

Заличаванията в документа са на основание на чл. 2, ал. 1 от Закона за защита на личните данни.

Техническо предложение

по процедура за БНБ - „Доставка и гаранционна поддръжка на компютърно оборудване, компютърни компоненти за него, софтуерни продукти и услуги по инсталиране и конфигуриране.“

Резюме

Предложението включва стратегия и планове за разширяване и внедряване на оборудването, софтуера и услугите обект на настоящата процедура

Телелинк ЕАД



Съдържание

1. Въведение	0
1.1.1. High-Level Design на HA	2
1.1.2. Реализация	4
1.2. Текущо състояние	8
2. Стратегически инициативи	11
2.1. Виртуализация	11
2.1.1. PowerVM	11
2.1.2. x86 виртуализация	30
2.2. Active-Active Datacenter	41
2.2.1. Развитие на HA Архитектурите за реализация на Active-Active DC	41
2.2.2. High-Level Design на HA	43
2.2.3. Реализация	45
2.3. Преминане към виртуални работни места - VDI	49
2.3.1. Концепция за внедряване	50
2.3.2. Стъпки на имплементация	53
2.4. Формиране на частен облак	55
2.4.1. IBM Cloud Computing Reference Architecture	55
2.4.2. Предложение за концепция за изграждане Cloud Enabled Data Center ..	57
2.4.3. Роли в Cloud Enabled DC	58
2.4.4. Use cases и micropatterns	58
2.4.5. Макро-шаблони	61
2.4.6. Реализация	62
2.5. Изграждане на отдалечен резервен сайт	63
3. Стратегии за развитие на мрежите и сигурността	64
3.1. Стратегия за развитие на комуникационната и мрежовата инфраструктура	64
3.1.1. Комуникационните системи и технологиите за виртуализация	64
3.1.2. Едновременна работа на информационните системи в два изчислителни центъра	68
3.1.3. Комуникационна инфраструктура за Центъра за възстановяване след инциденти	72

3.1.4. Механизми за автоматизация за провизиране на информационните системи	75
3.1.5. Стъпки на имплементация	77
3.2. Стратегия за развитие на информационната сигурността	81
3.2.1. Информационна сигурност (дефиниция/инструменти/мерки)	81
3.2.2. Концепция за развитие	84
3.2.3. Стъпки на имплементация	90
4. Описание на представяното оборудване	95
4.1. RISC сървъри	95
4.1.1. Power 710 (8231-E1D)	95
4.1.2. Power 740 (8205-E6D)	97
4.1.3. Power 770 (9117-MMD)	99
4.1.4. Power E870 (9117-MME)	102
4.1.5. Power S822 (8284-22A)	104
4.1.6. Power S824 (8286-42A)	106
4.1.7. Flex System p260 (7895-23X)	107
4.1.8. План за обновяване на текущата сървърна база	108
4.1.9. Възможности за интеграция на новите сървъри	114
4.1.10. Възможности за интеграция на новите сървъри във виртуалната инфраструктура на банката	115
4.1.11. Механизми за интегриране и пълноценна експлоатация на вече закупен софтуер	115
4.1.12. Възможност за развитие при добавяне на модули, компоненти, лицензи и системен софтуер от списъка по настоящата процедура към съществуващите сървъри.	115
1.1 x86 сървъри	116
1.1.1. Модули и елементи	116
1.1.2. Приоритетни инициативи	120
1.1.3. Оборудване	121
1.1.4. Концепция и стъпки на имплементация	127
4.2. Дискови масиви	132
4.2.1. Концепция за развитие	132

4.2.2.	Стъпки на имплементация.....	136
4.2.3.	Обобщение на използваната техника от списъка на предлаганото оборудване	140
4.2.4.	Оборудване.....	141
4.3.	Backup & Archiving	149
4.3.1.	Лентови библиотеки	151
4.3.2.	Tivoli Storage manager.....	153
4.4.	Системен софтуер.....	157
4.4.1.	Системи за наблюдение и управление на изчислителни ресурси.....	157
4.4.2.	Системи за наблюдение и управление на репликацията на данните ...	158
5.	Планове за внедряване и обслужване	159
5.1.	Процедури по управление на проекти	159
5.2.	Обучение	160
5.2.1.	Обхват.....	160
5.2.2.	Планиране	161
5.3.	Процедури по извършване на гаранционно обслужване	161
5.3.1.	Организация и структура на поддръжка	162
5.3.2.	Административна ескалация.....	174
5.3.3.	ON-LINE система (OTRS) за приемане и обработване на сервизни заявки	175
5.4.	Планиране на стратегическите инициативи	0

СТРАТЕГИЯ

за внедряване и използване на продуктите и услугите по обособена позиция 1 от процедурата - „Доставка и гаранционна поддръжка на компютърно оборудване, компютърни компоненти за него, софтуерни продукти и услуги по инсталиране и конфигуриране.“

1. Въведение

Българска Народна Банка играе изключително важна роля за нормалното функциониране на държавата и бизнеса. Основните процеси изпълнявани от БНБ са реализирани като компютърно базирани системи и обменят информация с останалите банки, бизнеса, партньорски организации и други. Други съществени фактори определящи важността на ИТ инфраструктурата са законовата рамка и спазването на добрите практики в изграждането и експлоатирането на информационни системи, задължителни за Централните Банки.

Тези предпоставки са в основата на изграждането и развитието на информационните системи.

През последните години се извършват големи изменения в начина, по който използваме компютрите. След прехода от монолитни специализирани изчислителни комплекси към високо продуктивни персонални компютри се наблюдава отново тенденция в консолидиране на изчислителните ресурси, но сега на ново ниво – консолидиране на критичните процеси върху виртуализирани платформи. Този преход е резултат от повишените изисквания от бизнеса към информационните системи, данните и достъпността им. Друг фактор влияещ върху процеса е възможността да се осигури висока надеждност на данните, резервирането им както по отношение на наличност на изчислителни ресурси или такива за съхранение на данни, а така също и възможност за по-стриктен контрол на достъпа до тях, разпределени

БНБ е в крак с тази тенденция – основните системи са консолидирани, а критичните за бизнеса системи са дублирани или работят в клъстерен режим. Осигурена е защита и архивиране на данните и системите на ленти.

В настоящия документ сме се опитали да предложим преглед на решенията възможностите за развитие и стъпки на различните сегменти на инфраструктурата, както и примерна зависимост на стъпките. Планирането е условно и се базира на презумпции възприети от нас. Разбира се, може да се предприемат и други подходи и различно разпределение и раздробяване на стъпките, както и корелация според бюджет и по-точни цели.

We transfer intelligence into network

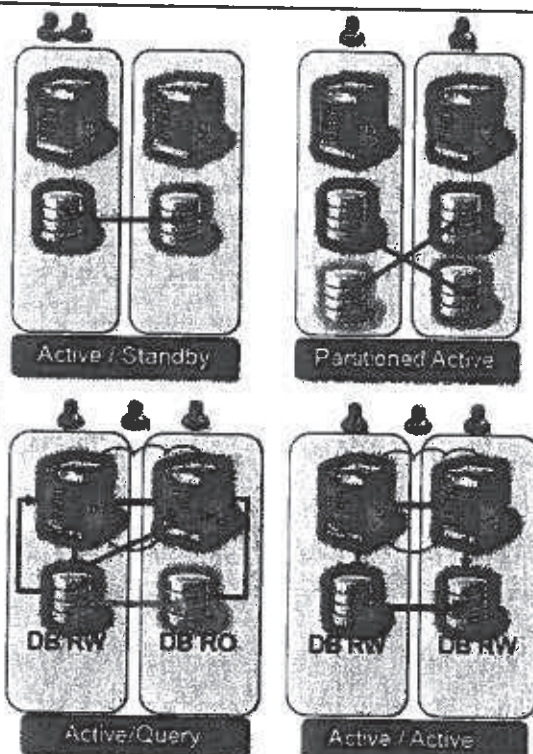




По-голямата част от промените, които са предложени в настоящия документ, няма да бъдат пряко видими за потребителите на банката. Изключения правят всички стъпки и мерки предложени в *Стратегия за развитие на информационната сигурността и Active-Active Datacenter*

Развитие на HA Архитектурите за реализация на Active-Active DC

Архитектурата „Active-Active Datacenter“ се използва за едновременно използване и резервиране на съществуващия капацитет, като основния фокус е защита от срыв и в по-малка степен ефективност при утилизация на оборудването.

Architecture	Description		
Active / Standby	• Traditional DR or warm standby environment • RTO = hours to days • RPO = 0?	Active / Standby	Partitioned Active
Partitioned Active (No WAN Clustering, unidirectional DB replication w/failover)	• Each site application cluster runs independently, as do the DB's. Users are directed to one or the other sites. DB's send records to Source of Record DB • RTO=hours • RPO=0?	Active/Query	Active / Active
Active / Query (WAN replication, unidirectional DB replication w/failover)	• Each site application cluster lives, reads performed from local DB, writes performed on primary DB only, aka activequery • RTO = minutes to hours • RPO = 0 to seconds		
Active / Active (WAN replication & bidirectional DB replication)	• All applications uncoupled and databases read/writable • RTO = seconds to minutes • RPO = 0 to seconds		

Active/Standby е традиционния вариант за архитектура от първите IT проблеми – стар, надежден и скъп за минималното предоставено покритие. Често резервния DC става идентичен на активния DC и това увеличава риска, защото много организации искат да използват резервния за развойна среда вместо да го оставят неработещ – в действителност увеличават значително тяхното RTO.

Partitioned Active е една стъпка напред пред Active/Standby в това че и двата DC обслужват клиенти като различни приложения се стартират на различните сайтове и се разменят във резервирането им. Този подход позволява да се резервират приложения без да се налага да бъдат променяни заради новата топология. Пренасочването става на база географско приложение, номер на акаунта, дирекция и др. – Характерното тук е че повечето потребители работят в едното DC, другите в друго но никога двете не смесват средите, с изключение на катастрофален срыв с останал един единствен DC. Разделянето на

потребителите позволява да се направи еднопосочна репликация от всяка система, недопускайки конфликти в данните и осигурвайки атомарна консистентност.

Asymmetric Active или **Active/Query** означава че само едната база е в режим read/write а нейната реплика може да се използва в read-only приложения. Потребителите които четат могат да бъдат обслужвани своята локална база данни, но потребителите обновяващи данните трябва да са свързани към първата. Приложенията трябва да бъдат променени, така че трябва да се препращат заявките към актуализиращата база. Съществуват мрежови устройства, които вършат такава работа, намалявайки администрирането на базите и намалява отражението върху базите.

Друг вариант е да се публикуват данните през web service или Layer 7 URI рутиране през Server Load Balancers или подобни. Както и предишните решения по-напредналите организации внедряват zero-outage приложения като използват N и N+1 конкуренти инсталации.

Active/Active означава, че всички DC предоставят една и съща услуга на всички свои потребители във всички DC синхронно. Този метод предоставя transparent fault tolerance включително и ниво „облак“, услугата продължава да работи при планирани или не планирани спирания, защото на практика е един и същи „облак“. Съществен елемент е осигуряване на консистентност на данните едновременно и на двете места.

Константността се осигурява от една страна от приложението, ако е подготвено за подобна работа, от друга страна с механизми, които позволяват приложенията да се абстрахират къде в действителност се намират техните данни – Storage Virtualization.

Данните са критична част от решението за Active/Active DC в среда на IBM дискови масиви съществуват два подхода, използвани за реализиране на синхронизацията:

HyperSwap - Power машините и DS8000 масивите работят съвместно, така че независимо от разположението на VM на една среда, тяхното преместване върху друг сървър или друг сайт. Те винаги работят с локалния дисков масив, за да се осигури максимална производителност и минимално закъснение.

Storage Virtualization – в този подход данните се презентират от виртуализационния слой в по-близкия до приложения SAN, но данните по-скоро са в модела Asymmetric Active и би могло да се получи значително натоварване при големи операции за обновяването им.

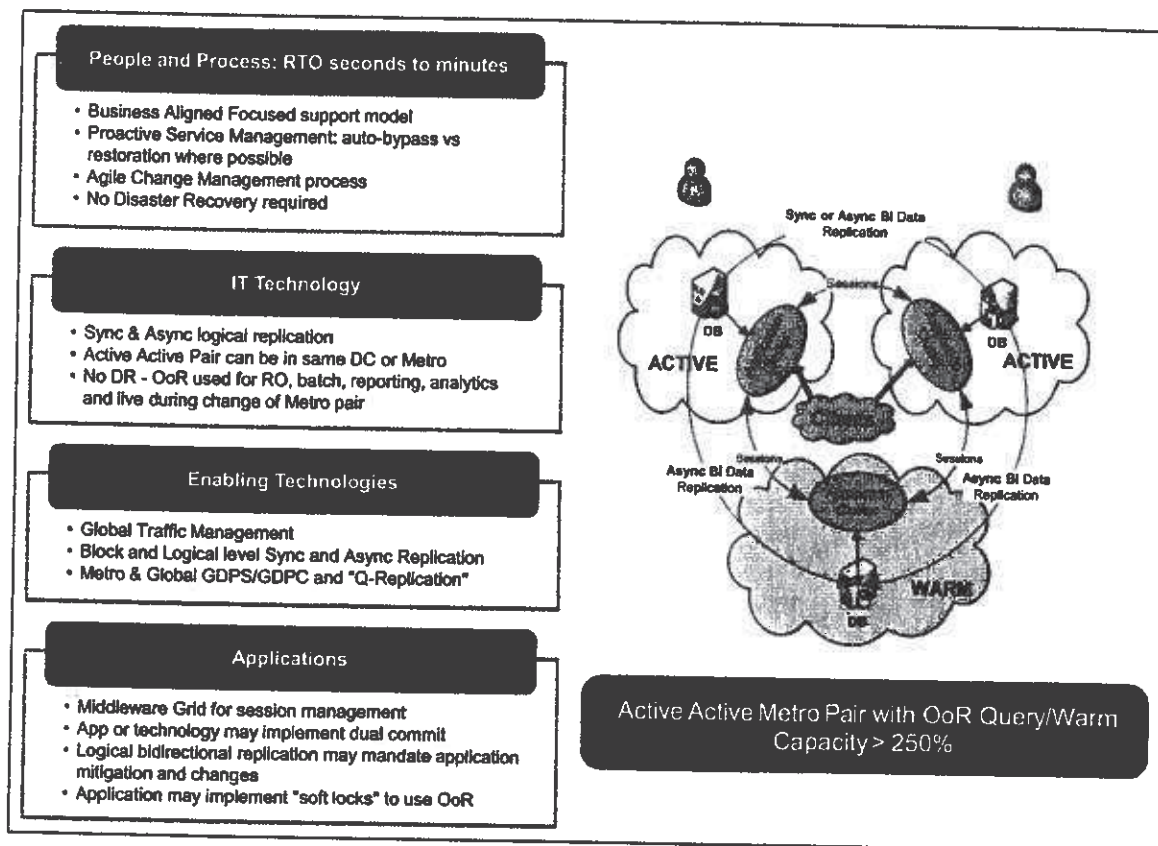
1.1.1. High-Level Design на HA

Въвеждаме някои понятия

OoR – Out of Reach – отдалечен DC

Active/Active в градски дистанции – Metro Area

Характерното на представения на схемата модел е, че осигурява възстановяването на работата в изключително кратки срокове – до няколко минути в случая, когато се рестартира върху отдалечения сайт.



Трябва да се има в предвид, че допълнителното резервиране на капацитета е по-голям от 250%, ако искаме освен данните да бъдат спазени и SLA за производителност при отпадане на цял сайт.

При модела отдалечения сайт се използва като RO или Test&Dev сайт, но не работи активно с приеманите данни. Ние предлагаме в отдалечения сайт да се извършват процедурите по архивиране на данните и тяхното складиране на ленти.

При изграждане на архитектура за резервиране базирана на ТРИ активни DC освен практически безотпадна работа на сайтовете, ефективността на ангажирувания капацитет е много по-голяма.

Обичайното резервиране е >250%, за да бъде постигнато същото обслужване при DR ситуация. При 3 активни DC е необходимо да бъде резервиран само един от тях, докато другите два продължават да работят, тогава необходимия за резервиране капацитет намалява до >150%



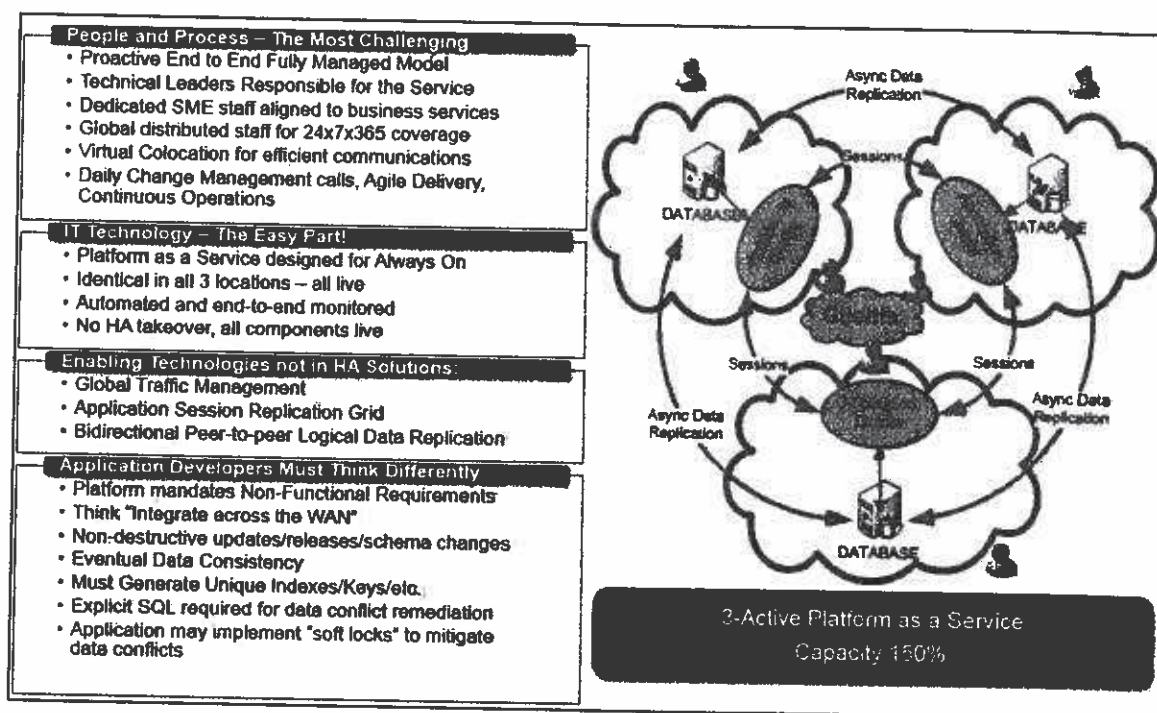


Figure 7. Three Active geographically distributed

1.1.2. Реализация

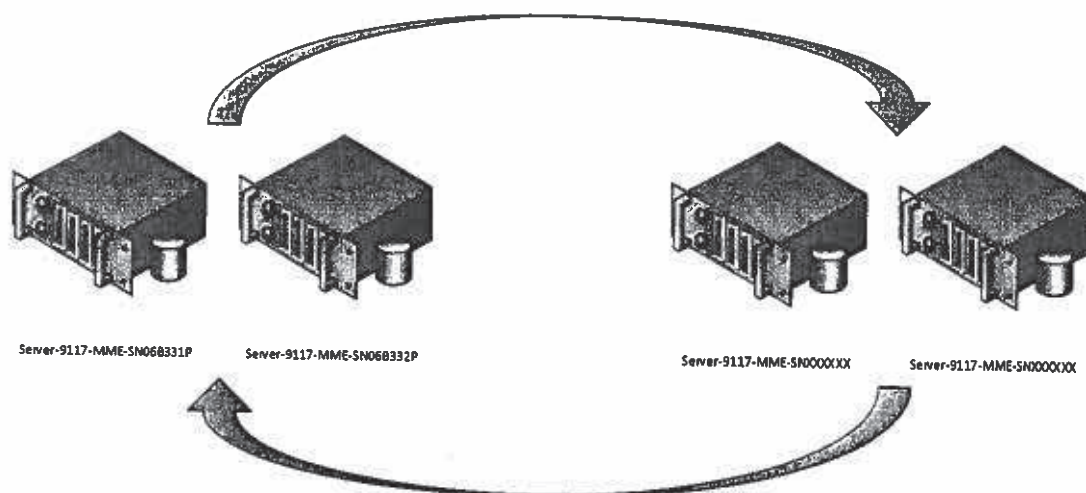
Active-Active DC ще осигури по-доброто оползотворяване на наличния ресурс, като се използва активно оборудването, както в близки така и в отдалечения DC. Позитивен страничен ефект е, че постоянно ще бъде поддържана среда с висока надеждност за комуникация и с възможност за преместване на виртуални среди между двата центъра за данни за планови спирания на сървъри и дискови масиви или при евентуална авария.

Изискванията за производителност лимитират разстоянието между сайтовете с връзката между тях. Тя трябва да е под 100 км., което е изпълнено, при използване на двата сайта в София. За да се елиминира "Split brain" проблема, трябва да бъде организиран трети логически сайт, който да участва в комуникацията на SAN и дисковите репликации независимо от основните, за него е достатъчно да бъде елиминирана вероятността да отпадне едновременно с някой от двата основни сайта. В идеалния случай това е изнесен офис с FC диск за кворум записите, но може да бъде и резервиран дисков масив в някой от DC със собствени линии за достъп до SAN и отделно захранване UPS.

За основните UNIX сървъри, първата стъпка е критичните системи, които работят в клъстерна среда да бъдат виртуализирани и да имат аналогични по производителност и архитектура членове в отдалечения сайт. Част от концепцията за осъвременяването на инфраструктурата.

За системите, за които не е предвиден PowerHA клъстерен софтуер ще се използва Live Partition Mobility, така че да е възможно ръчното преместване върху друга машина

(включително и върху отдалечения сайт), за да се осигури възможност за планово спиране на отделни сървъри. Отново условието е да се изравнят сървърите от двата центъра за данни.



Спазвайки стратегията на банката за това критичните системи да работят в клъстерен режим, препоръчваме клъстерираните VM да работят в един и същи сайт в конкурентен режим, а между сайтовете в active-standby.

Участващи машини (разчита се, че клъстерираните приложения вече са прехвърлени във виртуална среда – върху POWER 770) :

- Двойката Power 770 на основния сайт или техните наследници, според стратегията за обновяване ;
- Нова Power7 машини от същия клас или POWER8 машина в Касов център;
- Двата DS8x00 със стартирана репликация и интеграция на HyperSwap функционалността;

Storage design

Основната цел е да се елиминира опасността от отпадане на основния дисков масив, където работят всички членове на клъстаре, забавеното/ръчно рестартиране в отдалечения сайт. В active-active 2 sites конфигурация, HyperSwap автоматично поддържа репликация на данните между двата дискови масиви като едновременно с това осигурява на приложенията среда, в която да са Online. В случай, че основния дисков масив отпадне (планирани или не планирано), всички приложения се прехвърлят да работят в резервния дисков масив. В този случай PowerHA® SystemMirror® извършва прехвърлянето и след това новото синхронизиране на данните към възстановения масив.

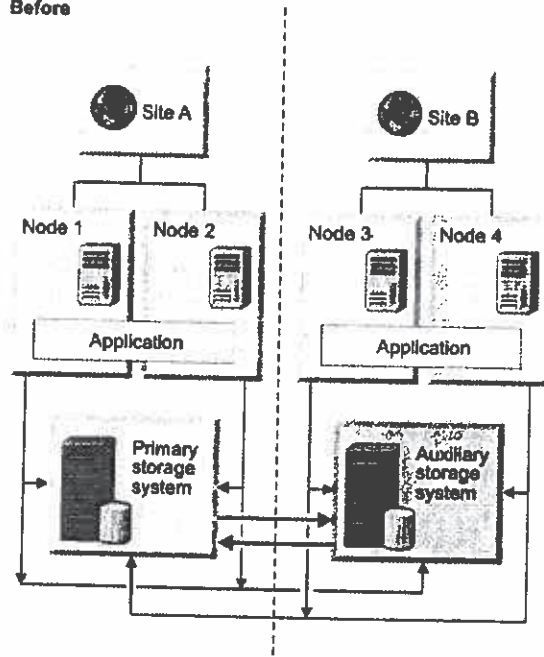
- Активните приложения работят и на двата сайта А и В;
- Има по две машини във всеки от сайтовете или общо 4 Power сървъри
- Всички участват в mirror groups, конфигурирани да използват HyperSwap® или традиционната in-band функция.

При необходимост приложението да премине от сайт А към сайт В (двата сървъра спират или са недостъпни, дисковия масив е отпаднал) приложението продължава да работи от втория сайт и втория масив става основен, процеса е автоматичен и с използването на HyperSwap дефинициите на пътищата се запазват.

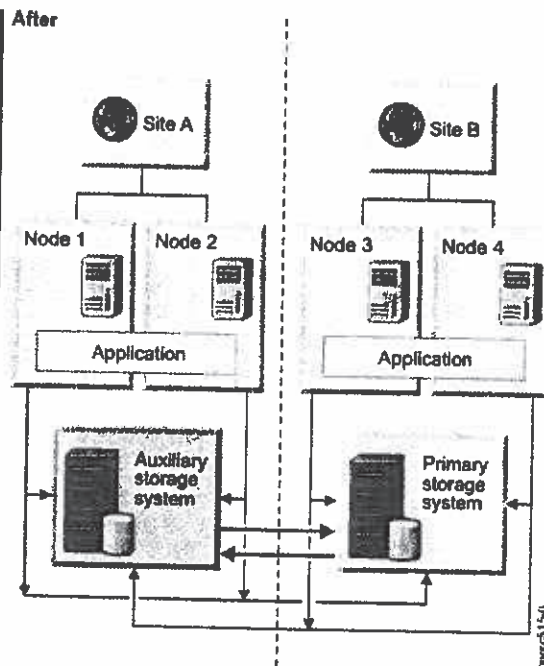
При възстановяване на първия масив, активния синхронизира обновяванията си с него и прехвърля обратно основните операции в него.

Приложенията

Before



After



За x86 машините, под управление на VMware трябва да бъде извършена миграция към виртуализирана среда под - VMware избраната виртуализационна платформа.

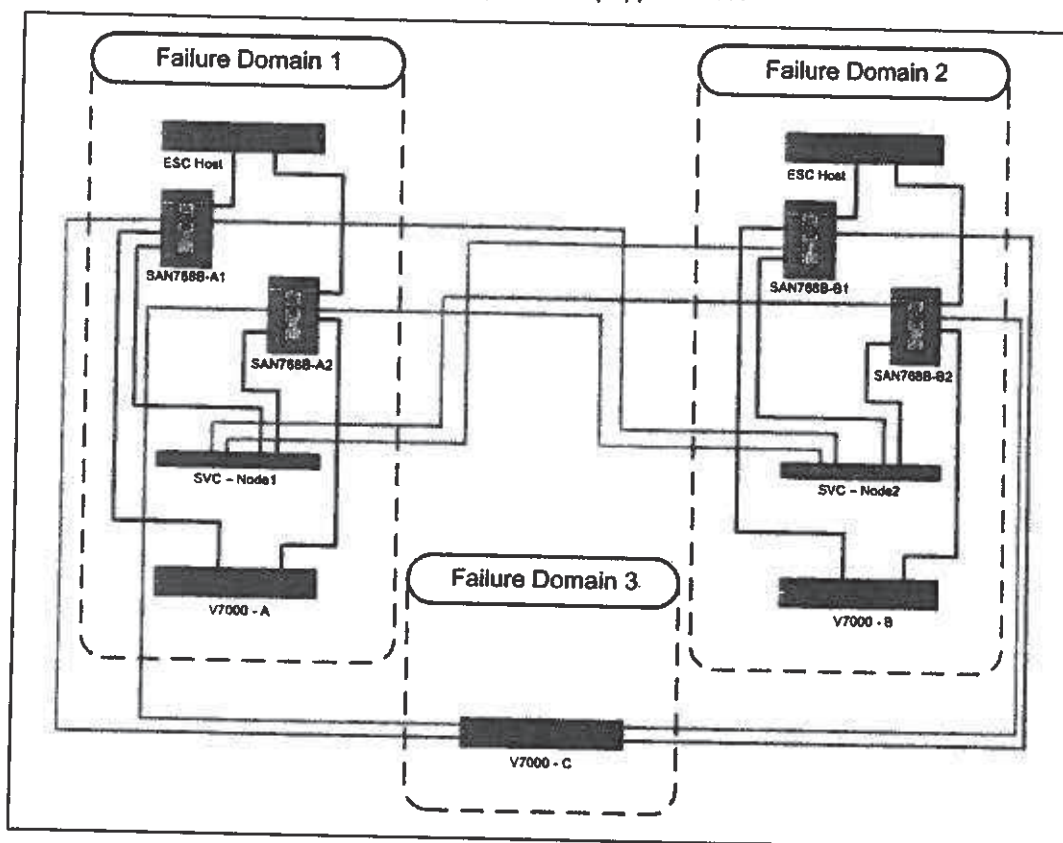
Участващи машини:

- x86 Blade servers на две шасита в двата сайта;
- Двупроцесорните сървъри x3560, 3550;
- Нови rack машини, в зависимост от нови натоварвания;
- Двата DS8x00 със стартирана репликация HyperSwap;

Тъй като по-старите дискови масиви DS8700 и DS8100, върху които текущо работи репликация са излезли от актуалните продуктови листи на IBM и са с лимитиран капацитет от 10 TB, ще трябва да се осигури нов дисков масив в основния сайт с достатъчен капацитет и функционалността така че двойката DS8870 да позволява основните системи да бъдат напълно резервирани и репликирани.



За осигуряване на подобно функционалност за некритичните системи предлагаме да се възползваме от резултатите по внедряване на виртуализирана SAN среда. След внедряване на SVC stretched cluster и интеграцията с x86 платформа и не-критични приложения върху Power платформа ще бъде осигурена репликация между сайтовете и консистентност на обръщенията от сървъри към SAN, включително и на виртуалната среда – NPIV.



SVC stretched клъстер трябва да е изграден на база две двойки SVC машини отговарящи за двете SAN фабрики - 205, 206. Софтуера ще позволи да се изградят единно представяне на данните от дисковите масиви към виртуалните среди.

VMWare от версия 5.5 поддържа работата на Stretched клъстер с „preferred path” оптимизирайки работата на SVC, както и да намали прехвърлянето на данните през линиите между сайтовете.

Неклъстерираните Power базирани приложения също могат да бъдат инсталирани, тъй че да ползват данните от дисковите масиви през SVC, но може да работят и върху двойката DS8870 масиви.

Преминаване към виртуални работни места - VDI.

1.2. Текущо състояние

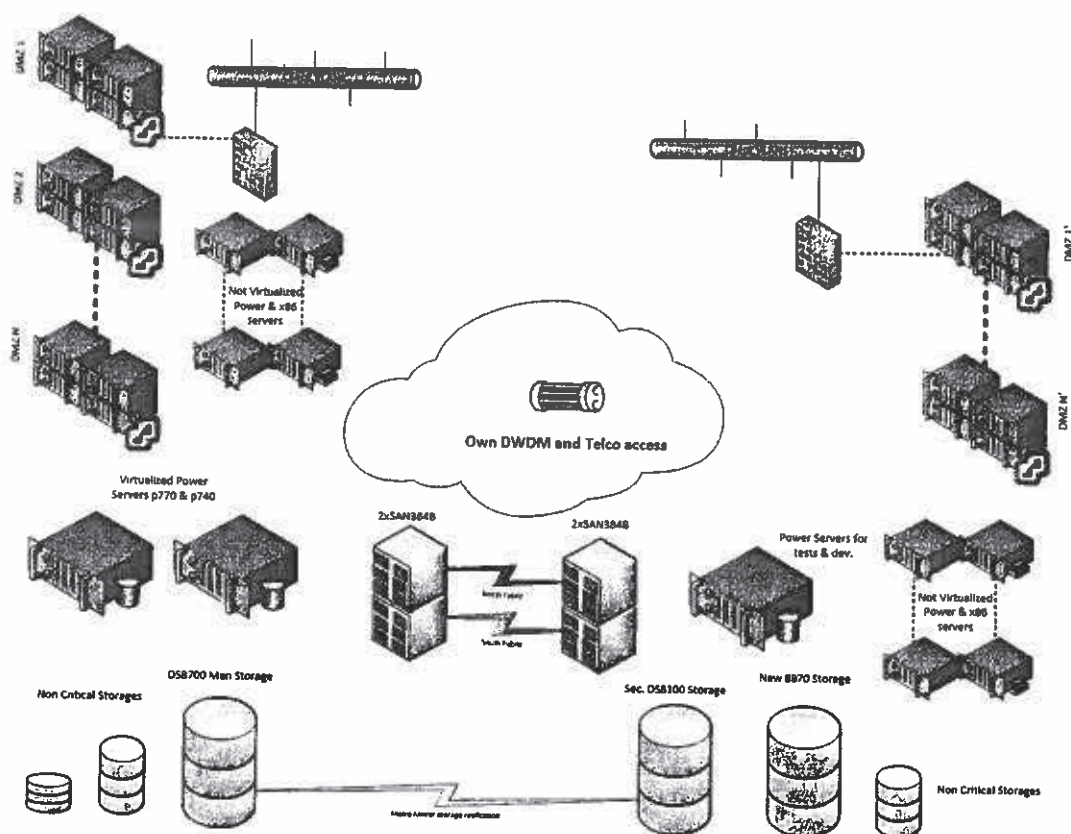
ИТ инфраструктурата на БНБ е изградена в съответствие с изискванията на стандартите на финансовите институции, добрите практики, индустриални стандарти и препоръките на партньорските организации.

Създадени са два центъра за обработка на данни, основен и резервен. В основния център оборудването е обособено в две отделни зали с резервиране на свързаността и електрическото захранване. Отдалеченият център се намира в рамките на същия град (разстояние по права линия 10 км.) и в него се резервират критичните за банката информационни системи и данни.

Двата центъра са оборудвани с резервирани независими захранвания и климатизация. Външната свързаност – интернет, връзки към външни организации и партньори е резервирана и е достъпна до двата центъра през основния център за данни.

Локалната мрежа е изградена на база високоскоростни комутатори от Cisco – Catalysts & Nexus series и е разделена на сегменти по бизнес направления и специализирани сегменти – администриране, IP гласови услуги, и др. От съображение за повишаване на сигурността са отделени DMZ сегменти за системите с достъп до интернет, външни услуги и организации. DMZ сегментите са изолирани чрез защитни стени.

Връзката между двата центъра се осъществява на база Cisco DWDM технология осигуряваща резервирана по различни трасета свързаност за LAN и за SAN трафика. Комуникационните трасета са с дължина съответно 14 км. и 17 км. и се осигуряват от двама доставчика на комуникационни услуги с взаимно независима инфраструктура. Скоростта на трансфер между сайтовете е Nx4 Gbps за SAN и Nx10 Gbps за LAN трафика.



В зависимост от изискванията за достъпност на услугата са формирани следните области:

- **Критични системи** – Базираны предимно върху IBM Power базирани машини и в зависимост от изискванията x86 базирани сървъри,. Реализирани са като клъстерно решение на основния сайт и неклъстерирана stand-by среда на резервния сайт. Данните на критичните системи се резервират главно посредством асинхронна репликация между клъстерната конфигурация на основния сайт и stand-by средата на резервния сайт. Съществуват системи които все още не разполагат със stand-by среда на резервния сайт. Техните данни се репликират на резервния сайт със синхронна репликация между дисковите системи, разположени на двата сайта.
- **Основни дискови масиви** - Основните информационни масиви на Банката са консолидирани върху дискови масиви на IBM от висок клас DS8x00, осигуряващи бързодействие и висока надеждност на данните в тях. Извършва се синхронна репликация на ниво дялове от дисков масив от основния към резервен център за данни за резервиране на данните.
- **Основна SAN фабрика** – съставена от две двойки SAN384B комутатори на 8 Gbps. В основния сайт двойката е разделена в различни зали, в резервния комутаторите са заедно.
- **Некритични сървъри** – Power и x86 базирани сървъри, върху които работят некритични приложения, извършват се тестове, обучения и разработка на нови приложения.



- **Допълнителни дискови масиви** - представляват отделни дискови масиви от IBM и EMC, използвани за съхраняване на временни данни на критични приложения (dumps, exports temp space etc.) и основна локация за данните на некритични приложения
- **Среда за архивиране на данните на БНБ** - Състои се от две лентови библиотеки за Backup & restore на цялата инфраструктура. Ритмичността за архивиране на данни се определя в зависимост от регулаторни изисквания и бизнес изискванията на различните системи. Двете лентови библиотеки са производство на IBM и са разположени на двата сайта на БНБ, като процеса по архивиране на системите е синхронизиран и се извършва едновременно на двата сайта. Средата се управлява от IBM TSM.

Възприети са следните принципи при изграждането на информационната инфраструктура и създаването на системи за БНБ:

- Оборудването на критичните системи на БНБ, включително и критичната комуникационна инфраструктура, задължително трябва да бъде резервирано, с цел елиминиране на всички единични точки на прекъсване.
- Опорните комуникационни връзки трябва да са сдвоени и резервирани по независими едно от друго трасета.
- Всички сървъри, дискови масиви, лентови библиотеки и критично комуникационно оборудване трябва да бъдат свързани към два независими източника на електрическо захранване, да са с резервирани LAN и SAN интерфейси и да бъдат инсталирани в стандартни сървърни шкафове.
- Компонентите на цялата ИТ инфраструктура трябва да позволяват отдалечено администриране и управление чрез системи за контрол и наблюдение на инфраструктурата.
- Основните информационни единици да бъдат изнесени и да работят върху дискови масиви, в зависимост от критичността им – върху основните или допълнителните дискови масиви.
- Критичните системи работят върху основния сайт, като данните им се репликират върху резервния.
- Основните приложения и бази данни да бъдат клъстеризирани, с цел намаляване на възможността за отпадане на услугата и загубата на данни.
- Възприета е единна политика за Backup & Restore, реализирана чрез лентовите библиотеки и TSM сървъри отговарящи за архивирането, възстановяването и защитата на данните от приложения, бази данни, операционни системи и системен софтуер.
- Извършват се регулярни тестове на правилното функциониране и необходимите действия при системни събития или сригове на елементи от ИТ средата.

В ход е инициатива за изграждане на високонадеждна среда разпределена на основния и резервния сайт, за предоставяне на услугите за вътрешните и външните потребители на БНБ, която за в бъдеще се предвижда да бъде разширена и до трети отдалечен сайт (около 150 км от основния и резервния) за възстановяване при бедствия и аварии. До момента е извършена



виртуализация на част от основните информационни системи, на базата на VMware и PowerVM и са подготвени комуникационните връзки между основния и резервния сайт.

2. Стратегически инициативи

2.1. Виртуализация

Фокуса на развитието на новите технологии в IT света е ориентирано към модели на споделено ползване на хардуера, в това число чрез средствата на виртуализацията.

БНБ се намира в процес на изместване на дискретните сървърни системи към виртуализирани комплекси от сървъри. Факторите, които задържат процеса по освобождаването, биха могли да се опишат като:

- Наличните сървъри са достатъчно производителни и надеждни за определените им цели, че да се налага замяната или включването им в виртуални пулове;
- В някои проекти трябва да бъде осигурена изолирана от останалите системи среда;
- Често администрирането на конкретен дискретен сървър е по-лесно, отколкото администрирането на виртуализирани среди.
- Остарели софтуерни приложения, за които не е целесъобразно или не е възможно да се изгради нова виртуализирана среда

Ползите от създаване на виртуална среда са много, както във финансово изражение, заради по-доброто използване на ресурсите, така също и заради улесненото провизиране на нови машини, по-високата надеждност и т.н.

Банката е избрала две hypervisor платформи за изграждане на виртуалната среда:

- За IBM Power базираните сървъри – PowerVM
- За x86 сървъри – VMWare

2.1.1. PowerVM

PowerVM позволява множество различни приложения да бъдат консолидирани върху един или няколко POWER сървъра, като се постигне по-добра производителност и надеждност, гъвкаво управление и разпределение на ресурсите. PowerVM предоставя сигурна и разширяема сървърна виртуализация за AIX, Linux, IBM i приложения едновременно.

- Предоставя услуги с висока ефективност чрез консолидиране на натоварванията;
- Предоставя бързо облачни услуги създадени като автоматизира конфигурирането и инициирането на виртуални машини в сървърите и дисковите масиви
- Оптимизира утилизацията на сървърните и дисковите ресурси и така намалява разходите по придобиване и експлоатация
- Възможности за ефективно увеличаване на капацитета чрез “scale-up” и “scale-out” архитектури

- Елиминира необходимостта от планирано спиране на услугите, предоставяйки мобилност между сървърите
- Предоставя високо качество на услугите чрез управление на виртуалните ресурси

В последните години IBM отделя голяма внимание върху опростяване на използването и администрирането на сървърните платформи и виртуализацията в две основни направления:

- Модернизира приложенията и интерфейса за администриране на Power сървърите – HMC, PowerVC, PowerVP като се пренаписват голяма част от функциите, които да автоматизират процесите по управление на ресурсите.
- Внедрява отворени стандарти и приложения, така че платформата да стане част от гъвкави Open Source решения и да бъде интегрирана в облачни услуги максимално лесно.

PowerVM е комбинация от хардуерни възможности и допълнителен софтуер, който разширява възможностите за:

- По-ефективно ползване на процесорите – разделяне на процесорите на части от процесорите - Micro-partitions, разделяна на физическите процесори/ядра от логическите - Logical partitioning, динамично присъединяване или изключване чрез Dynamic logical partitioning и Shared Processor Pools
- по-ефективно управление на паметта – заемане и отдаване на памет между виртуалните машини според текущите нужди на работещите приложения - Active Memory Sharing, Дедупликация - Active Memory Deduplication;
- Резервирани виртуални IO компоненти SCSI, Fiber Channel, NPIV support, Optical device & tape, SR-IOV;
- Надеждност – изолирани VM, на ниво хардуер, микрокод, сдвоени VIO сървъри за алтернативни пътища в рамките на виртуалната среда, приоритизация;
- Ефективно използване на ресурсите на дисковете – поддръжка на Thin & Thick provisioning, Shared storage pools за RootVG;

Features and technologies	Function provided by
PowerVM Hypervisor	Hardware platform
Logical partitioning	Hypervisor
Micro-partitioning	Hypervisor
Dynamic logical partitioning	Hypervisor
Shared Processor Pools	Hypervisor
Integrated Virtualization Manager	Hypervisor, VIOS, IVM
Shared Storage Pools	Hypervisor, VIOS
Virtual I/O Server	Hypervisor, VIOS
Virtual SCSI	Hypervisor, VIOS
Virtual Fiber Channel	Hypervisor, VIOS
Virtual optical device & tape	Hypervisor, VIOS
Live Partition Mobility	Hypervisor, VIOS

Partition Suspend/Resume	Hypervisor, VIOS
Active Memory Sharing	Hypervisor, VIOS
Active Memory Deduplication	Hypervisor
Active Memory Mirroring	Hypervisor
Host Ethernet Adapter (HEA) ^c	Hypervisor

В листа с Power Сървърите са предвидени две нива на PowerVM – Standard & Enterprise. от таблицата по-долу се вижда, че за осигуряване на по-висока надеждност и наличност на услугите на сървърите препоръчваме Enterprise, така ще се получи и по-добра утилизация на ресурсите.

PowerVM capability	PowerVM Express Edition	PowerVM Standard Edition	PowerVM Enterprise Edition
Maximum VMs	3 / Server	1000 / Server	1000 / Server
Micro-partitions	Yes	Yes	Yes
Virtual I/O Server Management	Yes (Single)	Yes (Dual)	Yes (Dual)
	VMControl, IVM	VMControl, IVM, HMC	VMControl, IVM, HMC
Shared dedicated capacity	Yes	Yes	Yes
Multiple Shared-Processor Pool	No	Yes	Yes
Live Partition Mobility	No	No	Yes
Active Memory Sharing	No	No	Yes
Active Memory Deduplication	No	No	Yes
Suspend/Resume	No	Yes	Yes
Virtual Fiber Channel	Yes	Yes	Yes
Shared Storage Pools	No	Yes	Yes
Thin provisioning	No	Yes	Yes
Thick provisioning	No	Yes	Yes

В допълнение на вградените функции в PowerVM, IBM предоставя допълнителен софтуер за наблюдение и управление на ресурсите – PowerVC, PowerVP и PowerSC.

В последните години PowerVM и Power хардуера се развива за да отговори на нуждите на клиентите като се добавят :

- Поддръжка на 20 партиции на ядро, удвоявайки броят им върху едно ядро. Това предоставя допълнителна гъвкавост и намалява минимума на заемане на процесор до 5%.
- Dynamic LPAR позволява динамично добавяне и махане на виртуални I/O адаптери от и към Virtual I/O Server партиции
- Възможност потребителя да дефинира Fibre Channel порт от някой или всички адаптери.

- Подобрена инсталация на Virtual I/O Server, настройка и валидиране от използвайки Runtime Expert.
- Live Partition Mobility поддържа до 16 конкурентни сесии LPM.
- Shared Storage Pools - създаване на области в дискове върху масиви за виртуалните процеси достъпвани и управлявани съвместно от всички участващи в Pool сървъри, с цел подобряване използването на пространството и намалява разходите за SAN. Повишената надеждност на Shared Storage Pools включва:
 - IPv6 и VLAN tagging (IEEE 802.1Q) поддръжка за интермодална комуникация между сървърите;
 - Повишена надеждност и достъпност на клъстерните услуги;
 - Подобрени статистики и отчети;
 - Непрекъсващи работата обновявания;
- Нов VIOS Performance Advisor, който да анализира Virtual I/O Server производителността и да дава насоки за оптимизации.
- PowerVM има и нови възможности предоставяни от VMControl, които да ускорят инсталирането на particии, оптимизиране на дисковете и достъпността чрез автоматизиране на процеса.
 - Свързани клонирани дискове позволяващи създаването на partition images;
 - Управление на системния пул за IBM i.;

2.1.1.1. IBM PowerVC – Virtualization Center

IBM® PowerVC Virtualization Center е предложение базирано на OpenStack, предоставящо опростено управление на виртуализацията на IBM AIX®, IBM i and Linux virtual machines (VMs) работещи върху IBM Power Systems™. PowerVC е създадено да увеличи продуктивността на администраторите и да опрости управлението на VMs и LPARs на Power Systems servers. PowerVC допълва възможностите на Power Systems за изграждане на разширяем гъвкав облак, включително и чрез тясната интеграция с higher-level cloud managers базирани на OpenStack technology.

PowerVC дава на клиентите възможността да създадат и управляват библиотека от виртуални машини, позволявайки на IT мениджърите бързо да създават виртуални среди, като стартират VM от дефинираните в библиотеката копия, вместо тепърва да инсталират всяка една по отделно. PowerVC позволява на IT мениджърите и администраторите да създават групи от ресурси, необходими за изпълнение на задачите. Те могат бързо да бъдат настроени според нуждите и да спомагат за по-добрата утилизация и намаляване на усилията и средствата за администриране, като правят IT по-гъвкави на бизнес и пазарните изисквания.

Архитектурата на PowerVC използва OpenStack платформата, за да предостави платформата за управление на виртуализацията на Power Systems. Това включва IBM Power®-специфичен потребителски интерфейс, IBM-specific OpenStack драйвери за Power Systems интерфейси за управление като hardware management console (HMC), в допълнение –

възможности за scheduling. Клиентите търсещи отворени виртуални инфраструктури могат да използват PowerVC за управление на своите PowerKVM внедрявания върху Power.

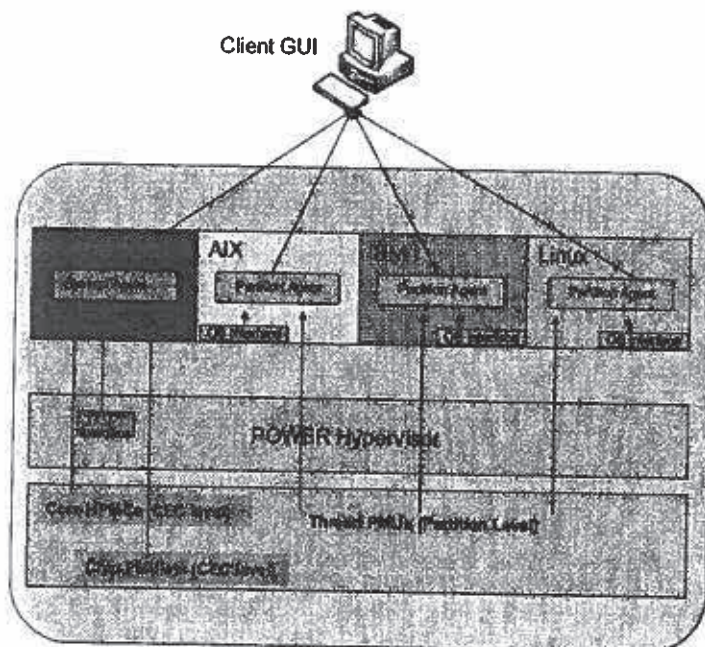
PowerVC се предлага единствено в Standard edition, която управлява виртуални системи контролирани от HMC и директно PowerKVM.

- Инсталиране и конфигуриране на целия хардуерен (host, storage and network) и софтуерен stack (PowerVC components)
- Лесна инсталация може да бъде инсталирано и конфигурирано за няколко часа от администраторите any skill level
- Близък до реалната работа процес включващ внедряването, оперативната работа и поддръжката
- Надеждна, разширяема и ценово ефективна платформа и стандартно API добавяща към виртуализацията характеристики на облачни услуги
- Лесно управление на виртуализацията на PowerVM и PowerKVM

2.1.1.2. IBM PowerVP Virtualization Performance

IBM PowerVP™ предоставя интелигентен анализ на текущите натоварвания с цел да се вземат подходящи решения в рамките на виртуална среда и хардуерни сървъри като разположението на виртуалните машини или утилизация на свободни сървърни ресурси като памет и процесор за оптимално изпълнение на процесите.

