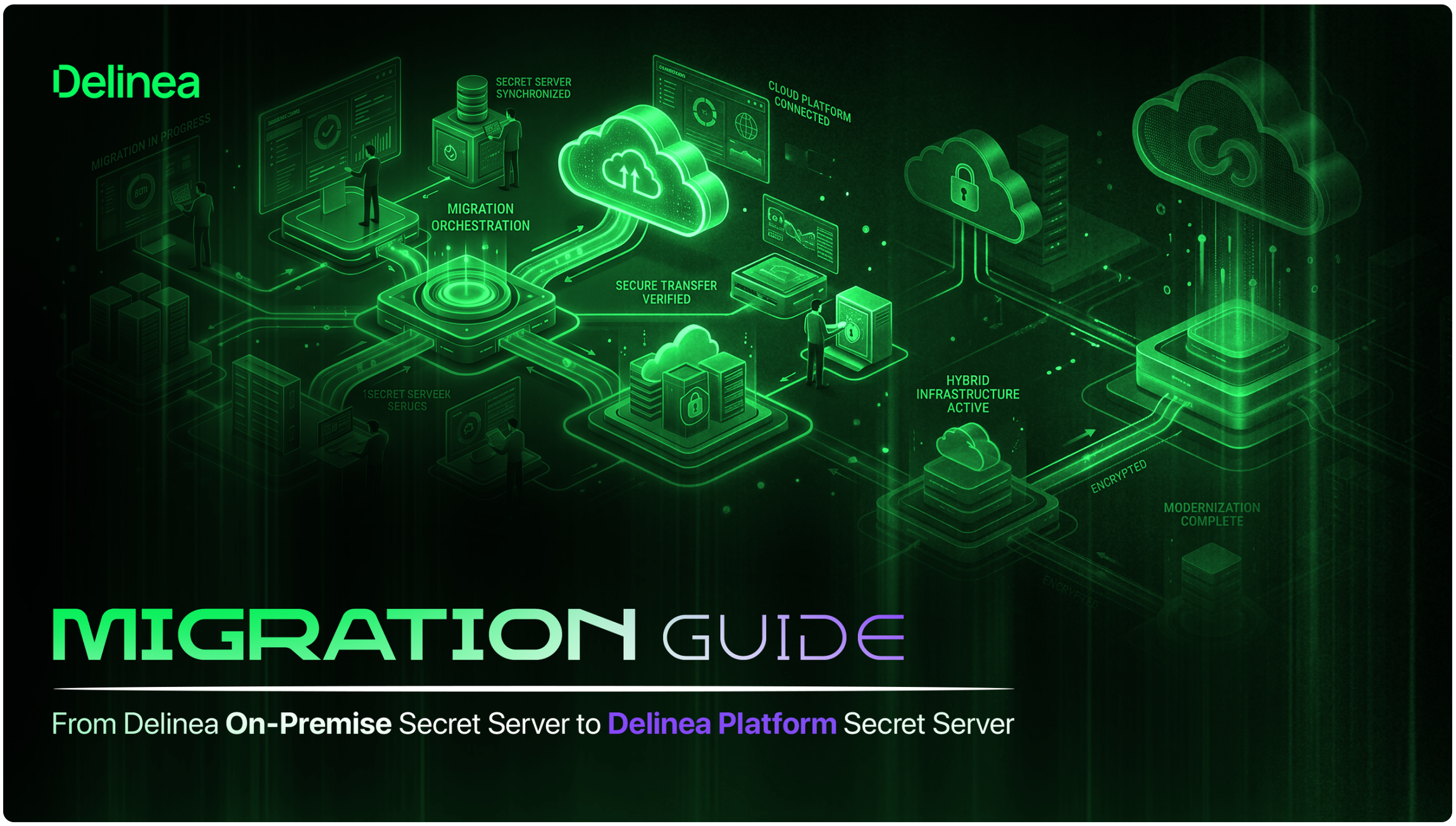

This expanded guide builds on the original outline by providing more in-depth explanations, additional considerations, best practices, and potential pitfalls for each step in migrating from Delinea Secret Server (on-premise) to the Delinea Platform (cloud-based Secret Server). The process requires careful planning to minimize risks like data loss, downtime, or security gaps. As before, this is based on official Delinea resources and general IT migration principles—always verify with Delinea's latest documentation, as features may evolve. Test everything in a non-production environment, and engage Delinea support or a professional services team for complex setups involving high volumes of data or custom integrations.

