

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: April 21, 2018

K. Grizzle, Ed.  
SailPoint  
B. Yoder  
Thycotic  
J. Jones  
Bomgar  
P. Lieberman  
Lieberman  
E. Nunez  
Cyberark  
October 18, 2017

**SCIM Extension for Privileged Access Management**  
**draft-grizzle-scim-pam-ext-01**

## Abstract

The System for Cross-domain Identity Management (SCIM) specification [[RFC7643](#)] provides schemas that represent common identity information about users and groups. Privileged Access Management (PAM) software typically makes use of common user and group models - as well as defining additional constructs - to provide fine-grained authorization and management for privileged access.

This document contains a SCIM 2.0 extension for Privileged Access Management, which includes extensions to the core User and Group objects, and new resource types and schemas for standard Privileged Access Management constructs. This extension is intended to provide greater interoperability between PAM software and clients, a common language for PAM concepts, and a baseline that can be further extended to support more complex PAM requirements.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 21, 2018.

## Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

|  |    |
|--|----|
| <a href="#">1. Overview</a>                                | 3  |
| <a href="#">1.1. Definitions</a>                           | 3  |
| <a href="#">1.2. Requirements Notation and Conventions</a> | 4  |
| <a href="#">2. Core Schema Extensions</a>                  | 4  |
| <a href="#">2.1. Linked Object</a>                         | 4  |
| <a href="#">2.1.1. Example</a>                             | 5  |
| <a href="#">2.1.2. Considerations for External Groups</a>  | 6  |
| <a href="#">3. Additional ResourceTypes and Schemas</a>    | 6  |
| <a href="#">3.1. Container</a>                             | 7  |
| <a href="#">3.1.1. Resource Type</a>                       | 7  |
| <a href="#">3.1.2. Schema</a>                              | 7  |
| <a href="#">3.1.3. Example</a>                             | 8  |
| <a href="#">3.2. PrivilegedData</a>                        | 9  |
| <a href="#">3.2.1. Resource Type</a>                       | 10 |
| <a href="#">3.2.2. Schema</a>                              | 10 |
| <a href="#">3.2.3. Example</a>                             | 10 |
| <a href="#">3.3. ContainerPermission</a>                   | 11 |
| <a href="#">3.3.1. Resource Type</a>                       | 11 |
| <a href="#">3.3.2. Schema</a>                              | 11 |
| <a href="#">3.3.3. Example</a>                             | 12 |
| <a href="#">3.4. PrivilegedDataPermission</a>              | 13 |
| <a href="#">3.4.1. Resource Type</a>                       | 13 |
| <a href="#">3.4.2. Schema</a>                              | 14 |
| <a href="#">3.4.3. Example</a>                             | 15 |
| <a href="#">4. Schema JSON Representations</a>             | 16 |
| <a href="#">5. Normative References</a>                    | 29 |
| <a href="#">Authors' Addresses</a>                         | 30 |

Grizzle, et al.

Expires April 21, 2018

[Page 2]

## 1. Overview

Most Privileged Access Management (PAM) software contains external APIs that can be used to manage users, groups, privileged access, and authorization to privileged data. However, these APIs are not consistent across different software (e.g. - some software uses REST and some uses SOAP), and each API exposes different functionality. This makes it difficult for a client to externally manage multiple PAM providers.

The System for Cross-domain Identity Management (SCIM) specification provides schemas that represent common identity information about users and groups. Privileged Access Management (PAM) software typically makes use of common user and group models - as well as defining additional constructs - to provide fine-grained authorization and management for privileged access.

This document contains a SCIM 2.0 extension for Privileged Access Management, which includes extensions to the core User and Group objects, and new resource types and schemas for standard Privileged Access Management constructs. This extension is intended to provide greater interoperability between PAM software and clients, a common language for PAM concepts, and a baseline that can be further extended to support more complex PAM requirements.

Some providers MAY not support all of the endpoints or data that is described in this extension. When this is encountered, the PAM provider can safely treat endpoints or data as optional.

### 1.1. Definitions

**User:** A user account that can be used to access the PAM system to manage or access privileged data. This user can either exist only in the PAM system or can be an external user that is defined in another system (e.g. - Active Directory or LDAP).

**Group:** A group of users or other groups that can be used to govern access within the PAM system. This group can either exist only in the PAM system or can be an external group that is defined in another system (e.g. - Active Directory or LDAP).

**Container:** A Container is a logical grouping of privileged data (credentials, etc...) that can be used for organizational or operational purposes. Access control lists (ACLs) can be applied to a container to control which users and groups have permissions to the privileged data in the container.

Grizzle, et al.

Expires April 21, 2018

[Page 3]

**Privileged Data:** Privileged data is secret information that is protected by the PAM system (e.g. - credentials for a privileged account, an SSH key, etc...). Privileged data MAY be stored inside of a Container, but does not have to be. Access control lists (ACLs) can be applied to privileged data to control which users and groups have permissions to the privileged data. More often, the ACL information is inherited from the container.

**Access Control List (ACL):** An access control list can be associated with a Container or Privileged Data. This contains information about which users and groups have access to the Container or Privileged Data, and what rights they have.

