



# Securing Data At-Rest

**Cynthia McGuire**  
Senior Staff Engineer  
Sun Microsystems, Inc.



**2008  
Sun Labs  
Open House**



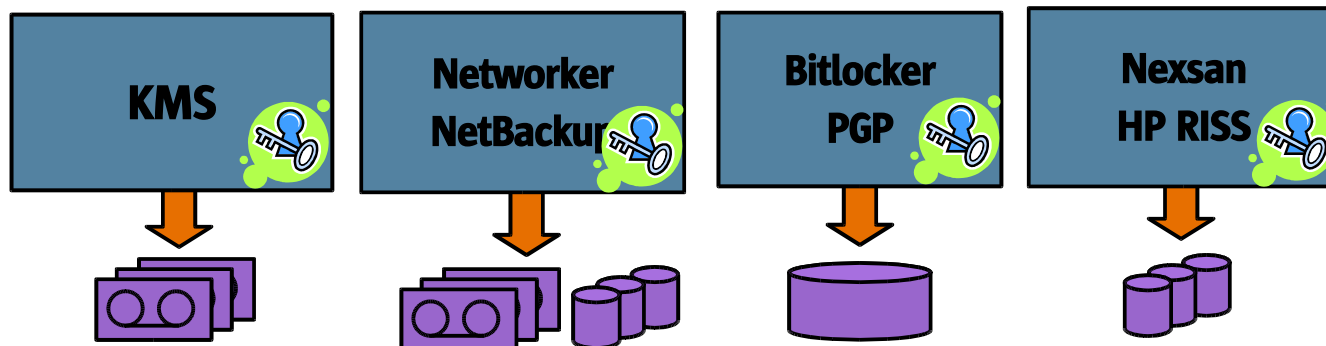
# Problem

- No cohesive solution for enterprise-class key management for encrypting stored data
  - > Ad-hoc solutions
    - Unbundled software, ISV option add-ons, and embedded in firmware
  - > OS and application tools are difficult to use
    - Configuration based on standards that are difficult to administer in a data center environment
    - Hard to keep track of keys
    - No auditing facilities
    - Misconfigs can lead to security breaches



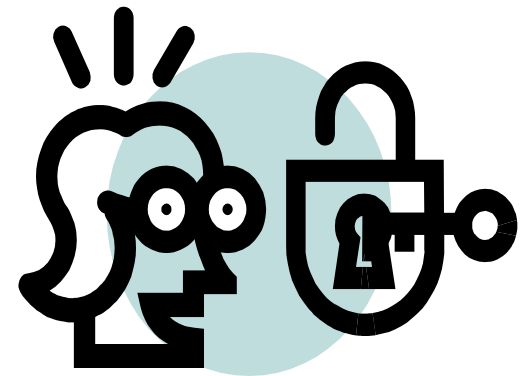
# Encryption in the Data Center

- No coordinated key management
  - > Independent keystores
  - > Hard to execute on compliance goals: retention periods, audit trails, restoration
  - > Hap-hazard administrative experience
- Varying levels of security: authentication, encryption strength and access control



# Who Cares?

- Customers need to secure at-rest data
  - > Compliance: HIPPA, PCI, GLBA, foreign and state regulations
  - > Secure sensitive data stored on and off site
  - > Secure encryption keys throughout data lifecycle, application and company changes
    - Employee turnover, application migration, and data relocation
- Customers need to have transparent access to encrypted data
  - > Quick access to clear-text data
    - Discovery and record retrieval
  - > Long term access to keys



# Encryption Strategies

- Host-based encryption
  - > Data encrypted/decrypted by the application or operating environment or application during creation or storage time
  - > Application-specific key management
    - Filesystems, e-mail servers, archive managers, back-up utilities
  - > High-level of security: data encrypted throughout lifecycle
  - > Can add compression and checksumming at same time

# Encryption Strategies

- Host-based encryption
  - > Processing at host can be expensive
  - > Difficult to manage data once encrypted: meta-data lost, can not compress after encryption
  - > Software used to encrypt must not change

# Encryption Strategies

- Appliance-based Encryption
  - > Data encrypted/decrypted by an in-band appliance
  - > Centralized key management
  - > Can add compression and checksumming at same time
  - > Off-host processing
  - > Mid-level of security
    - Data is encrypted mid-lifecycle
  - > Requires additional hardware that can be shared amongst several hosts