Prerequisites

These foundational requirements ensure a smooth migration by addressing access, data integrity, and compatibility upfront. Skipping any could lead to incomplete migrations or security vulnerabilities.

01

Access and Permissions:

You need full administrative privileges in the on-premise Secret Server, including database access for backups and exports. For the Delinea Platform, ensure you have tenant admin rights to create structures like folders and roles. If your organization uses role-based access control (RBAC), audit who has access to sensitive secrets during migration to prevent unauthorized exposure. Also, consider multi-factor authentication (MFA) enforcement on both sides to enhance security during the transition.

02

Backup:

Perform a comprehensive backup of the on-premise Secret Server, including the SQL database (using tools like SQL Server Management Studio), configuration files, and any custom scripts or extensions. Use Delinea's built-in backup features under Admin > Backup/Restore for a complete snapshot. Store backups in a secure, offsite location with encryption, and test restoration in a sandbox environment to confirm viability. This step is critical as a rollback mechanism if the migration encounters issues.

03

Compatibility Check:

Review your on-premise Secret Server version (e.g., ensure it's 10.9 or later for optimal tool support) against Delinea's migration compatibility matrix, available in their support portal. Check for deprecated features, like older proxy configurations, that might not directly translate to the cloud. If you're on an outdated version, plan an upgrade first to avoid data format mismatches.

04

Delinea Platform Setup

Provision your Delinea Platform tenant via the Delinea portal, selecting appropriate regions for data residency compliance (e.g., US, EU). Configure basic settings like email notifications and logging early on. If integrating with identity providers like Azure AD or Okta, set this up beforehand to streamline user imports later.

05

Tools:

Download Delinea's official migration utilities, such as the Secret Server Cloud Migration Tool or Bulk Operations scripts, from the customer portal. Familiarize yourself with the REST API documentation for custom exports. Ensure your migration workstation has secure tools like WinSCP for file transfers or PowerShell for automation.

06

Network and Security:

Establish secure channels for data transfer, such as VPN tunnels or SFTP with TLS encryption, to protect sensitive secrets in transit. Conduct a security review to comply with standards like SOC 2 or ISO 27001, including vulnerability scans on both environments. Define data classification to identify highly sensitive items that may require manual handling.

Delinea Platform Secret Server Initial Platform Setup

Before diving into the migration, properly setting up the Delinea Platform for Secret Server is essential. This section covers the initial provisioning and configuration steps, including establishing key components like identity providers, secret templates, policies, password requirements aligned with Group Policy Objects (GPO), breakglass accounts for emergencies, and adding additional platform modules. These setups ensure the platform is secure, compliant, and ready for imported data. Perform these in a test tenant first to validate configurations.

Provisioning the Tenant

Provisioning creates your cloud environment and grants initial access.

Contact Delinea sales or use the trial request form at delinea.com/contact-us to initiate a trial or production tenant.

Respond to the "Welcome to your Secret Server Cloud Trial on the Delinea Platform" email: Set up the initial administrator account, choose a hosting region (for compliance like GDPR), select a subdomain, allocate licenses, designate an alternate owner, and sign up for support.

Use the "Welcome to the Delinea Support Portal!" email to log in with the provided credentials.

Accept the invitation in the "You have been invited to the tenant-name tenant on Delinea Platform" email: Note the Cloudadmin username, accept the invite, bookmark the tenant URL, and set a strong password (auto-generated recommended) on first login.

