ORACLE

AUTONOMOUS DATABASE

LEARNING LOUNGE

Multicloud, scalable and fault-tolerant key management with Oracle Key Vault

Autonomous Database Learning Lounge

Hosted by Marcos Arancibia

Autonomous Database Product Management

Agenda

Peter Wahl

Topics

- Oracle engineered Oracle Key Vault to deliver performant, fault-tolerant, and flexible encryption key management for Transparent Data Encryption (TDE), part of Oracle Advanced Security.
- Key Vault has been purpose-built to support all database deployment options, including Autonomous Database.
- An Oracle Key Vault cluster can be deployed in several environments, including in OCI from the Oracle Cloud Marketplace, in AWS, in Azure or GCP, and even on-premises; or stretched across all those on-prem and cloud boundaries, providing continuous cross-cloud-and-on-prem key availability, purpose-built for Oracle Transparent Data Encryption.

Q&A

- **Product Managers will answer any questions**

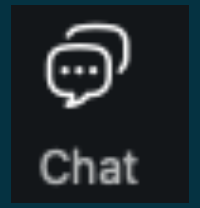
Before we begin...

This session is for you !!!

Ask your questions using **Q&A**

Product Managers are monitoring your questions

We will share links in **Chat**



The recording will be made available in a few days at
oracle.com/goto/adb-learning-lounge

Important links to bookmark

Links to get you started and to keep up to date with Autonomous Database

1. New Get Started page:
   bit.ly/adb-get-started

2. Join us:
   LinkedIn bit.ly/adb-linkedin-grp
   @AutonomousDW

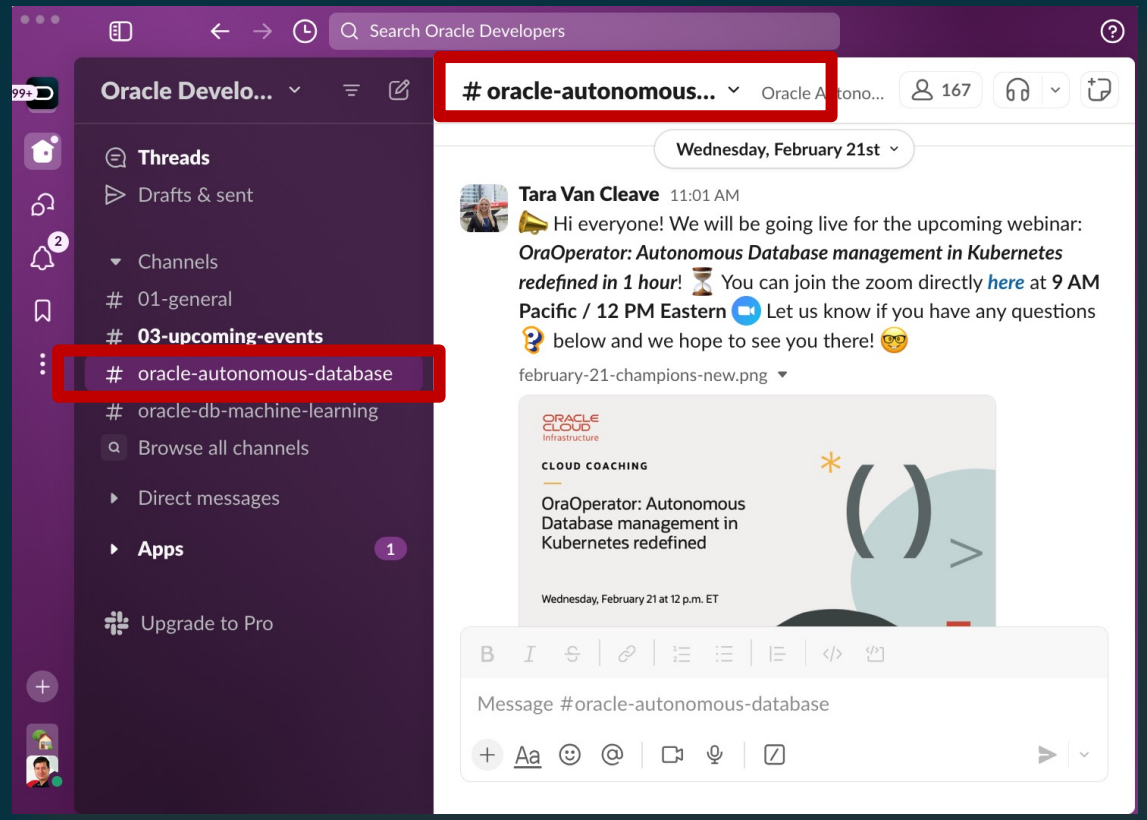
3. Got a question?
   We are on stackoverflow
   bit.ly/adb-stackoverflow

Join us on Developers Slack
(search #oracle-autonomous-database)
bit.ly/odevrel_slack (odevrel_slack)

Join our External Slack

STEP 1: bit.ly/odevrel_slack (odevrel_slack)

STEP 2: search for #oracle-autonomous-database at the top and click on the Channel



Speaker

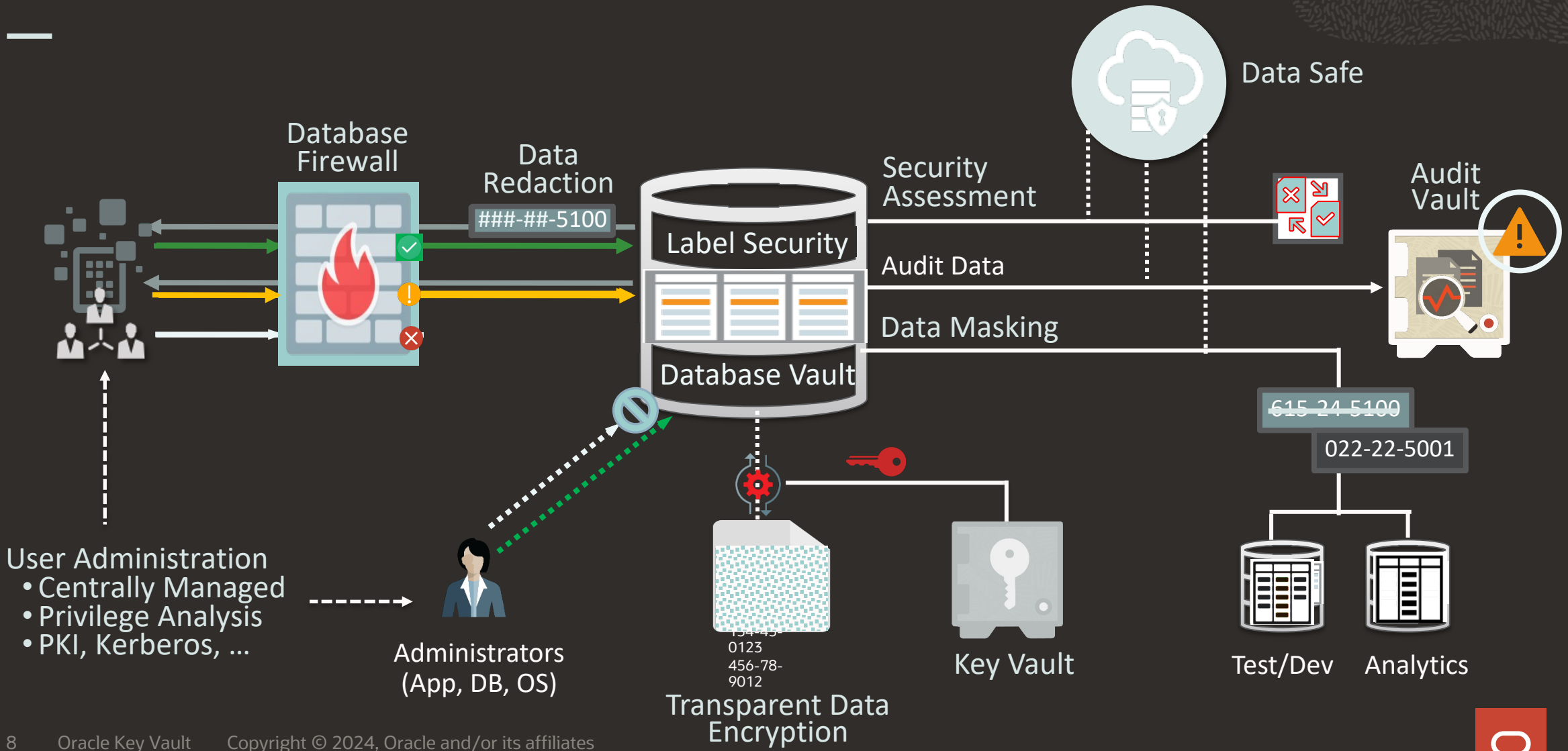
Peter Wahl

Insights into Data Encryption and Key Management

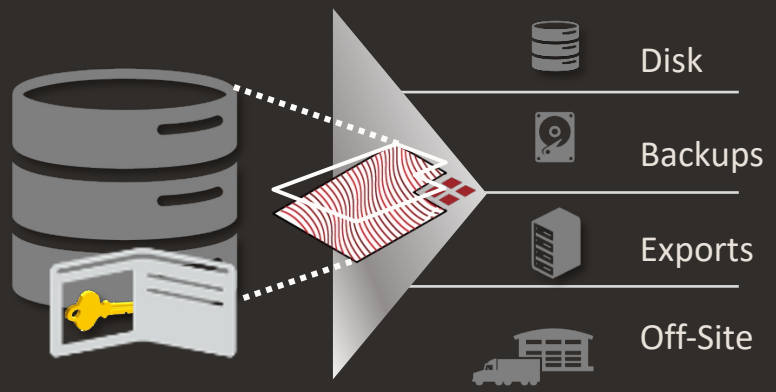
Peter Wahl

Senior Principal Product Manager
Encryption, Key and Secrets Management

Oracle Database Maximum Security Architecture



Encrypt data-at-rest with Transparent Data Encryption



- Encrypt tablespaces or columns
- AES128, AES192, AES256
- Requires no application changes
- Very low performance overhead
- On-line/off-line migration options
- Key Management with Wallets or Key Vault
- Integrated with Oracle technologies
  - Exa*, Compression, ACFS, Data Guard, GoldenGate, DataPump, Multitenant
  - Fusion Applications, eBusiness Suite, PeopleSoft, JD Edwards, SAP, …

Block **out-of-band** access to data-at-rest everywhere

Continued TDE innovations

Oracle Database 11.2.0.4, 12.1.0.2

- OFFLINE tablespace encryption
- Encrypt new tablespaces by default

Oracle Database 12.2.0.1

- ONLINE tablespace encryption & re-key
- ARIA, SEED and GOST encryption algorithms
- Separation of duty: Hide keystore password from DBAs

Oracle Database 18c

- `WALLET_ROOT` replaces dependency on `sqlnet.ora`
- Bring your own key (BOYK) for wallet-based TDE deployments
- Encrypt sensitive data in data dictionary tables
- RMAN: restore|duplicate as encrypted|decrypted

Continued TDE innovations

Oracle Database 19c

- Choose DB default algorithm
- Encrypt SYSTEM, SYSAUX, TEMP, and UNDO tablespaces.
- Encrypt LOB locator signature keys
- From 19.14: Isolated PDBs for everyone(*), everywhere(*)
- From 19.16: “split TDE”
- From 19.19: Re-key cloned/ relocated PDBs upon arrival

Oracle Database 21c

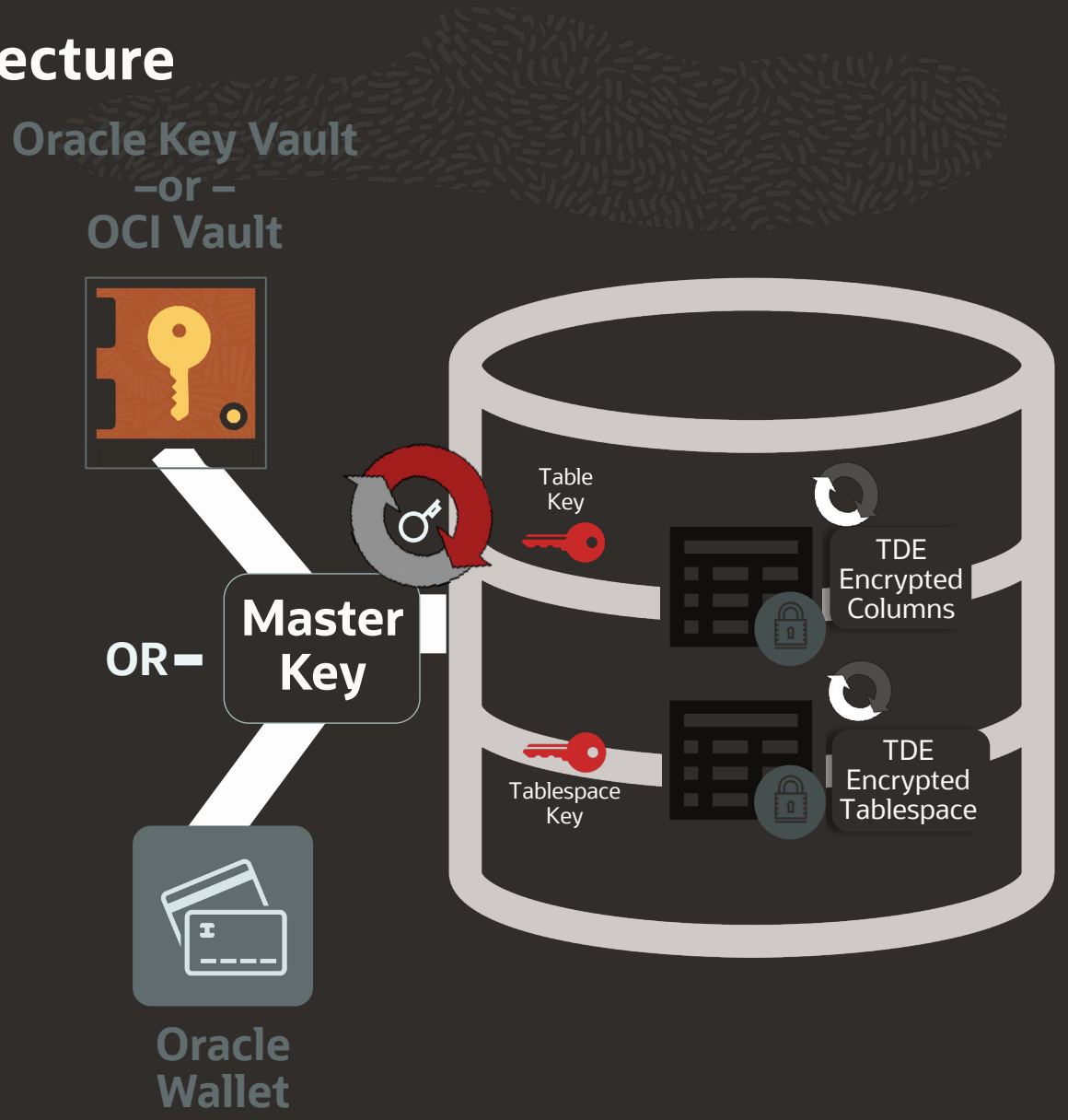
- Database Vault command rules for `administer key management` commands
- Database configuration assistant (`dbca`) creates encrypted databases
- New location for OKV’s PKCS#11 library allows upgrades without database restart

Oracle Database 23ai

- New cipher mode XTS replaces CFB
- AES256 default for TDE column and tablespace encryption

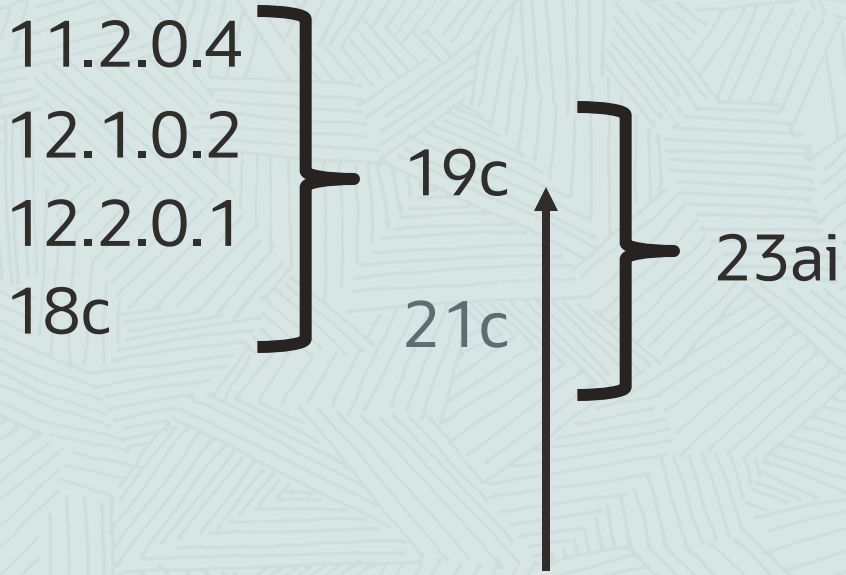
Transparent Data Encryption key architecture

- Two-tier encryption key
  - Data Encryption Key (Table or Tablespace Key)
  - Key Encrypting Key (Master Key)
- Data encryption keys are created and managed by TDE automatically
- The master encryption key encrypts the data encryption keys
- The master key is stored outside of the database
  - Encrypted Oracle wallet (on the server)
  - External key management system



Upgrade Considerations

Upgrade paths:



Mandatory: Use WALLET_ROOT and TDE_CONFIGURATION
Re-key tablespaces to AES (any length)
Otherwise: Upgrade pre-checks will fail

Centralized key management

Advantages

- Management at scale
- Encryption keys separate from the servers
- Easier to share keys across instances, standby databases, etc.
- Keys can be managed, backed up and recoverable

