midPoint Answers Product Evaluation Questions

2. Reporting and Auditing

1. What current and historical data is maintained for reporting? A detailed description of the historical auditing data https://wiki.evolveum.com/display/midPoint/Auditing Also, for a example log see midPoint Logging
2. Is the reason (automatic and manually approved) for all provisioning decisions and actions stored? If the reason is internal to midPoint, then yes, but there is not a way to record a reason for a manual action in the audit log. Can it be sent to an external system (Splunk, logstash, etc) data warehouse? Yes, the logger can be configured to write the audit to a file where an external system could pick it up, database queries are also possible
3. How is the data stored? The data is stored in database tables, and the schema is published. Can it be read by external systems? Yes, either directly from from the database or by configuring a logger.
4. Can we export the data in its entirety? Yes, via database export, or by building a report.
5. Can we control how long the data is maintained? I do not see a way to limit data retention, though direct database actions could be taken.
6. Does this product provide what our auditors and compliance officers need? Much of what I've heard requested, though not the ability to add notes manual actions (actions themselves are recorded)
7. Does this product provide what our application (target system) owners need? (Not sure how to answer this one)
8. Reporting (should we just combine audit and report?)
    a. What pre-built reports are available? Can they be customized? There are a few canned reports, including general audit report, and you can customize reports. https://wiki.evolveum.com/display/midPoint/Report+Configuration
    b. Can we build our own reports? Using a GUI? Non-GUI? There is a GUI for building reports, and you could of course use SQL. You can also import jasper reports.
    c. Does the product support reports on
        i. Access for an application (target system). Granting access would be recorded, but not user access of a target system
        ii. All access for a user, all users in a unit, all users for a supervisor. Session creation (login) as well as actions taken are recorded.
        iii. Elevated or high-risk access. All actions are recorded, but there is not a provided canned report to identify these.
        iv. Separation of Duties. All actions are recorded, but there is not a provided canned report to identify these.
    d. What output formats are available for reports (eg, PDF, CSV, HTML) All of these plus additional XML and jasper options.
    e. Is the data used for reports available for use by third-party reporting tools? Yes.
    f. Can reports be run on a schedule and sent by email or to a (possibly external) report repository, and/or made available via GUI? I do not see a way to schedule reports, but they are available in the GUI, and post report actions can be scripted, including shell actions. If available via GUI, what are the access controls? Reporting appears to be available to administrators, but I don't see a built in role to delegate.
9. Auditing
    a. Can we compare intended provisioning to the actual state of an application on demand? This is connector specific, but reconciliation is usually supported.
    b. Does the product audit changes made within it (eg, who made a change to group membership logic when, and what the change was). Yes
    c. Does the product support Separation of Duties audits? This would require a custom report.
    d. (If you do access reviews / attestations) does the product provide adequate support?
        i. review by person, unit, application Attestation is done via "campaigns" https://evolveum.com/blog/access-certification-in-midpoint/
        ii. review of only manually-decided access, exceptions only, etc It should be possible to build a custom campaigns that excludes role initiated auto approved actions, but nothing built in.
        iii. Can audit results include “comments” (eg, “access being removed because …”) that become part of the record No
        iv. Can the auditing work with an external ticketing system (eg, ServiceNow, Remedy) Documentation notes support for ITSM integration via plugins, but requires custom development.
        v. How does the product define and schedule reviews, notify and remind reviewers, etc? See the link in "i" Can the product send emails and/or use an external ticketing system? Nothing built in. Are reviews done within the product, or in a document sent to the reviewer? Within the product.
        vi. How does the reviewer to report results? Results are recorded within the product, and custom reports can be created. Is the effort required proportional to the number of changes? Yes, attestation is per approval.
        vii. Does the product support workflows, logic, etc. needed to implement access changes determined by a review? There is some workflow capability such as delegating a attestation approval.

1. Identity provisioning
    a. Identity matching
        i. Does your product provide an identity matching service?
            1. Describe how the identity matching service is configured, and any scoring or weighting of attributes.
            2. Describe how low quality matches are handled, and if there is a notion of matches in suspense, what are the mechanisms for making assertions about them.
            3. Can the matching service be run against an existing population seeking duplicates.
        ii. Does your product have the ability to use an external matching service?
            1. Describe the configuration of the external service.
            2. Describe how low quality matches indications are handled, and if there is a notion of matches in suspense, what are the mechanisms for making assertions about them.
            3. Describe and standards that are used in messaging or APIs for matching services.
    b. Username assignment
        i. Does your product support user selected usernames, if so, how are attempted duplicates handled.
        ii. Does your product support generated usernames, if so, describe the options and configuration.
        iii. Does your product support enrollment of new users, if so, please describe the configuration of the enrollment portal, and any support for workflow.
    c. Identifiers for services and target directories[1]

i. Describe how your product handles identifiers or accounts which may be different from the institutional identifier.
ii. Describe how accounts in other systems are provisioned, and any standards that are supported for provisioning.
iii. Describe how accounts in other systems are deprovisioned, including supported workflows.
iv. Describe your products support for deprovisioning identifiers, and any support for namespace preservation after deprovisioning.

d. Username changes
   i. Describe how your product handles username changes, including support for namespace protection and auditing, and any workflows.
   ii. Describe how your product can communicate username changes to other systems that might need to be informed

e. Social IDs
   i. Describe your products support for social IDs (Facebook, Google, etc.) in place of local identities[2] .
   ii. Describe your products support for social IDs that are connected to local identities.