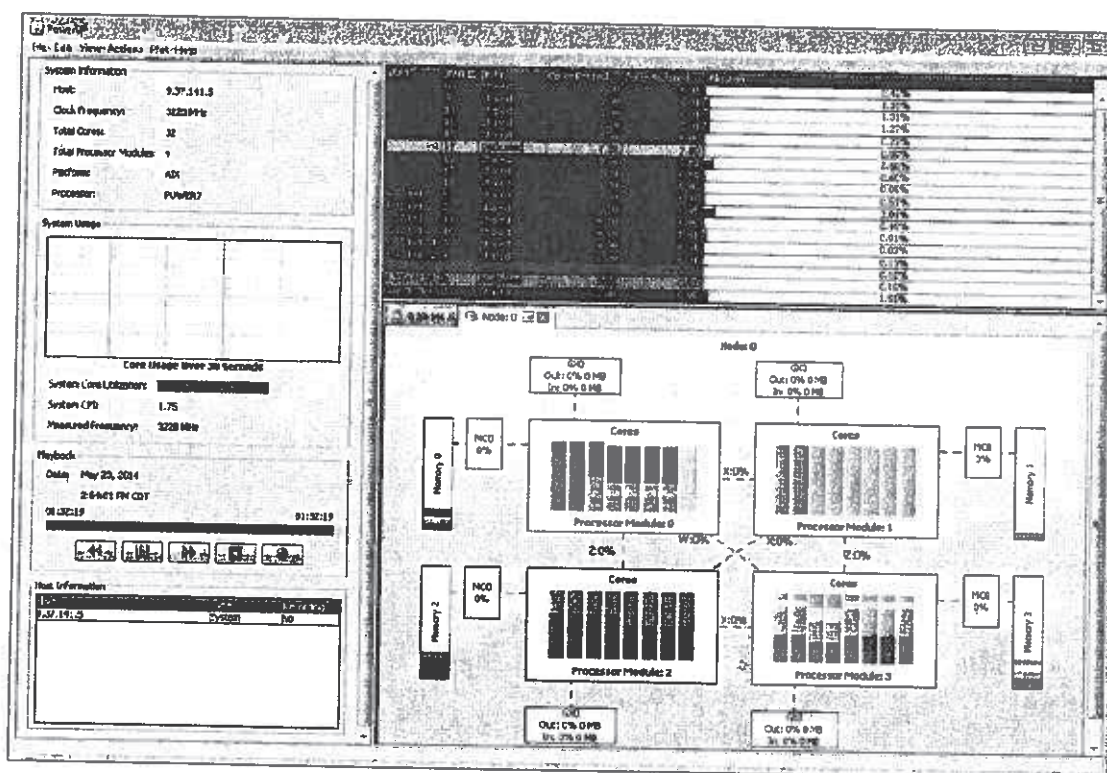
Архитектурата на IBM PowerVP™ е базирана на събирането и презентирането на информация от специализирани агенти на всяко ниво от инфраструктурата. Заедно с това е предвидена възможността да се „проиграят“ исторически данни.





- Оптимизират се виртуализираните IBM® Power Systems™;
- Да се види текущото натоварване от конкретния процес през виртуалните машини към хардуера;
- Удобна графична презентация в реално време като се подчертават претоварените ресурси;
- Възможност за проиграване на запазени исторически данни за натоварванията
- Ускорява разрешаването на проблеми с производителността;
- Проактивно наблюдение на натоварването на виртуализирани процеси.

Потребителския интерфейс е базиран на Java достъпен през повечето популярни операционни системи като интерпретира в реално време данните от агентите и потребителя може да разбере, кой процес в кои физически ядра е разположен, дали са оптимални пътищата на IO данните и използвания кеш.



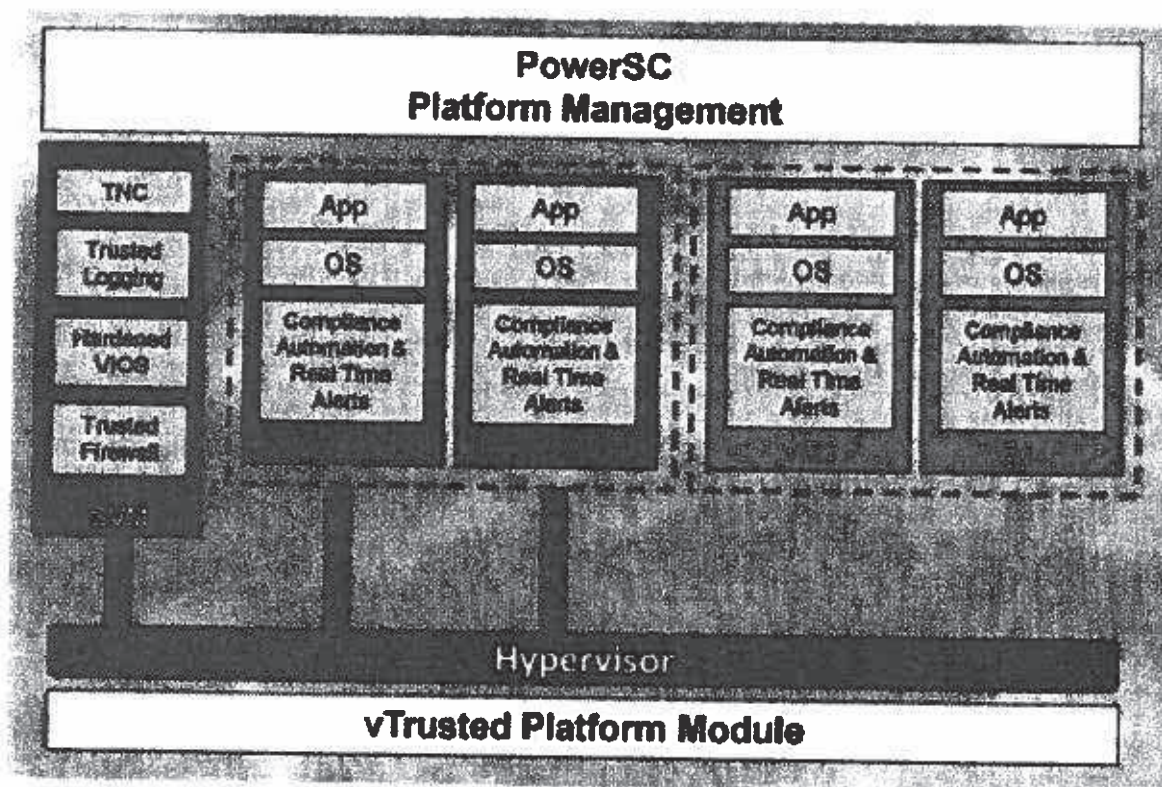
2.1.1.3. IBM PowerSC

IBM PowerSC™ добавя още едно ниво на сигурност и compliance, оптимизирано за виртуализирани среди на база Power Systems™ сървъри работещи под управлението на PowerVM®, AIX® и Linux. Контролите и съответствието със стандартите за сигурност са основни компоненти необходими за защита на виртуализираните центрове за данни и облачна инфраструктура срещу увеличаващите се заплахи за сигурността.



- Опростява управлението на сигурността и спазването на изискванията на добрите практики и стандарти;
- Намалява разходите за администриране на мерките по повишаване на сигурността и отговарянето на регулаторните изисквания;
- Осигурява същото ниво на сигурност на виртуалните среди като на отделни физически сървъри;
- Предоставя средства за проверка и одит на сигурността на виртуализирани системи;
- Намалява необходимото време и квалифицирана работа за подготовка на одити;

Сигурността и съответствието на регулациите е съществен елемент за банките и финансовите институции. Те често трябва да отговарят на високи изисквания на регулаторните органи, за да запазят персоналните и корпоративни данни от атаки. Осигуряването IT системите да отговарят на изискванията на общоприетите стандарти и препоръки може да бъде оптимизирано за виртуализирани среди от Power Systems™ сървъри, под управлението на PowerVM®.



PowerSC използва всички възможности на IBM Power Systems Software™ stack, от хипервайзора през микрокода и виртуализацията до нивото на AIX операционната система,

както е описано в горната графика, включвайки и мрежовия трафик между нивата. Основните компоненти са описани в таблицата по-долу.

Компонент	Описание	Версия	Предпоставки
Security and Compliance Automation	Автоматизира създаването, мониторинга и одитите на сигурността и съответствието на стандарти и регулации по сигурността по: Payment Card Industry-Data Security Standard v1.2 (PCI DSS) Sarbanes-Oxley Act and COBIT compliance (SOX/COBIT) US Department of Defense (DoD) Security Technical Implementation Guide (STIG) Health Insurance Portability and Accountability Act (HIPAA)	PowerSC Express Edition PowerSC Standard Edition	POWER5 IBM POWER6® IBM POWER7®
Real Time Compliance	Мониторинг на AIX системите за администриране и нотификация, в случай че системата не отговаря на заложените правила в конфигурационната политика.	PowerSC Express Edition PowerSC Standard Edition	There is no specific hardware requirement.
Trusted Boot	Проверява boot image, operating system, and applications, и потвърждава тяхната достоверност през virtual trusted platform module (TPM) технологията.	PowerSC Standard Edition	POWER7 firmware eFW7.4, or later
Trusted Firewall	Икономисва време и ресурси чрез внедряване на директен рутинг между виртуални LANs (VLANs) контролирани от един и същ Virtual I/O Server (VIOS).	PowerSC Standard Edition	POWER6 POWER7 Virtual I/O Server Version 2.2.1.4, or later
Trusted Logging	Събира централизирано логовете върху Virtual I/O Server в реално време. Тази функция предоставя tamperproof logging и удобен лог бекъп и управление.	PowerSC Standard Edition	POWER5 POWER6 POWER7 Virtual I/O Server Version 2.2.1.0, or later
Trusted Network Connect and Patch Management	Проверява дали всички AIX системи във виртуалната сред са на необходимия софтуерен и patch level. Предоставя средства, тъй че всички AIX systems да бъдат с необходимите обновявания. Изпраща съобщения, ако системи от виртуалната среда с по-ниско ниво се включват в мрежата или е необходимо да	PowerSC Standard Edition	POWER5 POWER6 POWER7 Virtual I/O Server Version 2.2.1.0, or later



Trusted Surveyor	се приложи някакво обновяване, върху повечето системи. Наблюдава сегрегацията на виртуалните мрежи.	PowerSC Trusted Surveyor	There is no specific hardware requirement.
---------------------	--	--------------------------------	---

2.1.1.4. Предложение за развитие на виртуализацията

От няколко години в банката тече процес по консолидация на приложенията и системите върху виртуална среда работеща на двойка сървъри от висок клас Power 770. Все още има достатъчно голям брой дискретни системи работещи върху по-стари сървъри или blade шасита, върху тях работят стари или непродукционни системи и среди, които ще бъдат прехвърлени върху друга среда в бъдеще.

Нашето виждане е, че всички основни системи на банката трябва да бъдат разположени върху няколко опорни сървъра и така цялата среда да бъде резервирана, както по отношение на достъпни ресурси памет и процесор вътре в отделния сървър, така и да бъде осигурена висока производителност и резервираност на свързаността към мрежата и дисковите масиви.

Преминаването върху няколко опорни сървъра ще постигне следните цели:

- Резервираност – фокуса ще бъде изместен върху резервирането на целите сървъри, а не на отделните инстанции
- Подобряване на утилизацията – свободния ресурс в системите е консолидиран на едно място и бива заеман и освобождаван динамично
- Стандартизация – по-лесно се създават шаблони и "golden copy" на операционни системи и приложения
- Автоматизиране на инсталацията – автоматично провизиране на цели среди напр. SAP, Oracle Apps.
- Миграция на виртуалните машини – Live partition Mobility, иницирана от администраторите миграция на виртуалните машини.
- Разпределени изчисления – улесненото дефиниране, управление и преместване на LPAR ще доведе до по-добро разпределение на функциите на средата и разпределение на натоварванията.
- Подготовка за следващите стъпки в стратегията- Active-Active DC и създаване на частен облак

Обхвата на работата зависи от готовността на бизнес потребителите да освободят по-старите машини, които не са предвидени за целта. Работата може да бъде приключена за около 2 месеца, при готовност от страна на банката.

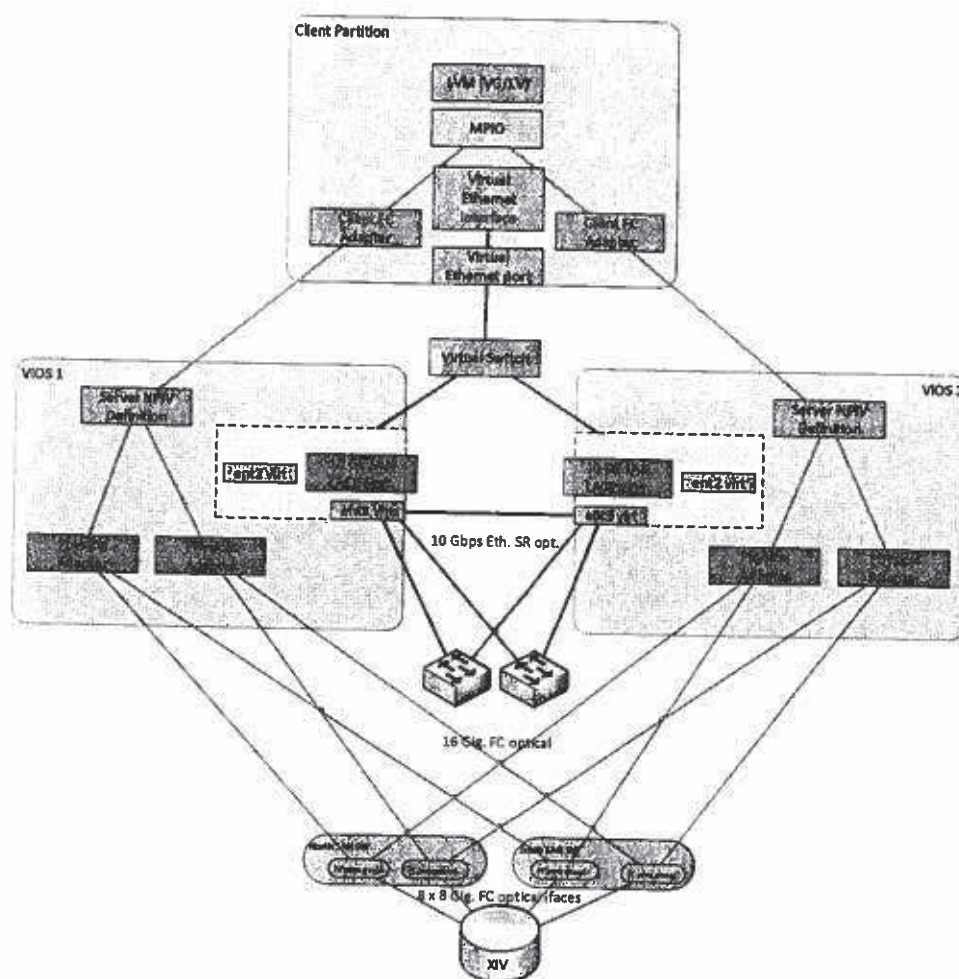
2.1.1.5. Резервиране

Традиционният подход при резервирането е добавяне на ресурс – процесори, памет, дискове, входно изходни адаптери, захранващи блокове и други с предвиден механизъм при отпадане на основния елемент работата да продължи върху резервния. Резервирането на входно-изходните операции се опростява значително, когато става въпрос за виртуализирани среди.

IBM Power сървърите обичайно се екипират така, че да се минимизира риска от отпадане на един елемент. Дублират се захранвания, дискове, мрежови интерфейси на мениджмънт контролерите, а от средния клас нагоре и самите контролери, HBA Fiber Channel & LAN интерфейси.

Концепцията за резервиране продължава и във виртуална среда. VIOS сървърите са резервирани, за да не повлияят на виртуалните машини, когато се наложи да бъдат рестартирани след Updates или др.

Виртуалните мрежови и SAN интерфейси също се резервират, или в “multipathing” режим или във Fail-Over в зависимост от приложенията



Резервирането на LAN в PowerVM става чрез агрегирането на няколко интерфейса в Etherchannel група и дефиниране на fail-over групи.

Резервирането на SAN или дисковото пространство става чрез поддръжката на дискова среда от тип Enterprise Storage Pool, FC multipathing, NPIV

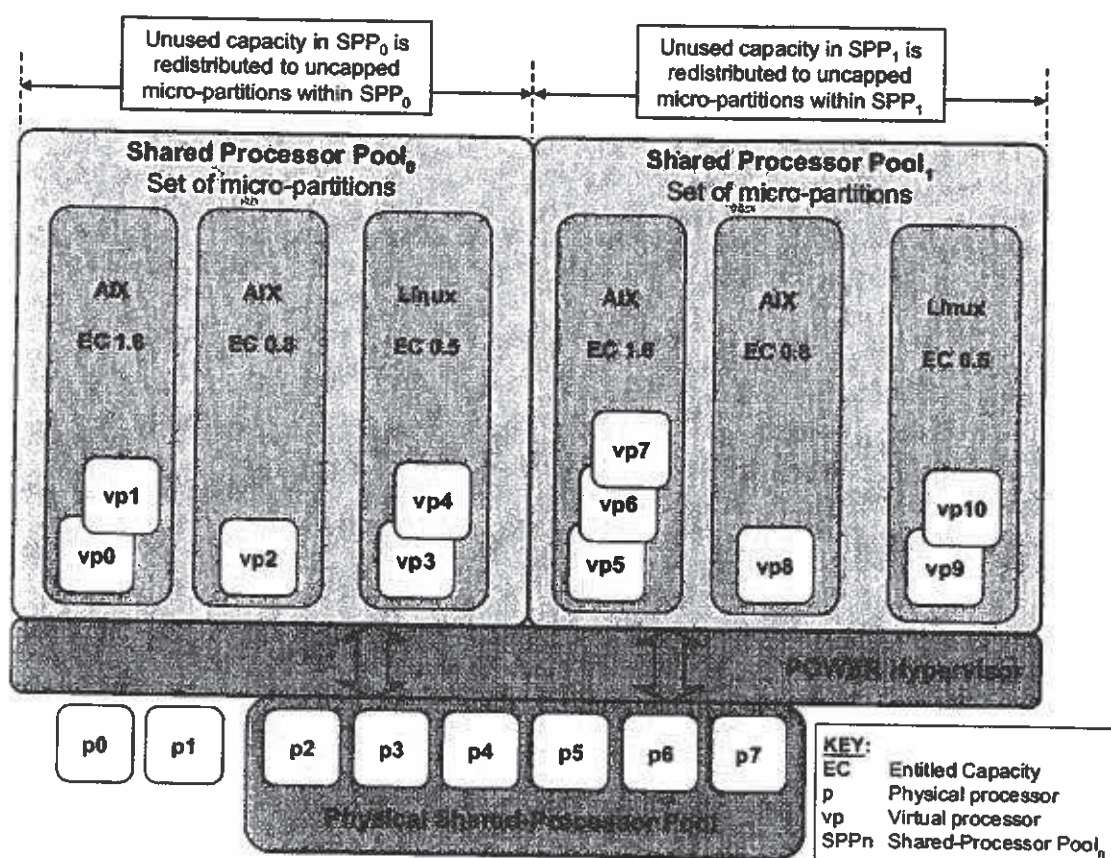
2.1.1.6. Подобряване на утилизацията

Основния проблем се корени в това, че обичайно тези резервни капацитети увеличават двойно цената на придобиване и експлоатация на оборудването, за това е от съществено значение да се осигури ефективното използване на скъп ресурс. Решението за входно-изходни операции са описани в по-горната точка, а за основните – памет и процесор IBM предоставя и други механизми.



Работата с Enterprise pools позволява незаети капацитет от един дял да бъде достъпен и от други, тъй че да бъде системата по-ефективна. Изолирането на отделните Pool е наложително заради:

- **Лицензиране** – Sub-capacity лицензирането позволява на банката да не лицензира цялата машина, а част от нея. Групирайки едни и същи приложения и бази данни в един Pool, с достатъчно резервно пространство им се предоставя гъвкавост на ресурса и ефективност по отношение цена
- **Смесване на типове операции** – Преливането на ресурс от batch заявки през нощта и към OLTP в работно време и обратно за различните системи, уплътнява ползването на ресурс и подобрява общата скорост на работа



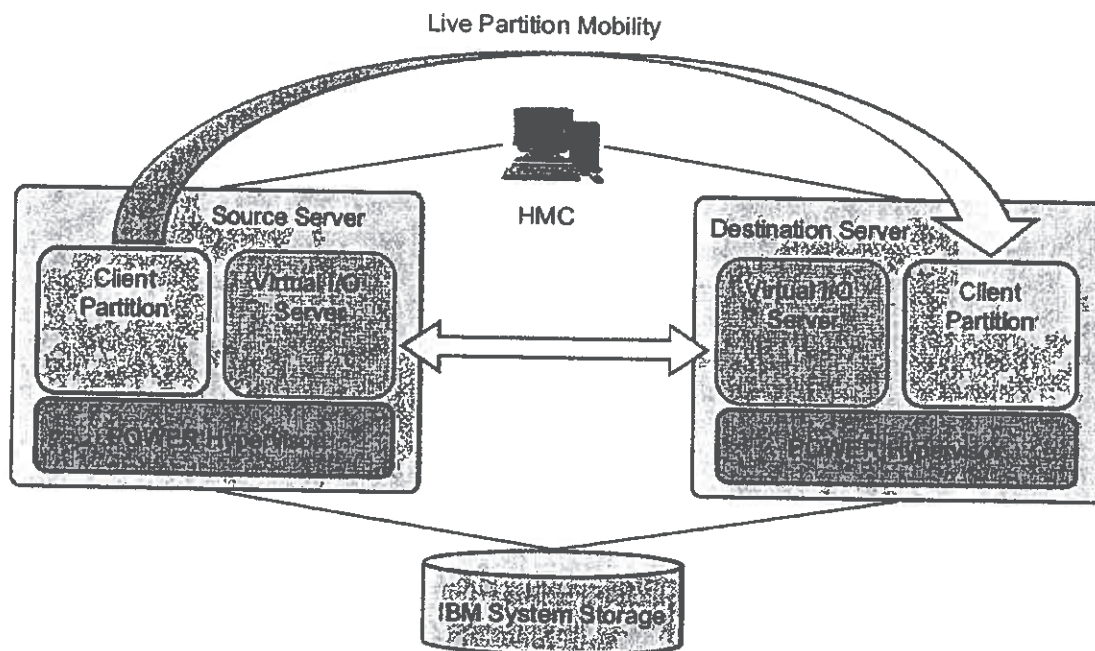
2.1.1.7. Стандартизация, automated provisioning

Стандартизирането на LPAR, и създаване на библиотека от "golden images" е първата стъпка към автоматизирането на инсталациите и в последствие облачните услуги. Следваща стъпка е автоматичното провизиране и освобождаване, това води до по-ефективна работа на

основните сървъри. Обичайно такива LPAR не са обвързани с конкретния хардуер и позволяват голяма гъвкавост при разпределение на натоварванията между отделните членове на пула.

2.1.1.8. Live Partition Mobility - LPM

След изпълнението на условия описани по-горе, свеждащи се то това – виртуалните машини LPAR да работят само през виртуални преместваеми интерфейси, приемащия сървър да има достатъчно капацитет, за да обслужи паметта, БНБ може да използва миграцията на работещи LPAR между машините



В резултат:

- Може да се освобождават планирано машини за извършване на спиране и др. за част или целия сървър;
- Може да се преместват LPAR, в зависимост от текущото натоварване без спиране на обслужването на клиенти;
- Може да се извършва HW upgrade или вкарване на нови сървъри, като те плавно се натоварват без да се налага спиране на процесите.;
- Основен елемент в Active-Active DC, където ще се постигне нормално използване и на двете групи хостове;
- В комбинация с клъстерния софтуер PowerHA дава автоматизация на резервирането на критични процеси;

2.1.1.9. Подготовка за стратегическите инициативи

Завършването на консолидирането на приложенията и тяхната виртуализацията е необходима стъпка за изпълнението на по-мощните стратегии по Active-Active DC и създаване на частен облак.

Управлението на виртуалните сървъри ще се комбинира с администрирането на ресурсите на мрежите и дисковите масиви, тъй че да се използва максимално наличния капацитет и да се осигури продължаване на работата при планирани спириания. Като се увеличи достъпността на услугата до 99.95% (около 4-5 часа годишно) на ниво виртуална машина за сървърите, елиминирайки времето за планиран downtime на сървърите.

2.1.1.10. Изключения

Трябва да се отбележи, че процеса не би трябвало да е самоцелен. Има системи, които работят по-изолирано, изискват специфично управление и хардуерна конфигурация или са логически самостоятелни. За тях препоръката е да се използват отделни сървъри, които да бъдат надеждни, производителни и с достатъчно възможности за разширяване. Приложенията работещи върху тях заемат сравнително скъп ресурси постоянно и може да не е ценово ефективно тези ресурси да бъдат заети от сървъри от висок клас.

Такива сървъри са:

- Management Servers - TPC, log и подобни. Софтуерните системи работещи върху тях трябва да бъдат независими от наблюдаваните и управлявани системи. При евентуални проблеми в основната среда, тези сървъри трябва да могат да укажат, къде и какво да се прави и информацията върху тях трябва да е достъпна независимо от състоянието на основните;
- Backup & Recovery Servers – за тях също важи условието, че трябва да бъдат отделени от основните машини. В случай, че има нужда от възстановяване на виртуална среда върху основните сървъри, няма да е необходимо да се възстановява и TSM и първа след това да се стартира възстановяване на средата, направо може да се започне възстановяването на виртуалната среда;
- Инсталационни сървъри NIM – те частично попадат в горните групи, но за тях е особено важно да са независими от средата;
- Изолирани среди – предполагаме, че независимо от възможностите за изолация виртуалните машини на PowerVM и PowerSC, някъде ще се наложи изграждане на изолирани среди, за повишаване на нивото на сигурността, географска изоланост и др. подобни, там би могло да се помисли за по-малки машини съобразени с конкретни изисквания.

Изолирането на сървъри може да става и заради

- По-високите изисквания за скорост и трафик през LAN и SAN – резервирането на LAN & SAN през VIOS сървъри изразходва и памет и CPU. Процесите по backup &



recovery са типични ползватели на този ресурс и не е целесъобразно TSM сървърите да изразходват продукционен ресурс през VIOS, когато тези машини могат директно да работят с високоскоростните SAN & LAN HBA по-ефективно. Резервирането на пътищата и системите става чрез клъстериране на самия TSM и вдвояването на адаптерите.

- Тестови и развойни среди – при внедряване на големи и нови системи няма натрупани данни, необходими за параметризирането на продукционните среди. Изолирането им върху други сървъри от класа на продукционните ще даде достатъчно данни, за това как да бъдат конфигурирани върху продукционни сървъри без това да изразходи техни ресурси или да повлияе върху продукционните среди. Допълнително може да бъдат отработвани сценарии, които са по-деструктивни – отпадане и възстановяване на сървъри или системи, без това да даде ефект върху основните.

2.1.1.11. Стъпки

СТЪПКА 1 – АКТУАЛИЗИРАНЕ НА ВИРТУАЛИЗАЦИЯТА, ТЕКУЩО СЪСТОЯНИЕ

В момента в банката приключва процес за консолидиране на операциите върху двете основни Power машини в основния сайт:

Managed System	Type Model	Serial	Tot Cores	Act Cores	Tot GB	Act GB
Server-9117-570-SN6566C4E	9117-570	6566C4E	16	8	64.00	48.00
Server-9117-MMA-SN0604214	9117-MMA	0604214	8	6	64.00	32.00
Server-9117-MMB-SN06B331P	9117-MMB	06B331P	36	20	320.00	192.00
Server-9117-MMB-SN06B332P	9117-MMB	06B332P	36	20	320.00	192.00

Работи се основната двойка сървъри 9117-MMB да бъдат готови за LPM, тъй като до скоро една от тях беше с 2 VIOS сървъра, а другата нямаше работещо втори VIOS и инсталираните LPAR бяха с една единствен път през VIOS.

Ресурса им е зает с текущите приложения и ако се налага да се прехвърли цялата работата от единия на другия няма да достигне паметта. Трябва да се направи анализ и да се пристъпи към увеличаване на паметта и отключване на процесорите.

9117-MMA и 9117-570 са с POWER6 процесор и обслужват SAP продукционната среда, която се прехвърля върху 9117-MMB машините и ще се освободи след това. Възможно е да бъдат прехвърлени върху отдалечения сайт и там да се реализира група сървъри с STDB-CC-8205-E6C-SN062718T и/или Server-9117-570-SN65ED6DA, които да посрещнат натоварването при изграждане на среда за разпределено обработка.

Това е в съзвучие със стратегията, че по-старите машини ще бъдат премествани върху текущия DR сайт, но неговата функция се променя на равноправен активен сайт. За това считаме, обаче че този клас сървъри трябва да бъде обновен преди това до POWER7/POWER8 за оптимално ползване на ресурсите, вградената виртуализация и др.

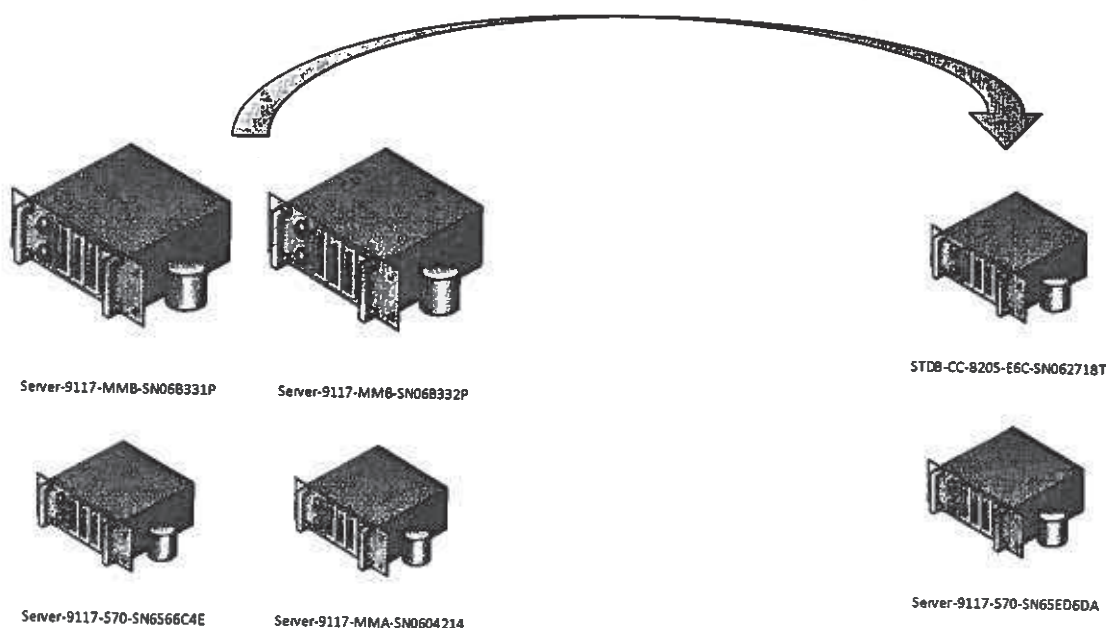


В резервния сайт сървърите се ползват за тестове и обучение, а в случай на нужда критичните приложения трябва да могат да се стартират върху тях. Производителността на сървърите е между 20-25% от тази на основния. При тях обаче не е извършвана реконфигурация за да може да бъдат виртуализирани техните ресурси.

Managed System	Type Model	Serial	Tot Cores	Act Cores	Tot GB	Act GB
RTGS_back-8203-E4A-SN06124D6	8203-E4A	06124D6	1	1	8.00	8.00
STDB-CC-8205-E6C-SN062718T	8205-E6C	062718T	6	6	64.00	64.00
Server-9117-570-SN65ED6DA	9117-570	65ED6DA	8	8	32.00	32.00
RTGS_back-8203-E4A-SN06124D6	8203-E4A	06124D6	1	1	8.00	8.00

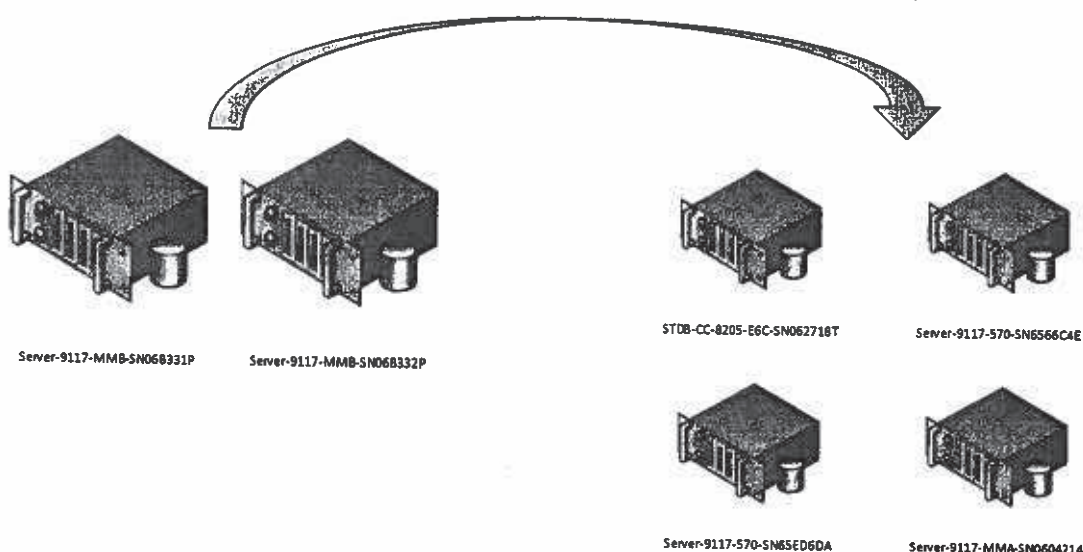
СТЪПКА 2 – ОБНОВЯВАНЕ

Основните сървъри 9117-MMB (Server-9117-MMB-SN06B331P и Server-9117-MMB-SN06B332P) са със зает капацитет. За реализиране на гъвкава среда, където едната машина може да поеме работата и на двете дори и при намаляване на производителността, поне паметта на приемащата машина трябва да има свободна част толкова, колкото заемат процесите на „източника“. Машините са от предишното поколение POWER7 процесори и би било добре да се обновят до по-новите POWER8



В основния сайт 9117-MMA и 9117-570 са с POWER6 процесор и обслужват SAP продукционната среда, която в момента се прехвърля върху 9117-MMB машините и ще се освободи след това. Възможно е да бъдат преместени върху „Касов център“ и там да се

реализира група сървъри с STDB-CC-8205-E6C-SN062718T и/или Server-9117-570-SN65ED6DA, които да посрещнат натоварването при изграждане на среда за разпределено обработка.



Това е в съзвучие в стратегията, че по-старите машини ще бъдат премествани върху текущия DR сайт, но неговата функция се променя на равноправен активен сайт. За това считаме, че този клас сървъри трябва да бъде обновен преди това до POWER7/POWER8 за оптимално ползване на ресурсите, вградената виртуализация и др.

Както в основния така и в отдалечения сайт има машини, които остават да бъдат дискретни като част от тях са сравнително стари - 9110-51A и 9111-520 според нас трябва да бъдат изведени от експлоатация и поддръжка.

По-новите машини са предвидени и работят за TSM и TPC приложенията и са с достатъчен капацитет и производителност за момента.

DC Централно управление

Managed System	Type Model	Serial	Tot Cores	Act Cores	Tot GB	Act GB
TPC-8205-E6C-SN062E81T	8205-E6C	062E81T	4	4	32.00	32.00
tsmprod1-8231-E1C-SN0682E1R	8231-E1C	0682E1R	4	4	32.00	32.00
tsmprod2-8231-E1C-SN0682EFR	8231-E1C	0682EFR	4	4	32.00	32.00

DC Касов център

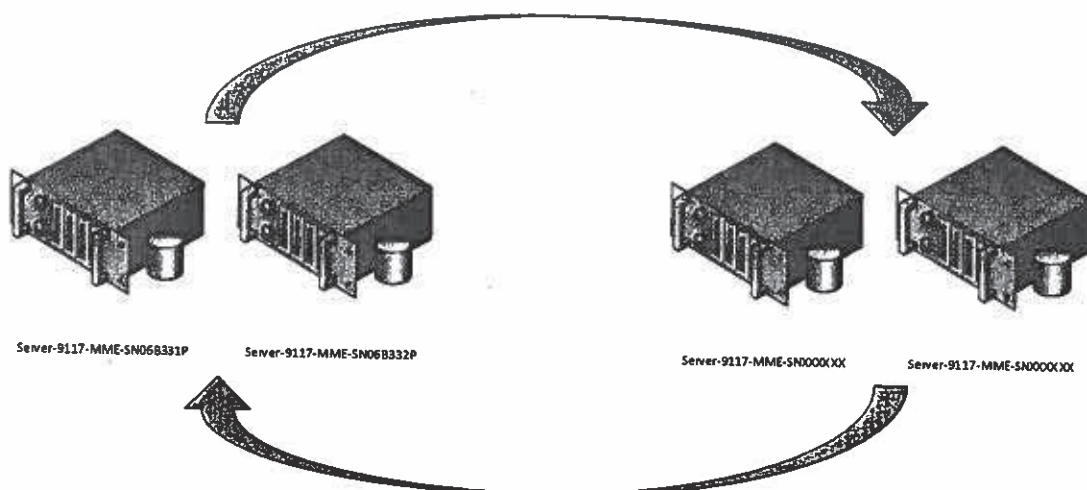
Managed System	Type Model	Serial	Tot Cores	Act Cores	Tot GB	Act GB
STDB-CC-8205-E6C-SN062718T	8205-E6C	062718T	6	6	64.00	64.00
Server-8231-E1C-SN0682E0R	8231-E1C	0682E0R	4	4	32.00	32.00

При готовност от страна на банката бихме могли да извършим процеса описан по горе в рамките на 2 календарни месеца.

Срока не отчита времето необходимо за реорганизация на работата.

СТЪПКА 3 - КРАЙНО СЪСТОЯНИЕ

Реализирането на Active-Active DC, заедно с нуждата от по-добро разпределение на изчислителните ресурси води до архитектура, в която в Централно управление имаме поне една двойка еднакви сървъри дублирани с една двойка в Касов център.



Може да се избере подхода, една от машините 9117-MMB да бъде прехвърлена в Касов Център и около нея да бъде създадена новата активна среда. За целта трябва да бъдат изпълнени следните предпоставки:

- Да бъде изградена мрежовата инфраструктура и преконфигурирани мрежовите сегменти, тъй че двата сайта да се „виждат“ идентично
- виртуалната среда на дисковите масиви да бъде изградена да представя по еднакъв начин капацитета на масивите и на двата сайта

Това изисква допълнителни дейности и време за осъществяването им и за това считаме за по-реалистичен, подхода при който се подготвят дискови масиви и мрежи за Active-Active DC и след това се развива втората двойка сървъри.

Капацитета необходим в разпределена среда, се комбинира с натоварването на всяка една от тях на ниво сайт, изисква във всички машини да има поне 50% резервиран капацитет, заедно с обичайното нарастване на необходимата изчислителна среда. Така се получават конфигурации близки до долните:

Основен център за данни София- ЦУ Батенберг

- два IBM POWER8 E870 сървъра всеки, всеки от които:
 - 28/40 (active/total) P8 cores
 - 512/1024 GB RAM

- 2 x Ethernet controller each 2 x 10 GE FCOE + 2 x 1 GE
- 4 x Quad Port 8 Gb Fiber Channel adapter
- PowerVM Ent. AIX 7.1 Ent
- Hardware Management console

Основен център за данни София- Касов Център

- два IBM POWER8 E870 сървъра всеки, всеки от които:
 - 28/40 (active/total) P8 cores
 - 512/1024 GB RAM
 - 2 x Ethernet controller each 2 x 10 GE FCOE + 2 x 1 GE
 - 4 x Quad Port 8 Gb Fiber Channel adapter
 - PowerVM Ent. AIX 7.1 Ent
- Hardware Management console

Предложените сървъри са от последното поколение Power Enterprise , позволяват да се увеличат отключените ядра до 40 и да се увеличи паметта близо двойно. При закупуване и на втори модул на E870 ще може да се удвои капацитета.

В Active-Active DC сценария, LPAR ще могат да бъдат мигрирани между двата сайта без това да се отразява на работата на клиентите с тях. Данните разположени върху дисковите масиви също трябва да могат да бъдат равноправно достъпвани от двата сайта, този механизъм се реализира от HyperSwarp функцията на DS8000. HyperSwarp синхронизира постоянно данните между двата основни дискови масиви и предоставя единна виртуална среда на дялове от двата масива и осигурява, че всяка машина ще работи с локалното си копие. При преместване на LPAR в отдалечения DC, новия дисков масив започва да работи с новата виртуална машина, обръщайки репликацията, така че първоначалния сторидж да не „изостава“.

Допълнителните сървъри обслужващи Power средата също ще се развиват и ще поемат нови функции. За наблюдение и управление на Power Servers преминават към PowerVC, PowerVP софтуерните пакети. Те се нуждаят от надеждна среда и достатъчно ресурс. TSM ще увеличава своето натоварване и включени функции, предлагаме една конфигурация, която може да замени текущите Power710 и 740 при необходимост:

- Един IBM POWER8 S822 сървър:
 - 16 активирани P8 ядра
 - 128 GB RAM
 - 2 x Ethernet controller each 2 x 10 GE FCOE + 2 x 1 GE
 - 2 x Dual Port 8 Gb Fiber Channel adapter
 - PowerVM Ent. AIX 7.1 Ent

Характерното за конфигурацията, че тя ще разчита отново на работа през VIOS независимо от завишените изисквания за IO респективно VIOS, но ще може да включи във себе си повече работещи приложения и няма да се различава съществено от основните E870 сървъри по отношение на входно-изходната конфигурация. Съществено за стандартизирането на дефинициите на виртуални машини, автоматизиране на deployment и подготовката за преминаване към облачни услуги.

При готовност от страна на банката бихме могли да извършим процеса описан по горе в рамките на 3 календарни месеца.

2.1.2. x86 виртуализация

Сървърната виртуализация и конкретно x86 виртуализацията е технология, чието създаване и бърз темп на развитие е в следствие на бума на микропроцесорните технологии, изчислителните ресурси и необходимостта за преодоляване на някои ограничения, наложени от използването на чисто физическа инфраструктура. Използвайки технологии за сървърна виртуализация IT инфраструктурите, постигат много по-високо консолидиране на услуги върху единица физически ресурс (15:1 и нагоре), което от своя страна води до драстично намаляване на разходите за хардуер, охлаждане и електричество. Допълнително виртуализацията осигурява логически слой, който поради изцяло софтуерната си натура позволява динамично и бързо конфигуриране на всеки един компонент – дискови устройства, мрежови устройства, процесори, памет и т.н.

2.1.2.1. Концепция за развитие

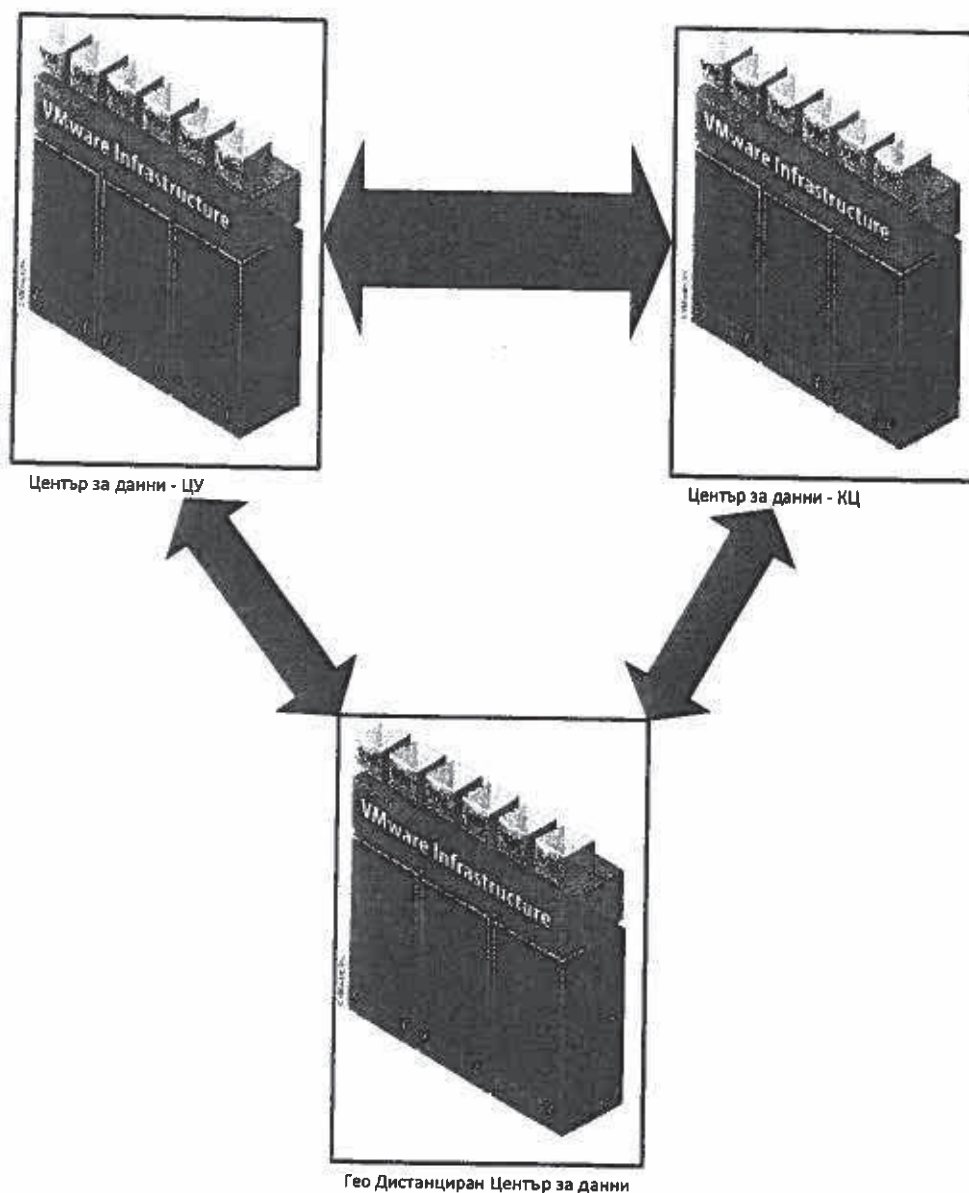
Целта на настоящата глава е да представи реалистична концепция и стратегия за развитието на решенията за x86 виртуализация в Българска Народна Банка. Крайната цел на стратегията/концепцията е, когато тя е изпълнена да съществува единна платформа за виртуализация на x86 сървъри, даваща централизирано управление, дълбока видимост на процесите случващи се вътре и адекватни методи и политики за наблюдение и самоуправление на платформата. За базова позиция се приема текущото състояние на платформата за виртуализация, която има следните недостатъци:

- Базирана е само в основния център за данни на банката – услугите не могат да мигрират свободно и автоматично между центровете за данни;
- Липсва адекватен начин за наблюдение и известяване при наличието на проблеми;
- Резервираността на центъра за данни се осъществява ръчно – при проблем виртуалните машини се стартират ръчно в резервния център за данни;
- Данните върху дисковите масиви се репликират, но отново при отпадане на основния център за данни е необходима ръчна намеса, за стартирането им в отдалечения център за данни;
- Липсва гео-дистанциран център за данни, който да се използва в случай на големи природни бедствия и аварии, които могат да засегнат метро района, в който в момента са ситуирани основния и резервния център за данни.

Крайния резултат от успешното изпълнение на стратегията за развитие на решенията за виртуализация, трябва да предоставя единна платформа за виртуализация, при която няма значение в кой център за данни работят услугите. Платформата трябва да работи напълно автономно, като сама се грижи за разпределението на ресурсите и автоматичното им стартиране в другия център за данни в случай на отпадане на хардуерен компонент от решението или на целия център за данни в следствие на природно бедствие или авария.



Платформата трябва да предоставя възможност най-критичните услуги да работят едновременно в двете локации, като по този начин при отпадане на хардуерен компонент, няма да има никакво прекъсване на услугата. Също така трябва да се извършва репликация на данните в отдалечен център за данни, като по този начин, се осигурява възможност за възстановяване на услугите в случай на природно бедствие или авария от Метро мащаб. Логически платформата трябва да изглежда по следния начин:



След успешно реализиране на стратегията, ще съществуват 3 центъра за данни, като два от тях – този в ЦУ и този в КЦ, ще работят в режим Active-Active, а отдалечения център за

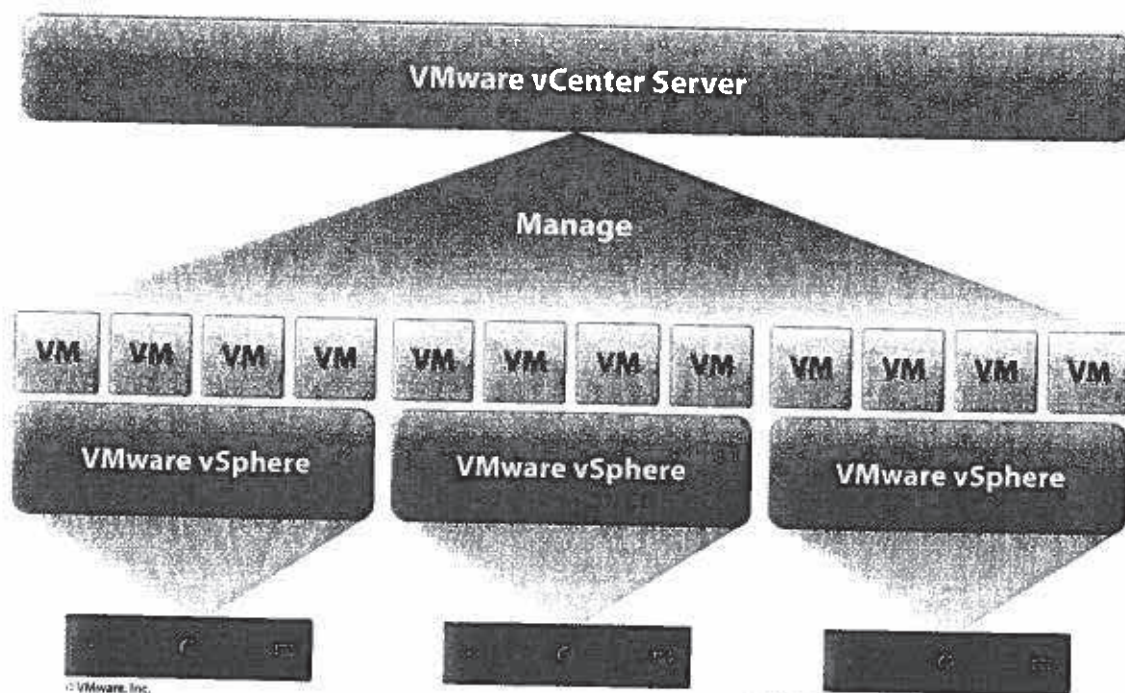


данни, ще работи в режим Stand-By спрямо останалите два центъра за данни. При невъзможност за работа на двата активни центъра за данни, услугите ще се стартират в Stand-By центъра за данни. При нормална работа услугите и приложенията, ще се преместват свободно между ЦУ и КЦ, за да се балансира натоварването на всеки един от центровете. В случай на необходимост за спиране на някой от центровете за данни – било то за профилактика или за отстраняване на проблем, услугите автоматично ще се мигрират в другия център за данни. При аварийно отпадане на компонент от инфраструктурата, автоматизация и предефинирани политики, автоматично ще преместят отпадналия виртуален ресурс върху работещи компоненти, без необходимост от човешка намеса. В същото време данните ще се репликират асинхронно в резервния център за данни. В случай на събитие, предизвикващо невъзможност услугите да работят в активните центрове за данни, най-критичните услуги, ще се стартират в резервния (Stand-By) център за данни.