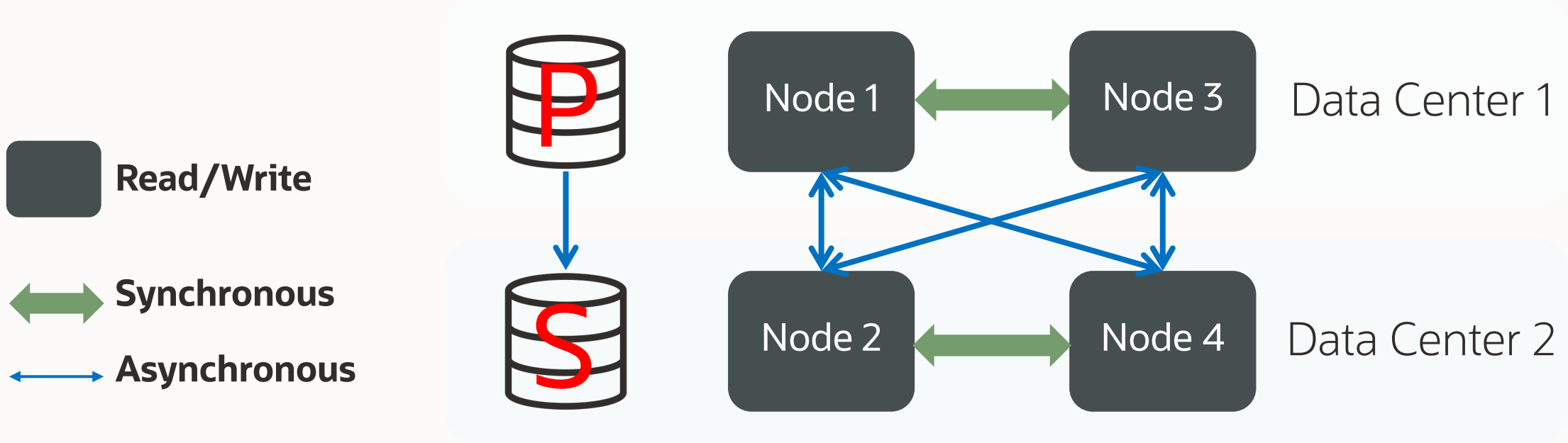
Requirements

- Keys secure from disclosure
- High availability
- Zero loss
- Scalable to 1,000s of databases
- Fast response times

Positioning Oracle key management solutions

	Oracle Key Vault	Cloud-Native key management
Oracle Databases Supported	• On premises, in-compute, third-party clouds: ExaDB-C@C, ADB-C@C; **OCI, Azure, GCP, AWS: ExaDB-D, ADB-D, ADB-S**	• Isolated key management services native to each cloud provider
Deployment	• On dedicated hardware, VMs, and in-compute on OCI and third-party clouds	• Cloud service
Third party cloud support	• Can be deployed in Azure, GCP, AWS	
HSM integration	• Supported as root-of-trust	--
Hold your own key (HYOK)	• By default	• OCI: Through integration with 3rd party HSM

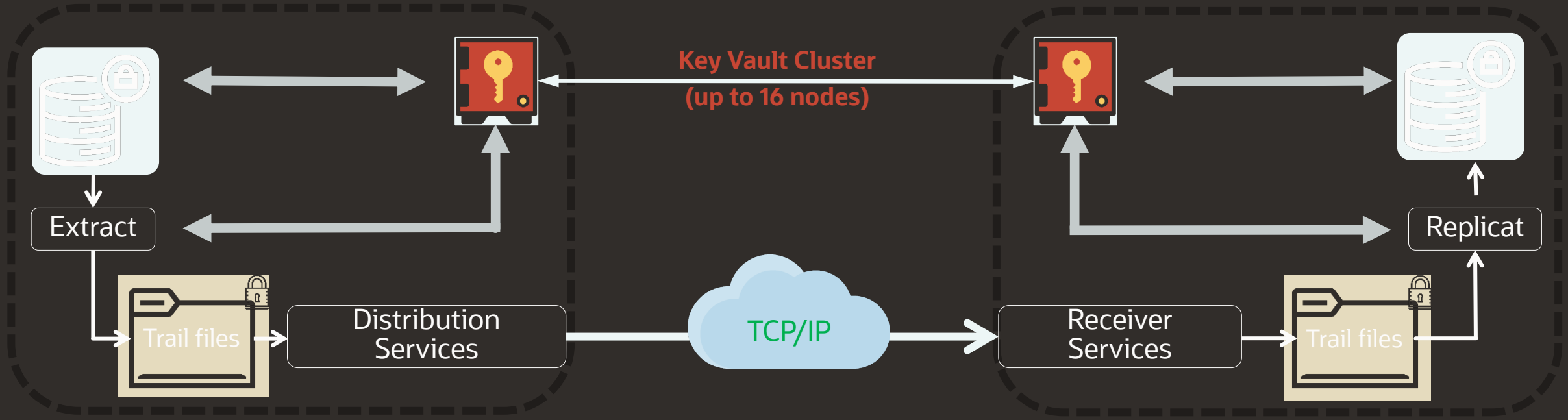
Scalability and deployment flexibility



Two nodes: Continuous read availability
Four and more (up to 16) nodes: Continuous read/write availability

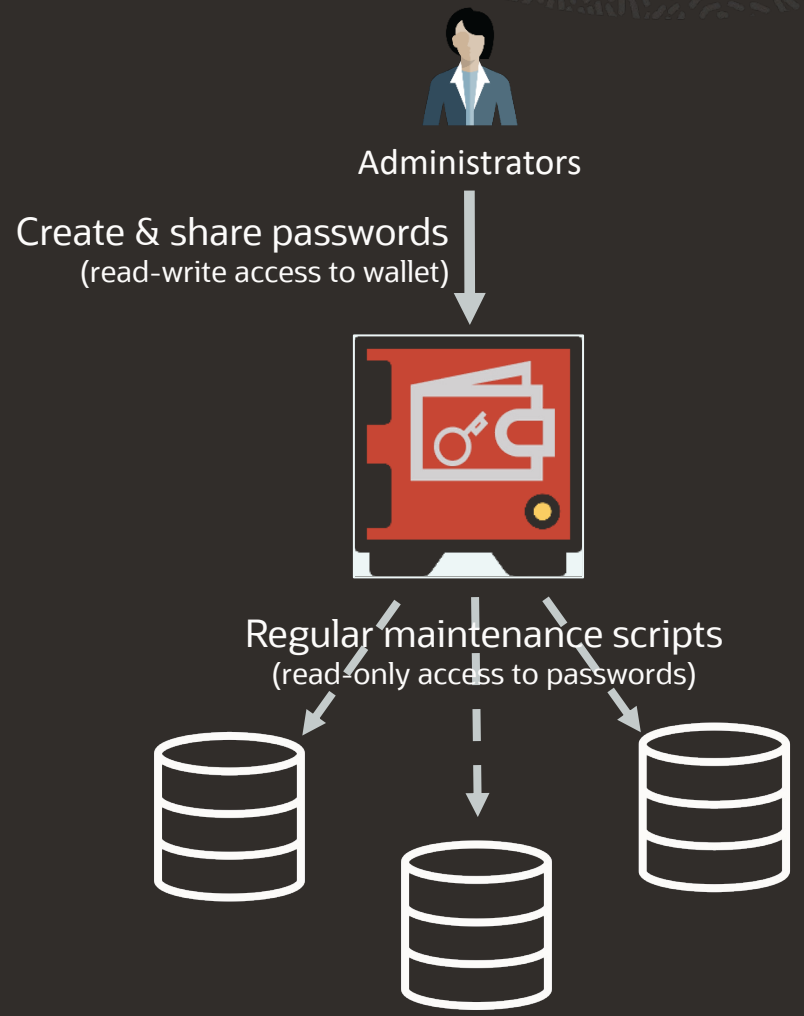
Oracle GoldenGate trail file key management with Oracle Key Vault

- Trail file encryption master keys are separated from the encrypted data
- Absolutely transparent – no changes to applications, established workflow
- Complete key lifecycle management incl. key rotation, key expiration
- Supports Bring-Your-Own-Key (BYOK)



Password management with Oracle Key Vault

- Passwords are centrally created and rotated
- Administrator grants or revokes read-only access of endpoints to the passwords
- Fetch of the passwords on-demand
- Zero password footprint on the endpoint host
- Stronger passwords with no human intervention
- Easily scriptable using REST API, C-SDK or Java SDK



ZDLRA archive encryption with Oracle Key Vault

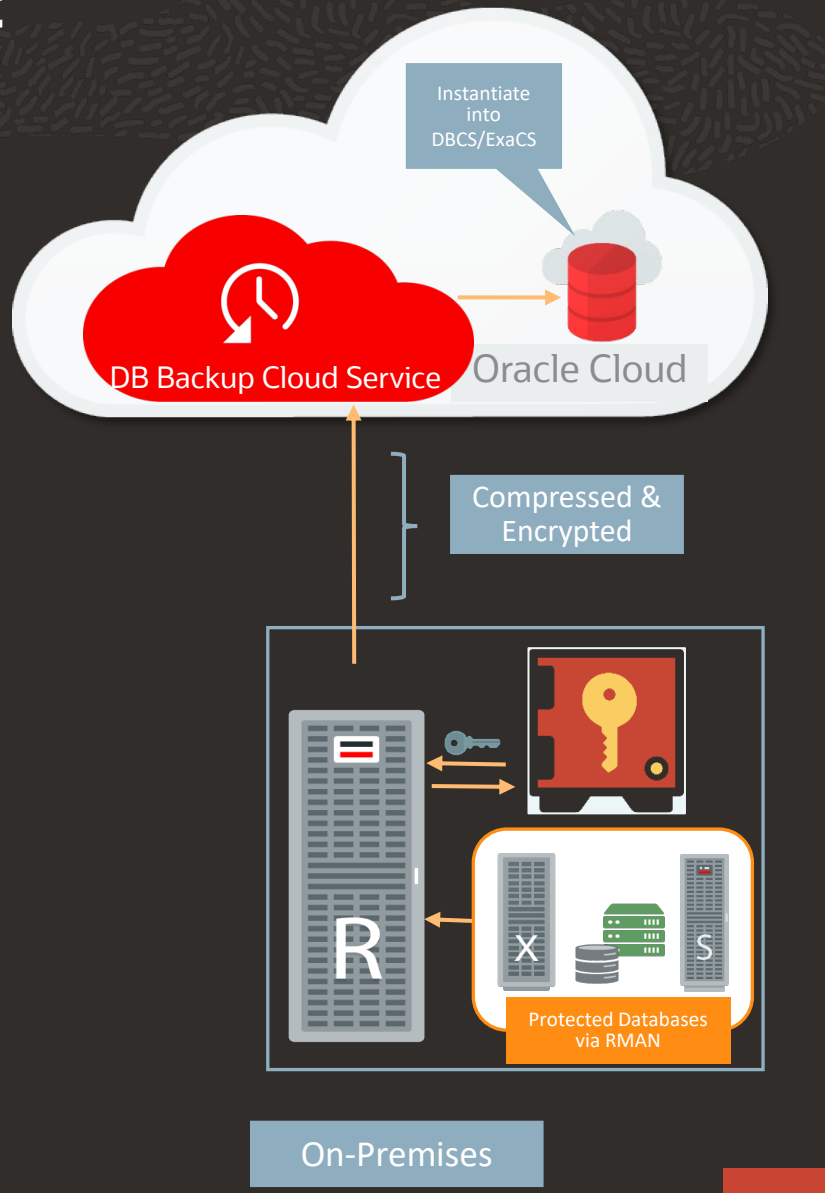
Stores backups in Oracle Database Backup Cloud Service

- Leverage a cost-effective cloud storage tier managed by Oracle, expanding options beyond on-premises tape
- Eliminate tape vaulting services

Accelerates journey into Cloud through easy provisioning of Cloud Databases directly from Cloud backup

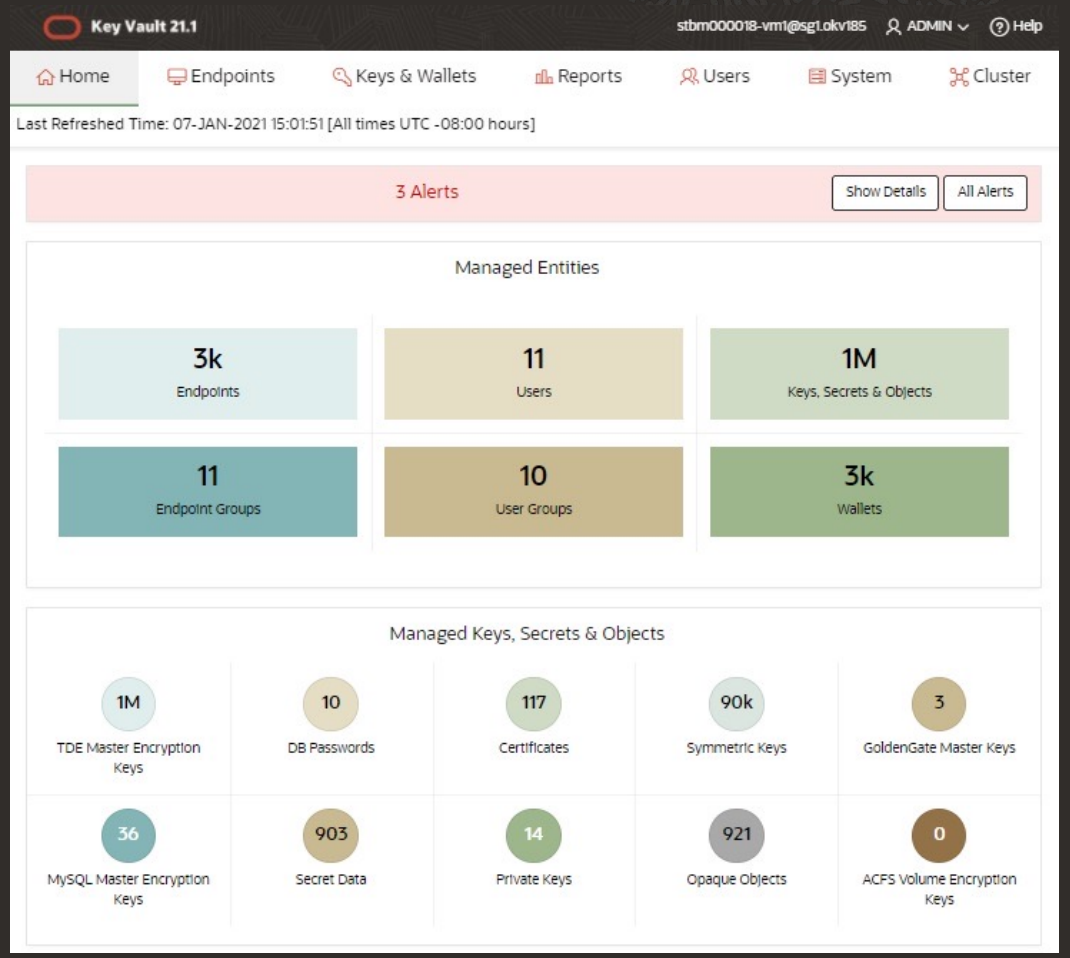
Archive backups are encrypted

- Uses Oracle Key Vault for Key Management



Responsive, scalable user interface

- Oracle Key Vault 21 introduced a new responsive user interface
  - Transparently adapts to different display sizes
  - Easy to navigate, responsive, simplifying common use-cases
  - Optimized for large deployments
- New dashboards enable administrators to quickly drill down and understand the various keys, secrets and other security objects under management



Oracle Key Vault automation APIs

New-look RESTful API interface for appliance automation includes

- Server administration
  - Endpoint deployment and administration
- Access management
  - Manages endpoint groups and wallets
  - Facilitate secure sharing of keys and secrets
- Security objects
  - Key and secrets life-cycle management
- Monitoring
  - Server health and configuration monitoring
- Backup and restore
  - Setup and schedule backup management to remote destinations

Get server status

```
$ okv server status get
 },
    "services" : {
      "RESTfulService" : "Up",
      "emailService" : "Not enabled",
      "KMIPService" : "Up",
      "storageDB" : "Up",
      "auditVaultAgentMonitor" : "Not enabled",
      "clusterService" : "Up"
    },
    "uptime" : "  7:02 HH:MM"
  }
```

Or just the uptime

```
$ ./bin/okv server status get | jq '.value.uptime'
"  7:02 HH:MM"
```

Support for Custom Endpoints

- Applications with KMIP interface can use OKV for key and secrets management out-of-the-box
- Using C and Java SDK, applications developers can quickly and easily
  - enable central key and secrets management
  - achieve compliance, and
  - improve security
- Database applications that encrypt and decrypt data using the Oracle Database's DBMS_CRYPTO PL/SQL package can now store and access its encryption key in Oracle Key Vault

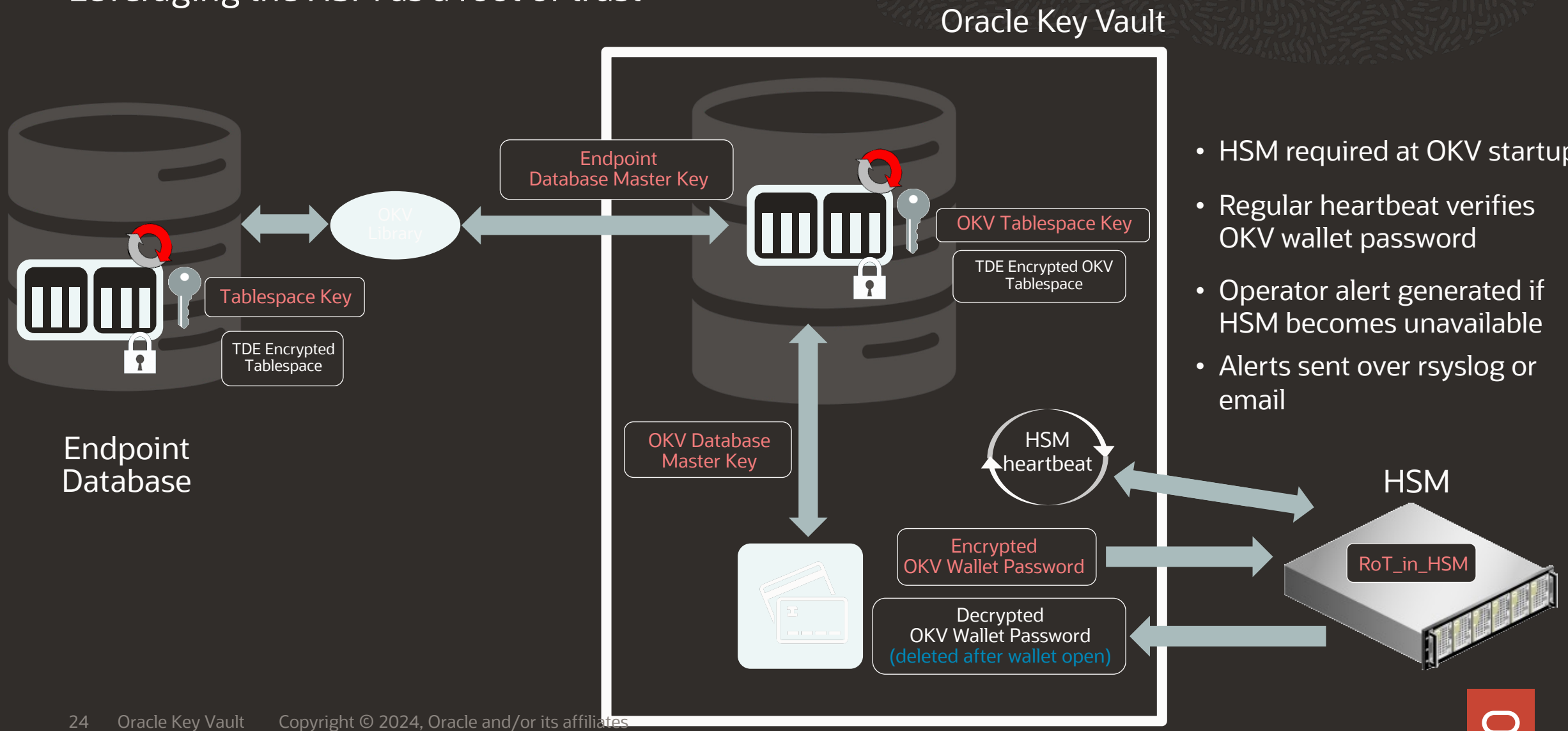
Persistent master key cache

- Persistent cache provides key availability when Oracle Key Vault goes down (during upgrades, unplanned emergencies) or if there is a network interruption
- This is optional, however can be deployed by customers to:
  - Reduce load on the OKV cluster during key management load spikes
  - Address network connectivity concerns between database and OKV cluster