# Encryption Strategies

- Device-base Encryption
  - > Data encrypted/decrypted at the device
  - > Device-specific key management
  - > Can add compression and checksumming at same time
  - > Processing at device
  - > Lower-level of security: data encrypted at end device
  - > Compatibility problems with back-up utilities
  - > Requires special hardware

# Point Solutions

- Vendor-specific key management and encryption throughout the storage hierarchy
  - > Keys and encrypted data managed independently
    - Back-up/Recovery:
      - NetBackup, BakBone, Networker, PGP
    - Content Addressable Storage
      - HP RISS, HDS Archiva, Nexsan Assureon

# Point Solutions

- NetApp DataFort and Lifetime Key Manager
  - > Centralized key management and encryption across the data center
  - > Separate appliance and software: not integrated with mainline hardware or software products

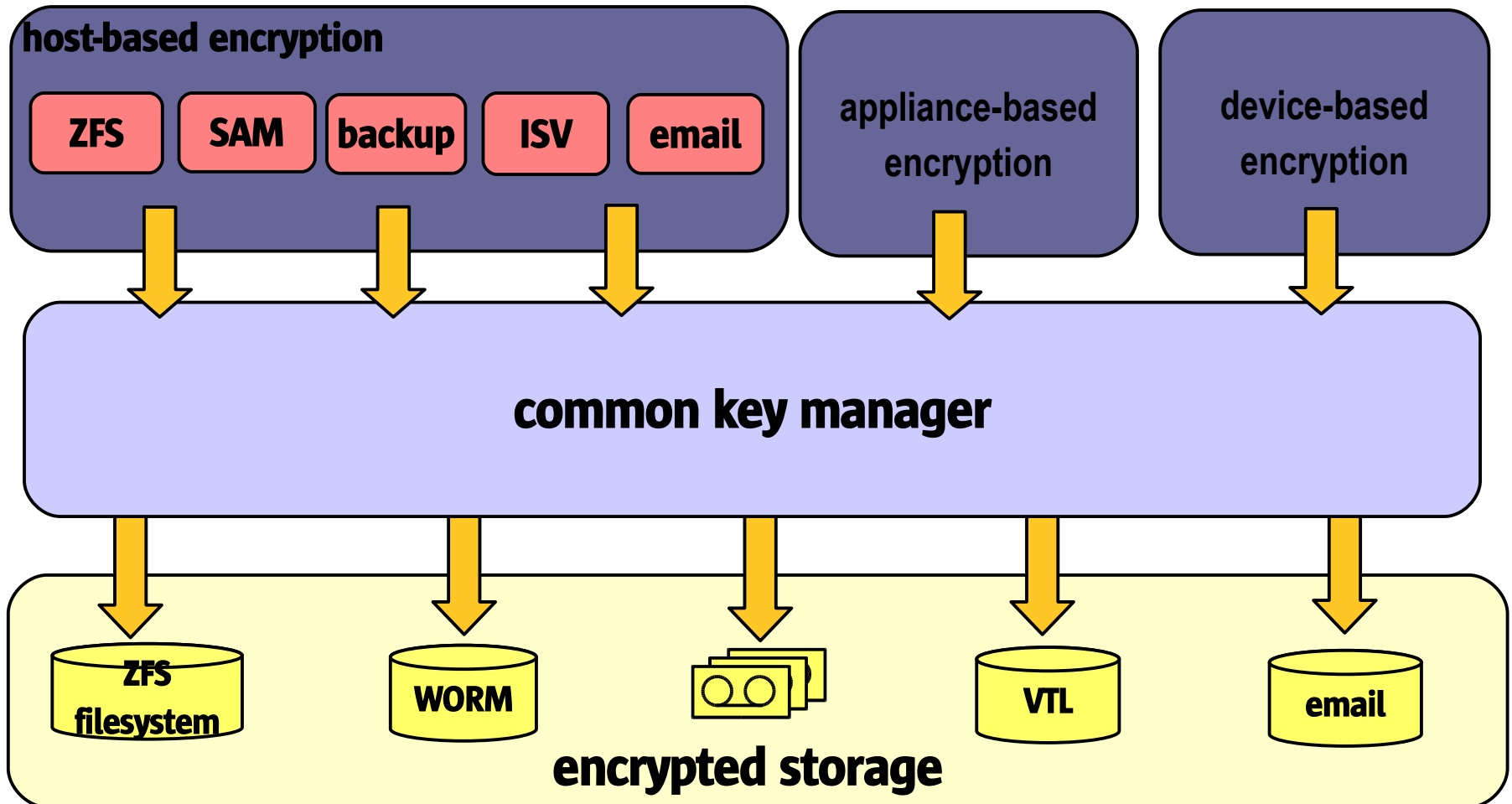
# The Strategy

- Opportunity to define a common key management strategy for storage products for encrypting data at-rest
  - > Leverage a single code base for different encryption software
  - > Build a distributed or consolidated key manager based on configuration options
  - > Share keys between a wide range of applications and products

