معماری امن ذخیره و بازیابی اثر بخش اطلاعات

رضا صاحب الزمانی

شرکت کاشف

معرفی

- 22 سال سابقه توسعه نرم افزار
- 10 سال سابقه مشاوره امنیت (نرم افزار و استراتژی امنیت)
- 8 سال امنیت سیستمهای ذخیره سازی و آرشیو
- 8 سال مشاوره بهینه سازی معماری ذخیره سازی اطلاعات
- دکتری مدیریت اجرایی


به رییس گفتم سیستم بالا نمیاد . بنظرم! عصبانی شد.
خودت بگو بک آپ چند روز دیگه بر می گرده ؟

بر اساس تحقیقات بعمل آمده حفاظت از اطلاعات سازمان جدی ترین دغدغه مدیران انفورماتیک می باشد.

در این حوزه عملیات بک آپ بسیار پر کار بوده و هزینه و زمان زیادی را صرف میکند .

با رشد اطلاعات ، حجم بک آپ ها در حدی زیاد شده که در سازمانهای بزرگ ، زمان برگرداندن بک آپ از زمان قابل تحمل توسط سازمان بیشتر است !

دردسر ها

هر 6 ماه یک مناقصه SAN داریم.

یا حداقل داریم هارد دیسک میخریم.

اتفاقات غیر مترقبه : 1 پتا بایت مدیریت اسناد، روزی چند صد هزار چک،...

عملیات پیچیده و مدیریت نشده

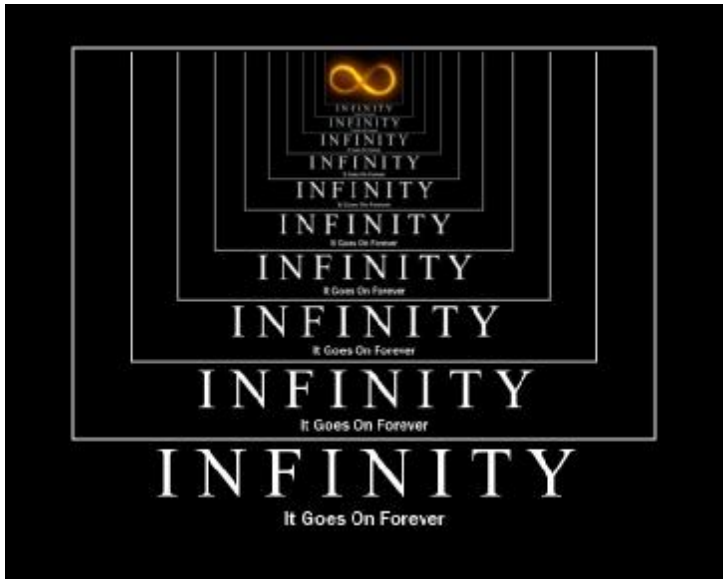
- 300 تا سیستم را بک آپ میگیریم.
- لیست واضح و شفاف نیست !
- تعهد پیمانکار : هرچی رو ریختی روی این سرور من روی Tape میبرم.
- شرح مناقصه : یک دیتا بیس داریم 10 ترابایت ، یکی دیگه داریم 50 ترابایت، 200 تا هم ماشین مجازی داریم یک پرتال هم داریم خیلیه ، اینا ما رو خسته کردن بابا!
- شعب هم خودشون روی تکنولوژی 15 سال پیش بک آپ میگیرند ، هیچکس هم چک نمیکنه!

دلخوشی ها

- یک کپی همزمان جای دیگر دارم ! (چه فرقی میکنه ؟!) اصلا بک آپی نمی خوام .
- بالای 95% دستکاریها توسط افراد مجاز انجام شده است.
- آیا قابلیت پیگیری وجود دارد؟
- You can not detect what you can not see !