- Two modes of persistent cache
  1. Endpoint-protected persistent cache
     - The persistent cache is protected by the endpoint password and must be used with password-protected connections only
  2. Database-protected persistent cache:
     - The persistent cache is password-protected wallet secured by a random database generated password

Oracle Key Vault HSM integration

Leveraging the HSM as a root of trust



- HSM required at OKV startup
- Regular heartbeat verifies OKV wallet password
- Operator alert generated if HSM becomes unavailable
- Alerts sent over rsyslog or email

OKV integrated with ADB-S

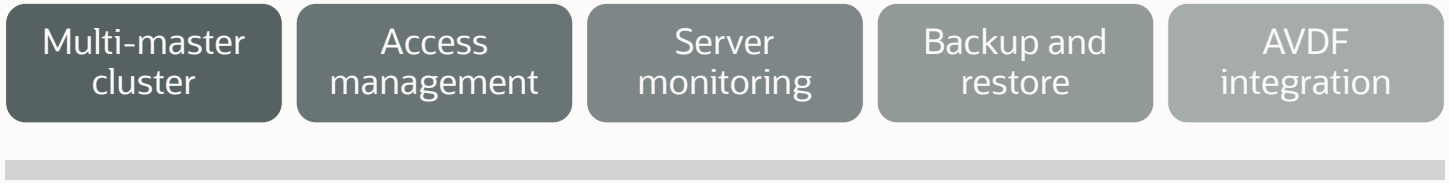
Oracle Key Vault capabilities for cloud databases

Key Reasons

- Customers prefer exclusive control of their encryption keys
- Continuously available, geographically distributed, and scalable
- Single solution for key management across OCI, Azure, GCP, AWS, and on-premises

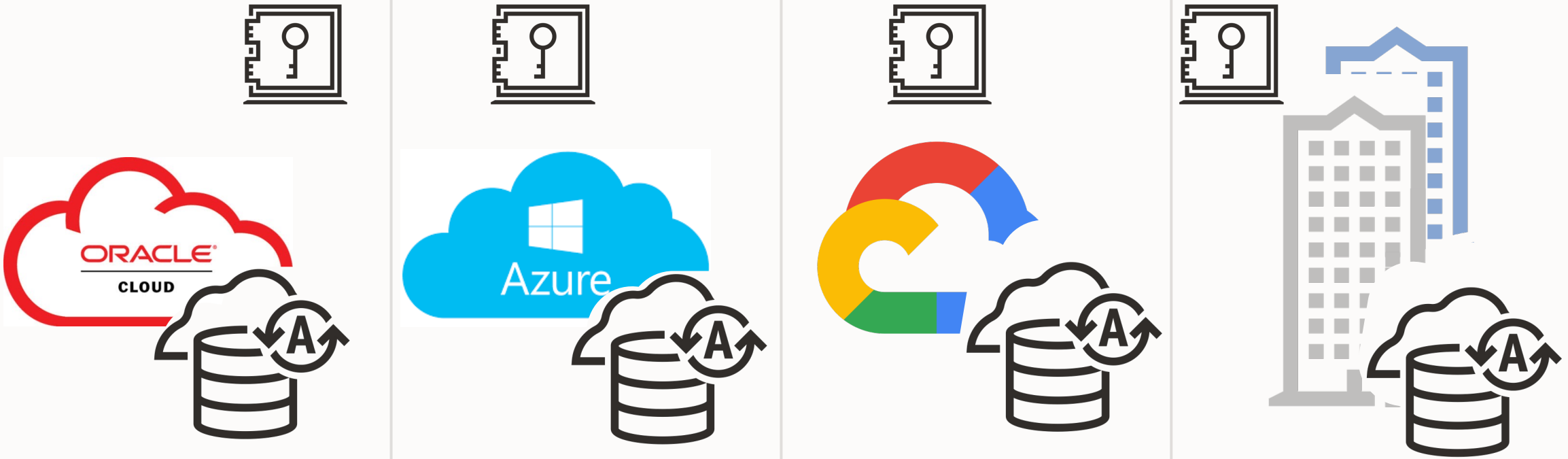
Key features facilitating integration

- Endpoint isolation
- Lifecycle management using OKV Restful API support



Autonomous Database Deployment Options – Available Today

Oracle Cloud Infrastructure	Azure (via Database@Azure)	Google (via Database@GCP)	Dedicated Cloud@Customer



Coming soon: *Oracle Autonomous Database @ AWS*

OKV and Centralized SSH key management

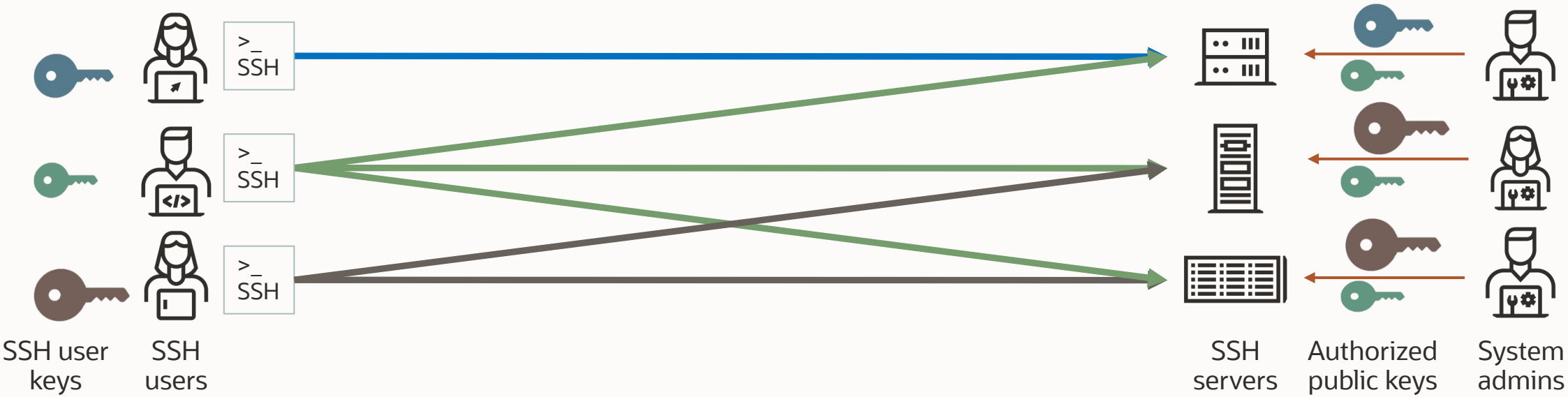
SSH key and access management is challenging

No SSH user key management

- ✗ Key sprawl
- ✗ Localized or no key rotation
- ✗ Different key sizes

Localized SSH server access

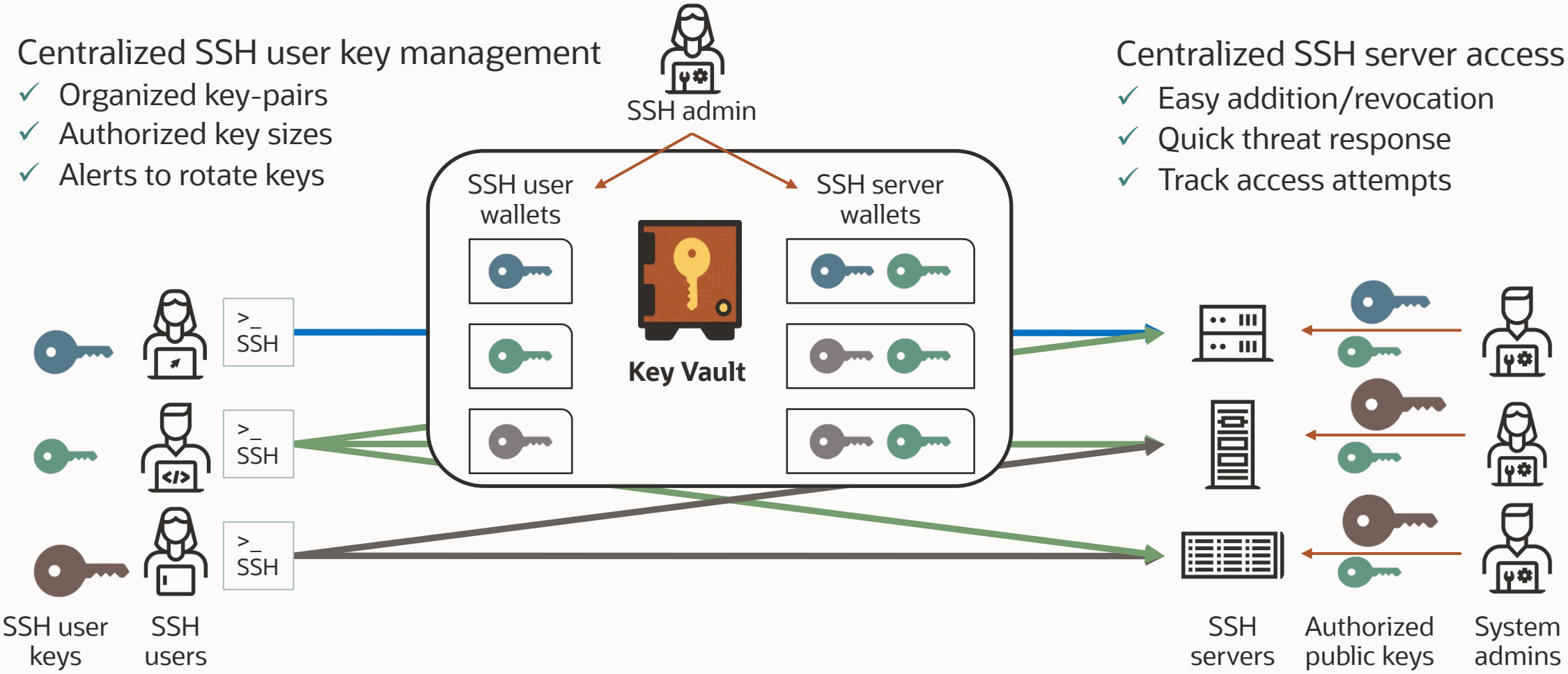
- ✗ Multiple admins make access control decisions
- ✗ Not updated when people/roles change
- ✗ Prone to human error



Centralized SSH key and access management in Oracle Key Vault 21.7

Centralized SSH user key management

- ✓ Organized key-pairs
- ✓ Authorized key sizes
- ✓ Alerts to rotate keys



Centralized SSH server access

- ✓ Easy addition/revocation
- ✓ Quick threat response
- ✓ Track access attempts

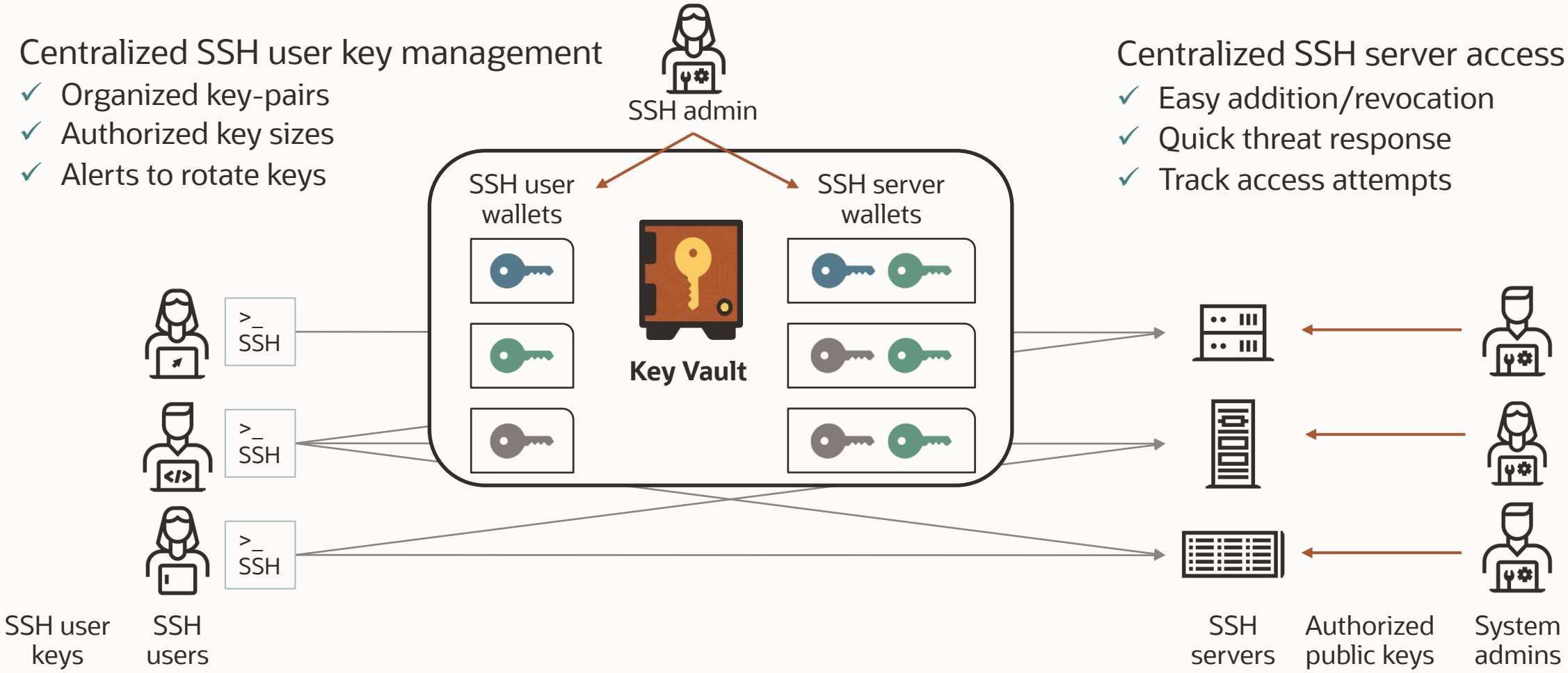
Centralized SSH key and access management in Oracle Key Vault 21.7

Centralized SSH user key management

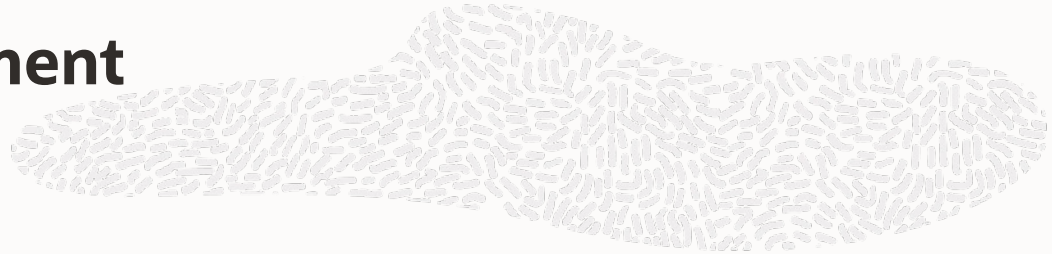
- ✓ Organized key-pairs
- ✓ Authorized key sizes
- ✓ Alerts to rotate keys

Centralized SSH server access

- ✓ Easy addition/revocation
- ✓ Quick threat response
- ✓ Track access attempts



Benefits of centralized SSH key management



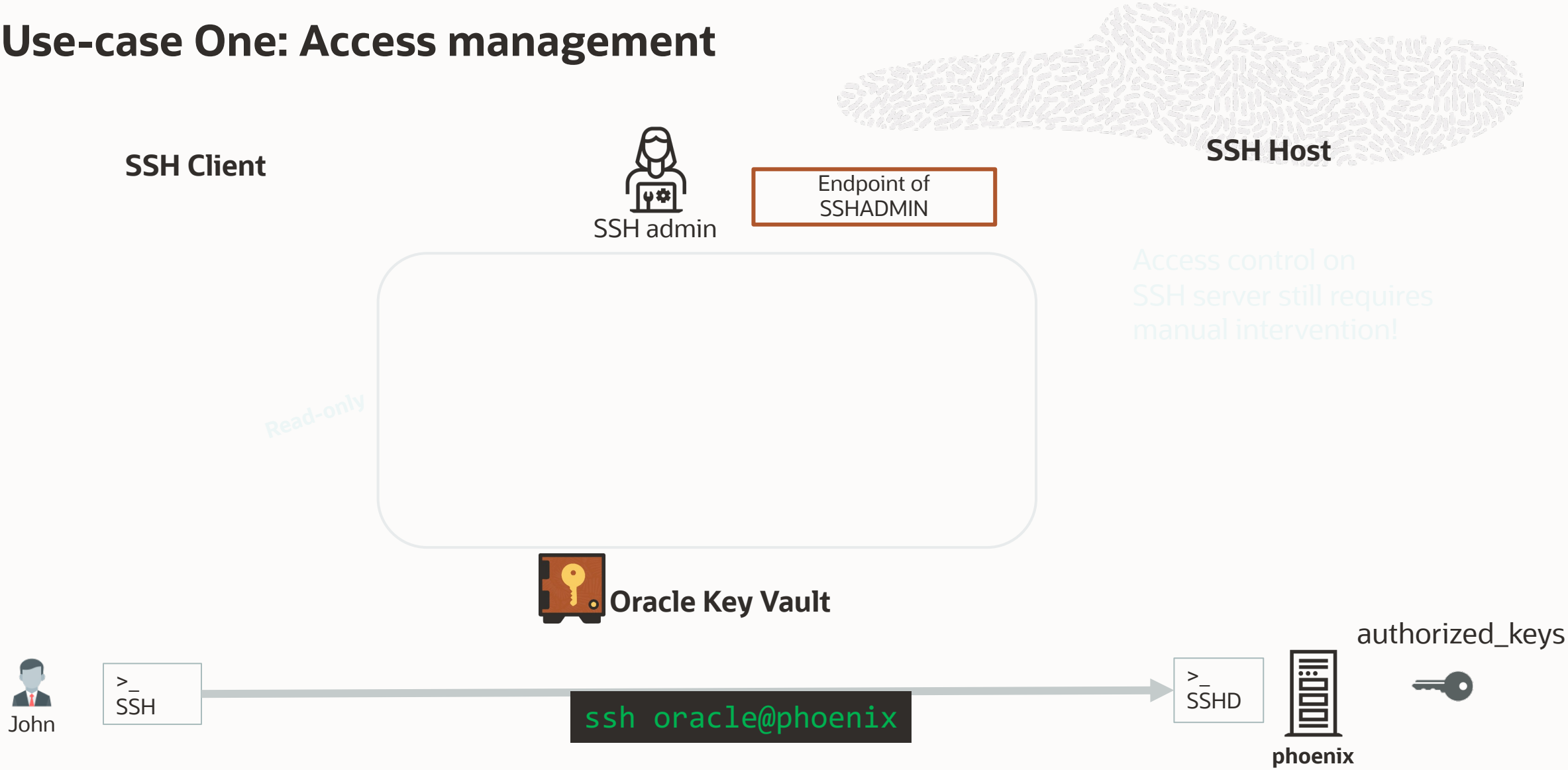
- ✓ Centrally control user/machine access to SSH hosts across the organization
- ✓ Enforce governance and key lifecycle management