2.1.2.2. Основни компоненти и инструменти на решение за сървърна виртуализация

За реализацията на крайната цел трябва да бъдат използвани добре познати и наложили се технологии, които ще гарантират безпроблемната работа на платформата. В този ред на мисли БНБ вече е избрало виртуализираща платформа базирана на VMWare. VMWare е един от водещите производители на подобни решение и изборът му е изцяло оправдан и правилен.

VMware – vSphere платформата се е наложила, като най-доброто решение за сървърна виртуализация базирана на x86 архитектура. На пазара е от повече от 10 години има над 50% пазарен дял в решенията за сървърна виртуализация. Логически основните компоненти изглеждат по следния начин:

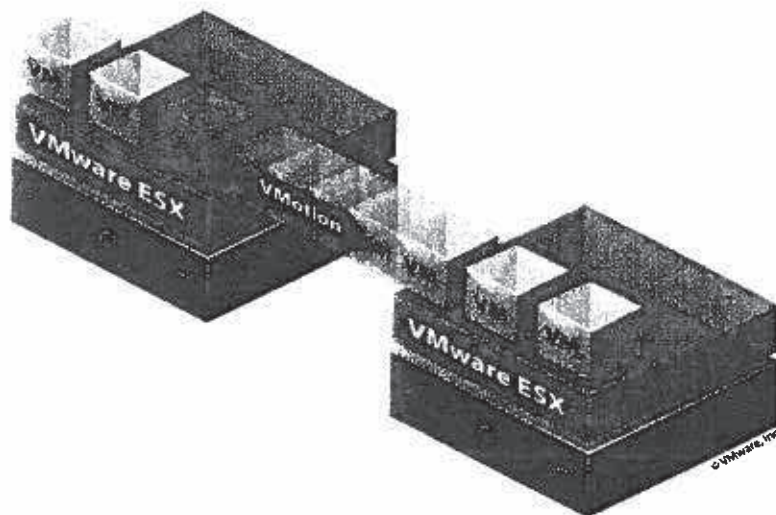


Физически сървъри – Физически сървъри са основния компонент в платформата за виртуализация. Те осигуряват изчислителния ресурс необходим на приложенията и операционните системи работещи в виртуализираната среда. За целта могат да бъдат използвани сървъри IBM с продуктов номер 5463L2G (примерна конфигурация 1) от настоящото рамково споразумение.

VMware vSphere е хипервайзор – софтуер с много малък дисков отпечатък, който се инсталира директно върху физически сървъри и осигурява виртуалния слой, в който се инсталират виртуализираните услуги/сървъри.

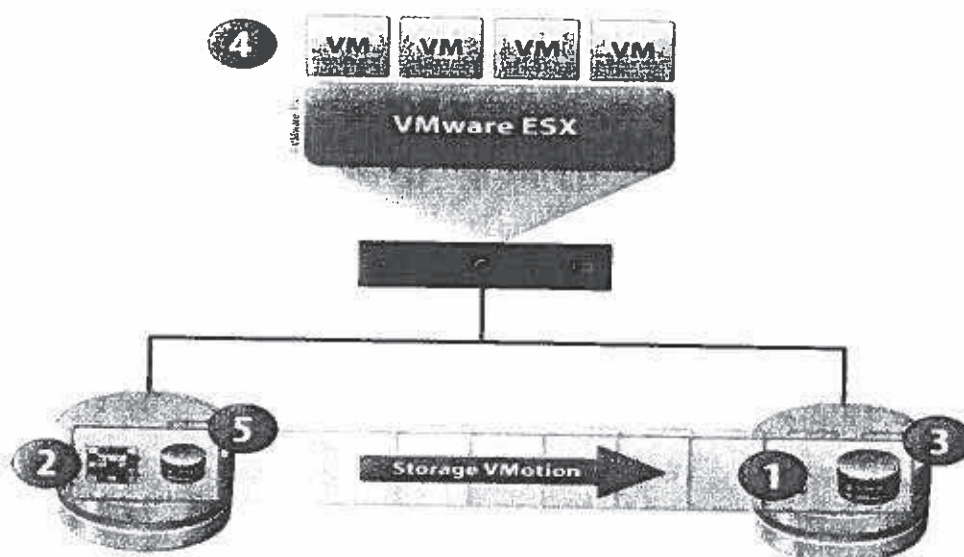
VMware vCenter Server е софтуерно приложение, което се инсталира във виртуализационна среда и осигурява надеждно и лесно конфигуриране и наблюдение на платформата за виртуализация. То комуникира през Layer 3 свързаност, директно с хипервайзорите и се използва за конфигурация на всички параметри по тях – мрежови настройки, виртуални комутатори, виртуални дискове, виртуални процесори и т.н.

VMotion е търговското наименование на технологията използвана в продуктите на VMware, която осигурява преместване на работеща услуга от един физически сървър (хипервайзор) на друг, без това да налага прекъсване на работата на услугите. Тази технология е основата на мобилността на приложенията и услугите между отделните активни изчислителни ресурси (хипервайзори). Без нея всяко преместване на активна услуга или приложение би било невъзможно без рестартиране на процесите и прекъсване на работата. Процеса отнема много малко време, като продължителността му зависи от скоростта на мрежовата свързаност на хипервайзорите и количеството оперативна памет използвана от преместваното приложение. Например, ако приложението има заделени 16 гигабайта оперативна и свързаността между сървърите е 10Gbit/s, времето необходимо за преместването, ще е под 25 секунди. През това време достъпа до работещите услуги, ще бъде прекъснат еднократно за по-малко от 250 милисекунди.

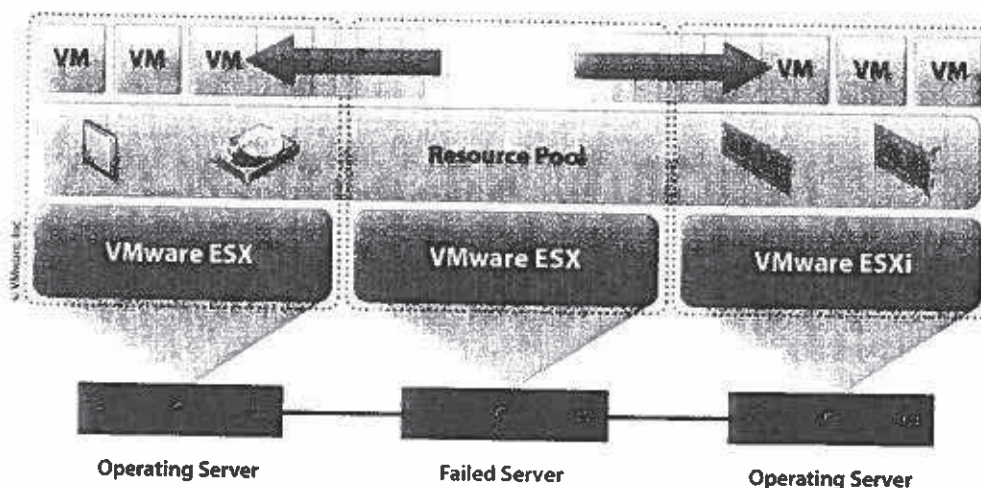


Storage VMotion е търговското наименование на технологията използвана в продуктите на VMware, която осигурява преместване на работеща услуга от един дисков масив или

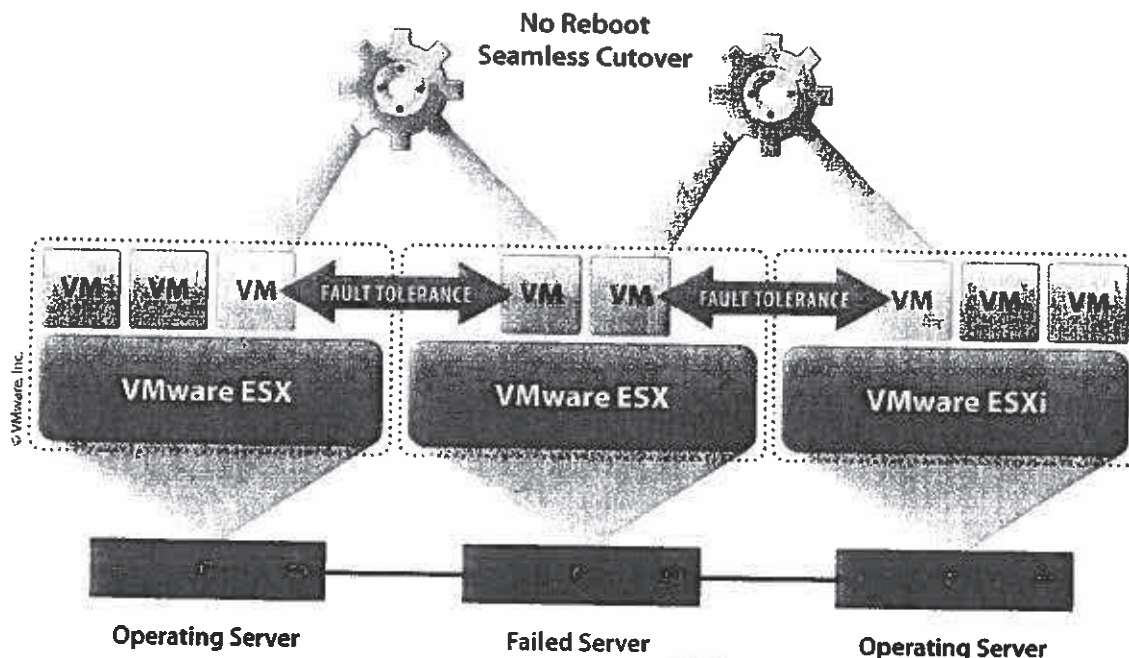
логически дял на друг без това да налага прекъсване на работата на услугите. Времето необходимо за преместването, зависи директно от производителността на дисковия масив, обема на виртуалната машина и скоростта на SAN мрежата. Например, ако имаме дисков масив с производителност при последователно четене на данните 800MB/c, скорост на SAN мрежата 16Gbit/s и обем на виртуалната машина 500 гигабайта – времето за миграция ще бъде приблизително 10 минути. През това време достъпа до работещите услуги, ще бъде прекъснат еднократно за по-малко от 250 милисекунди.



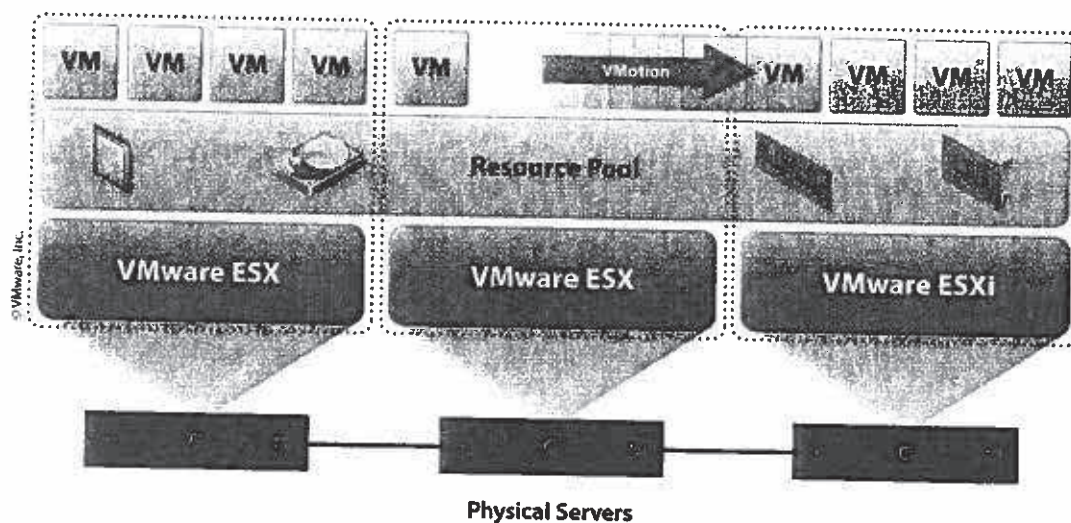
HA (High Availability) е търговското наименование на технологията използвана в продуктите на VMware, която осигурява рестартиране на услугите работещи върху отпаднал физически сървър (хипервайзор). Тази технология е в основата на резервирането на приложения и услуги от не-планирано отпадане на изчислителни ресурси. Процеса отнема толкова време, колкото е необходимо на операционната система и приложенията (услугите), да стартират. Процеса се контролира от самите хипервайзори, когато са сформирали HA клъстер и не е необходима интервенция от страна на системен администратор. Технологията използва мрежовата и SAN свързаността на физическите сървъри, за да наблюдава за отпадане на някой от тях. Ако се установи отпадане, услугите се стартират на друг сървър.



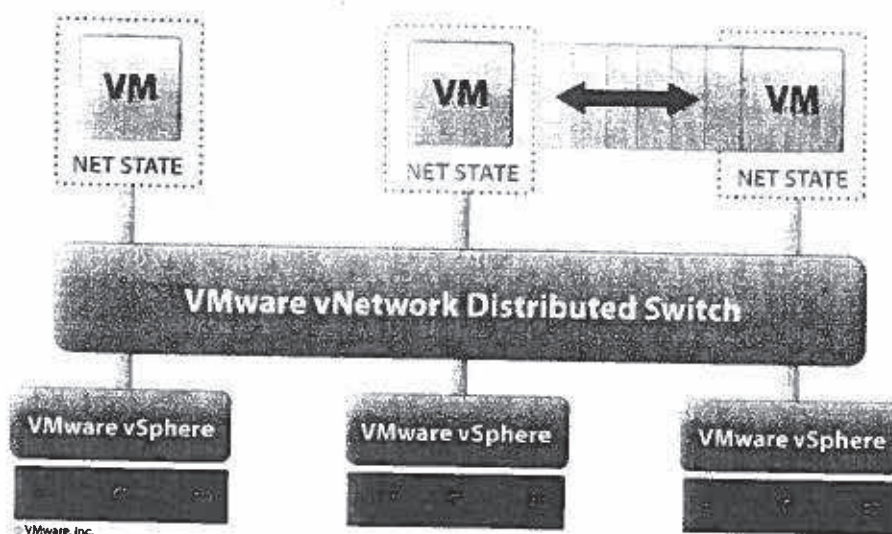
FT (Fault Tolerance) е търговското наименование на технологията използвана в продуктите на VMware, осигуряваща непрекъсваемост на критичните услуги в случай на отпадане на някой от хипервайзорите, върху които работят. Технологията стартира услугите едновременно върху два хипервайзора и се грижи за синхронизацията между тях, като репликира всички команди изпълнени от едната виртуална услуга (процесорни цикли, дискови операции и др. входно-изходни операции) върху другата. FT следи постоянно състоянието на основната услуга и сървъра, върху която тя работи. Ако се установи отпадане на сървъра или услугата, мигновено (в рамките на 150 милисекунди) втората (репликираната) услуга се активира и поема всички заявки първоначално обслужвани от вече отпадналата услуга. Този процес е напълно прозрачен за потребителя и от негова гледна точка, нищо не се е случило.



DRS (Distributed Resource Scheduler) е търговското наименование на технологията използвана в продуктите на VMware, която се грижи за равномерното разпределение на натоварването върху хипервайзорите. За реализацията и се следи натоварването на всеки един сървър (хипервайзор) и ако се забележи сериозна разлика в натоварването между тях се предприемат действия, за балансирането им. Използва се вече познатата технология VMotion, като се взема в предвид използвания от приложенията/услугите ресурс и се пресмята, как да бъдат преразпределени върху физическите сървъри, така че натоварването да бъде максимално балансирано. Процеса може да се конфигурира в детайли, като обект на конфигурация е при каква разлика в натоварването да се изпълнява балансиране, как да се изпълнява (автоматично или ръчно) и др.

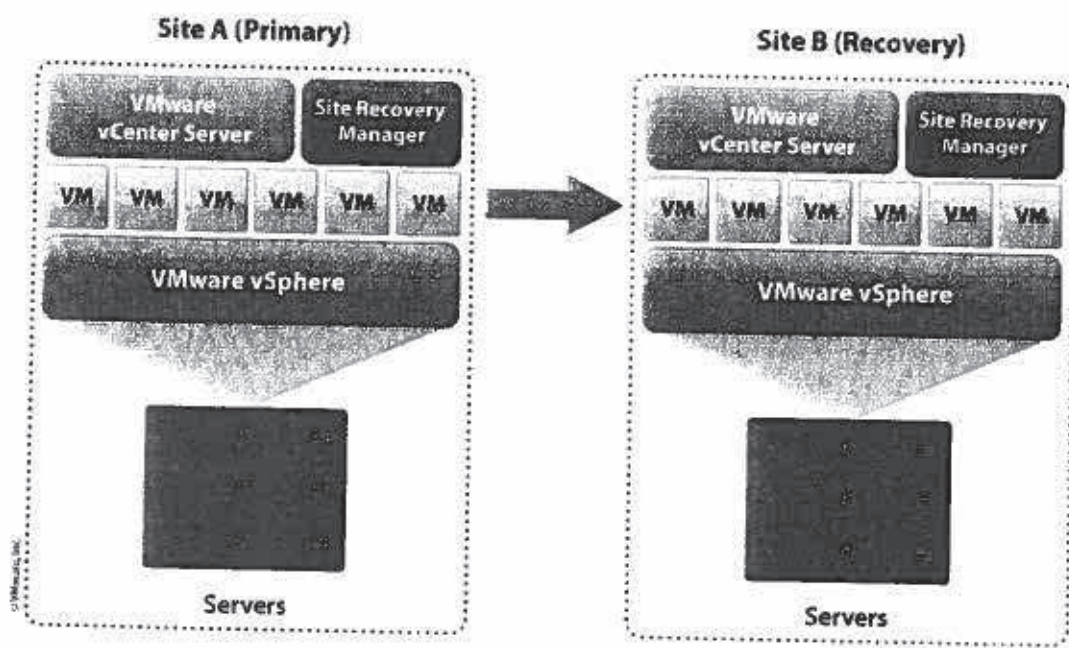


DVS (Distributed Virtual Switch) е търговското наименование на технологията използвана в продуктите на VMware, която осигурява единен виртуален комутатор във виртуализираната платформа. Това е необходимо, за да се осигури уеднаквяване на мрежовите компоненти в цялата среда. По този начин се избягват нежелани разлики в конфигурацията – например виртуална мрежа „X“ на единия хипервайзор е поставена във VLAN10, а на друг във VLAN11. Тази конфигурация е валидна, но ако преместим услуга, която използва виртуална мрежа „X“ от единия хипервайзор на другия, услугата ще загуби мрежова свързаност. DVS позволява такива грешки да бъдат избегнати, използвайки единна мрежова конфигурация във рамките на виртуалния клъстер. В същото време се грижи за синхронизацията на конфигурациите на виртуалните комутатори и напълно премахва възможността, за подобен вид грешки. В допълнение, дава възможност за налагане на политики, върху виртуалните мрежови портове на услугите и се грижи, тези политики да се преместват заедно с услугите, когато те сменят хипервайзора в следствие на VMotion, HA, FT или DRS събитие.



Storage Virtualization е технологията, която ще бъде използвана за предоставяне на едни и същи дискови ресурси едновременно в двата центъра за данни. Технологията предоставя възможност за логическо управление на ресурси, които не принадлежат на един физически контейнер (дисков масив). Виртуализацията на блоково ниво се постига благодарение на продукта на IBM - SAN Volume Controller (SVC), обект на настоящото рамково споразумение. Технологията е детайлно описана в точка 4.2. от настоящия документ. Важно е да се отбележи, че за работата на VMware клъстера в Active-Active режим, виртуализацията на дисковия масив е задължителна.

SRM (Site Recovery Manager) е търговското наименование на технологията използвана в продуктите на VMware, която осигурява възможност за планирано и в съответствие с политиките за възстановяване от природни бедствия и аварии, стартиране на всички компоненти на виртуалната платформа в отдалечен център за данни. Технологията използва наличните технологии, за да копира данните, като запазва конфигурацията и структура на отделните приложения и услуги, в отдалечен център за данни. В случай на необходимост от стартиране на услугите в отдалечения център за данни, всички останали работещи услуги на първичния център за данни се спират и се стартират отново в отдалечения център за данни. Това става по предварително създадени и описани политики и правила. В случай на необходимост операцията е обратима. Основния плюс на такова решение е възможността с натискането на един клавиш, всички услуги да бъдат прехвърлени в отдалечената локация, без необходимост от допълнителна човешка намеса.



2.1.2.3. Стъпки на имплементация

Етапите на изпълнение зависят пряко от готовността на инфраструктурните компоненти, приложенията и услугите използвани в ИТ инфраструктурата на банката. Към този момент готовността на инфраструктура е непълна и това налага предприемане на стъпки, за постигане на пълна готовност, всяка от които е описана в настоящия документ. Стъпките включват привеждане в готовност на няколко отделни компонента – мрежова инфраструктура (точка 3.1), SAN инфраструктура (точка 3.1), дискови масиви (точка 4.2), платформа за виртуализация (настоящата точка), приложения и услуги. В тази точка детайлно са засегнати само етапите свързани пряко с платформата за виртуализация. Останалите етапи от стратегията, са засегнати в текущия документ, но в други точки.

Долу изброените детайлни дейности не са с посочена индикативна продължителност защото зависят от много фактори, включително и наличието на време от страна на служителите на банката. Въпреки това спрямо опитана ни смятаме, че посочения период за цялата стъпка е реалистичен и изпълним.

СТЪПКА 1 – МЕЖДУИННО РЕЗЕРВИРАНЕ С FAULT TOLERANCE КОНФИГУРАЦИЯ

Към настоящия момент виртуализационната платформа е реализирана напълно само в Централно Управление и не предоставя възможности за резервиране на приложенията и услугите в случай на природно бедствие или авария засягащо района на Централно Управление. Възможно е да се използва Fault Tolerance функционалността налична във версия 6 на VMWare VSphere, при която синхронно между машините се репликира не само входно/изходните операции свързани с оперативната памет, а и тези свързани с дисковия



масив. Това ще позволи практически мигновено прехвърляне на дадена машина от единия сайт на другия.

За да бъде имплементирана Active-Active концепцията е необходимо да се изгради виртуализационен слой върху дисковите масиви. Преди това да се случи Active-Active концепцията не може да бъде имплементирана нормално. Тази стъпка е междинна, трябва да се случи след имплементирането на стъпка 1 описана в точка 3.1.5 и трябва да е временна.

- Изготвяне на архитектура на решението.
- Обновяване на наличната документация отнасяща се за x86 виртуализационната платформа.
- Обновяване на VMWare инфраструктурата до версия 6.0
- Пре-конфигуриране на VMware vSphere и vCenter Server за управление и конфигуриране на изчислителния ресурс.
- Конфигуриране на виртуалните комутатори и мрежи обезпечаващи безпрепятствена работа на услуги и приложения в двата центъра за данни.
- Тестване на функционалността с пилотна от виртуална машина.
- Конфигуриране на всички или избрана част от машините на въпросната функционалност.

При готовност от страна на банката бихме могли да извършим процеса описан по горе в рамките на **1 календарни месеца**.

Предимствата за банката ще са:

- Висока резервираност на част или всички x86 базирани виртуални машини

Допълнително или като заместител на Fault Tolerance решението, може да се използва Site Recovery Manager решение, за което обаче са необходими допълнителни лицензии. То ще позволи семи-автоматизирано или лесно ръчно включване на всички машини при отпадане на достъпа до основния storage, SRM решението ще използва репликираните копия, за машините, които са налични. Не развиваме детайлно този вариант, защото смятаме, че е по-удачно да се фокусираат средства и усилия за виртуализация на дисковия масив и преминаване към Стъпка 2.

Тази стъпка е пряко зависима от:

- Стъпка 1 – Съобразяване на дизайна в основните изчислителни центрове с най-добрите практики и преминаване към едновременно работна / **Мрежа**
- Стъпка 2 – Изграждане на инфраструктура за работа на два сайта за приложенията, които се достъпват от външни за банката потребители и са разположени в Интернет периметъра / **Мрежа**
- Стъпка 1 - Изграждане на дискова инфраструктура в първия център за данни / **дискови масиви / опционално**



Тази стъпка е косвено зависима от:

- Стъпка 1 – Оптимизиране на виртуалната инфраструктура. / **x86 сървъри**

СТЪПКА 2 – ПРЕМИНАВАНЕ КЪМ ПЪЛНА ACTIVE-ACTIVE КОНФИГУРАЦИЯ

Стъпките необходими за привеждане на платформата в готовност са следните:

- Изготвяне на архитектура на решението.
- Обновяване на наличната документация отнасяща се за x86 виртуализационната платформа.
- Физическо инсталиране на еднакъв брой сървъри във всеки един от центровете за данни, така оразмерени, че всеки един от центровете да може да поеме напълно натоварването на всички останали.
- Пре-конфигуриране на VMware vSphere и vCenter Server за управление и конфигуриране на изчислителния ресурс.
- Конфигуриране на дисковите ресурси, така че да се „виждат“ по един и същи начин от двата центъра за данни и от всички хипервайзори участващи в метро клъстера.
- Конфигуриране на Метро клъстер между центъра за данни Централно Управление и Касов Център. Трябва да бъдат използвани следните технологии гарантиращи непрекъсваемост, резервираност, мобилност на приложенията и балансиране на натоварването между двата центъра за данни: FT, HA, VMotion, DRS.
- Конфигуриране на виртуалните комутатори и мрежи обезпечаващи безпрепятствена работа на услуги и приложения в двата центъра за данни.
- Тестване на функционалността с пилотна група от виртуални машини.
- Имплементиране на функционалността за всички виртуални машини в клъстера.
- Конфигуриране на софтуер за наблюдение на средата за виртуализация vCenter Operations Manager.

При готовност от страна на банката бихме могли да извършим процеса по подготовка на платформата за виртуализация в рамките на **2 календарни месеца**.

Предимствата за банката ще са:

- 100% резервираност на x86 базираните виртуални машини;
- Автоматично разпределение на натоварването;
- Автоматично прехвърляне при проблем в някой от сайтовете;
- Възможност на всеки сайт да поеме изцяло натоварването на другия;
- Лесно управление и troubleshooting.

Тази стъпка е пряко зависима от:

- Стъпка 2 - Изграждане на Active-Active центрове за данни. / **x86 сървъри**
- Стъпка 1 - Изграждане на дискова инфраструктура в първия център за данни / **дискови масиви**

- Стъпка 2 - Изграждане на Stretched Cluster – Active-Active Datacenter.

Тази стъпка е косвено зависима от:

- Стъпка 3 - Оптимизиране на Active-Active центрове за данни. / **x86 сървъри**

СТЪПКА 3 – РАЗШИРЕНИЕ КЪМ ТРЕТИ ЦЕНТЪР

След изграждането на трети резервен отдалечен център за данни, решението за виртуализация трябва да бъде надградено с SRM функционалност.

Дейностите, които трябва да бъдат извършени са:

- Изготвяне на архитектура на решението.
- Обновяване на наличната документация отнасяща се за x86 виртуализационната платформа.
- Конфигуриране на репликация през SRM (Site Recovery Manager) между център за данни Централно Управление и резервния отдалечен център за данни.
- Конфигуриране на репликация през SRM между център за данни Касов Център и резервния отдалечен център за данни.
- Извършване на тестове.

При готовност от страна на банката бихме могли да извършим процеса по подготовка на платформата за виртуализация в рамките на **1 календарни месеца**.

Предимствата за банката ще са:

- Възможност за стартиране на 30% от ресурсите в отдалечения сайт при отпадане и на двата сайта;
- Лесно управление и възстановяване на инфраструктурата в първоначалния и вид;

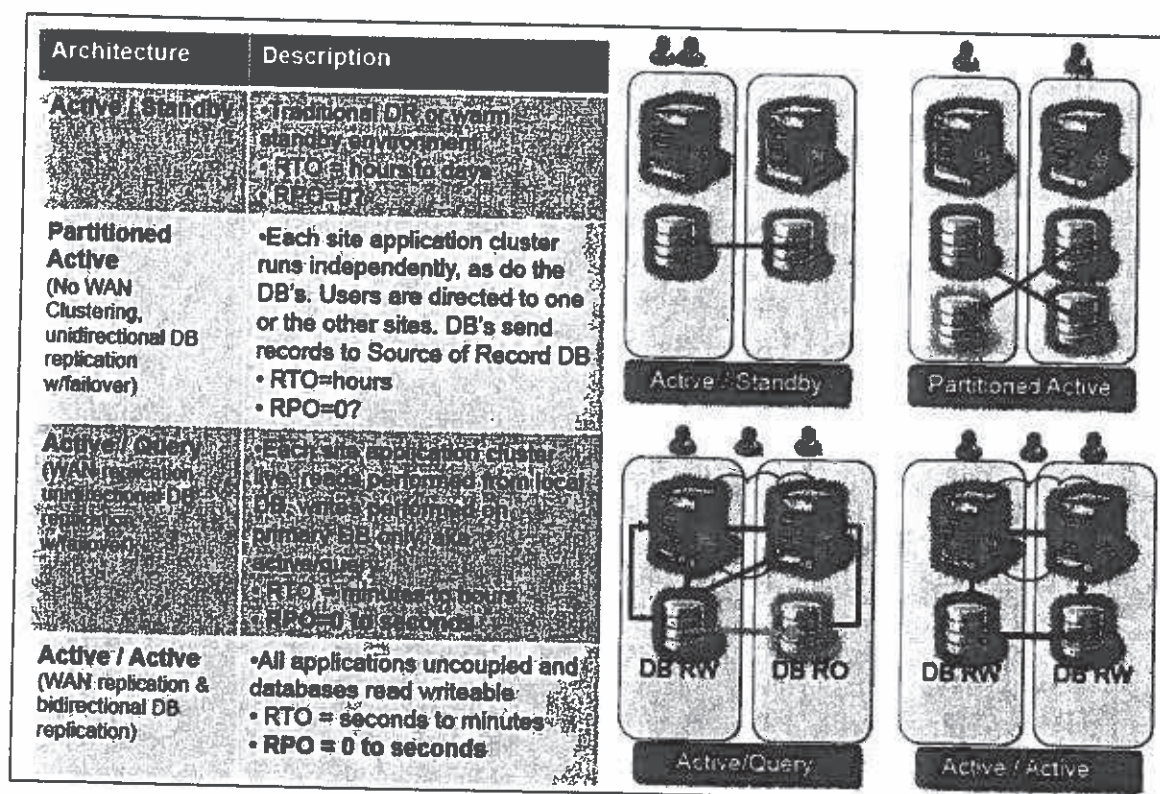
Тази стъпка е пряко зависима от:

- ИзСтъпка 3 – Изграждане на комуникационна инфраструктура за нуждите на Центъра за възстановяване след инциденти / **Мрежи**
- Стъпка 4 – изграждане на център за възстановяване при инциденти. / **x86 сървъри**
- Стъпка 3 - Защита на данните в DRC / **дискови масиви**

2.2. Active-Active Datacenter

2.2.1. Развитие на HA Архитектурите за реализация на Active-Active DC

Архитектурата „Active-Active Datacenter“ се използва за едновременно използване и резервиране на съществуващия капацитет, като основния фокус е защита от срив и в по-малка степен ефективност при утилизация на оборудването.



Active/Standby е традиционния вариант за архитектура от първите IT проблеми – стар, надежден и скъп за минималното предоставено покритие. Често резервния DC става идентичен на активния DC и това увеличава риска, защото много организации искат да използват резервния за развойна среда вместо да го оставят неработещ – в действителност увеличават значително тяхното RTO.

Partitioned Active е една стъпка напред пред Active/Standby в това че и двата DC обслужват клиенти като различни приложения се стартират на различните сайтове и се разменят във резервирането им. Този подход позволява да се резервират приложения без да се налага да бъдат променяни заради новата топология. Пренасочването става на база географско приложение, номер на акаунта, дирекция и др. – Характерното тук е че повечето потребители работят в едното DC, другите в друго но никога двете не смесват средите, с изключение на катастрофален срив с останал един единствен DC. Разделянето на потребителите позволява да се направи еднопосочна репликация от всяка система, недопускайки конфликти в данните и осигурвайки атомарна консистентност.

Asymmetric Active или **Active/Query** означава че само едната база е в режим read/write а нейната реплика може да се използва в read-only приложения. Потребителите които четат могат да бъдат обслужвани своята локална база данни, но потребителите обновяващи данните трябва да са свързани към първата. Приложенията трябва да бъдат променени, така че трябва да се препращат заявките към актуализиращата база. Съществуват мрежови устройства, които вършат такава работа, намалявайки администрирането на базите и намалява отражението върху базите.



Друг вариант е да се публикуват данните през web service или Layer 7 URI рутиране през Server Load Balancers или подобни. Както и предишните решения по-напредналите организации внедряват zero-outage приложения като използват N и N+1 конкуренти инсталации.

Active/Active означава, че всички DC предоставят една и съща услуга на всички свои потребители във всички DC синхронно. Този метод предоставя transparent fault tolerance включително и ниво „облак“, услугата продължава да работи при планирани или не планирани спирания, защото на практика е един и същи „облак“. Съществен елемент е осигуряване на консистентност на данните едновременно и на двете места.

Константността се осигурява от една страна от приложението, ако е подготвено за подобна работа, от друга страна с механизми, които позволяват приложенията да се абстрахират къде в действителност се намират техните данни – Storage Virtualization.

Данните са критична част от решението за Active/Active DC в среда на IBM дискови масиви съществуват два подхода, използвани за реализиране на синхронизацията:

HyperSwap - Power машините и DS8000 масивите работят съвместно, така че независимо от разположението на VM на една среда, тяхното преместване върху друг сървър или друг сайт. Те винаги работят с локалния дисков масив, за да се осигури максимална производителност и минимално закъснение.

Storage Virtualization – в този подход данните се презентират от виртуализационния слой в по-близкия до приложения SAN, но данните по-скоро са в модела Asymmetric Active и би могло да се получи значително натоварване при големи операции за обновяването им.

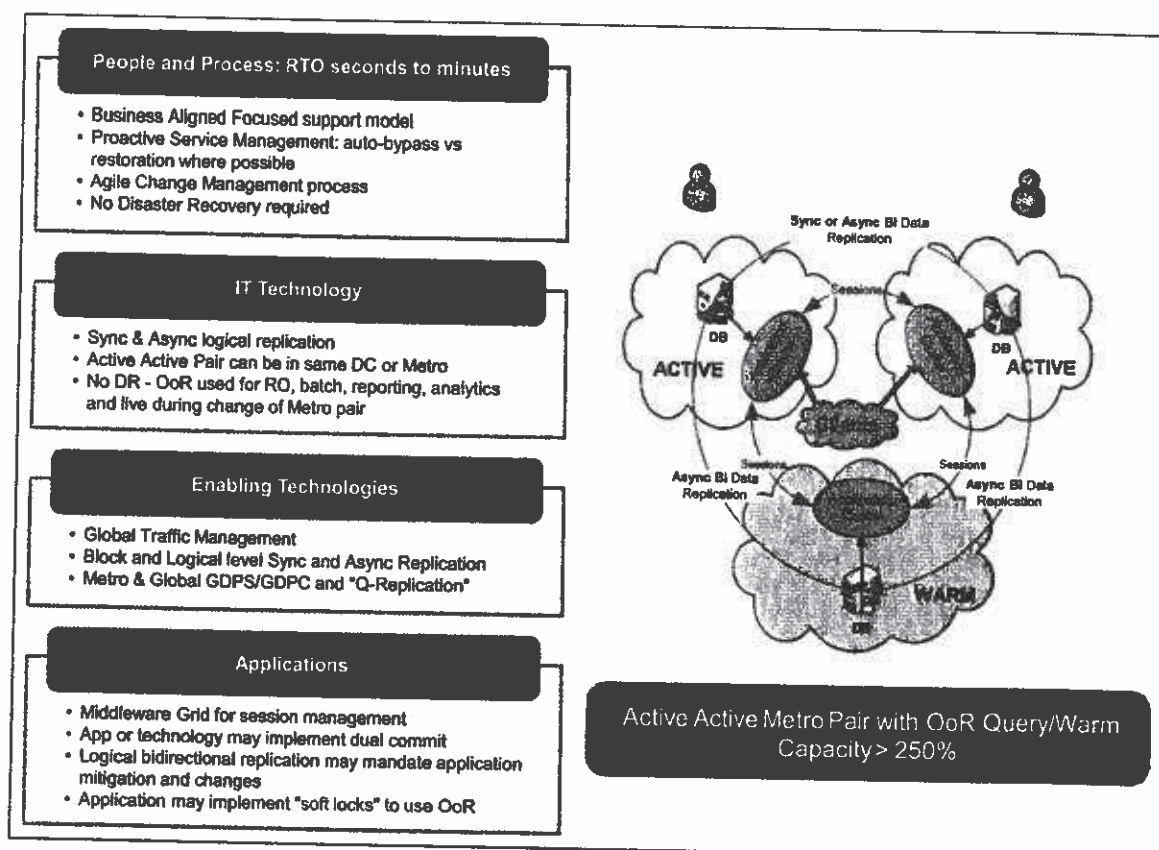
2.2.2. High-Level Design на HA

Въвеждаме някои понятия

OoR – Out of Reach – отдалечен DC

Active/Active в градски дистанции – Metro Area

Характерното на представения на схемата модел е, че осигурява възстановяването на работата в изключително кратки срокове – до няколко минути в случая, когато се рестартира върху отдалечения сайт.



Трябва да се има в предвид, че допълнителното резервиране на капацитета е по-голям от 250%, ако искаме освен данните да бъдат спазени и SLA за производителност при отпадане на цял сайт.

При модела отдалечения сайт се използва като RO или Test&Dev сайт, но не работи активно с приеманите данни. Ние предлагаме в отдалечения сайт да се извършват процедурите по архивиране на данните и тяхното складиране на ленти.

При изграждане на архитектура за резервиране базирана на ТРИ активни DC освен практически безотпадната работа на сайтовете, ефективността на ангажирания капацитет е много по-голяма.

Обичайното резервиране е >250%, за да бъде постигнато същото обслужване при DR ситуация. При 3 активни DC е необходимо да бъде резервиран само един от тях, докато другите два продължават да работят, тогава необходимия за резервиране капацитет намалява до >150%

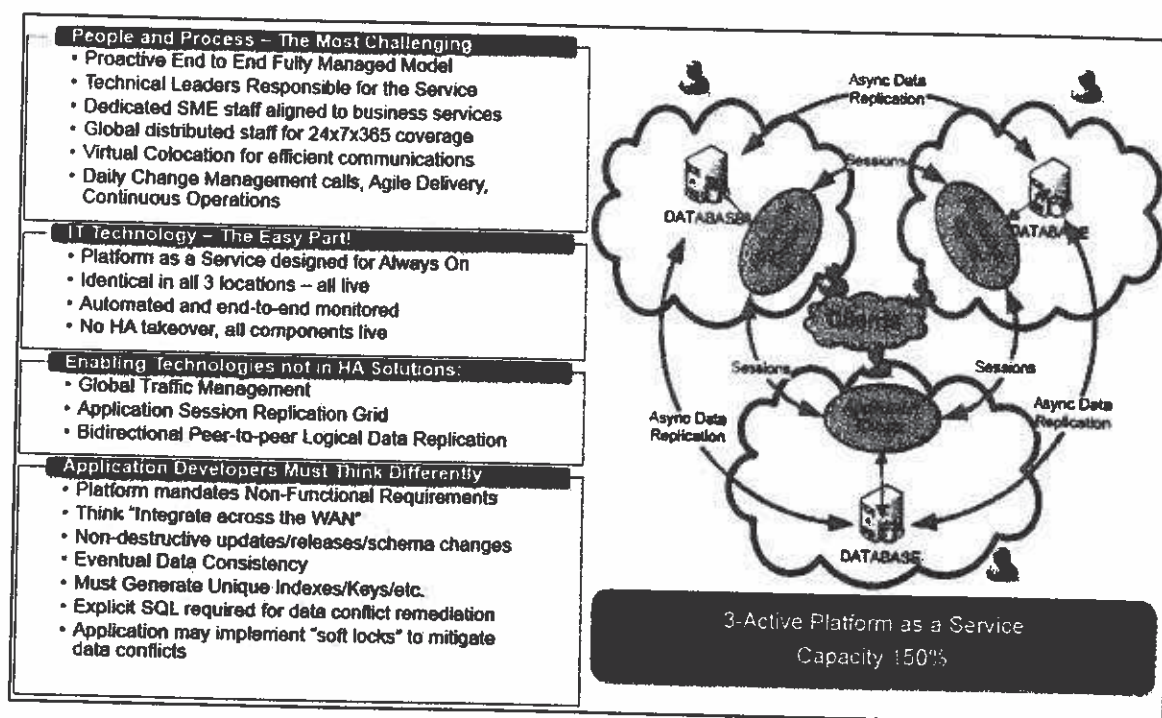


Figure 7. Three Active geographically distributed

2.2.3. Реализация

Active-Active DC ще осигури по-доброто оползотворяване на наличния ресурс, като се използва активно оборудването, както в близки така и в отдалечения DC. Позитивен страничен ефект е, че постоянно ще бъде поддържана среда с висока надеждност за комуникация и с възможност за преместване на виртуални среди между двата центъра за данни за планови спирания на сървъри и дискови масиви или при евентуална авария.

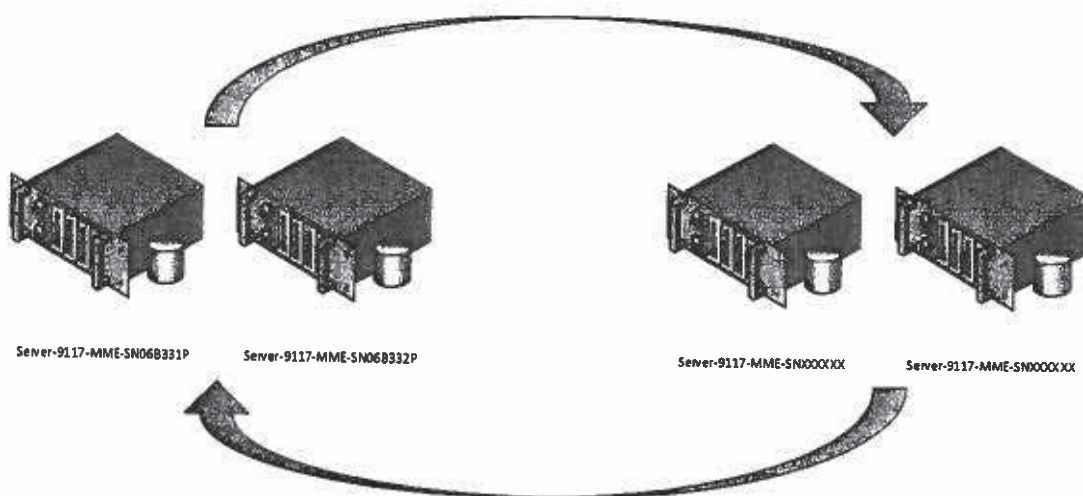
Изискванията за производителност лимитират разстоянието между сайтовете с връзката между тях. Тя трябва да е под 100 км., което е изпълнено, при използване на двата сайта в София. За да се елиминира "Split brain" проблема, трябва да бъде организиран трети логически сайт, който да участва в комуникацията на SAN и дисковите репликации независимо от основните, за него е достатъчно да бъде елиминирана вероятността да отпадне едновременно с някой от двата основни сайта. В идеалния случай това е изнесен офис с FC диск за кворум записите, но може да бъде и резервиран дисков масив в някой от DC със собствени линии за достъп до SAN и отделно захранване UPS.

За основните UNIX сървъри, първата стъпка е критичните системи, които работят в клъстерна среда да бъдат виртуализирани и да имат аналогични по производителност и архитектура членове в отдалечения сайт. Част от концепцията за осъвременяването на инфраструктурата.

За системите, за които не е предвиден PowerHA клъстерен софтуер ще се използва Live Partition Mobility, така че да е възможно ръчното преместване върху друга машина



(включително и върху отдалечения сайт), за да се осигури възможност за планово спиране на отделни сървъри. Отново условието е да се изравнят сървърите от двата центъра за данни.



Спазвайки стратегията на банката за това критичните системи да работят в клъстерен режим, препоръчваме клъстерираните VM да работят в един и същи сайт в конкурентен режим, а между сайтовете в active-standby.

Участващи машини (разчита се, че клъстерираните приложения вече са прехвърлени във виртуална среда – върху POWER 770) :

- Двойката Power 770 на основния сайт или техните наследници, според стратегията за обновяване ;
- Нова Power7 машини от същия клас или POWER8 машина в Касов център;
- Двата DS8x00 със стартирана репликация и интеграция на HyperSwap функционалността;

Storage design

Основната цел е да се елиминира опасността от отпадане на основния дисков масив, където работят всички членове на кълстаре, забавеното/ръчно рестартиране в отдалечения сайт. В active-active 2 sites конфигурация, HyperSwap автоматично поддържа репликация на данните между двата дискови масиви като едновременно с това осигурява на приложенията среда, в която да са Online. В случай, че основния дисков масив отпадне (планирани или не планирано), всички приложения се прехвърлят да работят в резервния дисков масив. В този случай PowerHA® SystemMirror® извършва прехвърлянето и след това новото синхронизиране на данните към възстановения масив.

- Активните приложения работят и на двата сайта А и В;
- Има по две машини във всеки от сайтовете или общо 4 Power сървъри
- Всички участват в mirror groups, конфигурирани да използват HyperSwap® или традиционната in-band функция.

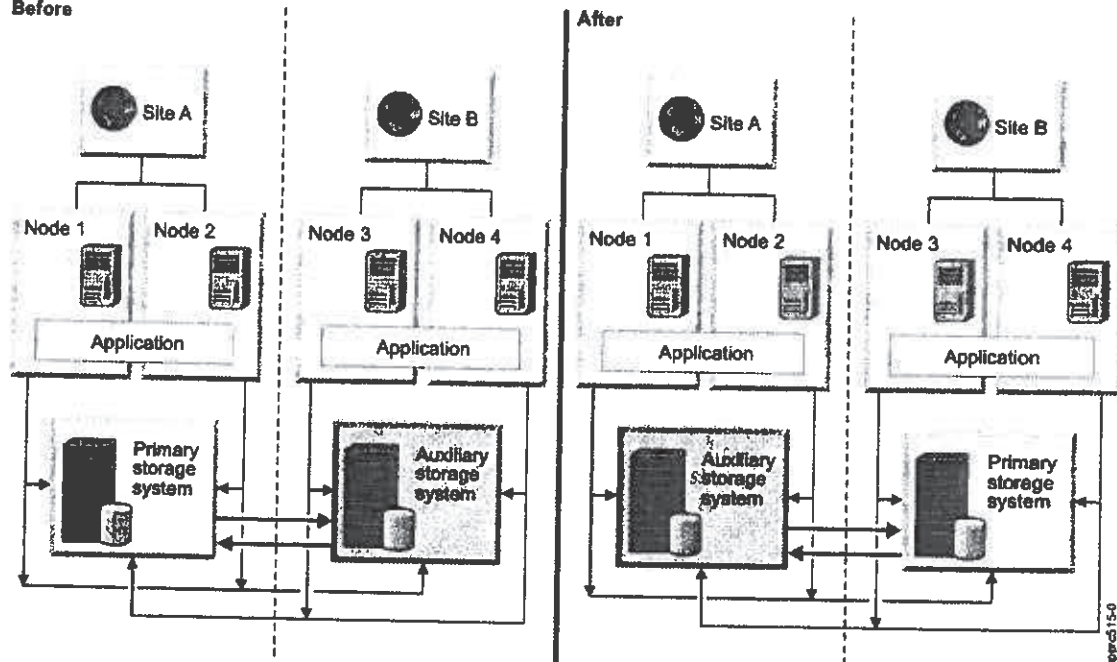


При необходимост приложението да премине от сайт А към сайт В (двата сървъра спират или са недостъпни, дисковия масив е отпаднал) приложението продължава да работи от втория сайт и втория масив става основен, процеса е автоматичен и с използването на HyperSwap дефинициите на пътищата се запазват.

При възстановяване на първия масив, активния синхронизира обновяванията си с него и прехвърля обратно основните операции в него.

Приложенията

Before



За x86 машините, под управление на VMware трябва да бъде извършена миграция към виртуализирана среда под - VMware избраната виртуализационна платформа.