# The Strategy

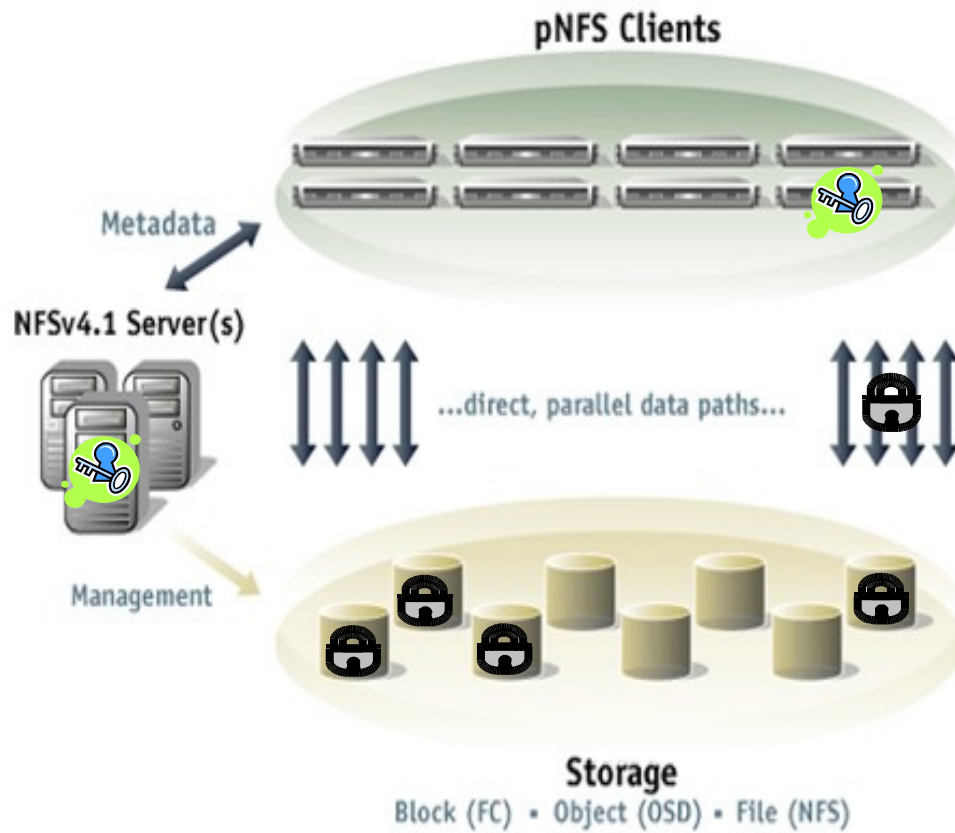
- Important to allow encryption at different levels in the storage hierarchy to meet business goals
- Build encryption functionality into storage technologies
  - > ZFS, next generation NAS and SAM, pNFS, VTL and tape, and e-mail server

