bmc AMI

BMC AMI Security Privileged Access Manager (PAM)

Axel Griepenstroh

Advisory SW Consultant
Axel_Griepenstroh@bmc.com

What is this about

Defining a privileged user:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Discussion: Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. Privileged roles include key management, account management, database administration, system and network administration, and web administration. A role-based access scheme organizes permitted system access and privileges into roles. In contrast, an attribute-based access scheme specifies allowed system access and privileges based on attributes.

Why do we care:

- Special monitoring/attention required
- Ability to harm the data/system
- Security concepts like Zero Thrust and principal of least privileges

Basic about BMC AMI Security Privileged Access Manager (PAM)

There are times when authorized users require elevated privileges, which are controlled by external security managers (ESM), like

- IBM Resource Access Control Facility (RACF)
- CA Access Control Facility 2 (ACF2)
- CA Top Secret Security (TSS)

To perform specific application or system changes. For certain critical or sensitive systems, having one or more users with permanent access privileges is a potential security risk.

PAM enables users who do not have system privileges on a permanent basis to request elevated privileges when required. All Security PAM activity is fully audited and can be associated with change control requests.

BMC AMI Security Privileged Access Manager provides multiple methods for accessing and grouping the temporary system privileges that you can request.

Basic about BMC AMI Security Privileged Access Manager (PAM)

BMC AMI Security Privileged Access Manager provides multiple methods for accessing and grouping the temporary system privileges that you can request.

Access modes

You can access Security PAM by using the following modes:

- User ID pools
  - Users get access to a temporary user ID from a predefined pool. You create user IDs in the ESM database, each of which is assigned the necessary permissions to perform a specific system maintenance role.
- Self-elevation
  - Users can have their own user ID privileges temporarily elevated. You grant them membership to privileged resources (for example RACF groups), each having the necessary permissions to perform a specific system maintenance role.

PAM Projects

Change management

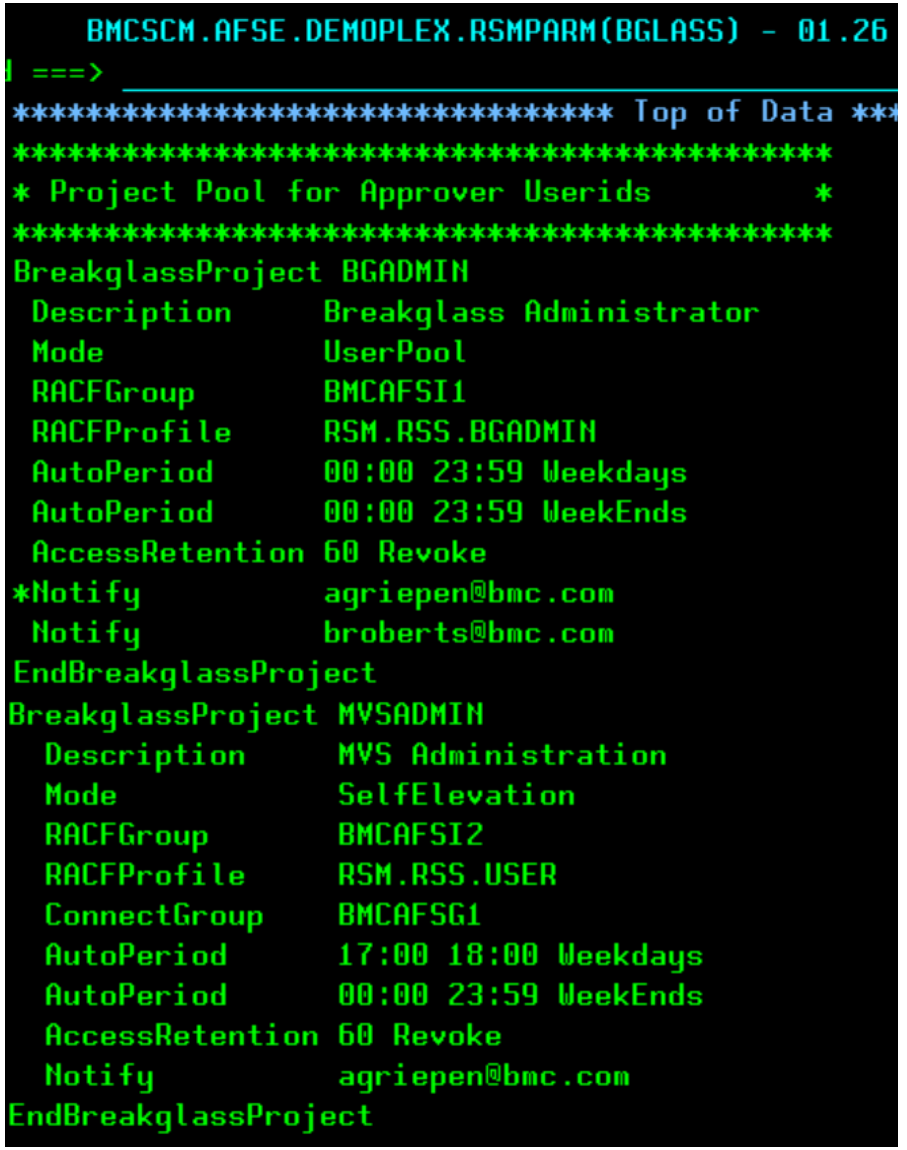
- All requests require a change control ID logged in, audit log, and optional SMF records