الزامات قانونی

- امنیت
- اطمینان از عدم تغییر



- دوره عمر نگهداری =

معمار اطلاعات کجاست؟

- همه چیز در همه
- اطلاعات قدیمی باعث درد سر هستند.
- همه جور اطلاعات یکجا جمع می شود.
- سیستمها مالکین متفاوتی دارند.
- پیمانکاران مختلفی داریم.

هزینه های زیادی صرف راه حلهای کوتاه مدت می شود

- بودجه
- انرژی
- نفر ساعت
- اعصاب
- آبرو

تفاوت طرز فکر بخشهای نرم افزار و زیر ساخت

- نرم افزار بالا باشد و کار کند ، کند نشه!
- کجا نگهش دارم!
- از دید یک نفر 50 گیگا بایت ، از دید دیگری 3 تا 40 ترابایت !
- دوره عمر اطلاعات باید مشخص باشد.

- توصیه : برای نرم افزار های جدید ، آمادگی بخش زیر ساخت و بودجه معماری مناسب ذخیره سازی نیز ، دیده شود.

چقدر وقت داریم به وضعیت عملیاتی برگردیم؟

- RTO
- زیر 4 ساعت !
- با حجم داده بانک غیر ممکن است.
- Dedup کمکی نمی کند
- اگر بالای 30 ترابایت اطلاعات دارید ، بانک ممکن است تعطیل شود !
- یکروز محاسبه سود را عقب بیافتم ، اوضاع پیچیده می شود.

راه حل

- چه چیزی را نگه داری میکنیم ؟
- ضریب اولویت و شناسایی CDA (اطلاعات چقدر مهم است X چند ساعت می توانم نداشتن آنرا تحمل کنم)
- طول عمر اطلاعات
- نگاه مدیریت ریسک
- بودجه

قیمت اطلاعات

ضرایب اهمیت از دست رفتن اطلاعات	
در این روش اولویت ها به شکل زیر تعریف میشوند:	
ظریب اهمیت از دست رفتن اطلاعات	شرح
0	اطلاعاتی که از دست رفتن آنها موجب تعطیلی بانک می شود
5	اطلاعاتی که از دست رفتن آنها موجب ضرر و زیان مالی بالای یکصد میلیار ریال به بانک میشود
4	اطلاعاتی که از دست رفتن آنها موجب خدشه دار شدن اعتبار بانک میشود
3	اطلاعاتی که از دست رفتن آنها باعث نارضایتی قابل جبران مشتریان میشود
2	اطلاعاتی که تاثیر عملیاتی مستقیم ندارند اما برای کاربرد های حقوقی یا تجاری نگهداری از آنها ضروری است
1	سایر اطلاعات
توضیح : اگر در محاسبات اولویت عددی برابر صفر شد ، آن مورد الزامی بوده و محاسبات Cost/Benefitبرای آن انجام نمی شود	
برای سایر موارد ضریب ، در محسابه ارزش ریسک در نظر گرفته میشود	
ممکن است از دیدگاه مدیریت ریسک ، فاصله ضرایب بیش از 1 باشد .	