# A General Approach to Key Management



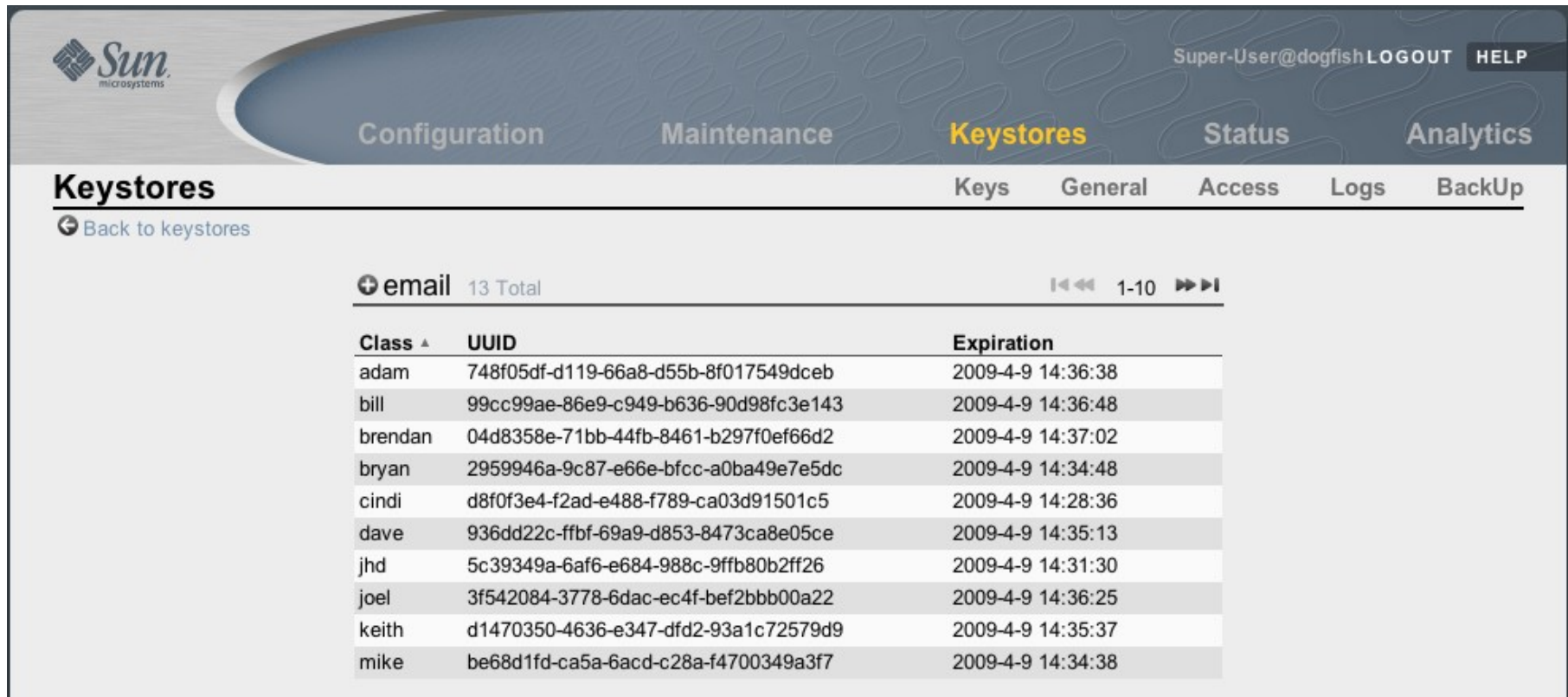
**With different deployment options...**

# Host-based



- Encryption possible at different levels
  - > Client: optimum security
  - > Server: optimum leverage
- Key management may be delegated or distributed
  - > Server: administrative control
  - > Client: user control

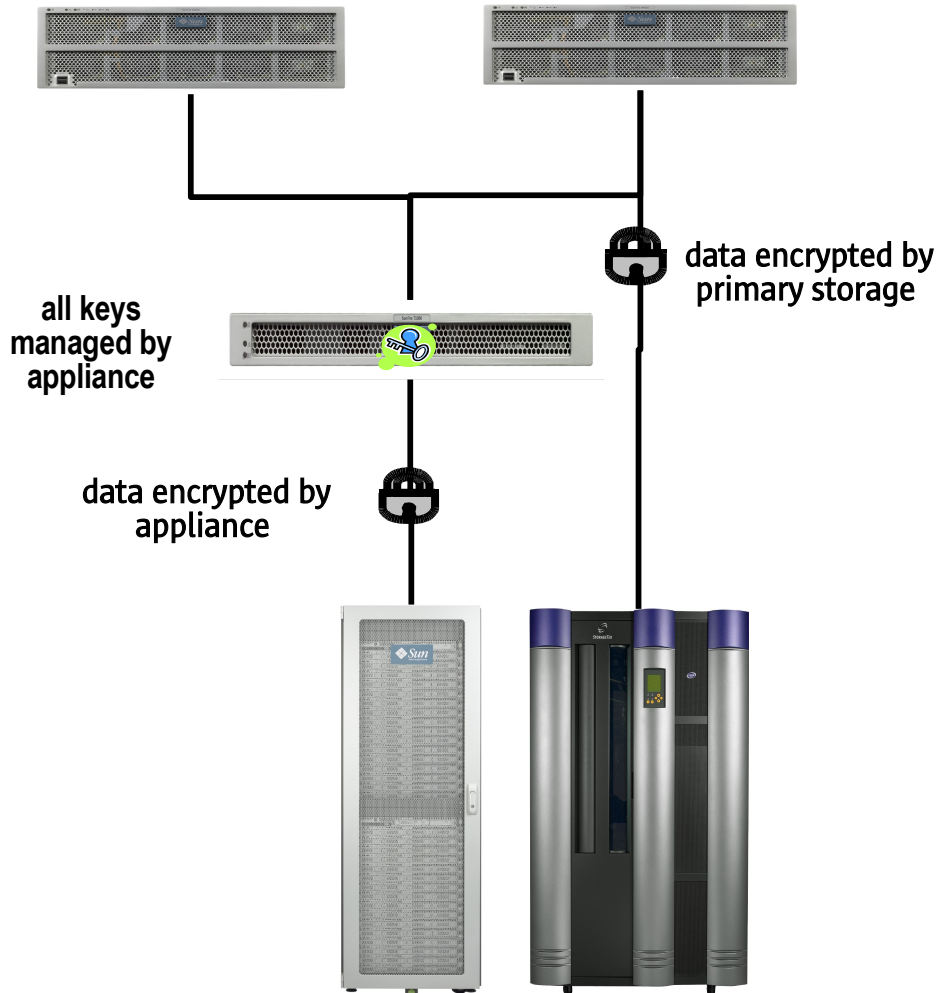
- Encryption at e-mail client
  - > optimum security
- Key management delegated to server
  - > administrative control



