Red Hat Identity Management Solution

Namespace Administration

by Thomas M. Berry

July 30th, 2025

Disclaimer: This document contains only vendor-specific information.

Problem Statement

Organizations with administrators dedicated to divisions, projects, locations, and/or departments need the ability to independently administer access management in Red Hat Identity Management. Providing these administrators with domain-wide administrative privileges requires trust, training, and constant awareness. Namespace administration addresses this by providing all administrative privileges within the context of object and container naming.

Terminology

**Namespace**: A prefix to an object name or the name of a container corresponding to a project, department, task, or location; namespace is applied to corresponding Role-Based Access Control. A namespace contains no periods (e.g. acme).

**SubNamespace**: Represents an object name that is prefixed with the namespace; this applies to the specific objects name (e.g. user or group) as well as object containers (e.g., automount, ID View, etc.). The namespace is separated from the subnamespace using a period (e.g. acme.dev). The subnamespace can itself be further divided with additional periods. (e.g. acme.test.software and acme.test.hardware).

Namespace Provisioning

|  |  |
| --- | --- |
| User groups  Name: acme.owner  Name: acme.admin  Hostgroup  Name: acme  automember host group rule  Name: acme  userclass: ^acme$  enrolledby: ^uid=acme-hostenroll,  Host-Based Access Control Rule:  Name: acme.admin  user group: acme.admin  hostgroup: acme  Sudo Rule:  Name: acme.admin  User group: acme.admin  Hostgroup: acme  ID View  Name: acme  automount  Name: acme | Role-Based Access Control: Role, Privilege, and Permissions  Role: Namespace Administrator   * Designates the specific purpose * Associates the users designated as namespace administrators   Privilege: Namespace Administration   * Association between the Role and its permissions   Permissions:   * Automount Manage Namespace * Automount Manage SubNamespace * Group IPAUsers Modify * Groups Manage Namespace * Groups Manage SubNamespace * HBAC Rule Manage * Host Manage * Hostgroups Manage SubNamespace * ID Override Manage Namespace * ID Override Manage SubNamespace * ID View Manage Namespace * ID View Manage SubNamespace * Netgroups Manage * NONPERSON Users Manage * Service Manage * Sudo Rule Manage * Sudo Commands Group Manage |

Example values applied to Role-Based Access Control

|  |  |
| --- | --- |
| Domain | idm.example.com |
| Search Base | dc=idm,dc=example,dc=com |
| Namespace | acme |
| SubNamespace | acme.\* |
| Permission Title Prefix | ACME |

User Assertions:

* Person user authentication
  + Allowed:
    - RADIUS (two-factor)
    - PKINIT
    - Smartcard derived SSH Key
  + Restricted:
    - No Password
    - No Keytab
    - No SSH Key other than those derived from smartcard
* Nonperson user authentication
  + Password: must be 20 characters or more, no expiration
  + Keytab
  + SSH Key

Automount

|  |  |
| --- | --- |
| Permission name | **ACME** Namespace Automount Manage |
| Description | Namespace automount container |
| Bind rule type | permission |
| Granted rights | add  delete  read  search  write |
| Type | <blank> |
| Subtree | cn=automount,dc=idm,dc=example,dc=com |
| Extra target filter | <blank> |
| Target DN | cn=**acme**,cn=automount,dc=idm,dc=example,dc=com |
| Effective attributes | automountinformation  automountkey  automountmapname  cn  createtimestamp  description  entryusn  modifytimestamp  objectclass |

|  |  |
| --- | --- |
| Permission name | **ACME** SubNamespace Automount Manage |
| Description | SubNamespace administration of automount containers |
| Bind rule type | permission |
| Granted rights | add  delete  read  search  write |
| Type | <blank> |
| Subtree | cn=automount,dc=idm,dc=example,dc=com |
| Target DN | cn=**acme**.\*,cn=automount, dc=idm,dc=example,dc=com |
| Effective attributes | automountinformation  automountkey  automountmapname  cn  createtimestamp  description  entryusn  modifytimestamp  objectclass |