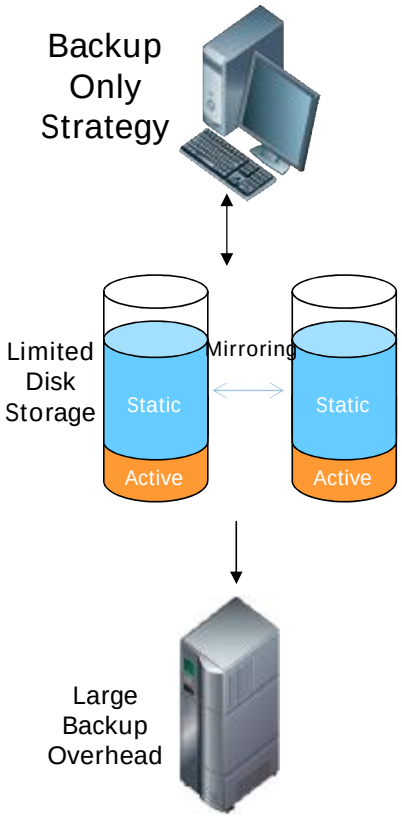
قیمت توقف

ضریب اهمیت بازیابی بر اساس زمان توقف قابل تحمل در ارایه سرویس تعیین میشود	
ضریب	شرح
0	حتی یک لحظه نباید سرویس ها متوقف شوند
A	حداکثر زمان قابل تحمل خرابی 1 ساعت می باشد
B	حداکثر زمان قابل تحمل خرابی 4 ساعت می باشد
C	حداکثر زمان قابل تحمل خرابی 24 ساعت می باشد
D	سرویس کلیدی نیست

داده ها در طول عمر خود نیازهای متفاوتی دارند.

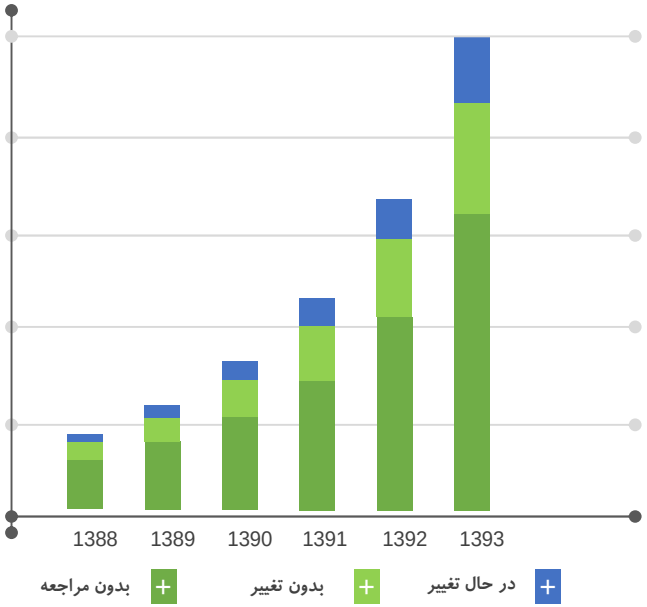
- اطلاعات دارای یک دوره عمر هستند.
- فاکتور عمر اطلاعات باید در انتخاب معماری لحاظ شود.
- اطلاعات در ابعاد چند هفته دارای تغییر و مراجعه هستند ، اما معمولا تا ابد باید نگهداری (آرشیو) شوند.

اتفاقی که در مرکز داده می افتد :



- حتی اگر 20 مرکز داده داشته باشیم و صدها کپی از اطلاعات نگه داریم ، صرفا نسبت بـه خرابـی هـای فیزیکـی ایمن خواهیم بود و در مقابل تهدیدهای سایبری مانند هک و ویروس ، هیچ امنیتی نداریم.
- حجم بک آپ ها به حدی زیاد است که زمان بازگرداندن آنها ، از زمان تحمل خرابی ، بیشتر است.
- سرورهای جاری سازمان ، به سرعت پر میشوند و هزینه زیادی صرف خرید تجهیزات ذخیره سازی میکنیم.
- عملیات بک آپ ، پر هزینه و پر درد سر بوده و نهایتا کامل قابل اطمینان نیست .
- سوابق تغییرات اطلاعات ، قابل پیگیری نیستند.
- خود Tapeها را باید دایما Recycleکنیم .
- Tapeنسبت به میدان مغناطیسی، حرارت، رطوبت و ضربه حساس است.
- نسبت به بمبهای الکترو مغناطیسی ، آسیب پذیریم.

