BSA Best Practices Webinars
Role Based Access Control

Sean Berry
Customer Engineering

Agenda

- Overview
- RBAC Objects
- Implementation
- Use Cases
  - Basic
  - Advanced
  - Multi-Tenancy
- GUI Tour

Overview

Access Control Quick Glossary

- Authentication: How you know that I am who I say I am
- Authorization: What I'm allowed to do
- Accounting/Audit Trail: What you did

Use Cases

- Simple environment setup (start with OOTB blcontent)
- Basic shared access content
  - Anyone within a role has full access
  - Anyone else has “read” access
- Basic exclusive access
  - Anyone within a role has full access
  - No access from other roles (by default)
- Multi-tenancy / multi-service
  - Few shared roles, some sharing within tenant/service
- Accountability: Who did what, where?
- AD integration

RBAC Challenges

- "ARM-like" use cases:
  - Content (software, policies, scripts) created/packaged by those without full production access
    - Testing
    - Promotion/Handoff
  - Content to be deployed should be tested, but probably not changed in-flight
  - Content deployed in production shouldn't be changed after validation
- Trust levels vary:
  - Some have full access to most servers (sysadmin-type roles)
  - Some have full access to limited subset of servers (app-specific roles, devs)
  - Some have limited access to most servers (IT Security / infrastructure app admins)
  - Some have limited access to a few servers (app admins, devs, chrooted or config audit)

Quick Architecture Review!

- Requests: GUI -> Appserver -> Agent
- Incoming connections go via: CONFIG/NSH_PROXY appservers
  - GUI traffic: CONFIG/ALL type appservers
  - NSH-only traffic: NSH_PROXY
  - Authentication (user/password etc.) is done at this level
- Agents hold access controls
  - Who can connect
  - Who they map to
  - At what privilege level (root/Admin, “nobody”, connection refused)

RBAC Objects

RBAC Overview

- **Roles**-- A grouping of Authorizations and Users. Defines the maximum amount of permissions that Users within that Role can perform. (The Authorizations defined on each object in BladeLogic determines whether or not an action is actually allowed.
- "How big is my world?"

vs.

RBAC Overview

- **Users** – Typically represent an actual person logging into BladeLogic, and can be associated with one or more Roles.
- **Authorizations**
  - **Commands** – Network Shell (NSH) commands that can be used to limit Users within a Role to specific NSH commands.
  - **System Authorizations** – Represents a specific action within the Server Automation Console, such as the ability to read, modify, or update a specific type of object.
  - "Server.Read", "BLPackage.Delete"

RBAC Object Overview

- **Authorization Profiles** – A group of Authorizations
  - "Execute Shell Scripts" = DepotObject.Read + Job.Execute + …
- **ACL Templates** – A group of Authorizations that can be applied to one or more objects, but in a non-persistent manner. Updating the ACL Template does not affect any objects that ACL Template may have been applied to previously.
  - ACL Templates can also be used to define **default permissions** to objects created by Users within a Role.
  - "stencil", "pattern"
- **ACL Policy** – A group of Authorizations that is directly tied to one or more objects. Updating the Policy automatically updates the permissions on each object the Policy is tied to.
  - "pointers", "set and forget"
- **ACL Templates/Policies = AuthProfiles + Role information**

RBAC Object Overview

- Object Permissions: "who's allowed to access this object?”
  - Everyone has keys, but only my family has keys to my house
  - Everyone at our company may have a badge that lets them in to shared office space
- Where can I see some sample RBAC content configurations?
  - Run blcontent!

Implementation

Roles in Detail

- Who do I map to on managed servers? (Admin/root/oracle/wsadmin)
- Prefer Auth Templates over individual authorizations
- Default Permissions Template
- Meta-roles: "read-only", "packager", "deployer", "sysadmin/full admin", RBACAdmin
- Service/Tenancy: 2-3 “meta-roles” for each application / service
- Details:
  - May replace local user accounts on many systems
  - Chroot capability
  - Time windows!