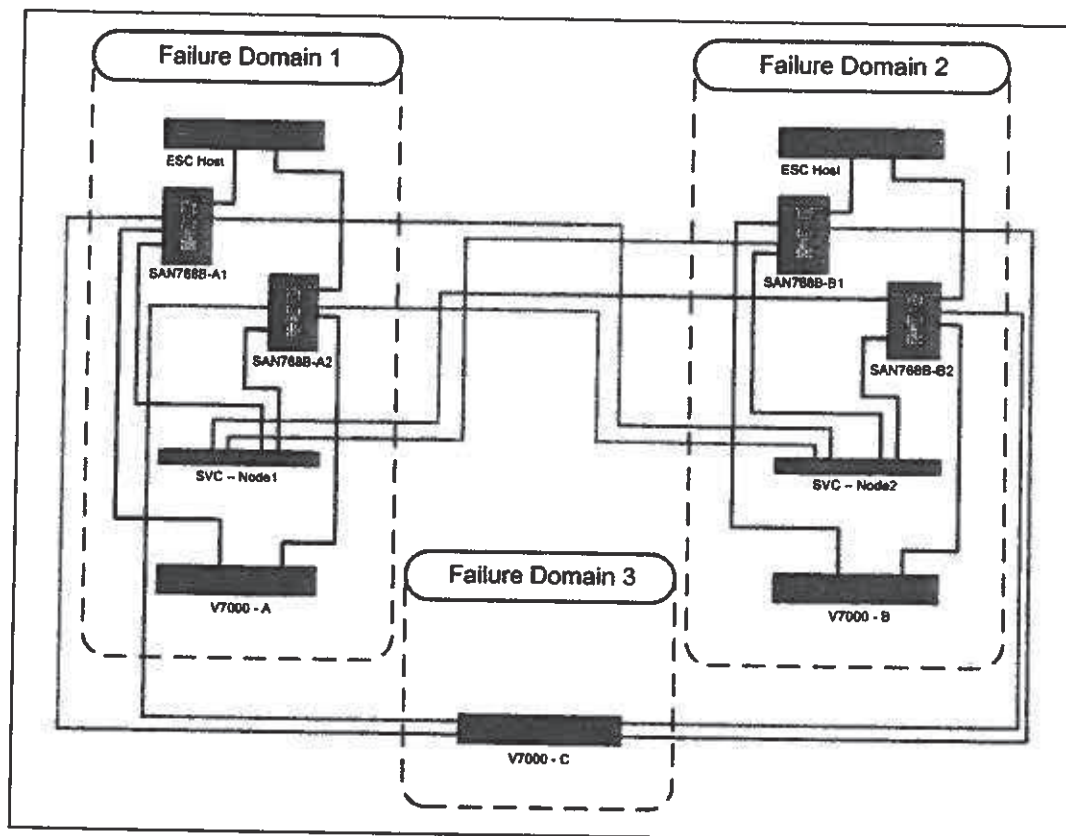
Участващи машини:

- x86 Blade servers на две шасита в двата сайта;
- Двупроцесорните сървъри x3560, 3550;
- Нови rack машини, в зависимост от нови натоварвания;
- Двата DS8x00 със стартирана репликация HyperSwap;

Тъй като по-старите дискови масиви DS8700 и DS8100, върху които текущо работи репликация са излезли от актуалните продуктови листи на IBM и са с лимитиран капацитет от 10 TB, ще трябва да се осигури нов дисков масив в основния сайт с достатъчен капацитет и функционалността така че двойката DS8870 да позволява основните системи да бъдат напълно резервирани и репликирани.



За осигуряване на подобно функционалност за некритичните системи предлагаме да се възползваме от резултатите по внедряване на виртуализирана SAN среда. След внедряване на SVC stretched cluster и интеграцията с x86 платформа и не-критични приложения върху Power платформа ще бъде осигурена репликация между сайтовете и консистентност на обръщенията от сървъри към SAN, включително и на виртуалната среда – NPV.



SVC stretched клъстер трябва да е изграден на база две двойки SVC машини отговарящи за двете SAN фабрики - 205, 206. Софтуера ще позволи да се изградят единно представяне на данните от дисковите масиви към виртуалните среди.

VMWare от версия 5.5 поддържа работата на Stretched клъстер с „preferred path“ оптимизирайки работата на SVC, както и да намали прехвърлянето на данните през линиите между сайтовете.

Неклъстерираните Power базирани приложения също могат да бъдат инсталирани, тъй че да ползват данните от дисковите масиви през SVC, но може да работят и върху двойката DS8870 масиви.





2.3. Преминаване към виртуални работни места - VDI

VDI (Virtual Desktop Infrastructure) е цялостно и комплексно решение за виртуализация на работните места на служителите. Решението се базира на технологията за виртуализация, в следствие на което наследява всички предимства, предоставяни от виртуализацията. Виртуализацията на работните места пренася потребителските работни станции в центъра за данни, като по този начин значително улеснява управлението им от гледна точка на поддръжка и от гледна точка на заемания изчислителен ресурс. Основните предимства на VDI е значителното намаляване на разходите за закупуване на нови работни станции. При VDI работните станции са заменени с така наречените „Тънки клиенти“, които от своя страна представляват много олекотени компютърни конфигурации. Тънките клиенти имат много ограничен изчислителен ресурс, които се използва единствено за осигуряване на достъп до виртуалната работна среда, това от своя страна води до много по-малки нужди от охлаждане и електрозахранване, поради което в тънките клиенти няма движещи се части. Липсата на механични движещи се части значително увеличава живота на един тънък клиент. Стандартно работните станции имат живот между 3 и 5 години, докато при тънките клиенти този период е увеличен до 10-12 години. В същото време разхода за придобиване е намален значително, защото тънките клиенти са много по-евтини от нормалните работни станции. Освен от тънки клиенти VDI инфраструктурата може да бъде достъпвана както от нормални работни станции, така и от всякакви видове мобилни устройства (таблети, смартфони и др.).

Важно предимство на VDI е значителното увеличаване на нивото на сигурност на информацията, тъй като реално данните никога не излизат от центъра за данни на банката. По този начин крайния потребител никога няма да има физически достъп до самите данни. От гледна точка на поддържащия ИТ персонал нивото на сигурност също може да бъде увеличено. За целта всяка система може да има само едно място за управление и наблюдение и това да е отделна виртуална работна станция, до която да има достъп само персонала отговарящ за поддръжката на дадената система. Достъпа до виртуалната работна станция може да бъде контролиран дву-фактурно, като се използва парола, смарт- карта или генератор на случайни числа.

От гледна точка на изчислителния ресурс и заеманото дисково пространство VDI позволява много високи нива на консолидация. При традиционните решения всеки има работна станция, на която има инсталирана операционна система заемаща дисково пространство. Тъй като всички останали имат инсталирани същите операционни системи съдържащи в себе си същите файлове, използвайки VDI решение всички тези повтарящи се файлове се съхраняват само веднъж, като по този начин значително се намалява необходимия дисков ресурс. Това от своя страна води до намаляване на разходите за електричество и охлаждане.

В случай на природно бедствие или авария в дадена локация, всички потребители могат да продължат работа от мобилни работни места, защото информацията, с която работят се намира в центъра за данни, а не на работно им място. В случай на случайно или умишлено заличаване на информация, отново в следствие на факта, че виртуалните работни станции



работят в центъра за данни и се подчиняват на политиките за резервираност и архивиране, данните могат лесно да бъдат възстановени.

2.3.1. Концепция за внедряване

Използването на VDI решение в Българска Народна Банка ще донесе безспорни позитиви от гледна точка сигурност на информацията; управление на крайните станции; консолидиране на изчислителния ресурс; повишена възвращаемост на инвестициите за крайни станции; и не на последно място намаляване на консумацията на електроенергия.

Сигурност на информацията

След пълно внедряване на VDI инфраструктура преносимите компютри се превръщат в терминали, които по никакъв начин не обработват или пазят временни копия на информацията, която се намира в изчислителния център на БНБ. Достъпът до въпросния изчислителен център може да става през Интернет или изобщо да бъде забранен извън банката. Допълнително може да се приложи дву- или ако е необходимо три-факторна защита както за достъп от вън така и за достъп от вътре. Като вземем в предвид и предложеното в точка 3.2 от настоящия документ внедряване на Right Management System и Data Leakage Prevention решения, практически неотторизирания достъп и изтичане на информация в следствие от кражба на преносимо устройство или откраднати credentials става изключително необичаен.

Консолидиране на изчислителен ресурс

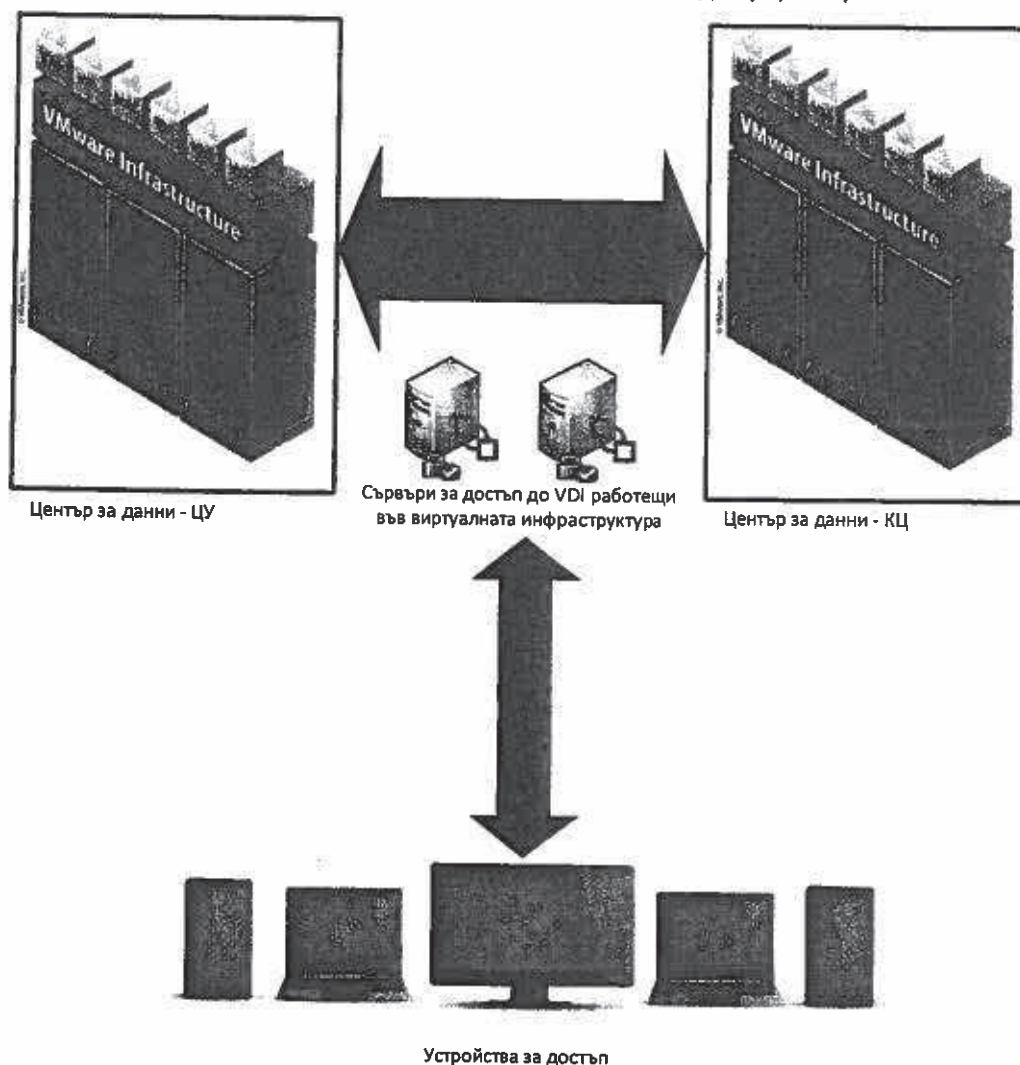
VDI инфраструктурата се нуждае от x86 базирани изчислителни ресурси (описани в точка **Error! Reference source not found.**) и от x86 виртуализационна платформа (описана в точка REF_Ref421095655 \r \h 2.1.2). И двата компонента са от изключителна важност за високата консолидация и надеждност на едно VDI решение. Текущата тръжна процедура има включени не малък брой x86 базирани машини, които могат да бъдат използвани и за виртуализация на работни станции. Самият Hypervisor е наличен в банката (от производител VMWare), той следва да бъде надграден с допълнителни лицензи, които не са обект на текущата процедура. С цел пълнота на концепцията - за всяка виртуална работна станция са необходими два лиценза: Microsoft VDA (Virtual Desktop Access) и VMware Horizon View.

При използване на VMWare базирана сървърна виртуализация коефициента на консолидация сравнително реалистично стига до 15:1, като за някои приложения може да надвиши това съотношение. Статистиката показва, че когато се добави и VDI виртуализация към вече налична сървърна такава, коефициента на консолидация на общия изчислителен ресурс се покачва. Средно цената на работно място намалява с между 20 и 30%.

В конкретния случай наличната инфраструктура в БНБ позволява лесно надграждане до напълно функционално VDI решение. БНБ има доста налични ресурс (сървъри, дискови масиви, мрежов ресурс), които могат да бъдат допълнително уплътнени и съответно да доведат до спестявания. За сравнение в организация, която няма изградена ИТ инфраструктура и това

трябва да се прави тепърва за нуждите на VDI, финансовата обосновка на едно такова решение е трудна. В БНБ случая не е такъв, а точно обратен.

Долу изложената фигура дава най-общ концептуален поглед върху VDI решение в банката.



Намаляване на консумацията на електроенергия

В много форуми, блогове и статии се говори за намаление на консумацията с между 80 и 90%. Истината е, че това зависи от значителен брой фактори и е въпрос на детайлен анализ. Част от факторите са – ефективността на текущите захранвания на наличните работни станции; натоварването на работните станции; закачената периферия; вида процесор, който се ползва; количеството RAM; поколението на твърдия диск и т.н.

Тънките клиенти консумират между 5 и 14W на час, за сравнение една PC конфигурация между 65 – 250 W. Това е основно породено от липсата на движещи се части в тънките клиент,

липсата на твърд диск, минимална изчислителна мощ и сравнително малкия обем оперативна памет. Една сървърна конфигурация, която реално доставя виртуалния работен плот консумира на 65-100 потребителя средно 450 – 650W за час, но работи 24 часа в денонощие (освен ако не е предвидена концепция за гасене и автоматично пускане, което е възможно с VMWare продуктите).

Една по реалистична сметка със следните параметри и цената на тока в България в момента води до спестявания в размер на около 53%.

Параметър	Стойност
Работни часове на ден	8
Дни в седмицата	5
Седмици в годината	50
Консумация на тънък клиент (active)	25 W/h
Консумация на тънък клиент (idel)	8 W/h
Консумация на PC (active)	80 W/h
Консумация на PC (idel)	60 W/h
Брой работни машини на сървър	75
Консумация на енергия от сървъра	475 W/h
Охлаждане на сървър	1414 BTU/hour

Специфики при изграждането на VDI решението

За целите на VDI решението е силно желателно към сървърните конфигурации да се добавят графични карти (GPU). По този начин, отново чрез използване на виртуализация, всяка виртуална работна станция, ще има достъп до видео ускорител, което значително подобрява производителността и позволява работа с приложения изискващи видео ускорители.

Добрите практики показват, че за максимално добро уплътняване на изчислителния ресурс и за максимална производителност на виртуалните работни станции, трябва да се използват сървърни системи с много на брой процесорни ядра и максимално количество оперативна памет. Оразмеряването на изчислителния ресурс зависи до голяма степен от вида на работа на крайните потребители:

- За потребители работещи предимно с обработка на текст е препоръчително 10 потребителя да използват 1 процесорно ядро;
- За потребители работещи с графики и текст се препоръчва максимум 6 потребителя да използват едно процесорно ядро и споделен графичен ускорител;



- За потребители работещи с тежки приложения, имащи нужда от много изчислителен ресурс (разработчици, видео-обработка и т.н.) се препоръчва максимум по 3 потребителя на процесорно ядро и заделен графичен ускорител.

Оразмеряването на оперативната памет се изчислява според нуждите на приложенията.

Спрямо текущото ни предложение, подходящи сървърни системи са тези описани в „Примерна Конфигурация 1“ посочена в точка **Error! Reference source not found.** от астоящия документ.

Изискванията към дисковите масиви зависят пряко от броя на виртуалните работни станции. Добрите практики показват, че най-добре е да се използват флаш базирани дискови масиви, заради високата си производителност от гледна точка на входно-изходни операции. В същото време технологиите използвани във VDI позволяват значително намаляване на необходимото дисково пространство, което от своя страна също е благоприятно за използване върху флаш дискови системи (заради ограничения им капацитет и високата им цена). Подходящи дискови системи от текущото предложение са „IBM FlashSystem 840“.

2.3.2. Стъпки на имплементация

Долу изброените детайлни дейности не са с посочена индикативна продължителност защото зависят от много фактори, включително и наличието на време от страна на служителите на банката. Въпреки това спрямо опитана ни смятаме, че посочения период за цялата стъпка е реалистичен и изпълним.

Внедряването на VDI решение се обуславя с една основна стъпка и n на брой следващи стъпки. Практически инфраструктурата на банката трябва да бъде обновена и да бъдат пуснати и тествани първите виртуални работни станции. При добър дизайн и архитектура следващите добавяния на виртуални работни станции могат да бъдат безброй и ще бъдат тривиални.

За целите на документа ще опишем в детайли дейностите в първата (основна) стъпка:

- Анализ на пилотната груба потребители, които ще бъдат мигрирани към виртуални работни станции;
- Определяне на типове потребители и тяхното разпределение в съответната група;
- Определяне на характеристики и хардуерни изисквания за всяка група;
- Анализ на съществуващото състояние на VMWare клъстера и определяне на необходимия нов хардуер, ако такъв е необходим. Възможно е разбира се и надграждане с модули и компоненти;
- Избора на тънки клиенти
- Обновяване на дизайна на VMWare клъстера;
- Имплементиране на дизайна:
 - Добавяне на допълнителни машини/компоненти
 - Създаване на шаблони за виртуалните машини
 - Инсталиране на операционни системи

- Инсталиране на системен софтуер
- Създаване на групи / аналогични на вече дефинираните потребителските групи
- Инсталация и конфигурация на софтуер за управление на тънките клиенти
 - Тестове с нова тестова виртуална машина
 - Пилотно мигриране на по една реална виртуална машина от тип
 - Анализ на резултатите и ако е необходимо до настройки
 - Мигриране на всички определени потребители
 - Приемни изпитания на решението

Документирането, имплементирането и тестването на тази стъпка би отнело **1 календарен месец**, при положение, че няма усложнения. Усложненията могат да се появят при наличие на специфична периферия, която се ползва на някой от потребителите, които ще се мигрират.

Всяка следваща стъпка за добавяне на допълнителни виртуални машини е аналогична на горе изложеното, като в ситуация, в която се ползват наличните групи потребители и няма необходимост от нов хардуер дейността се опростява значително.

Предимствата след имплементиране на тази стъпка са ясно изложени в началото на тази глава.

Тази стъпка е пряко зависима от:

- Стъпка 1 – Междинно резервиране с Fault Tolerance конфигурация / **x86 виртуализация**
- Стъпка 2 – Преминаване към пълна Active-Active конфигурация / **x86 виртуализация**
- Стъпка 1 - Изграждане на дискова инфраструктура в първия център за данни / **дискови масиви**
- Стъпка 2 - Изграждане на Stretched Cluster – Active-Active Datacenter. / **дискови масиви**
- Стъпка 4 - Изграждане на инфраструктура за предоставяне на виртуални работни места / **дискови масиви**

Тази стъпка косвено зависи от:

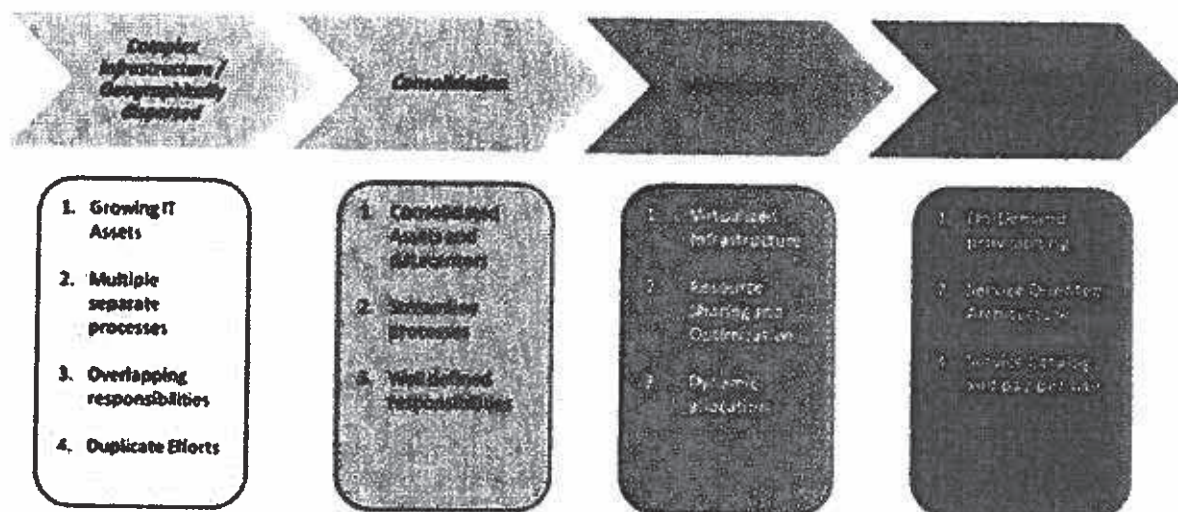
- Стъпка 1 – Съобразяване на дизайна в основните изчислителни центрове с най-добрите практики и преминаване към едновременна работа / **Мрежа**
- Стъпка 1 – Оптимизиране на виртуалната инфраструктура. / **x86 сървъри**
- Стъпка 2 - Изграждане на Active-Active центрове за данни. / **x86 сървъри**
- Стъпка 3 - Оптимизиране на Active-Active центрове за данни. / **x86 сървъри**

Зависимостта от други стъпки е условна и е базирана на презумпцията, че трябва да се постигне задоволително ниво на функционалност и резервираност. Съответно може да се предприеме и друг подход и различно разпределение и раздробяване на стъпките според бюджет и по-точни цели.

Обект на анализ е и необходимостта от закупуване на допълнително x86 сървърно оборудване и/или дискови масиви от тип non-enterprise applications.

2.4. Формиране на частен облак

Изграждането на частен облак не е самоцел, а начин да се добави цялостно управление на информационните ресурси и функции като резервиране на сървъри и дискови масиви, отдалечена репликация, сигурност и др.

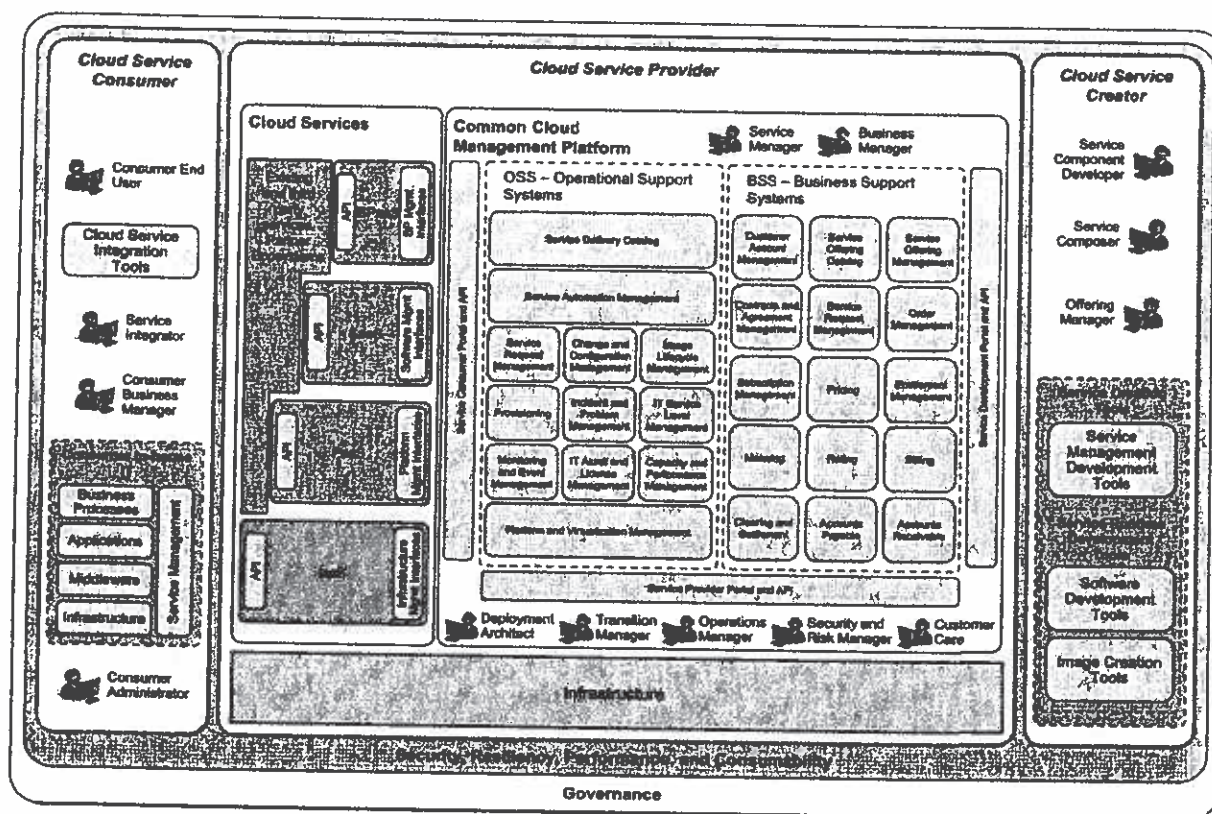


След приключване на консолидацията и виртуализацията инфраструктурата е готова да мине към нов тип управление на изчислителните ресурси. Основните характеристики на облака, които ще са от полза за банката са:

- Автоматизиране на изграждането на нови среди до ниво на „самообслужване“ на клиентите
- Отчитане на използването на ресурси по типове и по „клиенти“
- Внедряване и експлоатация на софтуерни приложения базирани на облачните архитектури – Big-data, Analytics, web services etc.

2.4.1. IBM Cloud Computing Reference Architecture

IBM CCRA е архитектура базирана на набор от допълващи модели за изграждане на облачни компютърни решения, които са организирани в четири основни модели. Моделите се категоризират на база облачни бизнес модели и технически цели. Те също представляват начинът, по който повечето клиенти подхождат при изграждането на облачните решения. За всеки от тези модели CCRA идентифицира обща архитектура, която описва технологиите, които лежат в основата на всеки вид на изпълнение на облачните решения.



Ето следните направления за внедряване на облачни услуги през CCRA

- Cloud Enabled Data Center adoption pattern

Cloud Enabled Center Data Моделът на внедряване обикновено е входната точка в пространството за облачни решения. Тя дава насоки за определянето, проектирането и внедряването на облачни компютърни решения, които доставят IaaS обикновено в границите на предприятието.

- Platform-as-a-service (PaaS) adoption pattern

PaaS описва как да се изработи облачни компютърни решения, които доставят предварително конфигурирани готови за изпълнение на среди или мидълуер стекове, върху която могат да бъдат разгърнати приложения. Той също така описва как да се връзва заедно разработката на приложения и процеси и разгръщането им в единен непрекъснат процес на доставка на базата на разработка на приложения и ИТ операции (DevOps) принципи.

- Cloud Service Providers adoption pattern

Cloud Service моделът е, когато доставчикът определя облачно базирани решения, които предоставят услуги в чрез модел на доставчик на услуги. Доставчикът на услуги е организация, която осигурява облака обикновено за външни клиенти.

Доставчикът на услуги, управлява и облачните услуги като общ доставчик, а не работа на обслужване на своята собствена организация.

- Software-as-a-service (SaaS) adoption pattern

SaaS дефинира архитектурата за дефиниране и използване на SaaS приложения. Доставчикът предоставя архитектурата, която позволява на SaaS приложения да бъдат управлявани и предлагани от доставчика на услуги облак. Доставчикът на услуги облак също подкрепя системи, които осигуряват средата, в която са реализирани SaaS бизнес модели.

Естествения модел за развитие на инфраструктурата в БНБ е Cloud Enabled Data Center, основния фокус е върху контрола върху управлението на ресурсите, автоматизиране на провизирането и освобождаване на ресурсите.

В много по-малка степен се очаква да се премине към внедряване на софтуер базиран в „облака“, най-вече заради естеството на работа на банката

2.4.2. Предложение за концепция за изграждане Cloud Enabled Data Center

Няколко основни идеи ще дефинираме за да подпомогнем стъпките за изграждане на частен облак:

Use-case packages

Използване на пакети, в които клиент се нуждае от определен тип услуга или ресурс. Например: различни функции на виртуализиран дисков масив или Use-cases използвани за идентификация и управления на достъпа.

Micropattern - Микро-шаблон

Микро-шаблон е колекция от свързаните пакети за ползване в конкретен случай. Например, микро-шаблон за виртуализация е колекция от използвани конкретни пакети за виртуализация на сървъри, виртуализация на съхранение на данни, мрежа за виртуализация и управление на хипервайзор.

Macropattern – Макро-шаблон

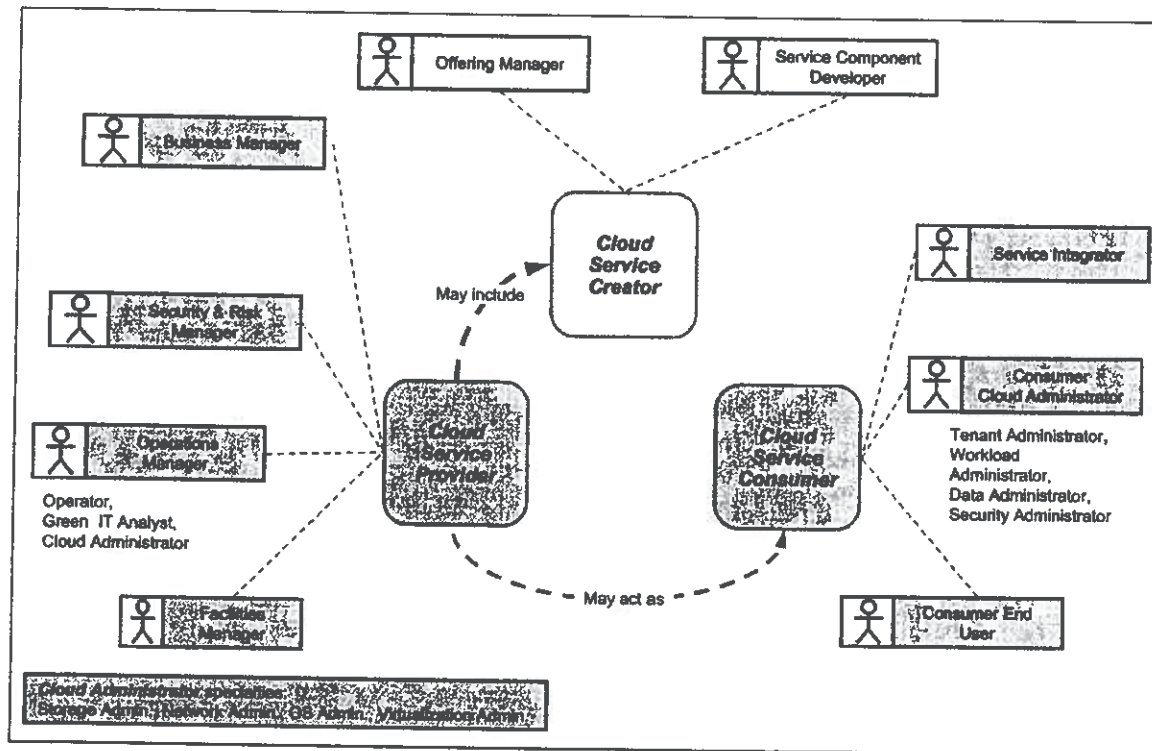
Макро-шаблон е колекция от микро-шаблони, които се прилагат заедно. Например, възможностите за провизиране, оркестрация на услуги и хибридни облачни услуги се изпълняват от "Advanced IaaS" macropattern. Също така, macropattern определя архитектурния изглед на компонентите, които го прилагат. Друга типична характеристика на macropattern е, че той обикновено се комбинира (от гледна точка на възможности и компоненти) на върха на предишните macropatterns и осигурява основата за изграждане на следващия macropattern.





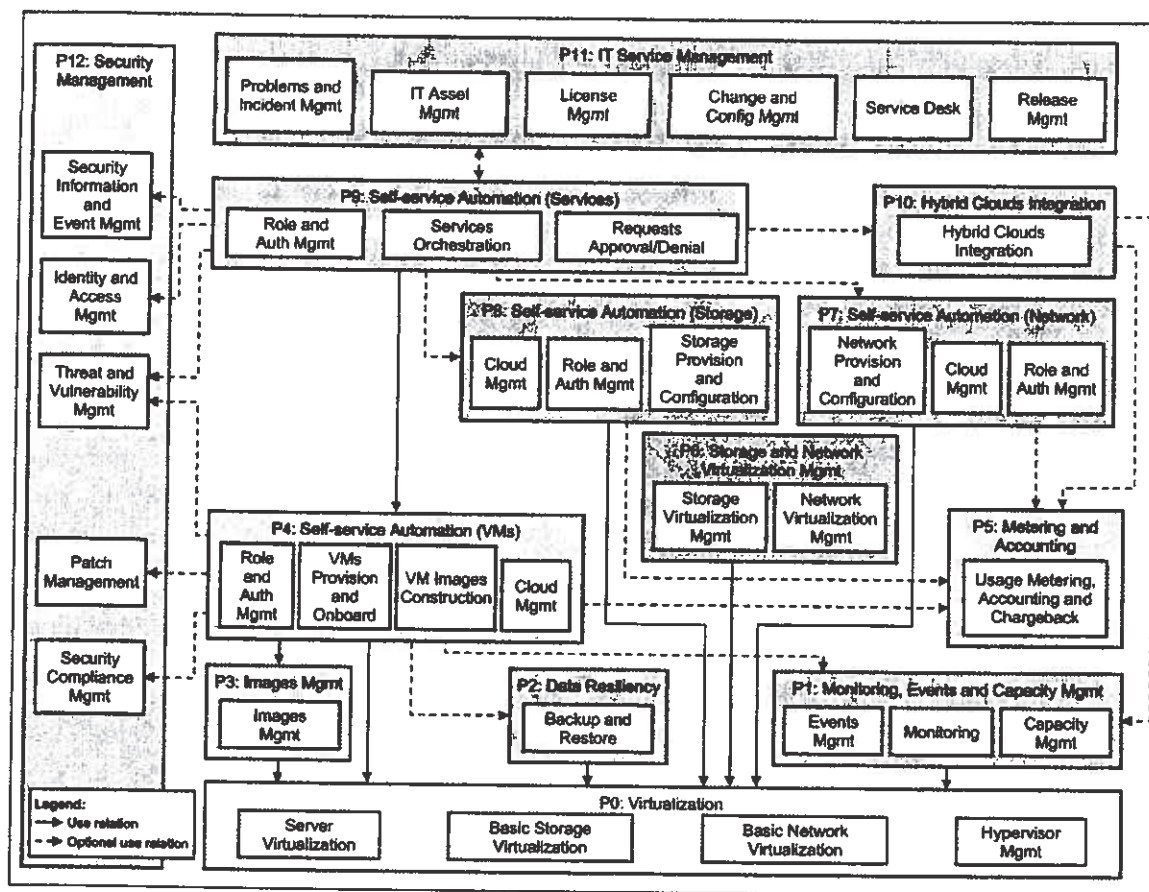
2.4.3. Роли в Cloud Enabled DC

Дефинират се и нови роли при определянето на облачни услуги в DC. Такива са ролите на разработващите, публикуващите, използващите, стартиране и администриране на нови услуги.



2.4.4. Use cases и micropatterns

CCRA дефинира основните use cases за Cloud Enabled DC внедрявания. Също се дефинират микро-шаблони, включващи свързаните случаи със очакваните имплементирани функции на всяко едно ниво. По-долу са показани micropatterns и техните асоциирани use-cases групи.



Virtualization (P0)

Включва compute, storage и network виртуализационни use cases, към управлението на hypervisor.

Monitoring and event and capacity management (P1)

Свързан с наблюдението на състоянието на облачната инфраструктура, събира и управлява събития в нея и осъществява планиране на капацитета.

Data resiliency (P2)

Включва backup на дисковите дялове, виртуални машини и възстановяването им в случай на отказ или прекъсване.

Image management (P3)

Управлява use cases свързани с регистриране на image и тяхното съхранение, image capturing, deep image, анализ на отклонения в различните версии, контрол на версиите и управление на ресурсите свързани с тях.

Self-service automation (P4)



Обхваща случаите за onboarding, provisioning, и управление на виртуални машини (VMs), достъпни през service catalog.

Metering and accounting (P5)

Включва use cases за измерване, отчет и заплащане на ресурсите в Cloud Enabled Data Center.

Storage and network virtualization management (P6)

Включва use cases свързани с разширените възможности за управление на виртуализирани дискови и мрежови среди, като discovery, provisioning, and monitoring.

Self-service automation (storage) (P7)

Включва функциите по - discovery, configuration, provisioning, commissioning, and decommissioning of storage use cases.

Self-service automation (network) (P8)

Включва use cases за откриване, конфигуриране и провизиране на виртуални мрежи и мрежови интерфейси. Такива устройства като virtual local area networks (VLANs), virtual routing and forwarding (VRF), load balancers и firewalls.

Self-service automation (services) (P9)

Включва use cases за провизиране и конфигуриране на комплексни услуги които включват повече от една VM, масив и мрежов елемент или се използват в продукционна среда.

Hybrid cloud integration (P10)

Включва use cases за внедряване на приложения в публични облаци, интеграция на управлението на услуги и governance през on-premise Cloud Enabled Data Center и публични облаци.

IT service management (P11)

Включва use cases за внедряване на ITIL процеси. Например процесите могат да са incident and problem management, change and configuration management, IT asset management, license management, service desk, и release management в частни облаци.

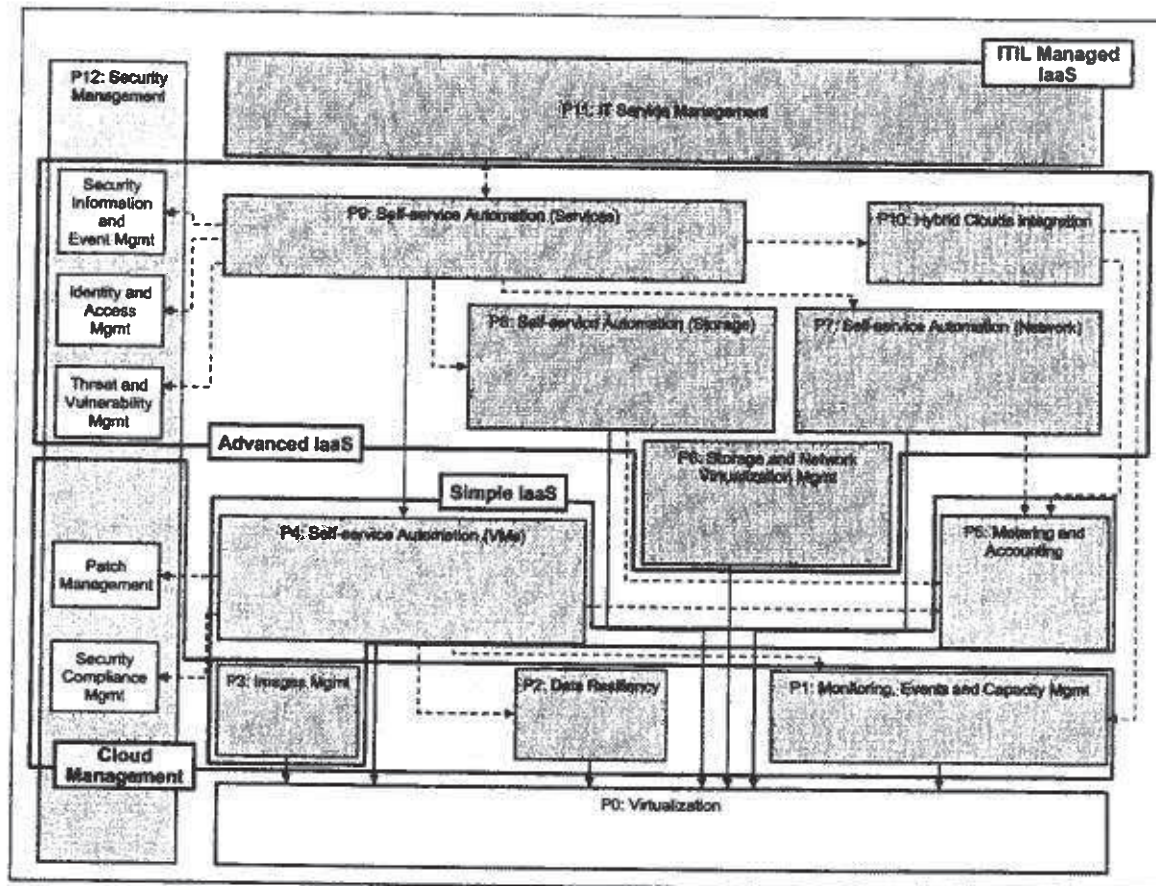
Security (P12)

Включва use cases за защита на различните нива на Cloud Enabled Data Center решението и инфраструктурата като идентификация и управление на достъпа, защита на виртуалната инфраструктура SIEM, автоматизиране на контролите по сигурността и други комплексни услуги.



2.4.5. Макро-шаблони

Ако се разглежда на по-високо ниво организацията на Cloud Enabled Data Center, се обединяват микро-шаблоните за инициативи. Характерно за тях е, че при реализацията си добавят набор от услуги и възможности на средата.



Всеки macropattern може да се представи като етап от внедряване на по-сложно и комплексно използване на облачните услуги

- **Simple IaaS (VM)**

Това macropattern е входната точка в облачната услуга IaaS. Може да се започне изграждането на multitenant облачна инфраструктура и модел, който осигурява прости виртуални машини (конфигуриран с подходяща мрежа и съхранението), която обхваща най-честите нужди на бизнеса

- **Cloud management**

Macropattern допълва Simple IaaS macropattern чрез добавяне на възможности за управление, които можете да използвате, за да управлява тези изисквания като SLAs, сигурност, гъвкавост и планиране на капацитета. Това macropattern помага допълнително оптимизиране на ИТ процесите, управление на сложност на виртуализация и автоматизация, както и



повишаване на ефективността както на инфраструктурата, която осигурява облака и както и облакът като услуга. Това macropattern отговаря и на нефункционални изисквания в областта на надеждността, достъпността и основно ниво на сигурност.

- **Advanced IaaS**

Този macropattern се използва за създаване на по-сложни клауд инфраструктури за доставка и управление на сложни и критични IaaS в силно взискателни среди. Той също така може да разположи услуги в повече от един център за данни или да мащабира до разполагане на среди в публични облаци.

Справянето с комплексни, продукционни или подобни среди е част от функциите на този macropattern като отговаря и на нефункционалните изисквания в областта на производителността, скалируемостта, разтегливост и подобрена сигурност.

- **ITIL managed IaaS**

За тази macropattern, е разширен Advanced IaaS с интегрирани процеси ITIL. Този macropattern дефинира облачна среда, който се интегрира със съществуващите корпоративни приложения, системи и процеси. Тази интеграция се постига чрез включване на инфраструктурата на облака и услуги в процесите на предприятието по ITIL. Този macropattern обикновено е последната стъпка в трансформацията на Cloud Enabled Data Center.

2.4.6. Реализация

В рамките на внедряване облачни услуги в БНБ ние предлагаме да се стигне до етапа Advanced IaaS като се внедрят някои политики от ITIL особено в организирането и планирането на внедряванията и във обслужването на заявките. Те ще спомогнат банката да получи по-ефективно управление на ресурсите си, автоматизация на провизирането на сървъри, дискови масиви, мрежи и сигурност. След изграждането на Advanced IaaS центровете за данни ще се разглеждат като общ ресурс и ще се позволи да се реализират задачи обхващащи цялата инфраструктура.

IBM предлага решения базирани на IBM Cloud Orcestrator в изграждането на облачни услуги:

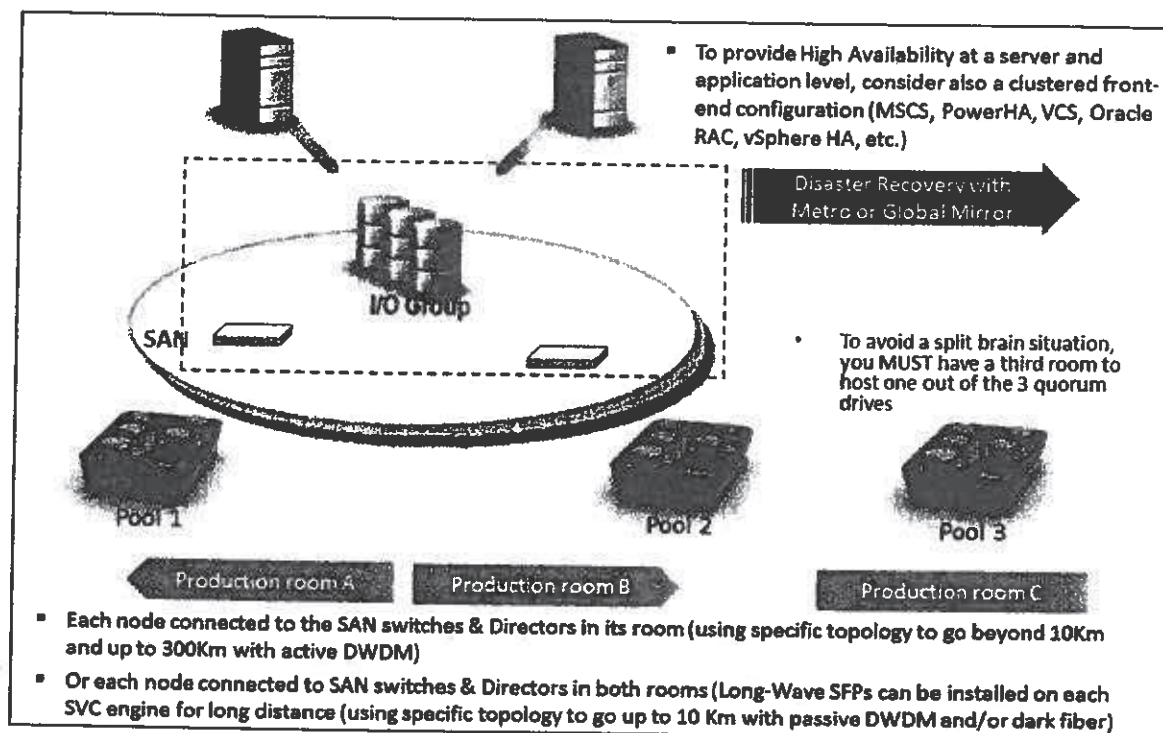
- По-бързо внедряване и разширяване на вътрешни и/или публични ресурси
- Провизиране на нови ресурси и услуги
- Намаляване на натоварването на администраторите и възможностите за грешки чрез автоматизиране на инсталациите
- Интеграция със съществуващата инфраструктура и приложения, използвайки програмни интерфейси и разширения на средствата за управление
- Предоставя услуги и интеграция с IBM SoftLayer, съществуващи OpenStack платформи, PowerVM, IBM System z, VMware или Amazon EC2.

Лицензирането и услугите по внедряване на това решение излизат извън обхвата на настоящата процедура и са свързани с обхвата на проекта – кои системи, кои потребители и кои приложения ще се „качат“ в облака.



2.5. Изграждане на отдалечен резервен сайт

Според изискванията и препоръките на стандартите в областта банката трябва да е в състояние да защити данните от бедствия и аварии на отдалечен сайт и да е в състояние да рестартира операциите от там. Резервния сайт трябва да е географски отделен от основните машини и да е в състояние да рестартира работа на основните ИС без загуба на данни и минимално време за спиране на работата



Основните направления са:

- Избор на обхвата на ИС, кои системи и с какви параметри като Recovery Time Objective, Recovery Point Objective, ще се намират в резервния сайт
- Какви процеси ще бъдат изпълнявани там. Например, архивиране
- Архитектура на отдалечения сайт – сървъри, дискови масиви, LAN & SAN
- За сървърите:
 - o Частична или пълна виртуализация на софтуерните системи, които работят върху тях.
 - o Методи и процедури за рестартиране на работата им
 - o Процедури за възстановяване на данни при срыв и неконсистентно копие
 - o Обратно възстановяване върху основния сайт
- Дисковите масиви

- Избор на топология и параметри на репликацията
- Внедряване на процедури в ИС за гарантиране на консистентно копие на данните
- Извършване на тестове и отработване на процедури за частична или пълна загуба на данните на основните сайтове
- Възстановяване от лентови носители

3. Стратегии за развитие на мрежите и сигурността

3.1. Стратегия за развитие на комуникационната и мрежовата инфраструктура

Стратегическите инициативи на БНБ целят развитието на информационната инфраструктура на банката през следващите четири години. Те се обединяват в следните направления:

- Внедряване на технологии за виртуализация;
- Едновременна работа на информационните системи в два изчислителни центъра;
- Изграждане на центъра за възстановяване след инциденти;
- Осигуряване на механизми за автоматизация за провизиране на информационните системи.

За постигането на стратегическите инициативи на БНБ е необходимо комуникационната инфраструктура да бъде подготвена спрямо изискванията на технологиите, които те ще обезпечат. За целта трябва да бъдат извършени следните промени и нововъведения:

- Virtualization - Подготовка на мрежовия дизайн за нуждите на виртуализацията на информационните ресурси и системи;
- Active – Active Datacenter Design – Осигуряване инструменти за едновременна работа на информационните системи на БНБ в два изчислителни центъра;
- Disaster Recovery Center - Осигуряване на комуникационна инфраструктура за нуждите на центъра за възстановяване след инциденти;
- Private Cloud - Подготовка на мрежовата инфраструктура за осигуряване на стандартизирани механизми за автоматизация на процесите по управление на информационните ресурси – мрежови, изчислителни, за съхранение на данни и т.н.

3.1.1. Комуникационните системи и технологиите за виртуализация

Основна стратегическа инициатива за БНБ е внедряването на системи за виртуализация, които да осигурят гъвкави механизми за автоматизация на процесите по обслужване на информационните системи в банката.



За да се гарантира надеждната работа на системите за виртуализация информационната структура на БНБ е необходимо да се извършат следните стъпки.

Развитие на дизайна на мрежовата инфраструктура

Постоянните промени с цел подобряването на работата в мрежата на БНБ и повишаването на информационната сигурност, както и добавянето на нови технологии и функционалности изисква дизайна ѝ да бъде регулярно ревизиран. Мрежовият дизайн трябва да е съобразен с най-добрите практики и да обезпечава технологиите, решенията и услугите внедрени в информационната инфраструктура на БНБ.

За да бъдат внедрени всички системи за виртуализация в БНБ, които ще работят като равноправни в двата основни изчислителни центъра, е необходимо мрежовия дизайн да бъде съобразен с техните основни изисквания:

- Високоскоростна резервирана Ethernet свързаност – минимум 10Gbps, с възможност за надграждане;
- Технологии за пренос на Layer 2 трафик между изчислителните центрове;
- Сигурност на предаваната информация и защита на сървърната инфраструктура.

Също така, дизайнът на комуникационната инфраструктура в двата изчислителни центъра трябва да следва обща визия и да бъде идентичен – т.е. в двата центъра за обработка на данни на БНБ трябва да бъдат изградени идентични мрежови слоеве, да бъдат внедрени еднакви технологии за пренос на данни и информационна сигурност. Това означава, че дизайнът на мрежовата инфраструктура в Касов центъра на БНБ трябва да бъде развит и променен така, че да отговаря на този в Централата на банката.