اطلاعات دارای تغییر و بدون تغییر



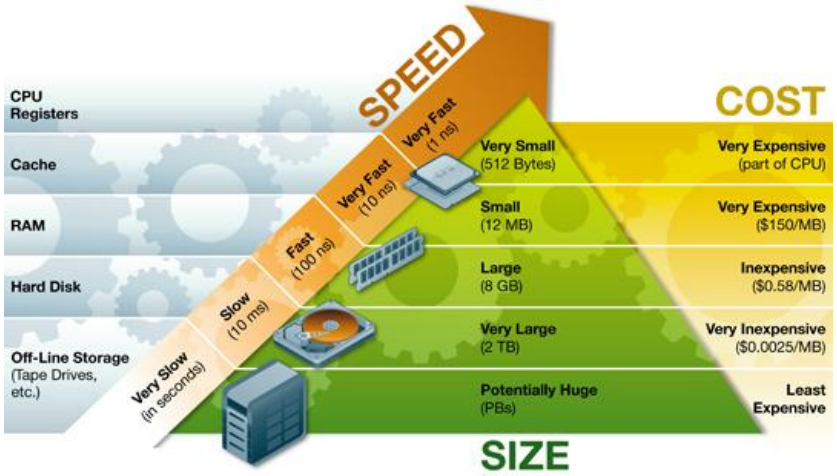
- بر اساس بررسی های بعمل آمده توسط موسسات Gartnerو IDC ، 80% از اطلاعات سازمان بدون تغییر بوده و به ندرت مورد مراجعه قرار میگیرند.
- بر اساس تحقیقات ،60 % از اطلاعات ، هیچگاه مورد مراجعه قرار نمی گیرند.
- در بانکها و سازمانهای دولتی 96,5 % اطلاعات ،ظرف یکسال گذشته مورد مراجعه قرار گرفته است .
- یعنی اگر نسخه قابل اطمینانی از 80% از اطلاعات داشته باشیم، لازم نخواهد بود دیگر از آن بک آپ هم بگیریم.

برای هر پیچ آچار مخصوصی وجود دارد

سوال؟	بک آپ	آرشیو
چه هست ؟	اقدام حفاظتی برای مراقبت از اطلاعات امروز	سوابق اطلاعاتی سازمان
چرا از آن استفاده کنیم؟	بازیابی : بعد از بروز خرابی یا از دست رفتن اطلاعات بتوانیم آنها را برگردانیم	اطلاعات در دسترس باشند ،بتوانیم هر اطلاعاتی خواستیم را سریعا داشته باشیم
چه کسی آنرا می خواهد؟	مدیر مرکز داده، مدیر انفورماتیک،مدیر عامل	همه افراد سازمان ، مراجع قانونی ، شرکتها هم خانواده
چه چیزی نیست؟	کپی همه چیز!	محیطی که بانک اطلاعاتی را از روی آن اجرا کنید
چندتا از آن داریم؟	خیلی ، تقریبا روزی یک عدد به ازای هر سیستم	فقط یکی ، آرشیو زیر ساخت امنی است که اطلاعات به آن اضافه میشوند.

Hierarchical Storage Management سیستم

- یک سیستم نرم‌افزاری و یا مجموعه از نرم‌افزار و سخت افزارهایی است که تعیین سیاستهای ذخیره سازی اطلاعات بر روی آن به سازمان اجازه می‌دهد سرورهای ذخیره سازی اطلاعات خود را به اقتصادی ترین شکل ممکن استفاده نماید. این سیستمها به شکل خودکار با در نظر گرفتن سیاستهای تعین شده توسط راهبر سیستم مجموعه از ابزارهای ذخیره سازی را به نحوی بکار می‌گیرند که سریعترین و گرانترین سیستم ذخیره سازی برای پرکاربرترین و پر مراجعه ترین سناریوهای دسترسی به فایل و ارزانترین آنها به کاربردهای با فواصل زمانی طولانی تر اختصاص یابد.