**External Store:** An External Store is a system that contains users and groups (e.g. - Active Directory or LDAP) that can be used by a PAM system. This allows using existing infrastructure and group definitions to provide authorization, authentication, and information within a PAM system.

## **1.2. Requirements Notation and Conventions**

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)] .

Throughout this document, values are quoted to indicate that they are to be taken literally. When using these values in protocol messages, the quotes MUST NOT be used as part of the value.

## **2. Core Schema Extensions**

In a PAM system, users and groups can either be locally or externally defined. When local, the user or group exists only on the PAM system. When external, the user or group is defined in an External Store, and is somehow synchronized into the PAM system. In this case, the PAM system keeps a record of the external user or group, along with a reference that can be used to correlate the record back to the External Store. To support this, an optional schema extension "urn:ietf:params:scim:schemas:pam:1.0:LinkedObject" SHOULD be added to the User and Group resource types.

### **2.1. Linked Object**

The "urn:ietf:params:scim:schemas:pam:1.0:LinkedObject" schema contains the following attributes.

Grizzle, et al.

Expires April 21, 2018

[Page 4]

source The name of the External Source from which the User or Group came. If this is a local User or Group, this is null. Required if nativeIdentifier is non-null.

nativeIdentifier The unique identifier of the User or Group on the External Source (e.g. - an LDAP distinguished name). If this is a local User or Group, this is null. Required if source is non-null.

### 2.1.1. Example

The following is a non-normative example of a User with the LinkedObject extension.

```
{  
  "schemas": [  
    "urn:ietf:params:scim:schemas:core:2.0:User",  
    "urn:ietf:params:scim:schemas:pam:1.0:LinkedObject"  
,  
  "id": "2819c223-7f76-453a-919d-413861904646",  
  "userName": "bjensen",  
  "name": {  
    "formatted": "Ms. Barbara J Jensen, III",  
    "givenName": "Barbara",  
    "familyName": "Jensen",  
    "middleName": "Jane",  
    "honorificPrefix": "Ms.",  
    "honorificSuffix": "III"  
  },  
  "displayName": "Babs Jensen",  
  "emails": [  
    {  
      "value": "bjensen@example.com",  
      "type": "work",  
      "primary": true  
    },  
    {  
      "value": "babs@jensen.org",  
      "type": "home"  
    }  
,  
  "active": true,  
  "groups": [  
    {  
      "value": "e9e30dba-f08f-4109-8486-d5c6a331660a",  
      "$ref": "https://example.com/v2/Groups/e9e30dba-f08f-4109-8486-  
d5c6a331660a",  
      "display": "Tour Guides",  
    }  
  ]  
}
```

"type": "direct"

Grizzle, et al.

Expires April 21, 2018

[Page 5]

```
},
{
  "value": "fc348aa8-3835-40eb-a20b-c726e15c55b5",
  "$ref": "https://example.com/v2/Groups/fc348aa8-3835-40eb-a20b-
c726e15c55b5",
  "display": "Employees",
  "type": "indirect"
}
],
"urn:ietf:params:scim:schemas:pam:1.0:LinkedObject": {
  "source": "Corporate Active Directory",
  "nativeIdentifier": "cn=Barbara Jensen,ou=Users,dc=example,dc=com"
},
"meta": {
  "resourceType": "User",
  "created": "2010-01-23 04:56:22 UTC",
  "lastModified": "2011-05-13 04:42:34 UTC",
  "location": "https://example.com/v2/Users/
2819c223-7f76-453a-919d-413861904646"
}
}
```

### 2.1.2. Considerations for External Groups

Members of external groups are stored and managed on the External Store, and not in the PAM system. As a result, the User and Group representations returned by the PAM system MAY return empty values for the "groups" and "members" attributes, respectively.

Additionally, the PAM system MAY choose to return an error response with the 400 status code and "invalidSyntax" error type for requests that attempt to modify or create a group with an invalid configuration. Examples include, but are not limited to:

- o An external group with any members.
- o An external group with local Users or Groups as members.
- o A local group with external Users or Groups as members.

### 3. Additional ResourceTypes and Schemas

PAM systems define additional constructs to provide enhanced authorization, authentication, and management for privileged data. To support this, the SCIM PAM extension defines additional ResourceTypes and Schemas that MAY be implemented by the service provider. If implemented, these ResourceTypes SHOULD support all SCIM operations [[RFC7644](#)]. All attributes defined in the schemas are optional unless explicitly marked as REQUIRED.

Grizzle, et al.

Expires April 21, 2018

[Page 6]

### [\*\*3.1. Container\*\*](#)

A Container is a logical grouping of privileged data that can be used for organizational or operational purposes.

#### [\*\*3.1.1. Resource Type\*\*](#)

The Container ResourceType supports reading and managing containers, and has the following properties.

