Customer Releasable

SAP ASE Options:
Security & Availability Update

Jeff Tallman jeff.tallman@sap.com
SAP ASE Product Management

Agenda

Security Update

- Options & Packaging
- SSL & Network Encryption
- Data/Database Encryption
- Granular Permissions

ASE Always-On

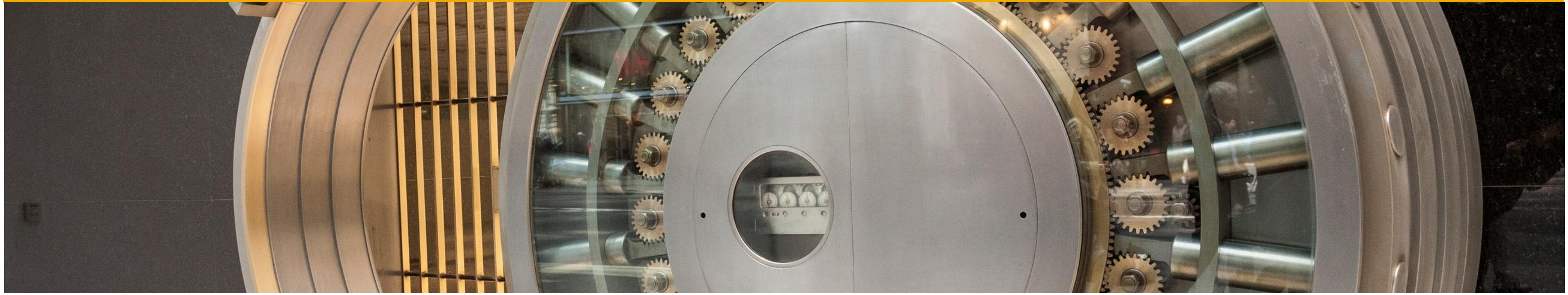
- Overview
- External Replication

Always-On Future Development/Roadmap

Legal Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. This presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this document is not a commitment, promise or legal obligation to deliver any material, code or functionality. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This document is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this document, except if such damages were caused by SAP´s willful misconduct or gross negligence.

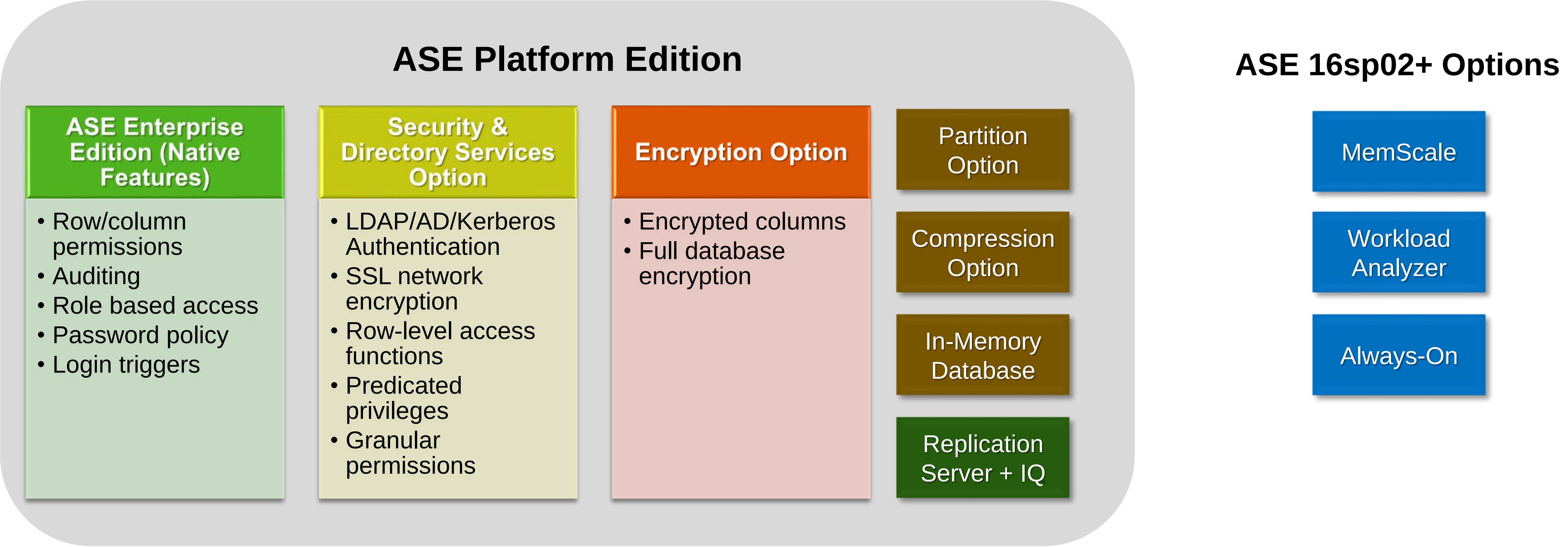
All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.



ASE Security

Features & Options

ASE Options & Bundling*



ASE Platform Edition

ASE Enterprise Edition (Native Features)

- Row/column permissions
- Auditing
- Role based access
- Password policy
- Login triggers

Security & Directory Services Option

- LDAP/AD/Kerberos Authentication
- SSL network encryption
- Row-level access functions
- Predicated privileges
- Granular permissions

Encryption Option

- Encrypted columns
- Full database encryption

Partition Option

Compression Option

In-Memory Database

Replication Server + IQ

ASE 16sp02+ Options

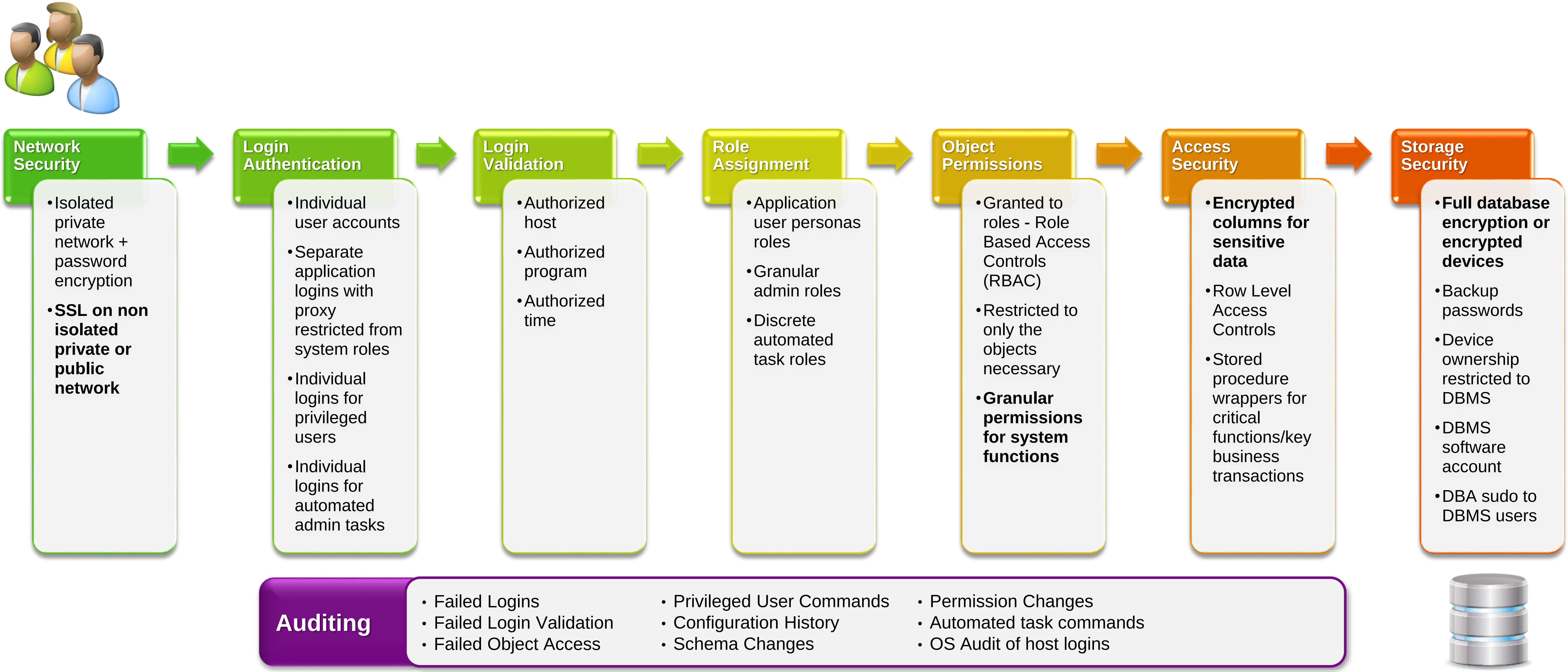
MemScale

Workload Analyzer

Always-On

*Please consult your sales rep for latest bundling/packaging details and any licensing/pricing questions

ASE Security Model → Defense in Depth (Multi-Layered)



Network Security

- Isolated private network + password encryption
- **SSL on non isolated private or public network**

Login Authentication

- Individual user accounts
- Separate application logins with proxy restricted from system roles
- Individual logins for privileged users
- Individual logins for automated admin tasks

Login Validation

- Authorized host
- Authorized program
- Authorized time

Role Assignment

- Application user personas roles
- Granular admin roles
- Discrete automated task roles

Object Permissions

- Granted to roles - Role Based Access Controls (RBAC)
- Restricted to only the objects necessary
- **Granular permissions for system functions**

Access Security

- **Encrypted columns for sensitive data**
- Row Level Access Controls
- Stored procedure wrappers for critical functions/key business transactions

Storage Security

- **Full database encryption or encrypted devices**
- Backup passwords
- Device ownership restricted to DBMS
- DBMS software account
- DBA sudo to DBMS users

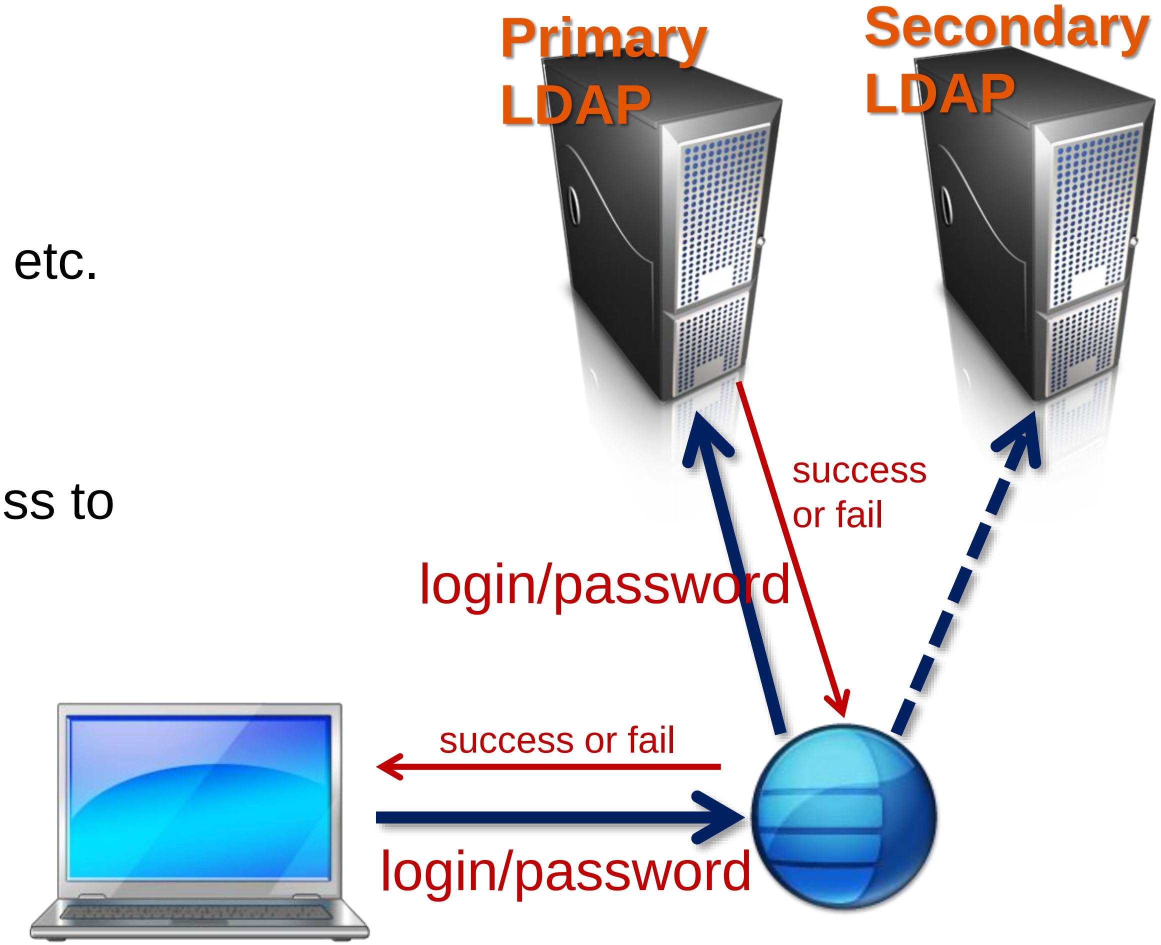
Auditing

- Failed Logins
- Failed Login Validation
- Failed Object Access
- Privileged User Commands
- Configuration History
- Schema Changes
- Permission Changes
- Automated task commands
- OS Audit of host logins