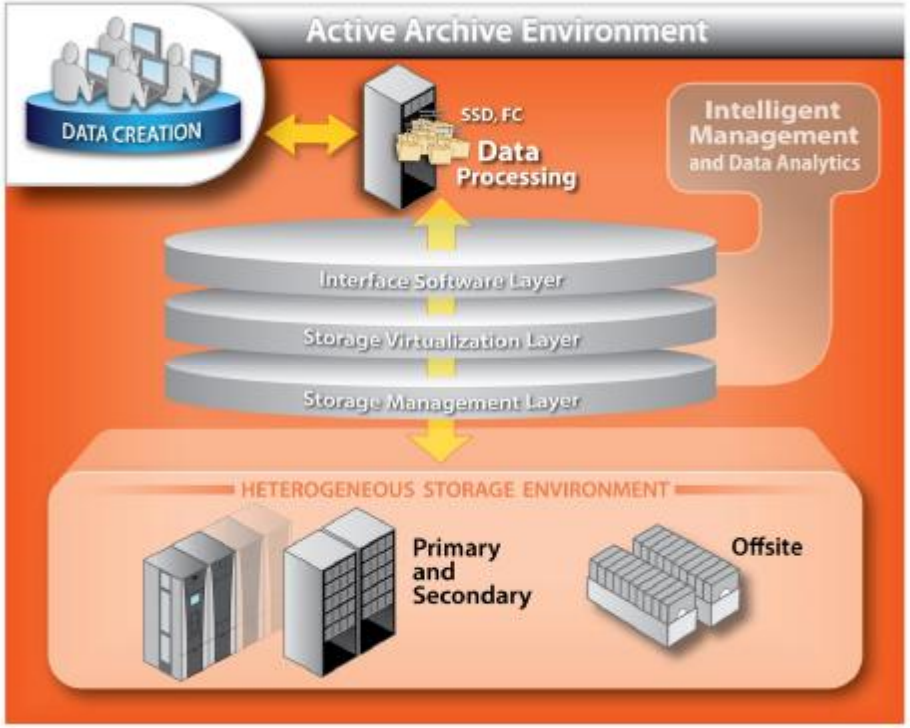
بیشترین هزینه و بالاترین سرعت :

RAM SAN & SSD

کمترین هزینه و سرعت قابل قبول :

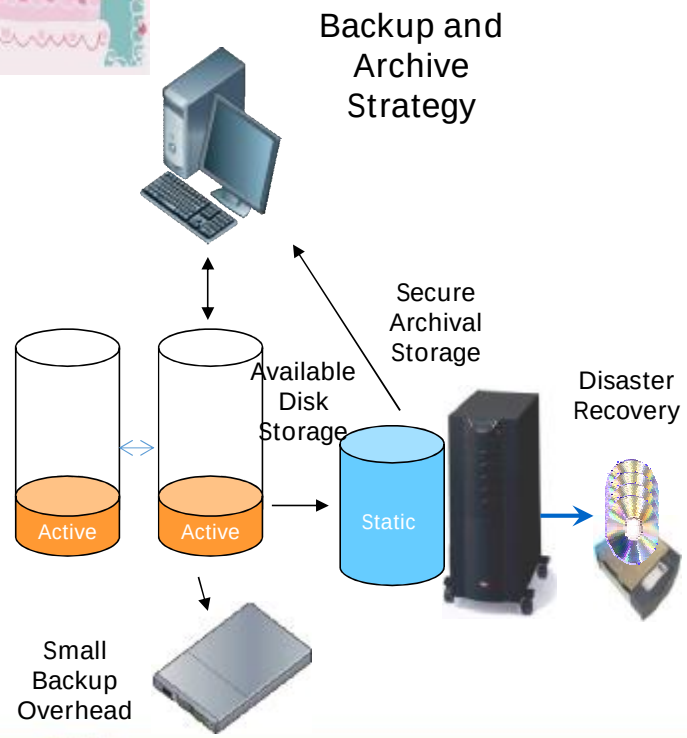
Blu-Ray 3

معماری Active Archive



- http://www.activearchive.com/
- هدف انتقال هوشمند و ترانسپارنت اطلاعات به لایه های مختلف بر اساس سرعت ، امنیت و دوره عمر
- مزایا کاهش هزینه ، افزایش امنیت و سهولت

