System Components and Inventory

Inventory Approaches

OSCAL makes two approaches available for depicting the system inventory:

- **Flat Approach**: Aligns with today's FedRAMP Integrated inventory workbook where all of the information on a spreadsheet row is captured in a single assembly.
- **Normalized Approach**: Common information is normalized as OSCAL components. inventory-items point to components for common information.

With the **flat approach**, all content on a spreadsheet row appears in a single OSCAL inventory-item assembly. This results in a great deal of redundant information but is a simple transition from the current spreadsheet approach.

See Inventory: Flat Approach for more information.

> ### Retrofit Adoption Path: MVP
>
> If you have an existing FedRAMP authorization and are using the FedRAMP inventory spreadsheet template, start with the flat approach, and migrate over time to the normalized approach.

With the **Normalized approach**, common information is captured once in a component assembly. Each instance of that component has its own inventory-item assembly, which cites the relevant component and only includes information unique to that instance.

See Inventory: Normalized Approach for more information.

> ### New Adoption Path: Core
>
> If you are adopting OSCAL at the beginning of your FedRAMP journey, define components first, then regerence those components as you generate inventory.

Example

The same Linux operating system is used as the platform for all database and web servers. Most details about operating system are captured once as a component, including OS name, version number, and patch level.

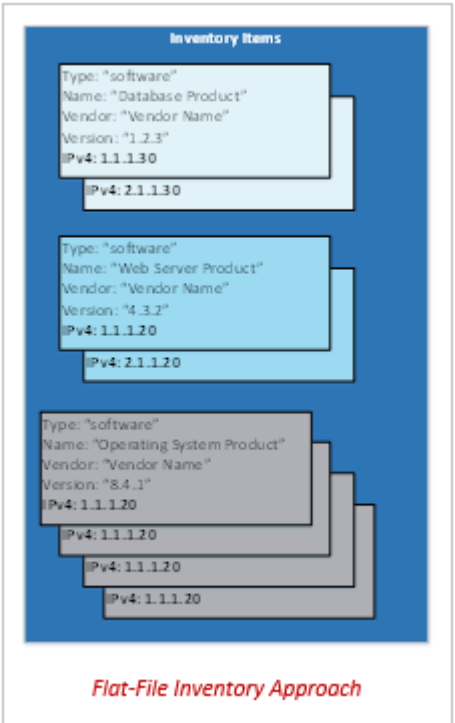
If four Linux instances are used, each instance is an inventory item with a unique IP address and MAC address. Only those unique pieces are captured at the inventory level. All four inventory-items are linked to the component.

Inventory: Flat Approach

The flat approach to inventory is only intended as a starting point for service providers converting from a legacy FedRAMP inventory spreadsheet template.

If you are not converting legacy inventory, use the Inventory: Normalized Approach.

With the **flat approach**, all content on a spreadsheet row appears in a single OSCAL inventory-item assembly. This results in a great deal of redundant information but is a simple transition from the current spreadsheet approach.



Flat-File Inventory Approach

Flat Representation

```
system-security-plan:
  uuid: 11111111-2222-4000-8000-000000000000
  system-implementation:
    inventory-items:
    - uuid: 11111111-2222-4000-8000-011000000001
      description: Legacy Example (No implemented-component).
      props:
      - name: asset-id
        value: unique-asset-ID-01
      - name: ipv4-address
```

```
    value: 10.1.1.1
  - name: ipv6-address
    value: 2001:db8:3333:4444:5555:6666:7777:8888
  - name: virtual
    value: 'no'
  - name: public
    value: 'no'
  - name: fqdn
    value: dns.name
  - name: uri
    value: uniform.resource.identifier
  - name: netbios-name
    value: netbios-name
  - name: mac-address
    value: 00:00:00:00:00:00
  - name: asset-type
    value: operating-system
  - name: serial-number
    value: 'Serial #'
  - name: asset-tag
    value: Asset Tag
  - name: vlan-id
    value: VLAN Identifier
  - name: network-id
    value: Network Identifier
  - name: scan-type
    ns: http://fedramp.gov/ns/oscal
    value: infrastructure
  - name: vendor-name
    ns: http://fedramp.gov/ns/oscal
    value: Big Vendor, Inc.
  - name: scan-type
    ns: http://fedramp.gov/ns/oscal
    value: database
  - name: allows-authenticated-scan
    value: 'no'
    remarks: If no, explain why. If yes, omit remarks field.
  - name: physical-location
    value: Physical location of Asset
  - name: is-scanned
```

```
      value: 'yes'
      remarks: If no, explain why. If yes, omit remarks field.
    - name: function
      value: Required brief, text-based description.
      remarks: Optional, longer, formatted description.
    links:
    - href: '#11111111-2222-4000-8000-009000000002'
      rel: validation
    - href: '#11111111-2222-4000-8000-001000000059'
      rel: baseline
    responsible-parties:
    - role-id: asset-owner
      party-uuids:
      - 11111111-2222-4000-8000-004000000016
    - role-id: asset-administrator
      party-uuids:
      - 11111111-2222-4000-8000-004000000017
    remarks: 'COMMENTS: Additional information about this item.

      This links to a FIPS 140-2 validated software component that is used by this
      inventory item. This type of linkage to a validation through the component
      is preferable to the link[rel=''validation''] example above.'
```