Security management

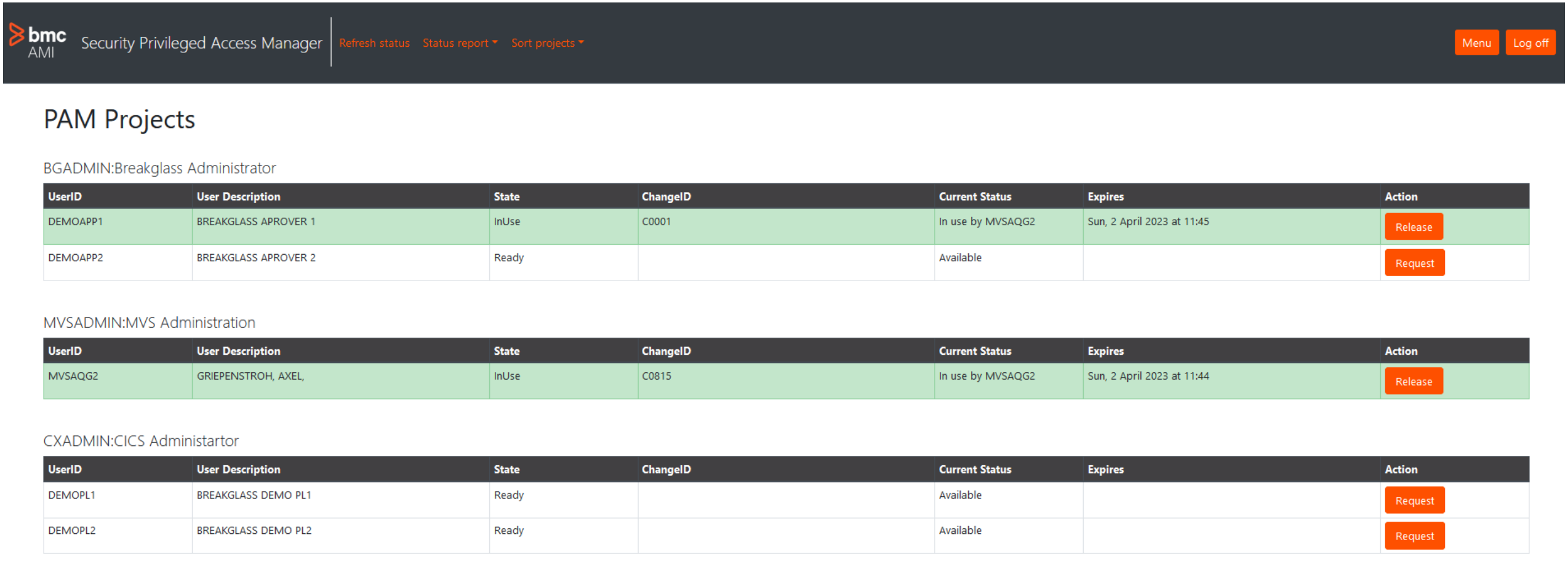
- multiple groups can be defined with different privileges for different projects and access needs