Remote Server access control and SSH key management with OKV

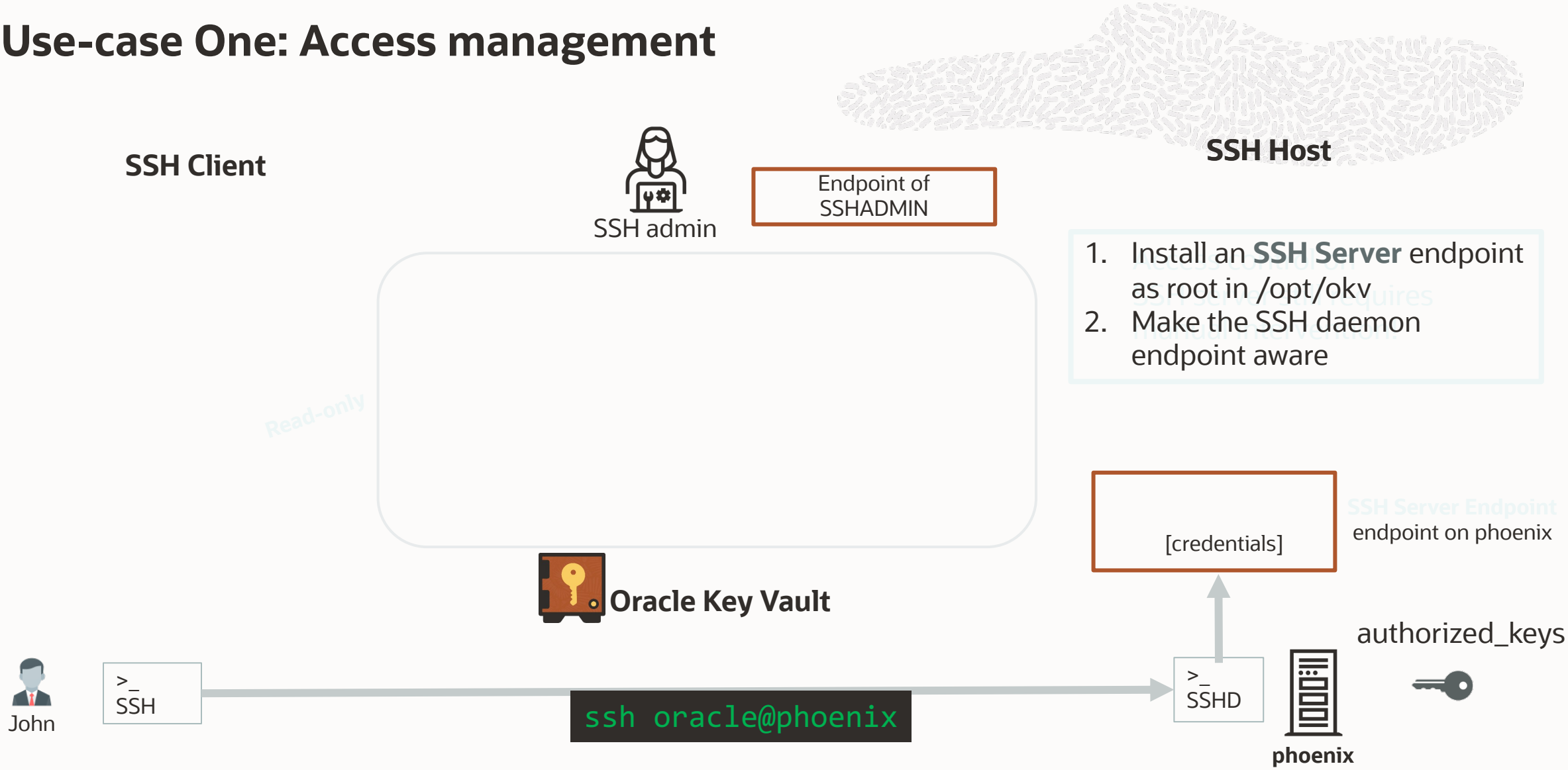
Agenda:

- Use-case One: Remote Server access management
- Use-case Two: SSH key management
- Use-case Three: The complete setup, Use-case One and Use-case Two combined