LDAP/Windows AD Authentication

External Authentication

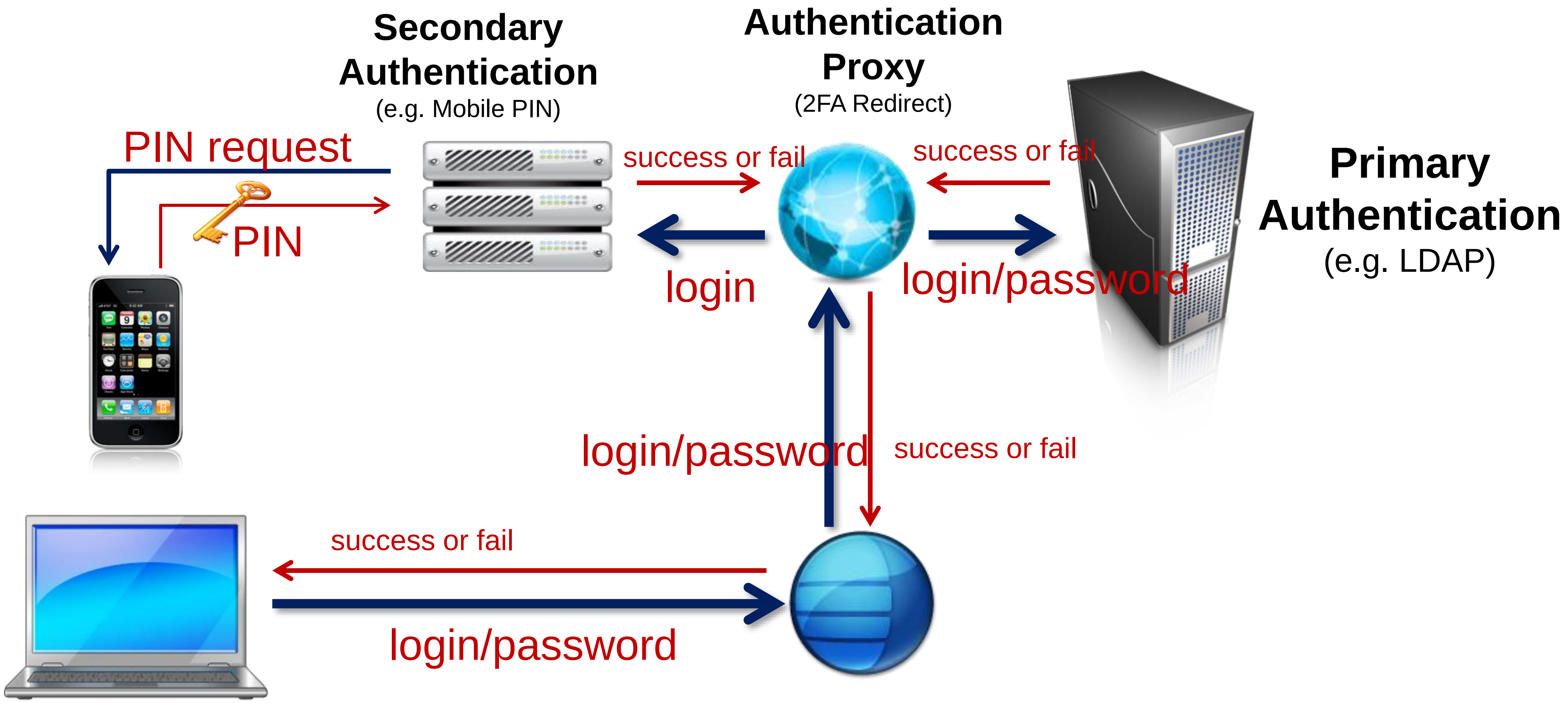
1. ASE receives user & password
2. Syslogins maps to external authentication
3. ASE sends login credentials to LDAP, AD, etc.
4. LDAP server validates credentials
5. LDAP sends success to ASE
6. ASE finishes connection and sends success to client



Two Factor Authentication (2FA)

Problem: Standard SQL API for login authentication only provides loginname & password (or token)

Solution: Use an authentication proxy to support 2FA or biometrics



ASE support for SSL/TLS

TLS 1.2 support

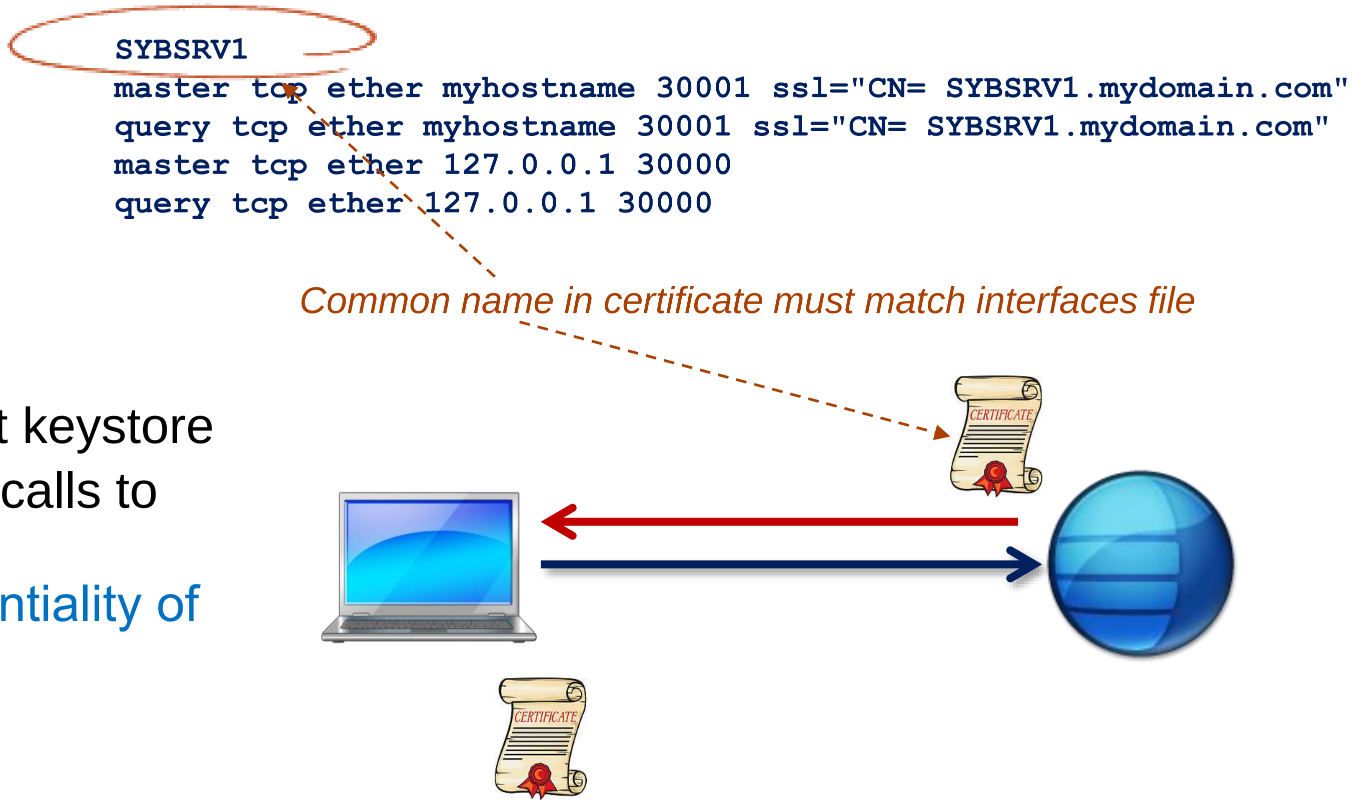
- ASE 15.7 sp137 or ASE 16 sp02 pl04
- Prior versions only supported TLS 1.0

Setting it up….can be a bit fun

- You have to get the certificate
- You have to set the server’s trusted CA list
- You have to configure an SSL listener
- You have to load the server certificate in client keystore
- You have to change your app connection API calls to invoke SSL (or conn props)
- See Security Admin Guide, section 9 ‘Confidentiality of Data’

There is performance overhead

- All encryption has overhead
- 40KB more memory per connection
- Can be 2x longer round trip time



```
SYBSRV1
master tcp ether myhostname 30001 ssl="CN= SYBSRV1.mydomain.com"
query tcp ether myhostname 30001 ssl="CN= SYBSRV1.mydomain.com"
master tcp ether 127.0.0.1 30000
query tcp ether 127.0.0.1 30000
```

Common name in certificate must match interfaces file

Server certificate must be in client keystore!!!

ASE 16 SP03 & SSL

Future

Currently both ASE & SRS use OpenSSL implementation

- FIPS/NIST certified OpenSSL implementation
- Problem is that with any large code project with code freeze >3 months before GA, the near constant patching of OpenSSL is a problem

SAP Common Cryptographic Library

- Supports SSL for network security
- Currently in last/final phase of FIPS/NIST certification
- Will replace OpenSSL starting with ASE 16 SP03 & SRS release Q2’17
- IQ will adopt at some point as well (schedule/release unknown)

Alternative to SSL

SSL has performance penalty

- Connection speed up to 2x slower
- Data transmit speeds up to 2x slower
- Performance penalty not completely offset by proprietary encryption chips on motherboard
  - ✓ May only help by 40% + limited platforms/versions
- However, it encrypts entire end-to-end data stream
  - ✓ Application to DBMS

Hardware Network Encryption

- Advantages
  - ✓ Transparent to applications
  - ✓ Easier implementation
  - ✓ Supports advanced policies
  - ✓ Much better performance
    - Low latency applications
  - ✓ Likely cheaper (priced per device vs. per core)
- Disadvantages
  - ✓ Susceptible to sniffing programs on same host as applications or DBMS
  - ✓ Need to purchase high-end units to support 10GbE
    - Entry level & mid-range only support 100Mbs or 1Gbs

ASE 16SP03 Feature: On Demand Encryption

Future

Problem

- Password encryption is enforced during login, but if user changes password, the old & new passwords are sent in clear unless using SSL
- Other commands with sensitive data have similar issues (e.g. encryption passwords, etc.)
  - ✓ See list
  - ✓ Intent is that programmer would invoke on demand encryption before sending these commands and likely disable afterwards

Encryption added to OpenClient directly

- no SSL necessary
- negotiated symmetric session key between client and server
- AES algorithm with 256 bit keys.
- Support in CTLib - probably JDBC & ODBC
- Isql will use “go encrypt” vs. “go” for command/batch terminator

```
alter encryption key
alter login
alter role
connect
create cluster
create encryption key
create login
create role
deploy plugin
drop encryption key
dump database
dump transaction
load database
load transaction
set cluster
set encryption passwd
set role
show agent
upgrade server
sp_addexternlogin
sp_addlogin
sp_companion
sp_encryption
sp_extrapwdchecks
sp_ldapadmin
sp_password
sp_ssladmin
```

Restrict Owner Permission

Similar to ‘restricted decrypt permission’….