Name: Container

Endpoint: /Containers

Schema: urn:ietf:params:scim:schemas:pam:1.0:Container

##### [\*\*3.1.1.1. Filtering\*\*](#)

Clients MAY have a reference to the Container name but not the ID. For this reason, it is RECOMMENDED that service providers implement filtering that allows equality matching on the "name" attribute. Example (note that escaping has been removed for readability):

```
GET /scim/v2/Containers?filter=name eq 'Admin Accounts'
```

#### [\*\*3.1.2. Schema\*\*](#)

The "urn:ietf:params:scim:schemas:pam:1.0:Container" defines all common attributes for a Container.

id The unique identifier of the Container. REQUIRED

name The name of the Container. REQUIRED

displayName The display name of the Container. OPTIONAL. If displayName is unassigned, the name MAY be used as the display name.

description The description of the Container. OPTIONAL

type The type of container. There are no canonical values defined for type, but service providers MAY choose to define the valid types. OPTIONAL if the PAM system does not support multiple types of Containers.

parent A complex attribute that defines the parent Container of this Container if the service provider supports hierarchies of containers. The following sub-attributes are defined.



value The ID of the Container that is the parent of this Container in the hierarchy.

\$ref A URI reference to the Container that is the parent of this Container in the hierarchy.

display The display name of the Container that is the parent of this Container in the hierarchy.

owner A complex attribute that defines the User that is the owner of this Container. OPTIONAL. The following sub-attributes are defined.

value The ID of the User that owns this Container.

\$ref A URI reference to the User that owns this Container.

display The display name of the user that owns this Container.

privilegedData A multi-valued complex attribute that contains the PrivilegedData that resides in this Container. Service providers MAY choose to make this attribute have a "returned" value of "request" if the list of privileged data could be very large. Using this option will prevent this attribute from being returned upon retrieval unless explicitly requested using the "attributes" query parameter. The following sub-attributes are defined.

value The ID of the PrivilegedData.

\$ref A URI reference to the PrivilegedData.

display The displayable value of the PrivilegedData.

type The type of the PrivilegedData.

### 3.1.3. Example

The following is a non-normative example of a Container.



```
{  
  "schemas": [  
    "urn:ietf:params:scim:schemas:pam:1.0:Container"  
,  
  "id": "ab8e901-883f-4109-8486-bab810943d93e",  
  "name": "prodDBAAccounts",  
  "displayName": "Production DBA Accounts",  
  "description": "This contains all DBA accounts for the production  
environment.",  
  "type": "safe",  
  "parent": {  
    "value": "78234914-7fb3-828e-7281-87234abe8300",  
    "$ref": "https://example.com/v2/Containers/  
78234914-7fb3-828e-7281-87234abe8300",  
    "display": "Root Container"  
  },  
  "owner": {  
    "value": "2819c223-7f76-453a-919d-413861904646",  
    "$ref": "https://example.com/v2/Users/  
2819c223-7f76-453a-919d-413861904646",  
    "display": "Babs Jensen"  
  },  
  "privilegedData": [  
    {  
      "value": "d973b5-8834f-1784-8734-caf833e9b3efa",  
      "$ref": "https://example.com/v2/PrivilegedData/d973b5-8834f-1784-8734-  
caf833e9b3efa",  
      "display": "root @ Oracle Financials Warehouse",  
      "type": "credential"  
    },  
    {  
      "value": "d249e9-92759-7883-88723-fa390734beba",  
      "$ref": "https://example.com/v2/PrivilegedData/d249e9-92759-7883-88723-  
fa390734beba",  
      "display": "root @ Enterprise Purchase Ordering",  
      "type": "credential"  
    }  
,  
  "meta": {  
    "resourceType": "Container",  
    "created": "2010-01-23T04:56:22.000Z",  
    "lastModified": "2011-05-13T04:42:34.000Z",  
    "location": "https://example.com/v2/Container/ab8e901-883f-4109-8486-  
bab810943d93e"  
  }  
}
```

### 3.2. PrivilegedData

Privileged data is secret information that is protected by the PAM system (e.g. - credentials for a privileged account, an SSH key, etc...). Privileged data MAY be stored inside of a Container, but does not have to be.

### 3.2.1. Resource Type

The PrivilegedData ResourceType supports reading and managing privileged data, and has the following properties.

Name: PrivilegedData

Endpoint: /PrivilegedData

Schema: urn:ietf:params:scim:schemas:pam:1.0:PrivilegedData

### 3.2.2. Schema

The "urn:ietf:params:scim:schemas:pam:1.0:PrivilegedData" defines all common attributes for a PrivilegedData.

id The unique identifier of the PrivilegedData. REQUIRED

name A descriptive name for this piece of PrivilegedData. For example, root@mylinuxhost. REQUIRED

description A description for this piece of PrivilegedData.

type The type of PrivilegedData. The value will be dependent on what is supported by the PAM system. Examples include 'credential', 'ssh key', 'file', etc... OPTIONAL.

### 3.2.3. Example

The following is a non-normative example of a PrivilegedData.

```
{  
  "schemas": [  
    "urn:ietf:params:scim:schemas:pam:1.0:PrivilegedData"  
,  
    "id": "d973b5-8834f-1784-8734-caf833e9b3efa",  
    "name": "root @ Oracle Financials Warehouse",  
    "description": "Full access to the Oracle Financials Warehouse database.",  
    "type": "credential",  
    "meta": {  
      "resourceType": "PrivilegedData",  
      "created": "2010-01-23T04:56:22.000Z",  
      "lastModified": "2011-05-13T04:42:34.000Z",  
      "location": "https://example.com/v2/PrivilegedData/d973b5-8834f-1784-8734-  
      caf833e9b3efa"  
    }  
}
```

Grizzle, et al.