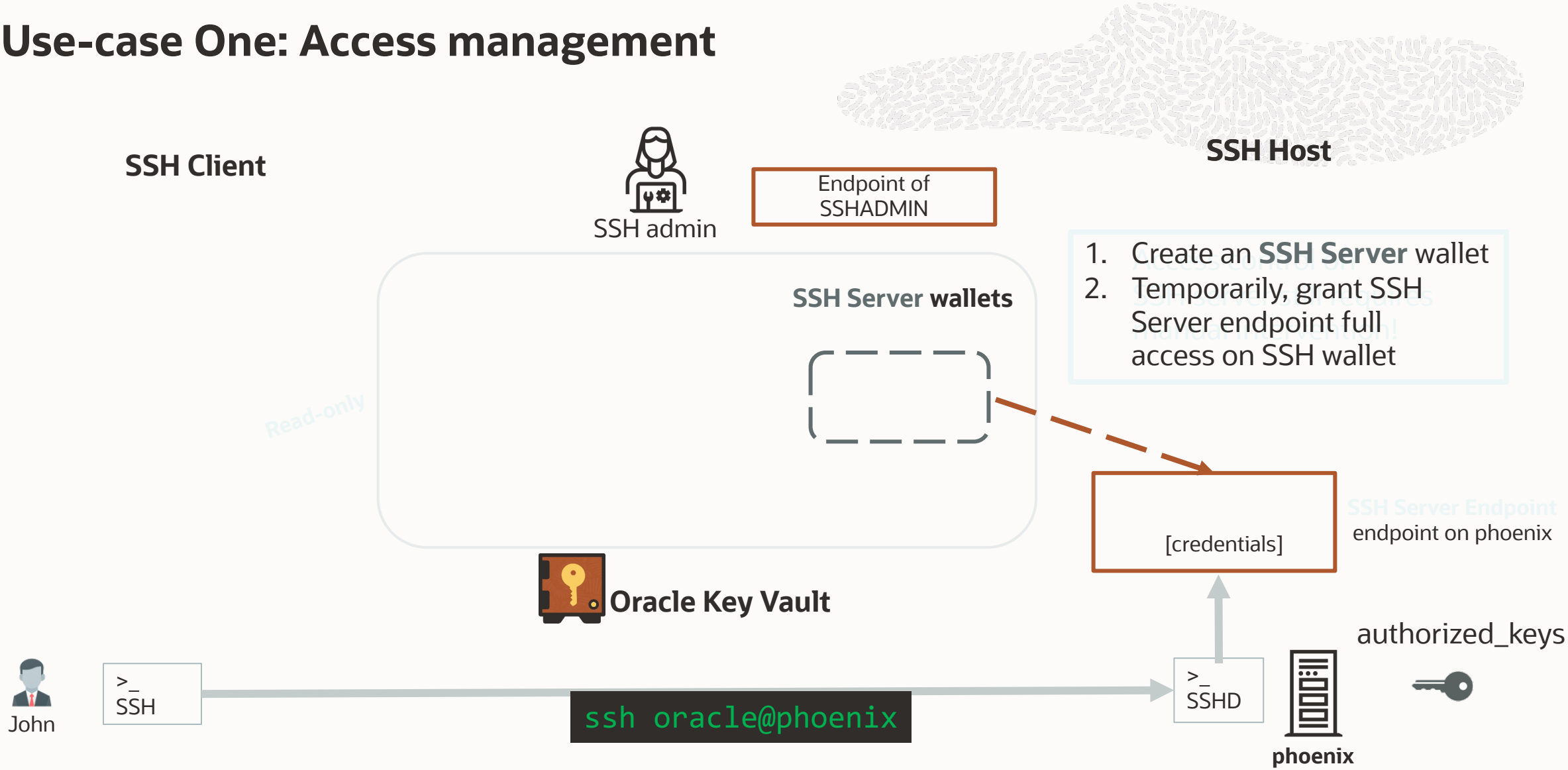
Use-case One: Access management



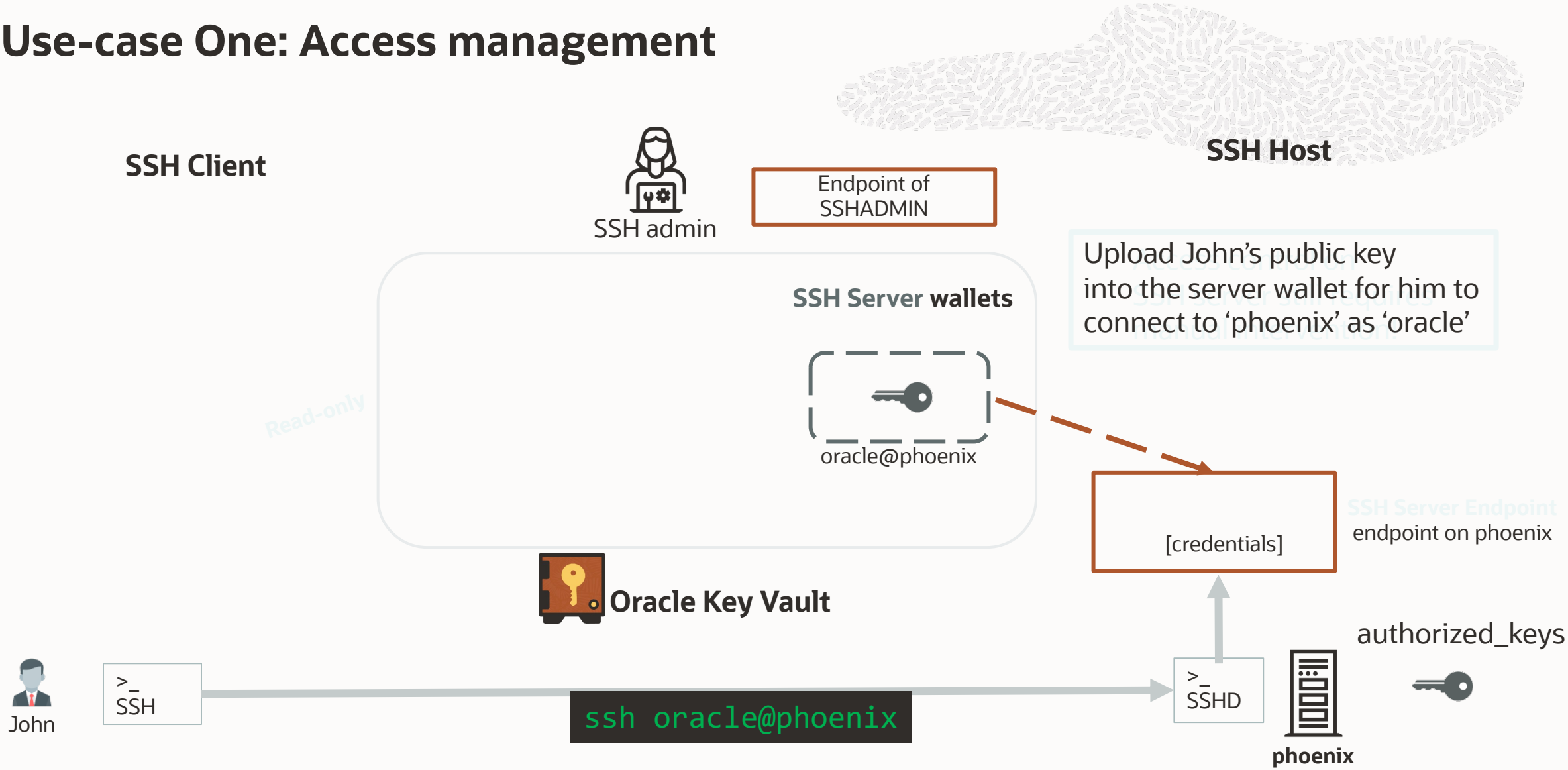
Use-case One: Access management



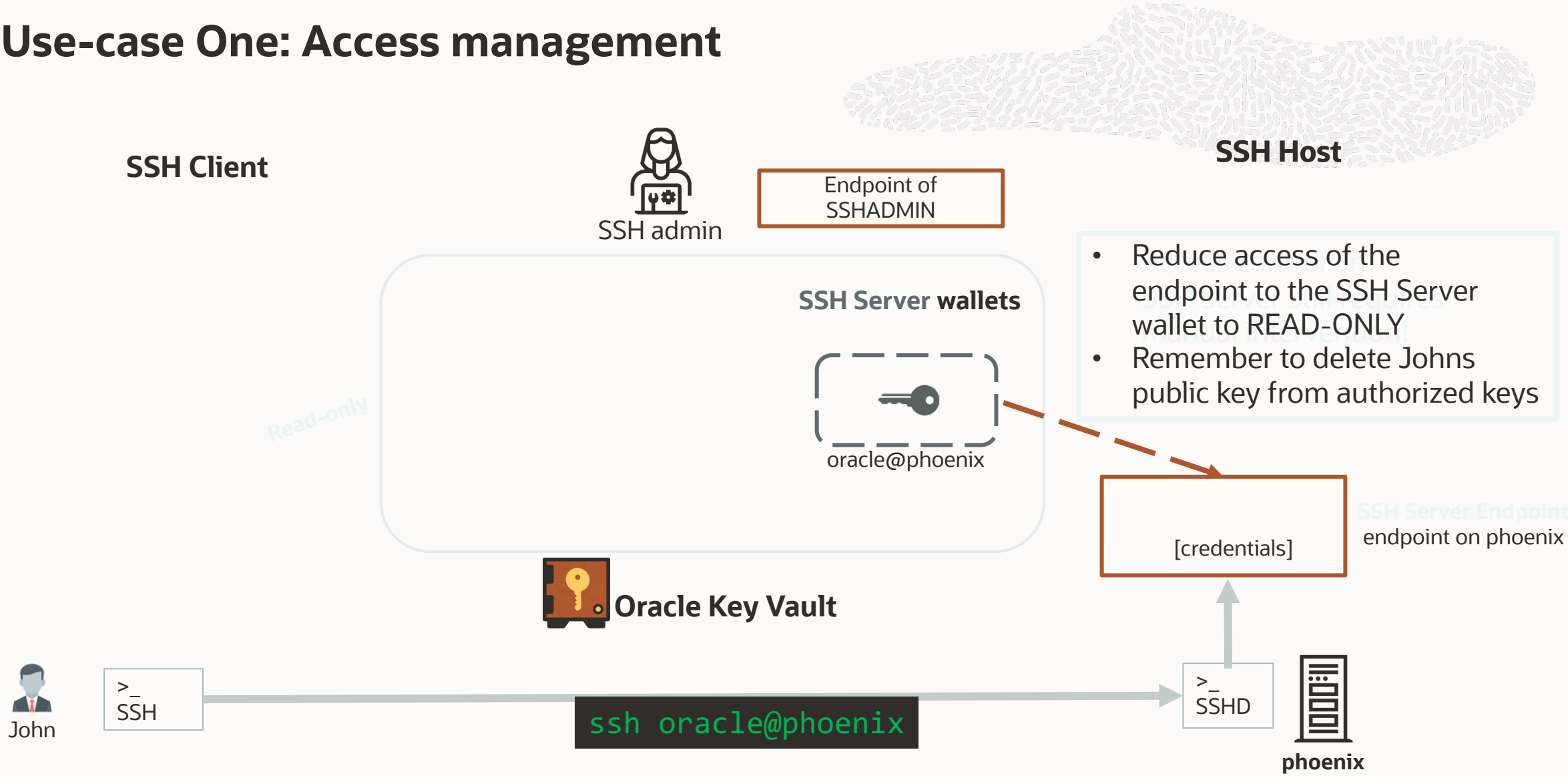
Use-case One: Access management



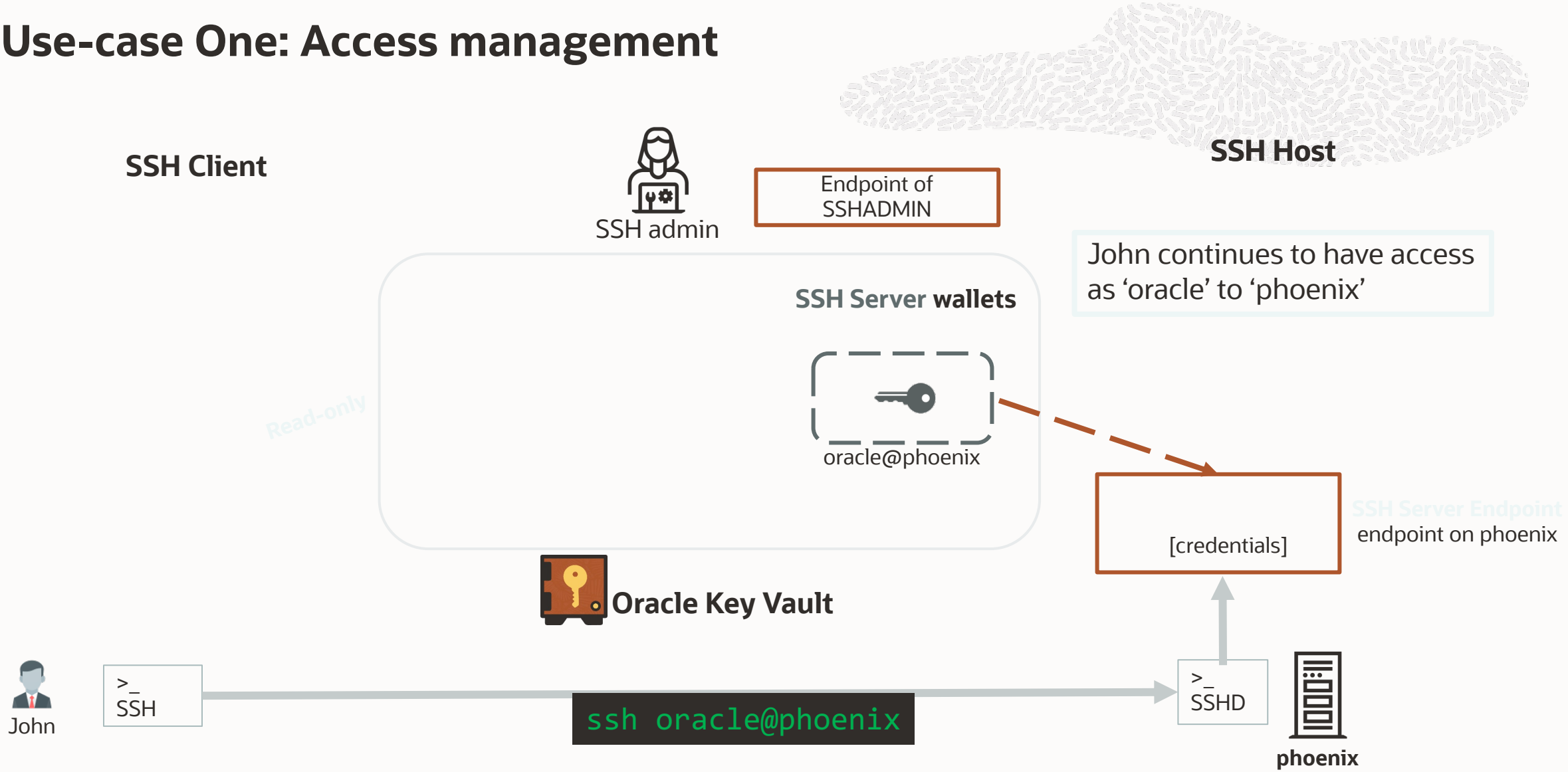
Use-case One: Access management



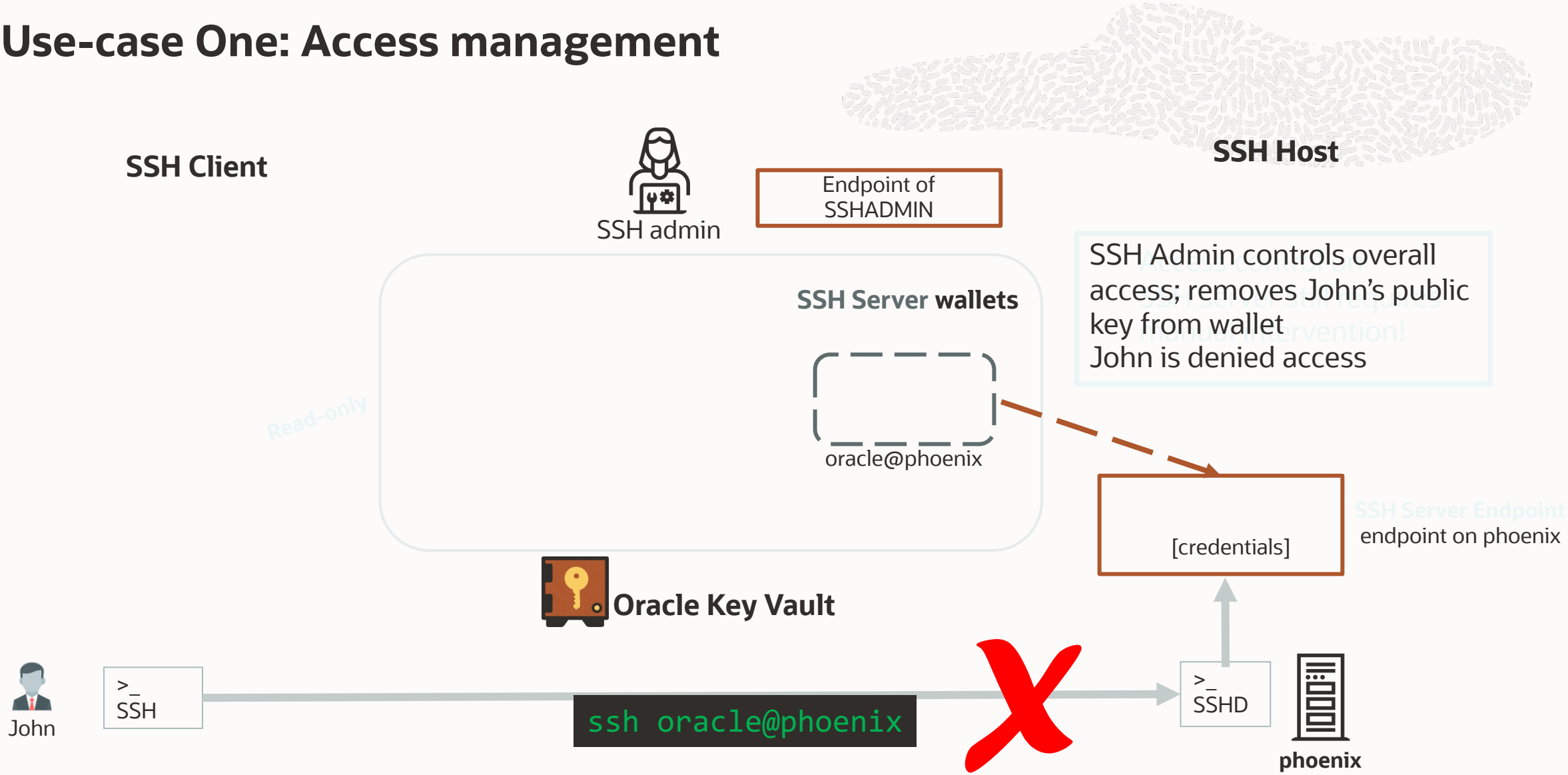
Use-case One: Access management



Use-case One: Access management



Use-case One: Access management



Who has SSH access to which server?

SSH Server Authorization Report

Close

Go

Actions

SSH Server	SSH Server Host User	SSH Server Wallet	SSH User	SSH User Public Key Fingerprint	SSH User Public Key Details
austin.oracle.com	opc	opc_ssh_wallet	Jane	SHA256:R4+IsT6af1+mC3+IQrhcxVwMSpTXtehsiuSImuHRhkU	
austin.oracle.com	oracle	oracle_ssh_wallet	John	SHA256:z+JQz0VnTQygl7Good5IcDVMsRNM+48i9Ww6RqIhIps	
austin.oracle.com	root	root_ssh_wallet_for_austin	Sam	SHA256:HZrIsgGHKr6D4SWT/b2Xb5CHHZByVmO+Dz19J9glj5c	
phoenix.oracle.com	opc	opc_ssh_wallet	Jane	SHA256:R4+IsT6af1+mC3+IQrhcxVwMSpTXtehsiuSImuHRhkU	
phoenix.oracle.com	oracle	oracle_ssh_wallet	John	SHA256:z+JQz0VnTQygl7Good5IcDVMsRNM+48i9Ww6RqIhIps	
phoenix.oracle.com	root	root_ssh_wallet_for_phoenix	Sally	SHA256:Ke4M7IYO4W4XRwpf5/fh3NLs0MgQpiqqirT27h4Dgfw	

1 - 6 of 6

Who attempted to access servers and when?

SSH Server Access Report

Close

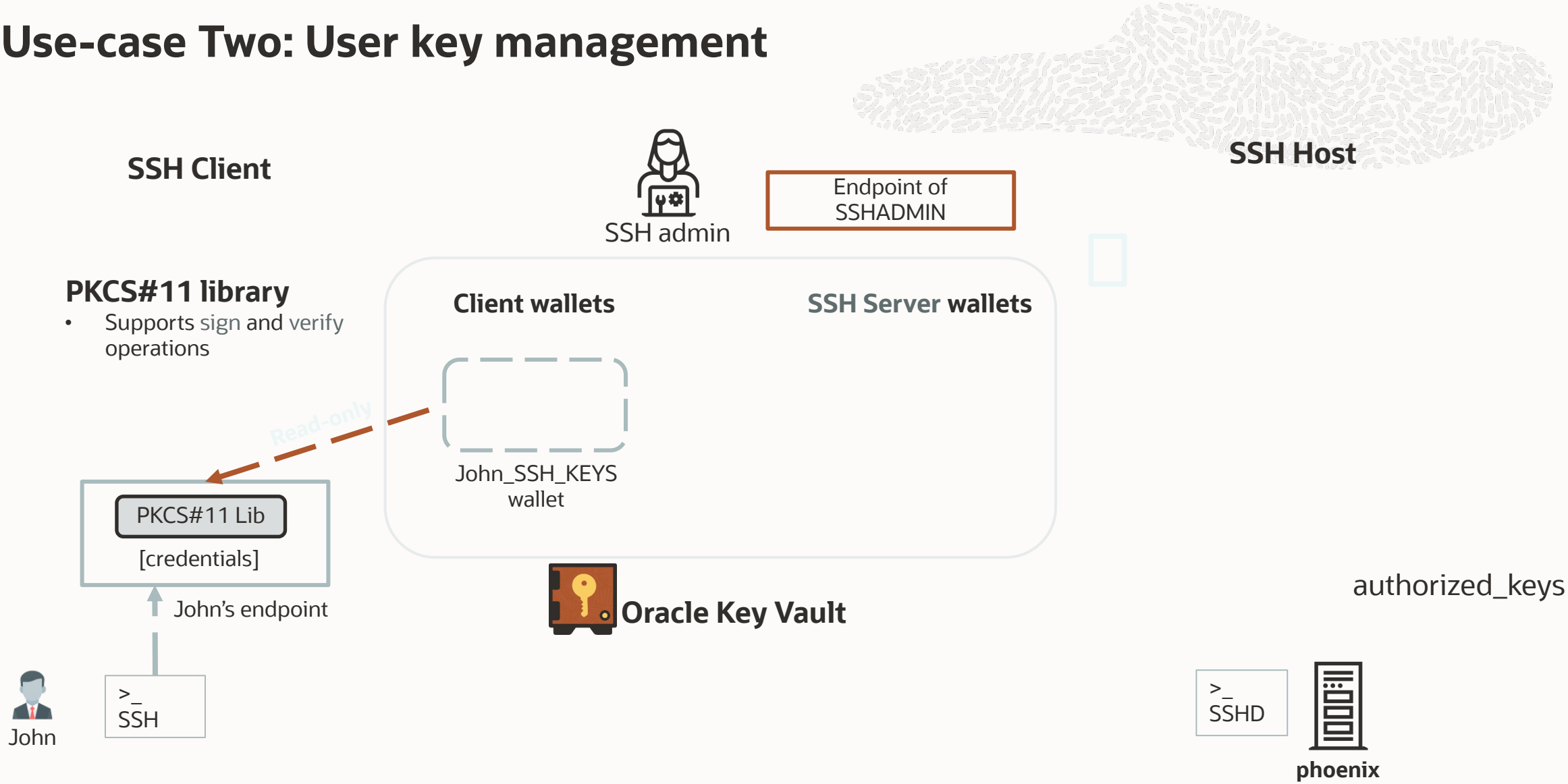
Go

Actions

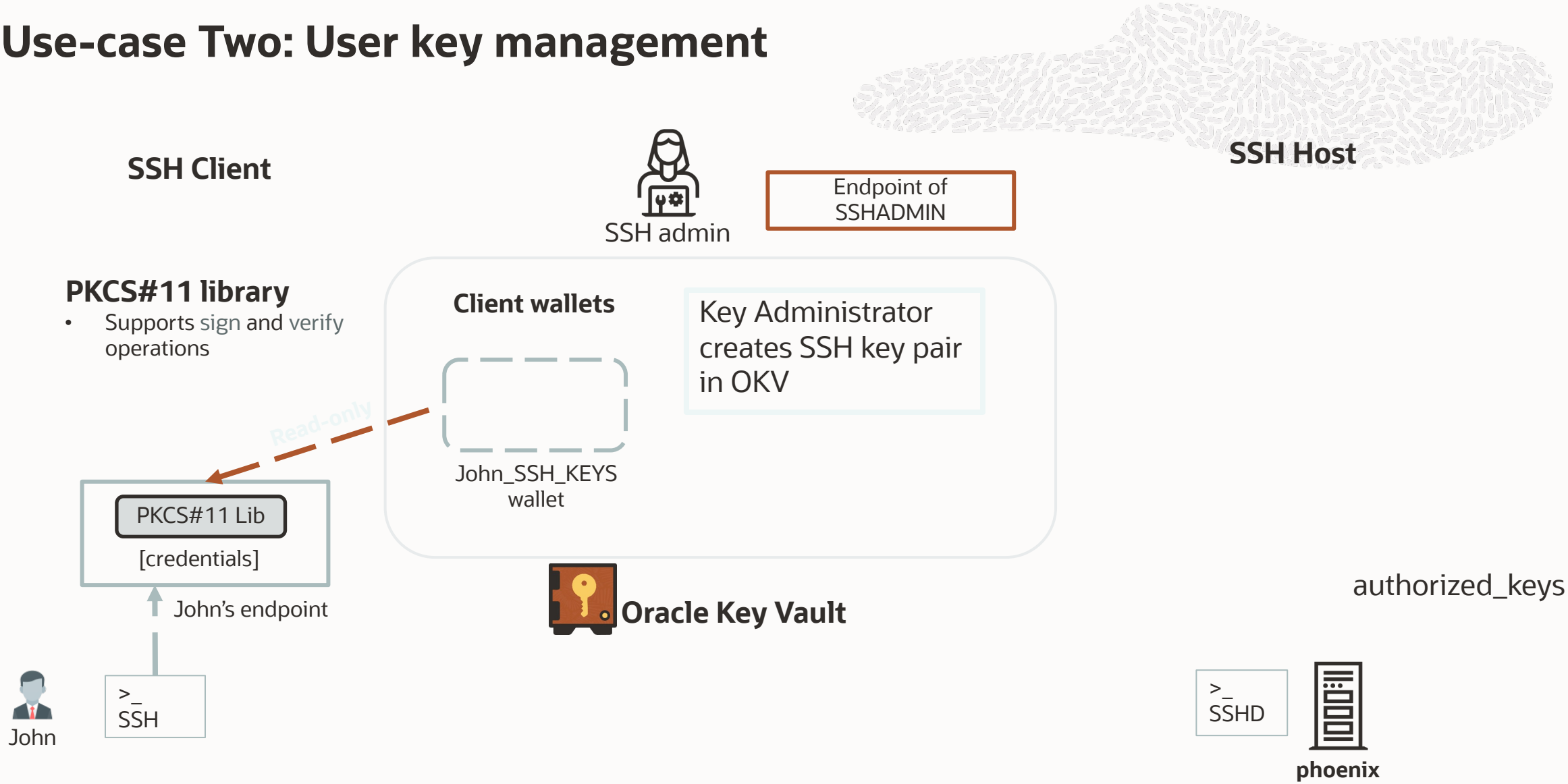
SSH Server	SSH Server Host User	SSH User	SSH User Public Key Fingerprint	Access Time	Result
phoenix.oracle.com	oracle	John	SHA256:z+JQz0VnTQygl7Good5IcDVMsRNM+48i9Ww6RqlhIps	07-OCT-2023 15:23:27	✓
phoenix.oracle.com	root	Sally	SHA256:Ke4M7IYO4W4XRwpf5/fh3NLs0MgQpiqqirT27h4Dgfw	07-OCT-2023 15:23:25	✓
phoenix.oracle.com	root	Malfoy	SHA256:a+f5d9UuF7JDYfiyRr1ej1lH2WkvQsp19Bh0Um0Yu44	07-OCT-2023 15:23:24	Failed
austin.oracle.com	opc	Jane	SHA256:R4+lsT6af1+mC3+IQrhcxVwMSpTXtehsiuSImuHRhkU	07-OCT-2023 15:23:24	✓
austin.oracle.com	root	Sam	SHA256:HZrIsgGHKr6D4SWT/b2Xb5CHHZByVmO+Dz19J9glj5c	07-OCT-2023 15:23:23	✓
austin.oracle.com	root	Malfoy	SHA256:a+f5d9UuF7JDYfiyRr1ej1lH2WkvQsp19Bh0Um0Yu44	07-OCT-2023 15:23:23	Failed
phoenix.oracle.com	oracle	John	SHA256:z+JQz0VnTQygl7Good5IcDVMsRNM+48i9Ww6RqlhIps	07-OCT-2023 15:12:50	✓
austin.oracle.com	opc	Jane	SHA256:R4+lsT6af1+mC3+IQrhcxVwMSpTXtehsiuSImuHRhkU	07-OCT-2023 15:12:20	✓
phoenix.oracle.com	oracle	John	SHA256:z+JQz0VnTQygl7Good5IcDVMsRNM+48i9Ww6RqlhIps	07-OCT-2023 15:04:41	✓
phoenix.oracle.com	oracle	John	SHA256:z+JQz0VnTQygl7Good5IcDVMsRNM+48i9Ww6RqlhIps	07-OCT-2023 13:40:36	✓
phoenix.oracle.com	root	Sally	SHA256:Ke4M7IYO4W4XRwpf5/fh3NLs0MgQpiqqirT27h4Dgfw	07-OCT-2023 13:40:35	✓