- Added in ASE 15.0+
- By default, with encrypted columns, the object owner has decrypt permission
  - ✓DBA’s with sa_role become ‘dbo’ in any database and could see the data
- Enabling the ‘restricted decrypt permission’…
  - ✓Blocks ‘owner’ from being able to decrypt data
  - ✓Only allows the SSO to grant decrypt permission
  - ✓SSO can grant decrypt permission ‘with grant option’ to allow others to grant decrypt

ASE 16 SP02 PL06 (or SP03) will add ‘restrict owner permission’

- By default, the object owner has full DML permissions on the object
- By enabling this, object owner no longer has DML permissions
  - ✓As with restrict decrypt permission, it will likely fall to the SSO and be grantable
- Keep in mind that this may make debugging queries more difficult
  - ✓Although there still is that ‘setuser’ command……(for Suite users, this is pretty normal)

Future

Granular Permissions (ASE 15.7 ESD #2)

Normally ASE has a few defined system roles

- sa_role, sso_role, oper_role

Problem

- Some sites need to restrict actions of junior DBA’s, outsourced DBA’s or 3rd party apps

Granular Permissions

- Provides ~50 DBA actions as separate grantable options
- Essentially makes sa_role more limited
  - ✓You will need to grant ‘sa’ permissions to do things that previously it could with sa_role
- Intent is that ‘sa’ would be only user with sa_role/sso_role
  - ✓You would then create multiple levels of sa/sso roles and grant as needed
    - Backup_role, recovery_role, dbcc_role
    - Manage_logins_role
    - hw_resource_role (e.g. ability to change caches, add/remove engines from thread pools, etc.)
  - ✓You could also grant dbcc and other permissions to schema owners

Automated processes & tiered DBA/SSO’s (1)

DBA Role	Granular permissions			
		DB Administration Roles		
dbcc_role	dbcc checkalloc any database dbcc checkcatalog any database dbcc checkdb any database dbcc checkindex any database	dbcc checkstorage any database dbcc checktable any database dbcc checkverify any database dbcc fix_text any database	dbcc indexalloc any database dbcc reindex any database dbcc tablealloc any database dbcc textalloc any database	manage checkstorage report checkstorage
pnt_role	dbcc tune kill any process checkpoint any database set switch set tracing any process	show switch manage any execution class manage any statistics reorg any table	manage any thread pool manage disk manage lock promotion threshold manage resource limit	manage server monitor qp performance manage abstract plans select any system catalog
backup_role	checkpoint any database	dump any database	quiesce any database	manage dump configuration
recovery_role	checkpoint any database quiesce any database mount any database	load any database online any database create database	manage any database unmount any database	identity_insert any table identity_update any table
dbmaint_role	manage any statistics	reorg any table	select any system catalog	
svradm_role	allow exceptional login connect dbcc tune kill any process manage any ESP	manage any thread pool manage cluster manage disk manage server manage server configuration	set switch show switch shutdown map external file	select on get_appcontext select on list_appcontext select on rm_appcontext select on set_appcontext
		DB Security Roles		
useradm_role	change password manage any login manage any login profile	manage any remote login manage roles	manage any user (in any database) update any security catalog (in any database)	show switch set tracing any process
ssoadm_role	manage security permissions manage auditing	manage security configuration alter any object owner (in any database)	decrypt any table (in any database) manage any encryption key (in any database)	select on authmech
devsec_role	manage any object permission	manage any user	manage database permissions	
devtest_role	setuser			

Automated processes & tiered DBA/SSO’s (2)

DBA Role	dbcc_role	pnt_role	mon_role	backup_role	recovery_role	dbmaint_role	svradm_role	sybase_ts_role	useradm_role	ssoadm_role	devsec_role	devtest_role
junior_dba	✓		✓	✓		✓						
senior_dba	✓	✓	✓	✓	✓	✓	✓	✓				
performance_dba		✓	✓					✓				
access_sec_sso									✓		✓	
system_sec_sso									✓	✓	✓	
app_developer (in dev/test)												✓

Column Encryption in ASE

Column Encryption (ASE 12.5.4 and later)

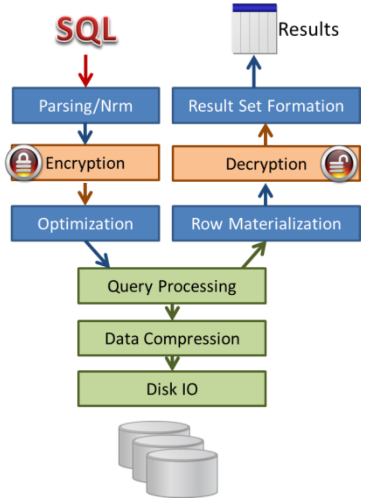
- Totally secure – encrypted on disk, in memory, in log, etc…..
- Each column can be encrypted with separate keys
  - Assumes different users with different access requirements
  - Prevents inadvertent disclosure to authorized users of system but not authorized for data
- Column decrypt permission with data masking (unique to ASE)
  - e.g. ###-##-####

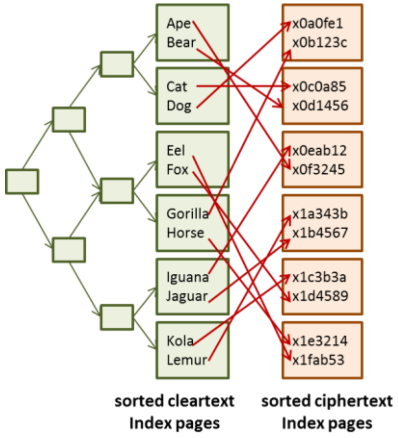
Impacts on performance

- Good news: Indexable encryption for Pkey and Fkey columns
  - Unique to ASE vs. Oracle and other competitive implementations
- Bad news:
  - Range queries (due to ciphertext sorting) and other qp issues
  - Blocks compression effectiveness (if a SALT/IV is used)

Certified with SAP applications….but….

- Only provides disk level protection as SAP uses common login





Works extremely well on account numbers, employee id, SSN, health test results, etc. (equi-SARGS)

Doesn’t work well on Date of Birth, Last Names, etc. due to range queries – nor also on ORDER BY/GROUP BY columns that are indexed (queries still work but could be slower or a lot slower)

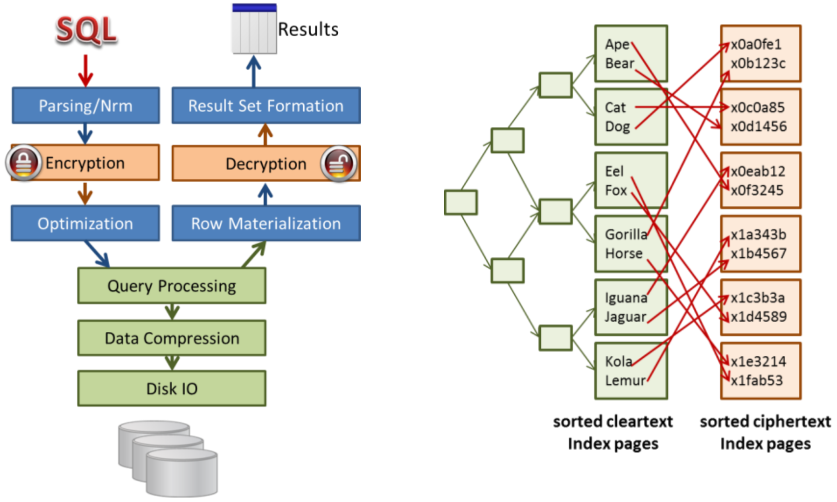
Full Database Encryption

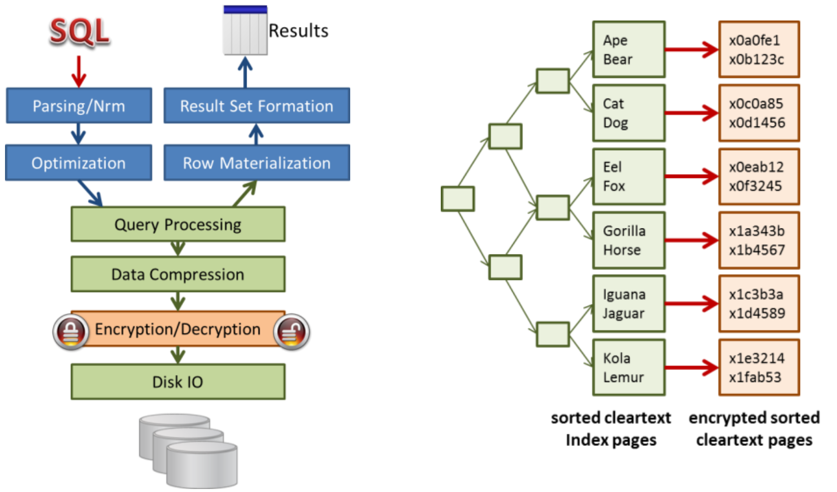
Full Database Encryption (new in ASE 16)

- Provides protection for an entire database, WITHOUT affecting existing applications
  - ✓All data, indexes, and transaction logs in database are encrypted
  - ✓Backed up database in encrypted form
  - ✓All authorized database users can see data
- No impact on range queries or compression
- Encryption is at page level
  - ✓as pages are written to disk, and decryption before they are loaded into memory
  - ✓Will be after/before Compression/Decompression
- Can be used with column encryption
- Dual key control with automatic startup

Can be implemented online w/o user impact

- Can be suspended/resumed for long run times





Database Encryption

Uses Database Encryption Key to encrypt a database – symmetric key

- User has to create the key before database encryption

```
create encryption key key_name [for AES] for database encryption
 [with {[master key] [keylength 256] [init_vector random] [[no]dual_control]}
```

  ✓Default is init_vector random (mandatory)

  ✓Example:

```
Create encryption key test_key for database encryption with master_key
Create encryption key test_key for database encryption with dual_control
```

- Master key and dual master key will be used to protect test_key

Create database with encryption

- Create a new encrypted database

```
Create [temporary] database database_name encrypt with key_name
```

- Alter an existing database to be encrypted

```
Alter database database_name encrypt with key_name
```

ASE Data Encryption/Data Security vs. Competition

Data Security Feature	ASE 16	MS 2016	Postgres	ORA 12
Transparent full database encryption	✓	✓	✗	✓
Encryption functions (for column/data encryption in SQL)	🛠	✓	✓	✓
Transparent column encryption (no application mods/key storage)	✓	✗	✗	✓
Decrypt permission on encrypted columns	✓	✗	✗	✗
Dynamic masking/redacting of cipher text on encrypted columns	✓	✗	✗	🛠
Encrypted cols in indexes/joins	✓	🛠	🛠	✗
DBA can be prohibited from viewing encrypted column data	✓	✓	?	🛠
Dual key control	✓	✗	?	✓
Export encrypted data	✓	☯	☯	✓
Row level access (using UDF or ACF in rules bound to table)	✓	✓	✓	🛠
Predicated Privileges (grant with where clause)	✓	✗	✗	

ASE Data Encryption/Data Security vs. Competition

Data Security Feature	ASE 16	Comments
Transparent full database encryption	✓	
Encryption functions (for column/data encryption in SQL)	🛠	Can be implemented via JAVA in ASE & SQLJ UDF
Transparent column encryption (no application mods/key storage)	✓	
Decrypt permission on encrypted columns	✓	
Dynamic masking/redacting of cipher text on encrypted columns	✓	
Encrypted cols in indexes/joins	✓	Natively supported as long as no SALT/IV
DBA can be prohibited from viewing encrypted column data	✓	
Dual key control	✓	
Export encrypted data	✓	Security on decrypt permission plus key export mechanisms allow secure transfer of encrypted data using bulk libraries via flat files
Row level access (using UDF or ACF in rules bound to table)	✓	
Predicated Privileges (grant with where clause)	✓	

ASE Data Encryption/Data Security vs. Competition

Data Security Feature	MS 2016	Comments
Transparent full database encryption	✓	
Encryption functions (for column/data encryption in SQL)	✓	Only supports encryption functions, which requires app changes to include encr f() in SQL as well as either embedding keys/passphrases in the app or integrating with external key management system.
Transparent column encryption (no application mods/key storage)	✗	
Decrypt permission on encrypted columns	✗	Anyone with key can encrypt & decrypt data. Consider internet and credit cards orders – users shouldn't be able to decrypt cc
Dynamic masking/redacting of cipher text on encrypted columns	✗	Data isn't protected from attempts to break encryption – e.g. low cardinality data can be easily broken if no SALT/IV.
Encrypted cols in indexes/joins	🛠	No explicit support, but might be achievable using function-based indices and using same keys on join columns
DBA can be prohibited from viewing encrypted column data	✓	If using .NET, the encryption functions are executed at the client, so DBA can't even determine the key to call functions directly
Dual key control	✗	Keys are not managed by DBMS/SSO
Export encrypted data	☯	Indirectly as table simply contain cipher text as if binary strings and key management is via application/external
Row level access (using UDF or ACF in rules bound to table)	✓	
Predicated Privileges (grant with where clause)	✗	

ASE Data Encryption/Data Security vs. Competition

Data Security Feature	Postgres	Comments
Transparent full database encryption	✗	Requires a work-around with encrypted file systems for storage as well as backup directories. DBMS needs key.
Encryption functions (for column/data encryption in SQL)	✓	Only supports encryption functions, which requires app changes to include encr f() in SQL as well as either embedding keys/passphrases in the app or integrating with external key management system.
Transparent column encryption (no application mods/key storage)	✗	
Decrypt permission on encrypted columns	✗	Anyone with key can encrypt & decrypt data. Consider internet and credit cards orders – users shouldn't be able to decrypt cc
Dynamic masking/redacting of cipher text on encrypted columns	✗	Data isn't protected from attempts to break encryption – e.g. low cardinality data can be easily broken if no SALT/IV.
Encrypted cols in indexes/joins	🛠	No explicit support, but might be achievable using function-based indices and using same keys on join columns
DBA can be prohibited from viewing encrypted column data	?	Unknown. If DBA can monitor SQL execution, they can see key and functions, therefore likely the answer is no.
Dual key control	?	Unknown. Examples only refer to passphrase vs. key encryption. Keys do not seem to be managed by DBMS/SSO.
Export encrypted data	☯	Indirectly as table simply contain cipher text as if binary strings and key management is via application/external
Row level access (using UDF or ACF in rules bound to table)	✓	
Predicated Privileges (grant with where clause)	✗	