The screenshot shows the Sun Keystores web interface. At the top, there is a navigation bar with the Sun logo on the left and user information 'Super-User@dogfish LOGOUT' and a 'HELP' button on the right. Below this is a secondary navigation bar with tabs for 'Configuration', 'Maintenance', 'Keystores' (which is highlighted in yellow), 'Status', and 'Analytics'. Under the 'Keystores' tab, there are sub-tabs for 'Keys', 'General', 'Access', 'Logs', and 'BackUp'. The main content area is titled 'Keystores' and includes a link 'Back to keystores'. Below this, there is a section for '+ email' with '13 Total' items and pagination controls showing '1-10'. A table lists the keys with columns for 'Class', 'UUID', and 'Expiration'.

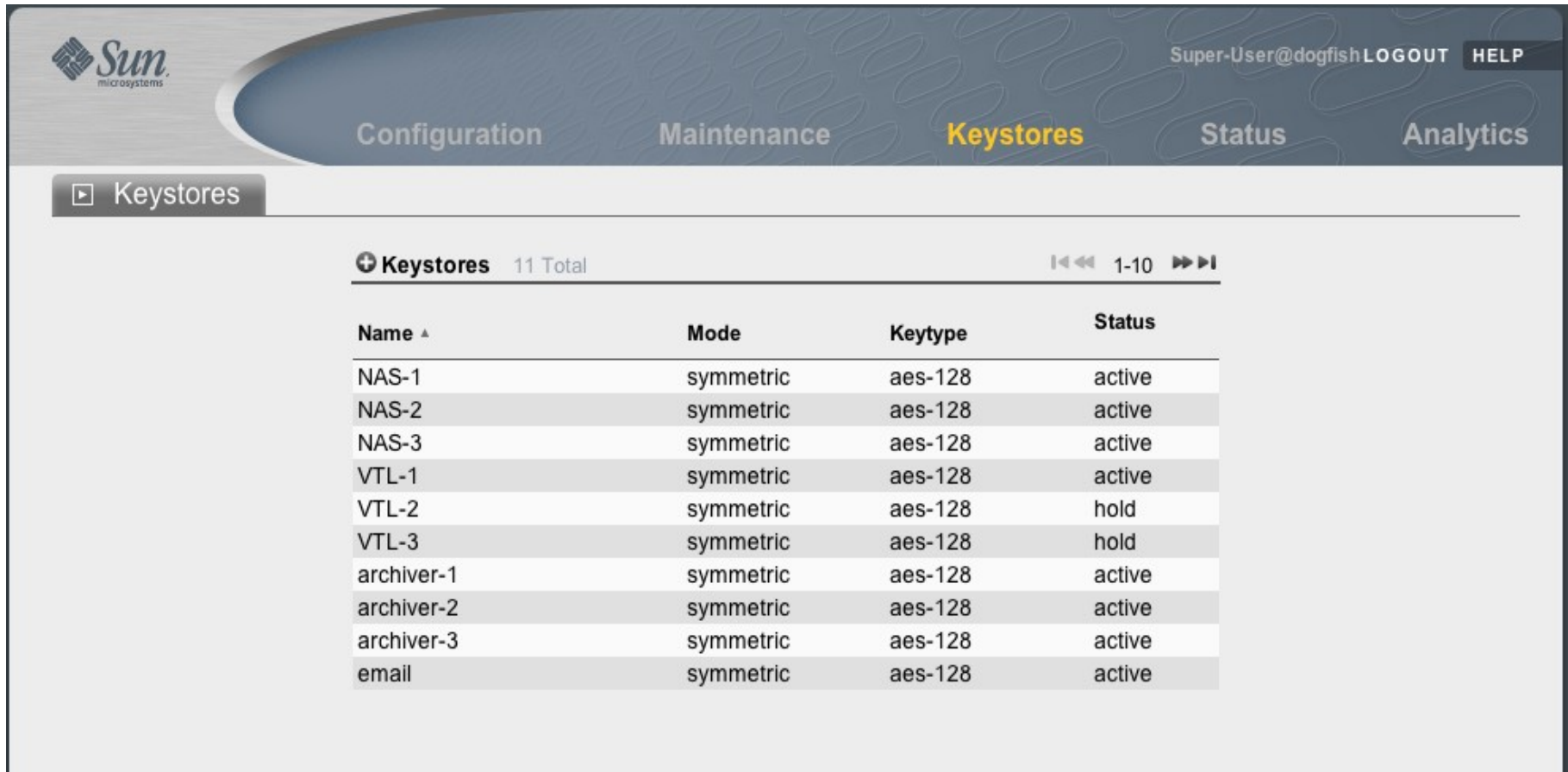
| Class ^ | UUID                                 | Expiration        |
|---------|--------------------------------------|-------------------|
| adam    | 748f05df-d119-66a8-d55b-8f017549dceb | 2009-4-9 14:36:38 |
| bill    | 99cc99ae-86e9-c949-b636-90d98fc3e143 | 2009-4-9 14:36:48 |