Log in to the platform dashboard to verify access and begin configurations.

Establishing Identity Provider

Set up authentication to manage user access securely, including integration with external identity providers (IdPs) like Active Directory (AD) or federated services.

01

Install the Delinea AD Connector:

Navigate to Settings > Connectors, add a connector, download the 64-bit installer, copy the tenant URL and registration code, run the wizard with the code, and select domains for login.

02

Configure federation for IdPs

Integrate via the Federation Management section to enable on-the-fly user addition upon login (users appear in Access > Users after first sign-in).

03

Install the Delinea AD Connector:

Go to Settings > Authentication Profiles, define MFA challenges (e.g., SMS, FIDO2), avoiding requirements that block setup (e.g., don't require a challenge during enrollment).

04

Create identity policies:

Navigate to Identity Policies, add a policy with a unique name and description, enable it, assign to specific groups or globally (test small first), link to an authentication profile, and add rules (e.g., by IP or device).

05

Set up conditional access:

Create a "Disallow Login Policy" with "Deny platform authentication" as default, assign to blocked groups, and order policies (top-down evaluation) to ensure only allowed users can log in.

06

Configure additional settings:

Enable "Keep me logged in," set session lengths (1-24 hours for browser, 1-90 days for apps), allow IWA, enable federation for MFA, set password complexity, and configure self-service resets.

Setting Up Secret Templates

Secret templates define the structure for storing secrets, ensuring consistency.

01

Access the template designer:

Go to Admin > Secret Templates.

02

Customize or create templates:

Review defaults (e.g., AD Account with fields like domain, username, password), duplicate for modifications, and use descriptive names.

03

Configure settings:

Add file attachment fields, enforce naming patterns with regex (e.g., RESOURCE\ACCOUNT), enable password history, set password requirements (e.g., 16 characters with complexity), define expiration intervals (e.g., 30 days), and set up launchers (e.g., RDP with hidden passwords).

04

Best practices:

Deactivate unused templates, limit admin access via roles, allow per-secret overrides, and plan templates before user adoption to avoid conversions.

Creating Secret Policies

Secret policies enforce rules across secrets and folders for centralized management.

01

Navigate to Admin > Secret Policies.

02

Create a policy:

Click Create secret policy, enter name and description, enable it, and save.

03

Configure parameters:

Edit subtabs (e.g., Security, Access) to set rules like password changing or permissions.

04

Apply policies:

Assign to secrets or folders to enforce collectively, overlapping with templates where needed (e.g., for expiration or validation).

Configuring Password Requirements to Match GPO

Align password rules with organizational GPO for compliance.

01

Create requirements:

Go to Admin > Secret Templates > Password Requirements tab, click Create, set name/description, minimum length, character set, and no-no checks (e.g., prevent username, patterns, dictionary words).

02

Set advanced rules:

Edit validation for dictionary prevention, starting/ending characters (e.g., require symbols), character counts (min/max, repeating), and resolve conflicts.

03

Assign to templates:

In a template's Fields tab, edit the Password field and select the requirement.

04

Match GPO:

Manually mirror GPO rules (e.g., length, complexity) as direct sync isn't supported; use reports to check compliance and customize per-secret if needed.

Managing the Breakglass Account

Breakglass provides emergency access; use Unlimited Administration Mode or other strategies.

01

Assign roles:

Create a role with Unlimited Administrator permission (default in Admin role), assign to emergency users.

02

Enable mode:

Go to Admin > Configuration > Change Administration Mode, activate, and add notes; access all secrets/folders/reports, override checkouts.

03

Set up scenarios:

Export secrets to encrypted files for offline access, create resilient local accounts with RBAC and auditing, enable mobile app caching, or configure PCS agents for offline OTP MFA.

04

Best practices:

Use temporarily, monitor audits/alerts, log all actions, and mitigate risks like credential compromise with dual controls.

Adding Delinea Platform Modules

Extend functionality with modules like engines, PRA, or MFA.