1 - 20 of 20

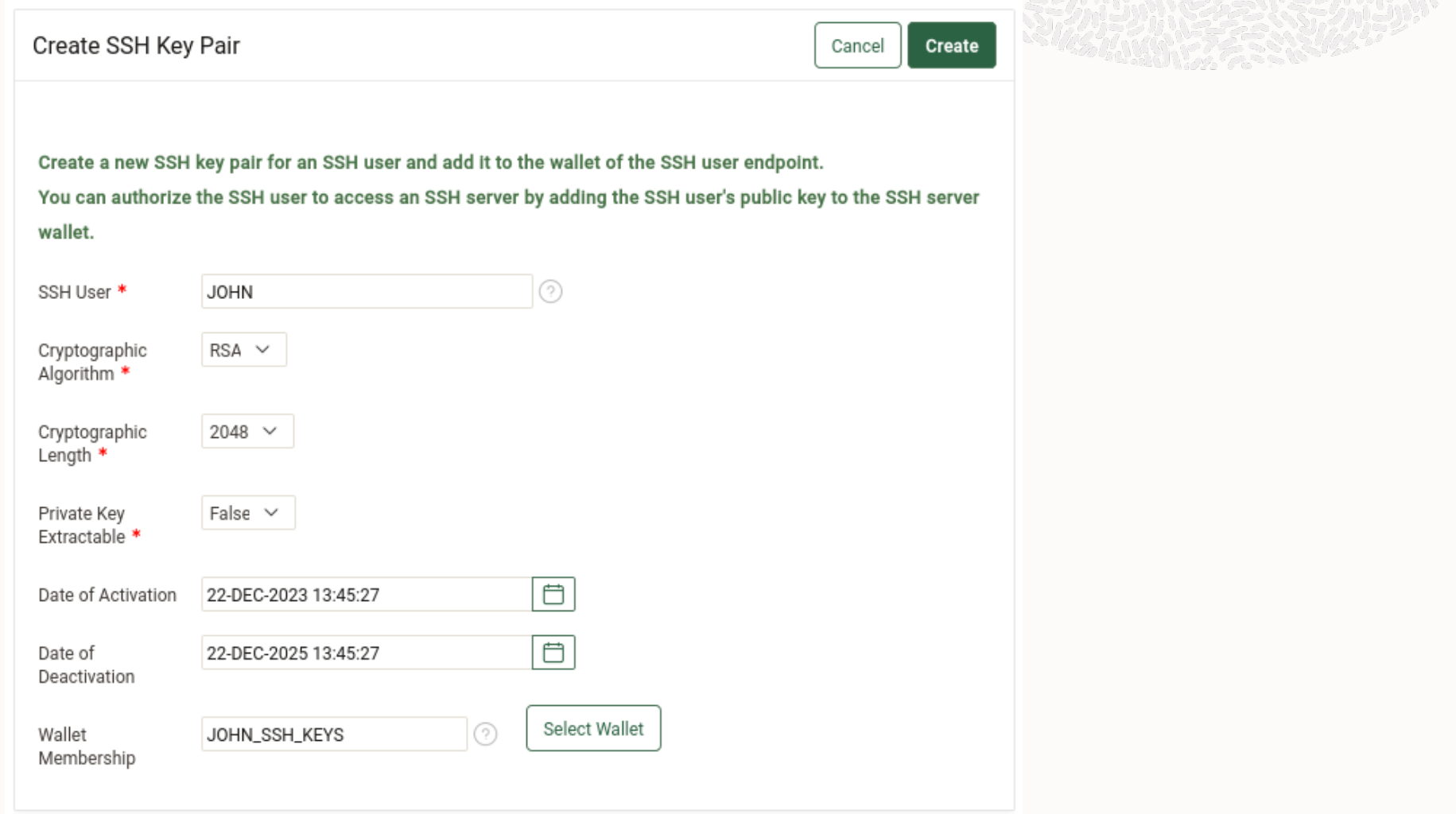
Use-case Two: User key management



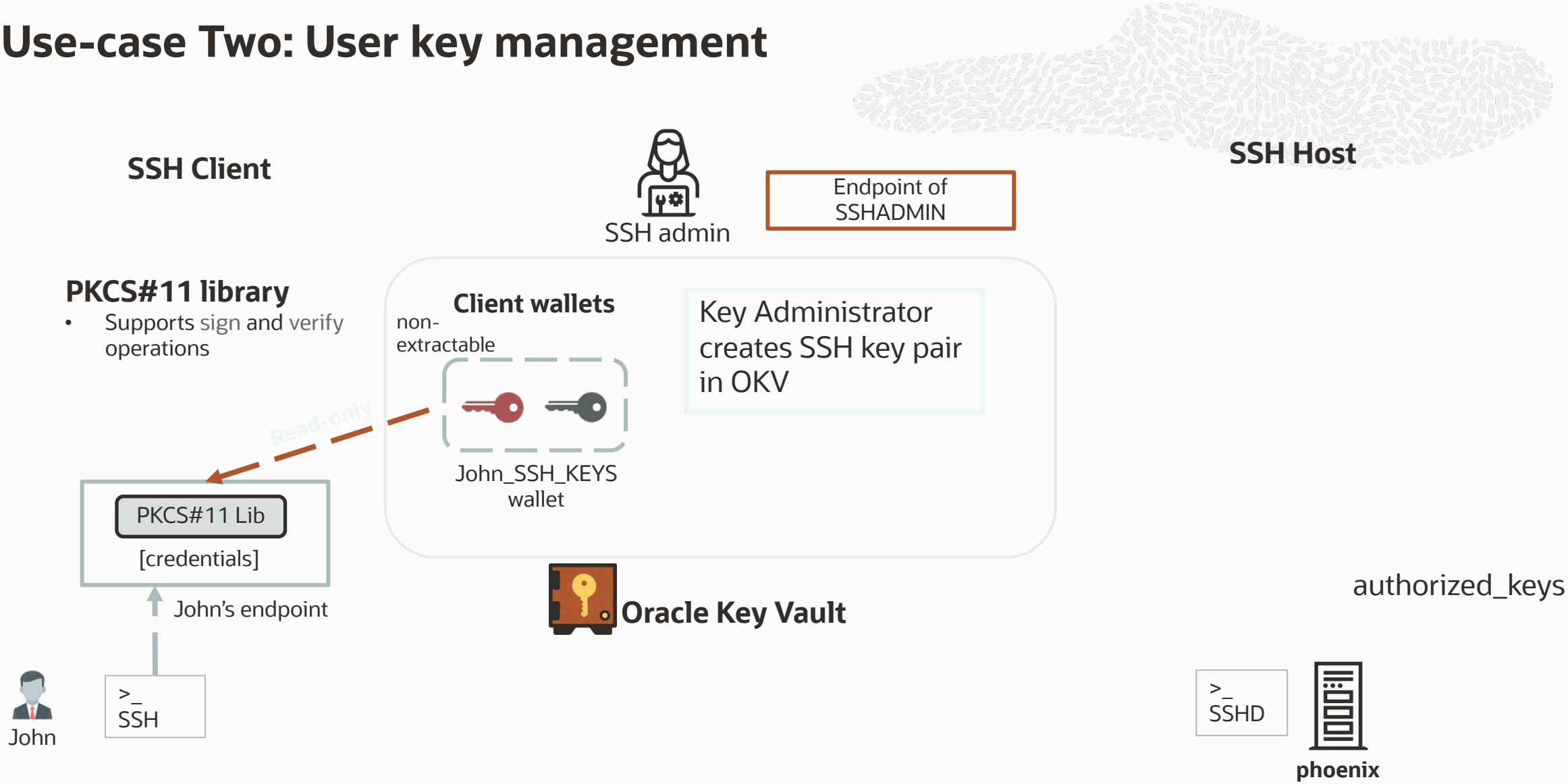
Use-case Two: User key management



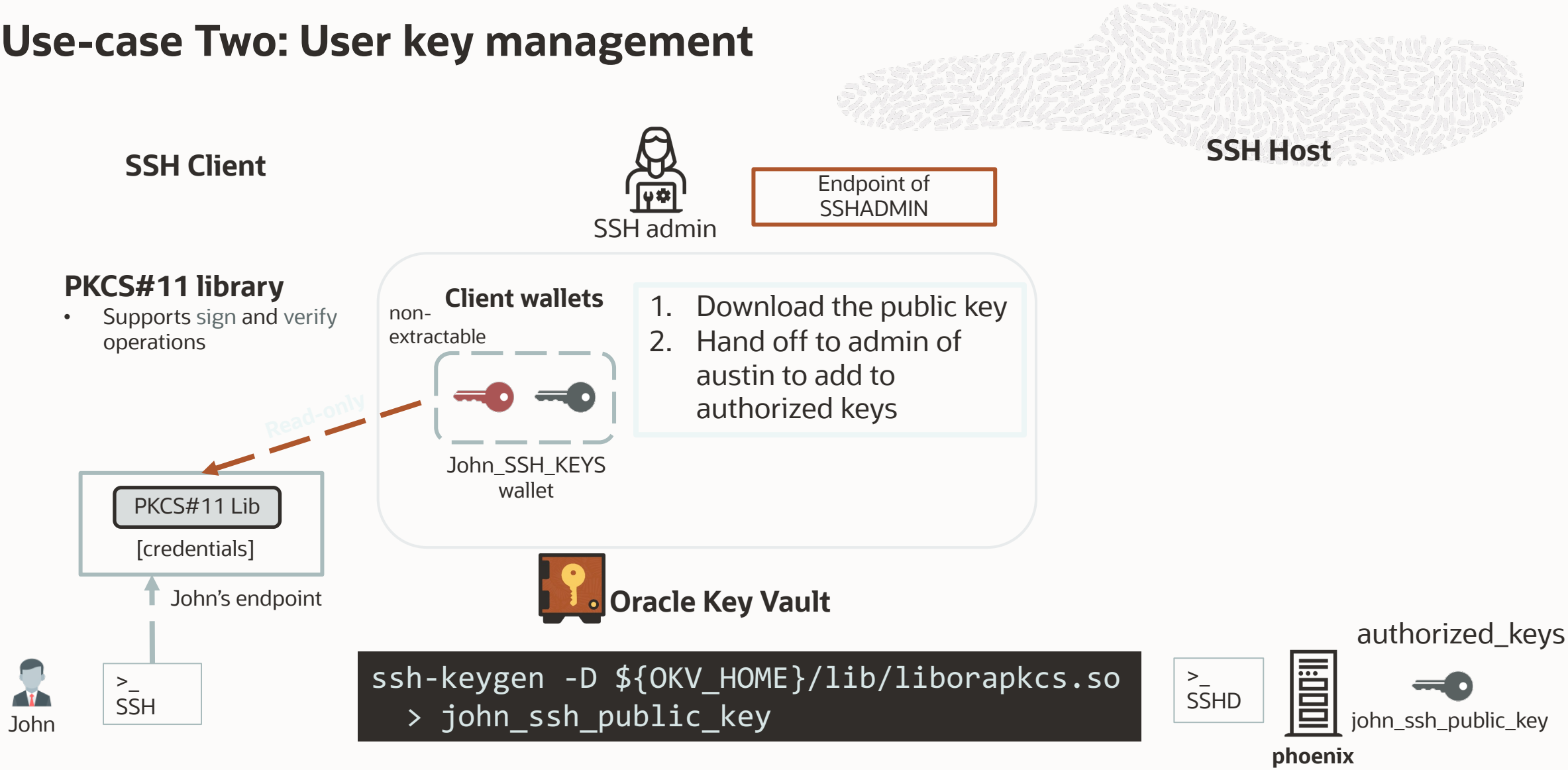
Use-case Two: User key management



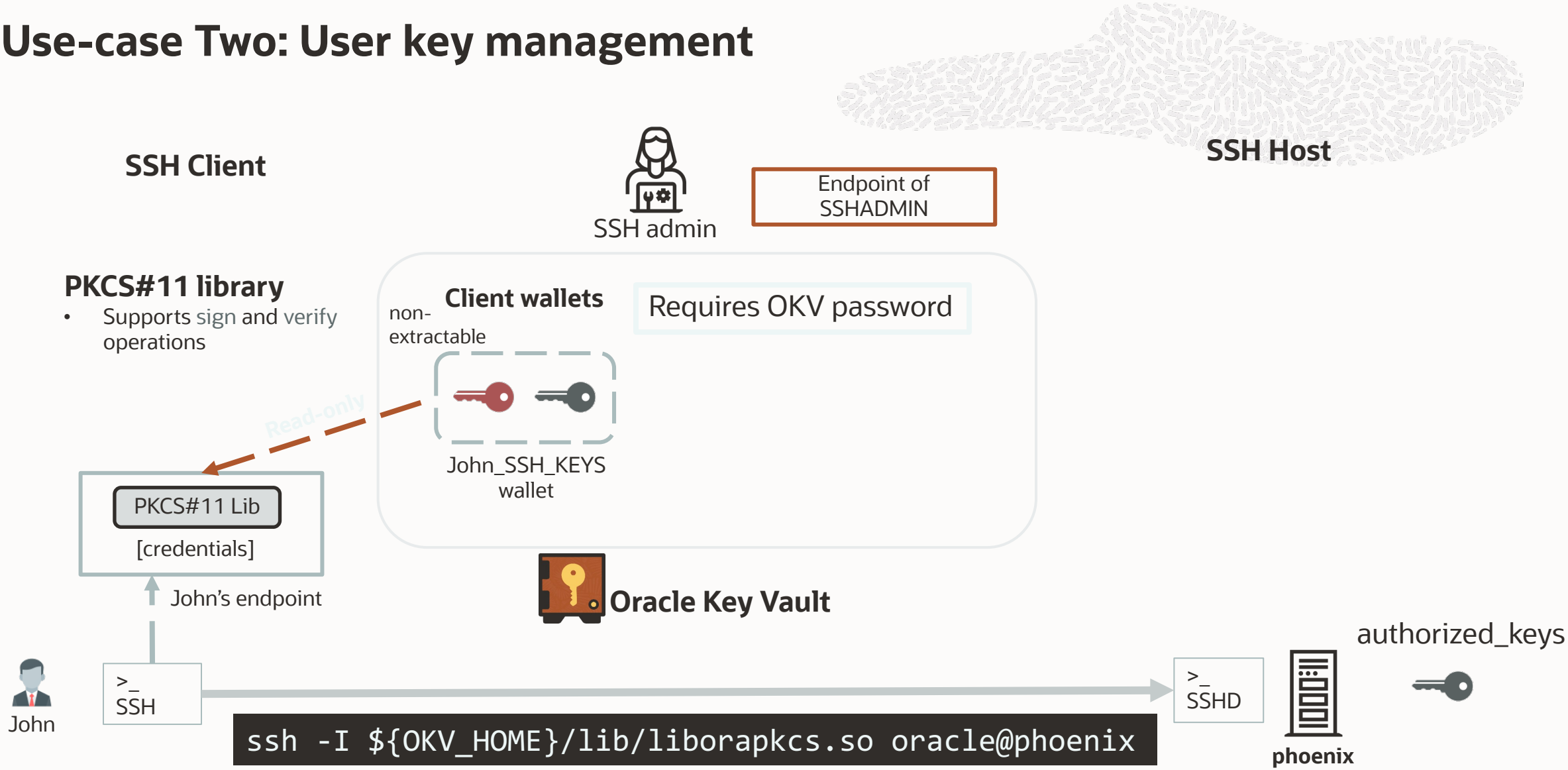
Use-case Two: User key management



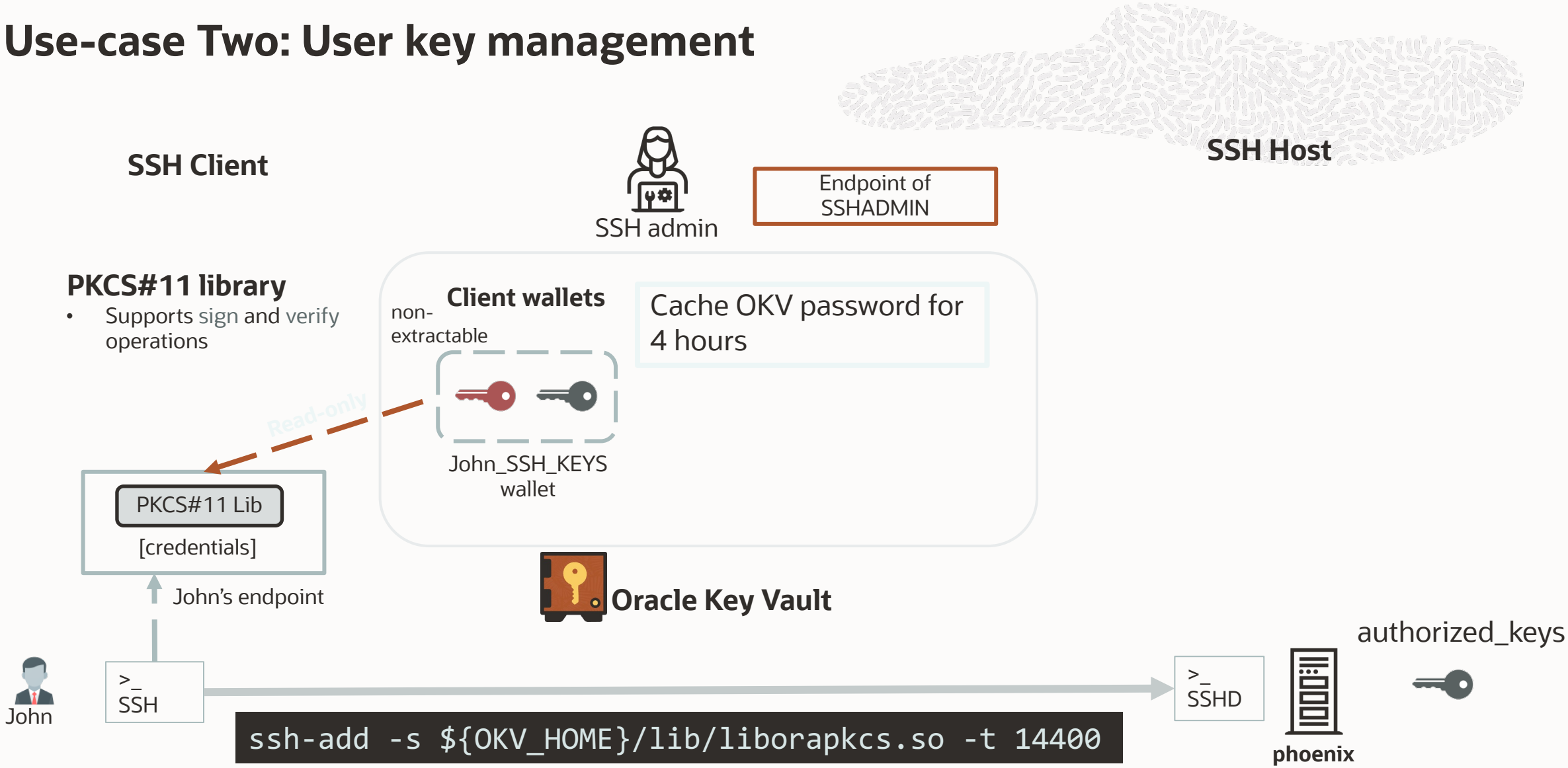
Use-case Two: User key management



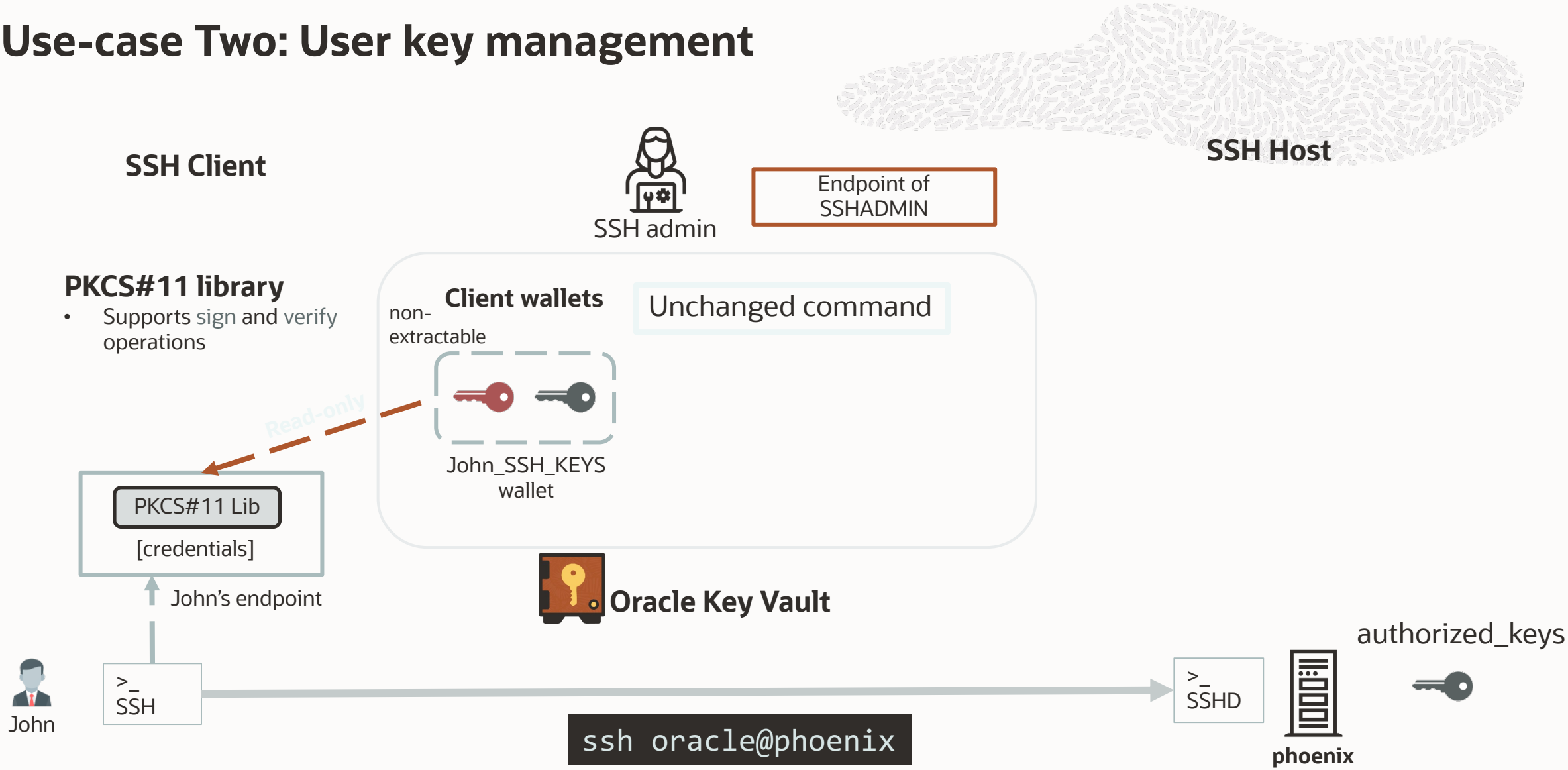
Use-case Two: User key management



Use-case Two: User key management



Use-case Two: User key management



Who has access to users private key ?

SSH Private Key Authorization Report

Close

Go Actions

SSH User	SSH User Key Fingerprint	User	Endpoint	Access Type	Access Through Wallet	SSH User Private Key Details
Sally	SHA256:Ke4M7IYO4W4XRwpf5/fh3NLs0MgQpiqqirT27h4Dgfw	-	SALLY_SYSADMIN_EP	Direct	Sally_sysadmin_SSH_Keys_Wallet	
Sally	SHA256:Ke4M7IYO4W4XRwpf5/fh3NLs0MgQpiqqirT27h4Dgfw	-	SSHADMIN	Creator		
John	SHA256:z+JQz0VnTQygl7Good5IcDVMsRNM+48i9Ww6RqIhIps	-	JOHN_EP	Direct	John_SSH_Keys_Wallet	
John	SHA256:z+JQz0VnTQygl7Good5IcDVMsRNM+48i9Ww6RqIhIps	-	SSHADMIN	Creator		
Jane	SHA256:R4+lsT6af1+mC3+IQrhcxVwMSpTXtehsiuSImuHRhkU	-	JANE_EP	Direct	Jane_SSH_Keys_Wallet	
Jane	SHA256:R4+lsT6af1+mC3+IQrhcxVwMSpTXtehsiuSImuHRhkU	-	SSHADMIN	Creator		
Malfoy	SHA256:a+f5d9UuF7JDYfiyRr1ej1lH2WkvQsp19Bh0Um0Yu44	-	MALFOY_EP	Direct	Malfoy_Wallet	