Преструктуриране на сървърните сегменти в изчислителните центрове

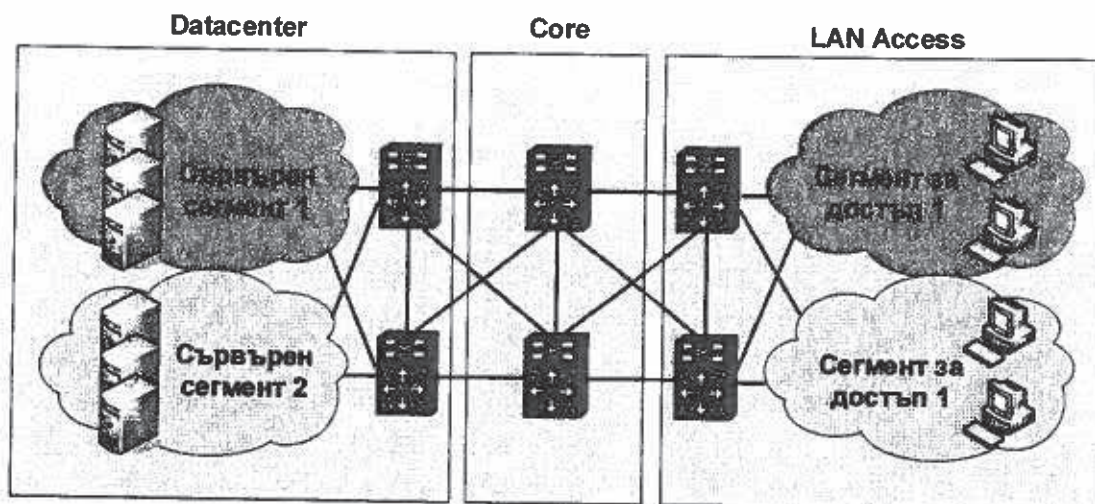
За да се гарантира по-голяма сигурност, по-добро наблюдение и стабилна работа на основните приложения и сървъри е необходимо да се обнови мрежовия дизайн в сървърния сегмент на БНБ. Това трябва да включва изграждане концепция за VLAN сегментиране и обособяване на виртуален Datacenter контекст на основните комуникационни устройства в банката Nexus 7010. По този начин сървърите ще бъдат обособени в отделна мрежова инфраструктура и в обособени сегменти на база тяхното предназначение и политиките за сигурност, които ще бъдат прилагани на връзките към тях и между тях.

Изготвянето на концепция за сегментиране на сървърния сегмент и прилагането ѝ, ще позволи създаването на прецизни политики за сигурност, които да гарантират високата степен на защита в отделните мрежови сегменти, както и ще осигури прецизен контрол и по-добро качество на услугите, предоставяни от отделните приложения.

Преструктурирането на сървърния сегмент и обособяването на сървърите и приложения в съответните VLAN мрежи и нов Datacenter контекст, ще позволи да се контролира трафика, както между самите тях, така и между сървърните и потребителите, които достъпват информационните ресурси на банката. По този начин може да бъдат изготвени и приложени политики за сигурност, които да позволят достъп на потребителите само до частта от сървърния



сегмент, в която се намират т.нар. front-end сървъри, към които се обръщат директно клиентските приложения. По същия начин може да се контролира трафика между отделните сървъри и да се осигури само мрежови достъп, необходим за коректната комуникация между тях. Целият останал мрежови достъп може да бъде забранен с цел повишаване на информационната сигурност.



Осигуряване на физическа резервираност на връзките към сървърите

Коректната работа на приложенията трябва да бъде гарантирана с помощта на надеждна физическа свързаност към сървърите, които ги обслужват. Тя трябва да е резервирана, като всеки от сървърите трябва да разполага с минимум два мрежови интерфейса. Всеки от мрежовите интерфейси на дадения сървър, трябва да бъдат свързани към отделни физически устройства. При използването на подобен тип мрежова свързаност, е необходимо да се позволява използването на коя да е от връзките, без това да влияе на работата на приложенията.

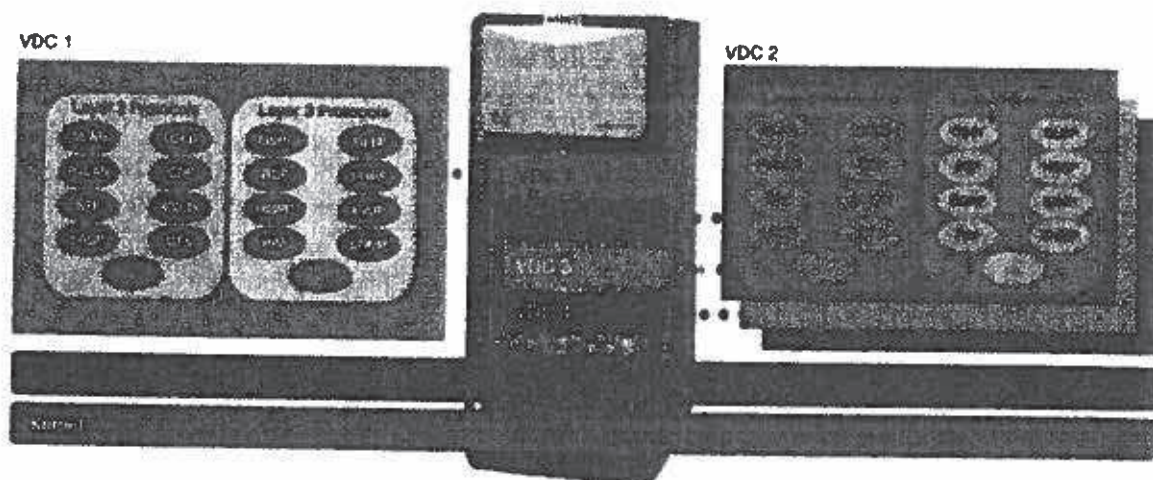
За да се постигне по-високо ниво на резервиране се препоръчва свързването на линиите от сървърите към устройства, които използват технология позволяващи им да работят като едно логическо устройство. Чрез използването на подобна технология от гледна точка на приложения/сървър двете връзки се терминират в едно устройство. Това значително улеснява резервирането, конфигурацията и работата на приложенията.

Виртуализация на мрежовата инфраструктура

Оборудването, което се използва в мрежовата инфраструктура на БНБ разполага с технологии за виртуализация, които ще бъдат използвани при подобряване на мрежовия дизайн в изчислителните центрове на банката. Устройствата Cisco Nexus 7010 работят с NX-OS - изцяло модулна операционна система, която позволява независимост между процесите работещи в едно физическо устройство. Поради наличието на отделни софтуерни модули в



архитектурата на Nexus 7010 изцяло се набляга на виртуализация на отделни процеси, което позволява от своя страна да се постигне логическо разделяне на отделни виртуални комутатори (VDC - Virtual Device Contexts).



Създавайки отделен виртуален комутатор се създава отделно логическо устройство. По този начин може да бъдат намалени разходите за допълнително оборудване, електрозахранване и климатизация в изчислителния център, като се запази търсената функционалност – логическо разделение на отделните сегменти в комуникационната инфраструктура. Всеки VDC(виртуален комутатор) притежава следните параметри:

- Всяко VDC представлява отделно устройство с предварително заделени физически и логически ресурси;
- Всяко VDC има отделни процеси за управление;
- Всяко VDC работи с независим от другите VDC софтуер.

За да се постигнат целите на стратегическите инициативи, опорните устройства в двата изчислителни центъра ще бъдат разделение на следните виртуални контексти:

- Core VDC – опорен контекст, който играе ролята на Layer 3 гръбнак на комуникационната инфраструктура;
- OTV VDC – контекст за осигуряване на Layer 2 свързаност между двата основните изчислителни центъра на БНБ;
- Datacenter VDC – контекст, който служи за осигуряване на мрежовата свързаност в сървърния сегмент на мрежата;
- Admin VDC – основен контекст за управление на опорните устройства Nexus 7010.



3.1.2. Едновременна работа на информационните системи в два изчислителни центъра

Основен приоритет при развитието на информационните системи на БНБ осигуряването на едновременната им работа в двата основни изчислителни центъра – Централно управление и Касов център. За да се постигне това е нужно комуникационната инфраструктура да бъде подготвена да отговори на всички изисквания, които и поставят приложенията, сървърните системи и системите за съхранение на данни.

Високоскоростна свързаност

За да се гарантира коректната едновременна работа на информационните системи в двата изчислителни центъра на БНБ е необходимо осигуряването на високоскоростна връзка между тях. Тази свързаност трябва да бъде с висока степен на надеждност и да позволява гъвкав пренос на различни мрежови технологии. Едновременно с това тя трябва да бъде резервирана и да позволява възстановяване при отпадане на една от линиите за изключително кратки интервали от време.

Тази свързаност между двата изчислителни центъра е осигурена, като за целта се използват 6 броя 10Gbps връзки, разпределени между двете двойки опорни комутатори Nexus 7010. За преносът им се грижи специализирано DWDM оборудване, което осигурява и преносът на Fiber Channel трафика между системите за съхранение на данни.

За обезпечаването на бъдещите системи и техните нужди за безпроблемна едновременна работа в двата центъра за обработка на данни е предвидена възможността за надграждане на линиите между тях, като за целта може да се използва съществуващото оборудване:

- Опорните комутатори Cisco Nexus 7010 разполагат със свободни слотове за модули с интерфейси, като имат възможност за добавяне на такива, поддържащи 100Gbps;
- DWDM устройствата, които осигуряват свързаността между двата изчислителни центъра могат да се надградят за да осигурят допълнителни канали за връзка за нуждите на комуникационното оборудване и системите за съхранение на данни.

Защита на предаваната информация

Връзката между двата изчислителни центъра на БНБ е от основно значение и през нея ще бъде пренасяна изключително критична за работата на банката информация. При използването на Dark Fiber оптични влакна и DWDM технологията се намалява значително риска от злонамерени действия и кражба на информация при предаването ѝ. Въпреки това тя се предава с чист вид и не е защитена с помощта на криптиране, което оставя минимална теоретичната възможност за кражбата на информация.

За повишаването на нивото на сигурност при предаване на данни между двата изчислителни центъра се препоръчва използването на технологии за криптиране на данните. С



тяхна помощ ще се постигне изключително високо ниво на сигурност. Предвид високите скорости на трансфер на данни между двата центъра и изискванията на приложенията за ниски закъснения между тях е необходимо да бъдат използвани технологии, които позволяват криптиране със скоростта на предаване на данните.

За да се гарантира сигурността на предаваната информация се налага се използването на а устройства поддържащи следните технологии:

- Криптиране на 1 Gbps Ethernet линии със скоростта на предаване на данните на Layer 2 – прозрачно за всички системи на банката;
- Криптиране на 10 Gbps Ethernet линии със скоростта на предаване на данните на Layer 2 – прозрачно за всички системи на банката;
- Криптиране на Fiber Channel със скоростта на предаване на данните, което е прозрачно за системите за съхранение на данни, с възможност за работа при скорости от 2/4/8/10 и 16-Gbps.

Използването на подобни технологии осигурява високоскоростно криптиране на данните между двата изчислителни центъра на БНБ, като това става прозрачно за приложенията и със скоростта на трансфер на данните.

Към момента в БНБ се използва технологията на Cisco за криптиране – MACsec, чрез която се извършва защита на предаваната информация по всички Ethernet канали между двата изчислителни центъра. За да се осигури максимално ниво на защита ще бъде внедрено мрежово SAN оборудване, което поддържа технологията Cisco TrustSec Fibre Channel Link Encryption позволяващата криптиране на Fiber Channel със скорости 2/4/8/10 и 16-Gbps.

Балансиране на натоварването и повишаване на сигурността

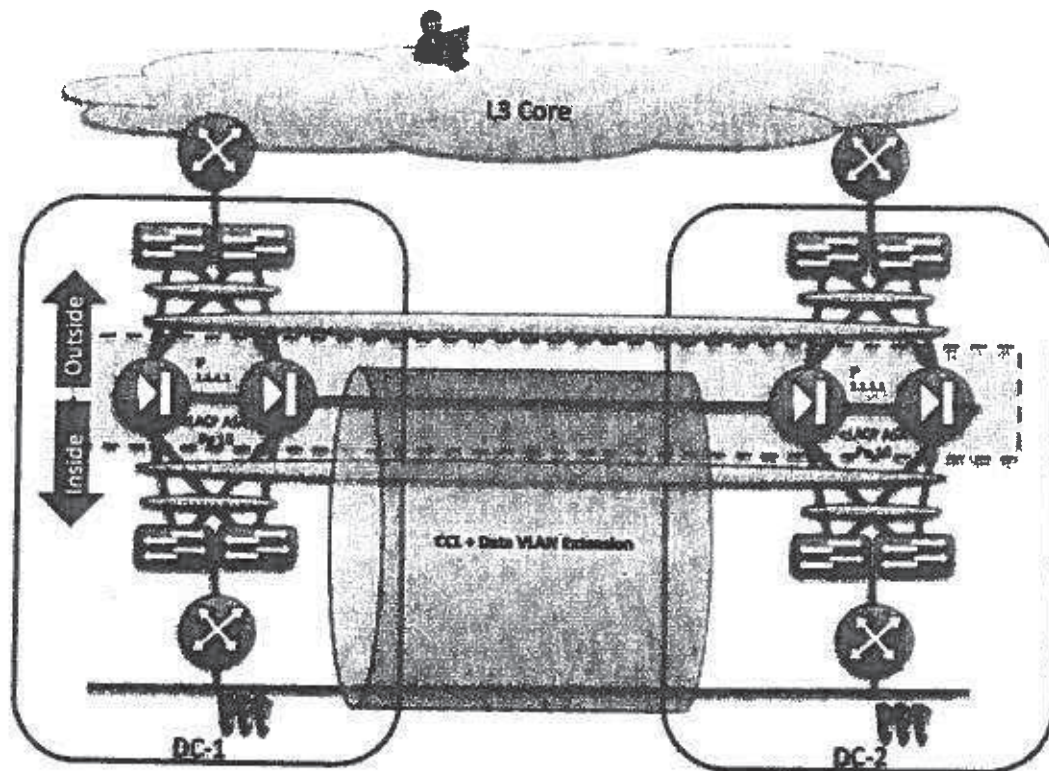
При изграждането на два изчислителни центъра, които трябва работят едновременно, е необходимо използването на технология, която да позволи разпределянето на заявките на клиентите към двата центъра. Технологията и респективно устройствата, които я поддържат трябва да позволяват балансиране на клиентския трафик между двата изчислителни центъра на БНБ.

За да се осъществи това, ще се използва технология, чрез която няколко защитните стени се обединяват в един логически клъстер. В случая ще се използват 4 броя защитните стени Cisco 5585X, разположени в две двойки в двата изчислителни центъра на БНБ. Двете двойки устройства ще се представят за една логическа защитна стена за всички останали устройства в мрежата на БНБ. По този начин ще се постигнат едновременно две от основните цели при изграждането на модерни изчислителни центрове – високи нива на сигурност и разширена функционалност, без това да внася допълнително сложност в комуникационна инфраструктура.

Cisco технологията за клъстериране на защитни стени Cisco 5585X разполага с вградени механизми за разпределение на клиентските заявки и може да играя и роля на устройство за

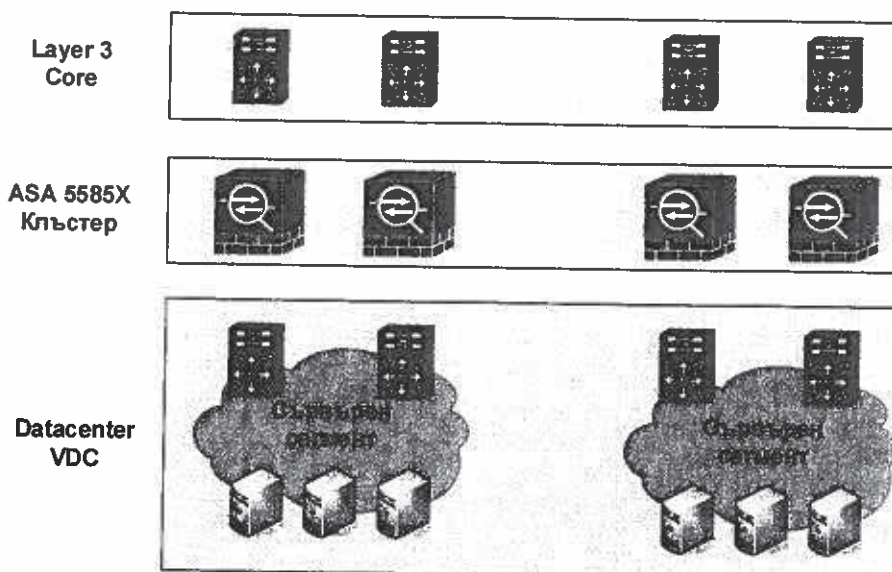


балансиране на натоварването. За да се гарантира коректното определяне на работоспособността на системи и приложенията и това, накъде трябва да бъде насочван трафикът, ще спомогнат вградените механизми в системите за виртуализация.



За да се постигне това, защитните стени ще бъдат разположени на Layer 3 пътя на трафика между Core сегмента в мрежата на БНБ и планирания за изграждане Datacenter сегмент. По този начин целият трафик от основните приложения на БНБ ще обработван от клъстера от защитните стени Cisco 5585X. Самият клъстер разполага с механизми, чрез които устройствата разпределят и обработват трафика помежду си, като за останалите части от мрежата се представят като едно логическо устройство и така не внасят допълнителна сложност дизайна.

Допълнително ниво на сигурност предлага и вградената в защитните стени Cisco 5585X Intrusion Prevention система от най-висок клас – Cisco FirePOWER. С помощта на IPS системата могат да бъдат предотвратени най-често използваните атаки срещу приложенията в сървърния сегмент, като това ще повиши значително информационната сигурност в информационната инфраструктура на БНБ.



Технология за балансиране на трафика към изчислителните центрове

Част от сървърите и приложенията на БНБ, които трябва да бъдат достъпвани от външни за банката потребители са разположени в Интернет периметъра, в съответните DMZ зони. За да се осигури едновременната им работа в двата изчислителни центъра, трябва да бъдат предвидени устройства, които да разполагат с механизми за постоянно следене на наличността им и в случай на проблем, да прехвърлят всички клиентски заявки към центъра, който е в момента е наличен. Тези устройства ще се използват и за пренасочване на заявките към третия център, който ще бъде изграден и ще служи за възстановяване на основните системи на банката в случай на инциденти и отпадане на основните два.

За да се гарантира високото качество на услугата и да се предотврати възможността за изпращане на заявки към приложения, които са натоварени или не са активни е необходимо устройствата за балансиране на натоварването към изчислителните центрове да могат да получават информация за натоварването и наличността на приложенията и на база на тази информация да пренасочват клиента към съответния център. Те могат да наблюдават зададените им параметри на сървърите и приложенията и да изпращат информация към устройствата за балансиране на ниво изчислителни центрове.

При използване на подобен тип решения прехвърлянето на заявките остава прозрачно за потребителите. Предимство в случая е възможността бързо и лесно да се пренасочи клиента към един от изчислителните центрове. Това решение може да се използва освен в случаите на проблем, така и в случай при необходимост от прекъсване на услугите в някой от центровете при планирана профилактика.

Осигуряване на защита за услугите за външни клиенти



Тенденциите при развитието на приложенията в глобален мащаб са преминаване към WEB базиран достъп. Това се налага най-вече от факта, че този тип достъп е универсален и независим от използваните устройства, операционни системи и програми. Тази тенденция се наблюдава и в Българска Народна Банка, където голяма част от приложенията са WEB базирани.

Все по-честото използване на WEB приложения и голямото развитие на средствата за атаки към тях налага осигуряването на тяхната защита. Също така естеството на работа на WEB приложенията налага едновременно с това да бъде осигурявана защитата на потребителите, които ги използват. За целта в комуникационната инфраструктура на БНБ е необходимо да се имплементира специализирано решение за защита на ниво WEB приложения.

Специализираната система, която ще бъде интегрирана в мрежата на БНБ трябва да отговаря на критериите на най-използваните стандарти за информационна сигурност при организации работещи във финансовия сектор. Тя трябва да поддържа надеждни механизми, които да защитават приложенията и Web услугите в БНБ от най-често използваните атаки. За да осигури надеждната защита на приложенията, специализираната система за Web защита трябва да инспектира целият трафик на приложно ниво.

Освен защитата на приложенията системата трябва да разполага с механизми за защита на потребители от злонамерени действия срещу тях. Все по-често в Интернет пространството се наблюдават атаки, които използват доверието на потребители към Web приложенията на финансови институции като БНБ, с цел да предприемат злонамерени действия срещу тях. За тази цел специализираната система за защита на Web приложенията трябва да осъществява защита както на приложенията, така и от атаки към потребителите.

3.1.3. Комуникационна инфраструктура за Центъра за възстановяване след инциденти

Осигуряване на комуникационната инфраструктура за нуждите на информационните системи в центъра за възстановяване след инциденти(DRC – Disaster Recovery Center) е първата стъпка при изграждане му. За надеждната работа на критичните системи и непрекъснатостта на финансовите и бизнес услугите на Българска Народна Банка е необходимо да се осигури, както обезпеченост на самите приложения и системи, така и на основните работни места.

За целта, в при обособяването на бъдещия център за възстановяване след инциденти ще бъде изградена комуникационна инфраструктура отговаряща на следните условия:

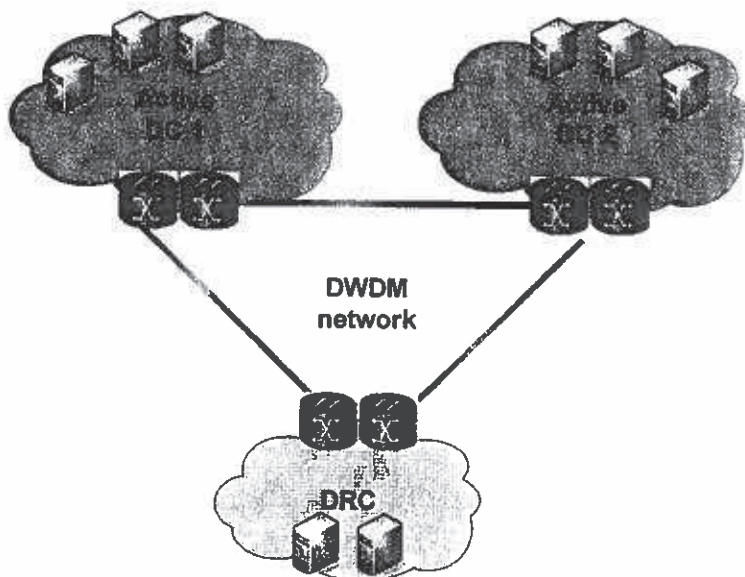
- Да бъде изградена локална мрежова инфраструктура;
- Да бъде обособена инфраструктура за клиентски достъп;
- Да бъде обособен сървърен сегмент;
- Да се осигурят необходимите MAN и Internet свързаност, които да гарантират достъпа на партньорите на БНБ до основните системи;
- Ще се осигури високоскоростна оптична свързаност с двата основни изчислителни центъра на БНБ;

- Ще се осигурят технологии и механизми за прехвърляне на клиентските заявки към този изчислителен център в случай на инцидент.

Осигуряване на DWDM свързаност към Центъра за възстановяване след инциденти

При изграждането на комуникационната инфраструктура в Центъра за възстановяване след инциденти е необходимо да се осигури надеждна и високоскоростна оптична връзка към основните изчислителни центрове на БНБ. За да се осигури оптичната свързаност, както за нуждите на сървърните системи, така и за системите за съхранение на данни е необходимо използването на DWDM технология, която да позволява използването на едно оптично влакно за множество цели. По този начин една оптична свързаност се превръща в множество независими виртуални оптични връзки като основното предимство е, че DWDM технологията е независима по отношение на предаваните протоколи и битрейт.

Основните технологии за пренос на данни в мрежата на БНБ са Ethernet и Fiber Channel технологиите. Чрез използването на DWDM оборудване за осигуряване на връзка между двата изчислителни центъра на БНБ и Центъра за възстановяване след инциденти ще се позволи едновременния пренос на няколко Ethernet и Fiber Channel канала по оптични влакна от тип „dark fiber“. С тази технология ще се предостави възможност да се пренасят едновременно Ethernet канали със скорост от 1 и 10 Gbps и Fiber Channel канали със скорости от 1,2, 4 и 8 Gbps по начина, по-който това се извършва и към момента между двата основни изчислителни центъра на банката.



Осигуряване на свързаност и оборудване за достъп до към Центъра за възстановяване след инциденти

Важно условие при изграждане на Центъра за възстановяване след инциденти и работата на критичните приложения, които ще бъдат резервирани в него е да се осигурят необходимите MAN, Internet и VPN свързаност, които да гарантират достъпа на партньорите на БНБ до основните системи. Това предполага, както осигуряването на резервна свързаност в този център, така и необходимото оборудване, което да може осигури нужната функционалност, като съответното криптиране за изграждане на защитените VPN връзки, Internet маршрутизиране и т.н.

При изграждането на Центъра за възстановяване след инциденти е необходимо да бъдат създадени процедури, които да вземат предвид партньорите на Българска Народна Банка и начина им ползване на услугите, които да определят достъпа до основните системи в него. Тези процедури трябва да съобразят типовете свързаност на клиентите към основните изчислителни центрове на БНБ и възможните механизми за прехвърляне на техните заявки към Центъра за възстановяване след инциденти в случай на нужда и отпадане на основните.

Обособяване инфраструктура за клиентски достъп

Комуникационната инфраструктура, която ще служи за потребителски достъп в сградата, в която е разположен изчислителния център за възстановяване след инциденти, трябва да бъде изградена спрямо най-добрите практики и да следва дизайна, който е одобрен от Българска Народна Банка и се използва в централата и касовия център. По този начин ще се гарантира високоскоростния, надежден и защитен достъп до ресурсите и услугите. Тя трябва да е проектирана със съответната многослойна архитектура и да разполага с необходимите устройства и обезпечаващ ги софтуер, които да осигурят необходимите функционалност и висока производителност.

За да се осигури безпроблемната работа на служителите и да се улесни процеса на работа на временните работни места при инциденти се препоръчва използването на две технологии, които ще подпомогнат процеса. Едната е използването на виртуална десктоп инфраструктура (Virtual Desktop Infrastructure), другата е осигуряването на безжичен достъп до информационните ресурси за мобилните работни станции. Виртуален десктоп или виртуална десктоп инфраструктура (Virtual Desktop Infrastructure) е технология, която позволява работната среда на потребителя се съхранява на сървър/сървъри, вместо на локалния компютър или друго изчислително устройство. По този начин ще може да се гарантира работата на потребителите от различни работни станции в случай на нужда.

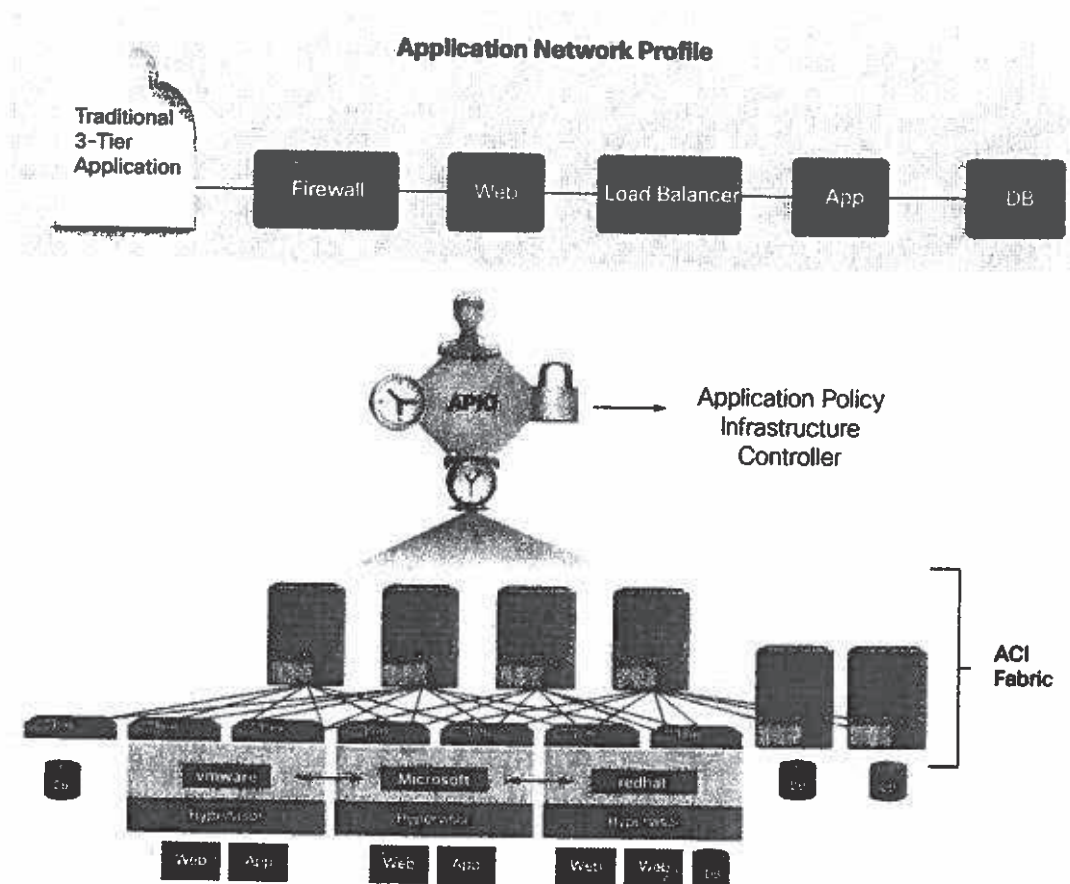
Осигуряване на допълнителна гъвкавост на работните станции може да се постигне и с изграждането на среда за безжичен достъп до информационните ресурси. Важно условие при изграждането на подобна среда е да се гарантира информационната сигурност, като това включва използването на редица системи и технологии:

- Система за управление на безжичните точки за достъп;
- Система за управление на мобилните потребители;
- Система за предотвратяване на изнасяне на конфиденциална информация и д.р.

3.1.4. Механизми за автоматизация за провизиране на информационните системи

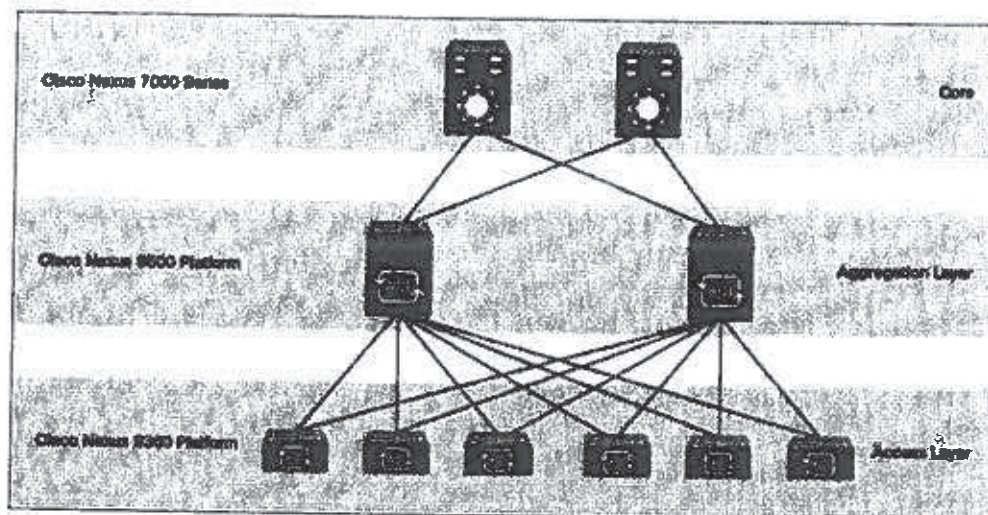
Внедряването оборудване от класа на Cisco Nexus 9000, което поддържа Cisco ACI архитектурата ще подобри процеса на внедряване на приложения в инфраструктурата на банката, информационната сигурност и мрежовите услуги. За това ще спомогне единната платформа за управление, която ще взаимодейства, както с мрежовото оборудване, така и със системите за виртуализация и съхранение на данни. Основните предимства на Cisco ACI архитектурата са:

- Системи архитектура, която дава възможност на цялостна визия за приложения и тяхната работа в мрежата, с централизирано управление и наблюдение в реално време на състоянието на приложенията, приложима както при физически, така и при виртуални среди
- Единна платформа за управление на физически, виртуални и cloud-базирани среди;
- Комбинира се производителността на хардуерните технологии и гъвкавостта, която предлага софтуера;
- Значително улесняване на процеса на имплементация и експлоатация чрез използването на единни политики, управление и модели, които биват използвани едновременно от мрежовите, сървърните и storage ресурсите;
- Отворени API(Application Programming Interface) и стандарти, които позволяват на разработчиците да голяма гъвкавост и лесна интеграция на приложенията в ACI инфраструктурата.



Основно предизвикателство пред сложни виртуални среди, като тази която ще бъде изградена в БНБ е интегрирането на управлението; лесното конфигуриране; унифицирането на конфигурациите; намаляването на грешки от провизиране; мобилност на виртуалните машини; възможност за управление на инфраструктура директно от апликациите; лесно сегментиране на виртуалния ресурс; виртуални мрежови функции. Всичко това се решава с модерни решения носейки на шумялото име Software Defined. В конкретния случай говорим за мрежа и съответно Software Defined Network (SDN) решения. Cisco ACI е такова решение, което ни позволява всичко описано по-горе.

Cisco ACI е софтуер, който работи в пряка интеграция и зависимост от комутатори от висок клас Nexus 9000. Nexus 9000 трябва да застане между сървърната инфраструктура и наличните комутатори Nexus 7000, както е показано на следващата фигура.



Cisco ACI ще се интегрира с VMWare клъстера в банката и ще позволи интегрирано управление, лесно конфигуриране и унифицираност на конфигурациите (възползвайки се от шаблони и не пряко конфигуриране на самите устройства от човек). За Cisco ACI е значещо IP-то на дадената машина и нейните услуги, съответно шаблоните и мрежовите политики за даденото IP се местят с него в цялата инфраструктура. Това позволява неограничена мобилност на виртуалните машини. Разбира се Nexus 9000 трябва да се имплементира и в трите сайта на банката.

3.1.5. Стъпки на имплементация

Долу изброените детайлни дейности не са с посочена индикативна продължителност защото зависят от много фактори, включително и наличието на време от страна на служителите на банката. Въпреки това спрямо опитана ни смятаме, че посочения период за цялата стъпка е реалистичен и изпълним.

СТЪПКА 1 – СЪОБРАЗЯВАНЕ НА ДИЗАЙНА В ОСНОВНИТЕ ИЗЧИСЛИТЕЛНИ ЦЕНТРОВЕ С НАЙ-ДОБРИТЕ ПРАКТИКИ И ПРЕМИНАВАНЕ КЪМ ЕДНОВРЕМЕННА РАБОТА

Стъпка 1 се фокусира в/у текущата нужда от редизайн на мрежовата инфраструктура в основните изчислителни центрове на БНБ, които цели сегментиране на различните части от мрежата спрямо най-добрите практики и повишаване на сигурността в сървърния сегмент. При успешното ѝ изпълнение ще се постигне възможност за работа на двата сайта едновременно, като по този начин всички заявки към сървърния сегмент могат да се обработват, както от приложенията в Централата на БНБ, така и от Касовия център.

Стъпка 1 включва освен работа по мрежовата част и анализ на приложенията в работещи в инфраструктурата на БНБ. Тези стъпки могат да бъдат изпълнени, за да може да се прехвърлят приложенията в съответните сървърни сегменти, да се определят политиките за сигурност и да се конфигурира мрежовото оборудване:



- Анализиране на всички сървърни приложения, които работят в информационната инфраструктура на БНБ;
- Определяне на възможностите им за виртуализация и изискванията им към сървърната и мрежовата инфраструктура;
- Определяне на основни типове приложения, по които да се класифицират и обединят работещите в банката;
- Определяне на принадлежността сървърните приложения към основните типове;
- Анализ на необходимостта от Layer 2 свързаност между двата изчислителни центъра за конкретните приложения;
- Анализ на изискванията към свързаността на сървърите и системите за съхранение на данни между двата изчислителни центъра.

В следващите точки са предложени детайлните дейности по редизайна на мрежовата инфраструктура в основните изчислителни центрове на БНБ:

- Изграждане на сървърен сегмент с помощта на функционалността на Nexus 7010 устройствата – Datacenter VDC;
- Инсталиране на клъстера от защитни стени ASA 5585X в двата изчислителни центъра;
- Изграждане на свързаност между Core и Datacenter сегментите на мрежата, която да преминава през клъстера от защитни стени;
- Прехвърляне на необходимите мрежови връзки от сървърите към обособеният Datacenter сегмент;
- Изграждане на Layer 2 свързаност между двата изчислителни центъра за сървърните сегменти, за които има такава необходимост;
- При необходимост, изграждане на допълнителна свързаност за нуждите на сървърите и системите за съхранение на данни;
- Извършване на тестове с приложение, за коректната работа на двата изчислителни центъра в Active/Active режим;
- Поетапно прехвърляне на приложенията в съответните сървърни сегменти съгласно класификацията има по общи признаци;
- При необходимост промяна на мрежовата адресация на приложенията, с ясната идея, че това може да доведе до преправяне на кода на приложенията;
- Поетапно описание на политики за сигурност за всяко от приложенията в клъстера от защитните стени;
- Тестове на работата на двата изчислителни центъра в Active/Active режим;
- Обособяване на сегмент за клиентски достъп;
- Прехвърляне на комутаторите за достъп в сегмента за клиентски достъп;

Очакваната продължителност на тази стъпка е в рамките на 12 календарни месеца

С приключването на Стъпка 1, БНБ ще:

- Ще бъде оптимизирана и сегментирана мрежовата инфраструктура съобразявайки се с най-добрите практики;



- Ще се обособят сървърни сегменти, в които ще се разположат приложения, класифицирани по общи признаци, за които могат да се наложат съответните политики за сигурност;
- Ще бъде повишена мрежовата сигурност и ще бъдат наложени стриктни политики за достъп до приложенията в сървърния сегмент;
- Приложенията ще започнат едновременна и равнопавна работата в двата основни изчислителни центъра на БНБ, като при проблем или планирана профилактика в кой да е от тях, няма да има прекъсване на услуги.

СТЪПКА 2 – ИЗГРАЖДАНЕ НА ИНФРАСТРУКТУРА ЗА РАБОТА НА ДВА САЙТА ЗА ПРИЛОЖЕНИЯТА, КОИТО СЕ ДОСТЪПВАТ ОТ ВЪНШНИ ЗА БАНКАТА ПОТРЕБИТЕЛИ И СА РАЗПОЛОЖЕНИ В ИНТЕРНЕТ ПЕРИМЕТЪРА

Стъпка 2 се фокусира в/у изграждането на надеждна инфраструктура в Internet периметъра на двата изчислителни центъра на БНБ, която да обслужва заявките от външни за банката потребители към системите разположени в съответните демитализирани зони.

В следващите точки са предложени детайлните дейности по осигуряването на системите в DMZ зоните на основните изчислителни центрове на БНБ:

- Осигуряване на необходимото оборудване за изграждане на Internet периметър;
- Изграждане на Internet периметър в Касовия център на БНБ;
- Осигуряване на необходимата свързаност – Internet, MAN и т.н. за пълното дублиране на Internet периметъра в Касов център на БНБ;
- Обособяване на съответните DMZ зони Касовия център на БНБ в съответствие с тези в централата на банката;
- Прилагане на политики за сигурност за DMZ зоните, съответстващи на тези в централата на БНБ;
- Дублиране на системите в Касовия център на БНБ;
- Извършване на тестове за коректната едновременна работа в два изчислителни центъра;
- Осигуряване на оборудване за балансиране на натоварването и WEB защита за нуждите на двата Internet периметъра на БНБ;
- Поетапно прехвърляне на заявките към приложенията в през системите за балансиране на натоварването и WEB защита;
- Извършване на тестове за коректната едновременна работа в два изчислителни центъра.

Очакваната продължителност на тази стъпка е в рамките на 8 календарни месеца

С приключването на Стъпка 2, БНБ ще:

- Ще бъде изградена инфраструктура в Internet периметъра на двата изчислителни центъра на БНБ и ще бъдат обособени съответните DMZ зони;



- Ще се осигури едновременната работа на два сайта на приложенията, които се достъпват от външни за банката потребители, като трафика към тях ще бъде балансиран с помощта на интелигентни механизми за разпределяне на натоварването и защита на WEB приложенията.

ИЗСТЪПКА 3 – ИЗГРАЖДАНЕ НА КОМУНИКАЦИОННА ИНФРАСТРУКТУРА ЗА НУЖДИТЕ НА ЦЕНТЪРА ЗА ВЪЗСТАНОВЯВАНЕ СЛЕД ИНЦИДЕНТИ

Стъпка 3 се фокусира в/у изграждането на цялостната комуникационна инфраструктура за нуждите на Центъра за възстановяване след инциденти, който ще осигури работата на критичните за Българска Народна Банка системи в случай на отпадането им в основните изчислителни центрове на БНБ в централата банката и в Касов Център.

Следващите точки са предложени детайлните дейности по осигуряването на системите в DMZ зоните на основните изчислителни центрове на БНБ:

- Осигуряване на необходимото оборудване за изграждане на мрежовата инфраструктура;
- Обособяване на съответните мрежови сегменти – сървърен сегмент, гръбнак на мрежата, сегмент за достъп;
- Изграждане на оптична свързаност към двата основни изчислителни центъра на БНБ;
- Изграждане на съответните Internet, MAN, VPN свързаности;
- Осигуряване на необходимото оборудване за изграждане на основните връзки към центъра – DWDM, маршрутизатори, защитните стени, VPN устройства, системи за балансиране на натоварването и т.н.
- Свързване на Центъра за възстановяване след инциденти към двата основни изчислителни центъра;
- Свързване на всички системи към мрежовата инфраструктура и извършване на съответните функционални тестове;
- Преминаване към активна работа на Центъра за възстановяване след инциденти

Очакваната продължителност на тази стъпка е в рамките на 6 календарни месеца

С приключването на Стъпка 3, БНБ ще:

- Ще бъде изградена комуникационна инфраструктура за нуждите на Центъра за възстановяване след инциденти, както и необходимите връзки - към двата основни изчислителни центъра в София, както и MAN и Internet свързаност;
- Ще се осигури надеждна инфраструктура, която да осигури работата на критичните системи за банката в случай на инцидент и отпадане им в основните центрове с София.

СТЪПКА 4 – ВНЕДРЯВАНЕ НА CISCO APPLICATION CENTRIC INFRASTRUCTURE

Стъпка 4 се съсредоточава върху внедряване на Cisco ACI решението плюс Access и Aggregation слой за нуждите на сървърната инфраструктура базирани на Nexus 9000.



Следващите точки са предполагаеми детайлните дейности по внедряване на ACI решението:

- Дизайн за внедряване на Nexus 9000 на ниво access и aggregation в работен режим на обикновени комутатори;
- Внедряване на Nexus 9000 в DRC сайта;
- Тестове на дизайна и решението;
- Внедряване на Nexus 9000 в другите два сайта;
- Анализ на всички виртуални машини в свързаната инфраструктура, техните услуги и текущите мрежови настройки, включително политики за достъп на мрежово ниво;
- Дефиниране на профили за всяка една от машините;
- Тестване на профилите и тяхната мобилност в рамките на един сайт в DRC сайта;
- Интеграция с VMWare VCenter Server
- Тестване за създаване и промяна на съществуващи машини от гледна точка мрежови настройки, ползвайки VMWare VCenter Server
- Документиране на пълното решение;
- Имплементиране на пълното решение във всички сайтове;
- Приемни изпитания.

Очакваната **продължителност** на тази стъпка е в рамките на **12 календарни месеца**.

С приключването на Стъпка 4, БНБ ще:

- Има внедрено Software Defined Network решение, което ще води след себе си до следните позитиви и възможности:
 - интегрирането на управлението на x86 виртуализацията и всички Data Center мрежови устройства;
 - лесното конфигуриране – VMWare VCenter и ACI;
 - унифицирането на конфигурациите – посредством шаблони;
 - намаляването на грешки от провизиране;
 - мобилност на виртуалните машини;
 - възможност за управление на инфраструктура директно от апликациите;
 - лесно сегментиране на виртуалния ресурс;
 - виртуални мрежови функции .

3.2. Стратегия за развитие на информационната сигурността

3.2.1. Информационна сигурност (дефиниция/инструменти/мерки)

Използването на информационните технологии за обработка и съхранение на чувствителна информация отдавна е стандарт по целия свят. Консумация на ИТ услугите и развитието на информационните технологии като цяло, водят до различни перспективи и

допринасят за по-добра работа, повече гъвкавост и сериозно развитие на всяка една организация. В днешно време информация вече се съхранява на дискови масиви, а не в папки и кабинети. Това съвсем естествено води до логичния въпрос – как тази информация се защитата от неоторизирани достъп, загуба и/или изтичане.

Като публична организация и пример за банковата система, Българска Народна Банка би следвало да полага необходимата грижа и отговорност към това да спазва законови рамки и стандарти както и световни добри практики, които гарантират правилното осигуряване и защита на лични данни, финансови информации и други данни, с които не е разрешено свободно ползване.

Концепцията за информационна сигурност представена в тази глава, приема горе посоченото като факт и определя като цел на информационната сигурност в БНБ, тя да е на максимално високо ниво независимо от това дали чувствителната информация се използва, пренася или съхранява. Целта на тази секция е да представи някои от основните технически изисквания за всяко едно състояние на информацията и това как тя да бъде защитена.

Защита по време на използване на чувствителна информация (Data in Use)

Дефинира се, че една информация се използва, когато тя е на разположение на крайни служители или клиенти. Такива примери могат да са обработка на документи, работа с бази данни, използване на различни видове софтуер за достъп до тези специфична информация която е маркирана като чувствителна. Защитата на информацията, при използване се фокусира в/у защита на крайните станции, на които тя се обработва. Някои от основните технически подходи за защита и контрол на крайни устройства са изброени долу

- **Centralized Endpoint Protection** – този вид решения предоставят защита и контрол на крайни работни станции и/или преносими компютри. В тези решения се включват
 - Antivirus-на защита
 - Защитни стени
 - AntiMalware защита
 - Отдалечен контрол на Операционна Система (Window, Linux, Mac)
- **Enterprise Mobility** – класическите решения за контрол и управление на крайни станции, еволюират и се съобразяват със навлизащите, много и разнообразни мобилни устройства, които все повече се ползват за достъп до корпоративна и чувствителна информация. Тези устройства се характеризират с голямо разнообрази и трудно управление. Решенията от типа Enterprise Mobility Management разширяват и/или се интегрират с функциите на Centralized Endpoint Protection решенията като обхващат и мобилни устройства и таблети. Поради спецификата на работа с в такива среди, решенията предоставят и допълнителни функционалности като:

- Контейнери в мобилните операционни системи за достъп до корпоративна информация
- Възможности за локализация на устройствата посредством GPS и мобилни комуникации
- Контрол на мобилните услуги (разговори, използване на данни в чужбина и други)
- Контрол на документите и приложенията на мобилните устройства
- **End-host Encryption** – добра практика е да се използват решения за криптиране на дисковете на крайни устройства които се изнасят от банката.
- **Centralized Identity Management** – големия брой на информационни системи и служители налага използването на решения за контролиране на достъпа до информация, историческата справка за това, кои използват информация и други нужди свързани с идентичността на клиентите. Решения от този род на производители като Microsoft и Novell, се фокусират върху автентикацията, оторизацията и обработването на тези политики към директориини услуги за управление на електронни профили на служители.

Защита на информацията в бази данни, файлови сървъри и други решение за съхранение (Data at Rest)

- **Vulnerability Management** – целта на Vulnerability Management решенията е постоянно да „изпитва“ инфраструктурата, в която се обработва и съхранява чувствителна информация.
- **Right Management System**
- **Database Security** – решенията за сигурност на бази данни, включват в себе си контролиран достъп до информацията на базите, проследяемост и аналитичност на действията с информацията в базите, както и допълнителни функционалности като криптиране на свързаност.

Защита на информацията по време на пренос (Data in Motion)

- **VPN** - виртуални тунелиране с допълнително криптиране е де-факто стандарт за пренос на данни от край до край една комуникационна инфраструктура
- **Encryption** – използване на технически похвати за защита на преносими устройства като USB или други дискове.
- **Mail/Web Security** – за да се защитят стандартните канали за пренос на информация като mail и web е препоръчително и в зависимост от стандартите – задължително, да се наблюдава входящия и изходящ трафик.

Изброените горе технологии и решения покриват голяма част от техническите изисквания за защита на информацията според добрите практики на производителите, както и



стандарт. Крайната цел на банката трябва да е да подреди правилните процеси и технологии за да достигне до желания резултат на сигурност.

Към горе изброените решения трябва да бъде добавено и така наречената Advanced SIEM система (Security Information and Event Management). Тя ще даде възможност за събиране на журнална информация от различните системи (не само за осигуряване на информационна сигурност), пакети от мрежата и тяхното правилно корелиране с цел анализ, идентифициране на аномалии и така наречения forensic analysis.

3.2.2. Концепция за развитие

Отбелязаните от банката в тръжната документация приоритетни инициативи ясно очертават пътят на развитие на информационните система в банката и тяхната основна и засилваща се роля в процесите и дейностите в нея. Лесно може да се направи извод, че БНБ има за цел повишаване на нивото на информационна сигурност и постоянното развитие в тази област. Изброените в предходната точка средства за защита на информацията представляват един сравнително пълен списък с мерки и инструменти, които трябва да бъдат имплементирани във всяка една организация, за която информационната сигурност е важна. В случая с БНБ част от мерките вече са имплементирани. В тази точка целим да предоставим конкретика, за това кои мерки и инструменти трябва да бъдат имплементирани или поне обсъдени сериозно. Приоритетни инициативи в областта на информационната сигурност е удачно да бъдат:

- Постоянен анализ и управление на ИТ пропуски в сигурността (Vulnerability Management)
- Наблюдение и контрол на електронната информация – Data Leakage Prevention (DLP)
- Наблюдение и анализ на информационни събития
- Система за управление и наблюдение на електронната идентичност на служителите – Identity Management
- Решение за контрол на електронната информация – Right Management System
- Контрол и защита на мобилни устройства – Enterprise Mobility Management

Система за анализ и управление на ИТ пропуски в сигурността (Vulnerability Management)

Целта на това решение е да предостави на БНБ, Vulnerability Management система която допринася за откриването и защитата на инфраструктурата от пролуки в сигурността на операционни системи, сървъри, виртуални и комуникационни среди, и софтуерни решения.

Опита ни в сферата ни кара да предложим като евентуално конкретно решение Qualys Vulnerability Management. Qualys VM е облачно решение, което предоставя незабавно, глобална видимост къде ИТ системите могат да бъдат изложени на най-новите Интернет заплахи и как да ги защитим.