Expires April 21, 2018

[Page 10]

### [\*\*3.3. ContainerPermission\*\*](#)

A ContainerPermission contains authorization information that describes which rights a User or Group has on a Container. This is a piece of an Access Control List that contains all information about a specific User or Group in relation to a specific Container. Typically, permissions that are granted on a Container apply to all privileged data that resides in the container.

#### [\*\*3.3.1. Resource Type\*\*](#)

The ContainerPermission ResourceType supports reading and managing permissions that a User or Group have on a Container, and has the following properties.

Name: ContainerPermission

Endpoint: /ContainerPermissions

Schema: urn:ietf:params:scim:schemas:pam:1.0:ContainerPermission

##### [\*\*3.3.1.1. Filtering\*\*](#)

It is expected that clients will need to find the all permissions on a specific Container, permissions that are granted to a specific User or Group, or permissions for a specific user or group on a specific container. For this reason, it is RECOMMENDED that service providers implement filtering that allows equality matching on the "container.value", "user.value", and "group.value" attributes. Example (note that escaping has been removed and newlines added for readability):

```
GET /scim/v2/ContainerPermissions?  
    filter=container.value eq '8729e778-9af6-874c-778a3-783956810384'  
  
GET /scim/v2/ContainerPermissions?  
    filter=user.value eq '2819c223-7f76-453a-919d-413861904646'  
  
GET /scim/v2/ContainerPermissions?  
    filter=container.value eq '8729e778-9af6-874c-778a3-783956810384' and  
        user.value eq '2819c223-7f76-453a-919d-413861904646'
```

#### [\*\*3.3.2. Schema\*\*](#)

The "urn:ietf:params:scim:schemas:pam:1.0:ContainerPermission" defines all common attributes for a ContainerPermission.

**id** The unique identifier of the ContainerPermission. REQUIRED

Grizzle, et al.

Expires April 21, 2018

[Page 11]

container A complex attribute that references the Container that these permissions apply to. The following sub-attributes are defined. REQUIRED

value The ID of the Container that these permissions apply to.

\$ref A URI reference to the Container that these permissions apply to.

name The name of the Container that these permissions apply to.

display The display name of the Container that these permissions apply to.

user A complex attribute that references the User that these permissions apply to. Either this attribute or "group" is required. The following sub-attributes are defined.

value The ID of the User that these permissions apply to.

\$ref A URI reference to the User that these permissions apply to.

display The display name of the User that these permissions apply to.

group A complex attribute that references the Group that these permissions apply to. Either this attribute or "user" is required. The following sub-attributes are defined.

value The ID of the Group that these permissions apply to.

\$ref A URI reference to the Group that these permissions apply to.

display The display name of the Group that these permissions apply to.

rights An array of strings that are the names of the rights that the User or Group has on this Container. There are no canonical values defined for rights, and these will vary between service providers.

### **3.3.3. Example**

The following is a non-normative example of a ContainerPermission.



```
{  
  "schemas": [  
    "urn:ietf:params:scim:schemas:pam:1.0:ContainerPermission"  
,  
  "id": "c387432-78823-87234-7832-93c9ae93745e",  
  "container": {  
    "value": "ab8e901-883f-4109-8486-bab810943d93e",  
    "$ref": "https://example.com/v2/Containers/ab8e901-883f-4109-8486-  
bab810943d93e",  
    "display": "Production DBA Accounts",  
    "name": "prodDBAAccounts"  
  },  
  "user": {  
    "value": "2819c223-7f76-453a-919d-413861904646",  
    "$ref": "https://example.com/v2/Users/  
2819c223-7f76-453a-919d-413861904646",  
    "display": "Babs Jensen"  
  },  
  "rights": [  
    "Connect",  
    "List Accounts",  
    "View Password"  
  ],  
  "meta": {  
    "resourceType": "ContainerPermission",  
    "created": "2010-01-23T04:56:22.000Z",  
    "lastModified": "2011-05-13T04:42:34.000Z",  
    "location": "https://example.com/v2/ContainerPermissions/  
c387432-78823-87234-7832-93c9ae93745e"  
  }  
}
```

### [3.4. PrivilegedDataPermission](#)

A `PrivilegedDataPermission` contains authorization information that describes which rights a User or Group has on a `PrivilegedData`. This is a piece of an Access Control List that contains all information about a specific User or Group in relation to a specific piece of privileged data. This resource MUST only return permissions that are granted directly to the `PrivilegedData`. Permissions that are inherited from a Container on the `PrivilegedData` MUST NOT be returned. This resource type and schema are OPTIONAL if the service provider does not support permissions on privileged data.

#### [3.4.1. Resource Type](#)

The `PrivilegedDataPermission` ResourceType supports reading and

managing permissions that a User or Group have on a PrivilegedData, and has the following properties.