Malfoy	SHA256:a+f5d9UuF7JDYfiyRr1ej1lH2WkvQsp19Bh0Um0Yu44	-	SSHADMIN	Creator		
Jill	SHA256:TqernzdN4VmZR1wfNpnXjYWolmoWUgBfII6yXNr1Cuc	SSH_ADMIN	-	Creator		
Sam	SHA256:HZrIsgGHKr6D4SWT/b2Xb5CHHZByVmO+Dz19J9glj5c	-	SAM_SYSADMIN_EP	Direct	Sam_sysadmin_SSH_Keys_Wallet	
Sam	SHA256:HZrIsgGHKr6D4SWT/b2Xb5CHHZByVmO+Dz19J9glj5c	-	SSHADMIN	Creator		

1 - 11 of 11

Who has access to the user's private key?

SSH Private Key Usage Report

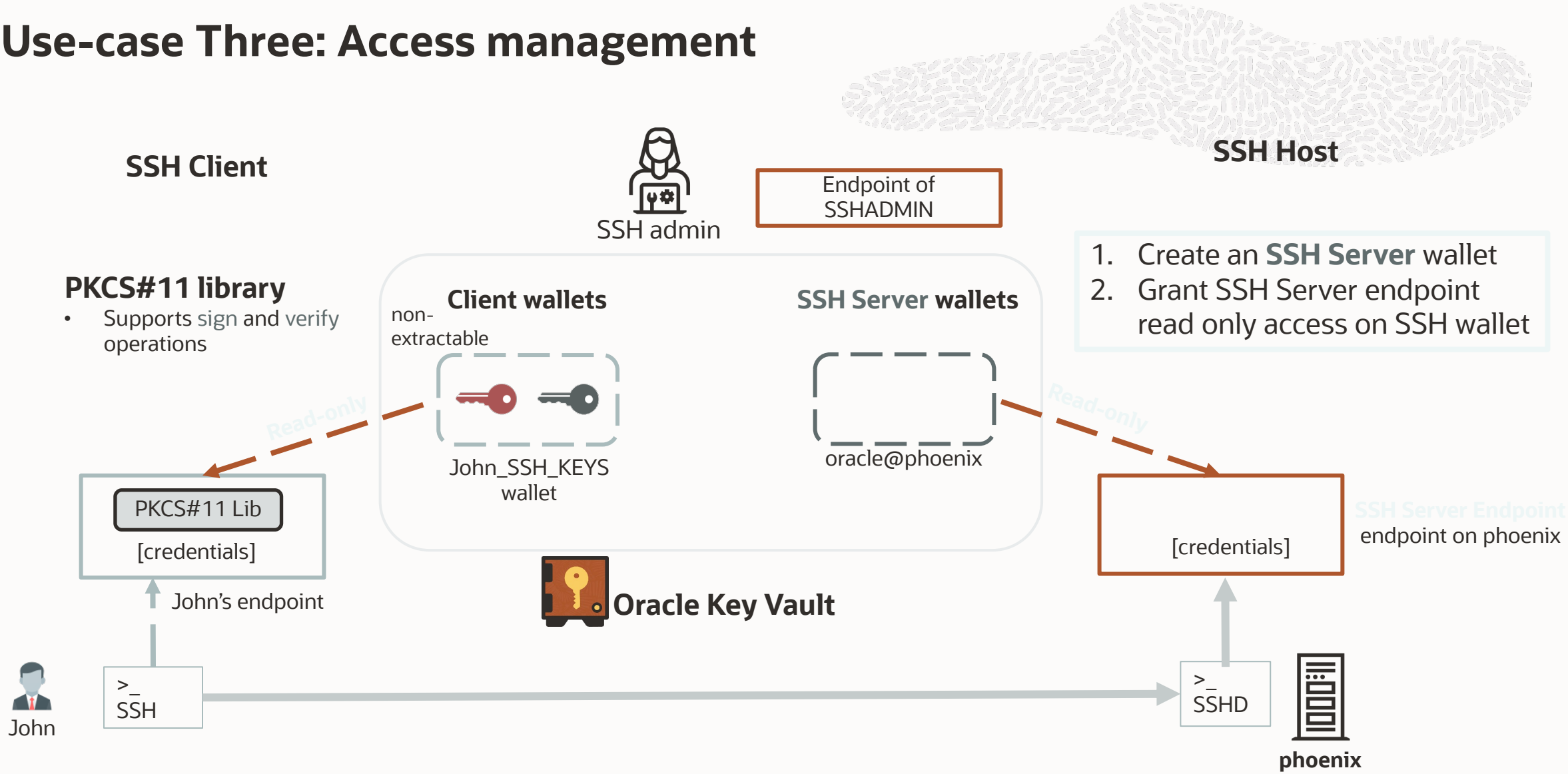
Close

Go Actions

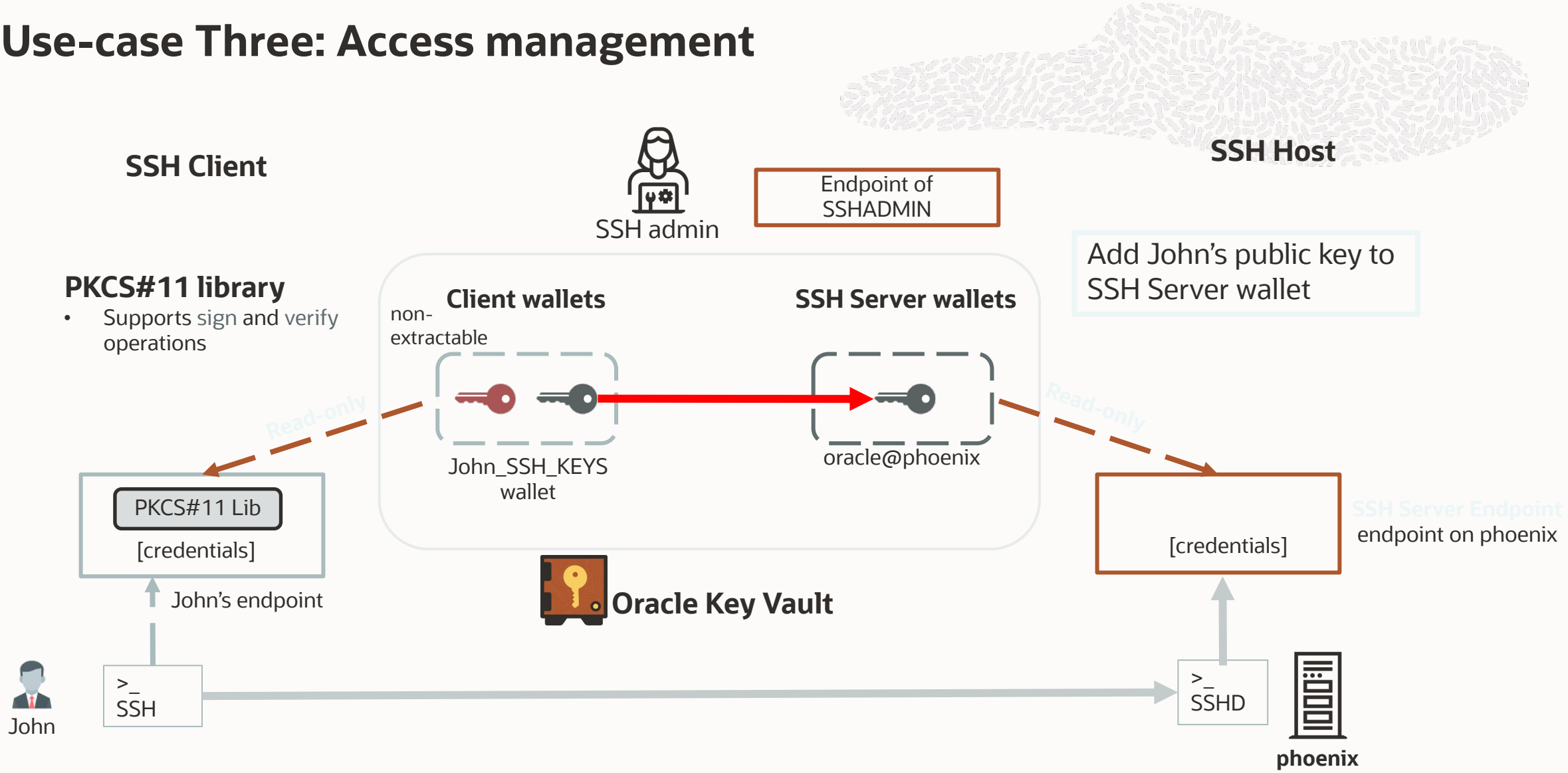
SSH User	SSH User Key Fingerprint	Operation	User	Endpoint	Time	Result
Jill	SHA256:TqernzdN4VmZR1wfNpnXjYWolmoWUgBfII6yXNr1Cuc	Create Key Pair	SSH_ADMIN	-	07-OCT-2023 15:18:03	✔
John	SHA256:z+JQz0VnTQygl7Good5IcDVMsRNM+48i9Ww6RqIhIps	Sign	-	JOHN_EP	07-OCT-2023 15:12:55	✔
John	SHA256:z+JQz0VnTQygl7Good5IcDVMsRNM+48i9Ww6RqIhIps	Get Attribute(s)	-	JOHN_EP	07-OCT-2023 15:12:55	✔
Jane	SHA256:R4+lsT6af1+mC3+IQrhcxVwMSpTXtehsiuSImuHRhkU	Sign	-	JANE_EP	07-OCT-2023 15:12:30	✔
Jane	SHA256:R4+lsT6af1+mC3+IQrhcxVwMSpTXtehsiuSImuHRhkU	Get Attribute(s)	-	JANE_EP	07-OCT-2023 15:12:30	✔
Jane	SHA256:R4+lsT6af1+mC3+IQrhcxVwMSpTXtehsiuSImuHRhkU	Get Attribute(s)	-	JANE_EP	07-OCT-2023 15:10:40	✔
John	SHA256:z+JQz0VnTQygl7Good5IcDVMsRNM+48i9Ww6RqIhIps	Sign	-	JOHN_EP	07-OCT-2023 15:04:50	✔
John	SHA256:z+JQz0VnTQygl7Good5IcDVMsRNM+48i9Ww6RqIhIps	Get Attribute(s)	-	JOHN_EP	07-OCT-2023 15:04:50	✔