| brendan | 04d8358e-71bb-44fb-8461-b297f0ef66d2 | 2009-4-9 14:37:02 |
| bryan   | 2959946a-9c87-e66e-bfcc-a0ba49e7e5dc | 2009-4-9 14:34:48 |
| cindi   | d8f0f3e4-f2ad-e488-f789-ca03d91501c5 | 2009-4-9 14:28:36 |
| dave    | 936dd22c-ffbf-69a9-d853-8473ca8e05ce | 2009-4-9 14:35:13 |
| jhd     | 5c39349a-6af6-e684-988c-9ffb80b2ff26 | 2009-4-9 14:31:30 |
| joel    | 3f542084-3778-6dac-ec4f-bef2bbb00a22 | 2009-4-9 14:36:25 |
| keith   | d1470350-4636-e347-dfd2-93a1c72579d9 | 2009-4-9 14:35:37 |
| mike    | be68d1fd-ca5a-6acd-c28a-f4700349a3f7 | 2009-4-9 14:34:38 |

# Appliance-based



- Centralized key management
  - > Centralized and secure keystores
  - > Centralized audit logs
- Common appliance look and feel
- Optional HA configurations
- Client has option to encrypt data bypassing appliance

- Keys centrally managed at appliance
- Distributed to encryption clients



Super-User@dogfish LOGOUT HELP

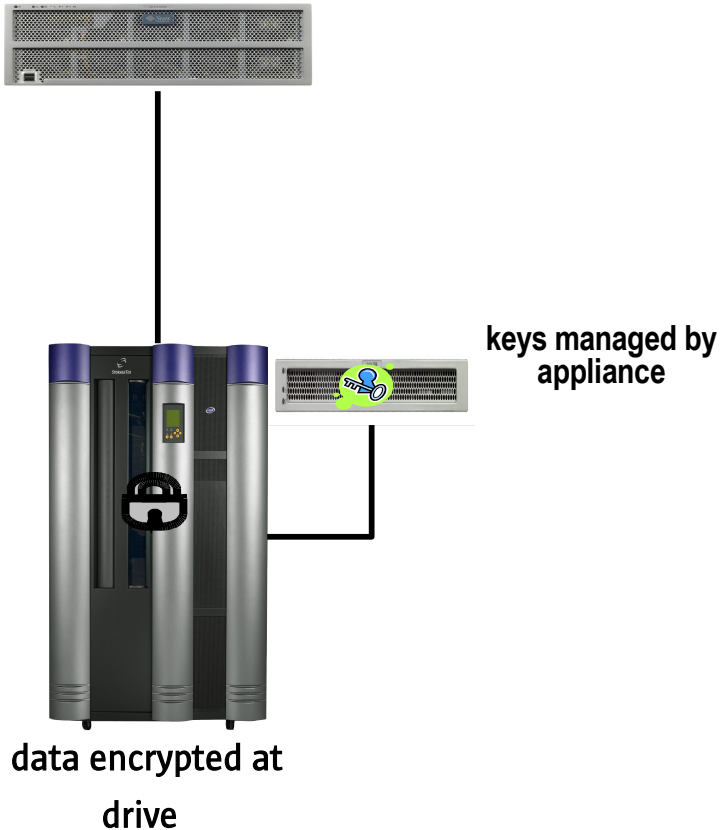
Configuration Maintenance **Keystores** Status Analytics