01

Install Platform Engine:

For AD integration or PRA, go to Engine Management, create a site, and follow setup (required for on-prem features).

02

Add Privileged Remote Access (PRA):

Install engine with PRA capabilities, associate secrets, and launch sessions via RDP/SSH from Secret Server.

Delinea:

Expanded Migration Guide: From Delinea On-Premise Secret Server to Delinea Platform Secret Server

Delinea

03

Configure MFA:

Set up authentication profiles/policies as above, assign to users, and define corporate IP ranges or RADIUS.

04

Enable Continuous Identity Discovery (CID):

Go to Identity Posture > Checks to identify unvaulted credentials.

05

Integrate others:

Add via dashboard (e.g., Privilege Manager for just-in-time access), ensuring licenses and dependencies.

Step-by-Step Migration Process

01

Plan the Migration

- Assess your current on-premise setup: Conduct a thorough audit using Delinea's reporting tools to list all secrets, their dependencies, access logs, and usage patterns. Categorize by type (e.g., passwords, SSH keys, API tokens) and criticality. This helps prioritize migration waves and identify redundancies.
- Identify what to migrate: Review secrets for expiration dates or inactivity—archive or delete obsolete ones to reduce migration scope. Consider regulatory requirements; for example, PCI DSS might mandate retaining certain audit trails.
- Map differences: Compare features side-by-side; the Platform offers cloud-native benefits like automatic scaling and AI anomaly detection, but on-premise custom SQL queries might need rewriting as Platform scripts. Document any gaps, such as third-party plugins that aren't cloud-compatible.
- Set a timeline and rollback plan: Create a phased schedule (e.g., pilot with 10% of secrets, then full cutover). Include milestones for testing and define triggers for rollback, like if more than 5% of imports fail. Involve IT, security, and business teams to align on downtime windows, ideally during off-peak hours.

02

Export Data from On-Premise Secret Server

- Use the built-in export features or Delinea's migration tools: Start with the web interface for small exports (Admin > Secrets > Export), selecting formats like encrypted XML for security. For larger-scale, leverage the migration utility to automate.
- Export secrets: Filter by folders or tags to avoid overwhelming files. Include metadata like notes, custom fields, and history. Encrypt exports with a strong passphrase and store temporarily in a secure vault.
- Export configurations: Capture users via Admin > Users > Export, ensuring group mappings are included. Use API endpoints (e.g., /api/v1/users) for granular control over roles and permissions.
- For large datasets, use the Secret Server REST API or PowerShell scripts to automate exports: Script batch exports with throttling to prevent server overload. Handle pagination in API calls to fetch all records.
- Handle attachments and dependencies: Separately export files attached to secrets (via API or manual download). Note dependencies like linked heartbeats or remote password changers, exporting their configs to recreate in the cloud.

03

Prepare the Delinea Platform

- Log in to your Delinea Platform tenant: Use the unified dashboard to navigate to the Secret Server module. Enable any preview features if they align with your needs.
- Configure initial settings: Set up authentication integrations early, such as SAML for SSO, to match on-premise setups. Configure audit logging to capture all actions for compliance.
- Create necessary structures: Manually recreate folder hierarchies using the Platform's bulk create tools. Import or define roles and groups to mirror permissions, ensuring least-privilege principles are maintained.

04

Import Data to Delinea Platform Secret Server

- Use the Delinea migration utility if available or the platform's import tools: The utility often includes validation scripts to check data integrity before import.
- Import secrets: In the Secret Server module, use the Import wizard to upload files, mapping fields like "Username" or "Password" if formats differ. Handle conflicts by merging or overwriting based on rules.
- Import users and permissions: If AD-integrated, use the Platform's sync features for automatic user population. For custom users, use CSV imports and assign roles carefully to avoid privilege escalation.
- Reconfigure integrations: Recreate proxies (e.g., Distributed Engines) in the cloud, testing connectivity to on-premise resources. Update discovery rules for automated secret scanning.
- Validate imports: Run post-import scripts or reports to check for completeness, such as comparing secret counts. Audit for any encryption key mismatches.