С помощта на Qualys VM, банката може да изгради пълен lifecycle на документиране на ИТ инфраструктурните си активи, да наблюдава заплахите на базата на вида крайни устройства

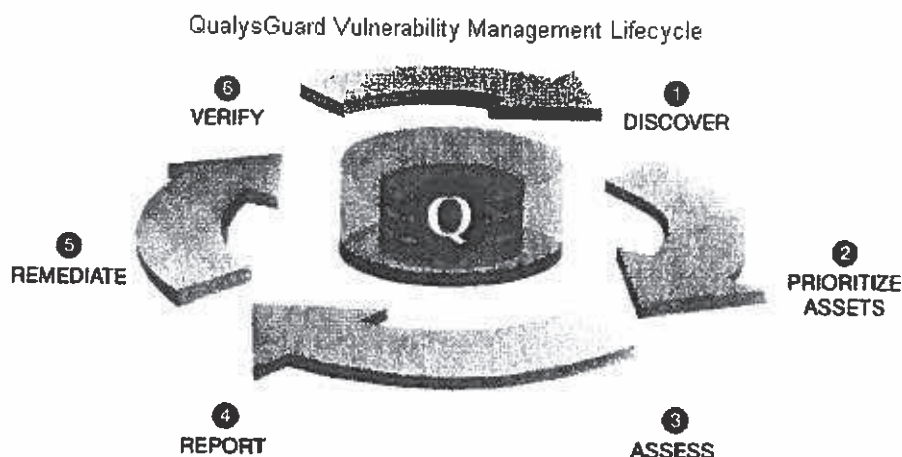


(компютри, сървъри, мрежови устройства и др.) и да изгради процес за правилното регулиране и премахване на тези заплахи.

Част от функционалността на решението включва

- Динамично обновяваща се База данни с регулираните активи
- Планирани сканирания за проблеми със сигурността на крайните активи
- Автоматично и ролево разпределяне на задачите на базата на заплахите и типа актив
- Специализирани процеси за сканирания на web базирани публични услуги
- Постоянно наблюдение на заплахите спрямо публичните услуги (Constant Monitoring)
- Гъвкавост в генерирането на различни доклади спрямо различни критерии (заплахи, активи, приравняване към различни международни стандарти (PCI, ISO2700x и др.)

Анализа и управлението на ИТ пропуските в сигурността трябва да бъде един постоянен процес, а не единичен или спорадичен акт. Фигурата по-долу представя концепцията възприета от Qualys като жизнен цикъл на един Vulnerability Management процес.



Система за наблюдение и контрол на електронната информация – Data Leakage Prevention (DLP)

Data Leakage Prevention е софтуерно решение, чиято цел е ефективно предпазване на клиентските данни, класифицирана информация или интелектуална собственост от напускане рамките на организацията както и вътрешен обмен между служители в случай, че гореспоменатите дейности са в разрыв с наложената политика за сигурност. Решението е насочено към ограничаване, и обучение на служителите за износът на информация чрез предварително дефинирани политики (методи) по следните начини:

- Проверка на съдържанието на изходящата поща за предварително дефинирана информация като конфиденциална и на прикачените файлове (документи) в



съобщението с опция за блокиране на изходящия мейл и нотификация на клиента чрез изскачащо съобщение;

- Проверка при опит за копиране на конфиденциални документи от локалния компютър на външни носители (USB, CD/DVD, FTP Server, IM software) с опция за блокиране на извършената операция и нотификация на клиента чрез изскачащо съобщение;
- Проверка на съдържанието въведено в web browser-a на клиентката машина както и clip board-a на операционната система (пример: функции за копиране на текст между различни файлове, в internet browser-a както и приложенията за комуникация през интернет - IM) с опция за блокиране на извършената операция и нотификация на клиента чрез изскачащо съобщение;
- Сканиране на вътрешни твърди дискове за поверителна информация с цел да се предприемат по-нататъшни стъпки за известяване на служителя за наличие на такава информация или преместване на документите в подсикурена директория (карантина) при което съдържанието на файлът на локалния компютър се замени с известие за предприетите мерки по подsigуряване на информацията;
- Проверка на съдържанието на документите при опит за принтиране с опция за блокиране на извършената операция и нотификация на клиента чрез изскачащо съобщение;

За да бъдат сведени до минимум грешните сработвания на системата и пропуските и за откриване на опити за изнасяне на информация е необходимо да се дефинират „политики“, които да описват типовете конфиденциална информация. Тези дефиниции се извършват на базата на методи за откриване на злоупотреби. Колкото по-богато е решението от към методи за откриване на злоупотреби толкова по-добро и гъвкаво е то. Съдейки от нашия опит бихме предложили, като евентуално решение за DLP, решението на Symantec.

Система за наблюдение и анализ на информационни събития

Днешните IT инфраструктури са по-големи и по-сложни от всякога, и защита им срещу злонамерен дейност е безкрайна задача. Организациите, които искат да защитят интелектуалната си собственост, защитят идентичността на клиентите им и да се избегне прекъсване на бизнес трябва да направи повече от наблюдение на събития (logs) или данни в мрежовия поток; нужен е метод за агрегиране и анализ на цялата информация с цел откриване на злонамерени действия. Решението за наблюдение и анализ на събития Security Information & Event Management (SIEM) може да служи, за да се съберат, нормализира и корелира налични данни по информационната инфраструктура. Резултатът е нещо, наречено интелигентна сигурност.

В основата на това решение е база данни, предназначена да улови данни в реално време на записите на събитията в информационния поток, разкривайки отпечатъци на кандидат-нападатели. SIEM е решение, което консолидира ежедневно данни от хиляди устройства, разпределени по цялата инфраструктура, съхранява всяка дейност в суров вид (raw format), и след това извършва корелационни действия за да се разграничат реалните заплахи от останалите действия и използване на електронната информация.

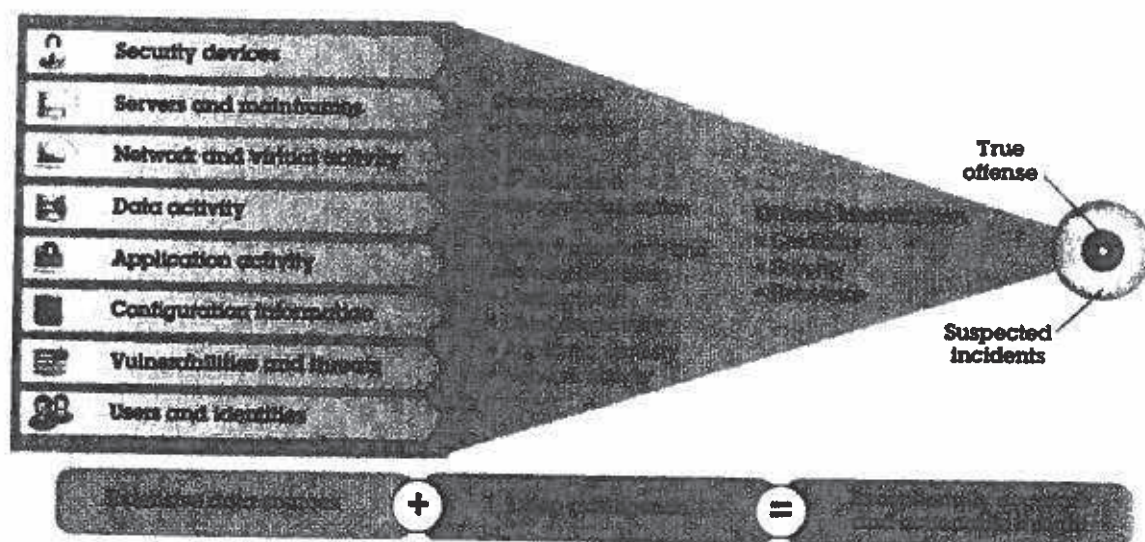
Добрите SIEM решения се характеризират с интуитивен потребителски интерфейс, който помага на ИТ персонала бързо да идентифицира атака. В това число се включва и възможност за възпроизвеждане на цяло събитие с цел задълбочен анализ.

Едно от световно доказалите се решения, с които ние работим е продуктът на IBM – QRadar. С цел пълнота на представянето ще изброим някои от основните характеристики на този продукт.

QRadar SIEM събира информация, която включва:

- Събития Сигурност: Събития от защитни стени, виртуални частни мрежи, системи за защита от интрузии и др.
- Събития Мрежа: Събития от комутатори, маршрутизатори, сървъри, крайни устройства и други информационни системи.
- Мрежови трафик: информация директно от комуникационната (физическа или виртуална) инфраструктура
- Действия на потребители или други IP базирани източници: информация агрегирана и получаваща от системи за управление на идентичността на потребителите или от решения за анализ на уязвимостите в инфраструктурата.
- Информация за Операционна система: име на доставчика и версия брой особености за мрежови активи
- Събития от приложения: Enterprise планиране на ресурсите (ERP) и други приложения свързани с работен процес или платформи за управление.

QRadar SIEM автоматично открива повечето устройства и източници на информация и събития и инспектира потока данни, за да открие и класифицира валидни сървъри (активи), приложения, протоколи, услуги, които те използват. Целта е приоритизиране на значещата информация и открояване на така наречения true offense. Илюстрацията по-долу изобразява опростен модел на работата на QRadar решението.



Стратегията на БНБ включва интензивно интегриране и широко използване на виртуална инфраструктура, която също може да има пролуки и заплахи както стандартната физическа среда, решението включва активно наблюдение и на виртуализационните решения на банката. Използването на технологии като VFlow позволява на ИТ специалистите на банката да получават детайлна информация и видимост в тази инфраструктура.

SIEM осигурява прозрачност, отчетност и измеримостта, които са от решаващо значение за успеха на една организация при изпълнението на регулаторните правомощия и отчитане на съответствието. Способността на решението да се съпоставят и анализират потоците от различни източници предоставя на ИТ одитори и оператори детайлни доклади в съпоставка с различни стандарти и регулации. Решението разполага с предварително изградени доклади и шаблони предназначени за следните разпоредби и контролни рамки: COBIT, SOX, GLBA, NERC / FERC, Isma, PCI DSS, HIPAA, UK GSi / GCSx, GPG и повече.

За да се постигне висока достъпност и възстановяване при бедствие, идентични система може да работи във втори и/или трети център за данни. В зависимост от архитектурата на решението различни модули се поставят на различни физически локации за да гарантира минимална загуба на информация в случай на отпадане или бедствие. Решението поддържа автоматично превключване на системата при отпадане, резервираност на хардуера и на информацията съдържаща се на дисковите масиви, като тази информация е допълнително криптирана за сигурност.

Система за управление и наблюдение на електронната идентичност

Управлението на електронната идентичност в една корпорация е въпрос на стабилна и добре описана политика описваща начина на работа в компанията за:

- ползването на информация



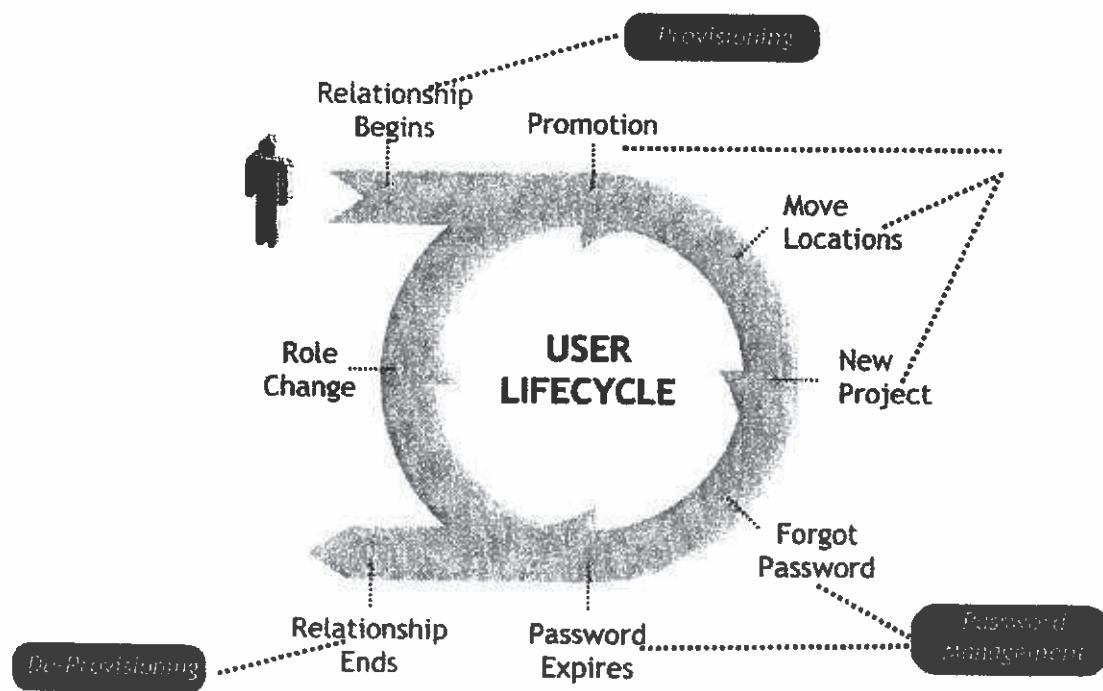
- правата на служителите
- техните правилни процеси на работа.

Решенията управляващи идентичността (Identity Management или Identity & Access Management – IDM) представляват интегрирани системи за:

- управление на електронната идентичност на служителя или друг електронно описан обект (хардуер, мрежови ресурс или софтуер)
- провизиониране и управление на ролите на служителите, спрямо правата/отделите и достъпа и управлението на корпоративна информация
- информация за самите служители (тяхната идентичност), както и кой може да ползва тази информация
- самоуправление на служители (password management, self-service portal и други услуги)
- одитиране на процесите и политиките за достъп и автентикация.

Управляваните обекти от такива решения могат да включват освен идентичността на служителите, а и крайни устройства (компютри или сървъри), мрежови ресурси и дори софтуерни продукти.

На долната диаграма е представен описание на примерен цикъл на живот на електронната идентичност на един служител.



Решение за контрол на електронната информация



С използването на решения за контрол на електронната информация (Right Management System (RMS)) БНБ, се възползва от възможността да защитава , контролира и доказва собственост на корпоративна информация, не зависимо от това къде се намира тя. Целта на RMS е да предпазва чувствителна информация като: финансови доклади, информация за нови продукти и услуги, лична информация, електронна поща и др.

За разлика от стандартното криптиране и sign-ване на предаване информация при която след декриптирането, ползвателя може да променя информацията, RMS решенията дават възможност тази документите да пренасят правата за четене и писане заедно с тях, ограничаващи достъпа и промяната им.

Контрол и защита на мобилни устройства

Мобилните устройства и ползването им за бизнес нужди, е факт който трудно може да се оспорва в днешно време. Развитието и разнообразието на различни преносими устройства представлява вече наболял проблем за ИТ администраторите в дадена корпорация.

Enterprise Mobility Management (EMM) е решение, което осигурява, наблюдава, управлява и поддържа правилната работа на мобилните устройства като smartphones, tablets и лични или служебни мобилни компютри (laptops). Обикновено функционалността му се изразява във

- контрол и наблюдение на настройките на устройства независимо от платформата им – iOS, Android, Windows, Blackberry
 - подготовка на настройки за използване на електронна поща, VPN или безжични комуникации
 - забраняване на ползването на камера в рамките на офисите на компанията
 - управление на сертификатите
 - контрол на паролите/пин на устройствата
 - и други
- управление на софтуерните приложения – контрол на публично достъпни приложения или такива които са вътрешна разработка само за целите на корпорацията
- управление на служебна информация
- управление на мобилните разходи (когато устройството използва мобилна свързаност)
- наблюдение и детайлни доклади за видовете устройства, операционни системи и други

3.2.3. Стъпки на имплементация

Предлаганата стратегия разделя на три различни фази за интеграция на отделните услуги, описани в секция „Приоритетни Инициативи“. Допълнително интегратора предлага няколко оптимизации извън описаните приоритети с цел текуща оптимизация на информационната сигурност на банката.



Долу изброените детайлни дейности не са с посочена индикативна продължителност защото зависят от много фактори, включително и наличието на време от страна на служителите на банката. Въпреки това спрямо опитана ни смятаме, че посочения период за цялата фаза е реалистичен и изпълним.

СТЪПКА 1 – ВНЕДРЯВАНЕ НА IDENTITY MANAGEMENT ЗА НУЖДТЕ НА БНБ

Стъпка 1 се фокусира в/у няколко конкретни сегашни нужди на банката с цел повишаване на сигурността и управлението на достъпа на служителите както до информация така и до самата ИТ инфраструктура на институцията. Нуждите са свързани главно с това, че банката разполага с различни решения за управление на идентичност на служителите си (Novell eDir и Microsoft Active Directory), има различни платформи (Windows Servers, Linux, AIX и др.) и в момента е в процес на имплементиране на контрол на достъп до комуникационната инфраструктура.

В тази секция са предложени детайлните дейности за интеграция на IDM и довършване на проекта за мрежови достъп.

- Анализиране на бизнес процесите, свързани с управлението на идентичностите и ролите на служителите на банката.
- Проектиране на архитектура и изграждане на ядрото на системата за управление на идентичностите и ролите.
- Проектиране и дефиниране на потребителските роли в системата за управление на идентичностите и ролите.
- Проектиране и дефиниране на потребителските роли в системата за контрол на мрежови достъп
- Интегриране на решението за управление на идентичността с корпоративната директория, MS активната директория и Novel eDir.
- Интеграция на решението за управление на идентичностите със системата за управление на човешките ресурси
- Интеграция на решението на контрол до комуникационната инфраструктура с IDM
- Интеграция на решението за контрол до комуникационната инфраструктура с мрежовите устройства
- Осигуряване на централизирано удостоверяване за администраторите на сървъри чрез корпоративната директория и ограничаване на локалния достъп. Сървърни платформи: Linux, AIX, Windows, Solaris
- Осигуряване на съвместимост на решението за управление на идентичностите с решение за виртуализирани десктоп системи.
- Изграждане на система за управление на привилегированите потребители (администратори)
- Изграждане на портал за self-provisioning на потребителите

Очакваната продължителност на тази стъпка е в рамките на 9 календарни месеца



С приключването на Стъпка 1, БНБ ще:

- Оптимизира процеса на работа с идентичността и контрола на крайни служители
- Ще организира процес за предоставяне на права за достъп до служебна информация
- Ще наблюдава и контролира достъпа до комуникационна инфраструктура и ще гарантира, че всяко устройство в ИТ средата на банката отговаря на изискванията за сигурност.
- Ще предостави на служителите портал за управление и заявки на правата си, възможност за смяна на парола и други услуги, освобождаващи администраторите от някои оперативни задължения.

СТЪПКА 2 – ПРОЕКТИРАНЕ И ИЗГРАЖДАНЕ НА СИСТЕМА ЗА АНАЛИЗ И НАБЛЮДЕНИЕ НА ИНФОРМАЦИОННИ СЪОБЩЕНИЯ И СИСТЕМА ЗА КОНТРОЛ НА ПРОПУСКИ В СИГУРНОСТТА

Втората стъпка обединява в себе си две приоритетни инициативи фокусирани върху анализа на служебната информация от ИТ инфраструктурата за пролуки в сигурността на всички нива – от крайни устройства и операционни системи, до комуникационна инфраструктура и софтуерни приложения.

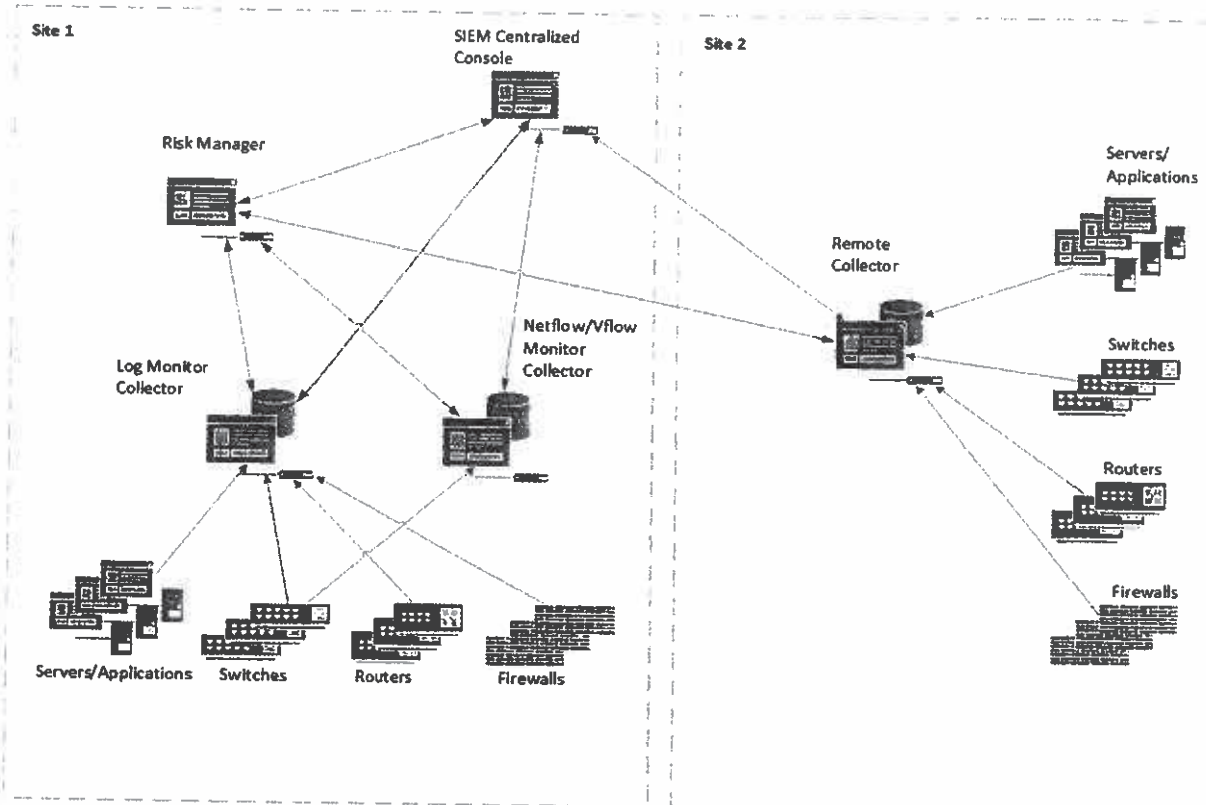
По време на писането на текущия документ банката разполага с Cisco Monitoring Analysis and Response System (MARS) решение, което изпълнява ролята на SIEM. Този продукт е морално остарял и няма техническа и софтуерна поддръжка от производителя си от края на 2014 година.

Предложените дейности в повече детайли за тази част от стратегията са:

- Анализ на текущите потоци и видове информация получавани от сегашното SIEM решение
- Анализ и дефиниране на източниците на информация агрегиращи се в дистрибутивна SIEM архитектура
- Анализ на риска при използване на ИТ инфраструктура. Дефиниране на Риска
- Анализ и опис на IP активите на банката
- Проектиране на архитектура за изграждане на система за наблюдение и анализ на информационни съобщения
- Проектиране на архитектура за управление на риска
- Проектиране на архитектура за изграждане на система за контрол на пропуските в сигурността
- Изграждане на проектираните архитектури
- Интеграция на Сървърните архитектури със SIEM
- Интеграция на комуникационните архитектури със SIEM
- Интеграция на Системата за управление на идентичността със SIEM
- Интеграция на системата за контрол на пропуските в сигурността със SIEM решението
- Анализ и оптимизация на изградените архитектури
- Обучение на персонала за работа с новите системи
- Дефиниране на автоматизация на работата за справяне с откритите уязвимости и пробиви в сигурността



- Дефиниране на детайлизирани доклади за работата на системите



БНБ SIEM ПРЕДЛОЖЕНА АРХИТЕКТУРА

Предвижда се подобен проект да завърши в рамките на 6 месеца от старта на началните анализи.

Предимствата за БНБ след тази стъпка са:

- Централизиране на наблюдението и управлението на ИТ сигурността на банката
- Управление на уязвимостите в инфраструктурата
- Процесиране и автоматично разпределени на задачите по отстраняване на уязвимостите
- Автоматизация на стандартни доклади, представяни по време на одити
- Намаляване на натовареността на екипа за информационна сигурност чрез автоматизиране на анализа на събитията в инфраструктурата на банката

СТЪПКА 3 – КОНТРОЛ НА ЕЛЕКТРОННАТА ИНФОРМАЦИЯ В БАНКАТА – ВНЕДРЯВАНЕ НА СИСТЕМИ ЗА КОНТРОЛ НА ИЗТИЧАНЕ НА ИНФОРМАЦИЯТА И ЕЛЕКТРОННО УПРАВЛЕНИЕ НА ДОКУМЕНТИ.

Последната стъпка в предложената стратегия се фокусира върху електронното управление и маркиране на документи и наблюдението и защитата от тяхното изтичане от вътрешния периметър на банката. Трите предложени решения в приоритетните инициативи са:



- Решение за контрол на електронната информация (Right Management System)
- Система за защита на информацията (Data Leakage Prevention)
- Контрол и защита на мобилните устройства

Предвижданите дейности (в детайл) за интеграция са:

- Анализ на електронните документи в банката
- Дефиниране на собствеността на електронната информация в банката
- Анализ на видовете електронна информация (типове електронни документи, електронна поща, сканирани документи, бази данни, мрежови ресурси и други.)
- Анализ на използваните мобилни устройства в банката за служебни цели (smartphones, tablets, laptops) и нуждите на служителите
- Дефиниране на политика за използване на мобилни устройства в зависимост от техния тип – служебни или собствени
- Проектиране на система за контрол и разписване на електронни документи
- Проектиране на система за контрол електронната информация
- Проектиране на система за управление на мобилни устройства
- Изграждане на решение за контрол и разписване на електронни документи - RMS
- Описания и разписване на съществуващите електронни документи на банката – ДЛП
- Изграждане на система за защита на данните
 - Изграждане на система за защита на данните в комуникационната инфраструктура
 - Изграждане на система за защита на данните в бази данни и мрежови ресурси (file share, share point и др.)
 - Изграждане на система за защита на данните в крайни устройства (Desktops, Laptops)
- Интеграция на системата за защита на данните със решението за маркиране на данни
- Изграждане на решение за контрол на мобилни устройства
- Дефиниране и на планирани доклади от системите
- Интеграция на DLP системата със SIEM

След тази стъпка, с предвиждана **продължителност от 10 месеца**, банката ще разполага със цялостно решение за наблюдение и контрол на електронната информация в банката независимо от това в какво състояние се намира тя (in use, in rest, in motion) или на каква система се използва (desktop, laptop, smartphone, tablet). Отново, администраторите ще се възползват от делегиране на част от задълженията им към собствениците на чувствителна



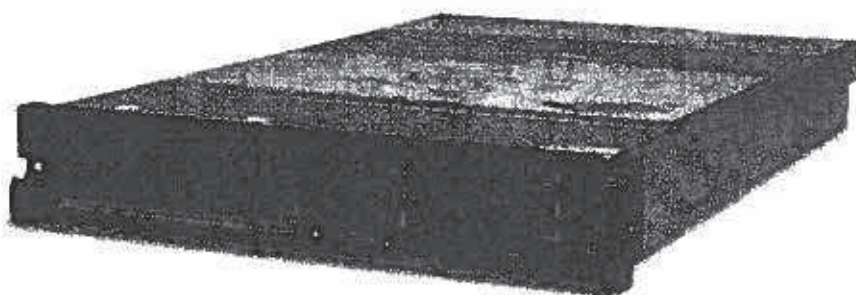
информация, които ще са отговорни да докладват и спомагат за оптимизирането на работата и процесите.

4. Описание на представяното оборудване

4.1. RISC сървъри

Power Servers включени в листа по рамковия договор са представители на две поколения POWER базирани процесори. Препоръчваме POWER7+ сървърите и съпътстващите ги модули да бъдат използвани за разширяване на функционалността или капацитета на текущите сървъри, а при необходимост за нови машини да се залага на POWER8. Последното поколение POWER8 процесор е на пазара от повече от една година и се очаква в близко бъдеще сървърите с по-старото поколение POWER7 процесори да спрат да се предлагат.

4.1.1. Power 710 (8231-E1D)



Power 710 е еднопроцесорен сървър, при който паметта и процесорните ядра са предварително разрешени. Често изпълнява роля на мениджмънт и специализиран Backup & Recovery сървър, но е подходящ и за front-end сървър за приложения.

За този клас сървъри е характерно, че нямат част от RAS характеристиките на големите сървъри – сдвоени мениджмънт модули, преместване на процесите от дефектирал процесор върху друг без прекъсване на работата на системите, но са по-малки 2U и продължават да имат възможността за 2 VIOS сървъра с алтернативни пътища към дискове, LAN и SAN.

Този сървър е подходящ за специализирани приложения или да работи в изолирани среди, така както и в момента се използва същата серия с по-старите процесори POWER7. В последната си генерация този сървър пристига с високоскоростни слотове за разширение PCI Express Generation2 8x, които го правят добър избор за Backup или мрежови сървър.

CONFIGURATION OPTIONS

MODELS 8231-E1D



POWER7+ PROCESSOR MODULES—ONE PER SYSTEM	4-core 3.6 GHz or 6-core 4.2 GHz or 8-core 4.2 GHz
SOCKETS	1
LEVEL 2 (L2) CACHE	256 KB per core
LEVEL 3 (L3) CACHE	10 MB per core
MEMORY	8 GB to 256 GB of RDIMM DDR3 Active Memory Expansion Up to six SFF drives or Up to six SFF SAS drives Up to 5.4 TB Slimline for DVD-RAM Half height for tape drive ¹ or removable disk Five PCI Express Generation2 8x low profile Four Ethernet 10/100/1000 Mbps ports One controller for SAS DASD/SSD w/ RAID 10 and DVD-RAM Optional protected 175 MB cache with RAID 5, 6
SOLID-STATE DRIVES (SSD)	8 Gigabit Fibre Channel
DISK DRIVES	2-port 16 Gbps Fibre Channel
DISK CAPACITY	2-port 10GbE RoCE
MEDIA BAYS	Dual port 10 Gigabit Ethernet Dual port 10 Gigabit Fibre Channel over Ethernet Dual port QDR Infiniband 6Gbps SAS RAID controller
PCI ADAPTER SLOTS	Three USB, two HMC, two system ports
STANDARD ETHERNET	One GX++ (not available with 4-core processor)
INTEGRATED SAS CONTROLLER	ECC memory with Chipkill Processor Instruction Retry Alternate Processor Recovery Service processor with fault monitoring Hot-plug disk bays Hot-plug and redundant power supplies and cooling fans Dynamic component Deallocation
HIGH-PERFORMANCE PCI ADAPTERS	AIX IBM i Linux for POWER® IBM PowerHA® family
OTHER INTEGRATED PORTS	100 V to 240 V ac, single phase
GX SLOTS	
RAS FEATURES	
PROCESSOR INSTRUCTION RETRY	
ALTERNATE PROCESSOR RECOVERY	
SERVICE PROCESSOR WITH FAULT MONITORING	

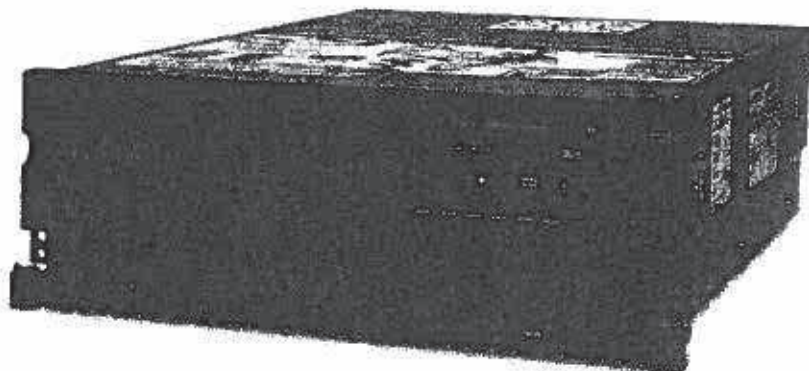
Типична системна конфигурация за нуждите на TSM или друг софтуер е:

№	P.N./ F.C.	ОПИСАНИЕ НА ПРОДУКТА	QTY.
---	------------	----------------------	------



1	8231-E1D	- Сървър за вграждане в индустриален шкаф - Процесор: 1 x 8-core 4.2 GHz POWER7+ Processor Module Processor Activation for Processor Feature for all cores - Памет: 16GB Memory DIMMs, 1600 MHz - Твърд диск: 1 x 146GB 15K RPM SFF SAS Disk Drive (AIX/Linux) - Backplane да позволяват разделяне на дисковете през два вградени независими SAS канала и контролери - 1 мрежови адаптер тип на слота PCIe2 - 4 порта 1 Gbps - два захранващи модула за 220V 50Hz - Софтуер: AIX Standard Edition Version 7.1, PowerVM EE с лицензи за всички ядра	1
2	EN0L	PCIe2 LP 4-port(10Gb FCoE & 1GbE) SFP+Copper&RJ45	1
3	EN0Y	PCIe2 LP 8Gb 4-port Fibre Channel Adapter	2
4	EM4B	16GB (2x8GB) Memory DIMMs, 1066 MHz, 4Gb DDR3 DRAM	3
5	ESDT	146GB 15k RPM SAS SFF-3 Disk Drive (AIX/Linux)	3

4.1.2. Power 740 (8205-E6D)



Power 740 е двупроцесорен сървър, при който отново паметта и процесорните ядра са предварително разрешени. Заради по-мощните процесори изпълнява роля на мениджмънт и специализиран за приложения и за бази данни. Стандартния софтуерен пакет включва AIX Standard PowerVM Ent. Ed. Позволяващи му гъвкава работа, както като отделен сървър така и в рамките на по-голям пул от сървъри.

За този клас сървъри е характерно, че нямат част от RAS характеристиките на големите сървъри – сдвоени мениджмънт модули, преместване на процесите от дефектирал процесор върху друг без прекъсване на работата на системите, но са по-малки 2U и продължават да имат възможността за 2 VIOS сървъра с алтернативни пътища към дискове, LAN и SAN.

Този сървър е подходящ за специализирани приложенията или да работи в изолирани среди, така както и в момента се използва същата серия с по-старите процесори POWER7. В последната си генерация този сървър пристига с високоскоростни слотове за разширение PCI Express Generation2 8x Full Size и опционално Half-size, които го правят добър избор за DB или сървър с множество директно свързани дискове и разширителни карти през GX++ слотове.



CONFIGURATION OPTIONS	MODELS 8205-E6D
POWER7+ PROCESSOR	6-core or 12-core 4.2 GHz or
MODULES—ONE OR TWO PER SYSTEM	8-core or 16-core 3.6 GHz or
SOCKETS	8-core or 16-core 4.2 GHz
LEVEL 2 (L2) CACHE	1 or 2
LEVEL 3 (L3) CACHE	256 KB per core
MEMORY	10 MB per core
	8 GB to 512 GB of RDIMM DDR3 - 1 processor
	8 GB to 1024 GB of RDIMM DDR3 - 2 processors
	Active Memory Expansion available
SOLID-STATE DRIVES (SSD)	Up to eight SFF drives
DISK DRIVES	Up to eight SFF SAS drives
DISK CAPACITY	Up to 7.2 TB
MEDIA BAYS	Slimline for DVD-RAM
	Half height for tape drive ¹ or removable disk
PCI ADAPTER SLOTS	Five PCI Express 8x Generation2
	plus optional four PCI Express Generation2 low profile
STANDARD ETHERNET	Four Ethernet 10/100/1000 Mbps ports
INTEGRATED SAS CONTROLLER	One controller for SAS DASD/SSD w/ RAID 10 and DVD-RAM
	Optional protected 175 MB cache with RAID 5, 6
HIGH-PERFORMANCE PCI ADAPTERS	4-port 8 Gigabit Fibre Channel
	2-port 16 Gigabit Fibre Channel
	2-port 10GbE RoCE
	10 Gigabit Ethernet
	10 Gigabit Fibre Channel over Ethernet
	Dual Port Quad Data Rate IB
	6Gbps SAS RAID controller
OTHER INTEGRATED PORTS	Three USB, two HMC, two system ports
GX SLOTS	Two GX++ (available with two processors)
RAS FEATURES	ECC memory with Chipkill
	Processor Instruction Retry
	Alternate Processor Recovery
	Service processor with fault monitoring
	Hot-plug disk bays
	Hot-plug and redundant power supplies and cooling fans
	Dynamic component Deallocation
PROCESSOR INSTRUCTION RETRY	AIX
	IBM i
ALTERNATE PROCESSOR RECOVERY	Linux for POWER®
SERVICE PROCESSOR WITH FAULT MONITORING	IBM PowerHA® family
	100 V to 240 V ac, single phase

Типична системна конфигурация за нуждите за бази данните:

№	P.N./ F.C.	ОПИСАНИЕ НА ПРОДУКТА	QTY.
---	------------	----------------------	------



1	8205-E6D	Сървър за вграждане в сървърен шкаф - 4U - Процесор: 1 x 8-core 4.2 GHz POWER7+ Processor Module - Памет: 64GB (8x8GB) Memory DIMMs, 1066 MHz - Твърд диск: 1 x 146GB 15K RPM SFF SAS Disk Drive (AIX/Linux) - 1 мрежови адаптер тип на слота PCIe2 - 4 порта 1 Gbps - Backplane да позволяват разделяне на дисковете през два вградени независими SAS канала и контролери - Софтуер: AIX Standard. Edition Version 7.1, PowerVM Enterprise Edition с лицензи за всички ядра	1
2	EPCR	8-core 4.2 GHz POWER7+ Processor Module	1
3	EN0H	PCIe2 4-port (10Gb FCoE & 1GbE) SR&RJ45	2
4	EPDR	One Processor Activation for Processor Feature #EPCR	8
5	EM4B	16GB (2x8GB) Memory DIMMs, 1066 MHz, 4Gb DDR3 DRAM	4
6	ESDT	146GB 15k RPM SAS SFF-3 Disk Drive (AIX/Linux)	3
7	EN0A	PCIe2 16Gb 2-port Fibre Channel Adapter	2

И двата представени сървъра Power 710 и Power 740 работят с контролерите на текущите Power7 сървъри и така че има възможност текущите сървъри да бъдат Upgrade с тях.

4.1.3. Power 770 (9117-MMD)



Power 770 е сървър от среден до висок клас, с изключително големи възможности за растеж и вградени механизми за висока производителност и надеждност на системата. Банката залага на този клас сървъри за консолидиране на приложенията върху него. Power 770 има



модулен дизайн, който позволява да се отговори максимално добре на текущите нужди, запазвайки възможността да се расте в случай на необходимост.

Power 770 се базира на Capacity-on-Demand ползване на ресурсите като предоставя гъвкави възможности за лицензиране на ядра и памет. Не-отключените ядра и обем памет участват в резервирането на работещите и при отпадане на ресурс от основните системата автоматично и без прекъсване на работата ги заема отново. Дадена е възможност "dark" ресурсите да бъдат отключени за използване с пакети с Linux LPAR, като по този начин ефективно се утилизира машината и се предоставят значителни изчислителни ресурси за нови приложения.

Заради повечето и по-мощни процесори, големия обем памет, и IO изпълнява роля на консолидиращ множество корпоративни приложения и основни бази данни. AIX Enterprise и PowerVM Ent. Ed. са необходими за отключване на пълните възможности на сървърите.

Притежава повечето от RAS характеристиките необходими големите сървъри – сдвоени мениджмънт модули, преместване на процесите от дефектирал процесор върху друг без прекъсване на работата на системите, подмяната на CEC модули, възможността за 2 и повече VIOS сървъра с алтернативни пътища към дискове, LAN и SAN.

Този сървър е подходящ за основен сървър за бази данни и корпоративни приложения, така както и в момента се използва същата серия с по-старите процесори POWER7. В последната си генерация този сървър пристига с високоскоростни слотове за разширение PCI Express Generation2, които го правят добър избор за DB или сървър с множество директно свързани дискове и разширителни карти през GX++ слотове.

CONFIGURATION OPTIONS	PER BUILDING BLOCK	SYSTEM MAXIMUM
PROCESSORS	16 x 3.8 GHz POWER7+ processor cores or 12 x 4.2 GHz POWER7+ processor cores	64 x 3.8 GHz POWER7+ processor cores or 48 x 4.2 GHz POWER7+ processor cores
SOCKETS	Four	Sixteen
LEVEL 2 (L2) CACHE	256 KB L2 cache per core	256 KB L2 cache per core
LEVEL 3 (L3) CACHE	10 MB L3 cache per core (eDRAM)	10 MB L3 cache per core (eDRAM)
ENTERPRISE MEMORY	Up to 1 TB of 1066 MHz DDR3 Active Memory Expansion Up to six SFF SAS drive bays	Up to 4 TB of 1066 MHz DDR3 Active Memory Expansion Up to 24 SFF SAS drive bays
INTEGRATED SAS BAYS FOR SOLID STATE DRIVES (SSD) OR HARD DISK DRIVES (HDD)		
INTEGRATED MEDIA BAYS	One slimline for SATA DVD-RAM	Four slimline for SATA DVD-RAMs
INTEGRATED PCI ADAPTER SLOTS	Six PCIe Gen2 slots Up to one per enclosure: Dual 10 Gb + Dual 1 Gb	24 PCIe Gen2 slots Up to four per system: Dual 10 Gb + Dual 1 Gb
INTEGRATED MULTIFUNCTION CARD	Two SAS DASD/SSD controllers One SATA media controller	Eight SAS DASD/SSD controllers Four SATA media controllers
INTEGRATED SAS CONTROLLERS	Three USB; two HMC; two SPCN	Nine USB; four HMC; four SPCN
OTHER INTEGRATED PORTS	Two	Eight
GX SLOTS (12X)	Up to 4 PCIe 12X I/O drawers	Up to 16 PCIe 12X I/O drawers
I/O EXPANSION	Up to 8 PCI-X DDR 12X I/O drawers	Up to 32 PCI-X DDR 12X I/O drawers



HIGH-BANDWIDTH PCI ADAPTERS

6 Gigabit SAS
8 Gigabit Fibre Channel
10 Gigabit Ethernet
10 Gigabit Fibre Channel over Ethernet
40 Gigabit QDR

OTHER PCI ADAPTERS SUPPORTED

SAS, Fibre Channel, Ethernet, SCSI, WAN/Async, USB, Crypto, iSCSI

Типична системна конфигурация за нуждите за бази данни е:

№	P.N./ F.C.	ОПИСАНИЕ НА ПРОДУКТА	QTY.
1	9117-MMD	Сървър за вграждане в сървърен шкаф - 4U на модул процесор: 1 x 4.22 GHz Proc Card, 0/12 Core POWER7+, 16 DDR3 Memory Slots памет: 2 x 0/32GB DDR3 Memory (4X8GB) DIMMS - 1066MHz - POWER7+ CoD Memory 32 x Activation of 1 GB DDR3 POWER7+ Memory 175MB Cache RAID - Dual IOA Enablement Card 4 вградени интерфейса 10 GE и 1 GE вградени на дъното два двупортови адаптера - PCIe Fibre Channel 8 Gbps Захранване: 2 x System AC Power Supply, 1925 W Форм фактор: rack Софтуер: AIX Enterprise Edition Version 7.1, PowerVM Enterprise edition с лицензи за всички ядра	1
2	1886	146GB 15K RPM SFF SAS Disk Drive (AIX/Linux)	6
3	2146	Primary OS - AIX	1
4	3671	Serv Interface Cable- 2, 3, and 4 Enclosure	1
5	3715	Processor Cable, Two, Three-Drawer System, 4 socket	1
6	3716	Processor Cable, Two, Three, Four-Drawer System, 4 socket	1
7	5532	System AC Power Supply, 1925 W	4
8	5652	Disk/Media Backplane	2
9	5662	175MB Cache RAID - Dual IOA Enablement Card	1
10	5771	SATA Slimline DVD-RAM Drive	1
11	6006	Power Control Cable (SPCN) - 3 meter	1
12	7995	PowerVM - Enterprise Edition	4
13	9169	Order Routing Indicator- System Plant	1
14	9300	Language Group Specify - US English	1
15	9440	New AIX License Core Counter	4
16	EB33	Dynamic Platform Optimizer	1
17	EB85	System CEC Enclosure with IBM BEZEL, I/O Backplane, and System Midplane	2
18	EC53	Operator Panel	1
19	EM40	0/32GB DDR3 Memory (4X8GB) DIMMS - 1066 MHz - POWER7+ CoD Memory	4
20	EMA2	Activation of 1 GB DDR3 POWER7+ Memory	24
21	EN10	Integrated Multifunction Card w/ 10GbE RJ45 & Copper Twinax	2
22	EPM0	4.22 GHz Proc Card, 0/12 Core POWER7+, 16 DDR3 Memory Slots	2
23	EPMA	1-Core Activation for Processor Feature EPM0	4



24	EU09	Service Processor-3	2
25	EN0Y	PCIe2 LP 8Gb 4-port Fibre Channel Adapter	4

Забележка: Представената конфигурация е примерна и може да не съдържа всички необходими на банката елементи, модули и софтуер.

Сървърите Power 770 с POWER7+ позволяват на банката да увеличи производителността на текущите си опорни сървъри с между 10-30% в зависимост от типа на натоварването и да мигрират към Power E870 и POWER8 платформа, където увеличената производителност е близо 50%, като същевременно се запазят инвестициите в софтуерни лицензи и не се прекъсва работата на производствените системи.

4.1.4. Power E870 (9117-MME)



Power E870 е сървър от висок клас (Enterprise server), анонсиран в края на миналата 2014 година работещ с най-новото поколение POWER8 процесори с изключително големи възможности за растеж и вградени механизми за висока производителност и надеждност на системата. Базиран е на модулния дизайн на 770/780 сървърната платформа, но е предоставя много по-големи възможности за производителност и разширяемост.

Банката ще ползва сървърите за консолидиране на основните си приложения и изграждане на изчислителна среда с големи възможности за растеж.

E870/E880 са проектирани на база на успешните 770/780 архитектури и имат много общи черти – модулна архитектура, за повишаване на гъвкавостта и възможностите за растеж, всеки



от CEC съдържа, както процесори и памет така също и PCI слотове, комуникацията между модулите се осъществява директно (any-to-any pairing) през високоскоростни интерфейси.

Паметта и процесорите се отключват на база CoD механизми, като са предвидени гъвкави схеми за заявяване и отчитане на ползването в зависимост от бизнес модела на клиента. От 2013 година е въведена „мобилност“ в схемата за CoD, в която отключените ресурси на сървърите от високия клас, могат да се преместват от един на друг сървър в зависимост от нуждите на клиента, без да се налага промяна в работещите приложения.

Този сървър е подходящ за основен сървър за бази данни и корпоративни приложения, така както и в момента се използва същата серия с по-старите процесори POWER7. В последната си генерация този сървър пристига с високоскоростни слотове за разширение PCI Express Generation2, които го правят добър избор за DB или сървър с множество директно свързани дискове и разширителни карти през GX++ слотове.

CONFIGURATION OPTIONS	PER BUILDING BLOCK	SYSTEM MAXIMUM
PROCESSORS	32 x 4.02 GHz POWER8 40 x 4.19 GHz POWER8	64 x 4.02 GHz POWER8 80 x 4.19 GHz POWER8
SOCKETS	Four	Eight
LEVEL 2 (L2) CACHE	512 KB L2 cache per core	512 KB L2 cache per core
LEVEL 3 (L3) CACHE	8 MB eDRAM shared L3	8 MB eDRAM shared L3
ENTERPRISE MEMORY	Up to 1 TB of 1066 MHz DDR3 Active Memory Expansion	Up to 4 TB of 1066 MHz DDR3 Active Memory Expansion
LEVEL 4 (L4) CACHE	Up to 128 MB eDRAM L4 (off-chip) per socket	
RAM	4 TB	8 TB
OTHER INTEGRATED PORTS	Three USB; two HMC; two SPCN	Nine USB; four HMC; four SPCN
I/O EXPANSION	8 PCIe Gen.3 adapter slots Up to 4 PCIe I/O drawers	16 PCIe Gen.3 adapter slots Up to 8 PCIe I/O drawers
SYSTEM DIMENSIONS	7 EIA (12U) space in a 19-inch rack	12 EIA (12U) space in a 19-inch rack
SYSTEM CONTROL UNIT	One	
FLEXIBLE SERVICE PROCESSORS	Two in system control unit	

Типична системна конфигурация за нуждите за консолидационна платформа е:

№	P.N./ F.C.	ОПИСАНИЕ НА ПРОДУКТА	QTY.
1	9117-MMD	Модулен сървър за вграждане в сървърен шкаф -Процесор: 4.19 GHz, 40-core POWER8 Processor 4x 1-core activation of #EPBC - Памет: 64GB (4X16GB) CDIMMs, 1600 MHz, 4GBIT DDR3 DRAM, - Твърд диск: 6+6 storage backplane with split bay option, 146GB 15K RPM SFF3 SAS Disk Drive (AIX/Linux) - Софтуер: AIX Enterprise Edition PowerVM Enterprise edition с лицензи за всички ядра - redundant AC Power supply - 220V 50Hz	1
2	9440	New AIX License Core Counter	8
3	465	SSD Placement Indicator - 5887, EL1S	1
4	728	EXP24S SFF Gen2 Load Source Specify (#5887 or #EL1S)	1
5	1953	300GB 15k RPM SAS SFF-2 Disk Drive (AIX/Linux)	2
6	5228	PowerVM Enterprise Edition	8



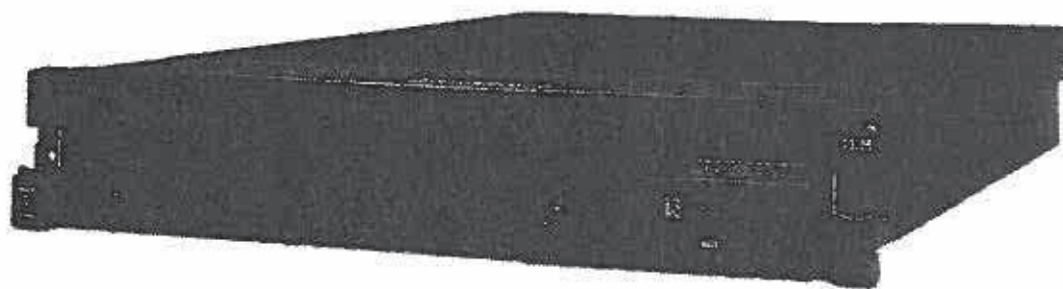
7	5260	PCIe2 LP 4-port 1GbE Adapter	1
8	5273	PCIe LP 8Gb 2-Port Fibre Channel Adapter	1
9	5887	EXP24S SFF Gen2-bay Drawer	1
10	6577	Power Cable - Drawer to IBM PDU, 200-240V/10A	10
11	EBA0	5U system node drawer	2
12	EBA2	IBM Rack-mount Drawer Bezel and Hardware	2
13	EBAA	AC Power Chunnels	2
14	EM8J	64GB (4X16GB) CDIMMs, 1600 MHz, 4GBIT DDR3 DRAM	8
15	EMA5	1GB Memory Activation	128
16	EN0B	PCIe2 LP 16Gb 2-port Fibre Channel Adapter	2
17	EN0L	PCIe2 LP 4-port(10Gb FCoE & 1GbE) SFP+Copper&RJ45	2
18	EPBA	4.02 GHz, 32-core POWER8 processor	2
19	EPBJ	1 core Processor Activation for #EPBA	8
20	EU0A	Service Processor	2
21	EJ0M	PCIe3 LP RAID SAS ADAPTER	4

Забележка: Представената конфигурация е примерна и може да не съдържа всички необходими на банката елементи, модули и софтуер или да отговаря на текущите нужди.