Keystores

Keystores 11 Total 1-10

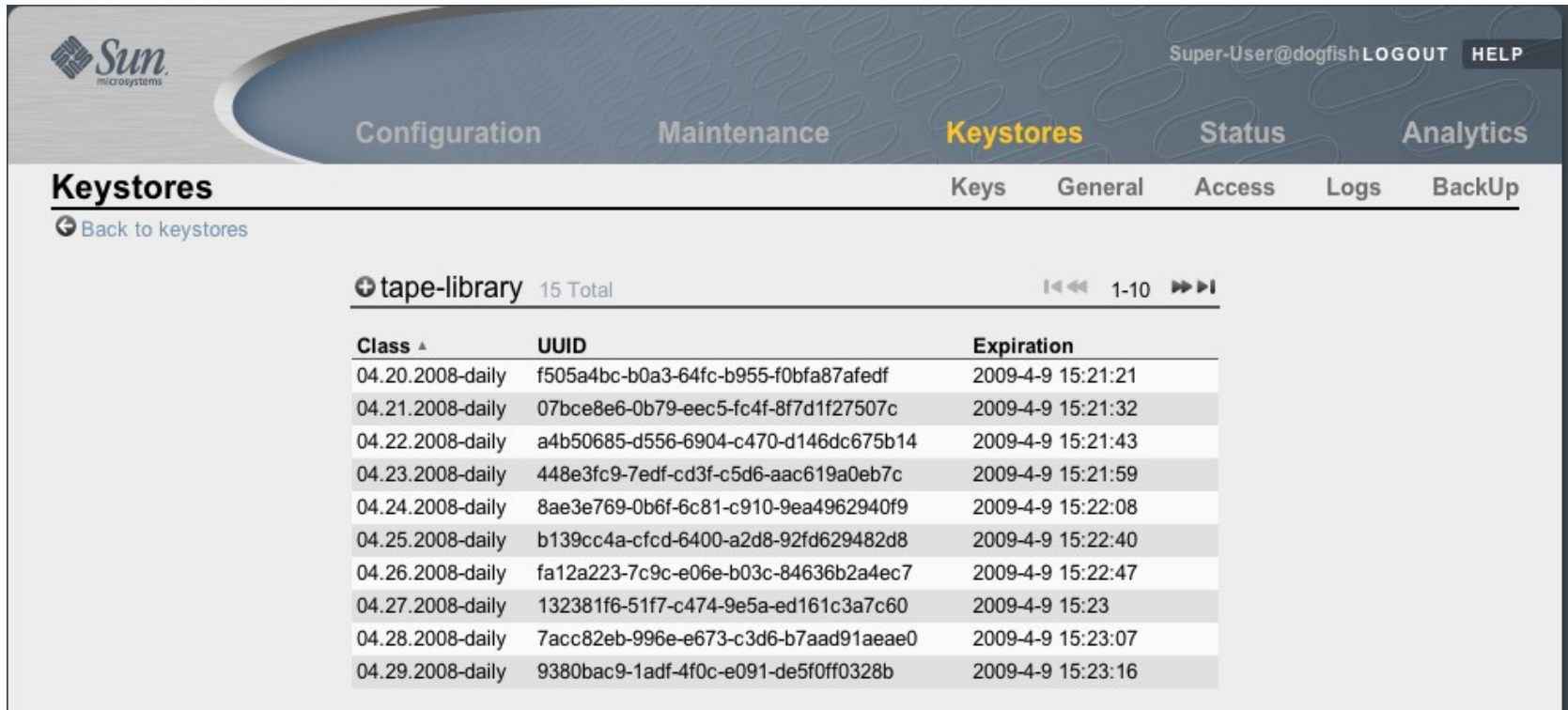
| Name ^     | Mode      | Keytype | Status |
|------------|-----------|---------|--------|
| NAS-1      | symmetric | aes-128 | active |
| NAS-2      | symmetric | aes-128 | active |
| NAS-3      | symmetric | aes-128 | active |
| VTL-1      | symmetric | aes-128 | active |
| VTL-2      | symmetric | aes-128 | hold   |
| VTL-3      | symmetric | aes-128 | hold   |
| archiver-1 | symmetric | aes-128 | active |
| archiver-2 | symmetric | aes-128 | active |
| archiver-3 | symmetric | aes-128 | active |
| email      | symmetric | aes-128 | active |