05

Configure and Customize

- Update workflows and policies: Rebuild event pipelines for actions like secret expiration notifications. Test check-out policies with sample users to ensure enforcement.
- Integrate with other Delinea Platform modules: Link to Privilege Manager for just-in-time access or Connection Manager for secure sessions, enhancing overall PAM capabilities.
- Test integrations: Validate API endpoints (cloud URLs differ from on-premise), updating scripts with new authentication tokens. Simulate real-world usage, like CI/CD pipelines fetching secrets.

06

Test the Migration

- Perform end-to-end testing: Simulate full user journeys, from secret retrieval to rotation, using test accounts.
- Security audit: Use tools like vulnerability scanners to check for exposed secrets; review access logs for anomalies.
- User acceptance testing (UAT): Gather feedback on usability differences, such as the Platform's modern UI versus on-premise.
- Performance check: Benchmark response times for secret access, noting cloud benefits like reduced latency for global teams.

07

Go-Live and Cutover

- Schedule downtime if needed: Aim for zero-downtime with parallel running, gradually redirecting traffic.
- Switch endpoints: Update all clients (e.g., via configuration management tools like Ansible) to the new cloud API URLs.
- Monitor post-migration: Use the Platform's analytics dashboard for real-time metrics on usage and errors.
- Decommission on-premise: Securely wipe data from the old server, retaining archives for a defined retention period.

08

Post-Migration Best Practices

- Train users on the new interface and features: Offer webinars or guides highlighting cloud advantages like mobile access.
- Optimize for cloud: Enable features like auto-rotation and threat detection to maximize value.
- Regular backups: Configure automated snapshots with versioning for quick recovery.
- Support: Establish a monitoring routine and maintain a relationship with Delinea for updates and optimizations.

Challenges

Migrations to cloud platforms like Delinea can introduce several hurdles, particularly in enterprise environments with complex setups. Below are expanded details on common challenges, including their potential impacts and why they arise.

Delinea:

Expanded Migration Guide: From Delinea On-Premise Secret Server to Delinea Platform Secret Server

01

Data Volume:

In environments with thousands or tens of thousands of secrets (e.g., 10,000+ entries), exports and imports can become time-consuming and resource-intensive, leading to extended processing times, potential timeouts, or even partial data corruption if not handled properly. This is exacerbated by attachments, historical logs, or custom fields that inflate file sizes, straining network bandwidth during transfers and increasing the risk of incomplete migrations.

02

Custom Scripts and Integrations:

Many on-premise setups rely on bespoke scripts, plugins, or integrations (e.g., with legacy systems or custom APIs) that reference local paths, IP addresses, or on-premise-specific endpoints. These may not port directly to the cloud due to differences in API structures, authentication methods (e.g., shifting from basic auth to OAuth), or environmental variables, resulting in broken automation, failed workflows, or the need for significant redevelopment, which can delay the project and introduce bugs.

03

Compliance and Regulatory Issues

Organizations in regulated industries (e.g., finance, healthcare) must navigate strict requirements like GDPR for data privacy, HIPAA for health data protection, or PCI DSS for payment information. Challenges include ensuring data residency (e.g., keeping data in specific geographic regions), maintaining audit trails during the transition, and avoiding any temporary exposure of sensitive data in transit, which could lead to compliance violations, fines, or legal repercussions if not meticulously planned.

04

Costs:

Beyond the obvious subscription fees for the Delinea Platform, hidden costs can accumulate from data egress charges during large transfers, additional storage for backups, professional services for assistance, or downtime-related business impacts. Unexpected scaling needs in the cloud (e.g., higher-tier plans for performance) can also inflate budgets, especially if the migration uncovers inefficiencies in the on-premise setup that require extra optimization.

