [https://github.com/IBM/compliance-trestle-arc42-demo/](https://github.com/IBM/compliance-trestle-arc42-demo/)
Agile Authoring: SSP generation

- Requirement: As an a ‘system security plan’ author I need a workflow that allows me to have SMEs authors and reviewers edit and approve in parallel.

- ‘System security plans’ are complex documents requiring multiple users to edit and review

- Migrated SSP creation to per-control markdown in Github enterprise allowing users to edit individual files.

- Markdown provides an easy transformation path to oscal / HTML / other outputs.

- [trestle author ssp-generate](#) and ssp-assemble manage the workflow allowing information to be aggregated.

- CICD to validate that users content.

- Used for producing audited documentation currently.
# Boundary Protection

## Control Statement

The information system:

- (a) Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;

- (b) Implements subnetworks for publicly accessible system components that are isolated from internal organizational networks; and

- (c) Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

## Control guidance

Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses.
---

```
x-trestle-set-params:
  sc_7_prm_1:
    select: choice:
      - physically
      - logically
    sort-id: sc-07
---
```

## sc-7 - `[System and Communications Protection]` Boundary Protection

### Control Statement

The information system:

- `[a.]` Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;

- `[b.]` Implements subnetworks for publicly accessible system components that are `{[insert: param, sc_7_prm_1]}` separated from internal organizational networks; and

- `[c.]` Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

### Editable Content

```yaml
<!- Make additions and edits below -->
<!- The above represents the contents of the control as received by the profile, prior to additions. -->
<!- If the profile makes additions to the control, they will appear below. -->

### Control additional_fs_cloud_guidance

The organization "service delivery" and "corporate" environments must be maintained as separate environments. That is, clear physical and/or logical boundaries separating the two environments must exist.
<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Description</th>
<th>NIST Mappings</th>
<th>Resource</th>
<th>Parameter</th>
<th>Value (Default/Alternative)</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpc_security_groups_inbound_no_wh_port</td>
<td>Ensure Virtual Private Cloud (VPC) security groups have no incoming rules that specify source IP 0.0.0.0/0 to SSH port.</td>
<td>AC-4 CMF-2 SC-7 (3) SC-7 (3)</td>
<td>VPC</td>
<td></td>
<td>SSH Port in_wh_port</td>
</tr>
<tr>
<td>vpc_security_groups_inbound_no_dnp_port</td>
<td>Ensure Virtual Private Cloud (VPC) security groups have no incoming rules that specify source IP 0.0.0.0/0 to RDP port.</td>
<td>AC-4 CMF-2 SC-7 (3) SC-7 (3)</td>
<td>VPC</td>
<td></td>
<td>RDP Port in_dnp_port</td>
</tr>
<tr>
<td>vpc_no_default_security_group_rules</td>
<td>Ensure Virtual Private Cloud (VPC) has no rules in the default security group.</td>
<td>AC-4 CMF-2 SC-7 (3) SC-7 (3)</td>
<td>VPC</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**OSCIA JSON**

```json
{"component_definition": {"id": 5412302, "title": "Ensure Virtual Private Cloud (VPC) security groups have no incoming rules that specify source IP 0.0.0.0/0 to SSH port.", "resource": "vpc_security_groups_inbound_no_wh_port", "description": "Ensure Virtual Private Cloud (VPC) security groups have no incoming rules that specify source IP 0.0.0.0/0 to SSH port.", "parameters": ["SSH Port in_wh_port", "ZZ"]},

{"component_definition": {"id": 5412302, "title": "Ensure Virtual Private Cloud (VPC) security groups have no incoming rules that specify source IP 0.0.0.0/0 to RDP port.", "resource": "vpc_security_groups_inbound_no_dnp_port", "description": "Ensure Virtual Private Cloud (VPC) security groups have no incoming rules that specify source IP 0.0.0.0/0 to RDP port.", "parameters": ["RDP Port in_dnp_port", "3389"]},

{"component_definition": {"id": 5412302, "title": "Ensure Virtual Private Cloud (VPC) has no rules in the default security group.", "resource": "vpc_no_default_security_group_rules", "description": "Ensure Virtual Private Cloud (VPC) has no rules in the default security group.", "parameters": ["VPC"]}
```
---
x-trestle-rules:
  - vpc_security_groups_inbound_no_ssh_port
  - vpc_security_groups_inbound_no_rdp_port
  - vpc_no_default_security_group_rules

sort-id: sc-07
---

# sc-7 - [System and Communications Protection] Boundary Protection

## Control Statement

The information system:

- [a.] Monitors and controls communications at the external boundary of ...
- [b.] Implements subnetworks for publicly accessible system component ...
- [c.] Connects to external networks or information systems only ...

## What is the solution and how is it implemented?

<!-- Enter implementation details in the parts below. -->

## Overall Control

## Implementation a.

The provider should ensure VPC security groups have no inbound rules ...

## Implementation b.

## Implementation c.

The provider should ensure VPC has no rules in the default security group ...