ASE Data Encryption/Data Security vs. Competition

Data Security Feature	ORA 12	Comments
Transparent full database encryption	✓	
Encryption functions (for column/data encryption in SQL)	✓	This was oracle's first attempt at column encryption – tried to claim app transparency via instead of triggers
Transparent column encryption (no application mods/key storage)	✓	Supported after complaints about app impact of encrypt functions
Decrypt permission on encrypted columns	✗	Anyone table permissions can encrypt & decrypt data. Consider internet and credit cards orders – users shouldn't be able to decrypt cc
Dynamic masking/redacting of cipher text on encrypted columns	🛠	Requires Oracle Vault – which supports masking/redacting any column
Encrypted cols in indexes/joins	✗	Indexing encrypted columns not supported. Different tables use different keys, therefore joins and fkey not supported
DBA can be prohibited from viewing encrypted column data	🛠	Requires Oracle Vault
Dual key control	✓	
Export encrypted data	✓	
Row level access (using UDF or ACF in rules bound to table)	🛠	Requires Oracle (I forget name) package which supports a typical Oracle package API (procs) vs. declarative SQL. However, it does support where clauses (not sure if subqueries) as API params if I remember correctly.
Predicated Privileges (grant with where clause)		

SAP Adaptive Server Enterprise (ASE)
Product road map overview - key themes and capabilities

Recent innovations

XOLTP Enhancements
- Lockless Cache
- Latch-Free B-Tree
- NVCache
- SNAP (Compiled Queries)

Data Center Operations & Security
- Always-On
  - HADR Clusters
  - External Replication Support
- Workload Analyzer
- DSAM (storage tiering)
- SAP ASE Cockpit

Cloud Services
- AWS, Azure as BYOL
- Docker support
- HCP & MCD DBaaS

SAP HANA Integration
- A4A

Business Suite/SAP Applications
- CDS functionality Phase 1

ASE 16 SP02 PL05 is current release

2017 – Planned innovations

XOLTP Enhancements
- In-Memory Row Store
- Hash based index
- MVCC

Data Center Operations & Security
- Always-On Enhancements
- CCL for SSL
- Idle timeout
- Granular Auditing
- On Demand Network Encryption

Cloud Services
- Cloud backup services

SAP HANA Integration
- SAP HANA Schema
- SAP HANA SQL Script

Business Suite/SAP Applications
- CDS functionality Phase 2
- Technical Monitor Cockpit
- Built-in SAP ASE Long term performance Data Repository (BALDR)

2018 – Product direction

XOLTP Enhancements
- In-Memory Only Tables
- Temporal SQL/Time Series
- >4TB memory & >32K connections
- Proc cache enhancements
- C UDF, JSON, etc.

Data Center Operations & Security
- 64 bit MDA + MDA repository
- Role based resource limits
- Always-On Enhancements
  - Support CI mode for non-HADR
  - XA Support, Standby Database
- HSM, LDAP Groups
- Data Masking

Cloud Services
- Cloud DR services

SAP HANA/IQ Integration
- Optimized, zero loss data movement to SAP HANA & IQ
- Common Tooling (phase 1)

Business Suite/SAP Applications
- CDS functionality Phase 3

2019 – Product vision

XOLTP Enhancements
- Lazy Persistence
- Non-locking R/O tables/partitions

Data Center Operations & Security
- Workload Analyzer with MDA
- Workload network replay
- Page migration utility
- Undo/redo log utility
- User certificate authentication

Cloud Services
- Cloud services phase 3

SAP HANA/IQ Integration
- Query Enhancements
- Common Tooling (phase 2)

Business Suite/SAP Applications
- CDS functionality Phase 4
- FSI Solutions
- Blockchain, Data lineage, Forensic auditing

This is the current state of planning and may be changed by SAP at any time.

ASE 16sp02 Always-On Option

ASE High Availability + Disaster Recovery

Technology Trends

Most DBMS HA solutions are moving to HADR clusters using streaming replication

Rationale

- Hardware, OS & Storage agnostic
  - ✓No need for shared disk
  - ✓No need for OS HA services nor special storage protocols
- Much more supportable in cloud deployments (private or public)
- Supports in-memory processing techniques vs. shared disk clusters (SDC)

Technology du-jour for “NewSQL”

- MemSQL, Postgres, et al.

Only vendors staying with HW/OS implementations are Oracle & IBM

- But then they have a vested interest in HW
- Both also have HADR clusters

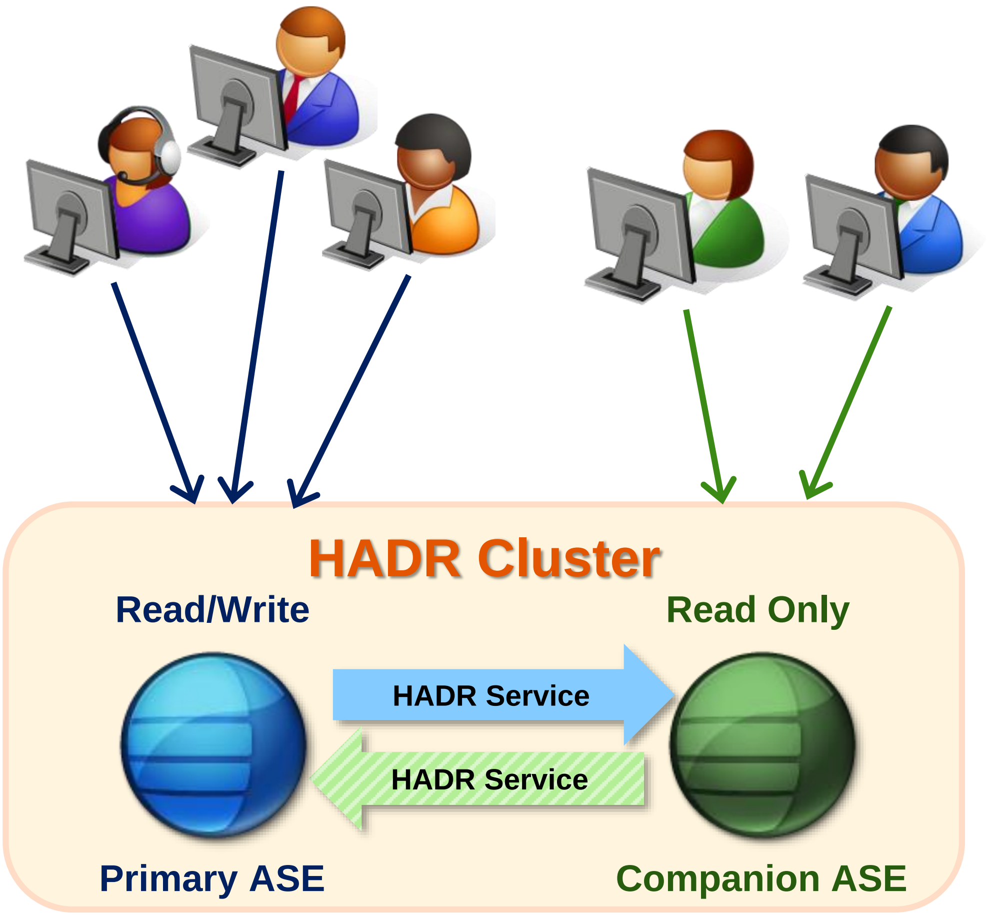
HADR Clusters (e.g. ASE Always On)

Core technology

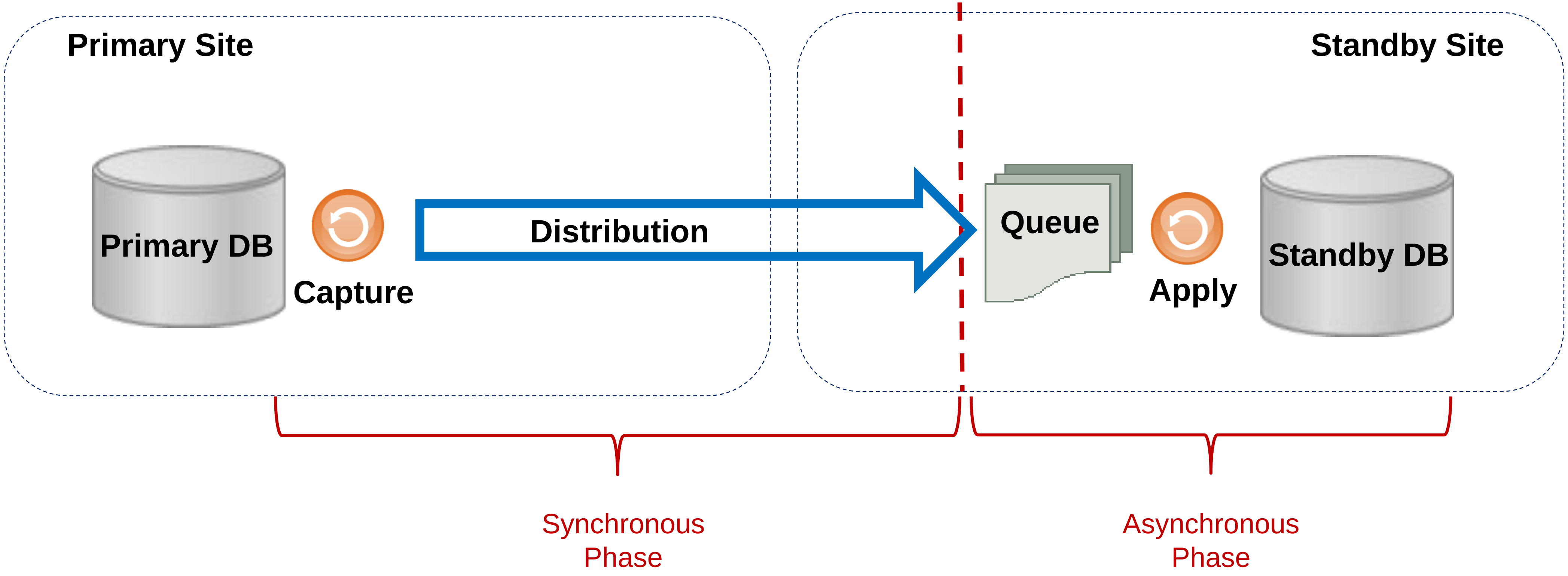
- Log record-based *streaming* data replication
- Usually supports sync, near-sync and async modes
  - ✓Sync → commit on recv persistence/async apply
  - ✓Near-Sync → commit on recv receipt/async apply
  - ✓Async → commit immediately/async send & apply

2 Classes Types

- Physical
  - ✓Log records are applied as log records/log replay mode
- Logical
  - ✓Log records are translated into SQL for apply



HADR Fundamental Data Synchronization



The 2 choices: Physical vs. Logical Apply

Physical Apply

- Copies log records by copying log blocks physically and transmitting binary page/block image to remote copies
- Remote system simply re-applies log image
- Advantages
  - ✓ No problems with large transactions, SQL handling
- Disadvantages
  - ✓ Cannot handle schema changes (application upgrade availability scenarios)
  - ✓ If log block images vs. log records, still could incur log page corruptions
  - ✓ Database must be page-for-page mirror image
  - ✓ The above blocks DB maintenance on standby

Used by:

- Everyone else (Oracle, IBM, MSSQL)

Logical Apply

- Copies & batches up only necessary log records
  - ✓ E.g. can skip index inserts, allocation records, etc.
- Remote system applies via SQL language
- Advantages
  - ✓ Lower bandwidth
  - ✓ Don't need to replicate reorg actions, etc.
  - ✓ Database does not have to be completely page for page mirror image
    - Allows reorgs, update stats, etc. on standby
  - ✓ Can handle schema changes (provided transport supports transformation capabilities)
- Disadvantage
  - ✓ Large txns, long running txns, SQL issues
  - ✓ Performance can take some tuning

Used by:

- ASE Always-On, Oracle DataGuard (Logical Apply mode)

