Using CredHub to Increase the Security of Your Platform
Dan Jahner, Senior Product Manager, Pivotal
The Next 30 minutes

• Why
• What
• How
• The Future
• Questions
Why create CredHub?
Leaked credentials can be catastrophic

Deloitte is a sitting duck: Key systems with RDP open, VPN and proxy 'login details leaked'

Equifax used the word 'admin' for the login and password of a database

OneLogin breached, hacker finds cleartext credential notepads
'Store your firewall password here' notes pillaged
By Darren Paul 31 Aug 2016 at 06:07

Hacking Slack accounts: As easy as searching GitHub
Bot tokens leaked on public sites expose firms' most sensitive business secrets.

93% of phishing emails are now ransomware
As of the end of March, 93 percent of all phishing emails contained encryption ransomware, according to a report released today.
Cloud Foundry uses _a lot_ of credentials

- autoscale-db-credentials
- autoscaling.broker_credentials
- autoscaling.encryption_key
- backup.prepare.backup_encryption_key
- bulk_api_credentials
- cc-db-credentials
- cloud_controller.db_encryption_credentials
- cloud_controller.encrypt_key
- cloud_controller.locket_client_cert
- cluster_health_user
- dashboard_credentials
- diego-db-credentials
- diego-instance-identity-intermediate-ca
- diego-instance-identity-root-ca
- diego.brain.cc_uploader_server_cert
- diego.brain.ssh_host_key
- diego.database.bbs_encryption_passphrase
- diego.database.locket_server_cert
- diego.database.silk_controller_server_cert
- diego.database.silk_daemon_client_cert
- doppler.doppler_tls_cert
- doppler.metron_tls_cert
- doppler.shared_secret_credentials
- doppler.syslogdrainbinder_tls_cert
- galera.sidecar_user
- haproxy_forward_tls.backend_ca
- internal_api_user_credentials
- ldap.server_ssl_cert
- locket-db-credentials
- loggregator_trafficcontroller.statsinjector_tls_cert
- loggregator_trafficcontroller.trafficcontroller_tls_cert
- mysql-backup-server-db-credentials
- mysql-bootstrap-db-credentials
- mysql-diag-agent-db-credentials
- mysql-metrics-db-credentials
- mysql-monitor-db-credentials
- mysql_app_usage_credentials
- mysql_admin_credentials
- mysql_backups.s3.access_key_id
- mysql_backups.scp.user/key
- nats.credentials
- network-policy-server-db-credentials
- nfs-broker-push-db-credentials
- nfs-volume-db-credentials
- nfs_server.blobostore_cert
- nfs_server.blobostore_secret
- notifications-db-credentials
- notifications.encryption_key
- properties.auctioneer_client_cert
- properties.auctioneer_server_cert
- properties.bbs_client_cert
- properties.bbs_server_cert
- properties.cloud_controller_client_cert
- properties.cloud_controller Mutual_cert
- properties.consul_agent_cert
- properties.consul_encrypt_key
- properties.consul_server_cert
- properties.loggregator_client_cert
- properties.mysql_backups.azure.storage_access_key
- properties.mysql_backups.gcs.service_account_json
- properties.mysql_backups.s3.secret_access_key
- properties.network_policy_agent_cert
- properties.network_policy_server_cert
- properties.networking.po_encryption
- properties.nfs_volume_driver_enable.idap_service_account_password
- properties.rep_client_cert
- properties.rep_server_cert
- properties.smtp_credentials
- properties.system_blobstore.external_secret_key
- properties.system_blobstore.external.azure.access_key
- properties.system_blobstore.external.gcs.secret_key
- properties.tps_client_cert
- properties.uaa.idap_credentials
- push-apps-manager-973907364123335069
- push-usage-service.secret_token
- router.route_services_secret
- routing-db-credentials
- silk-db-credentials
- smtp_crammd5_secret
- staging_upload_credentials
- status_credentials
- syslog_adapter.adapter_rlp_tls
- syslog_adapter.adapter_tls
- syslog_scheduler.scheduling_api_tls
- syslog_scheduler.scheduling_client_tls
- syslog_tls.ca_cert
- system_blobstore.external_access_key
- system_blobstore.external_gcs_access_key
- system_database.external.app_usage_service_username/password
- system_database.external.autoscale_username/password
- system_database.external.cardb_username/password
- system_database.external.diego_username/password
- system_database.external.locket_username/password
- system_database.external.netpolicyserver_username/password
- system_database.external.nfsvolume_username/password
- system_database.external.notifications_username/password
- system_database.external.routing_username/password
- system_database.external.silk_username/password
- uaa-db-credentials
- uaa.admin_client_credentials
- uaa.admin_credentials
- uaa.apps_manager_client_credentials
- uaa.apps.metrics_credentials
- uaa.apps.metrics_processing_credentials
- uaa.autoscale_client_credentials
- uaa.cc_client_credentials
- uaa.cc_routing_credentials
- uaa.cc_service_dashboards_credentials
- uaa.cloud_controller_username_lookup_credentials
- uaa.cloudcache_broker_client_credentials
- ...
Manually managing credentials is hard