1 - 22 of 22

Use-case Three: Access management

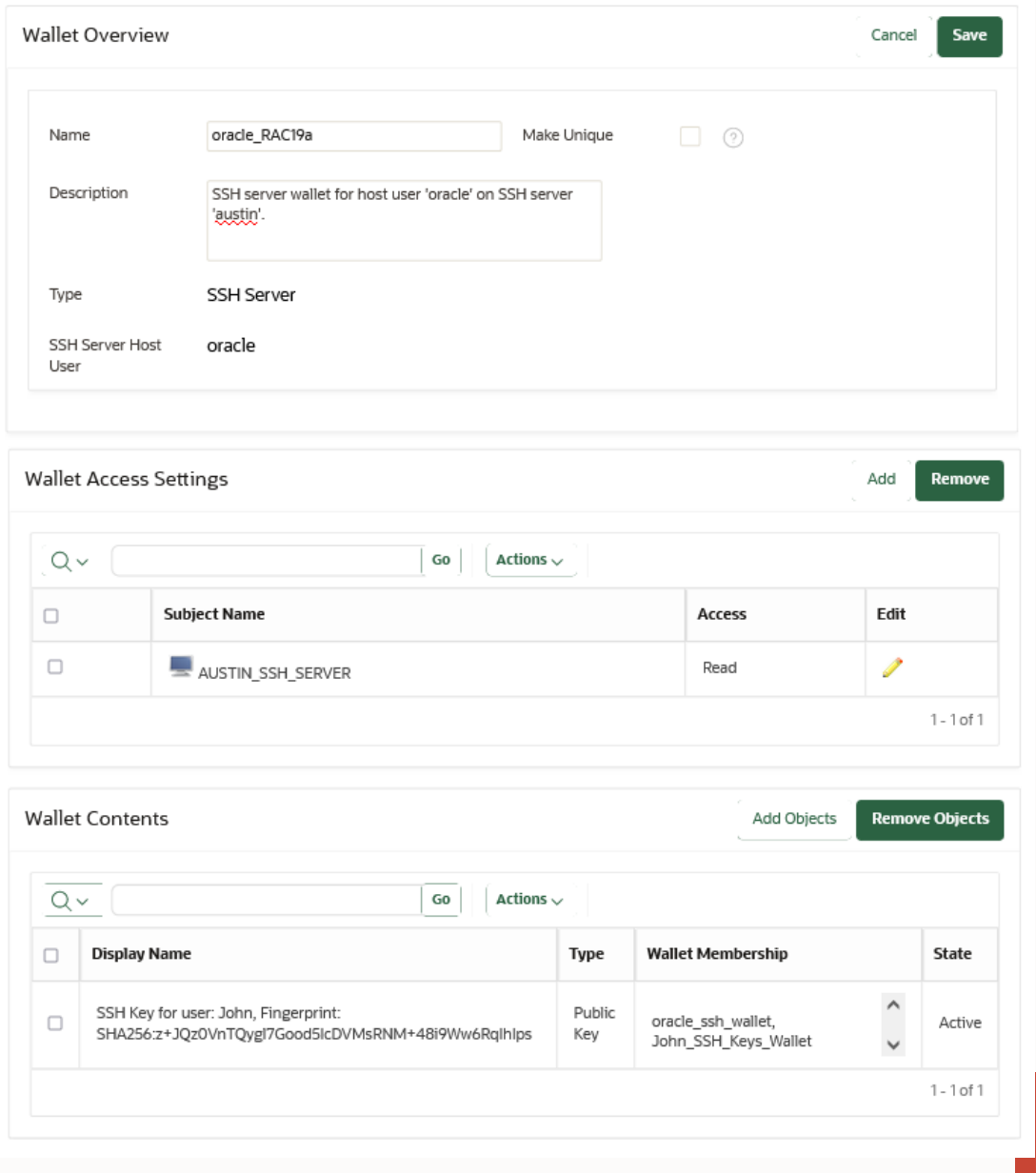


Use-case Three: Access management

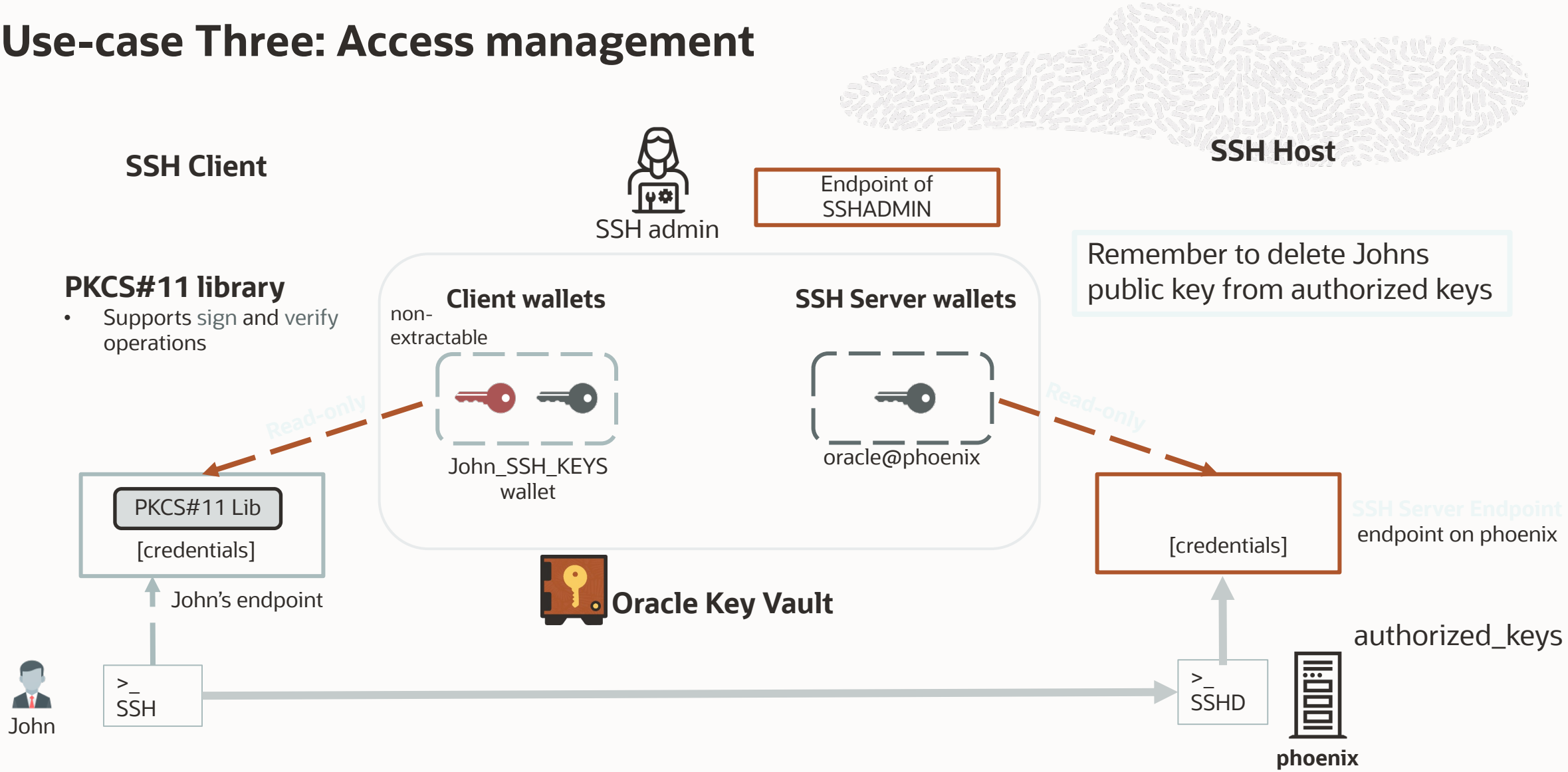


Johns public key in SSH Server Wallet

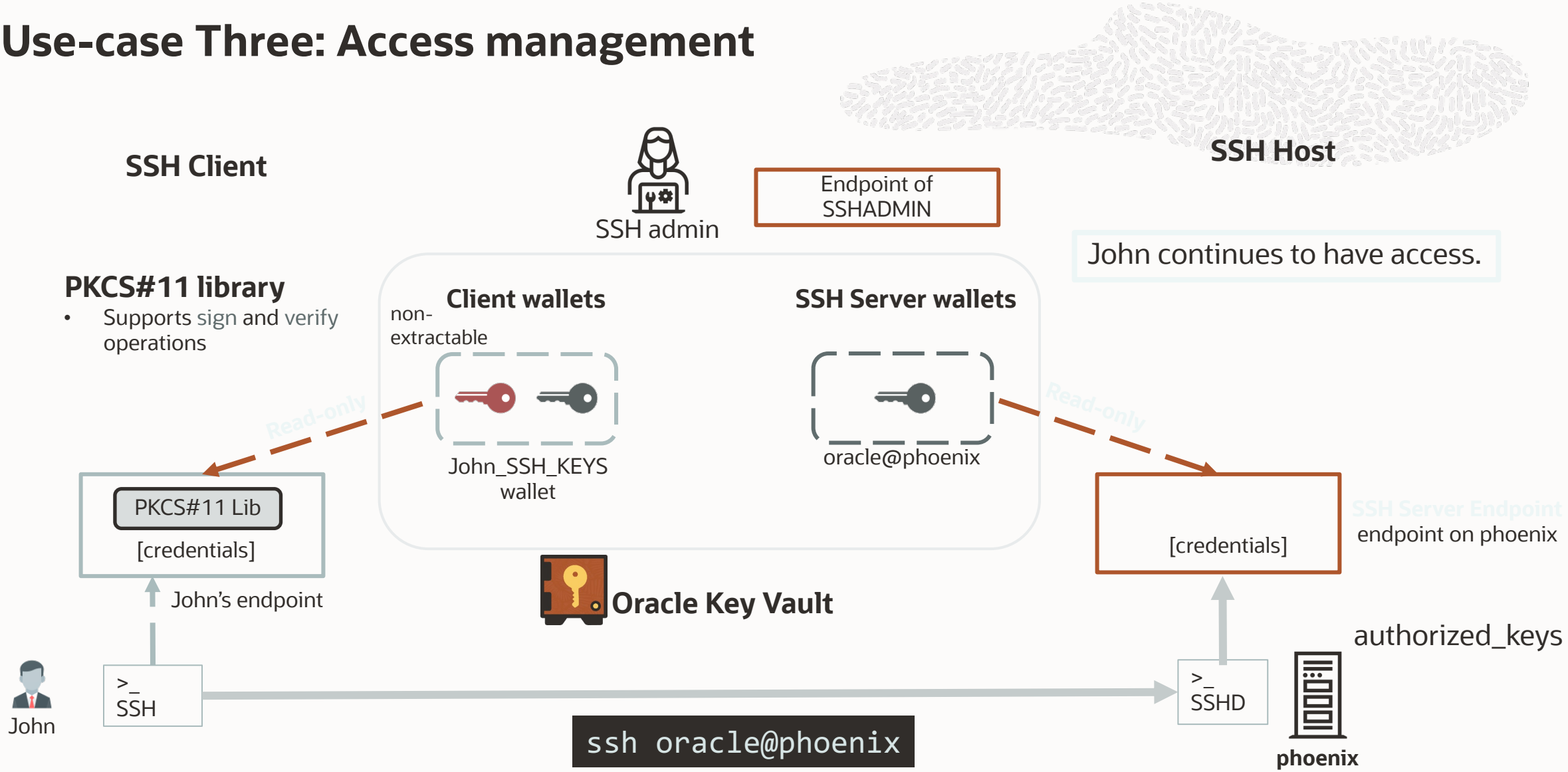
- SSH Server Austin has read-only access on oracle_RAC19a
- oracle_RAC19a has John's public key



Use-case Three: Access management



Use-case Three: Access management



Who has SSH access to which server?

SSH Server Authorization Report

Close

Go

Actions

SSH Server	SSH Server Host User	SSH Server Wallet	SSH User	SSH User Public Key Fingerprint	SSH User Public Key Details
austin.oracle.com	opc	opc_ssh_wallet	Jane	SHA256:R4+IsT6af1+mC3+IQrhcxVwMSpTXtehsiuSImuHRhkU	
austin.oracle.com	oracle	oracle_ssh_wallet	John	SHA256:z+JQz0VnTQygl7Good5IcDVMsRNM+48i9Ww6RqIhIps	
austin.oracle.com	root	root_ssh_wallet_for_austin	Sam	SHA256:HZrIsgGHKr6D4SWT/b2Xb5CHHZByVmO+Dz19J9glj5c	
phoenix.oracle.com	opc	opc_ssh_wallet	Jane	SHA256:R4+IsT6af1+mC3+IQrhcxVwMSpTXtehsiuSImuHRhkU	
phoenix.oracle.com	oracle	oracle_ssh_wallet	John	SHA256:z+JQz0VnTQygl7Good5IcDVMsRNM+48i9Ww6RqIhIps	
phoenix.oracle.com	root	root_ssh_wallet_for_phoenix	Sally	SHA256:Ke4M7IYO4W4XRwpf5/fh3NLs0MgQpiqqirT27h4Dgfw	

1 - 6 of 6

Who attempted to access servers and when?

SSH Server Access Report

Close

Go Actions

SSH Server	SSH Server Host User	SSH User	SSH User Public Key Fingerprint	Access Time	Result
phoenix.oracle.com	oracle	John	SHA256:z+JQz0VnTQygl7Good5IcDVMsRNM+48i9Ww6RqlhIps	07-OCT-2023 15:23:27	✓
phoenix.oracle.com	root	Sally	SHA256:Ke4M7IYO4W4XRwpf5/fh3NLs0MgQpiqqirT27h4Dgfw	07-OCT-2023 15:23:25	✓
phoenix.oracle.com	root	Malfoy	SHA256:a+f5d9UuF7JDYfiyRr1ej1lH2WkvQsp19Bh0Um0Yu44	07-OCT-2023 15:23:24	Failed
austin.oracle.com	opc	Jane	SHA256:R4+lsT6af1+mC3+IQrhcxVwMSpTXtehsiuSImuHRhkU	07-OCT-2023 15:23:24	✓
austin.oracle.com	root	Sam	SHA256:HZrIsgGHKr6D4SWT/b2Xb5CHHZByVmO+Dz19J9glj5c	07-OCT-2023 15:23:23	✓
austin.oracle.com	root	Malfoy	SHA256:a+f5d9UuF7JDYfiyRr1ej1lH2WkvQsp19Bh0Um0Yu44	07-OCT-2023 15:23:23	Failed
phoenix.oracle.com	oracle	John	SHA256:z+JQz0VnTQygl7Good5IcDVMsRNM+48i9Ww6RqlhIps	07-OCT-2023 15:12:50	✓
austin.oracle.com	opc	Jane	SHA256:R4+lsT6af1+mC3+IQrhcxVwMSpTXtehsiuSImuHRhkU	07-OCT-2023 15:12:20	✓
phoenix.oracle.com	oracle	John	SHA256:z+JQz0VnTQygl7Good5IcDVMsRNM+48i9Ww6RqlhIps	07-OCT-2023 15:04:41	✓
phoenix.oracle.com	oracle	John	SHA256:z+JQz0VnTQygl7Good5IcDVMsRNM+48i9Ww6RqlhIps	07-OCT-2023 13:40:36	✓
phoenix.oracle.com	root	Sally	SHA256:Ke4M7IYO4W4XRwpf5/fh3NLs0MgQpiqqirT27h4Dgfw	07-OCT-2023 13:40:35	✓

1 - 20 of 20

Want to learn more?

Free hands-on labs that help you learn how to use the different security features and options

bit.ly/golivelabsdbsec

Database Security office hours – second Wednesday of each month

bit.ly/asktomdbsec

Securing the Oracle Database – a technical primer (fifth edition)

oracle.com/securingthedatabase

Questions?

Thank you!

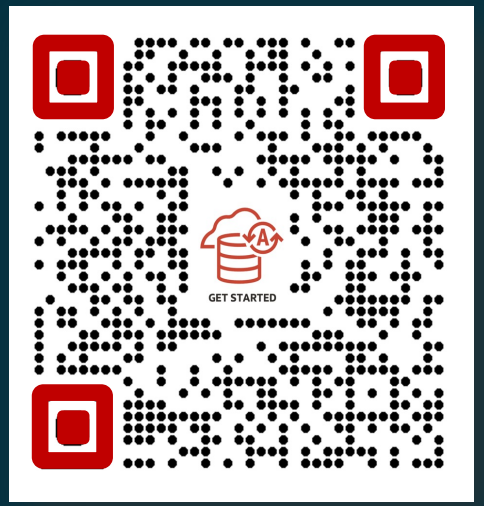
Peter Wahl
Peter.Wahl@oracle.com

Q&A Open

Important links to bookmark

Links to get you started and to keep up to date with Autonomous Database

1 **New Get Started Page:**
bit.ly/adb-get-started



2 **Join us:**

LinkedIn
bit.ly/adb-linkedin-grp

X
@AutonomousDW

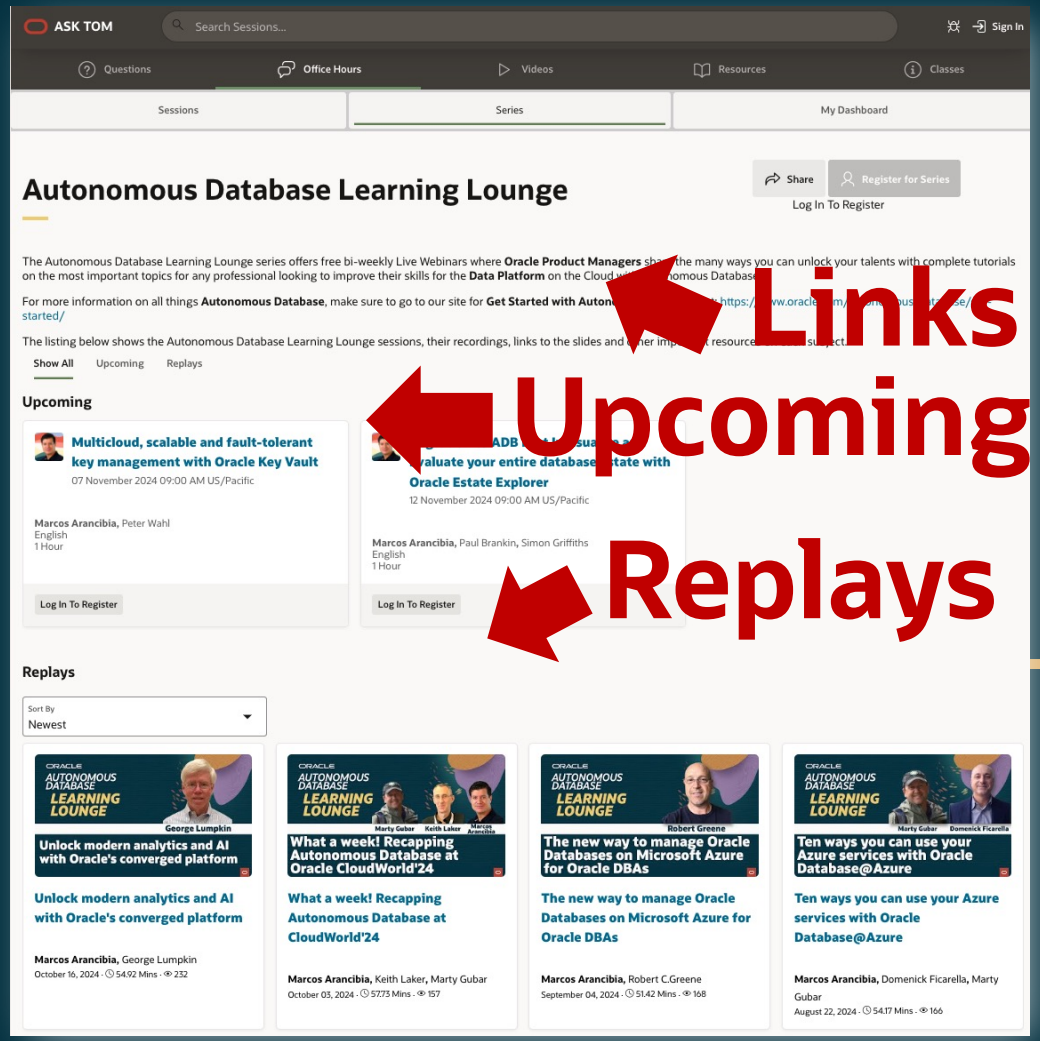
3

Got a question?
We are on stackoverflow
bit.ly/adb-stackoverflow

Join us on Developers Slack
(search #oracle-autonomous-database)
bit.ly/odevrel_slack (odevrel_slack)

Final Thoughts

oracle.com/goto/adb-learning-lounge



Upcoming Session

AUTONOMOUS DATABASE

LEARNING LOUNGE

Thank you for joining today's webinar !!!

—