Notes:

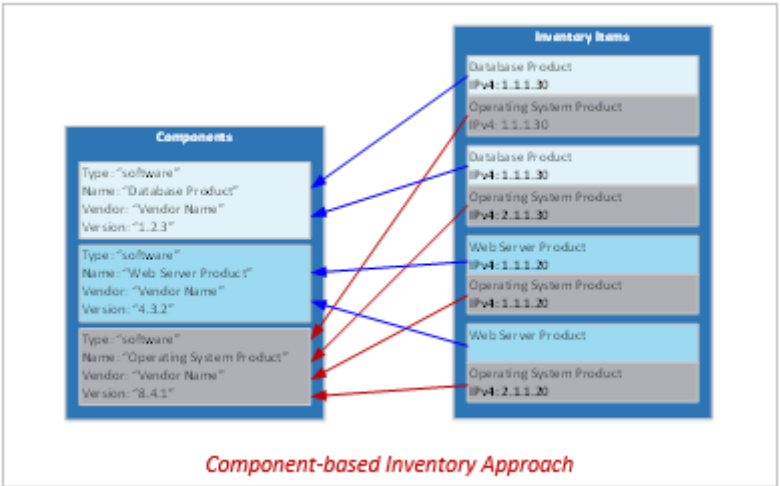
The value of asset-type determines whether the identified asset-administrator is managing a system or an application. Currently, any FedRAMP-defined asset-type implies the management of a system, and therefore, is to be scanned as infrastructure.

Inventory: Normalized Approach

The normalized approach is prefered. Organizations starting new with no legacy inventory reporting should use this.

For organizations converting from a legacy FedRAMP inventory spreadsheet template, consider starting with the Inventory: Flat Approach and migrating to the normalized approach over time.

With the **Normalized approach**, common information is captured once in a component assembly. Each instance of that component has its own inventory-item assembly, which cites the relevant component and only includes information unique to that instance.



Component-based Inventory Approach

Component-based Representation

```
system-security-plan:
  uuid: 11111111-2222-4000-8000-000000000000

  system-implementation:
    components:
    - uuid: 11111111-2222-4000-8000-009000300300
      type: software
      title: Linux Operating System
      description: This is a web server that communicates with a database via an encrypted
connection
      props:
      - name: asset-type
```

```
      value: operating-system
    - name: allows-authenticated-scan
      value: 'yes'
    - name: scan-type
      ns: http://fedramp.gov/ns/oscal
      value: web
    links:
    - href: '#11111111-2222-4000-8000-001000000059'
      rel: baseline
    status:
      state: operational

inventory-items:
- uuid: 11111111-2222-4000-8000-011000000023
  description: Instance of the Linux Operating System
  props:
  - name: asset-id
    value: unique-asset-ID-23
  - name: asset-type
    value: operating-system
  - name: ipv4-address
    value: 10.23.23.23
  - name: ipv6-address
    value: 0000:0000:0000:0000:0000:ffff:0a17:1717
  - name: virtual
    value: 'yes'
  - name: public
    value: 'no'
  - name: fqdn
    value: linux-host.example.internal
  - name: physical-location
    value: Primary Data Center
  - name: is-scanned
    value: 'yes'
  - name: scan-type
    ns: http://fedramp.gov/ns/oscal
    value: infrastructure
  responsible-parties:
  - role-id: asset-owner
    party-uuids:
```

```
      - 11111111-2222-4000-8000-004000000010
    - role-id: asset-administrator
      party-uuids:
      - 11111111-2222-4000-8000-004000000017
  implemented-components:
  - component-uuid: 11111111-2222-4000-8000-009000300300
```

Notes:

- If component-sample is an image of a Linux virtual machine (VM), and 10 instances of that VM are in use, there would be one (1) component assembly and ten (10) inventory-item assemblies, all referencing the same component.