Name: PrivilegedDataPermission

Endpoint: /PrivilegedDataPermissions

Schema: urn:ietf:params:scim:schemas:pam:1.0:PrivilegedDataPermission

### [\*\*3.4.1.1. Filtering\*\*](#)

It is expected that clients will need to find the all permissions on a specific PrivilegedData, permissions that are granted to a specific User or Group, or permissions for a specific user or group on a specific privileged data item. For this reason, it is RECOMMENDED that service providers implement filtering that allows equality matching on the "privilegedData.value", "user.value", and "group.value" attributes. Example (note that escaping has been removed and newlines added for readability):

```
GET /scim/v2/PrivilegedDataPermissions?  
    filter=privilegedData.value eq '2746c134-59e8-848a-874d3-782303476812'  
  
GET /scim/v2/PrivilegedDataPermissions?  
    filter=user.value eq '2819c223-7f76-453a-919d-413861904646'  
  
GET /scim/v2/PrivilegedDataPermissions?  
    filter=privilegedData.value eq '2746c134-59e8-848a-874d3-782303476812'  
and  
    user.value eq '2819c223-7f76-453a-919d-413861904646'
```

### [\*\*3.4.2. Schema\*\*](#)

The "urn:ietf:params:scim:schemas:pam:1.0:PrivilegedDataPermission" defines all common attributes for a PrivilegedDataPermission.

**id** The unique identifier of the PrivilegedDataPermission. REQUIRED

**privilegedData** A complex attribute that references the PrivilegedData that these permissions apply to. The following sub-attributes are defined. REQUIRED

**value** The ID of the PrivilegedData that these permissions apply to.

**\$ref** A URI reference to the PrivilegedData that these permissions apply to.

**display** The display name of the PrivilegedData that these permissions apply to.

Grizzle, et al.

Expires April 21, 2018

[Page 14]

user A complex attribute that references the User that these permissions apply to. Either this attribute or "group" is required. The following sub-attributes are defined.

value The ID of the User that these permissions apply to.

\$ref A URI reference to the User that these permissions apply to.

display The display name of the User that these permissions apply to.

group A complex attribute that references the Group that these permissions apply to. Either this attribute or "user" is required. The following sub-attributes are defined.

value The ID of the Group that these permissions apply to.

\$ref A URI reference to the Group that these permissions apply to.

display The display name of the Group that these permissions apply to.

rights An array of strings that are the names of the rights that the User or Group has on this PrivilegedData. There are no canonical values defined for rights, and these will vary between service providers.

### 3.4.3. Example

The following is a non-normative example of a PrivilegedDataPermission.



```
{
  "schemas": [
    "urn:ietf:params:scim:schemas:pam:1.0:PrivilegedDataPermission"
  ],
  "id": "f823414-872344-77381-ab93489d83ea87",
  "privilegedData": {
    "value": "d973b5-8834f-1784-8734-caf833e9b3efa",
    "$ref": "https://example.com/v2/PrivilegedData/d973b5-8834f-1784-8734-
caf833e9b3efa",
    "display": "root @ Oracle Financials Warehouse"
  },
  "group": {
    "value": "e9e30dba-f08f-4109-8486-d5c6a331660a",
    "$ref": "https://example.com/v2/Groups/e9e30dba-f08f-4109-8486-
d5c6a331660a",
    "display": "Tour Guides"
  },
  "rights": [
    "Connect",
    "View Password"
  ],
  "meta": {
    "resourceType": "PrivilegedDataPermission",
    "created": "2010-01-23T04:56:22.000Z",
    "lastModified": "2011-05-13T04:42:34.000Z",
    "location": "https://example.com/v2/PrivilegedDataPermissions/
f823414-872344-77381-ab93489d83ea87"
  }
}
```

#### **4. Schema JSON Representations**

The following section provide representations of schemas for the schema extensions and new schemas introduced in this document.

```
{
  "id": "urn:ietf:params:scim:schemas:pam:1.0:LinkedObject",
  "name": "Linked Object",
  "description": "A LinkedObject contains information about the source that an object came from. For example, a User or Group that comes from an external AD.",
  "attributes": [
    {
      "name": "source",
      "type": "string",
      "multiValued": false,
      "description": "The name of the external application on which the object"
    }
  ]
}
```

lives.

```
If this is a PAM local object, this is null.",  
"required":false,  
"caseExact":false,  
"mutability":"readWrite",
```

```
        "returned":"default",
        "uniqueness":"none"
    },
    {
        "name":"nativeIdentifier",
        "type":"string",
        "multiValued":false,
        "description":"The native identifier of the object on the external
application
            (eg - the LDAP DN). If this is a PAM local object, this is null.",
        "required":false,
        "caseExact":false,
        "mutability":"readWrite",
        "returned":"default",
        "uniqueness":"none"
    }
],
},
{
    "id":"urn:ietf:params:scim:schemas:pam:1.0:Container",
    "name":"Container",
    "description":"A Container is a logical grouping of privileged data
(credentials,
    etc...) that can be used for organizational or operational purposes.",
    "attributes":[
        {
            "name":"id",
            "type":"string",
            "multiValued":false,
            "description":"The unique identifier of the Container",
            "required":false,
            "caseExact":true,
            "mutability":"readOnly",
            "returned":"always",
            "uniqueness":"server"
        },
        {
            "name":"name",
            "type":"string",
            "multiValued":false,
            "description":"The name of the container.",
            "required":true,
            "caseExact":false,
            "mutability":"readWrite",
            "returned":"default",
            "uniqueness":"server"
        },
        {