The Competition: Oracle DataGuard & IBM DB2 HADR

No one is TRULY Synchronous

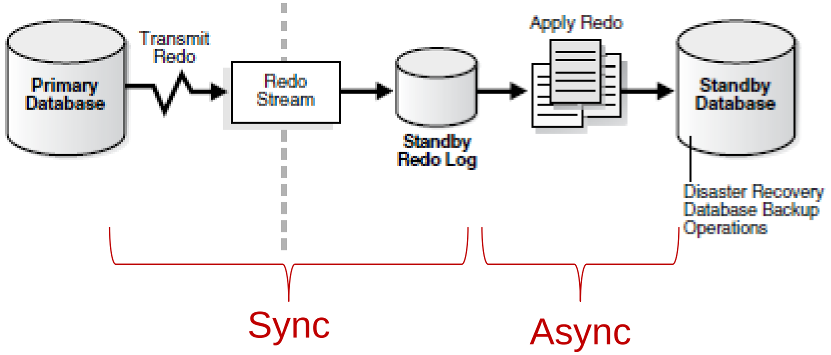
Oracle DataGuard

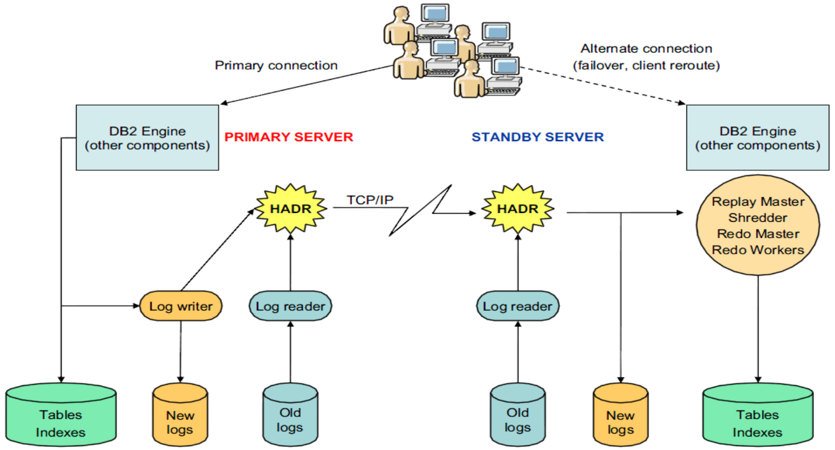
- Synchronous to Remote Redo Log
- Asynchronous Redo Apply
  - ✓Real-Time Apply is supposed to reduce the latency
  - ✓Applies by reading redo log from received buffers vs. rescanning redo log from disk

IBM DB2 HADR

- Synchronous to remote txn in-memory buffer
- Async apply from in-memory buffer
- If buffer fills….primary also suspends
  - ✓You can tune buffer size (DB2_HADR_BUF_SIZE)

Source: Oracle® Data Guard Concepts and Administration 12c Release 1 (12.1), September 2014





(source: High Availability and Disaster Recovery Options for DB2 for Linux, UNIX, and Windows; IBM Redbooks; October 2012)

Common Issues with HADR Clusters

Applying at standby is slower than primary

- One common reason is that at primary there is a lot of effort in logging to speed txn throughput
  - ✓Hence txn rollbacks tend to be slower than txn commits.
  - ✓Group commits, ULC caches/PLC queues, etc.
- Another reason is that user actions (e.g. query) prefetches page to cache
  - ✓At standby, to reapply the insert, often requires a physical read of data & index pages
- Another reason is that users on standby running reports may contend with replay
- Use of in-memory queues tends to limit surge capacity and cause primary outages (e.g. DB2)
- Oracle has attempted to work around this lately by supporting parallel threads in sender/receiver as well as out of order commit sequencing

Biggest issues

- Due to page-for-page mirror image, can’t run reorgs, update stats, alternative indexing on standby
  - ✓Would cause pages to change or move wrecking page mirror image
  - ✓Result is primary is inflicted with memory and cpu requirement of DBMS maintenance
- No real integration with enterprise data replication for other topologies
  - ✓They have pictures in the book suggesting how to do it, but largely, it becomes a science project to implement
    - – Commonly point to replicating from standby - but what happens in a failover - how do you fail replication over to new standby….if it is available
  - ✓Because of the typical ASE customer has a large SRS topology, this is one of the biggest challenges we needed to address

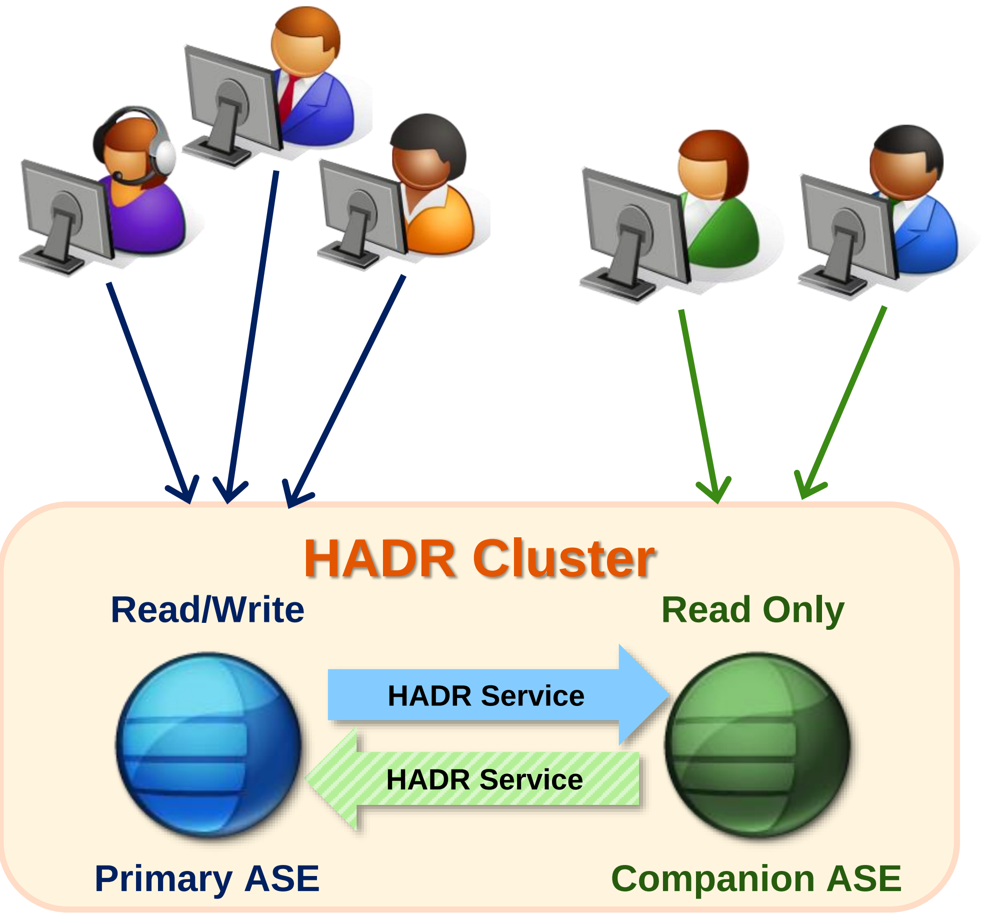
Always-On

HADR Cluster

- Single cluster is limited to 2 nodes
  - ✓Additional standby nodes via external replication
- Log-based Logical Replication Based
  - ✓Synchronous, Near-Synchronous, Asynchronous
  - ✓Zero Data Loss in Synch (RPO=0)
- Fast failover (<2 minutes normally)
  - ✓Planned failovers <1 minute
- GUI (ASE Cockpit – replaces SCC)

Capabilities

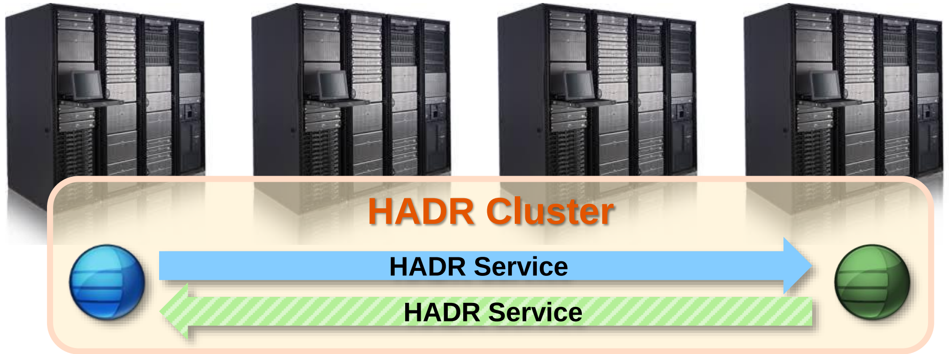
- Automated fault detection
- Automated transparent client failover
  - ✓Planned and unplanned failover support
- Companion can be read-only for reporting
- Zero-down time major upgrades
- Cloud friendly deployment
  - ✓vs. OS & Shared Disk Clusters
- Supports In-Memory XOLTP optimizations in ASE



Two Common Installation Architectures

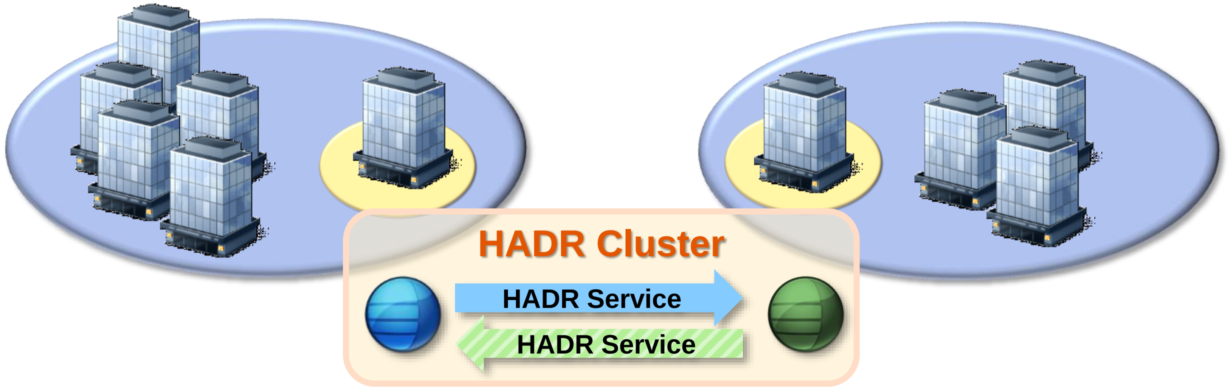
Within same datacenter → HA Focus

- One of the biggest outage reasons within datacenters is individual rack failures or entire row failures due to localized power/switch failure
  - ✓ This often takes out clusters as commonly the nodes of the clusters are within the same rack/row to shorten interconnect distance
  - ✓ …or shared disk SAN is impacted which takes out entire cluster
- HADR allows two different independent systems on opposite ends of datacenter



Between two datacenters → HA + DR

- Must be short distance due to synchronous replication
  - ✓ e.g. similar to disk replication distances
  - ✓ The higher speed the link, the longer the distance
  - ✓ Needs to be at least 1Gbs or higher
- Bandwidth between sites also needs to support user activity if offloading reporting



Always-on HADR cluster architecture & components

Primary & Companion ASE's (ASE 16sp02+)

- HADR mode enabled (e.g. soft quiesce support, etc.)

Primary & Companion SRS

- HADR capable (SRS 15.7.1sp303+)
- Pre-tuned for high volume/low latency

Primary & Companion RMA

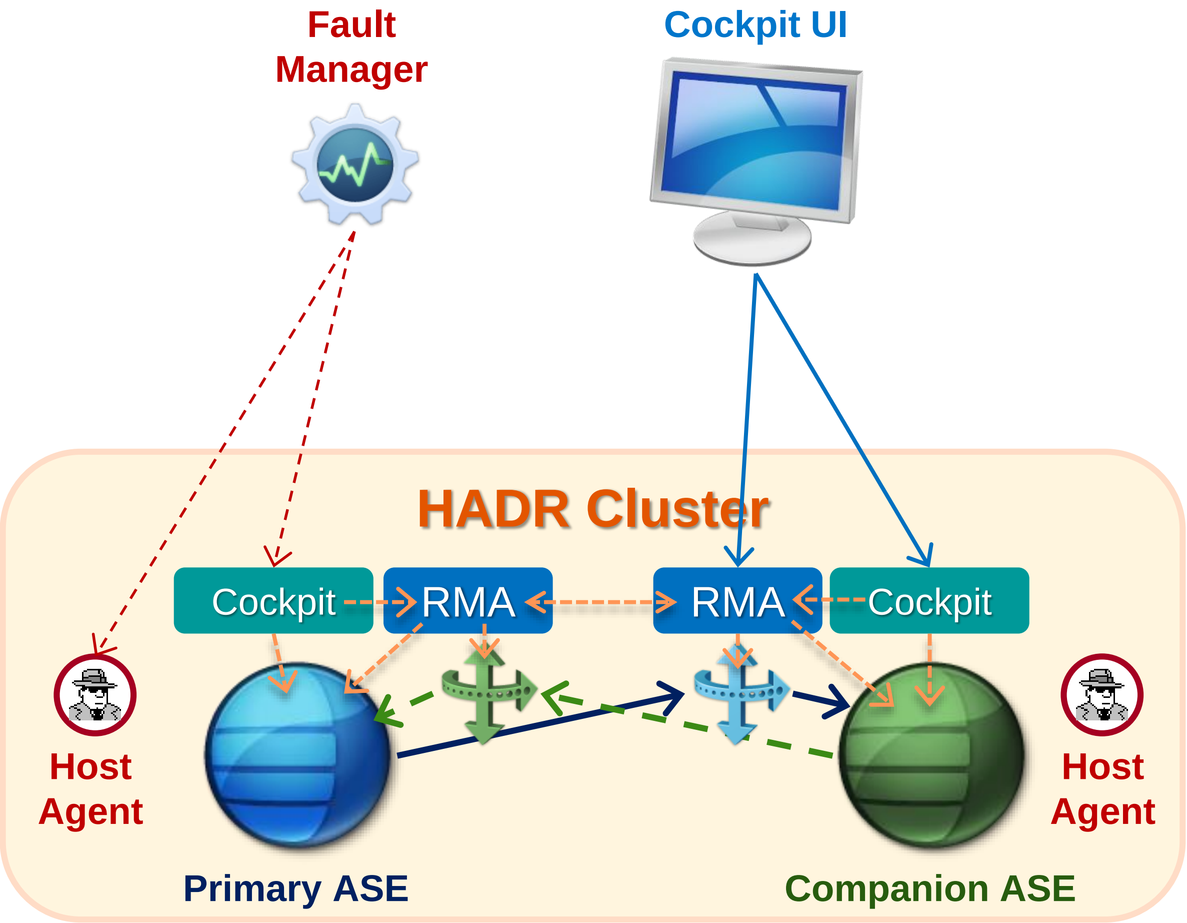
- Provides simplification installation & operations
- E.g. sap_materialize, sap_failover