Users (nonperson) and ipausers Group Management

|  |  |
| --- | --- |
| Permission name | **ACME** Group IPAUSERS Modify |
| Description | This is permission is required to enable the administrator to add and remove nonperson users.  Note: Although ipausers group permissions does not present a significant risk, this risk increases when the user group is applied to any access management object. To mitigate this risk, further custom IPA API development is needed to enforce the association between namespace administrator, nonperson user member management, and the ipausers user group  This needs to be secured with custom plugin to enforce namespace prefix. |
| Bind rule type | permission |
| Granted rights | write |
| Type | User Group |
| Subtree | cn=ipausers,cn=groups,cn=accounts,dc=idm,dc=example,dc=com |
| Extra target filter | <blank> |
| Target DN | cn=ipausers,cn=groups,cn=accounts,dc=idm,dc=example,dc=com |
| Effective attributes | member |

User Group Management

|  |  |
| --- | --- |
| Permission name | **ACME** Namespace Group Manage |
| Description | Namespace administration of user groups |
| Bind rule type | permission |
| Granted rights | read  search  write |
| Type | <blank> |
| Subtree | cn=groups,cn=accounts,dc=idm,dc=example,dc=com |
| Extra target filter | <blank> |
| Target DN | cn=**acme**,cn=groups,cn=accounts,dc=idm,dc=example,dc=com |
| Effective attributes | cn  createtimestamp  description  entryusn  gidnumber  ipauniqueid  member  membermanager  mepmanagedby  mepmanagedentry  modifytimestamp  objectclass |

|  |  |
| --- | --- |
| Permission name | **ACME** SubNamespace Group Manage |
| Description | SubNamespace administration of user groups |
| Bind rule type | permission |
| Granted rights | read  search  write  add  delete |
| Type | <blank> |
| Subtree | cn=groups,cn=accounts,dc=idm,dc=example,dc=com |
| Extra target filter | <blank> |
| Target DN | cn=**acme**.\*,cn=groups,cn=accounts,dc=idm,dc=example,dc=com |
| Effective attributes | cn  createtimestamp  description  entryusn  gidnumber  ipauniqueid  member  membermanager  mepmanagedby  mepmanagedentry  modifytimestamp  objectclass |

HBAC Rule Management

|  |  |
| --- | --- |
| Permission name | **ACME** HBAC Rule Manage |
| Description |  |
| Bind rule type | permission |
| Granted rights | read  search  write  add  delete |
| Type | <blank> |
| Subtree | cn=hbac,dc=idm,dc=example,dc=com |
| Extra target filter | (&(cn=**acme**.\*)(objectclass=ipahbacrule)) |
| Target DN | ipauniqueid=\*,cn=hbac,dc=idm,dc=example,dc=com |
| Effective attributes | cn  description  gidnumber  ipaenabledflag  memberhost  memberservice  memberuser |

Host Management

|  |  |
| --- | --- |
| Permission name | **ACME** Host Manage |
| Description | Allows namespace administration of a host when it is not associated with any namespace or enforces association of the host with the namespace value applied to userclass. |
| Bind rule type | permission |
| Granted rights | read  search  write  add  delete |
| Type | <blank> |
| Subtree | cn=computers,cn=accounts,dc=idm,dc=example,dc=com |
| Extra target filter [breakout for clarity] | (&  (|  (!(userclass=\*))  (userclass=**acme**)  (userclass=**acme.**\*)  )  (objectclass=ipahost)  ) |
| Target DN | cn=computers,cn=accounts,dc=idm,dc=example,dc=com |
| Effective attributes | createtimestamp  description  enrolledby  entryusn  fqdn  ipaallowedtoperform  ipaallowedtoperform;read\_keys  ipaallowedtoperform;write\_keys  ipaassignedidview  ipaprotectedoperation;write\_keys  ipasshpubkey  krbcanonicalname  krblastpwdchange  krbprincipalkey  krbprincipalname  modifytimestamp  nshardwareplatform  nshostlocation  nsosversion  objectclass  usercertificate  userclass  userpassword |

Hostgroups Management

|  |  |
| --- | --- |
| Permission name | **ACME** Hostgroups Manage SubNamespace |
| Description | Hostgroup permission only applies to subnamespace hostgroups; namespace hostgroup is managed by automember host group rule. |
| Bind rule type | permission |
| Type | <blank> |
| Granted rights | read  search  write  add  delete |
| Subtree | cn=hostgroups,cn=accounts,dc=idm,dc=example,dc=com |
| Extra target filter | <blank> |
| Target DN | cn=**acme**.\*,cn=hostgroups,cn=accounts,dc=idm,dc=example,dc=com |
| Effective attributes | cn  description  member |