```

```
"name":"displayName",  
"type":"string",
```

```
  "multiValued":false,
  "description":"The display name of the container. This is optional. If
null,
    the name will be used as the display name.",
  "required":false,
  "caseExact":false,
  "mutability":"readWrite",
  "returned":"default",
  "uniqueness":"none"
},
{
  "name":"description",
  "type":"string",
  "multiValued":false,
  "description":"The description of the container.",
  "required":false,
  "caseExact":false,
  "mutability":"readWrite",
  "returned":"default",
  "uniqueness":"none"
},
{
  "name":"type",
  "type":"string",
  "multiValued":false,
  "description":"The type of container (eg - management set or account
store).
  This is optional if the PAM system does not support multiple types of
  containers.",
  "required":false,
  "caseExact":false,
  "mutability":"readWrite",
  "returned":"default",
  "uniqueness":"none"
},
{
  "name":"owner",
  "type":"complex",
  "multiValued":false,
  "description":"The user that owns this container.",
  "mutability":"readWrite",
  "required":false,
  "returned":"default",
  "uniqueness":"none",
  "subAttributes":[
    {
      "name":"value",
      "type":"string",

```

```
"multiValued":false,  
"description":"The ID of the user that owns this container",
```

```
        "required":false,
        "caseExact":false,
        "mutability":"readWrite",
        "returned":"default",
        "uniqueness":"none"
    },
{
    "name":'$ref',
    "type":"reference",
    "referenceTypes":[
        "User"
    ],
    "multiValued":false,
    "description":"A URI reference to the user that owns this
container.",
    "required":false,
    "caseExact":false,
    "mutability":"readWrite",
    "returned":"default",
    "uniqueness":"none"
},
{
    "name":"display",
    "type":"string",
    "multiValued":false,
    "description":"The display name of the user that owns this
container",
    "required":false,
    "caseExact":false,
    "mutability":"readOnly",
    "returned":"default",
    "uniqueness":"none"
}
],
},
{
    "name":"privilegedData",
    "type":"complex",
    "multiValued":true,
    "description":"The privileged data that resides in this container.",
    "required":false,
    "mutability":"readWrite",
    "returned":"default",
    "uniqueness":"none",
    "subAttributes":[
        {
            "name":"value",
            "type":"string",

```

```
"multiValued":false,  
"description":"The ID of the privileged data.",
```

```
        "required":false,
        "caseExact":false,
        "mutability":"readWrite",
        "returned":"default",
        "uniqueness":"none"
    },
{
    "name":"$ref",
    "type":"reference",
    "referenceTypes":[
        "User"
    ],
    "multiValued":false,
    "description":"A URI reference to the PrivilegedData",
    "required":false,
    "caseExact":false,
    "mutability":"readWrite",
    "returned":"default",
    "uniqueness":"none"
},
{
    "name":"display",
    "type":"string",
    "multiValued":false,
    "description":"The displayable value of the PrivilegedData",
    "required":false,
    "caseExact":false,
    "mutability":"readOnly",
    "returned":"default",
    "uniqueness":"none"
},
{
    "name":"type",
    "type":"string",
    "multiValued":false,
    "description":"The type of the PrivilegedData.",
    "required":false,
    "caseExact":false,
    "mutability":"readOnly",
    "returned":"default",
    "uniqueness":"none"
}
]
}
],
{
    "id":"urn:ietf:params:scim:schemas:pam:1.0:PrivilegedData",
```

Grizzle, et al.

Expires April 21, 2018

[Page 20]

```
"name":"Privileged Data",
"description":"Privileged data is secret information that is protected by the
PAM
    system (eg - a credential, an SSH key, etc...). Privileged data MAY be
stored
    inside of a Container, but does not have to be.",
"attributes": [
    {
        "name":"id",
        "type":"string",
        "multiValued":false,
        "description":"The unique identifier of the PrivilegedData.",
        "required":false,
        "caseExact":true,
        "mutability":"readOnly",
        "returned":"always",
        "uniqueness":"server"
    },
    {
        "name":"name",
        "type":"string",
        "multiValued":false,
        "description":"A descriptive name for this piece of PrivilegedData.
            For example, root@mylinuxhost",
        "required":true,
        "caseExact":false,
        "mutability":"readWrite",
        "returned":"default",
        "uniqueness":"none"
    },
    {
        "name":"description",
        "type":"string",
        "multiValued":false,
        "description":"A description for this piece of PrivilegedData.",
        "required":false,
        "caseExact":false,
        "mutability":"readWrite",
        "returned":"default",
        "uniqueness":"none"
    },
    {
        "name":"type",
        "type":"string",
        "multiValued":false,
        "description":"The type of PrivilegedData. The value will be dependent
on what
            is supported by the PAM system. Examples include 'credential', 'ssh'
```

```
key',  
      'file', etc...",  
    "required":false,  
    "caseExact":false,
```

Grizzle, et al.