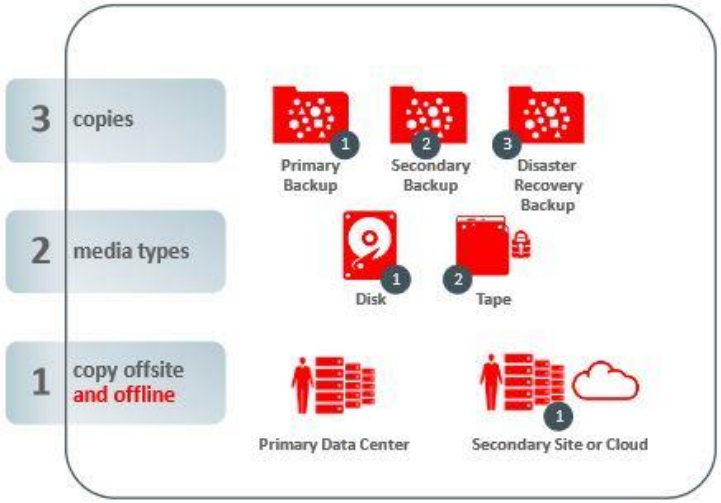
نتیجه بکار گیری معماری Active-Archive



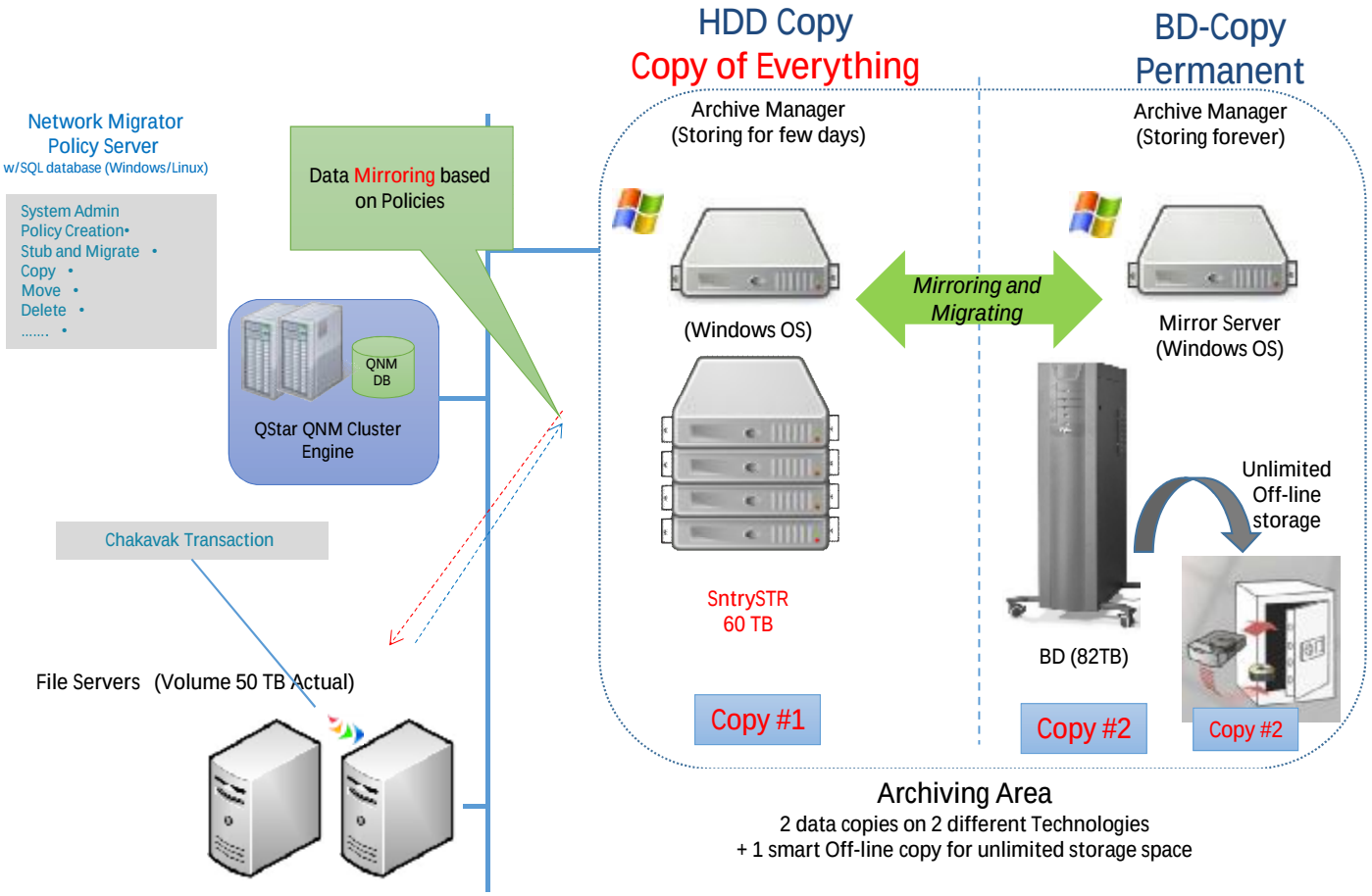
- از 80% اطلاعات دیگر نیاز نیست بک آپ بگیریم.
- فضای سرورهای گران لایه 1 ، به شدت آزاد میشود.
- زمان برگشت از از وضعیت خرابی ،20% زمان فعلی خواهد بود .
- سوابق تغییرات اطلاعات موجود است.
- هزینه ذخیره سازی اطلاعات تقریبا یک هشتم ، میشود.
- همه اطلاعات همیشه ، در دسترس هستند.
- کلیه عملیات ، بصورت خودکار انجام میشود.