Users

- Typical auth: SRP
- LDAP Sync to sync LDAP containers -> Roles
- AD Authentication integration: authenticate to AD
- GUI tools for the end user:
  - “Reconnect”
  - “Switch Role”
  - “Change Password”

Agent ACLs

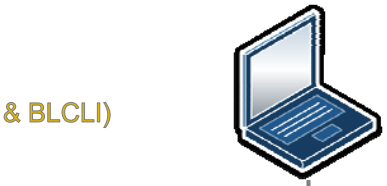
- Exports
  - "* ro" allows all clients to connect (unless "nouser" + no users/users.local entries)
  - "192.168.1.30 ro" IP-based entries will restrict connections to those IPs
- Users.local
  - Static, not updated by PushACLs job
  - Usually used for failsafe configurations
  - BLAdmins:* or equivalent for "failsafe"
- Users
  - Updated by PushAcls
  - "nouser" configuration:
    - If nouser exists in the users file then you are not allowed access unless you are explicitly mentioned in the users or users.local file.
    - If it does not exist and you are not listed, you will be mapped to Anonymous or nobody access. See documentation for detailss
- Do not push ACLs to the file server!

BMC Server Automation (BladeLogic) Logical Architecture

CONSOLE

MID TIER

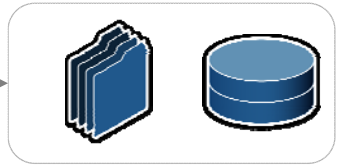
NODES



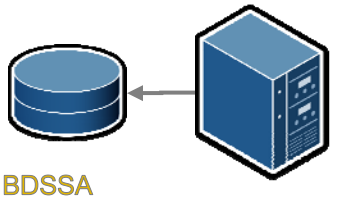
Management Consoles
- Graphical Interface
- Command Line Interface (NSH & BLCLI)
- Authentication,

Web-based Reporting Portal
- Standard and Custom Reports

Application Servers
- Automation Engine
- Load Balanced
- Job Partitioning
- Role-Based Access Control

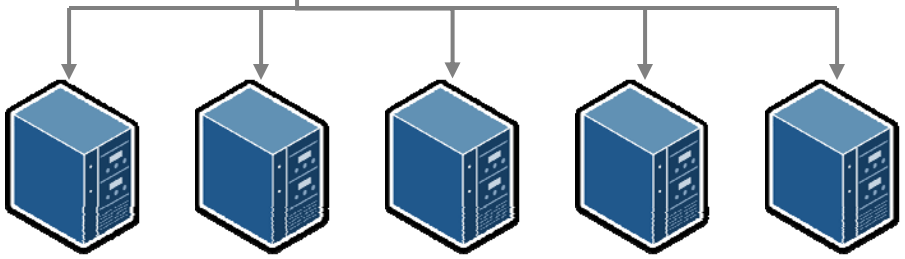


Depot
- File Server: Local Disk, SAN, NAS
- Database: Oracle, SQL Server



BDSSA (Reports) Data Warehouse

BDSSA (Reports)



RSCD Agent
- Windows, Linux, Unix, ESX
- Lightweight service or daemon
- Encrypted communication
- Single TCP port

BMC Server Automation (BladeLogic) Client Access With NSH Proxy

bmcsoftware

CONSOLE

MID TIER

NODES

Management Consoles
- Graphical Interface
- Command Line Interface (NSH & BLCLI)
- Authentication,

Web-based Reporting Portal
- Standard and Custom Reports

BDSSA
(Reports)
Data
Warehouse

BDSSA
(Reports)

Audit at Proxy Level

BMC Server Automation (BladeLogic) Service Provider Network Model

bmcsoftware

CONSOLE

MID TIER

NODES

Management Consoles
- Graphical Interface
- Command Line Interface (NSH & BLCLI)
- Authentication,

Web-based Reporting Portal
- Standard and Custom Reports

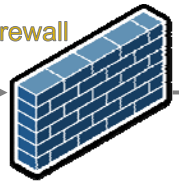
Depot

BDSSA (Reports) Data Warehouse

BDSSA (Reports)

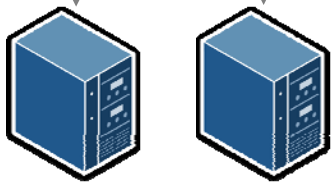
Application Servers
- Automation Engine
- Load Balanced
- Job Partitioning
- Role-Based Access Control

Firewall



SOCKS Proxy

Unrestricted Networks



Remote Network(s): Overlapping IP networks or restrictive firewalls

“Out of the Box”

- What's the default behavior of the RBAC "out of the box", at a high level?
  - (Run blcontent to build out sample roles after install)
  - Objects are generally visible to others
  - By default, only the roles that create or own an object will be able to modify it
- Great for “basic” installations, but most customers will need a bit more.