Primary & Companion Cockpit

- Server side agent has logic
  - ✓ Server-sides supports stop/start/errorlog scan
  - ✓ Issues commands to RMA for HADR operations
- Client UI is web browser

Fault Manager

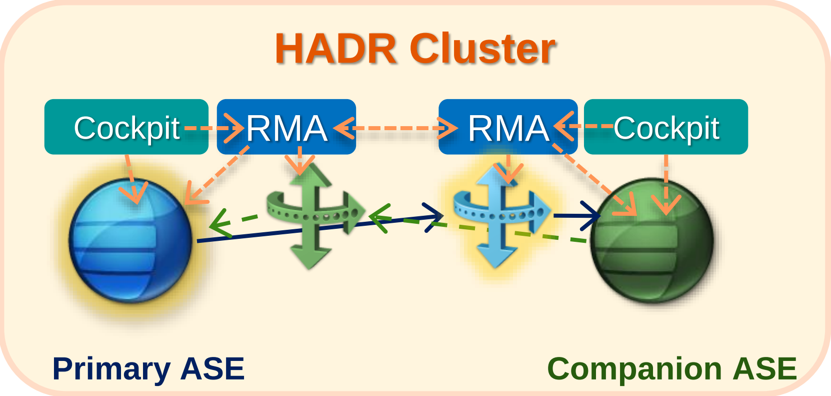
- Installed on 3rd node
- Uses ASE Cockpit and SAP Host Agent to detect and control failover



Old friends….New features

ASE 16sp02 support for HADR

- HADR (virtual) cluster aware w/o HW or quorum devices
  - ✓ Knows which other nodes are in the cluster & state (primary/standby)
- Supports for soft quiesce
  - ✓ Allows zero-downtime planned failovers vs. the typical brief stopping of applications
- Supports client failover & login redirection
  - ✓ None privileged users connecting to the standby are transparently redirected to the primary
- New failover API
  - ✓ Provides state transition messages during planned failovers
- HADR permissions and roles for limiting standby access and HADR admin



SRS 15.7.1sp30x support for HADR

- CI Mode RepAgent with synchronous transfer
  - ✓ New high speed queue for CI mode RepAgent
- Pre-tuned out of the box for high-speed/low latency
  - ✓ All the magic go faster features enabled and memory caches pre-tuned for performance
  - ✓ May need minor tweaking for large txns/batch
  - ✓ Possible future T-shirt sizing pre-tuning to eliminate need to tweak
- Large transaction mode
  - ✓ Allows large txns to start being applied at the standby prior to SRS seeing the commit from primary
  - ✓ Reduces latency caused by waiting for the commit

Recent Developments

ASE 16sp02 pl05+

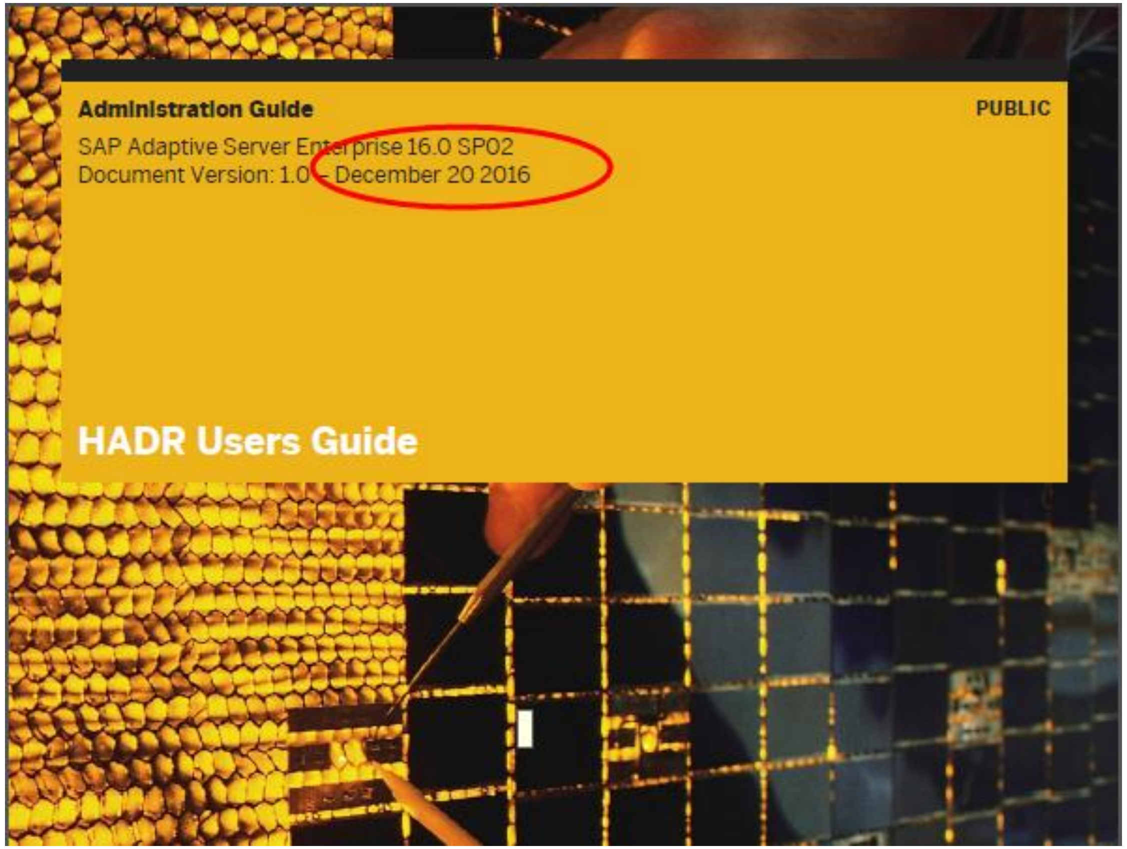
External Replication Support

Key Assumptions

- If replication already exists, no need to tear down implementation to implement Always-On for any single node
- HADR Users Guide PL05 has details on how to setup/configure in Chapter 5
  - ✓Sections 5.2.1 & 5.2.2 setting up new
  - ✓Section 5.2.4 migrating existing systems

Some notes/restrictions

- Will require some downtime to avoid data loss between HADR cluster and external nodes
- May need to change some corp ‘standards’ (such as aliasing maintuser to dbo)



Administration Guide

PUBLIC

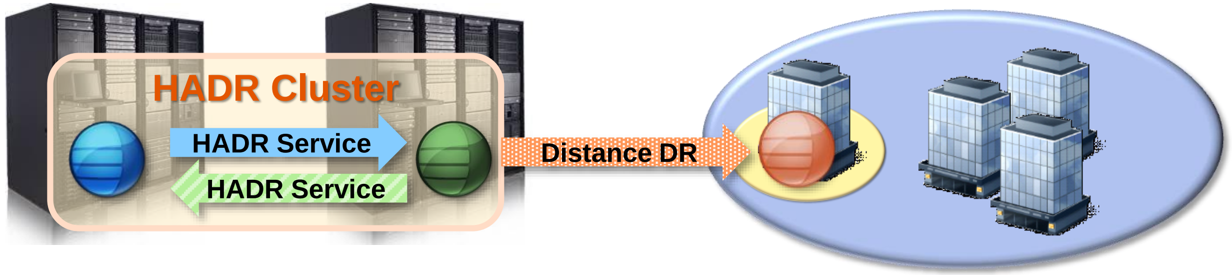
SAP Adaptive Server Enterprise 16.0 SP02
Document Version: 1.0 – December 20 2016

HADR Users Guide

Always-On + External Replication: Multi-Node Support

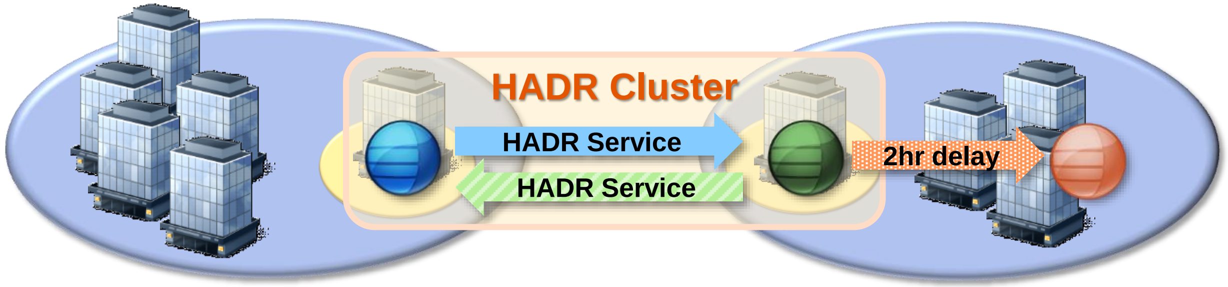
3rd Node: HA+DR

- HADR cluster for HA within the datacenter
- DR coverage is purely disaster recovery
  - ✓ Not intended for long term usage
  - ✓ Apps may have degraded capabilities
    - e.g. no HA, no reporting offload, etc.



3rd Node: Delayed

- HADR primarily for HA or HADR
- 3rd node primarily to protect against errant transactions
  - ✓ Assumption is that errant transaction can be spotted and blocked from 3rd node within the delay time frame
  - ✓ Data values would be extracted from 3rd node and re-injected into primary vs. failover to 3rd node
    - Attempts to skip the errant transaction could result in further issues due to subsequent transactions which would prolong the failover to the 3rd node if intent was to failover to it once it was back in sync time wise



Always-On + External Replication → Dual Cluster implementation

1st Goal – survive multiple failovers

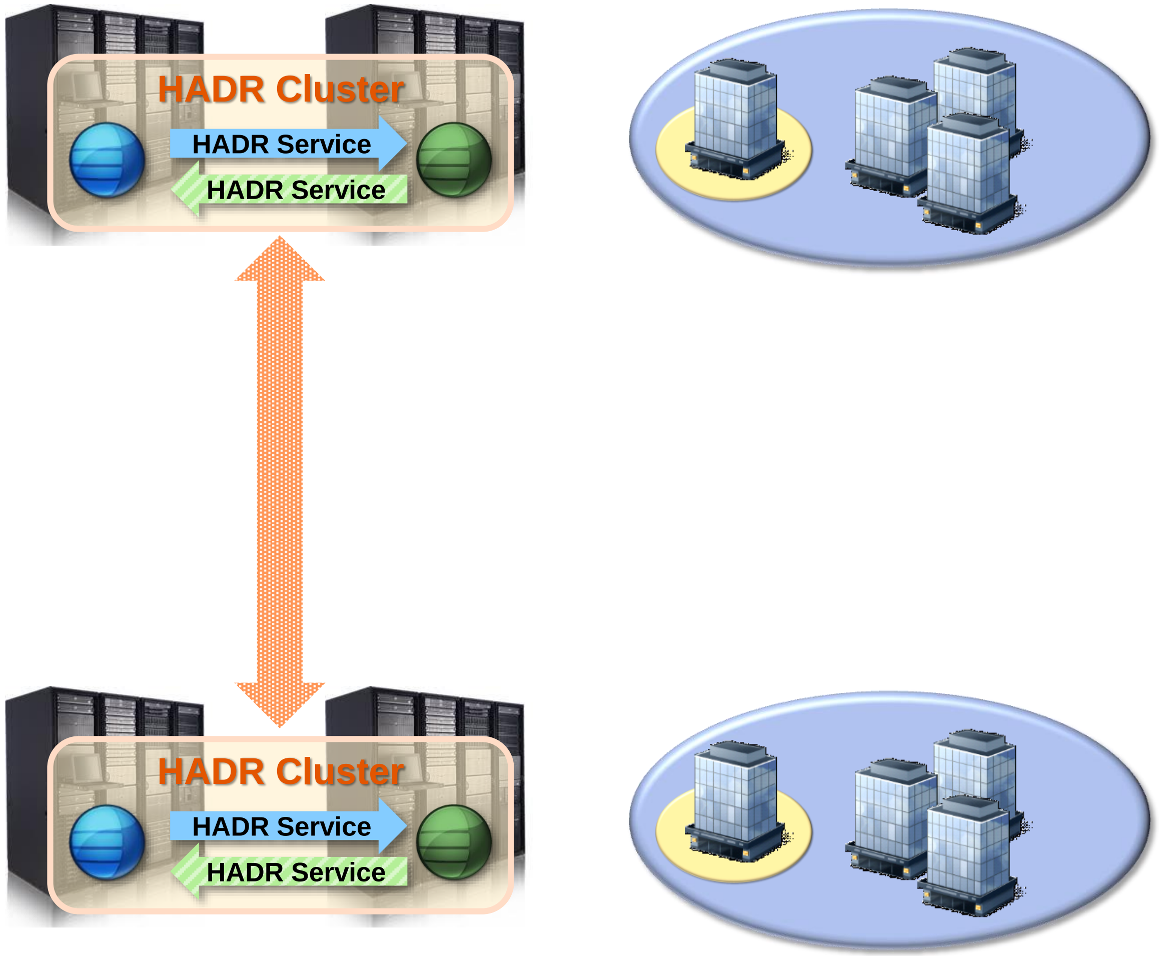
- DC failure
- Subsequent HW or SW failure in DR site
- In other words, full HA capabilities and report offloading is maintained even if DC fails