Expires April 21, 2018

[Page 21]

```
        "mutability": "readWrite",
        "returned": "default",
        "uniqueness": "none"
    },
]
},
{
  "id": "urn:ietf:params:scim:schemas:pam:1.0:ContainerPermission",
  "name": "Container Permission",
  "description": "ACL information that is attached to a container.",
  "attributes": [
    {
      "name": "id",
      "type": "string",
      "multiValued": false,
      "description": "The unique identifier of the ContainerPermission.",
      "required": false,
      "caseExact": true,
      "mutability": "readOnly",
      "returned": "always",
      "uniqueness": "server"
    },
    {
      "name": "container",
      "type": "complex",
      "multiValued": false,
      "description": "The container that these permissions apply to. REQUIRED",
      "required": true,
      "mutability": "readWrite",
      "returned": "default",
      "uniqueness": "none",
      "subAttributes": [
        {
          "name": "value",
          "type": "string",
          "multiValued": false,
          "description": "The ID of the container that these permissions apply
to.",
          "required": true,
          "caseExact": false,
          "mutability": "readWrite",
          "returned": "default",
          "uniqueness": "none"
        },
        {
          "name": "$ref",
          "type": "reference",
          "referenceTypes": [
            "Container"
          ]
        }
      ]
    }
  ]
}
```

"Container"

Grizzle, et al.

Expires April 21, 2018

[Page 22]

```
],
  "multiValued":false,
  "description":"A URI reference to the container that these
permissions apply to.",
  "required":true,
  "caseExact":false,
  "mutability":"readWrite",
  "returned":"default",
  "uniqueness":"none"
},
{
  "name":"display",
  "type":"string",
  "multiValued":false,
  "description":"The display name of the container",
  "required":false,
  "caseExact":false,
  "mutability":"readOnly",
  "returned":"default",
  "uniqueness":"none"
},
{
  "name":"name",
  "type":"string",
  "multiValued":false,
  "description":"The name of the container",
  "required":false,
  "caseExact":false,
  "mutability":"readOnly",
  "returned":"default",
  "uniqueness":"none"
}
],
},
{
  "name":"user",
  "type":"complex",
  "multiValued":false,
  "description":"The User that these permissions apply to. Either this or
group
  is required.",
  "required":false,
  "mutability":"readWrite",
  "returned":"default",
  "uniqueness":"none",
  "subAttributes":[
    {
      "name":"value",
```

"type":"string",  
"multiValued":false,

Grizzle, et al.

Expires April 21, 2018

[Page 23]

```
        "description": "The ID of the user that these permissions apply to.",
        "required": false,
        "caseExact": false,
        "mutability": "readWrite",
        "returned": "default",
        "uniqueness": "none"
    },
    {
        "name": "$ref",
        "type": "reference",
        "referenceTypes": [
            "User"
        ],
        "multiValued": false,
        "description": "A URI reference to the user that these permissions
apply to.",
        "required": false,
        "caseExact": false,
        "mutability": "readWrite",
        "returned": "default",
        "uniqueness": "none"
    },
    {
        "name": "display",
        "type": "string",
        "multiValued": false,
        "description": "The display name of the user",
        "required": false,
        "caseExact": false,
        "mutability": "readOnly",
        "returned": "default",
        "uniqueness": "none"
    }
]
},
{
    "name": "group",
    "type": "complex",
    "multiValued": false,
    "description": "The Group that these permissions apply to. Either this or
user
        is required.",
    "required": false,
    "mutability": "readWrite",
    "returned": "default",
    "uniqueness": "none",
    "subAttributes": [
        {
            "name": "id",
            "type": "string",
            "multiValued": false,
            "description": "The ID of the group that these permissions apply to."}
```

"name":"value",  
"type":"string",

Grizzle, et al.

Expires April 21, 2018

[Page 24]

```
        "multiValued":false,
        "description":"The ID of the group that these permissions apply to.",
        "required":false,
        "caseExact":false,
        "mutability":"readWrite",
        "returned":"default",
        "uniqueness":"none"
    },
    {
        "name": "$ref",
        "type": "reference",
        "referenceTypes":[
            "Group"
        ],
        "multiValued":false,
        "description": "A URI reference to the group that these permissions
apply to.",
        "required":false,
        "caseExact":false,
        "mutability":"readWrite",
        "returned":"default",
        "uniqueness":"none"
    },
    {
        "name": "display",
        "type": "string",
        "multiValued":false,
        "description": "The display name of the group",
        "required":false,
        "caseExact":false,
        "mutability":"readOnly",
        "returned":"default",
        "uniqueness":"none"
    }
]
},
{
    "name": "rights",
    "type": "string",
    "multiValued":true,
    "description": "The rights that the user or group has on this container.",
    "required":true,
    "caseExact":false,
    "mutability":"readWrite",
    "returned":"default",
    "uniqueness":"none"
}
]
```

,

Grizzle, et al.