Inventory Data Locations and XPath Queries

The following queries are intended to show where to find each piece of information within the system inventory template.

		Guidance	Valid Values	Requirement	Component	Inventory-Item	OSCAL Cardinality	Data Location: XPath Notation (CASE SENSITIVE)	NOTES
All Inventories	UNIQUE ASSET IDENTIFIER	Unique Identifier associated with the asset. This Identifier should be used consistently across all documents, 3PAOs artifacts, and any vulnerability scanning tools. For OS/Infrastructure and Web Application Software, this is typically an IP address or URL/DNS name. For a database, it is typically an IP address, URL, or database name. A CSP's own naming scheme is also acceptable as long as it has unique identifiers.	Must be unique.	Mandatory for all inventory records.		X	1	/*/system-implementation/system-inventory/inventory-item/prop[@asset-id="___"]/@value OR /*/system-implementation/component/prop[@name="asset-id"]/@value	The system-specific "Unique Asset Identifier" must be set as the asset-id flag on the inventory-item field.
	IPv4 or IPv6 Address	If available, state the IPv4 or IPv6 address of the inventory item. This can be left blank if one does not exist, or if it is a dynamic field. If the IP address is used as the Unique Asset Identifier, then this field will duplicate the contents of the Unique Asset Identifier column. If a device has multiple IP addresses, then include one row in this inventory for each IP address.		Optional, unless used as Identifier in vulnerability scans or security assessments.		X	0 - ∞	/*/system-implementation/system-inventory/inventory-item/prop[@name="ipv4-address"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="ipv6-address"]/@value	One prop field per IP address, if more than one.
	Virtual	Is this asset virtual?	Yes or No.	Mandatory for OS/Infrastructure, Software, and Database.	X	X	1	/*/system-implementation/component/prop[@name="virtual"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="virtual"]/@value	Must have "Virtual" at the inventory item-level either explicitly, or via a linked component. May define it at component level and propagate to inventory-item.
	Public	Is this asset a public facing device? That is, is it outside the boundary? If so, it is an entry point.	Yes or No.	Mandatory for OS/Infrastructure, Software, and Database.		X	1	/*/system-implementation/system-inventory/inventory-item/prop[@name="public"]/@value	
	DNS Name or URL	If available, state the DNS name or URL of the inventory item. This can be left blank if one does not exist, or it is a dynamic field.	Valid DNS name or URL.	Optional, unless used as Identifier in vulnerability scans or security assessments.		X	0 - ∞	/*/system-implementation/system-inventory/inventory-item/prop[@name="fqdn"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="uri"]/@value	May use either DNS name, URL, or both. Use a separate prop field for each DNS name and/or URL.