2nd Goal – R/O scale out

- Users in second business location have reduced latency for reading data/reduces bandwidth requirements to primary site
- Spread out reporting across nodes
  - ✓ Current OLTP reports and historical often have competing resource requirements
  - ✓ DC 1 Standby → OLTP reports (e.g. order status checks)
  - ✓ DC 2 node 1 → EOM/EOY reports
  - ✓ DC 2 node 2 → adhoc/historical reports

3rd Goal – Bi-directional Apps

- Site autonomy/better HW utilization



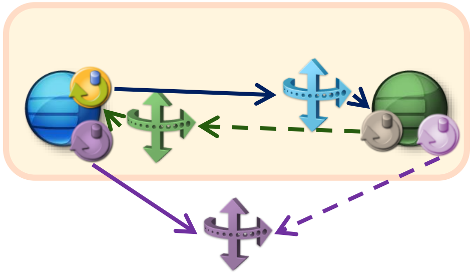
External Replication Support

Split into two problems

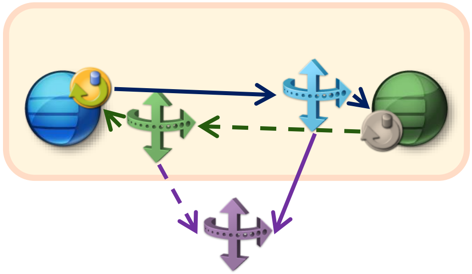
- HADR as a source
- HADR as a target

HADR as Source: 4 Solutions

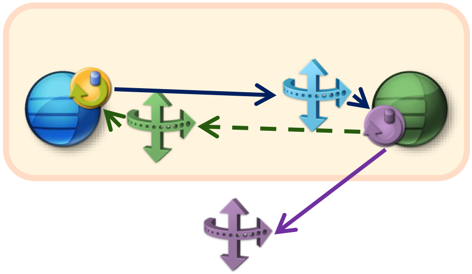
- MPR RepAgent
  - ✓If sync, slows down HADR
  - ✓If async, susceptible to data loss & impacts STP
  - ✓Failover would result in different OQID’s
- Route from HADR
  - ✓Failover coordination issues
    - Wait for route queue to drain before failover or …
    - Wait for route queue to drain before starting failover RepAgent
  - ✓Different OQID issues with Route
- Re-replicate from Standby
  - ✓Competition uses this
  - ✓Issue is on failover - either MPR or manually switch RepAgent to old primary….if available
    - Coordination issue - wait until log read before switch (remember we have different OQIDs from other source)???
- Something else (option 4)



MPR RepAgent



HADR Route



Re-Replicate fm Standby

External Replication Support: HADR as a source

CI RepAgent internal to SRS (SRS 15.7.1 sp305+)

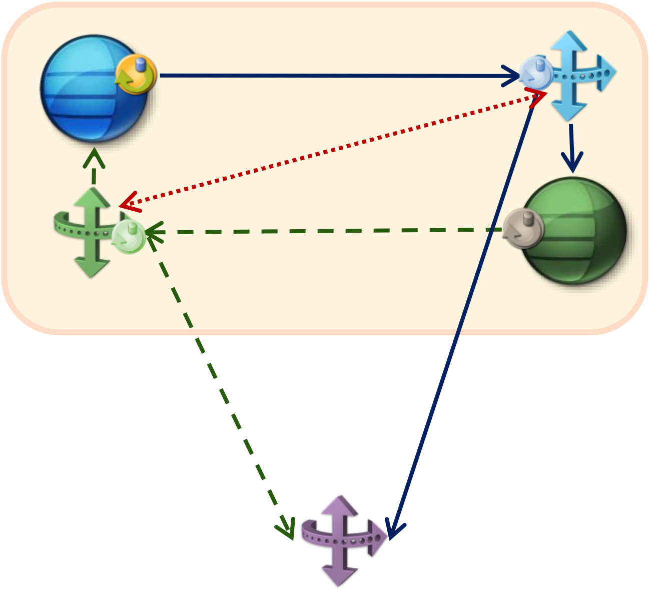
- Would scan log records from SPQ
- Connects to external SRS as a database

Advantages

- Zero Data Loss
- Looks to external as ASE RepAgent
  - ✓Preserves existing topologies with no need to drop/recreate repdefs
- Reading inbound queue too late due to RepDef normalization already missed

Challenges

- On failover, HADR needs to switch RepAgents and tell SRS to rs_zeroltm



External Replication Support: HADR as a target

On Surface, this appears easy

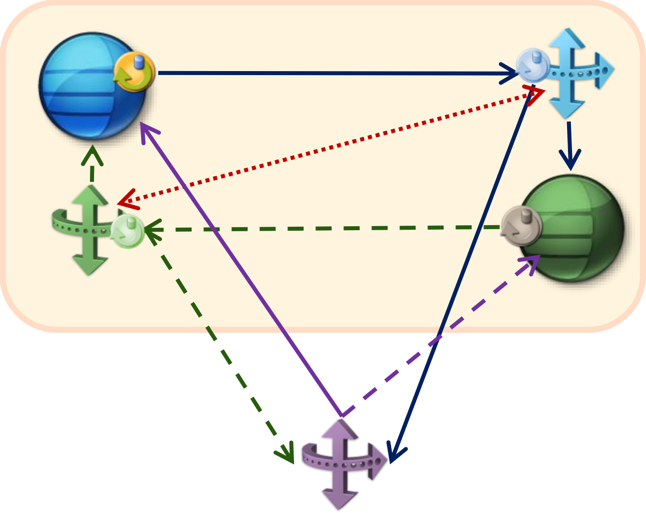
- DSI has been HA aware since SRS 12.0

Challenges

- We want external SRS DSI's to failover but not the HADR DSI's
- We don't want to confuse rs_lastcommit, etc.
- Need to avoid cyclic replication when HADR is both source & target

Solution

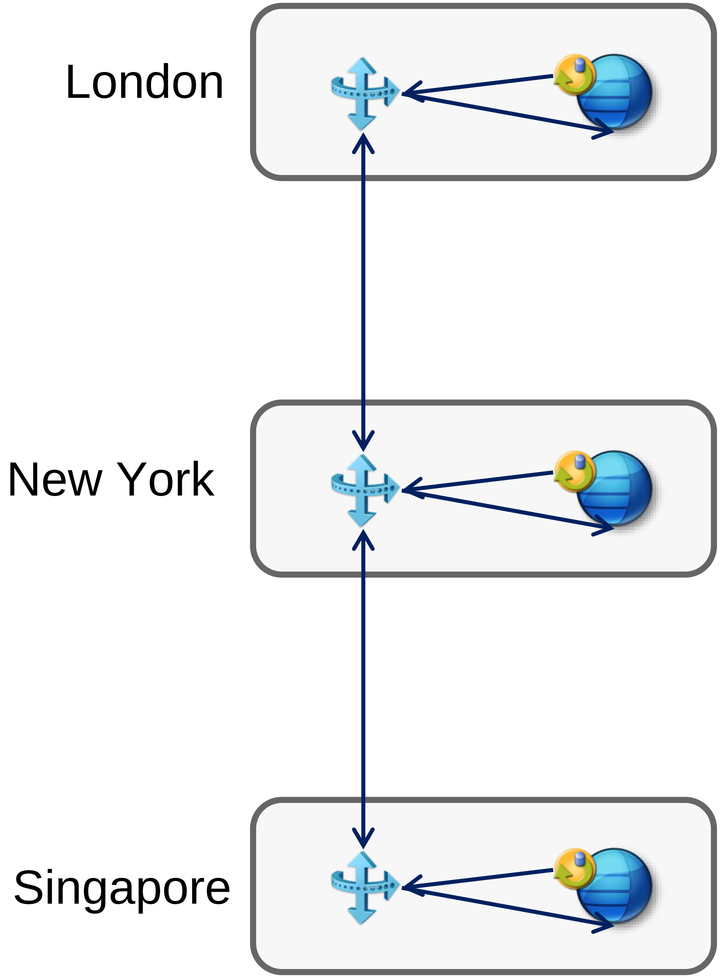
- External SRS connects as different maintenance user vs. DR_maint
  - ✓ Separate set of rs_lastcommit tables…e.g. dbmaint.rs_lastcommit
- External SRS connection doesn't have HADR privileges
  - ✓ So it would failover with other connections
  - ✓ Would need replication_role due to column encryption, materialized columns, etc. replication
- SPQ RepAgent can filter out external maint user txns as it does today
- HADR RepAgents run in WS mode to pick up and fwd warm standby txns to other HADR nodes



A Sample Walkthrough

Key Assumptions

- If replication already exists, between 3 sites
- We want to implement Always-On in NYC first (and then may also in London)
- ASE is already ASE 16sp02 PL05+



High-level Steps To Enable External Replication (1)

Upgrade external SRS to 15.7.1 sp305+

- Assumption is ASE is already sp02 pl05

Suspend DSI into target

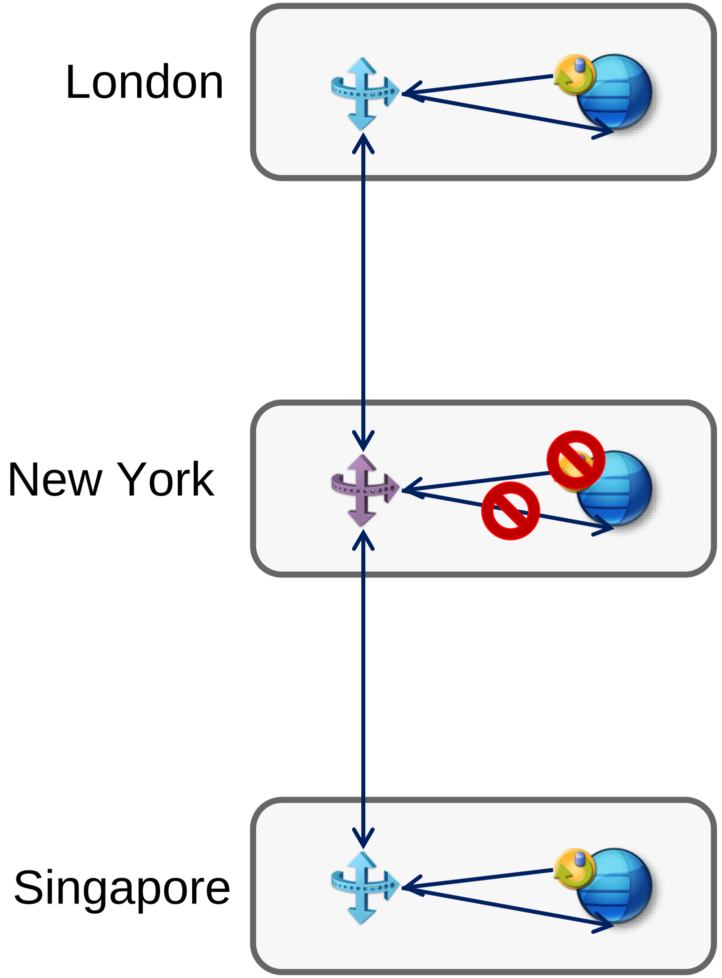
- Ideally you will want to do this during a lull in upstream/downstream activity so that the build up in OBQ is minimized

Teardown the Source RepAgent

- Remove secondary truncation point

Fix the maintuser

- Unalias as dbo
- Revoke sa_role, hadr privileges from maintuser if previously set