Notes from a subsequent discussion on identity matching, need to work this in.

- where does a person start (eg, HR, or self-service from person registry)
- match methodology (scoring, etc), is match process in person registry, or one or more of the authoritative systems
- processes for handling dups, possible matches (in registry, systems of record, and possible downstream systems)
- HR, Admissions, IAM responsibilities
- are social ids involved? Do you need a match-social-id-to-person-in-registry process?
- do sponsored (loosely-affiliated) & contractors use the same processes?
- is an external identity service involved?

- Tom: Identity matching is a registry function - receiving person data from multiple sources. Do other institutions see it as a different function?
- Ethan - person registry is also a source of record at UNC
- Is the person registry/identity matching part of provisioning or something that happens before?
- One of the competencies that a person registry needs to have is identity matching, whether it's part of the provisioning infrastructure or upstream
- How centralized is the institution's ERP
- May want to survey BTAA about scoring systems and matching rules - there may be a variety
- Karen - incoming students will use a guest account in the person registry and will link it to their institutional identity
- Tom - Madison is thinking about models where there's a low bar for creating a profile (that has an institutional or social credential associated). When a user establishes a role (student enrollment, employment, etc), we can provide the role owner (registrar, HR) a mechanism to bind the role to the user's profile, or we can use the fact that the role was established via an authenticated session with the user's profile to bind the role to the user. (Tom and Jon have been pondering ways to "prove" the logged-in session, since we have historical issues with sources guessing at identifiers instead of resolving them in a login.)
- Identity matching is not 'one size fits all,' but may be part of the provisioning process. Need to add to the identity provisioning portion of the survey

---

5. Credential provisioning

a. Password rules and policies

i. Describe the password policies you support with regard to complexity, length, and any dictionary checks. Include character classes supported in complexity checks. (Call nist) midPoint supports a wide veriety of checks, including character classes and length restrictions. Character classes are conveyed in regex like lists of characters, so sub members of classes can be excluded. https://wiki.evolveum.com/display/midPoint/Password+Policy

ii. Does your product support flexible password policy based on password length? For example support pass phrases but requiring additional character sets for shorter passwords. Not clear if midPoint supports an notion of "OR" on limits, documention states that "AND" is implied on multiple limits. midPoint does support scripted limits, so this could be done via scripting rather than configuration.

iii. Describe your support for passwords in multiple languages. I was not able to locate documentation for this, but don't see any reason character classes could not include non-english characters.

iv. Describe your products support for password expiration, including any support for flexible expiration based on grouping, assurance, or other factors such as password quality. Password expiration is a function of the maximum age stanza of the security policy. Security policies can be for organizational units, we are group structures, so flexible expiration could be handled there, or via scripting.

v. Describe how your product conveys password quality to end users. I do not see a configurable way to convey password quality to end uers.

vi. Describe how you product meets accessibility guidelines Surprisingly I was not able to find information on accessibility.

b. Initial password setting (credential activation?, initial login?)

i. Describe how your product assures initial password setting is being done by the appropriate authority, such as invitations, one time and/or short lived tokens etc. midPoint supports invitations via email and SMS with support for expiring invitations, and custom forms can be created to validate demographics.

ii. Describe your products support for terms of use and informed consent when getting a credential. Support for consent in the current version would require a custom form. midPoint is proposing consent for GDPR compliance in future versions https://wiki.evolveum.com/pages/viewpage.action?pageId=24675082

iii. What platforms are supported for end user devices setting initial and subsequent passwords, including any required technologies. End user interface is simple html/js/css and should be broadly supported.

iv. Describe any features your product has to deter attacks on unclaimed credentials. Invitation expiration.

v. Describe how your product handles multiple credential stores. As long as passwords are stored in an encrypted rather than hashed format, passwords can be synced via an resource connector.

c. Assignment of additional authentication factors

i. Describe your support for certificate based authentication. midPoint is spring security based, so a wide range of authentiction methods are supported including certificates.

ii. Describe your support for multifactor enrollment, specifying supported technologies and products, explicitly address U2F support. I don't find any explicit support.

iii. Describe any support you have for challenge response questions. Password reset documentation mentions support for security questions, but I haven't found further documentation.

iv. Describe any unlisted additional authentication factors, and any features that help user recognition such as image validation. Possible via custom forms.

v. How do you handle loss of a (perhaps only) two factor device, such as one time tokens Support for time based token expiration and re-issue.

d. Deprovisioning of credentials

i. Describe the states supported by your product for credentials, such as open, expired, disabled, locked/unlocked, security deny, etc.

ii. Describe any workflow available for deprovisioning, time based, approval based, and any attribute or membership checks that can be used for deprovisioning workflow.

iii. Describe any controls for sanity checks in your product to prevent accidental mass deprovisioning.

iv. Describe the administrative capabilities your product has for deprovisioning and deprovisioning intervention, include any delegation features.

v. Describe how your product handles deprovisioning of credentials w/r/t propagation to multiple credential stores.