Auditing

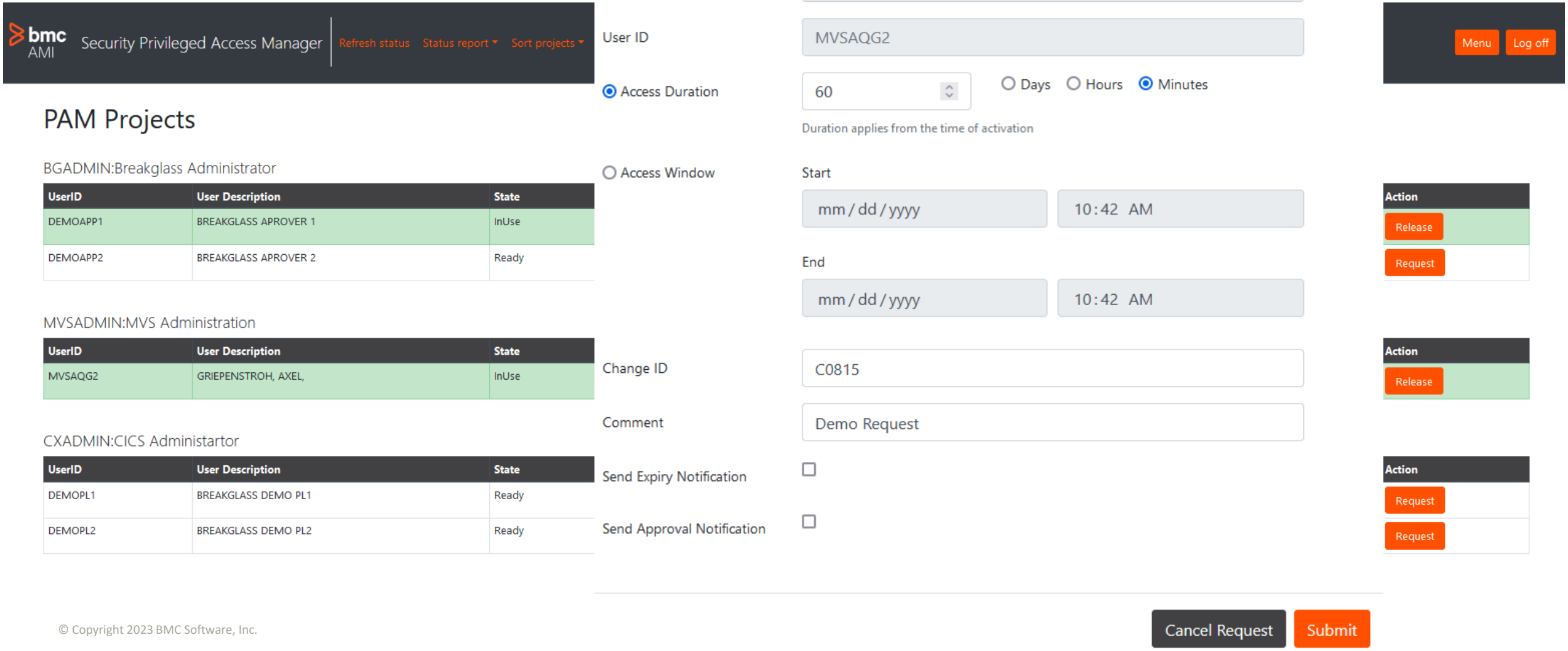
- assignment and approval of temporarily raised privileges, fully audited and trackable online, and optionally via SMF and console messages