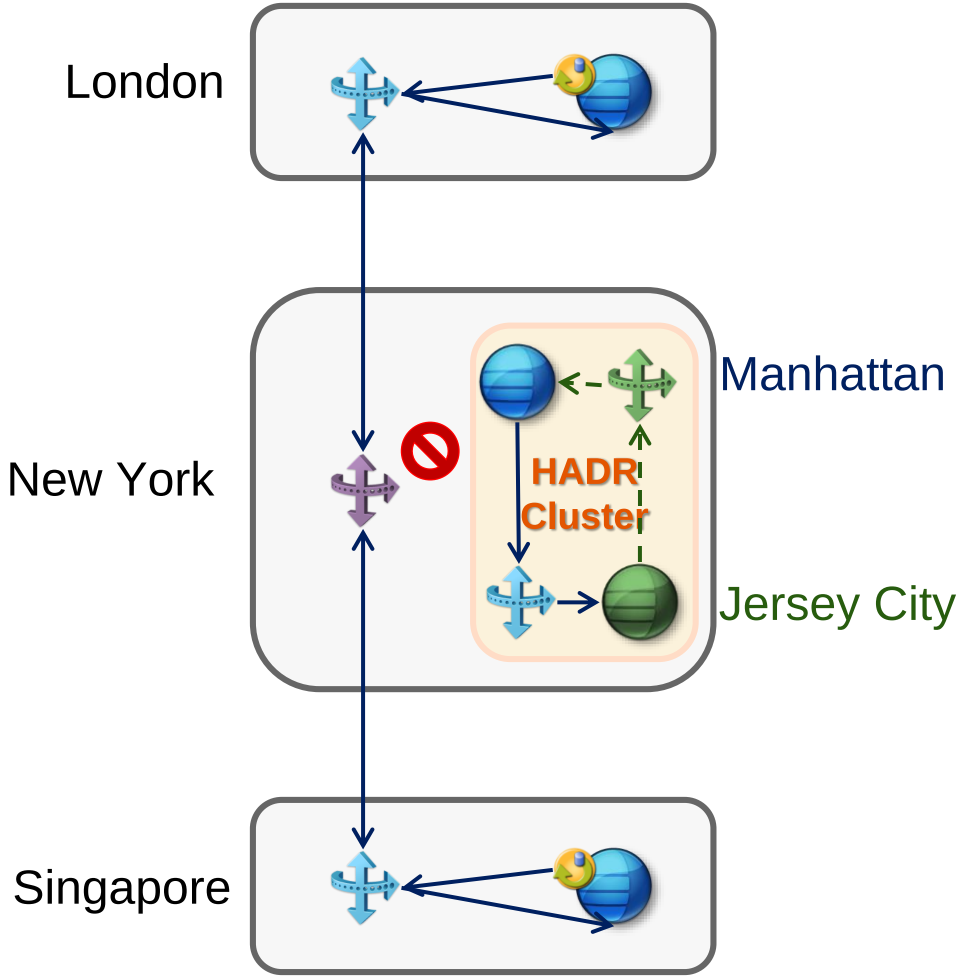
High-level Steps To Enable External Replication (2)

Setup Always-On for current site

- Ideally you will want to do this during a lull in upstream/downstream activity so that the build up in OBQ is minimized

During this time, primary apps should be down

- Otherwise, you will lose data going to external sites as external replication isn't enabled yet



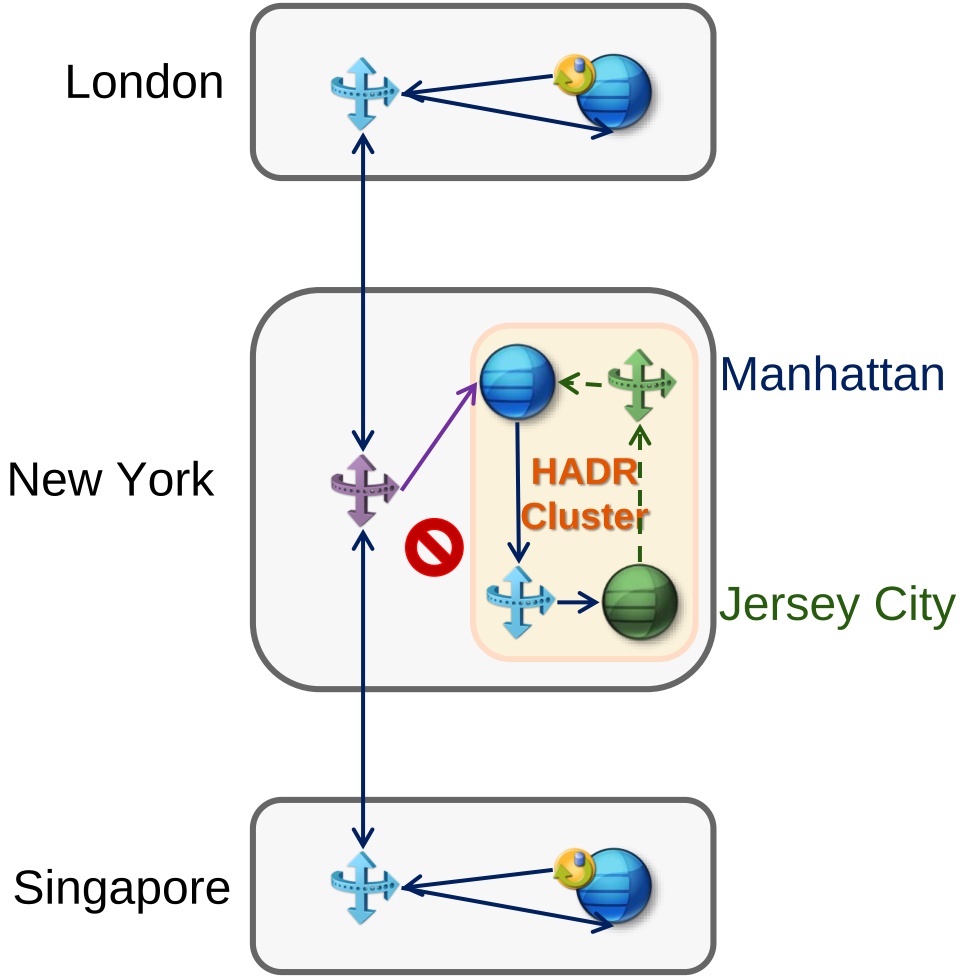
High-level Steps To Enable External Replication (3)

Prepare to re-enable Replication into cluster

- Load rs_install_primary as maintuser
- Grant maint user granular permissions
- If replicating DDL (MSA), grant maint user proxy authorization and set dsi_replication_ddl to true
- Revoke sa_role, hadr privileges from maintuser if previously set

Enable DSI to primary

- Add both primary & standby to external SRS interfaces
- Alter connection to connect to HADR
  - ✓See documentation
- Resume connection



High-level Steps To Enable External Replication (4)

Prepare to re-enable Replication into cluster

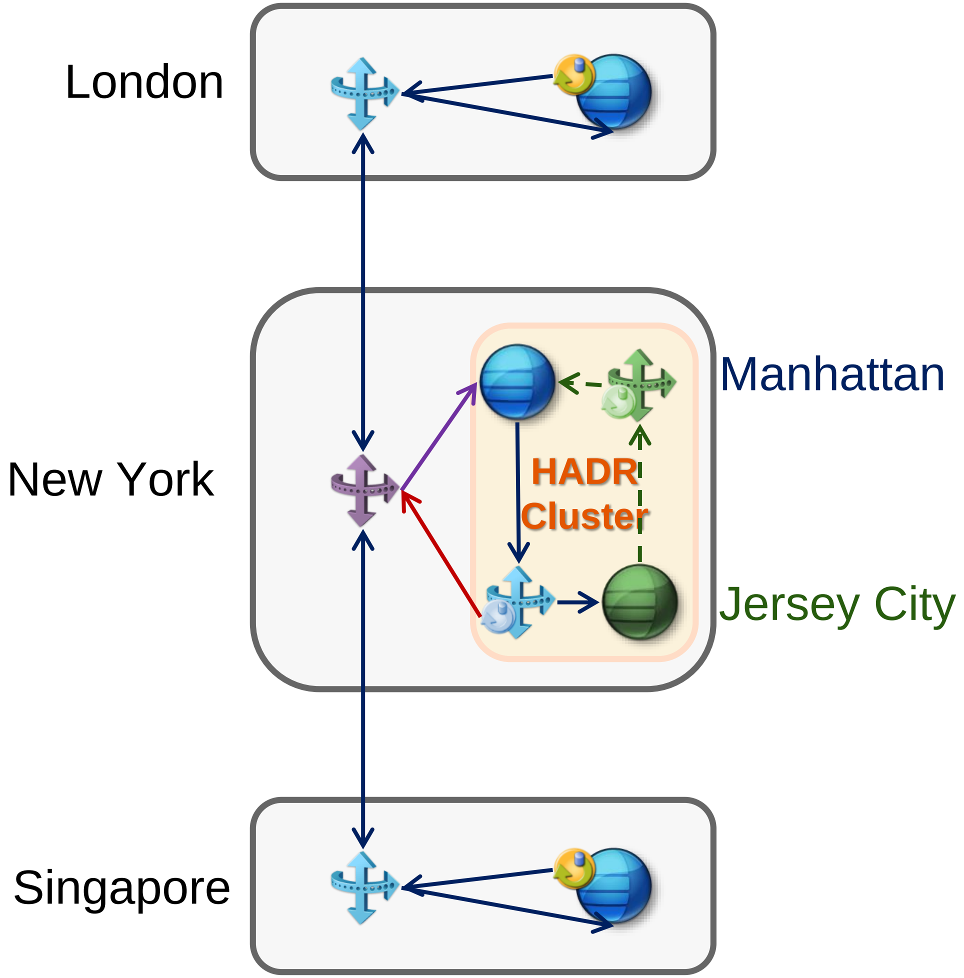
- Load rs_install_primary as maintuser
- Grant maint user granular permissions
- If replicating DDL (MSA), grant maint user proxy authorization and set dsi_replication_ddl to true

Add users to SRS's

- Add db maint user to HADR SRS's and grant manage spq_agent permission
- Add spq_ra_user to external SRS and grant connect source permission

Alter connection to external SRS to add SPQ repagent

Issue sap_enable_external_replication <dbname> in RMA



Roadmap/Future Development

Improvements we are planning or thinking about

SAP Adaptive Server Enterprise (ASE)

Product road map overview – key themes and capabilities

Recent innovations

XOLTP Enhancements

- Lockless Cache
- Latch-Free B-Tree
- NVCache
- SNAP (Compiled Queries)

Data Center Operations & Security

- Always-On
  - HADR Clusters
  - External Replication Support
- Workload Analyzer
- DSAM (storage tiering)
- SAP ASE Cockpit

Cloud Services

- AWS, Azure as BYOL
- Docker support
- HCP & MCD DBaaS

SAP HANA Integration

- A4A

Business Suite/SAP Applications

- CDS functionality Phase 1

ASE 16 SP02 PL05 is current release

2017 - Planned innovations

XOLTP Enhancements

- In-Memory Row Store
- Hash based index
- MVCC

Data Center Operations & Security

- Always-On Enhancements
- CCL for SSL
- Idle timeout
- Granular Auditing
- On Demand Network Encryption

Cloud Services

- Cloud services phase 1

SAP HANA Integration

- SAP HANA Schema
- SAP HANA SQL Script

Business Suite/SAP Applications

- CDS functionality Phase 2
- Technical Monitor Cockpit
- Built-in SAP ASE Long term performance Data Repository (BALDR)
- Read-Only Standby

2018 - Product direction

XOLTP Enhancements

- In-Memory Only Tables
- Temporal SQL/Time Series
- >4TB memory & >32K connections
- Proc cache enhancements
- C UDF, JSON, etc.

Data Center Operations & Security

- 64 bit MDA + MDA repository
- Role based resource limits
- Support CI mode for normal SRS
- Always-On Enhancements
  - XA Support, Standby Database
- HSM, LDAP Groups
- Data Masking

Cloud Services

- Cloud services phase 2

SAP HANA/IQ Integration

- Optimized, zero loss data movement to SAP HANA & IQ
- Common Tooling (phase 1)

Business Suite/SAP Applications

- CDS functionality Phase 3

2019 - Product vision

XOLTP Enhancements

- Lazy Persistence
- Non-locking R/O tables/partitions

Data Center Operations & Security

- Workload Analyzer with MDA
- Workload network replay
- Page migration utility
- Undo/redo log utility
- User certificate authentication

Cloud Services

- Cloud services phase 3

SAP HANA/IQ Integration

- Query Enhancements
- Common Tooling (phase 2)

Business Suite/SAP Applications

- CDS functionality Phase 4

FSI Solutions

- Blockchain, Data lineage, Forensic auditing

This is the current state of planning and may be changed by SAP at any time.

THANK YOU

For more information on SAP ASE 16 visit:

www.sap.com/ase

http://help.sap.com/ase1602/

https://ideas.sap.com/SAPASE

Jeff Tallman
jeff.tallman@sap.com

© 2017 SAP AG or an SAP affiliate company. All rights reserved.