Текущите сървъри Power 770 са с POWER7 и позволяват на банката да мигрира към POWER8 сървъри като се запазят серийните номера на машините и инвестициите във софтуер – AIX, PowerHA, PowerVM, Oracle, IBM SW etc. “Model change” позволява новите машини да получат досегашните лицензи за CoD за памет и процесори, като това ще запази текущата инвестицията в сегашните сървъри. При използване на този подход горната конфигурация ще бъде с 40 разрешени процесора и 448 GB памет.

В резултат имаме увеличена производителност на текущите си опорни сървъри с между 80-100%, като същевременно се запазят инвестициите в софтуерни лицензи и не се прекъсва работата на продукционните системи.

4.1.5. Power S822 (8284-22A)





Power S822 е двупроцесорен сървър базиран на POWER8, при който отново паметта и процесорните ядра са предварително разрешени. Процесорите позволяват по-високи скорости на обмен на данни с паметта и IO и SMP8.

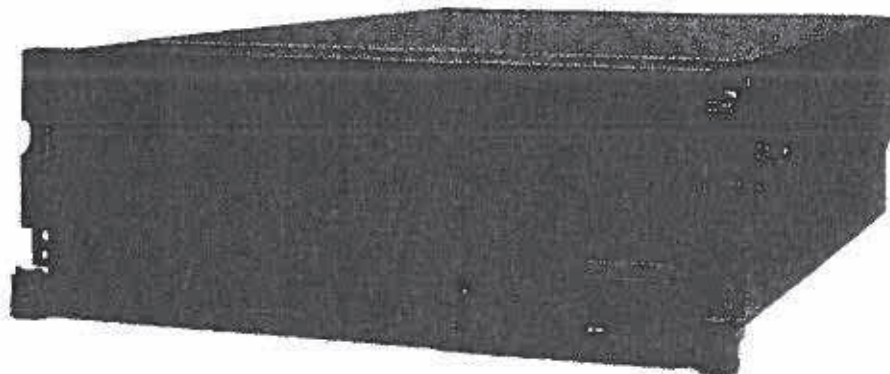
Заради по-мощните процесори може да изпълнява роля на мениджмънт и специализиран за приложения и за бази данни. Стандартния софтуерен пакет включва AIX Standard и PowerVM Ent. Ed. Позволяващи му гъвкава работа, както като отделен сървър така и в рамките на по-голям пул от сървъри.

CONFIGURATION OPTIONS	MODELS 8284-22A
MICROPROCESSORS	One or two 6-core 3.89 GHz POWER8 processor cards or One or two 8-core 4.15 GHz POWER8 processor cards or One or two 10-core 3.42 GHz POWER8 processor cards
SOCKETS	1 or 2
LEVEL 2 (L2) CACHE	512 KB L2 cache per core
LEVEL 3 (L3) CACHE	8 MB L3 cache per core
LEVEL 4 (L4) CACHE	16 MB per DIMM
MEMORY MIN/MAX	16 GB, 32 GB and 64 GB 1600 MHz DDR3 module 16 to 512 GB (1S) 32 to 1 TB (2S)
PROCESSOR-TO-MEMORY BANDWIDTH	192 GBps per socket
STANDARD BACKPLANE WITH DUAL IOA HIGHER FUNCTION BACKPLANE	12 SFF Hard Disk Drive (HDD)/Solid State Disk (SSD) 8 SFF HDD/SSD plus 6 1.8-inch bays for SSD
MEDIA BAYS	One slimline DVD
INTEGRATED SAS CONTROLLER	Standard RAID 0,5,6,10. optional: 7200 MB* cache & easy tier function Included one x8 PCIe slots must contain a 4-port 1 Gb Ethernet LAN available for client use
ADAPTER SLOTS	Nine PCIe Gen3 slots with concurrent maintenance: four x16 plus five PCIe Gen3 x8 Two CAPI adapters per processor module
I/O BANDWIDTH	96 GBps per socket
MAX PCIE GEN3 I/O DRAWER	1
POWER SUPPLY	200 V to 240 V
RAS FEATURES	Processor instruction retry Alternate processor recovery Selective dynamic firmware updates Chipkill memory Error correcting code (ECC) L2 cache, L3 cache Service processor with fault monitoring Hot-swappable disk bays Hot-plug concurrent maintenance PCIe slots Hot-plug and redundant power supplies and cooling fans Dynamic processor deallocation Extended error handling on PCI slots
OS SUPPORT	AIX Linux for POWER®

В зависимост от нуждите, базовата конфигурация може да бъде екипирана с допълнителен процесор и памет, както и да се увеличи броя на дисковете – ефективен начин за изграждане на NIM или TSM сървър, независим от SAN.



4.1.6. Power S824 (8286-42A)



Power S824 е двупроцесорен сървър базиран на POWER8, при който отново паметта и процесорните ядра са предварително разрешени. Процесорите позволяват по-високи скорости на обмен на данни с паметта и IO и SMP8. За разлика от S822 той работи с процесори с по-висока честота, а при

Заради по-мощните процесори може да изпълнява роля на мениджмънт и специализиран за приложения и за бази данни. Стандартния софтуерен пакет включва AIX Standard и PowerVM Ent. Ed. Позволяващи му гъвкава работа, както като отделен сървър така и в рамките на по-голям пул от сървъри.

CONFIGURATION OPTIONS

MICROPROCESSORS	One or Two 6-core 3.89 GHz POWER8 processor cards or One or Two 8-core 4.15 GHz POWER8 processor cards or Two 12-core 3.52 GHz POWER8 processor cards
SOCKETS	1 or 2
LEVEL 2 (L2) CACHE	512 KB L2 cache per core
LEVEL 3 (L3) CACHE	8 MB L3 cache per core
LEVEL 4 (L4) CACHE	16 MB per DIMM
MEMORY MIN/MAX	16 GB, 32 GB, 64 GB and 128 GB 1600 MHz DDR3 module, 32 to 1 TB (1S) 32 to 2 TB (2S) Active Memory Sharing
PROCESSOR-TO-MEMORY BANDWIDTH	192 GBps per socket
STANDARD BACKPLANE WITH DUAL IOA HIGHER FUNCTION BACKPLANE	12 SFF Hard Disk Drive (HDD)/Solid State Disk (SSD) 18 SFF bays for HDD/SSD plus 8 1.8-inch bays for SSD
MEDIA BAYS	One slimline DVD
INTEGRATED SAS CONTROLLER	Standard RAID 0, 5,6,10. optional: 7200 MB* cache & easy tier function
ADAPTER SLOTS	Included one x8 PCIe slots must contain a 4-port 1 Gb Ethernet LAN available for client use



I/O BANDWIDTH
MAX PCIE GEN3 I/O DRAWER
POWER SUPPLY
RAS FEATURES

Eleven PCIe Gen3 slots with concurrent maintenance: four x16 plus seven PCIe Gen3 x 8
Two CAPI adapters per processor module
96 GBps per socket
1
200 V to 240 V
Processor instruction retry
Alternate processor recovery
Selective dynamic firmware updates
Chipkill memory
Error correcting code (ECC) L2 cache, L3 cache
Service processor with fault monitoring
Hot-swappable disk bays
Hot-plug concurrent maintenance PCIe slots
Hot-plug and redundant power supplies and cooling fans
Dynamic processor deallocation
Extended error handling on PCI slots
AIX, IBM i Linux for POWER®

OS SUPPORT

В зависимост от нуждите, базовата конфигурация може да бъде екипирана с допълнителен процесор и памет, както и да се увеличи броя на дисковете – ефективен начин за изграждане на NIM или TSM сървър, независим от SAN. Възможностите за разширяване на конфигурацията са по-големи с оглед на повечето интерфейси и контролери, които могат да бъдат добавени.

4.1.7. Flex System p260 (7895-23X)



Flex System p260 е модул в Flex System шаши, създаден за висока плътност на сървърите, входно-изходните адаптери, процесори и памет. Компромиса, който е направен за да се вмести този сървър в по-компактни размери са ограничените до 2 позиции за контролери и 2-та локални диска. Тези сървъри са предвидени да работят в виртуална среда и VM да се стартират и работят изцяло от SAN.

Интерфейсите и контролерите са високо производителни около 30-40 Gbps например 4x10 GE или 2 x 16 Gbps FC, паметта и процесорните ядра също са големи. Като цяло този сървър е на равнището на Power 740.



Този сървър е подходящ за изграждане на DR, при специализирани приложенията с необходимост от висока производителност и голяма плътност на сървърите.

CONFIGURATION OPTIONS

POWER7+ PROCESSOR MODULES—ONE OR TWO PER SYSTEM	2, 4, 8 or 16 cores, POWER7+, 64-bit processors with VSX, Memory Expansion acceleration and Encryption acceleration Configuration Options: 2-core 4.0 GHz 4-core 4.0 GHz 8-core 3.6 GHz 8-core 4.1 GHz
SOCKETS	1 or 2
LEVEL 2 (L2) CACHE	256 KB per core
LEVEL 3 (L3) CACHE	10 MB per core
MEMORY	8 GB up to 512 GB, 16 DIMM slots, ECC IBM Chipkill DDR3 SDRAM running at 1066 MHz plus Active Memory Expansion with hardware assist Up to two 2.5-inch Hard Disks or two 1.8-inch Solid State Drives
INTERNAL DISK STORAGE	Two PCIe Expansion Slots
NETWORKING/EXPANSION SYSTEMS MANAGEMENT	Integrated systems management processor, light path diagnostics, Predictive Failure Analysis, Cluster Systems Management (CSM), Serial Over LAN, IPMI compliant
RAS FEATURES	Chassis redundant/hot-plug power and cooling Front Panel and FRU/CRU LEDs Concurrent code update and Processor deallocation Compute node hot plug and Dual VIOS support Dual AC Power Supply Auto reboot on power loss Internal and chassis-external temperature monitors System management alerts IBM Chipkill ECC detection and correction
PROCESSOR INSTRUCTION RETRY	AIX 6.1, AIX 7.1 IBM i 6.1 and 7.1 RHEL 5.7, 6.2; SLES11 SP2

4.1.8. План за обновяване на текущата сървърна база

Инфраструктурата на банката се състои от няколко поколения сървъри и дискови масиви. Част от тях се намират в експлоатация и обслужват некритични системи – развойни и тестови среди.

Managed System	Install year	Type Model
NIM1-Server-9110-51A-SN06616D0	2007	9110-51A
RTGS life-8203-E4A-SN06124E6	2007	8203-E4A
RTGS test-8203-E4A-SN06124F6	2007	8203-E4A
SAA7B-Server-9110-51A-SN06A09E2	2008	9110-51A
SAA7L-8203-E4A-SN06125A6	2007	8203-E4A
SAA7T-Server-9110-51A-SN06A0A52	2008	9110-51A
Server-9117-570-SN6566C4E	2007	9117-570



Server-9117-MMA-SN0604214	2009	9117-MMA
Server-9117-MMB-SN06B331P		9117-MMB
Server-9117-MMB-SN06B332P		9117-MMB
TPC-8205-E6C-SN062E81T		8205-E6C
TSM2-Server-9110-51A-SN06616C0	2007	9110-51A
TSTST-Server-9110-51A-SN06A0A02	2008	9110-51A
VACANT1-9110-51A-SN06D81F1	2008	9110-51A
VACANT2-9110-51A-SN06D81D1	2008	9110-51A
VACANT3-9110-51A-SN06A09F2	2008	9110-51A
tsmprod1-8231-E1C-SN0682E1R		8231-E1C
tsmprod2-8231-E1C-SN0682EFR		8231-E1C
RTGS_back-8203-E4A-SN06124D6	2010	8203-E4A
STDB-CC-8205-E6C-SN062718T		8205-E6C
Server-8231-E1C-SN0682E0R		8231-E1C
Server-9110-51A-SN06D81E1	2008	9110-51A
Server-9111-520-SN656666D		9111-520
Server-9111-520-SN65667AD		9111-520
Server-9117-570-SN65ED6DA		9117-570

Има машини, които се ползват от около между 7 и 10 години независимо, че част са във от поддръжка евентуален срив е много вероятен и би добавил риск за проблеми в останалите машини.

Не е малък дела на машини, които са на възраст между 4 и 7 години, преобладаващата част е в експлоатация и са в договор за извън гаранционна поддръжка. Обичайно след изтичане на гаранционната поддръжка в периода между 4 и 5 година производителите увеличават таксите за поддръжка заради завишените рискове от срив, нуждата от по-голям склад и поддръжка. По-ниската производителност на процесорите, по-бавните I/O подсистеми и ограничената памет ги прави още по-неефективни спрямо текущата технология.

Ние препоръчваме консолидирането и виртуализирането на средите да протече максимално бързо и старите сървъри да бъдат извадени от експлоатация и да бъде използван момента с навлизането на POWER8 процесорите и базираните на тях сървъри.

IBM подпомага този процес в две направления:

- Софтуерните лицензи като AIX и PowerHA могат да бъдат прехвърляни на нови машини като се запазва класа – Standard, Enterprise;
- За машини, които са в поддръжка (може и извънгаранционна) може да се използва Model Change процедура, традиционно ползвана за обновяване на поколенията;

При втория подход съществуват ограничения за машините които могат да се използват като база. Те трябва да бъдат минимум 570 с процесор POWER6



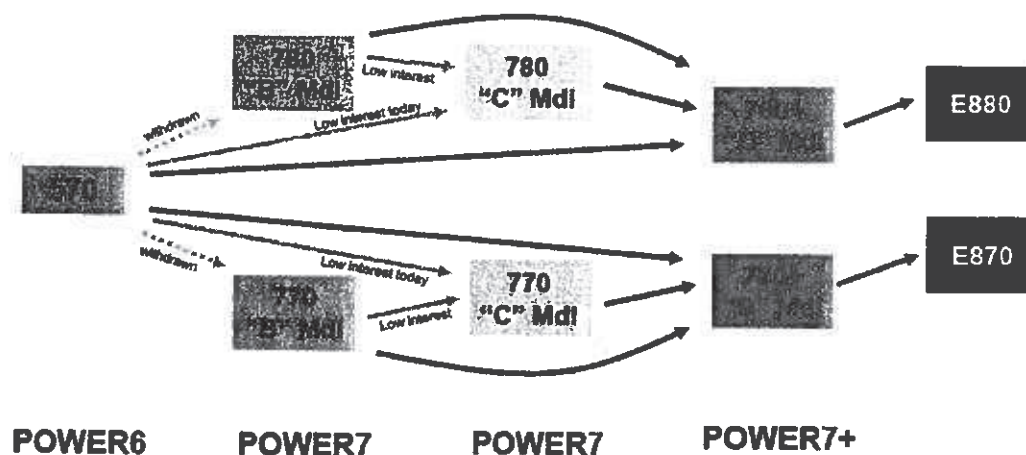
4.1.8.1. Model Change

IBM гарантира пълната съвместимост на кода и операционните системи върху новите сървъри, а така също е възможна миграция върху новите поколения машини без downtime, използвайки възможностите на Active Partition Mobility.

Софтуерните продукти, които се лицензират на машина обичайно зависят от серийния ѝ номер. IBM предоставя механизъм, по който инвестициите направени в софтуера се запазват като номера на новата машина се запазва..

Особеното е, че няма директна миграция от Power7 и по-стари процесори, към POWER8. Необходимо е първо системата да заработи с MMD – (Power7+). Не се налага да се инсталират два пъти нови машини, а формално се минава през процедурата за миграция към "D" модел.

770/780 Model Upgrades (Same Serial Number)



Ние предлагаме да се използва този механизъм за миграцията за 770 машините към E870, за да се запази големия брой разрешени ядра и закупен софтуер PowerVM и PowerHA.

Managed System	Type Model	Serial	Tot Cores	Act Cores	PowerHA	Tot GB	Act GB
Server-9117-570-SN6566C4E	9117-570	6566C4E	18	8	0	64.00	48.00
Server-9117-MMA-SN0604214	9117-MMA	0604214	8	6	0	64.00	32.00
Server-9117-MMB-SN06B331P	9117-MMB	06B331P	36	20	4	320.00	192.00
Server-9117-MMB-SN06B332P	9117-MMB	06B332P	36	20	4	320.00	192.00



Предложените машини в основния сайт са в момента на активна поддръжка в IBM и моделите MMA и MMB са подходящи за миграция. Заради по-големия брой отключени ядра и памет си заслужава да се провери, възможността това да бъде направено за 9117-570.

При извършване на обновяване на моделите се запазва нивото и сроковете на поддръжка.

4.1.8.2. Software reuse

Според условията на IBM AIX и PowerHA, както и повечето от останалите лицензи за системен софтуер – TSM, TPC PowerVC, PowerVP, System Director, не са обвързани с конкретна машина, а принадлежат на организацията.

Тези лицензи могат да бъдат асоциирани с други машини, ако са под софтуерна поддръжка – SWMA.

Съществена стъпка преди стартиране на модернизацията на сървърите е да се направи одит на съществуващите лицензи и да се изберат машините „донори“ на лицензи, които да се консолидират върху нови машини.

Managed System	Type Model	Serial	Tot Cores	Act Cores
	8203-E4A	06124F6	1	1
	8203-E4A	06124F6	1	1
	9110-S1A	06A09F2	1	1
	8203-E4A	06125A6	1	1
	9110-S1A	06A0A52	1	1
	9117-570	6566C4E	16	8
	9117-MMA	06D8114	8	5
	9110-S1A	06616C0	1	1
	9110-S1A	06A0A02	1	1
	9110-S1A	06D81F1	1	1
	9110-S1A	06D81D2	1	1
	9110-S1A	06A09F2	1	1
	9110-S1A	06D81F1	1	1
	9111-520	654BAFE	1	1
	9111-520	656667D	1	1
	9111-520	65667AD	1	1
	9117-570	65ED6DA	8	8

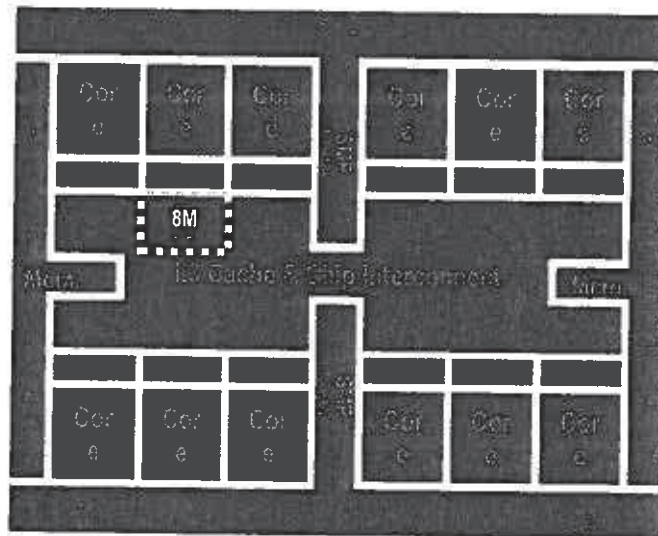
В списъка има потенциал за над 30 лицензи AIX, които да бъдат прехвърлени върху нови машини, което е съществена икономия при закупуване на нови машини.

4.1.8.3. Миграция към POWER8

С развитие на технологиите и иновациите IBM се стреми да предложи на своите клиенти най-оптималните възможности за развитие на основна сървърна инфраструктура. Новата



архитектура процесори POWER8 е създадена да отговори на завишените изисквания за производителност, надеждност и гъвкавост в скалирането.



- 22nm SOI - Single Chip Module
- 8, 10 or 12 cores per socket
- 3.02 – 4.35 GHz processors
- Up to 8 threads per core
- Integrated eDRAM L3, L4 Cache
- Improved SMP topology
- Dual memory controllers
- Dual on-chip PCIe Gen3 I/O controllers

Основния фокус на разработките на новия процесор е в увеличаване на производителността на отделното ядро чрез добавяне на специализирани модули в ядрото, в удвояване на SMP от 4 към 8 опашки, в увеличаване и оптимизиране на кеш паметта за по-добро хранване на ядрото с данни, в увеличаване на пропускателната способност на всички шини – към RAM (до 512 GB/s per socket), към входно-изходни устройства (SCM 2x PCI Gen.3 x16, DCM 2x PCI Gen.3 x16, 2x PCI Gen.3 x8), в увеличаване на обема и скоростта за достъп до RAM и въвеждане на L4 кеш за оптимизиране на паметта.

За осигуряване на достатъчен поток от данни към тези процесори се заедно с текущите карти се въвеждат и нови PCI Gen.2 и PCI Gen.3 мрежови, SAN и SAS контролери с висока скорост на обмен и плътност на интерфейсите, така че да отговарят на завишените изисквания на производителност.

Трябва да се отбележи, че резултатите на POWER8 ядра, вече надвишават производителността на най-бързите до момента процесори - P6 ядра в p595 на 5.0 GHz, видно от изведените по-долу резултати от тестове rPerf:



Model	CPU/core	GB	Result for whole system				Results per core ¹			
			P7+ Std	P7+ SMP2	P7+ SMP4	P7+ SMP8	P7+ Std	P7+ SMP2	P7+ SMP4	P7+ SMP8
770	P7/36	3.7			395.4				11.0	
770	P7+/36	3.7			517.6				14.3	
770	P7/32	3.3			321.2				8.9	
770	P7+/32	3.3			481.0				15.0	
770	P7+/36	4.22			478.9				13.3	
770	P7+/48	4.22			652.7				17.3	
770	P7+/32	3.80			410.8				12.8	
770	P7+/48	3.80			591.1				17.8	
595	P6/8	5.0		87.1				10.9		
E870	p8/32	4.02	648.8	969.8	1260.8	1349.0	10.5	15.2	19.7	21.1
E870	p8/64	4.02	1287.6	1939.6	2521.6	2698.0	10.6	15.4	20.0	21.4
E870	p8/80	4.19	848.8	1230.7	1599.9	1711.9	10.6	15.4	20.0	21.4

В резултат POWER8 базираните сървъри показват ефективно увеличаване на производителността спрямо P7+ поне с 40-50% и 70-80% спрямо Power7 сървъри със същите характеристики.

- Увеличената производителност води до по-голяма ефективност на софтуерните лицензи при лицензиране на ядра. Софтуерните производители не са коригирали цените си при въвеждането на POWER8, а едно ядро е близо 2-пъти по-производително от тези на предишните поколения в същия клас сървъри.
- По-голямата плътност и брой ядра на процесорите позволява, завишените изисквания за производителност да се удовлетворяват и от по-малки сървърни конфигурации, с по-ниско TCO.
- Увеличения брой LPARs, които могат да се дефинират на едно ядро до 20, позволява да се гранулира по-точно необходимите ресурси.
- SMT8 – едновременно изпълняване на до 8 нишки, осигурява допълнителна производителност при многопотребителски процеси. Това се комбинира с изключително големия кеш 10MB L3 на ядро и допълнителен L4 в паметта. Нишки за изпълнение с подобни или еднакви данни и код се зареждат в едни и същи ядра и така се намалява времето на процесора за чакане на данни от други процесори, RAM или диск.
- Компресия на паметта – реализиран софтуерно в Power7 (в свободните цикли на процесора) и хардуерно в POWER8 - механизъм, който осигурява допълнително памет над реално достъпната, като част от RAM се компресира и така се разполага

¹ Стойностите са изчислени на база тестовия резултат за цялата машина. За SMP4,SMP8 резултати се използват LPAR с 20 или 40 дефинирани ядра



върху DRAM. Хардуерния модул в процесора извършва компресията и декомпресията във фонов режим и работи директно в кеша и паметта, като по този начин натоварва по-малко шините памет.

- Миграцията на работещи LPAR от една машина на друга – Partition Mobility е ефективно средство за осигуряване на висока надеждност, при планирани действия от администраторите. Тя е ефективна при висока скорост на обмен на данни по LAN и SAN, области, в които има голям напредък от предишните поколения сървъри насам.
- Enterprise Pools – мобилно лицензирани памет и ядра могат да бъдат премествани от една в друга машина в рамките на един и същ pool, в зависимост от текущите нужди на приложенията. Това не налага намеса в LPAR и приложенията, а те получават повече памет и процесорно време през PowerVM.
- Разширяването на POWER Linux базираните решения в IBM е дългосрочна инициатива, в резултат на което се предоставя алтернативна на AIX платформа подходяща за съвременните софтуерни решения:
 - Почти целия софтуер разработван и предлаган от IBM работи и върху Power Linux
 - Лицензирането, а от там и цената софтуерния лиценз на ядро е значително по-ниско в полза на Power Linux (P7-P8 running AIX PVU – 120, running Linux PVU – 70)
 - IFL - IBM предоставя възможности за по-ефективно използване на неотключения наличен капацитет, със закупуване на Linux лиценз (4 cores и 32 GB), на цена по-ниска от нормален x86 сървър с подобни параметри.
 - Нова линия сървъри работещи само с Linux, подходящи за интернет приложения базирани на софтуер с отворен код, традиционни Linux софтуерни пакети, облачни услуги и др.

4.1.9. Възможности за интеграция на новите сървъри

4.1.9.1. Hardware Management Console

Администрирането на Power Server от всички поколения е HMC конзолата чрез нея се дефинират политики за ползване и разпределение на ресурси, въвеждат се лицензи и се управляват динамично CoD ресурсите. HMC е задължителен при управлението на виртуализирани сървъри с PowerVM VIOS и PowerHA.

HMC е мястото, от което се управлява Live Partition Mobility, през конзолата оператора инициира прехвърлянето от една на друга машина. PowerVP и PowerVC работят активно с HMC, за да събират данни за поведението на наблюдаваните машини.

Новото сървъри ще изискват обновяване на софтуера на текущите HMC, но напълно се вписват в текущата реализация и ще могат да бъдат администрирани от там.



4.1.10. Възможности за интеграция на новите сървъри във виртуалната инфраструктура на банката

IBM предоставя механизми за миграция към по-нови версии със средствата на операционната система – sysbackup/sysrestore. При правене на backup се съхраняват отделно уникалните за съответната виртуална машина настройки, инсталиран софтуер и топология на устройствата, при възстановяване може да се избере да се възстановят само те и така да се мигрира към нови версии.

Друг механизъм използван активно за работа на по-стари OS е IBM Workload Partitions, механизъм базиран Software Partitioning (подобен на BSD Jails) на емуляцията на работата на по-стари версии на операционната система върху по-нова в рамките на една и съща виртуална машина.

БНБ с течение на годините е обновила генерацията на операционните системи до AIX 7.1 и VIOS 2.x, което е достатъчно високо ниво, за да е възможно и работещи машини да бъдат мигрирани към по-нови генерации на сървърите включително и без прекъсване чрез Live Partition Mobility.

В обичайния случай е необходимо LPAR да се изгаси от старата и рестартира във новата среда, като цялата специфика в разликите в драйвери и архитектури на машините се покриват от Firmware & PowerVM.

4.1.11. Механизми за интегриране и пълноценна експлоатация на вече закупен софтуер

От Power4 нататък IBM гарантира binary съвместимост на изпълнението на код върху своите машини, а от Power6 и AIX 5L, виртуалните машини могат да бъдат премествани върху по-нови поколения машини.

PowerVM, AIX и firmware осигуряват среда, максимално близка до тази на предишните поколения, виртуални интерфейси съвместими с по-старите VM LPAR, осигурявайки SMP2, SMP4, за отделни LPAR (работейки върху POWER8) като това не ограничава по-новите среди да се възползват от SMP8.

Текущия софтуер е лицензиран на ядра или PVU (логически единици съответстващи на производителността на процесорните ядра).

4.1.12. Възможност за развитие при добавяне на модули, компоненти, лицензи и системен софтуер от списъка по настоящата процедура към съществуващите сървъри.

IBM и партньорите ѝ се стремят да осигурят високата производителност на сървърите и тяхната дълга и безпроблемна експлоатация. Обичайно машините от висок клас са закупени в



конфигурация, осигуряваща висока надеждност, производителност и достатъчни ресурси, но при промяна на натоварването се налага увеличаване на памет, процесори и контролери.

Ефективен механизъм за намаляване на цената за придобиване и ROI е Capacity on Demand CoD предоставянето на ресурси. БНБ ефективно ползва механизма при основните сървъри 570, 770:

EPMA	1-Core Activation for Processor Feature EPM0
EMA2	Activation of 1 GB DDR3 Power7+ Memory

По-новите контролери FC HBA могат да бъдат използвани в съществуващите Power7 сървъри, при необходимост от по-висока скорост на обмен на данните в SAN.

С въвеждането на 10GE Ethernet преноса се налага в съществуващите сървъри да се инсталират нови комбинирани контролери с интерфейси 2 x 10GE и 2 x 1 GE, където е възможно.

Power 740 сървърите закупени за TPC са доставени без виртуализация PowerVM, това лимитира силно възможните му приложения. При необходимост може да бъде закупен лиценз за PowerVM и да бъде инсталиран върху машините.

По подобен начин машините, които участват в клъстерна конфигурация и изпитват претоварване и се нуждаят от допълнителен ресурс могат да разчитат на Upgrade на PowerHA в рамките на съществуващата процедура.

1.1 x86 сървъри

1.1.1 Модули и елементи

X86 сървърите в текущото предложение са представени от серията System X на Lenovo. System X е серия сървъри създадена от IBM, като исторически преминава през няколко трансформации на името си – IBM PC Server, Netfinity и eServer xSeries. През 2014 серията бе закупена от Lenovo. Въпреки многото промени свързани със System X, серията запазва основата си, а то е използването на изчислителната мощ на x86 процесорите.

x86 е набор архитектурни инструкции за първи път представен от Intel през 1976 в техния 8086 процесор. От тогава тези процесори се използват за изчислителна мощ на повечето персонални компютри и сървър по света. x86 сървърите са всички сървърни конфигурации които използват x86 процесори. Двата основни производители на такива процесори в наши дни са AMD и Intel, като в този документ ще се съсредоточим предимно на продуктовата гама на Intel, понеже предимно тя се използва в описаните сървъри на Lenovo.

Основните блокове които изграждат един x86 сървър са:

Процесор



Представени са от сървърните процесори на Intel Xeon, чрез двете си серии E5 и E7 и две генерации v.2 и v.3. Главното предимство на тези процесори пред останалите процесори, например тези за работните станции, е възможността за едновременната работа на повече от 1 процесор в един сървър, по високия брой ядра и поддръжката на ECC памет. Всяка от споменатите серии има по няколко модела, които споделят обща архитектура и функции, и се различават предимно по главните си параметри, работна честота, брой ядра и кеш памет. Тука правилото е, колкото са по-високи като стойност тези параметри, толкова е по-моощен процесора, и съответно цената му е по-висока.

В зависимост от предназначението на сървъра, трябва да се избере и подходящ процесор, който да балансира между производителността и цената си. Представените сървъри в този документ могат да се използват за виртуализация или като самостоятелни сървъри.

При виртуализацията обикновено е добра практика да се използват процесори с по-високи параметри и те да са поне 2 броя за един сървър. Главния параметър който се отчита е броя на ядрата, което директно влияе на броя на виртуалните процесори, които могат да се използват. Например при система която използва 2 броя процесори с по 8 ядра, виртуализацията получава 16 виртуални процесора. Ако на същата система се пусне технологията hyper-threading (позволяваща всяко ядро да изпълнява две едновременни независими задачи), виртуализацията получава двойно повече виртуални процесори – 32. Съответно колкото е по-висока работната честота, толкова по-бързо ще работи всеки един от тези виртуални процесора.

Ако сървър се самостоятелно, за определен специфичен софтуер, то параметрите на използваните процесори изцяло зависят от съответните изисквания на използваното приложение, операционна система или бази данни. Може да се използва както единичен процесор с най-ниските параметри, примерно за някаква система за наблюдение или управление, до 8 процесора от най-висок клас за приложения или бази данни с високи изисквания.

Оперативна памет

При сървърите основния параметър който се търси при паметта е големината и, като за единичен сървър тя може да започне от 2 GB и да достигне до няколко TB. Максимума памет който може да се постави в един сървър зависи от това колко е голяма всяка използвана плочка памет и колко слота за плочки памет предоставя сървър за всеки свой процесор.

Най-новите серии System X сървъри поддържат така наречената TruDDR4 памет. TruDDR паметта използват най-високо качество компоненти от Tier 1 производителните на памети, като се използват единствено памети които покриват точно определени изисквания.

При избирането на паметта за всеки сървър има определени правила:

- В един сървър могат да се използват RDIMM (Registered Memory) или LRDIMM (Load Reduced Memory), като двата вида не трябва да се използват едновременно в една конфигурация. Поради използваната технология LRDIMM паметите са с доста по-



висок капацитет, като обикновено RDIMM са плочки с големина 4, 8, 16 GB, а LRDIMM са с големина 32 и 64 GB.

- Максималния брой памети които могат да бъдат инсталирани зависи от броя на инсталираните процесори, като в зависимост от сървъра всеки процесор поддържа точно определен брой максимален брой памети, обикновено на най-новото поколение сървъри това е 12. Например за стандартен сървър с 2 процесора, могат да се сложат максимално 24 плочки, ако се използват тези с големина 64, то може да се постигне максимална памет 1 536 GB.
- Всички памети в един сървър работят на една и съща скорост, която се определя от по-малката от:
 - Скорост на паметта поддържана от използвания процесор.
 - Най-ниската от максималната скорост за дадена конфигурация от памети, която зависи от броя на използваните плочки на канал. Пример за определен модел и даден в следната таблица:

DIMM specification	RDIMM			LRDIMM
Rank	Single rank	Dual rank		Quad rank
Part numbers	46W0784 (4 GB) 46W0788 (8 GB)	46W0792 (8 GB)	46W0796 (16 GB) 95Y4808 (32 GB)	46W0800 (32 GB) 95Y4812 (64 GB)
Rated speed	2133 MHz	2133 MHz	2133 MHz	2133 MHz
Rated voltage	1.2 V	1.2 V	1.2 V	1.2 V
Maximum quantity supported**	24	24	24	24
Maximum DIMM capacity	8 GB	8 GB	32 GB	64 GB
Maximum memory capacity	192 GB	192 GB	768 GB	1.5 TB
Maximum memory at rated speed	128 GB	128 GB	512 GB	512 GB
Maximum operating speed				
1 DIMM per channel				
2 DIMMs per channel				
3 DIMMs per channel	1600 MHz	1600 MHz	1866 MHz	1866 MHz

** За 2 инсталирани процесора.

Вътрешен дисков капацитет

Дисковия капацитет изцяло зависи от големината, броя и защитния механизъм (RAID) на използваните дискове. Всеки модел сървър поддържа точно специфичен максимален брой и вид дискове. Дисковете сами по себе си се различават по няколко параметъра:

- ✓ Скорост – в зависимост от скоростта на въртене на диска- 7.2K, 10K или 15K, както и Flash дискове. От това зависи и производителността им, която обикновено се измерва в IOPS, или входно изходни операции за секунда. Тази стойност е около 85 IOPS за 7.2K



дискете, 140 IOPS за 10K, 180 IOPS за 15K и от 5000 до над 100 000 IOPS за Flash дискете в зависимост от модела му.

- ✓ Големината – 2.5 или 3.5 инча, това се определя от използвания модел сървър. Обикновено бързите дискове могат да бъдат и двата фактора, а високо-капацитетните 7.2K само 3.5 инча.

Защитата на данните от загуба обикновено се осъществява чрез RAID технология, като най-използваните са:

- ✓ RAID 1 (Mirror, Огледално копие) – осъществява се от 2 диска, като едни и същи данни се записват и на двата диска, така при повреда на един от двата нямаме загуба на информация. При този метод се губи половината капацитет, или от двата диска използваме капацитета само на единия.
- ✓ RAID 5 – използват се 3 или повече дискове. На част от дискете се записват данните, а на последния се изчислява и записва контролна сума. Тези суми се разпределят на всички дискове. При отпадане на един диск нямаме загуба на информация. При този метод губим само един диск независимо колко броя използваме в една група.

Избора на RAID групиране се избира между компромиса между капацитет, защита и бързодействие. RAID 1 има най-високо бързодействие и защита, но голяма загуба на капацитет. RAID 5 е компромисно решение, като има по-слабо бързодействие и защита но минимална загуба на капацитет.

В сървърните системи, защита на данните е задължителна, като RAID функционалността се извършва обикновено от специализирани контролери, като специфичния контролер има съответната функционалност каква RAID защита може да извършва. Допълнителна функционалност е бързодействието чрез добавяне на кеш памет и защита на данните чрез батерия.

Обикновено използването на вътрешен дисков капацитет в сървърите не е задължително, като съответния капацитет се предоставя от някакъв вид външен дисков масив. Използването на външен дисков масив обикновено е добра практика, поради факта че там данните са многократно по-защитени, а понякога и е задължително, например при клъстеризирани системи, изискващи едновременно използване на едни и същи данни. Споделянето на едни и същи данни между голям брой сървъри е основата на виртуализацията работеща с дисков капацитет.

Комуникационни модули

Тези модули изцяло зависят от изискванията ни за свързаност, като това могат да бъдат както свързване към LAN или WAN, така и връзката ни към дисковите масиви.

Ethernet свързаността обикновено е вградена в сървърите като в зависимост от модела може да им от 2, 4 или повече броя Gigabit порта. Допълнително портове могат да се увеличат чрез модули предоставящи 2 или повече Gigabit или 10Gb порта. Тези модули могат да използват за свързаност мед или оптика.



Свързаността към дисковите масиви може да се осъществи по няколко начина. Директна връзка чрез съответните Host Buss Adapter-и, чрез Fibre Channel протокол (оптична свързаност) или FCoE и iSCSI протоколи чрез Ethernet модулите, които поддържат тази функционалност.

Захранване

Добрите практики показват че е изключително важно резервирането на захранването. В зависимост от модела на сървъра, могат да се инсталиран едновременно да работят 1, 2 или повече захранващи модула. Добре е да се стремим винаги да използваме минимум 2 броя, като всеки модул по възможност да е свързан към различен захранващ кръг. Това ни предпазва както от повреда на едно от захранването, така и при отпадането на един от захранващите кръгове. Допълнително е задължително защита на захранването чрез UPS устройства, което предпазва сървърната ни инфраструктура както от внезапно спиране на захранването, така и от пикове, шумове и други проблеми със захранващата мрежа.

1.1.2 Приоритетни инициативи

Виртуализация

Сървърната виртуализация е технология, чието създаване се е наложило поради много бързото развитие в последните години на микропроцесорните технологии, изчислителните ресурси и необходимостта за преодоляване на някои ограничения, наложени от използването на чисто физическа инфраструктура. Използвайки технологии за сървърна виртуализация IT инфраструктурите, постигат много по-високо консолидиране на услуги върху единица физически ресурс, което от своя страна води до драстично намаляване на разходите за хардуер, охлаждане и електричество. Допълнително виртуализацията осигурява логически слой, който поради изцяло софтуерната си натура позволява динамично и бързо конфигуриране на всеки един компонент – дискови устройства, мрежови устройства, процесори, памет и т.н.

В инфраструктурата на BNB се използват 2 типа виртуализация, определени от използваната технология и работещите услуги върху тях.

- **PowerVM** – Е виртуализацията осъществена върху POWER сървъри. Предназначена е за системи, приложения и бази данни високи изисквания към ресурсите. Тази виртуализация ще се използва за така наречените Enterprise Applications (услуги). Повече за самата PowerVM виртуализация може да бъде прочетено в точка 2.1.1 от настоящия документ.
- **x86 Server** – Осъществява се върху x86 сървъри, като се използва серията System X на Lenovo и UCS на Cisco. Тази инфраструктура се използва главно за Windows базираните виртуални машини, както и допълнителни услуги свързани с инфраструктурата, управление, конфигуриране, Novel и други които нямат големи изисквания към ресурсите. В БНБ виртуализацията се осъществява чрез VMware vSphere софтуер, като има възможност при желание да се използват и други технологии като Microsoft Hyper-V, Citrix Xen, KVM и други. Повече за самата x86 виртуализация може да бъде прочетено в точка 30 от настоящия документ.



В момента са виртуализирани само част от системите в банката, като целта е в бъдеще всички системи които позволяват да бъдат прехвърлени на виртуалната x86 инфраструктура, с което да се направи пълна сървърна консолидация, което да помогне в управлението, поддръжката както и другите приоритетни инициативи като частен облак, Active-Active център за данни, и център за защита при аварии.

При избора на сървър за x86 виртуализация е хубаво да се спазват следните добри практики:

Процесор

2 процесора е най-оптималната бройка при виртуализация. Добре е процесора да е последно поколение, с минимум 8 ядра и възможно най-висока работна честота. Примерен процесор отговарящ на тези условия е Intel Xeon 2690v3 (12 ядра и 2.6 GHz работна честота).

Оперативна памет

При виртуализация трябва да се предвиди голямо количество памет. Оптимален минимум може да се приеме 256 GB като може да се мисли и за двойно по-голямо количество.

Дисков капацитет

Данните на виртуалните машини работещи върху сървъра, задължително се разполагат на външен дисков масив. За работата на самата виртуализация, е добре да се ползва дисков капацитет, разположен в сървъра за да е независима работата ѝ, от тази на дисковия масив. 2 броя твърди дискове, защитени чрез RAID 1 е подходяща конфигурация.

Active-Active DataCenter

За изграждането на Active-Active център за данни е нужно сървърите като ресурс да са разпределени по-равно между дават сайта. Допълнително е нужно ресурсите във всеки от сайтовете да е така оразмерен, че да поеме цялата инфраструктура при отпадане на единия център за данни.

DRC

Този център за данни е нужен при отпадане на другите два сайта, в случай на някаква авария. В този сайт ще се прави копие на всички данни, и при авария ще се възстановят най-критичните услуги. Поради това е нужно да се предвидят x86 сървъри, чиито ресурси като големина е добре да са на ниво колко 30% от основните центрове за данни.

1.1.3 Оборудване

В текущото предложение има няколко модела x86 сървъри, които са разделени на две основни групи, такива за вграждане в сървърен шкаф и такива предназначени за блейд шаси.

Сървърите предназначени за вграждане в сървърен шкаф, са представени от серията System x3xxx като следващите цифри в сървърния модел са:

- ✓ 2-та цифра се увеличава в зависимост от възможностите на сървъра.

- ✓ 3-тата цифра е 0 за свободно стоящите модели и 5 за сървърите за вграждане в шкаф.
- ✓ 4-тата цифра е 0 за Intel процесори и 5 за AMD Opteron процесори.

В представения лист с компютърно оборудване и компоненти са предоставени 3 модела в няколко базови конфигурации с минимално количество оперативна памет и поне 2 вида процесори в зависимост от нуждите. Допълнително са предоставя възможност за добавяне на най-различни компоненти, като допълнително процесори, допълнителна памет, дискове и други.

Съответните предоставени модели са:

- **Lenovo System x3550 M5** – базов модел. Подходящ за виртуализация.



- ✓ **Фактор:** 1U за вграждане в сървърен шкаф
- ✓ **Процесори:** до 2 броя Intel Xeon E5-2600 v3 серия
- ✓ **Памет:** до 1.5 TB
- ✓ **Дисков капацитет:** до 24 TB за 3.5 инчовите модели и 14.4 TB за 2.5 инчовите модели

Моделът 1 с големина 1U, поради това заема малко място. Поддържа използването на малък брой дискове и допълнителни PCI платки. Поради тези факти е изключително подходящ за виртуализация – при нея не се изисква особено голям вътрешен дисков капацитет и допълнителни комуникационни модули.

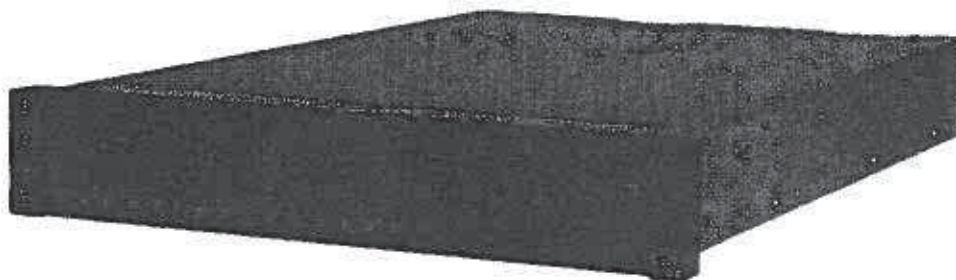
Примерна Конфигурация 1 е конфигуриран сървър с 2 процесора Intel Xeon E5-2690v3 със 384GB оперативна памет, 2 диска 300GB, и HBA платка за връзка към SAN инфраструктурата:

Примерна Конфигурация 1

PN	Описание на продукта	Брой
5463L2G	IBM System x3550M5 Процесор: Xeon 12C E5-2690v3 135W 2.6GHz/2133MHz/30MB Памет: 1x16GB TruDDR4 Memory PC4-17000 LP RDIMM Твърд диск: 2.5in HS SAS/SATA, без диск И/О адаптери: 1 x четири-портов Ethernet (вграден) RAID контролер: SR M5210	1

	Захранване: 1 x 750W Форм Фактор: Rack	
00KA076	Intel Xeon 12C Processor Model E5-2690v3 135W 2.6GHz/2133MHz/30MB	1
46W0800	32GB TruDDR4 Memory (4Rx4, 1.2V) PC417000 CL15 2133MHz LP LRDIMM	12
00AJ081	IBM 300GB 15K 6Gbps SAS 2.5in G3HS HDD	2
42D0510	QLogic 8Gb FC Dual-port HBA for IBM System x	1
00KA079	System X 750 W High Efficiency Titanium AC Power Supply (200- 240V)	1

- **Lenovo System x3650 M5** – Подходящ е да се използва в случай когато се изисква по-голям брой вътрешни дискове или разширителни платки.



- ✓ Фактор: 2U за вграждане в сървърен шкаф
- ✓ Процесори: до 2 броя Intel Xeon E5-2600 v3 серия
- ✓ Памет: до 1.5 TB
- ✓ Дисков капацитет: до 86.4 TB за 3.5 инчовите модели и 31.2 TB за 2.5 инчовите модели

Модел с големина 2U, което му позволява да използва значително по-голям брой дискове и разширителни плаки. Поради това е подходящ както за виртуализация така и за самостоятелен сървър където се изисква по-голям вътрешен дисков капацитет или в случай когато се изискват по-голям брой комуникационни модули.

В Примерна Конфигурация 2 е конфигуриран сървър с 2 процесора Intel Xeon E5-2640v3 с 64GB оперативна памет, 8 диска 900GB и допълнителна кеш памет за RAID контролера:

Примерна Конфигурация 2



P.N.	Описание на продукта	Брой
5462F4G	IBM System x3650 M5 Процесор: Xeon 8C E5-2640v3 90W 2.6GHz/1866MHz/20MB Памет: 1x16GB TruDDR4 Memory Твърд диск: 2.5in HS SAS/SATA, без диск И/О адаптери: 1 x четири-портов Ethernet (вграден) RAID контролер: SR M5210 Захранване: 1 x 750W Форм Фактор: Rack	1
00FK644	Intel Xeon Processor E5-2640 v3 8C 2.6GHz 20MB Cache 1866MHz 90W	1
46W0796	16GB TruDDR4 Memory (2Rx4, 1.2V) PC4-17000 CL15 2133MHz LP RDIMM	3
00NA296	IBM 900GB 10K 12Gbps SAS 2.5in G3HS 512e SED	8
47C8656	ServerRAID M5200 Series 1GB Cache/RAID 5 Upgrade for IBM Systems	1
00FK932	System x 750W High Efficiency Platinum AC Power Supply	1

- **Lenovo System x3850 X6** – 4-процесорен модел, подходящ за приложения изискващи големи изчислителни мощности.



- ✓ Фактор: 4U за вграждане в сървърен шкаф
- ✓ Процесори: до 4 броя Intel Xeon E7-4800/8800 v3 серии
- ✓ Памет: до 6 TB



- ✓ Дисков капацитет: до 8 броя 2.5 инчови диска или 16 броя 1.8 инчови SSD диска.

Поради факта че този модел поддържа 4 процесора и голямо количество оперативна памет, той е подходящ за самостоятелен сървър (без виртуализация) на който има нужда да работи приложение изискващо голяма изчислителна мощност, например голяма база данни с включени аналитични функции.

В Примерна Конфигурация 3 е конфигуриран сървър с 4 процесора Intel Xeon E7-4890v2 с 1536GB оперативна памет, 2 диска 300GB за операционна система и 2 допълнителни Flash контролера, всеки с капацитет 2600GB:

Примерна Конфигурация 3

P.N.	Описание на продукта	Брой
3837C4G	IBM System x3850M6 Процесор: 2x Compute Book Xeon 15C E7-4890v2 155W 2.8GHz/1600MHz/37.5MB Памет: 4X8GB Твърд диск: 2.5in HS SAS/SATA, без диск И/О адаптери: 1 x дву-портов Ethernet (вграден) RAID контролер: SR M5210 Захранване: 2 x 900 W Форм Фактор: Rack	1
44X3996	X6 Compute Book Intel Xeon 15C Processor Model E7-4890v2 155W 2.8GHz/1600MHz/37.5MB	3
46W0676	32GB (1x32GB, 4Rx4, 1.35V)PC3L-12800 CL11 ECC DDR3 1600MHz LP LRDIMM	48
00NA281	IBM 300GB 15K 12Gbps SAS 2.5in G3HS 512e SED	2
00JY001	IBM 2600GB Enterprise io3 Flash Adapter for System x	2
44X4132	IBM 900W Power Supply	2

Блейд серията сървъри System X на Lenovo са предназначени за вграждане в Flex System на Lenovo. Flex System е интегрирана инфраструктурна платформа изградена от изчислителен ресурс (сървъри), дисков масив и мрежови ресурси. Основата на системата е шаси с големина 10U, което побира 14 устройства, като е лесно скалируема чрез добавяне на допълнителни шасита. Освен System X сървъри, Flex System поддържа работата и на Power Systems сървъри.