PAM Projects



PAM Projects



Who can do what, still in the ESM

```
    BMCSCM.AFSE.DEMOPLEX.RSMPARM(BGLASS) - 01.26
 ===>
**********************************************
BreakglassProject MVSADMIN
  Description     MVS Administration
  Mode            SelfElevation
  RACFGroup       BMCAFSI2
  RACFProfile     RSM.RSS.USER
  ConnectGroup    BMCAFSG1
  AutoPeriod      17:00 18:00 Weekdays
  AutoPeriod      00:00 23:59 WeekEnds
  AccessRetention 60 Revoke
  Notify          agriepen@bmc.com
EndBreakglassProject
```

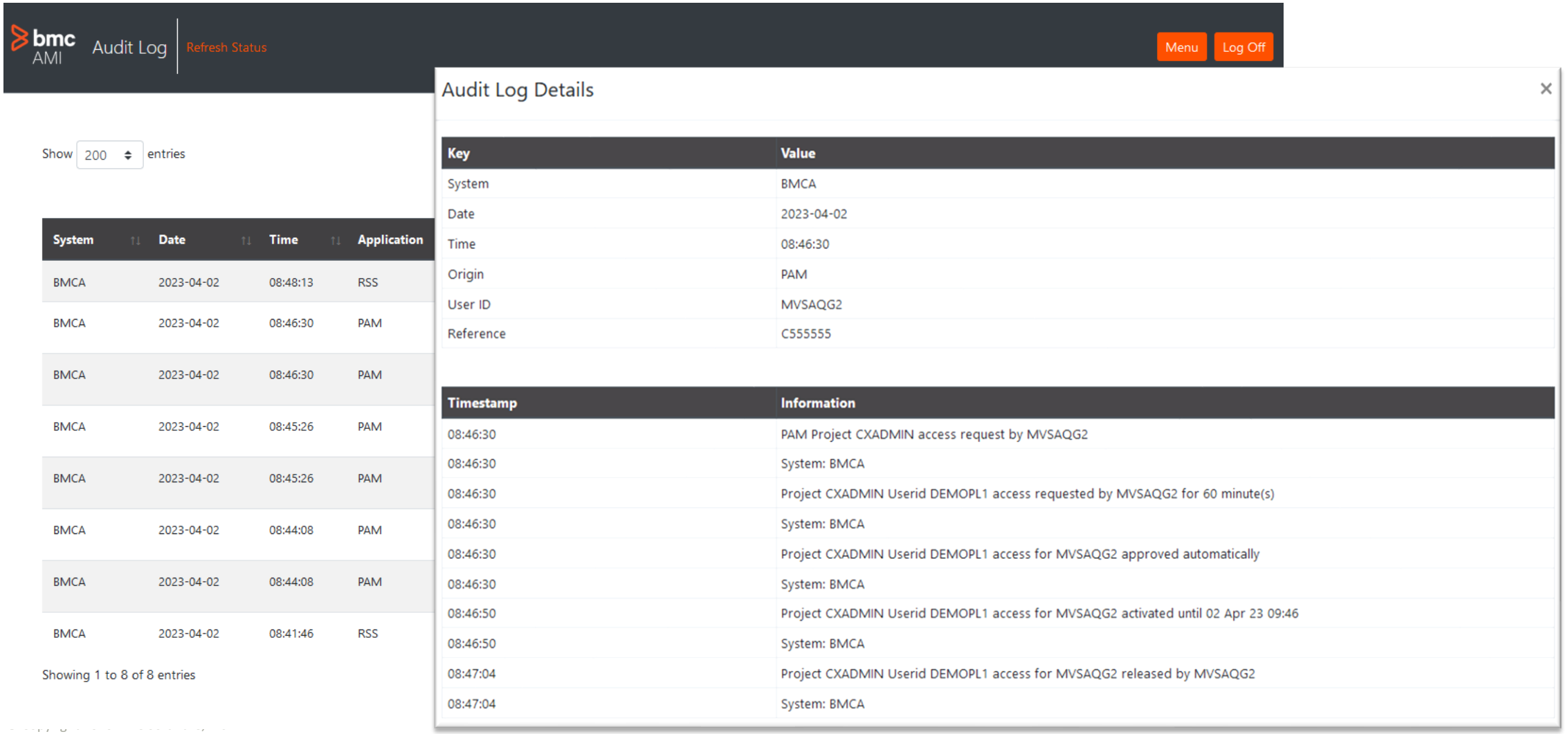
Who can use a project:

- **RACFPROFILE**
  - To request access to a project (user level), users must have READ access to the resource profile.
  - To approve access to a project (manager level), users must have ALTER access to the resource profile.

What will happen by requesting a project:

- **RACFGROUP**
  - User IDs defined for a particular project must be connected to the group
- **ConnectGroup**
  - ESM user-access resources provide projects with access to required system resources.

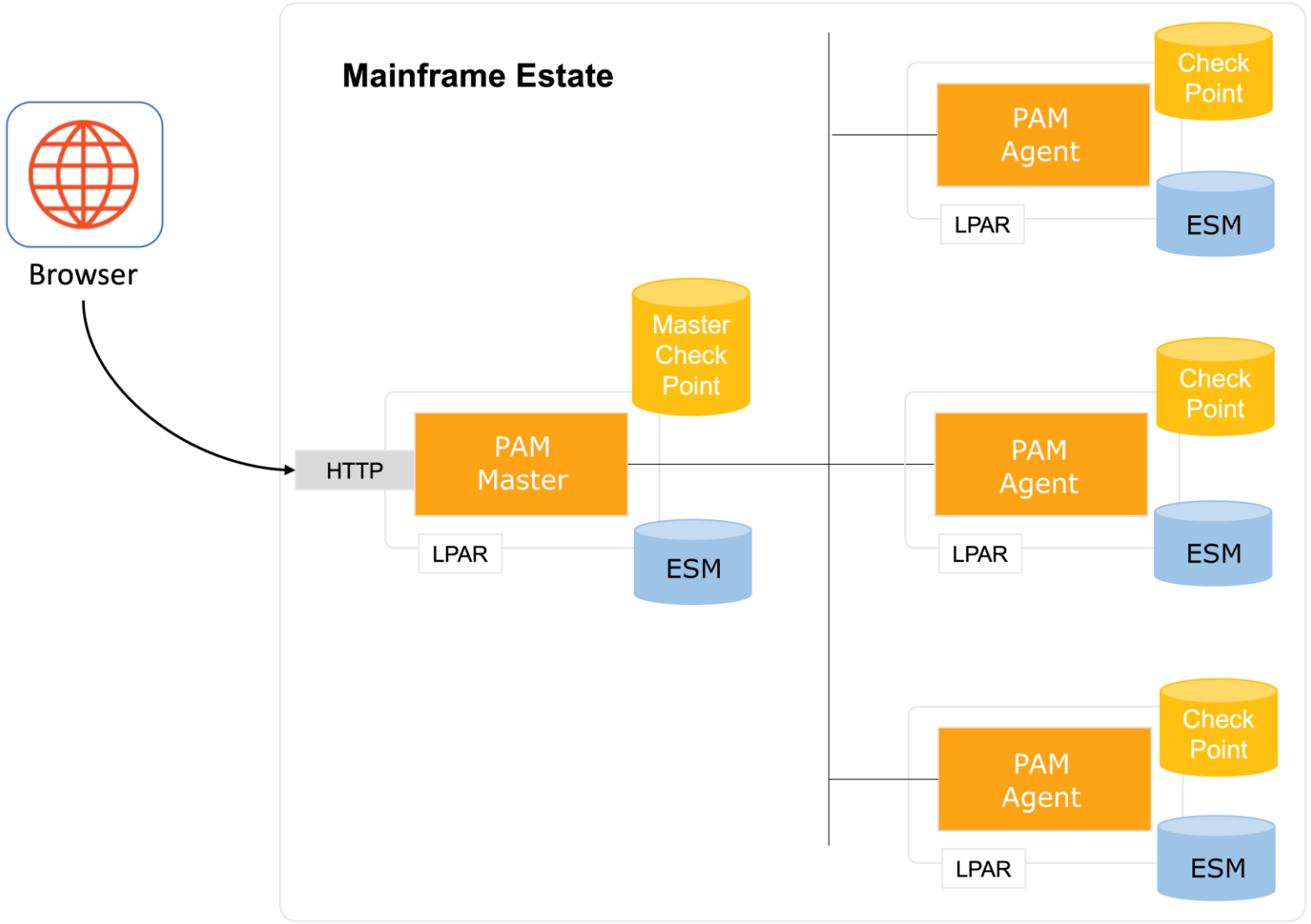
Logging and writing of an SMF record



Multi-system configuration

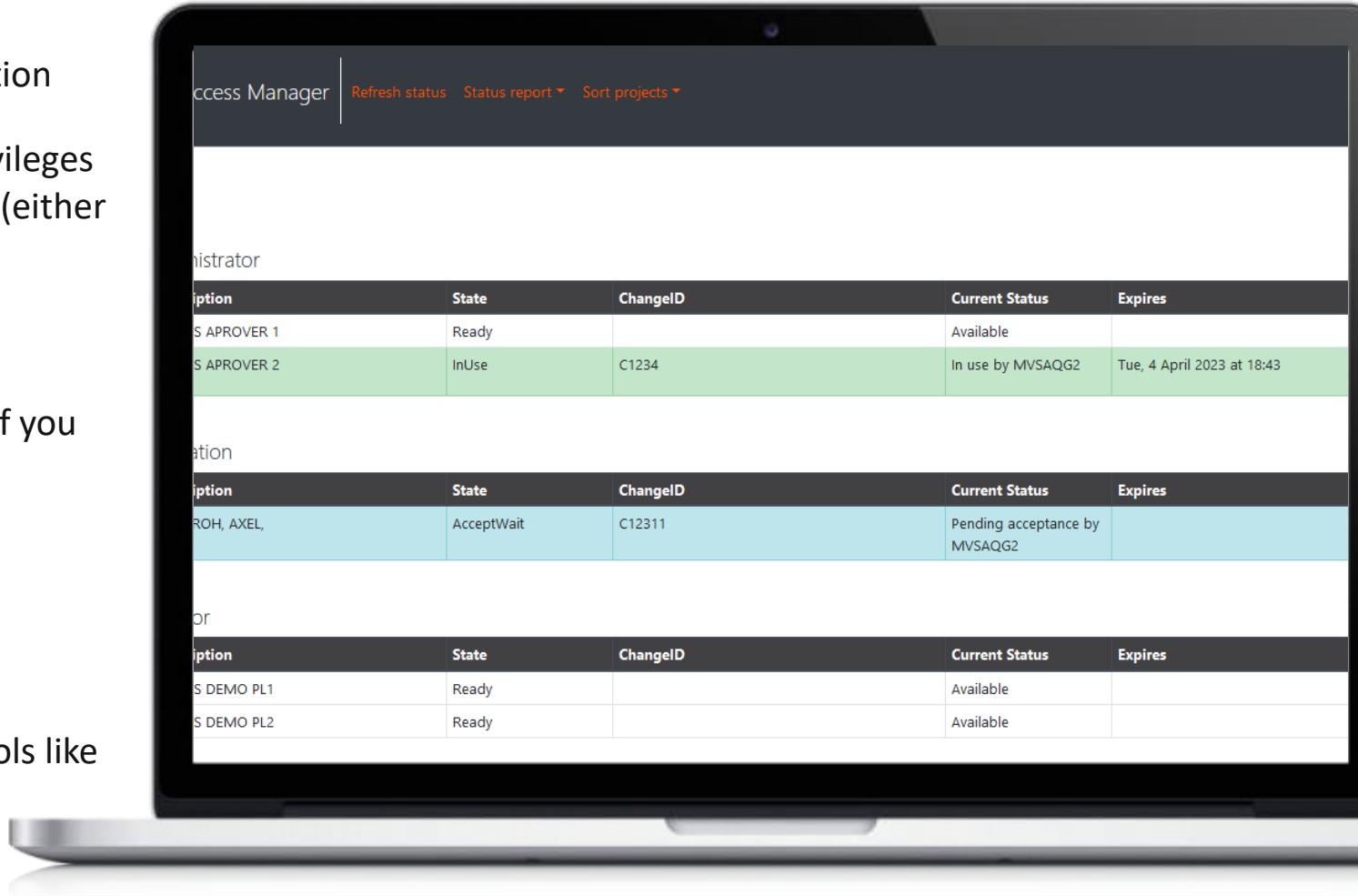
The user submits a request on multiple systems, and one or more of the systems is down.