		Guidance	Valid Values	Requirement	Component	Inventory-Item	OSCAL Cardinality	Data Location: XPath Notation (CASE SENSITIVE)	NOTES
OS/Infrastructure Inventory	**NetBIOS Name**	If available, state the NetBIOS name. May be left blank if one does not exist, or dynamic.	Valid NetBIOS name.	Optional, unless used as Identifier in scans or security assessments.		X	0 - ∞	/*/system-implementation/system-inventory/inventory-item/prop[@name="netbios-name"]/@value	One prop field per NetBIOS name, if more than one.
	MAC Address	If available, state the MAC Address. May be left blank if one does not exist, or dynamic.	Valid MAC Address.	Optional, unless used as Identifier in scans or security assessments.		X	0 - ∞	/*/system-implementation/system-inventory/inventory-item/prop[@name="mac-address"]/@value	One prop field per MAC address, if more than one.
	Authenticated Scan	Is the asset is planned for an authenticated scan?	Yes or No.	Mandatory for OS/Infrastructure. Leave blank for Software and Database.	X	X	1	/*/system-implementation/component/prop[@name="allows-authenticated-scan"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="allows-authenticated-scan"]/@value	Must have "Authenticated-Scan" at the inventory-item level either explicitly or via a linked component. May define it at component level and propagate to inventory-item.
	Baseline Configuration Name	If available, provide the name of the configuration template used within the CSP configuration management.		Mandatory for OS/Infrastructure. Leave blank for Software and Database.	X	X	0 or 1	/*/system-implementation/component/prop[@name="baseline-configuration-name"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="baseline-configuration-name"]/@value	Must have "Baseline Configuration Name" at the inventory-item level either explicitly or via a linked component. May define it at component level and propagate to inventory-item.
	OS Name and Version	Operating System Name and Version running on the asset.		Optional for OS/Infrastructure. Leave blank for Software and Database.		X	0 or 1	/*/system-implementation/component/prop[@name="software-name"][@ns="https://fedramp.gov/ns/oscal"]/@value /*/system-implementation/component/prop[@name="version"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="software-name"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="software-version"]/@value	Use software name and version and set asset-type of "os". Required for operating systems. Must have "OS Name and Version" at the inventory-item level either explicitly or via a linked component. May define it at the component level and propagate to inventory item.
	Location	Physical location of hardware. Could include Data Center ID, Cage#, Rack# or other meaningful location identifiers.	Valid locations for CSP infrastructure.	Optional for OS/Infrastructure. Leave blank for Software and Database.		X	0 or 1	/*/system-implementation/system-inventory/inventory-item/prop[@name="physical-location"]/@value	
	Asset Type	Simple description of the asset's function (e.g., Router, Storage Array, DNS Server, etc.)		Mandatory for OS/Infrastructure. Leave blank for Software and Database.	X	X	1	/*/system-implementation/component/prop[@name="asset-type"]/@value /*/system-implementation/system-inventory/inventory-item[@name="asset-type"]/@value	Must use an Accepted Value (see Registry) if an applicable one exists. Must have "Asset Type" at the inventory-item level, either explicitly or via a linked component. May define it at component level and propagate to inventory-item.
	Hardware Make/Model	Name of the hardware product and model.		Mandatory for OS/Infrastructure. Leave blank for Software and Database.	X	X	0 or 1	/*/system-implementation/component/prop[@name="vendor-name"]/@value /*/system-implementation/component/prop[@name="model"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="vendor-name"][@ns="https://fedramp.gov/ns/oscal"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="hardware-model"]/@value	Must have "Hardware Vendor" and "Hardware Model" at the inventory item-level either explicitly, or via a linked component. May define it at component level and propagate to inventory-item. **NOTE**: @name="model" at component level, but @name="hardware-model" at inventory level.
	In Latest Scan	Should the asset appear in the network scans, and can it be probed by the scans creating the current POA&M?	Yes or No.	Mandatory for OS/Infrastructure. Leave blank for Software and Database.		X	1	/*/system-implementation/system-inventory/inventory-item/prop[@name="is-scanned"]/@value	

		Guidance	Valid Values	Requirement	Component	Inventory-Item	OSCAL Cardinality	Data Location: XPath Notation (CASE SENSITIVE)	NOTES
Software and Database Inventories	**Software/ Database Vendor**	Name of Software or Database vendor.	If open source (e.g., there is no "vendor), enter "Open Source" as the vendor name.	Mandatory for Software and Database. Leave blank for OS/Infrastructure.	X	X	0 or 1	/*/system-implementation/component/prop[@name="vendor-name"][@ns="https://fedramp.gov/ns/oscal"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="vendor-name"][@ns="https://fedramp.gov/ns/oscal"]/@value	Must have "Software/Database Vendor" at the inventory-item level either explicitly or via a linked component. May define it at component level and propagate to inventory-item.
	Software/ Database Name & Version	Name of Software or Database product and version number.		Mandatory for Software or Database. Leave blank for OS/Infrastructure.	X	X	0 or 1	/*/system-implementation/component/prop[@name="software-name"][@ns="https://fedramp.gov/ns/oscal"]/@value /*/system-implementation/component/prop[@name="version"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="software-name"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="software-version"]/@value	Required for software or database. Omit for OS/Infrastructure
	Patch Level	If applicable.		Optional if applicable. Otherwise, leave blank.	X	X	0 or 1	/*/system-implementation/component/prop[@name="patch-level"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="software-patch-level"]/@value	The "Patch Level" may be specified at the component or inventory-item level.
	Function	For Software or Database, the function provided by the Software or Database for the system.		Mandatory for Software or Database. Leave blank for OS/Infrastructure.	X	X	0 or 1	/*/system-implementation/component/prop[@name="function"]/@value /*/system-implementation/component/prop[@name="function"]/remarks /*/system-implementation/system-inventory/inventory-item/prop[@name="function"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="function"]/remarks	Must have a brief, text-base "function" description in the value flag at the inventory item-level. May define it at component level and propagate to inventory-item. May have a separate "function" at the component level. May have an expanded, formatted function description in the remarks.