Expires April 21, 2018

[Page 25]

```
{  
  "id": "urn:ietf:params:scim:schemas:pam:1.0:PrivilegedDataPermission",  
  "name": "Privileged Data Permission",  
  "description": "ACL information that is attached to privileged data.",  
  "attributes": [  
    {  
      "name": "id",  
      "type": "string",  
      "multiValued": false,  
      "description": "The unique identifier of the PrivilegedDataPermission.",  
      "required": false,  
      "caseExact": true,  
      "mutability": "readOnly",  
      "returned": "always",  
      "uniqueness": "server"  
    },  
    {  
      "name": "privilegedData",  
      "type": "complex",  
      "multiValued": false,  
      "description": "The PrivilegedData that these permissions apply to.  
REQUIRED",  
      "required": true,  
      "mutability": "readWrite",  
      "returned": "default",  
      "uniqueness": "none",  
      "subAttributes": [  
        {  
          "name": "value",  
          "type": "string",  
          "multiValued": false,  
          "description": "The ID of the PrivilegedData that these permissions  
apply to.",  
          "required": true,  
          "caseExact": false,  
          "mutability": "readWrite",  
          "returned": "default",  
          "uniqueness": "none"  
        },  
        {  
          "name": "$ref",  
          "type": "reference",  
          "referenceTypes": [  
            "PrivilegedData"  
          ],  
          "multiValued": false,  
          "description": "A URI reference to the PrivilegedData that these  
permissions
```

```
    apply to.",  
"required":true,  
"caseExact":false,
```

```
        "mutability": "readWrite",
        "returned": "default",
        "uniqueness": "none"
    },
    {
        "name": "display",
        "type": "string",
        "multiValued": false,
        "description": "The display value of the PrivilegedData",
        "required": false,
        "caseExact": false,
        "mutability": "readOnly",
        "returned": "default",
        "uniqueness": "none"
    }
],
},
{
    "name": "user",
    "type": "complex",
    "multiValued": false,
    "description": "The User that these permissions apply to. Either this or
group
    is required.",
    "required": false,
    "mutability": "readWrite",
    "returned": "default",
    "uniqueness": "none",
    "subAttributes": [
        {
            "name": "value",
            "type": "string",
            "multiValued": false,
            "description": "The ID of the user that these permissions apply to.",
            "required": false,
            "caseExact": false,
            "mutability": "readWrite",
            "returned": "default",
            "uniqueness": "none"
        },
        {
            "name": "$ref",
            "type": "reference",
            "referenceTypes": [
                "User"
            ],
            "multiValued": false,
            "description": "A URI reference to the user that these permissions
```

```
apply to.",  
      "required":false,
```

Grizzle, et al.

Expires April 21, 2018

[Page 27]

```
        "caseExact":false,
        "mutability":"readWrite",
        "returned":"default",
        "uniqueness":"none"
    },
    {
        "name":"display",
        "type":"string",
        "multiValued":false,
        "description":"The display name of the user",
        "required":false,
        "caseExact":false,
        "mutability":"readOnly",
        "returned":"default",
        "uniqueness":"none"
    }
]
},
{
    "name":"group",
    "type":"complex",
    "multiValued":false,
    "description":"The Group that these permissions apply to. Either this or
user
        is required.",
    "required":false,
    "mutability":"readWrite",
    "returned":"default",
    "uniqueness":"none",
    "subAttributes":[
        {
            "name":"value",
            "type":"string",
            "multiValued":false,
            "description":"The ID of the group that these permissions apply to.",
            "required":false,
            "caseExact":false,
            "mutability":"readWrite",
            "returned":"default",
            "uniqueness":"none"
        },
        {
            "name":"$ref",
            "type":"reference",
            "referenceTypes":[
                "Group"
            ],
            "multiValued":false,
```

"description": "A URI reference to the group that these permissions apply to.",

```
        "required":false,
        "caseExact":false,
        "mutability":"readWrite",
        "returned":"default",
        "uniqueness":"none"
    },
    {
        "name":"display",
        "type":"string",
        "multiValued":false,
        "description":"The display name of the group",
        "required":false,
        "caseExact":false,
        "mutability":"readOnly",
        "returned":"default",
        "uniqueness":"none"
    }
]
},
{
    "name":"rights",
    "type":"string",
    "multiValued":true,
    "description":"The rights that the user or group has on this privileged
data.",
    "required":true,
    "caseExact":false,
    "mutability":"readWrite",
    "returned":"default",
    "uniqueness":"none"
}
]
}
```

## 5. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC7643] Hunt, P., Ed., Grizzle, K., Wahlstroem, E., and C. Mortimore, "System for Cross-domain Identity Management: Core Schema", [RFC 7643](#), DOI 10.17487/RFC7643, September 2015, <<https://www.rfc-editor.org/info/rfc7643>>.

Grizzle, et al.

Expires April 21, 2018

[Page 29]

[RFC7644] Hunt, P., Ed., Grizzle, K., Ansari, M., Wahlstroem, E., and C. Mortimore, "System for Cross-domain Identity Management: Protocol", [RFC 7644](#), DOI 10.17487/RFC7644, September 2015, <<https://www.rfc-editor.org/info/rfc7644>>.

#### Authors' Addresses

Kelly Grizzle (editor)  
SailPoint

Email: [kelly.grizzle@sailpoint.com](mailto:kelly.grizzle@sailpoint.com)

Benjamin Yoder  
Thycotic

Email: [ben.yoder@thycotic.com](mailto:ben.yoder@thycotic.com)

Jason Jones  
Bomgar

Email: [jjones@bomgar.com](mailto:jjones@bomgar.com)

Philip Lieberman  
Lieberman Software

Email: [phil@liebsoft.com](mailto:phil@liebsoft.com)

Edward Nunez  
CyberArk

Email: [Edward.Nunez@cyberark.com](mailto:Edward.Nunez@cyberark.com)