The request proceeds with the remaining systems. The master instance continuously checks the status of the associated systems. When the system becomes available, the user can complete the request for that system.



Summary & Question

- **Who has access to which privileges is in the ESM**
  - PAM projects can be part of the role definition
  - With PAM user get request the needed privileges when they need it in a self-service manner (either with or without manager approval)
  - Following the least privilege approach
  - Only have privileges assigned to your user if you need it.
- **PAM can be integrated in overall processes**
  - Verify active change exists
  - Offer a REST API so it can be called from tools like CyberArc



NIST Cybersecurity Capability Tool Chain

bmc Solutions

Identify

- Data Discovery — BMC Helix Discovery
- Data Discovery Program — BMC Mainframe Services

Protect

- Network Micro Segmentation — BMC EC for Illumio
- Digital Certificate Management — BMC EC for Venafi
- Privileged Access Management — BMC PAM
- Policy Configuration Audit — BMC SPM
- Role Based Access Management — BMC EC for OIM
- Security Admin Managed Services — BMC Mainframe Services
- Penetration Tests — BMC Mainframe Services
- Vulnerability Assessments — BMC Mainframe Services
- Security Assessments — BMC Mainframe Services
- SWIFT Assessments — BMC Mainframe Services
- Role Based Access Management — BMC Mainframe Services
- Training & Education — BMC Mainframe Services
- Security Engineering & Architecture — BMC Mainframe Services

bmc Products

bmc Services

Detect

- Alerts/Indicators of Compromise — BMC Command Center
- SOC & SIEM Integration — BMC Command Center
- File Integrity Monitoring — BMC MainTegrity FIM+
- File integrity Monitoring — BMC Mainframe Services
- Security as a Service — BMC Mainframe Services

Respond

- Incident Response — BMC Command Center & SPM
- Automated Response — BMC Command Center & SPM
- Forensic Investigation — BMC Security Session Manager
- Forensic Investigation BMC Mainframe Services
- Inacident Response — BMC Mainframe Services

Recover

- Data Recovery — BMC S- multiple
- Security Remediation — BMC Mainframe Services
- Security Policy Updates — BMC Mainframe Services

Withstand, Respond to, Recover

BMC AMI Security

Datastream
Enriched Mainframe data

Security Policy Manager

Privileged Access Manager

Self service Password Reset

Enterprise: Illumio & Venafi

esmGUI
Multi esm administrator

Security Session Monitor

Maintegrity + Partners

BMC AMI Command Center for Security

Single browser based UI

Collated data for analytics

SIEM

ITSM Workflows

SOC

Compliance Reporting

Real time alerting & Response

Trend analysis

Sophisticated cross product intelligence

Self healing mainframe


bmc
Run and Reinvent