بهینه و ایمن ترین روش نگهداری طولانی مدت اطلاعات چیست؟

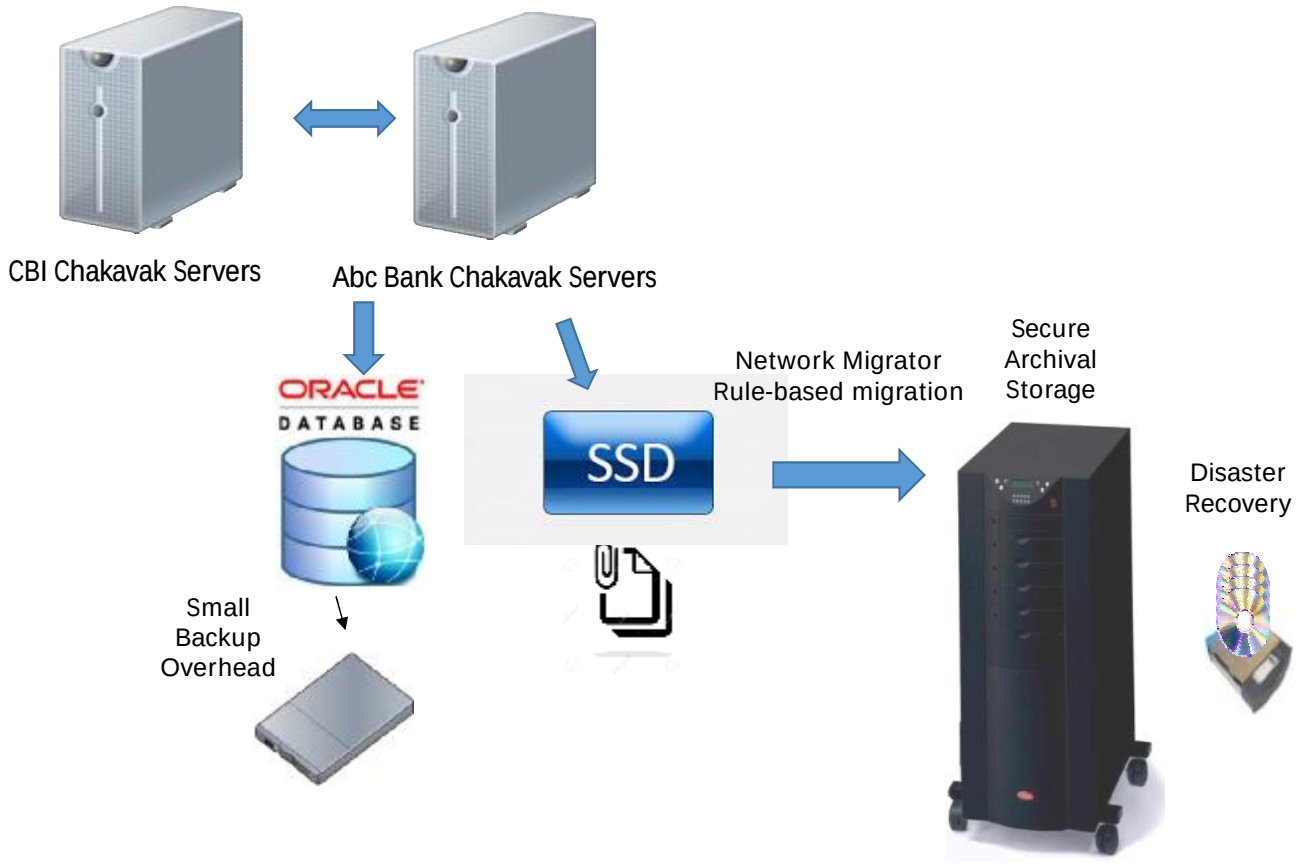
- موسسه تحقیقاتی گارتنر چند هزار سازمان بزرگ در دنیا را بررسی نموده و در نتیجه تحقیقات خود بهترین روش ذخیره سازی اطلاعات یا روش 3-2-1 را معرفی نمود . 3-2-1 یعنی :
- 3 : حداقل سه کپی از اطلاعات مهم داشته باشیم
- 2 : فن آوری ذخیره سازی 2 تا از کپی ها باید متفاوت باشد، بطور مثال اگر یکی از آنها مبتنی بر RAID (هارد دیسک) است دیگری باید Optical(دیسکهای نوری) باشد.
- 1 : حداقل مدیای 1 لایه باید قابل انتقال به سایت دیگر باشد.



Active Archive ایجاد سیستم



شماتیک نحوه اجرا



توصیه های سازمانهای موفق:

- ایجاد یک روش همگام برای استفاده از کپی پشتیبان (Backup) برای بازیابی عملیاتی و آرشیو برای حفظ و کشف
- کمینه کردن تعداد کپی‌های ایجاد شده به عنوان نسخه‌های پشتیبان برای کاهش هزینه‌های ذخیره و ساده‌سازی فرآیندهای مربوط به مدیریت
- همگام‌سازی سیاست‌ها حفاظتی برای نسخه‌های پشتیبان با سیاست‌های مربوطه آرشیو کردن اطلاعات (Archiving)
- کمیته یا مسوول معماری اطلاعات را مشخص نمایید.
- شرکت کاشف هم در خدمت شماست.

امام علی علیه السلام :

ثَمَرَةُ التَّفريطِ النَّدامَةُ، و ثَمَرَةُ الحَزمِ السَّلامَةُ؛
نتیجه کوتاهی در کار، پشیمانی است و نتیجه دور اندیشی، سالم ماندن.
نهج البلاغه، حکمت 181

r_Sahebzamani(at)kashef.ir
www.kashef.ir

نظام کنترل امنیت شبکه و فوریت های بانکی