Auth Types and Automation Principals

- Authentication types (SRP, AD, RSA, LDAP etc.)
  - https://docs.bmc.com/docs/display/public/bsa82/Implementing+authentication
  - Integration setup
  - AD->Role sync
- Automation Principals
  - When do I want to use Automation Principals and how do I set them up?
  - https://docs.bmc.com/docs/display/bsa83/Creating+automation+principals
  - Agent installs / bundles
  - SQL Server software install, anything that requires a "real" local user, anything that needs to run as a domain user

Use Cases

Basic Use Cases

- How does content get created: what permissions are on it?
  - Default ACL Template
- How do I set and propagate permissions down to folders and objects in those folders?
  - Apply Permissions (with recurse)
- Who needs to share content with others?
  - Include the others' roles in the Default ACL Template
- Who needs to keep their content private?
  - Remove "Everyone.Read" from their templates
- Accountability: who accessed what, when, from where? (rscd.log, NSH Proxy)

Basic Use Cases

- Content development & promotion ("classic" ARM)
  - Developer creates, promotes
  - QA tests (deploy), promotes or demotes
  - Production deploys to prod
- LDAP/AD Synchronization
- How do Authorizations work when importing or exporting an object?
  - RBAC doesn't go with an object, dropped on export and re-set on import
- Map many users in a role to one application id with accountability

Basic Use Cases

- Multi-customer within one enterprise:
  - Access to servers by "service":
    - email admins vs. web apps groups,
    - see only their server smart groups & servers.
    - Permissions at the Group/SmartGroup **and** Server level (otherwise can just build a new SSG and "find" the other servers.)

Advanced Use Cases

- Access to one or few objects
- Access to dev servers (full access) for dev/engineers
- Readonly access as root (app owners)

Advanced Use Cases

- Multi-tenant within a service provider
- Multiple roles per customer (CUSTOMER property)
- How roles can share access to some objects
- Different admin accounts
- Two different "admin" roles when transitioning/aligning Administrator accounts
- Parameterized "admin" accounts
  - When there are many (or even one for every server) local admin accounts

Advanced Use Cases

- Chrooted access (partial access to sensitive servers, only one directory, no nexec?)
- Limited NSH remote access
- How do I limit the specific commands which a user can execute on an agent in the users file?
- Map many users in a role to one application id with accountability

Advanced Use Cases

- Permission mapping on imports
- Time window based access
- Temporary access: add, use, remove access (CLI?)
- BLCLI & SSO caching (for Orchestration: 9999 hour cred)
- Timeouts (10 hrs for GUI, sometimes longer for automation engines)

Known issues / risks

- Older agents: reverse resolution of hosts in exports file (use IPs when possible, remote resolution is not reliable)
- ACLs are read every new connection: keep them reasonable in size.
- BSA ACL Policy performance prior to 8.2 GA
- Don’t push ACLs to the file server! Will result in unpredictable performance.

Reporting

- OOTB RBAC Reports: https://docs.bmc.com/docs/display/public/bdssa83/Built-in+RBAC+reports
- GUI: "Show Effective Permissions"

Where do I find RBAC in the GUI?

- Top of screen: Role, User, appserver
- Authentication Profile setup screen
- Permissions pane
- RBAC workspace
- Automation principals
- Unified Installer
- Reconnect
- Switch Role
- Change Password

Next time!

- Shorter call! (30 min)
- Several videos available ahead of the call
- Highlights / best of during the live call
- More time for Q&A

RBAC Manager Workspace