In addition to the above, include documentation of your APIs related to all of the above functional areas.

6. Target Directories and Service Provisioning

a. Linking identities between directories or services
    i. Describe how your product links an identity in a source directory to the same identity in the target (and service?)
    ii. Are your user linkage attributes characterized as follows:
        1. Immutable
        2. Static
        3. Globally unique
    iii. What is the process of account matching if accounts already exist?
    iv. How flexible is customization of the IDM connector that provisions the account?
b. Communicating updates to target directories
    i. Describe the transport mechanism used for updating target directories and services
    ii. What protocols does your product support for provisioning of accounts (for example, SOAP/REST, LDAP, Messaging, JDBC)
    iii. What supported standards can your product use? (e.g., SCIM, LDIF, SPML, etc.)
    iv. Describe how your product batches or queues large quantities of updates.
c. Provisioning models: when to provision
    i. Describe how your product supports “Just-in-Time” provisioning model-- on demand provisioning when the user logs in.
    ii. Describe how you support the “Just-in-Case” provisioning model-- pre-provisioning accounts en masse
    iii. Workflow-based provisioning model
        1. Describe how your product handles automated workflows.
        2. Describe how your product handles manual intervention by an admin.
        3. Describe how your product supports end-user self-service workflows.
    iv. Do you support a threshold to alert for large quantity of updates?
d. Reconciliation
    i. How does your product ensure the target directory or service has state in sync with the source?
    ii. Does your product support rollback or transaction?
e. Fine-grained authorization
    i. Describe what authorization sources your product supports (e.g., Grouper, LDAP, Active Directory)
    ii. Is the same mechanism for account provisioning used for authorization provisioning?
    iii. What protocols for transmitting authorization does your product support? (e.g., Messaging, SOAP/REST, LDAP, JDBC)
    iv. What supported standards can your product use for authorization? (e.g., SCIM, LDIF, SPML, etc.)
    v. Does your product allow support for custom or proprietary interfaces for authorization?
    vi. How does your product links or maps internal groups and roles to external service-level fine-grained authorizations?
f. Deprovisioning and repatriation
    i. Describe how your product triggers deprovisioning of identities in a target directory or service.
    ii. Describe the process of deprovisioning identities in a target directory or service.
    iii. How is authorization removal handled for deprovisioned users?
    iv. Describe how your product supports repatriating a service account from institutional to personal.
    v. Do you support a threshold to alert for large quantity of changes?

8. Groups and roles

a. Types of groups
   i. Describe how your product supports a list of definable groups.
   ii. Describe how your product supports a hierarchy of groups (i.e., nesting and relationships between groups)
      1. What entities can be members of groups?
   iii. ?? What upstream data sources does your product readily support?
   iv. Do you support sets of groups associated together? (i.e., base, exceptions, includes/excludes)
b. Administration
   i. Describe delegated access administration features for group management.
   ii. How does your product deal with “orphaned” delegation? (When previous admins are no longer there.)
   iii. Do you provide APIs that would allow an external group and access management tool to drive your product’s groups and group memberships
   iv. Do you support attribute-based (ABAC) or role-based (RBAC) concepts to drive groups and group membership?
   v. Can groups have permissions associated with them?
   vi. What sort of attributes or metadata about groups are available?
   vii. Does your product support automatic review of roles/groups (attestation)?
c. Guidance for architecting
   i. How does your product expose or link groups or roles for fine-grained service authorizations?
   ii. How do you support Attribute-based access control?
   iii. How do you support Role-based access control?
      1. Are roles managed within the product?
   iv. How does your product define a default role or template (set of groups) for new entities?
   v. How are groups updated/kept in sync?
   vi. Describe synchronization mechanisms, i.e., changelog vs. full sync

10. Product Cost/Vendor Considerations

a. License

   i. What is your Software licensing cost structure (Enterprise vs non)? The software is open source. I don't believe there are separate versions. Enhancements are submitted through JIRA. Enhancements requests are driven by customers with support contracts.
   ii. If one of your license model is pay-per-active-account , how do you consider the following populations? : N/A
      1. Alumni users
      2. Guest users
      3. Extended Community users (Parents, Propsect Students , Applicants, Continuing Ed students ,ec..)
      4. Social identities that are linked to Idm system
   iii. Do you provide any Higher Ed discount ? N/A
b. Vendor Support and Maintenance (On going)
   i. What is your on-going service support contract structure ? There are two support subscription models (8x5, and 24x7).
c. Vendor Stability
   i. How long is your product being in the market ? The source code originated in 2011. There are 34 contributors, 49 releases and 18,500 commits. The project is active and there are daily commits.
   ii. How many Higher Ed clients do you have ? Three listed in their references (University of Illinois, Western University Canada, University of Selye).