```json

```
```
### Component Definition

#### Spreadsheet

<table>
<thead>
<tr>
<th>rule_name_id</th>
<th>check_name_id</th>
<th>NIST Mappings</th>
<th>Resource</th>
<th>Check Implemented</th>
</tr>
</thead>
<tbody>
<tr>
<td>ufc_security_groups_inbound_no_ssh_port</td>
<td>check_ufc_security_groups_inbound_no_ssh_port</td>
<td>AC-4, CM-2, SC-7 (3), SC-7 (5)</td>
<td>VPC</td>
<td>yes</td>
</tr>
<tr>
<td>ufc_security_groups_inbound_no_rdp_port</td>
<td>check_ufc_security_groups_inbound_no_rdp_port</td>
<td>AC-4, CM-2, SC-7 (3), SC-7 (5)</td>
<td>VPC</td>
<td>yes</td>
</tr>
<tr>
<td>ufc_no_default_security_group_rules</td>
<td>check_ufc_no_default_security_group_rules</td>
<td>AC-4, CM-2, SC-7 (3), SC-7 (5)</td>
<td>VPC</td>
<td>no</td>
</tr>
</tbody>
</table>

#### OSCAL JSON

```json
"component-definition": {
  "uuid": "10849229-4361-4599-b013-d54702b7ba37",
  "metadata": {
    "title": "Component definition for NIST Special Publication 800-53 Revision 4 profiles"
  },
  "last-modified": "2022-05-17T18:15:41-04:00",
  "version": "1.0.2",
  "oscal-version": "1.0.2",
  "roles": [],
  "parties": [],
  "responsible-parties": [],
  "components": {
    "": {},
    "": {
      "uuid": "043132f2-304a-4d27-97d6-a0728e688258",
      "type": "Validation",
      "title": "TOOLCHAIN",
      "description": "TOOLCHAIN"
    }
  },
  "control-implementations": {
    "": {
      "uuid": "053132b2-51f8-455a-9e34-7638b3e13842",
    }
  }
}
```
---
x-trestle-props:
  control-origination:
  - Shared Service Provider and Customer Responsibility
  implementation-status:
  - implemented
  responsible-roles:
  - Customer

sort-id: sc-07
---

## sc-7 - \System and Communications Protection\ Boundary Protection

### Control Statement

The information system:

- `[a]` Monitors and controls communications at the external ...
- `[b]` Implements subnetworks for publicly accessible ...
- `[c]` Connects to external networks or information systems only through ...

### Control guidance

Managed interfaces include, for example, gateways, routers, firewalls ...

### What is the solution and how is it implemented?

1. Please leave this section blank and enter implementation details in the parts below. -->

### Overall Control

In IBM platform deny by default is implemented for all public ingress/egress traffic with network policies in place to specifically allow approved traffic.

### Implementation a.

---

---

### Implementation c.

---
GRC Framework

- **SCC (Technical)**
  - generic automated orchestrator
  - Policy Profile as Compliance as Code
  - Result, Inventory
  - Exchange Protocol (OSCAL-based)

- **BPM (Process)**
  - generic process orchestrator

- **Manual (Admin, Facilities)**
  - Exchange Protocol (OSCAL-based)

- **Cloud Policy and Rules Orchestrators**
  - Red Hat ACM/ACS
    - OpenShift specialized orchestrator
    - Policy as Kubernetes resource
    - Result, Inventory
    - Kubernetes Interface
    - OpenSCAP specialized rules assessment and enforcement
  - IBM SCC
    - IBM specialized orchestrator & rules assessment & enforcement
    - Policy as custom artifact
    - Custom Interface
  - Tanium
    - specialized orchestrator

- **Cloud Platform Rules Tools**
  - OCP Compliance Operator
    - Container/OS rules assessment
  - OCP GateKeeper
    - Container rules (Kube policy) enforcement
  - Custom Interface
  - No Result

- **Operating System Rules Tools**
  - Red Hat CIS
    - Result, Inventory
    - Custom Interface
  - Windows CIS
    - Custom Interface
  - OpenSCAP
    - specialized rules assessment and enforcement

- **GUI** Governance, Risk, and Compliance (GRC)
  - Regulations, Standards, Laws
  - (full posture orchestrator)