Secure platform config

Insecure platform config
Common concerns should be automated

Secure platform config
What is CredHub?
Product Goals

• The central point of control for credential generation, storage, rotation, logging and access control in CF
Product Goals

- The **central point of control** for credential generation, storage, rotation, logging and access control in CF
Product Goals

• The central point of control for credential generation, storage, rotation, logging and access control in CF
Product Goals

• The central point of control for credential generation, storage, rotation, logging and access control in CF
Product Goals

• The central point of control for credential generation, storage, rotation, logging and access control in CF
Product Goals

- The central point of control for credential generation, storage, rotation, **logging** and access control in CF
Product Goals

• The central point of control for credential generation, storage, rotation, logging and **access control** in CF
Product Goals

• A first class, open source integration that specifically addresses the concerns of Cloud Foundry
  • Focus on priority use cases for Cloud Foundry users
  • Native integrations with CF components
  • Working with component teams to implement best practices for credential management
How does CredHub work?
BOSH deployment credentials

• Problems
  • Manifests must be managed with same controls as credentials
  • Complexity of manually generating credential values
  • BOSH stores manifests containing credentials
  • No straightforward way to do rotation
  • Credential access is not controlled or audited

• Solution
  • Director-recognized variable syntax in manifests: ((variable))
  • Director integration with CredHub to retrieve or generate variables whenever needed
Concourse pipeline credentials

• Problems
  • Pipeline configs must be managed with same controls as credentials
  • Concourse stores manifests containing credentials
  • No straightforward way to do rotation
  • Credential access is not controlled or audited

• Solution
  • Concourse-recognized variable syntax in manifests: ((variable))
  • Concourse integration with CredHub to retrieve variables whenever needed
Cloud Foundry service credentials

• Problems
  • Transiting credentials between components increases risk of disclosure
  • Access to service credentials is not controlled or logged
  • Leaking environment variables to logs increase risk of disclosure
  • Rotating credentials delivered via the environment require container recreation

• Solution
  • Alternative credential delivery workflow for service brokers and apps
  • Platform and Spring connector options to reduce app dev burden
Cloud Foundry service credentials
Cloud Foundry service credentials
Cloud Foundry service credentials
Cloud Foundry service credentials
Cloud Foundry service credentials
What’s next?
The wish list

• Automated CF credential rotation
• Application credential management workflows
• Pluggable encryption provider interface
• Encryption-as-a-Service
• Pluggable credential types
• …
Get Involved!

• Talk to me
  • Project office hours on Thursday @ 3:00pm

• Repos
  • github.com/cloudfoundry-incubator/credhub
  • github.com/cloudfoundry-incubator/credhub-cli

• Slack
  • Cloud Foundry #credhub