ID View Manage Namespace

|  |  |
| --- | --- |
| Permission name | **ACME** ID View Manage Namespace |
| Description | The namespace ID View is created during namespace provisioning; this is intended to be permanent for the life of the namespace |
| Bind rule type | permission |
| Granted rights | read  search  write |
| Type | <blank> |
| Subtree | cn=views,cn=accounts,dc=idm,dc=example,dc=com |
| Extra target filter | (objectclass=ipaidview) |
| Target DN | cn=**acme**,cn=views,cn=accounts,dc=idm,dc=example,dc=com |
| Effective attributes | cn  description |

ID View Manage SubNamespace

|  |  |
| --- | --- |
| Permission name | **ACME** ID View Manage SubNamespace |
| Description | ID View SubNamespace permission to allow create, modify, and delete of the subnamespace containers |
| Bind rule type | permission |
| Granted rights | read  search  write  add  delete |
| Type | <blank> |
| Subtree | cn=views,cn=accounts,dc=idm,dc=example,dc=com |
| Extra target filter | (objectclass=ipaidview) |
| Target DN | cn=**acme**.\*,cn=views,cn=accounts,dc=idm,dc=example,dc=com |
| Effective attributes | cn  description |

ID Override User and ID Override Group Management

|  |  |
| --- | --- |
| Permission name | **ACME** ID Override Manage Namespace |
| Description | Permission to enable management of ID Override Namespace user and group ID View entries |
| Bind rule type | permission |
| Granted rights | read  search  write  add  delete |
| Type | <blank> |
| Subtree | cn=views,cn=accounts,dc=idm,dc=example,dc=com |
| Extra target filter | (&(ipaanchoruuid=\*)(|(objectclass=ipauseroverride)(objectclass=ipagroupoverride))) |
| Target DN | cn=**acme**,cn=views,cn=accounts,dc=idm,dc=example,dc=com |
| Effective attributes | cn  description  gidnumber  homedirectory  ipaanchoruuid  loginshell  member  uid  uidnumber |

|  |  |
| --- | --- |
| Permission name | **ACME** ID Override Manage SubNamespace |
| Description | Permission to enable management of ID Override SubNamespace user and group ID View entries |
| Bind rule type | permission |
| Granted rights | read  search  write  add  delete |
| Type | <blank> |
| Subtree | cn=views,cn=accounts,dc=idm,dc=example,dc=com |
| Extra target filter | (&(ipaanchoruuid=\*)(|(objectclass=ipauseroverride)(objectclass=ipagroupoverride))) |
| Target DN | cn=**acme**.\*,cn=views,cn=accounts,dc=idm,dc=example,dc=com |
| Effective attributes | cn  description  gidnumber  homedirectory  ipaanchoruuid  loginshell  member  uid  uidnumber |

Netgroups Management

|  |  |
| --- | --- |
| Permission name | **ACME** Netgroups Manage |
| Description | Use of IPA netgroups is discouraged as HBAC rules and Sudo rules address all use cases (e.g. access management, shared account for system environment and access); IPA automatically manages “compat” netgroups based on corresponding hostgroup; these netgroups have been modified for compatibility with network storage devices. |
| Bind rule type | permission |
| Granted rights | read  search  write  add  delete |
| Type | <blank> |
| Subtree | cn=ng,cn=alt,dc=idm,dc=example,dc=com |
| Extra target filter | (&(cn=**acme**.\*)(objectclass=ipanisnetgroup)) |
| Target DN | ipauniqueid=\*,cn=ng,cn=alt,dc=idm,dc=example,dc=com |
| Effective attributes | cn  createtimestamp  description  entryusn  hostcategory  ipauniqueid  modifytimestamp  nisdomainname  nisnetgrouptriple  objectclass  usercategory |