		Guidance	Valid Values	Requirement	Component	Inventory -Item	OSCAL Cardinality	Data Location: XPath Notation (CASE SENSITIVE)	NOTES
Any Inventory	Comments	Any additional information that could be useful to the reviewer.		Optional for OS/Infrastructure, Software and Database.	X	X	0 or 1	/*/system-implementation/component/remarks /*/system-implementation/system-inventory/inventory-item/remarks	May have comments in either the component level, inventory-item level, or both.
	Serial #/Asset Tag#	Product serial number or internal asset tag #.		Optional for OS/Infrastructure, Software, and Database.		X	0 or 1	/*/system-implementation/system-inventory/inventory-item/prop[@name="serial-number"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="asset-tag"]/@value	
	VLAN/ Network ID	Virtual LAN or Network ID.		Optional for OS/Infrastructure, Software, and Database.		X	0 - ∞	/*/system-implementation/system-inventory/inventory-item/prop[@name="vlan-id"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="network-id"]/@value	
	System Administrator/ Owner	Name of the system administrator or owner.		Mandatory for HIGH impact systems. Optional for Low and Moderate impact systems.	X	X	0 - ∞	COMPONENT OWNER (Person): /*/metadata/party[@uuid=/*/system-implementation/component/responsible-role[@role-id="asset-owner"]/party-uuid]/name COMPONENT ADMINISTRATOR (Org): /*/metadata/party[@uuid=/*/system-implementation/component/responsible-role[@role-id="asset-administrator"]/party-uuid]/name INVENTORY ITEM OWNER (Person): /*/metadata/party[@uuid=/*/system-implementation/system-inventory/inventory-item/responsible-party[@role-id="asset-owner"]/party-uuid]/name INVENTORY ITEM ADMINISTRATOR (Org): /*/metadata/party[@uuid=/*/system-implementation/system-inventory/inventory-item/responsible-party[@role-id="asset-administrator"]/party-uuid]/name	Must have "System Owner/Administrator" at the inventory item-level. May define it at component level and propagate to inventory-item. May have a separate "system owner/administrator" at the component level.
	Application Administrator/ Owner	Name of the application administrator or owner.		Optional for OS/Infrastructure, Software, and Database.	X	X	0 - ∞	COMPONENT OWNER: /*/metadata/party[@uuid=/*/system-implementation/component/responsible-role[@role-id="asset-owner"]/party-uuid]/name CMPONENT ADMINISTRATOR: /*/metadata/party[@uuid=/*/system-implementation/component/responsible-role[@role-id="asset-administrator"]/party-uuid]/name INVENTORY ITEM OWNER: /*/metadata/party[@id=/*/system-implementation/system-inventory/inventory-item/responsible-party[@role-id="asset-owner"]/party-id]/person/person-name INVENTORY ITEM ADMINISTRATOR: /*/metadata/party[@uuid=/*/system-implementation/system-inventory/inventory-item/responsible-party[@role-id="asset-administrator"]/party-uuid]/name	Must have "Application Owner/Administrator" at the inventory item-level. May define it at component level and propagate to inventory-item. May have a separate "system owner/administrator" at the component level.
ADDITIONAL	Scan Type	Indicate which scan type(s) the item is subjected to.	infrastructure, database, web	Mandatory	X	X	1 - ∞	/*/system-implementation/component/prop[@name="scan-type"][@ns="https://fedramp.gov/ns/oscal"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="scan-type"][@ns="https://fedramp.gov/ns/oscal"]/@value	Valid values: infrastructure, web, database. If more than one type is applicable, use one field per type.
	FIPS 140-2 Validation	Indicate the certificate information for an inventory item with a FIPS 140-2 validated cryptographic module.	component-id	Mandatory for any item involving cryptography. Omit otherwise.	X	X	1w - ∞	/*/system-implementation/component/prop[@name="validation"][@ns="https://fedramp.gov/ns/oscal"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="validation"][@ns="https://fedramp.gov/ns/oscal"]/@value	If an item has more than one cryptographic module, use one entry per validation certificate. May define "FIPS 140-2 validation" at the component level and propagate to the inventory-item level.