# Device-based



- The same hardware
- The same code base
- Appliance integrated into storage device enclosure
  - > tape, library or VTL
- Encryption may be off loaded to appliance

- Device dedicated encryption
- Key manager embedded within the tape library chassis



The screenshot shows the Sun Keystores web interface. At the top, there is a navigation bar with the Sun logo, the user 'Super-User@dogfish', and a 'LOGOUT' button. Below the navigation bar are tabs for 'Configuration', 'Maintenance', 'Keystores' (which is active), 'Status', and 'Analytics'. Under the 'Keystores' tab, there are sub-tabs for 'Keys', 'General', 'Access', 'Logs', and 'BackUp'. A 'Back to keystores' link is visible. The main content area shows a table of keys for the 'tape-library' class, with 15 total keys. The table has columns for 'Class', 'UUID', and 'Expiration'. The keys listed are for dates from 04.20.2008 to 04.29.2008, all with an expiration date of 2009-4-9.

| Class ^          | UUID                                 | Expiration        |
|------------------|--------------------------------------|-------------------|
| 04.20.2008-daily | f505a4bc-b0a3-64fc-b955-f0bfa87afedf | 2009-4-9 15:21:21 |
| 04.21.2008-daily | 07bce8e6-0b79-eec5-fc4f-8f7d1f27507c | 2009-4-9 15:21:32 |
| 04.22.2008-daily | a4b50685-d556-6904-c470-d146dc675b14 | 2009-4-9 15:21:43 |
| 04.23.2008-daily | 448e3fc9-7edf-cd3f-c5d6-aac619a0eb7c | 2009-4-9 15:21:59 |
| 04.24.2008-daily | 8ae3e769-0b6f-6c81-c910-9ea4962940f9 | 2009-4-9 15:22:08 |
| 04.25.2008-daily | b139cc4a-cfcd-6400-a2d8-92fd629482d8 | 2009-4-9 15:22:40 |
| 04.26.2008-daily | fa12a223-7c9c-e06e-b03c-84636b2a4ec7 | 2009-4-9 15:22:47 |
| 04.27.2008-daily | 132381f6-51f7-c474-9e5a-ed161c3a7c60 | 2009-4-9 15:23    |
| 04.28.2008-daily | 7acc82eb-996e-e673-c3d6-b7aad91aeae0 | 2009-4-9 15:23:07 |
| 04.29.2008-daily | 9380bac9-1adf-4f0c-e091-de5f0ff0328b | 2009-4-9 15:23:16 |

# Laptop



data encrypted on laptop



keys held at central office

- Data encrypted on the laptop using filesystem encryption
- Keys stored at the central office key manager
- Automatic secure communication to authenticate user and unlock data
- Access to data not allowed without authentication to central office
- Keys never stored on laptop or take-along device

# Key Manager Features

- Common OpenSource infrastructure and API for OS, application and hardware vendors
- Built on OpenSSL libraries for portability
  - > Compliance: FIPS-140-2, PKCS
- Audit log for keystore admin operations
- Distributed key managers for HA
- Ephemerization mode for assured delete of keys and encrypted data

# Key Manager Features

- Secure authentication and communication between remote key managers and consumers
- Common OpenSource infrastructure and API for OS, application and hardware vendors
- Built on OpenSSL libraries for portability
  - > Compliance: FIPS-140-2, PKCS

# Key Manager Features

- Ability to manage multiple keystores
  - > Configurable key type and strength
    - asymmetric/symmetric
  - > Key classification bindings
    - Retention period, organization, policy
    - Permits greater sharing of keys and fewer keys to manage
  - > Per-key UUID
  - > Configurable keystore locations
    - Filesystem, USB device, crypto hardware
  - > Keystore replication, back-up and recovery



**Cynthia McGuire**

cindi@sun.com



**2008  
Sun Labs  
Open House**