NONPERSON Users Management

|  |  |
| --- | --- |
| Permission name | **ACME** NONPERSON Users Manage |
| Description | Person users are automatically synchronized with the logical access directory gold source. Nonperson users, also known as application accounts, are available to create when prefixed with the namespace. Namespace can then be removed with ID Override User. |
| Bind rule type | permission |
| Granted rights | read  search  write  add  delete |
| Type | <blank> |
| Subtree | cn=users,cn=accounts,dc=idm,dc=example,dc=com |
| Extra target filter | <blank> |
| Target DN | uid=**acme**.\*,cn=users,cn=accounts,dc=idm,dc=example,dc=com |
| Effective attributes | cn  createtimestamp  displayname  entryusn  gecos  gidnumber  givenname  homedirectory  ipasshpubkey  ipauserauthtype  loginshell  mepmanagedentry  modifytimestamp  objectclass  sn  uid  uidnumber  userclass  userpassword |

Service Management

|  |  |
| --- | --- |
| Permission name | **ACME** Service Manage |
| Description | Manage service principals for hosts |
| Bind rule type | permission |
| Granted rights | read  search  write  add  delete |
| Type | <blank> |
| Subtree | cn=services,cn=accounts,dc=idm,dc=example,dc=com |
| Extra target filter | (&(objectclass=ipaservice)(|(!(ipaAllowedToPerform=\*))(ipaAllowedToPerform=acme.admin))) |
| Target DN | krbprincipalname=\*,cn=services,cn=accounts,dc=idm,dc=example,dc=com |
| Effective attributes | createtimestamp  entryusn  ipaallowedtoperform  ipakrbprincipalalias  krbextradata  krblastpwdchange  krbprincipalkey  krbprincipalname  objectclass |

Sudo Rule Management

|  |  |
| --- | --- |
| Permission name | **ACME** Sudo Rule Manage |
| Description | Sudo rule for namespace administration (acme.admin) are created during the namespace provisioning; this permission gives the namespace administrators an ability to create SubNamespace Sudo rules. |
| Bind rule type | permission |
| Granted rights | read  search  write  add  delete |
| Type | <blank> |
| Subtree | cn=sudo,dc=idm,dc=example,dc=com |
| Extra target filter | (&(cn=**acme**.\*)(objectclass=ipasudorule)) |
| Target DN | cn=sudo,dc=idm,dc=example,dc=com |
| Effective attributes | cmdcategory  description  externalhost  externaluser  hostcategory  ipaenabledflag  ipasudoopt  ipasudorunas  ipasudorunasextuser  ipasudorunasgroupcategory  ipasudorunasusercategory  memberallowcmd  memberhost  memberuser  sudoorder  usercategory |

Sudo Commands Group Management

|  |  |
| --- | --- |
| Permission name | **ACME** Sudo Commands Group Manage |
| Description | Permission that allows administrators to manage Sudo Commands Group prefixed with the namespace. |
| Bind rule type | permission |
| Granted rights | read  search  write  add  delete |
| Type | <blank> |
| Subtree | cn=sudocmdgroups,cn=sudo,dc=idm,dc=example,dc=com |
| Extra target filter | (&(cn=**acme**.\*)(objectclass=ipasudocmdgrp)) |
| Target DN | cn=sudocmdgroups,cn=sudo,dc=idm,dc=example,dc=com |
| Effective attributes | description  member |

Ancillary Domain Management Processes

usersync: Manages the person users (personnel); synchronizes basic user settings from the directory gold source. Interval: Runs hourly.

shortsync: Manages the authentication settings of person users (personnel). Suspends ability to authenticate when identity is suspended. Interval: Runs every 15 minutes.

sudocmdrm: Removes sudo commands not associated with sudo commands group or Sudo rule policy. Interval: Runs daily.

hbacsvcrm: Removes HBAC services not associated with HBAC services group or HBAC rule policy. Interval: Runs daily.

Custom IPA API Plugin: host\_callbacks.py

Purpose: To enforce host association with namespace and subnamespace based on host-based attribute: userclass

A custom IPA API plug-in enforces an association between hosts and their associated namespace using host attributes userclass. Applies to hostgroup membership, HBAC Rule policy, and Sudo Rule policy.

Namespace enforcement applies to user gropu association with nested user groups, HBAC Rule policy (Who), Sudo Rule policy (Who).

Namespace enforcement applies to hostgroup association with nested hostgroup, HBAC Rule policy (Accessing this host) and Sudo Rule policy (Accessing this host).

Any hosts not associated with a namespace are available to assign to any namespace, therefore it is important for namespace administrators to apply “class” with a value of the namespace when adding the host to the domain or after the host is enrolled with the domain.