05

Downtime and Business Disruption:

Achieving minimal or zero downtime is challenging, particularly for 24/7 operations, as switching endpoints or reconfiguring integrations can cause temporary outages. User resistance to changes in the interface or processes can further complicate adoption, leading to productivity dips or increased support tickets.

06

Security Risks During Transition:

The migration window creates vulnerabilities, such as potential data exposure if exports aren't encrypted properly or if there's a misconfiguration in access controls during imports. Hybrid setups (running both on-premise and cloud temporarily) can introduce attack surfaces, like inconsistent patching or overlooked permissions overlaps.

Tips

To mitigate the above challenges and ensure a successful migration, follow these detailed tips, which include proactive strategies, tools, and best practices drawn from real-world experiences.

01

For Data Volume:

Break the migration into manageable phases, such as by department, secret type, or criticality level (e.g., start with non-sensitive test secrets). Use compression tools on exports (e.g., ZIP with encryption) to reduce transfer sizes, and employ parallel processing in scripts to speed up operations. Monitor system resources with tools like Performance Monitor on Windows servers to avoid overloads, and consider staging data in a secure intermediary storage like AWS S3 with temporary access policies.

02

For Custom Scripts and Integrations:

Conduct a code audit early using version control systems like Git to track changes. Refactor scripts incrementally in a development environment, testing against the cloud API sandbox provided by Delinea. Leverage migration tools that automate some conversions, and document all changes with comments for future maintenance. If possible, adopt cloud-native alternatives, like using Delinea's event pipelines instead of custom cron jobs.

03

For Compliance and Regulatory Issues:

Engage compliance experts or legal teams from the planning stage to map requirements. Use Delinea's built-in compliance reports and logging features to generate auditable trails. Opt for data residency options in the Platform setup, and perform dry runs with anonymized data to validate adherence. Tools like encryption key management services (e.g., Azure Key Vault) can help maintain control over sensitive elements.

04

For Costs:

Create a detailed cost model upfront, including estimates for data transfer (use calculators from cloud providers) and potential overages. Optimize by cleaning up redundant data pre-migration and selecting cost-effective Platform tiers. Negotiate with Delinea for migration credits or bundled services, and track expenses with budgeting tools to adjust as needed.

05

For Data Volume:

Implement a phased cutover with blue-green deployment strategies, where the cloud runs in parallel until validated. Communicate changes via change management processes, including training sessions and FAQs. Use automation tools like Terraform for infrastructure-as-code to quickly rollback if issues arise.

06

For Security Risks During Transition:

Enforce zero-trust principles, such as encrypting all data in transit and at rest using AES-256 standards. Conduct penetration testing on the migration setup and use Delinea's security features like anomaly detection post-migration. Limit access to migration tools with just-in-time privileges, and monitor logs in real-time with SIEM tools for any suspicious activity.

07

General Troubleshooting:

If issues arise, start with Delinea's knowledge base, support portal, or community forums for version-specific solutions. Search for error codes or symptoms, and provide detailed logs (e.g., API responses, timestamps) when opening tickets. Join Delinea user groups or webinars for peer insights, and consider hiring certified partners for hands-on help in complex scenarios.

In conclusion, migrating from Delinea’s on-premise Secret Server to the Delinea Platform requires a comprehensive, methodical approach to ensure a seamless transition with minimal risk. By following the detailed steps outlined in this guide, organizations can ensure data integrity, optimize security, and maintain operational continuity throughout the migration process. It’s essential to carefully plan each phase, from prerequisites and backups to testing and go-live strategies, while also considering potential challenges like data volume, custom integrations, and compliance issues. Adopting best practices such as phased migrations, leveraging Delinea’s tools, and engaging with professional services when necessary will mitigate risks and streamline the process. With thorough preparation, testing, and post-migration validation, this transition will not only improve security and performance but also set the stage for a more scalable, efficient cloud-based infrastructure. Always remember to consult Delinea’s latest documentation and support resources for up-to-date guidance and solutions to any emerging issues during the migration journey.