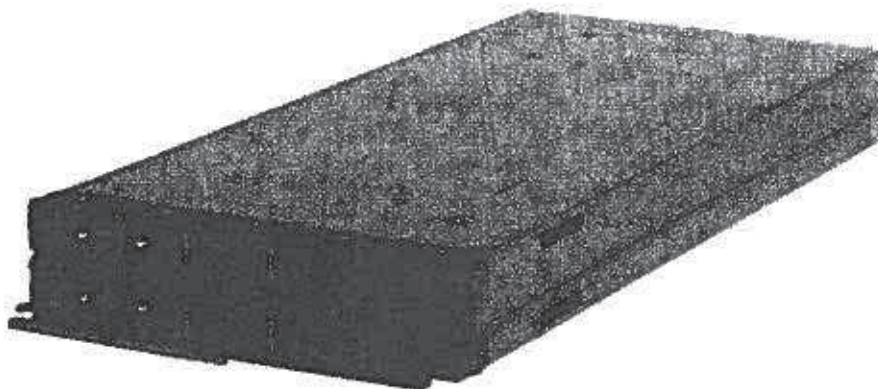
В текущото предложение са включени следните сървърни модели System X за работа с Flex System:

- Flex System x220 – базов модел предназначен за не-виртуализирани системи.

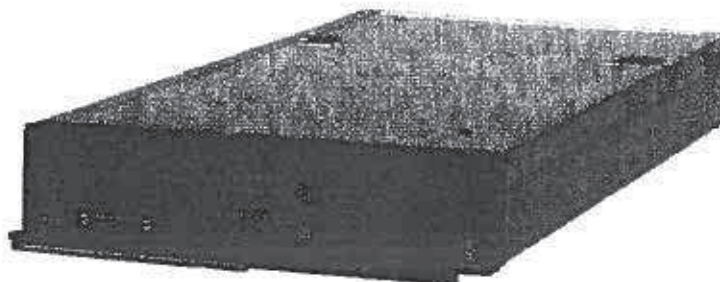


- ✓ Фактор: Half-Wide за вграждане във Flex System.
- ✓ Процесори: до 2 броя Intel Xeon E5-2400 серия.
- ✓ Памет: до 192 GB.
- ✓ Дисков капацитет: до 2 броя 2.5 инчови диска.

- Flex System x222 – модел съставен от 2 отделни сървъра. Подходящ за е нужно постигане на голям брой сървъри на ограничено място. Двата сървъра работят самостоятелно и не могат да се комбинират като 4-процесорен сървър.



- ✓ Фактор: Half-Wide за вграждане във Flex System.
 - ✓ Процесори: до 2 броя Intel Xeon E5-2400 серия за всеки сървър.
 - ✓ Памет: до 192 GB за всеки сървър.
 - ✓ Дисков капацитет: до 1 брой 2.5 инчов диск за всеки сървър.
- Flex System x240 M5 – модел подходящ за виртуализация и самостоятелни системи с високи изисквания.



- ✓ Фактор: Half-Wide за вграждане във Flex System
- ✓ Процесори: до 2 броя Intel Xeon E5-2600 v3 серия.
- ✓ Памет: до 1.5 TB
- ✓ Дисков капацитет: до 2 броя 2.5 инчови диска.

Следващата Примерна Конфигурация 4 е съставена от 1 Flex System шаси, с 6 сървъра System x240 M5 всеки с по 2 процесора Intel Xeon E5-2670v3, 256 GB оперативна памет и 2 диска. Допълнително за свързаност шасито е конфигурирано с 2 Converged комутатора за LAN и SAN свързаност.

Примерна Конфигурация 4

P.N.	Описание на продукта	Брой
8721A1G	IBM Flex System Enterprise Chassis with 2x2500W PSU, Rackable	1
43W9049	IBM Flex System Enterprise Chassis 2500W Power Module	2
00D5823	IBM Flex System Fabric CN4093 10Gb Converged Scalable Switch	2
68Y7030	IBM Flex System Chassis Management Module	1
43W9078	IBM Flex System Enterprise Chassis 80mm Fan Module Pair	2
9532J6G	IBM Flex System x240 M5 Compute Node, Xeon 12C E5-2670v3 120W 2.3GHz/2133MHz/30MB, 1x16GB, O/Bay 2.5in SAS	6
00JX054	Intel Xeon Proc E5-2670 v3 12C 2.3GHz 30MB Cache 2133MHz 120W	6
95Y4821	16GB TruDDR4 Memory (2Rx4, 1.2V) PC4-17000 CL15 2133MHz LP RDIMM	90
00AJ081	IBM 300GB 15K 6Gbps SAS 2.5in G3HS HDD	12

1.1.4 Концепция и стъпки на имплементация

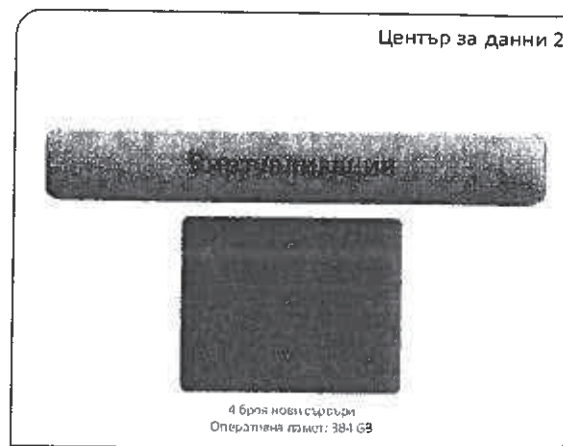
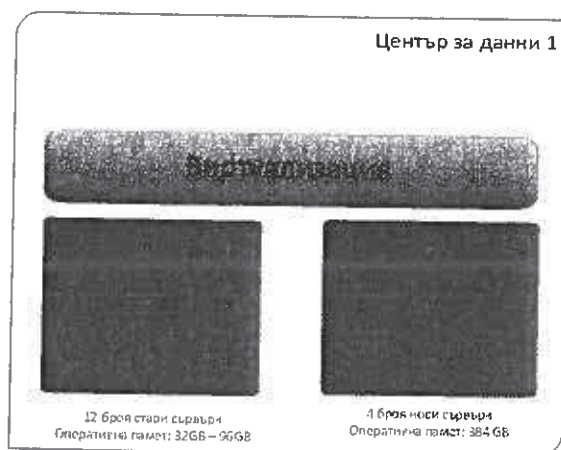
1.1.4.1 Текущо състояние

В момента в БНБ сървърните ресурс са разпределени в двата центрове за данни на банката, като сървърите могат да се разделят на 2 основни групи – виртуализирани сървъри и физически самостоятелни сървъри.

Виртуалната инфраструктура в основния сайт е съставена от 12 стари сървъра. Всички те са IBM, като се състоят от няколко поколения и модели сървъри – x346, x345, x3550, x3650, x3650 M2 и x3650 M3. Допълнително има и няколко BladeCenter сървъра – HS20, HS21.

Допълнително тази година са закупени 8 нови сървъра с последно поколение процесори и 384GB оперативна памет. Тези сървъри са разпределени по 4 в двата центъра за данни.

Допълнителните хардуерни не-виртуализирани сървъри по принцип работят приложения с ниски изисквания към ресурсите.



1.1.4.2 Възможности за обновяване на текущата сървърна база и добавяне на модули компоненти, лицензи за ОС и системен софтуер към наличната инфраструктура.

Главната стратегия при x86 сървърите е да се премине на изцяло виртуализирана среда, с може би малко изключения при някои инфраструктурни услуги за управление.

Част от текущите сървъра които образуват виртуалната среда, въпреки че не са последно поколение, могат да продължат да се използват известно време. За някои от тях (тези от сравнително не толкова старата серия x3650 M3) е добре да се закупи допълнителна оперативна памет. Допълнително може на част от сървърите да се закупят нови комуникационни платки – 10Gbps или допълнително дискове при нужда. Поради факта че текущите сървъри и всички нови продукти са от един производител (IBM/Lenovo), то всички добавени компоненти не нарушават гаранцията и поддръжката на съществуващите сървъри.

Основната стратегия при текущата стара сървърна инфраструктура е постепенно да се започне замяната на старата техника с нова, като най-старото поколение ще се извади от експлоатация, и тези от по-ново поколение ще се използват в текущата инфраструктура за управление и наблюдения или като DMZ сървъри. Новите сървъри ще запазят използването на съществуващите платформи на операционните системи, и системен софтуер, понеже са от същата серия – System X.

1.1.4.1 Интеграция на новите сървъри в използваните в банката системи за мониторинг и управление

Всички закупени нови сървъри съдържат в себе си модула за управление и наблюдение Integrated Management Module II (IMM2). Чрез него сървърите могат директно да се управляват или да се интегрират в текущата инфраструктура за управление на банката и инфраструктурата за наблюдение като Nagios.

Допълнително сървърите са оборудвани със следните модули:

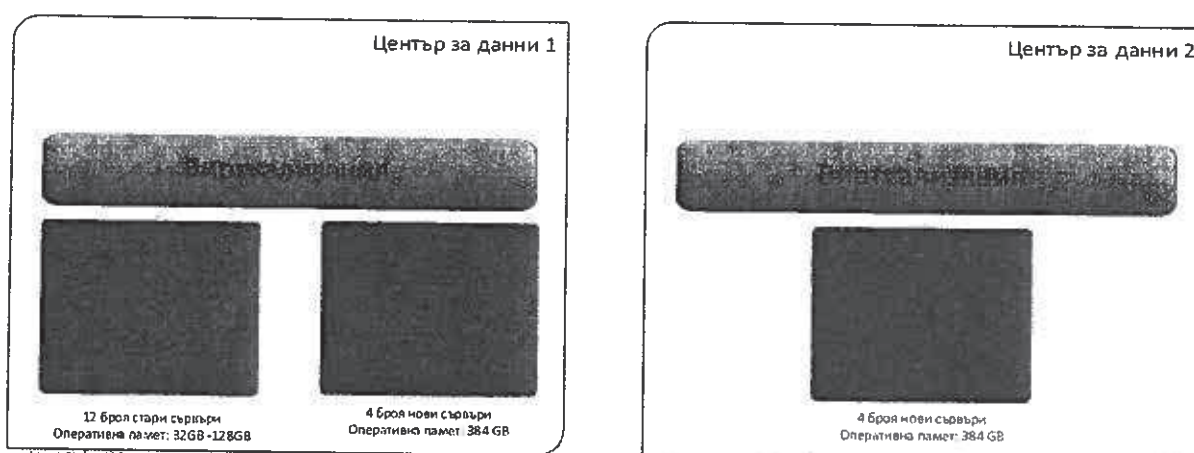


- UEFI – за подобро инсталиране, конфигуриране и обновяване на системните софтуери на сървърите.
- Интеграция с IBM Systems Director предоставящ разширени възможности за управление.
- Интегрирани Trusted Platform Modules (TPMs) даващи възможност за разширени криптографска защита.

1.1.4.2 Стъпки за развитие на сървърната x86 инфраструктура

СТЪПКА 1 – ОПТИМИЗИРАНЕ НА ВИРТУАЛНАТА ИНФРАСТРУКТУРА.

В тази стъпка ще се използва текущата виртуална инфраструктура в двата центъра за данни, като на част от старите сървъри ще се направи ъпгрейд на оперативната памет до 128 GB.



При тази стъпка не са необходими значителни промени в текущата инфраструктура и ще позволи пълноценно да се използват закупената до този момент сървърна инфраструктура. Реално тази стъпка може да продължи докато не започне изграждането на Active-Active сайтовете. Фази на тази стъпка:

- ✓ Анализ на съществуващата инфраструктура и планиране на изпълването и закупуването на нови компоненти.
- ✓ Закупуване на нови компонент и добавянето им към текущите сървъри.

Тази стъпка би отнема 1 календарен месец.

Тази стъпка не зависи пряко от която и да е друга стъпка в документа.

Преимствата за банката, ще бъдат увеличен ресурс на съществуващите сървъри и по-пълноценното им използване при x86 виртуализацията.



СТЪПКА 2 - ИЗГРАЖДАНЕ НА ACTIVE-ACTIVE ЦЕНТРОВЕ ЗА ДАННИ.

Целта в тази стъпка е максимално да се изравнят ресурсите в двата центрове за данни. Това ще стане като се запази текущата инфраструктура в основния сайт и се закупят 4 нови сървъра (Примерна Конфигурация 1) във втория сайт. Състои се от следните фази:

- ✓ Закупуване на нови сървъри
- ✓ Инсталиране и виртуализиране на новите сървъри във втория център за данни
- ✓ Изграждане на единна виртуална инфраструктура между двата сайта



Тази стъпка би отнела **2 календарни месеца**.

Тази стъпка не зависи пряко от която и да е друга стъпка в документа.

Тази стъпка ще позволи използването на виртуалната структура активно в двата центъра за данни, като при завършването и заедно с съответните промени в мрежовата инфраструктура, на практика ще се изпълни стратегията за Active-Active DC.

СТЪПКА 3 - ОПТИМИЗИРАНЕ НА ACTIVE-ACTIVE ЦЕНТРОВЕ ЗА ДАННИ.

В бъдеще ще се изравнят напълно ресурсите в двата центъра за данни, като се извадят от експлоатация всички стари сървъри и ще се заменят с 4 нови – Примерна Конфигурация 1. Съдържа в себе си следните фази:

- ✓ Закупуване на нови сървъри
- ✓ Интеграция на новите сървъри в текущата виртуална инфраструктура
- ✓ Постепенното премахване на старите сървъри от виртуалната инфраструктура
- ✓ Преизползване на старите сървъри в инфраструктурата на банката ако е технически възможно и изваждане от експлоатация на ненужните сървъри



Тази стъпка би отнела **3 календарни месеца**.

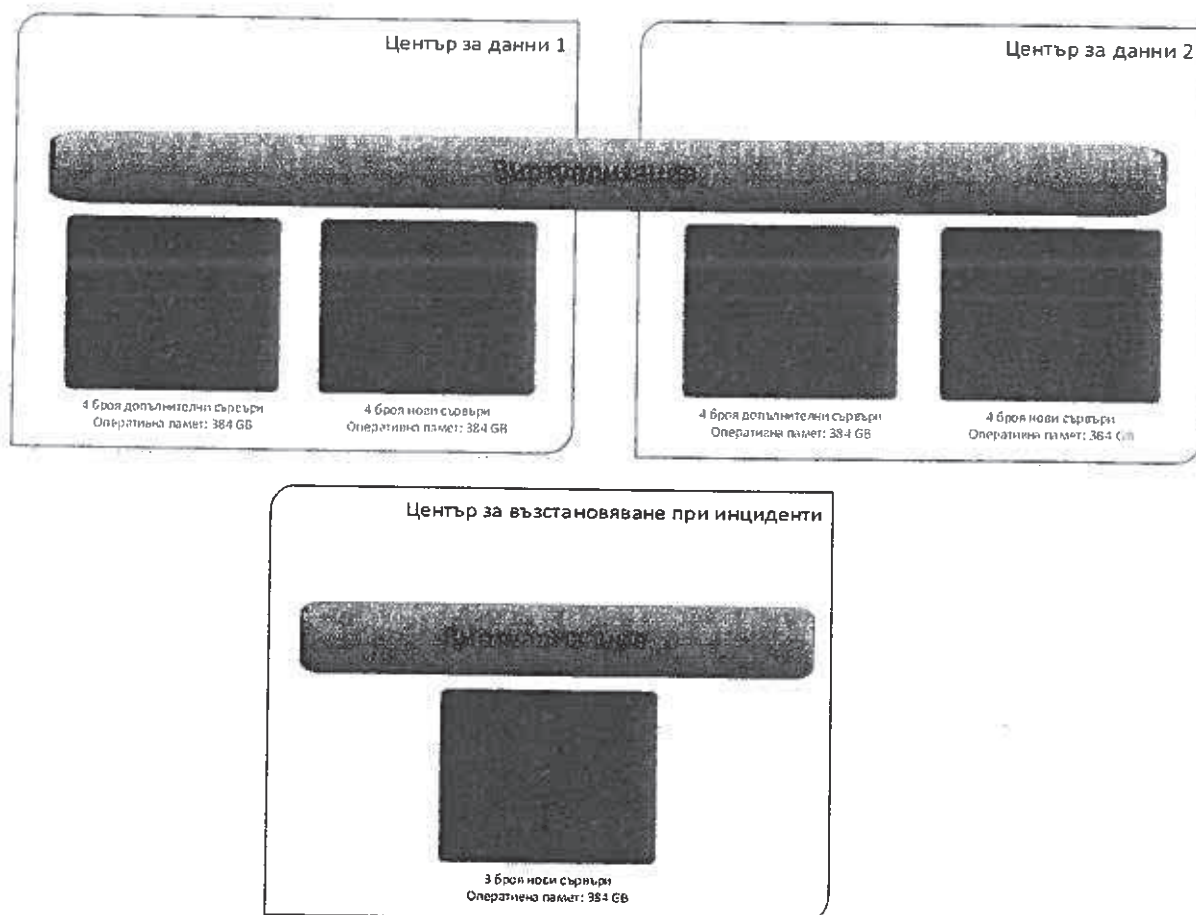
Тази стъпка не зависи пряко от която и да е друга стъпка в документа.

В този момент банката ще има напълно работеща и оптимизирана Active-Active сървърна инфраструктура. Същевременно ще се освободи ресурс на старите сървъри за да се преизползва където е нужно. Най-старите сървъри ще се премахнат от инфраструктурата което ще спести на Банката плащането на ненужна поддръжка и ще подобри сигурността на база отказо-устойчивост на техниката.

СТЪПКА 4 – ИЗГРАЖДАНЕ НА ЦЕНТЪР ЗА ВЪЗСТАНОВЯВАНЕ ПРИ ИНЦИДЕНТИ.

Свързана е с изграждането на център за възстановяване при инциденти, където ще бъде предоставен ресурс приблизително около 30 % от основните сайтове:

- ✓ Закупуване на нови сървъри
- ✓ Интегриране на новите сървъри в текущата инфраструктура
- ✓ Тестване и подготвяне на новата техника да поеме услуги в случай на инцидент



Тази стъпка би отнела **1.5 календарни месеца**.

Тази стъпка не зависи пряко от която и да е друга стъпка в документа.

В този момент Банката ще има сървърна инфраструктура изградена по най-добрите световни практики, с два активни сайта и един отдалечен резервен сайт за работа по време на инциденти. Тази инфраструктура ще даде на банката достатъчно ресурси и сигурност на всички текущи и бъдещи ИТ услуги.

4.2. Дискови масиви

4.2.1. Концепция за развитие

Дисковите масиви са един от основните блокове за постигане на всички стратегически инициативи на банката. Те се грижат за съхранението, управлението и защитата на най-важния ресурс за всяка организация – данните/информацията.

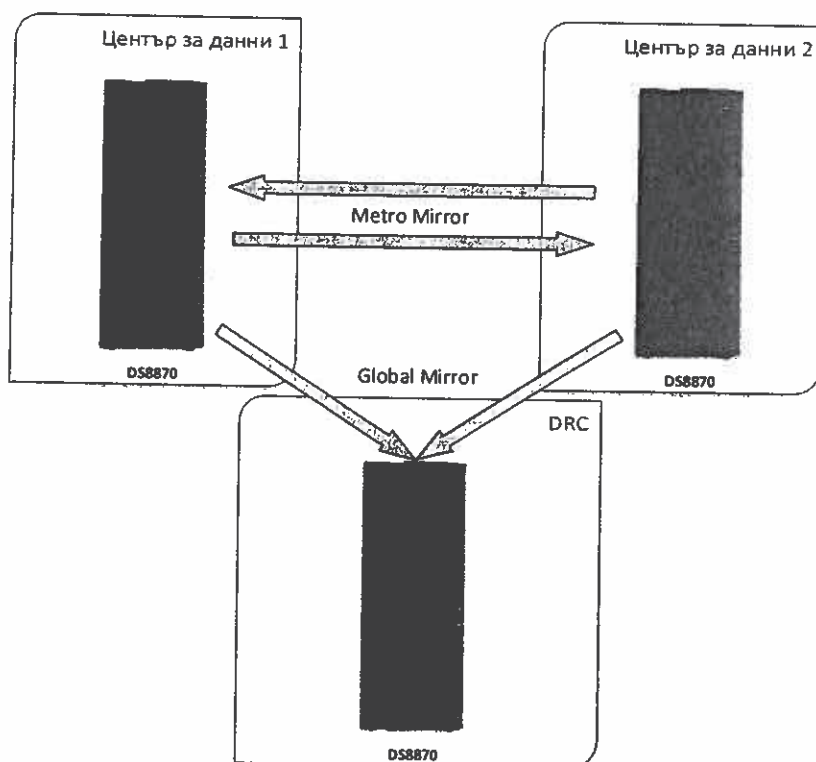
Най-общо можем да разделим дисковите масиви в банката на две основни групи, такива които работят с Enterprise приложения, и такива които ще обслужват Non-Enterprise приложения.



4.2.1.1. Дискови масиви за работа с Enterprise приложения

Основната концепция на работата на enterprise приложенията е постигането на активна работа на услуги и в двата основни центъра за данни, или Active-Active Data Center. Основната задача на дисковите масиви в тази концепция е грижата всички данни да са консистентни и в двата сайта. Това позволява както активната работа на дадена услуга в кой да е от двата сайта, така и непрекъсваемостта при отпадане на един от центровете. Допълнително данните ще се копират и на третия отдалечен DRC сайт за допълнителна защита при инциденти.

Описаната до тук концепция, функционалности както и стандартното съхранение, управление и защита на данните се предоставя от серията enterprise дискови масиви DS8000 или конкретно модела DS8870. За да се постигнат споменатите вече стратегически инициативи като Active-Active центрове за данни и DRC, ще се нуждаем от дисков масив DS8870 във всеки от трите сайта.



Активните данни ще се копират синхронно между двата основни центрове за данни чрез Metro Mirror. Допълнително чрез HyperSwarm данните равноправно ще бъдат достъпвани от двата сайта. HyperSwarm чрез Metro Mirror синхронизира постоянно данните между двата основни дискови масиви и предоставя единна виртуална среда на дялове от двата масива и гарантира, че всяка машина ще работи с локалното си копие. При преместване на LPAR в отдалечения DC, новия дисков масив започва да работи с новата виртуална машина, обръщайки репликацията, така че първоначалния дисков масив да не „изостава“. В случай, че



основния дисков масив отпадне (планирани или не планирано), всички приложения се прехвърлят да работят в резервния дисков масив.

Данните към DRC ще се копират асинхронно чрез Global Mirror. Така ще имаме допълнително копие на всички данни в отдалечени център за данни, и при отпадане на двата основни сайта, критичните услуги могат ръчно да се пуснат да работят там временно.

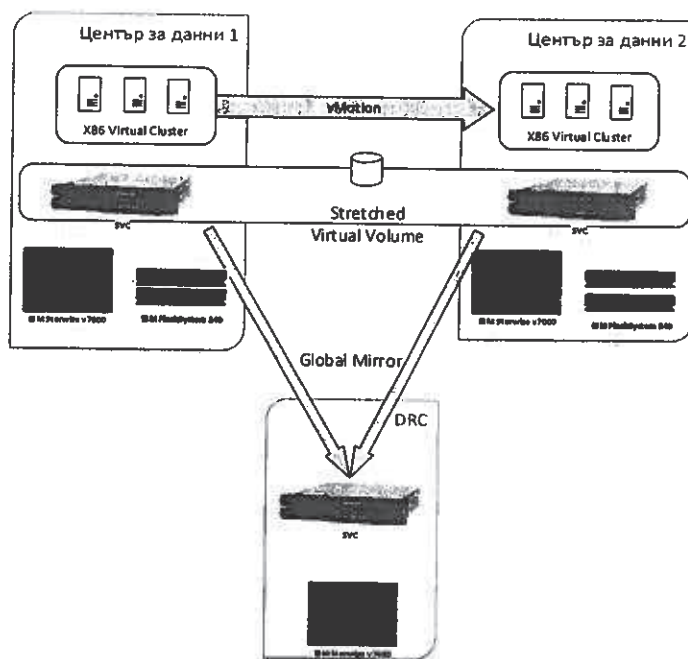
В конфигурацията трябва да бъде предвиден и механизъм за превенция, от така наречения split-brain ефект. При IBM решенията това се постига, чрез така наречения quorum диск. При клъстериране на два или повече дискови масива има специфичен алгоритъм, който може да бъде повлиян от потребителя посредством ръчни настройки. Идеята е да се определи един кворум диск, който се използва по две причини:

- Да определи активния node когато точно половината от членовете на клъстер грубата отпадна (split brain prevention)
- Да пази на себе си най-важната системна конфигурация, за клъстера.

4.2.1.2. Дискови масиви за работа с non-enterprise приложения

Тази група от дискови масиви ще работи предимно с x86 сървърната виртуална инфраструктура където работят предимно non-enterprise услуги базирани на Windows или Linux операционни системи, включително и не малка част от инфраструктурата на банката (Active Directory, File Servers и други).

При тази група концепцията за Active-Active DataCenter и DRC е подобна на описаната по-горе, осъществена с DS8870. Тука основните функции ще се поемат от SAN Volume controller (SVC), чрез виртуализация на дисковото пространство предоставено от съответните дискови масиви от среден клас и изцяло flash базирани масиви. SVC ще предостави определена enterprise функционалност на тези дискови масиви като Metro Mirror и Global Mirror, както и единен централизиран панел за управление на всички виртуализирани дискови масиви.



Концепцията да се изгради така наречения SVC stretched cluster, който ще се интегрира изцяло с виртуалната сървърна инфраструктура на VMware. Това ще позволи виртуалната инфраструктура да се възползва от всички функционалности като преместване на виртуални машини в реално време (vMotion), Storage vMotion и VMware HA между двата сайта.

Клъстера ще бъде изграден, като се използва SVC устройства разположени в двата основни сайта. Допълнително ще се поставят SVC устройства в DRC сайта, където ще се прави още едно асинхронно копие на данните за защита при инциденти.

Основния виртуализиран дисков капацитет ще бъде предоставен от дискови масиви среден клас Storwize v7000, където ще са разположени основната част от данните използвани от x86 виртуалната инфраструктура. За да се увеличи бързодействието на дисковото пространство и за да се посрещнат високите изисквания на инфраструктурата за предоставяне на виртуални работни места (VDI), ще се добавят допълнително изцяло flash дискови масиви от типа IBM FlashSystem 840.

Важно е да се отбележи, че SVC решението позволява работа и с non-IBM дискови системи. Това означава, че банката може да включи към виртуалния disk pool и всички налични дискови масиви.

Тук отново ще се ползва quorum диск концепцията представена в предходната точка, за адресиране на split-brain проблема.

4.2.1.3. Дискови масиви за Backup & Archive

Освен описаните по-горе концепции за използване на дискови масиви, ще е нужен допълнителен дисков капацитет за извършването на Backup to disk. Според добрите практики



тези защитени копия на данните не трябва да се съхраняват на същите дискови масиви които работят с работните данни. Затова е добре да се закупят допълнителни устройства за извършването на резервни копия. Тази концепция е представена в раздела „Backup & Archiving“ в този документ.

Като цяло е добре да бъдат предвидени още една тройка V7000 дискови масиви, с различна конфигурация (по-бавни дискове, по-висока плътност). Не е необходимо те да бъдат виртуализирани.

4.2.2. Стъпки на имплементация

В банката в момента работят няколко дискови масива. В основния сайт работят DS8700, DS6800 и един не IBM дисков масив. Част от тези масиви се използват от x86 виртуалната инфраструктура, а друга част от Power сървърите. Във втория център за данни работят DS8100 и един нов DS8870. Стратегията за използване на дисковите масиви и постигане на стратегическите инициативи могат да се разделят в следните направления:

Долу изброените детайлни дейности не са с посочена индикативна продължителност защото зависят от много фактори, включително и наличието на време от страна на служителите на банката. Въпреки това спрямо опитана ни смятаме, че посочения период за цялата фаза е реалистичен и изпълним.

4.2.2.1. Дискови масиви за работа с enterprise приложения

Основната стратегия в това направление е да се заменят старите DS дискови масиви с нови DS8870 и се запази в сегашната инфраструктура само наличния DS8870. Постигането на тази стратегия може да се раздели на следните стъпки:

СТЪПКА 1 - ЗАКУПУВАНЕ НА НОВ DS8870 В ОСНОВНИЯ ЦЕНТЪР ЗА ДАННИ;

Новия дисков масив ще замени изцяло работещия в момента с enterprise приложения DS8700, имплементацията ще се извърши на следните фази:

- ✓ Анализ и дизайн на Enterprise дисковите системи;
- ✓ Оразмеряване на необходимия нов дисков масив;
- ✓ Доставка на нов дисков масив DS8870 с необходимите лицензии за replication and virtualization;
- ✓ Инсталация, конфигурация и подготовка за експлоатация;
- ✓ Тестове на системата;
- ✓ Мигриране на всички данни от DS8700 на новия DS8870;
- ✓ Преместване на данните, които се ползват в основния център, но са разположение в касовия център, поради липса на пространство в момента;
- ✓ Изваждане от експлоатация на стария DS8700 (от гледна точка enterprise приложения);
- ✓ Обновяване на наличната документация;

Тази стъпка би отнела 2 календарни месеца.



Тази стъпка не зависи пряко от която и да е друга стъпка в документа.

Тази стъпка ще предостави следните предимства за банката:

- Увеличаване на дисковото пространство, с колкото е необходимо плюс запас;
- Наличие на два enterprise клас дискови масиви във всеки един център за данни;
- Еднопосочна синхронна репликация в посока основен -> резервен;

СТЪПКА 2 - ИЗГРАЖДАНЕ НА ACTIVE-ACTIVE DATACENTER

За постигането на Active-Active Datacenter е нужно да се направи подготовка на съществуващия DS8870, като се закупят хардуерни ъпгрейди като капацитет и допълнителни модули, за да се изравни като конфигурация на новия DS8870 в основни сайт. Допълнително ще се закупят софтуерни лицензи, което ще позволи отключването на нужните функционалности за репликация на данни:

- ✓ Анализ на текущата конфигурация на DS8870 във втория сайт;
- ✓ Закупуване на нови хардуерни компоненти и софтуерни лицензи;
- ✓ Хардуерна инсталация и обновяване на софтуера;
- ✓ Изграждане и тестове двупосочна репликацията на данни между двата сайта;
- ✓ Финализиране и въвеждане в експлоатация на синхронната репликация чрез HyperSwap и Metro Mirror;

Тази стъпка би отнела **2 календарни месеца**.

Тази стъпка не зависи пряко от която и да е друга стъпка в документа (с изключение на предходните от тази глава).

Чрез тази стъпка ще бъде изграден Active-Active Datacenter, което ще предостави активни enterprise услуги и в двата сайта и непрекъсваемост на работата при отпадане на единия център за данни.

СТЪПКА 3 - ИЗГРАЖДАНЕ НА DRC

Тази стъпка ще се осъществи като се закупи 3-ти DS8870 разположен в резервния център за данни:

- ✓ Доставка на нов дискови масив DS8870;
- ✓ Инсталация, конфигурация и подготовка за експлоатация;
- ✓ Изграждане на Global Mirror репликация между 3-те дискови масива DS8870;
- ✓ Тестове и въвеждане в експлоатация;

Тази стъпка би отнела **1.5 календарни месеца**.

Тази стъпка не зависи пряко от която и да е друга стъпка в документа (с изключение на предходните от тази глава).

Тази стъпка ще предостави допълнителна защита на данните на enterprise приложенията в отдалечен резервен център за данни, което ще предостави възможност за продължаване на работата на част от услугите в случай на инцидент в основните сайтове.



4.2.2.2. Дискови масиви за работа с non-enterprise приложения

В това направление ще се закупят нови дискови масиви среден клас и flash специализирани дискови масиви. Върху тази основа ще се изгради виртуализация на дисковите системи, с което ще се обедини работа на новите и на част от старите системи и ще се осъществи репликирането на данните между центровете за данни. Стария DS6800 ще се извади от експлоатация. Текущия DS8700 също ще се извади от експлоатация, като това се синхронизира с предното направление, понеже този дисков масив се използва и за enterprise приложения;

СТЪПКА 1 - ИЗГРАЖДАНЕ НА ДИСКОВА ИНФРАСТРУКТУРА В ПЪРВИЯ ЦЕНТЪР ЗА ДАННИ

Тези системи ще бъдат свързани с работата на x86 виртуализацията и изграждането на инфраструктура за предоставяне на виртуални работни места (VDI):

- ✓ Архитектура и дизайн на Non-enterprise storage системата;
- ✓ Доставка на SVC устройства и нов Storwize v7000;
- ✓ Хардуерна инсталация и конфигурация на новата техника;
- ✓ Мигриране на данните от DS6800 към съществуващите дискови масиви и ново доставения такъв;
- ✓ Изваждане от експлоатация на DS6800;
- ✓ Изграждане на виртуализация върху всички налични дискови масиви за non-enterprise приложения в основния център;
- ✓ Преразпределение и оптимизиране на виртуализирани дисков капацитет;
- ✓ Обновяване на наличната документация за конкретната система.

Тази стъпка би отнела **2 календарни месеца**.

Тази стъпка не зависи пряко от която и да е друга стъпка в документа.

Тази стъпка ще предостави защитен и оптимизиран за работа с x86 виртуализация дисков капацитет. Допълнително чрез виртуализацията на дисковите масиви ще предостави възможност за прибавяне на нови масиви от среден и нисък клас и ще ги надгради със enterprise функционалности.

СТЪПКА 2 - ИЗГРАЖДАНЕ НА STRETCHED CLUSTER – ACTIVE-ACTIVE DATACENTER.

На тази стъпка ще се изгради инфраструктурата във втория център за данни. Ще се закупи нов дисков масив среден клас Storwize v7000 и капацитетът му ще се виртуализира чрез SVC. Отново чрез функционалността на SVC ще се изгради Stretched Cluster между двата основни сайта:

- ✓ Доставка на SVC устройства и нов Storwize v7000 за касовия център;
- ✓ Хардуерна инсталация и конфигурация на новата техника;
- ✓ Изграждане на сървърна виртуализация;
- ✓ Виртуализиране на капацитета на новия v7000 и стария DS8100 (в касовия център);
- ✓ Мигриране на данните от DS8100;



- ✓ Изваждане от експлоатация на DS8100 (възможно е да остане като дисков масив за не критични данни, като част от виртуализирания ресурс);
- ✓ Изграждане на Stretched Cluster между двата сайта чрез SVC;
- ✓ Обновяване на наличната документация.

Тази стъпка би отнела **2 календарни месеца**.

Тази стъпка не зависи пряко от която и да е друга стъпка в документа (с изключение на предходните от тази глава).

Чрез тази стъпка ще бъде изграден Active-Active Datacenter, което ще предостави единен синхронизиран x86 виртуален клъстер работещ едновременно в двата сайта и непрекъсваемост на работата при отпадане на единия център за данни. Това ще позволи пълно разгръщане на x86 виртуализационната платформа и всички позитиви произтичащи от това.

СТЪПКА 3 - ЗАЩИТА НА ДАННИТЕ В DRC

Данните от Active-Active Datacenter ще се защитят допълнително в DRC сайта, чрез закупуване на нов дисков масив Storwize v7000 и SVC, и изграждане на асинхронна репликация чрез Global Mirror:

- ✓ Доставка на SVC устройства и нов Storwize v7000;
- ✓ Хардуерна инсталация и конфигурация на новата техника;
- ✓ Изграждане на виртуализация;
- ✓ Виртуализиране на капацитета на новия v7000;
- ✓ Изграждане и въвеждане в експлоатация на репликация на данни от двата основни центрове за данни в DRC чрез Global Mirror;

Тази стъпка би отнела **1 календарен месец**.

Тази стъпка не зависи пряко от която и да е друга стъпка в документа (с изключение на предходните от тази глава).

Тази стъпка ще предостави допълнителна защита на данните на приложенията работещи върху x86 виртуализацията в отдалечен резервен център за данни, което ще предостави възможност за продължаване на работата на част от услугите в случай на инцидент в основните сайтове.

СТЪПКА 4 - ИЗГРАЖДАНЕ НА ИНФРАСТРУКТУРА ЗА ПРЕДОСТАВЯНЕ НА ВИРТУАЛНИ РАБОТНИ МЕСТА

Виртуалните работни места ще работят върху x86 виртуализацията и SVC виртуализацията на дисковия капацитет (повече информация може да бъде прочета в точка 2.2 от настоящия документ). Поради спецификата на работа на виртуалните работни места и



високите им изисквания за бързодействие на дисковите масиви, ще бъдат закупени допълнително IBM FlashSystem 840 устройства.

- ✓ Архитектура и дизайн на flash системата;
- ✓ Доставка на FlashSystem 840 устройства в двата основни сайта;
- ✓ Хардуерна инсталация и конфигурация на новата техника;
- ✓ Виртуализиране на капацитета чрез SVC;
- ✓ Подготовка за работата на дисковите масиви с виртуални работни места;

Тази стъпка би отнела **1 календарен месец**.

Тази стъпка не зависи пряко от която и да е друга стъпка в документа (с изключение на предходните от тази глава).

Тази стъпка практически ще предостави изключително висока стойност на дискови входно/изходни операции, които ще позволяват масовото имплементиране на VDI за служителите на банката. Допълнително системата може да бъде ползвана и за определена друга информация, която се нуждае от висок брой IOPS.

4.2.2.3. Дискови масиви за Backup & Archive

Конкретните дейности свързани с въпросните дискови масиви са описани в глава Tivoli Storage manager част от настоящия документ.

4.2.3. Обобщение на използваната техника от списъка на предлаганото оборудване

4.2.3.1. Подход по замяна или обновяване на текущите в нови дискови масиви

- ✓ Всички по стари дискови масиви – DS6800, DS8100 и DS8700 ще бъдат постепенно изведени от експлоатация;
- ✓ Ще бъдат закупени нови DS8870 дискови масиви за работата на enterprise приложенията;
- ✓ Ще бъдат закупени нови Storwize v7000 дискови масиви за работата на x86 виртуализацията;
- ✓ Ще бъдат закупени нови FlashSystem 850 flash дискови масиви за работата на виртуалните работни места;

Всички представени по-горе платформи са обект на въпросната тръжна процедура.

4.2.3.2. Надграждането на текущите дискови масиви с модули, дискове и софтуерни лицензи от предложените от участника;

- ✓ Ще бъде извършено надграждане на съществуващия дисков масив DS8870 което ще спомогне за изпълнението на стратегическите инициативи. Всички възможни модули, дискове и софтуерни лицензи на това надграждане са от списъка с предлаганото оборудване са от същия производител - IBM и са предназначени за този модел – DS8870;
- ✓ Tivoli Productivity Center - е инсталиран и работи в средата на IBM дискови масиви, банката активно използва неговата функционалност за наблюдение на работата и контрол на ресурсите на масивите, комутаторите и свързаните с тях сървъри. Повече детайли са дадени в 4.4.1.1
- ✓ Tivoli Productivity Center for Replication – Допълнение на функционалността на TPC, контролиращ репликацията между двата дискови масива 8700 и 8100. TPC-R е критичен елемент, контролиращ репликацията между двата дискови масива. В бъдеще ще се разчита отново на него, за да се осигури консистентност на групите прехвърляни дялове.
- ✓ Администрирането на дискови масиви от висок клас изисква продължителна и сериозна подготовка и най-вече опит в експлоатацията с оборудването. Спецификата на банката, не позволява изнасянето на обслужваното оборудване във външни организации. Така ролята на екипа, който поддържа и развива инфраструктурата и приложенията е от изключително голяма важност. При преминаване към друга платформа тепърва ще трябва да се натрупва опит в спецификите на работата, а направените усилия до този момент, ще бъдат до голяма степен загубени.

4.2.3.3. Подход за виртуализация на дисковите системи;

- ✓ Всички дискови масиви свързани с работата на x86 виртуализацията, в това число и виртуалните работни места ще бъдат виртуализирани чрез IBM SVC;
- ✓ Виртуализацията на дисковите масиви ще предостави както допълнителна функционалност като синхронна и асинхронна репликация на данни, така и съвместната работа на различни модели и класове дискови масиви от различни производители.

4.2.4. Оборудване

4.2.4.1. Enterprise решения (IBM DS8870)

Масивът за съхранение на данни IBM DS8870 е проектиран да се справя успешно и ефективно с широкия спектър натоварвания, присъщи за съвременните инфраструктури за съхранение на данни. Причината този продукт да се използва в Enterprise средите е високата производителност, надеждност и сигурност, които осигурява. Новото поколение flash и хибридни flash системи значително подобряват производителността при чувствителните към време анализи. DS8870 има функционалност да оптимизира автоматично производителността,



в зависимост от нуждите, което води до намаляване на времето за управление и поддръжка на дисковия масив. Този тип устройства поддържат криптиране на всички дискове.



ХАРДУЕРНИ СПЕЦИФИКАЦИИ:

Дисковите масиви от серията DS8870 имат следните хардуерни спецификации:

- Поддържат два броя контролери от серията Power7+ съответно с 2, 4, 8 или 16 ядра.
- Могат да разполагат с до 1TB cache памет.
- Могат да се инсталират до 1536 диска, като могат да се добавят още 120 flash карти с размер 1,8 инча във допълнителния модул High-Performance Flash Enclosure (HPFE)
- Могат да се инсталират 2,5 инчови дискове със скорост на въртене 10K и 15K оборота в минута, както и 3,5 инчови Nearline-SAS дискове.
- Поддържат инсталирането на до 8 допълнителни модула (Nearline-SAS) за системата.
- Максималният капацитет за съхранение на данни на системата е 3072TB.
- Поддържат резервираност тип RAID 5, 6, 10.

ПОДДЪРЖАНИ ФУНКЦИОНАЛНОСТИ:

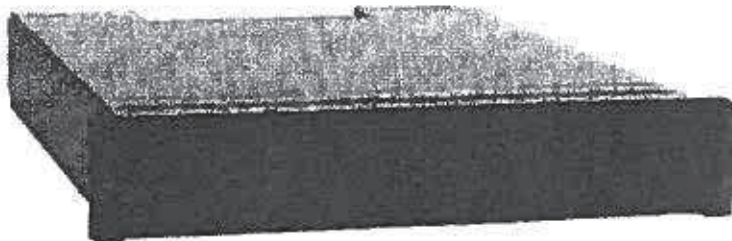
- **Thin provisioning** – Позволява дефинирането на повече пространство от реално използваното.
- **Compression** – Използва се за освобождаване на място на дисковия масив. Служи за съхранението на по-голямо количество данни за едно и също физическо пространство, без да се налага потребителите да премахват архивирани данни.
- **Encryption** – Техника, използвана за криптиране на данни с криптиращ ключ (encryption key), като по този начин данните могат да бъдат прочетени само при наличие на декриптиращ ключ (decryption key).



- **Snapshot** – Възможност за създаване на копие от точка във времето (point-in-time). При създаването му не се прекъсва достъпът до данните. Дава добра възможност за бързо възстановяване и лесно резервиране.
- **Clones** – Възможност за копиране на данни с цел резервираност.
- **Metro Mirror, Global Copy, Global Mirror** – Предоставят допълнителни функционалности, необходими за осигуряване на непрекъснатост в случай на възникнал проблем.
- **IBM HyperSwap** – Осигурява бърз и едновременен достъп до единично копие от данни от центрове за данни на разстояние до 300km.

4.2.4.2. Среден клас устройства за съхранение на данни (Storwize V7000)

Storwize V7000 е система за съхранение на данни от блоков тип, която комбинира хардуерни и софтуерни компоненти, за да осигури единна точка за контрол и по този начин да увеличи ефективността. Системата предлага лесни за употреба и ефикасни възможности за управление, подходящи както за нови, така и за съществуващи IT структури.



ХАРДУЕРНИ СПЕЦИФИКАЦИИ

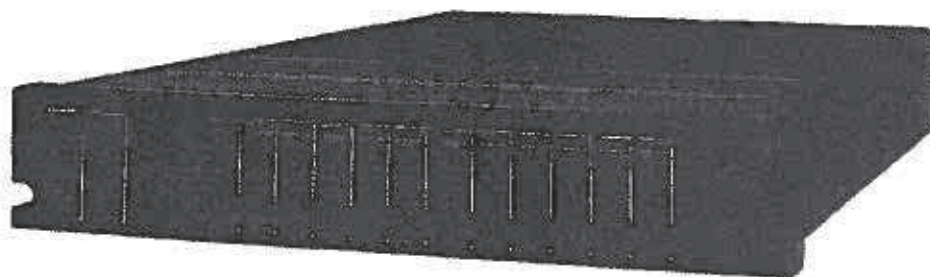
- Шаси за монтаж в 19 инчов комуникационен шкаф с размер 2U (Rack Units).
- Възможност за 6 различни модела шасита.
 - Шаси за контрол тип 2076-112 с до 12 3,5 инчови диска.
 - Шаси за контрол тип 2076-112 с до 12 3,5 инчови диска + 10Gb iSCSI.
 - Шаси за контрол тип 2076-112 с до 24 2,5 инчови диска.
 - Шаси за контрол тип 2076-112 с до 24 2,5 инчови диска + 10Gb iSCSI.
- Резервираност тип RAID 5, 6, 10.
- Поддържа до 240 диска за шаси и до 960 за cluster.
- Поддържа до 64GB cache памет за cluster.
- Максимално тегло с включени дискове – 29,6kg.

ПОДДЪРЖАНИ ФУНКЦИОНАЛНОСТИ

- **FlashCopy** – Технология, позволяваща почти мигновеното създаване на точки във времето (snapshots) на цели логически дялове или масиви от данни.
- **Metro Mirror (synchronous), Global Mirror (asynchronous)**
- **Thin provisioning** – Позволява дефинирането на повече пространство от реално използваното.
- **IBM Easy Tier** – Осигурява автоматичното преместване на често използвани данни в по-бърза работна среда (включително flash) за по-бърз достъп.
- **Unified Storage** – Осигурява единен потребителски интерфейс за управление както на файлове, така и на блоковипоточни линии.
- **IBM HyperSwap** – Осигурява бърз и едновременен достъп до единично копие от данни от центрове за данни на разстояние до 300km
- **Block-data encryption** – Осигурява допълнителна защита на данните.

4.2.4.3. Flash Дисков масив (IBM FlashSystem 840/ V840)

IBM FlashSystem 840/ V840 е изцяло flash-базирано устройство за съхранение на данни, чиято цел е да направи приложенията и data центровете по-бързи и по-ефикасни. Разликата между вариантите 840 и V840 е, че вторият поддържа виртуализация. Основното нещо, върху което е наблегнато при проектирането на тези устройства е бързодействието.



ХАРДУЕРНИ СПЕЦИФИКАЦИИ

- Шаси за монтаж в 19 инчов комуникационен шкаф с размер 2U (Rack Units).
- Поддържа стандарти за резервираност тип RAID 0, RAID5.
- До 40TB достъпно пространство при резервираност тип RAID5 (65TB без резервираност)
- По-малко от 135 микросекунди закъснение при произволно четене.

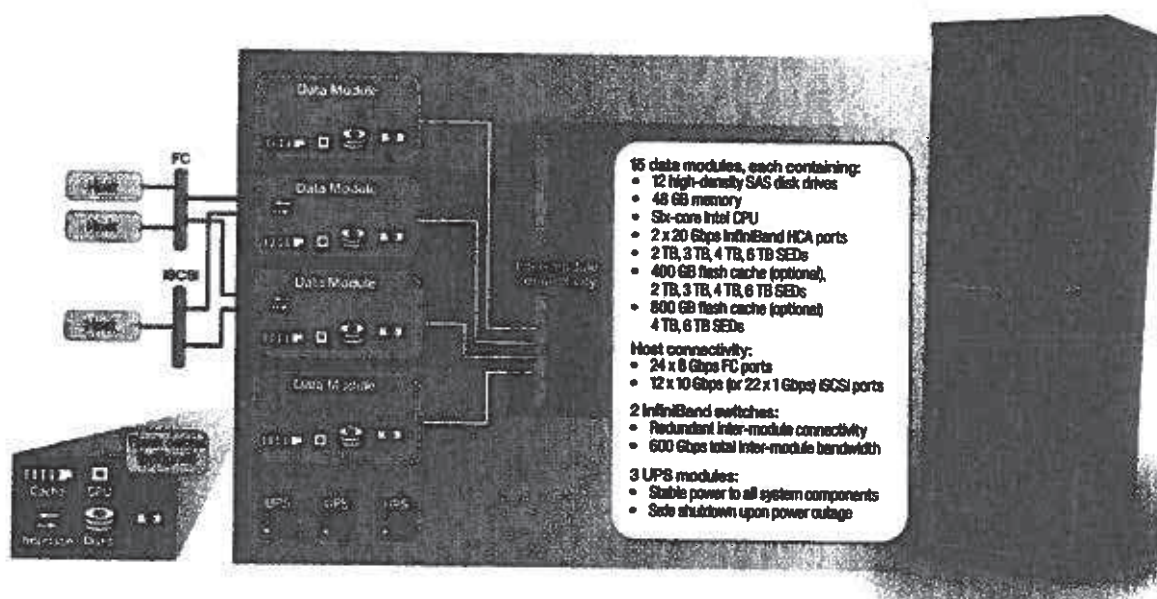
ПОДДЪРЖАНИ ФУНКЦИОНАЛНОСТИ



- **Storage virtualization technology** – Спомога за управлението на други дискови масиви с технологии за възстановяване. Улеснява миграцията на данни от едно устройство за съхранение на данни на друго.
- **Easy Tier** – Осигурява автоматична миграция на често използваните данни на flash памет с висока производителност, като по този начин повишава производителността.
- **Бързодействие** – около 10 пъти по-бърз в сравнение с други решения.
- **Flash Caching** - Осигурява до 4,5 пъти подобрение на производителността при натоварвания.
- **LDAP** удостоверяване.
- **IBM Real-time Compression** – Намалява до 5 пъти ефективния капацитет за всеки дял, без допълнителни хардуерни или смесени натоварвания.

4.2.4.4. Система за съхранение на данни IBM XIV

Системата за съхранение на данни IBM XIV е проектирана да осигурява добра производителност, сигурност и лесно управление. Системата се състои от отделни модули, всеки от които е независим със самостоятелна памет, дискове, между системни връзки и т.н. Модулите са свързани помежду си в паралел с помощта на технологията InfiniBand.



ХАРДУЕРНИ СПЕЦИФИКАЦИИ

- Поддържа до 15 Intel Xeon E5645 процесора.

- До 90 физически ядра (180 логически, ако се използва технологията Intel Hyper-Threading)
- До 180 бр. твърди дискове.
- Поддържа до 720GB оперативна памет.

ПОДДЪРЖАНИ ФУНКЦИОНАЛНОСТИ

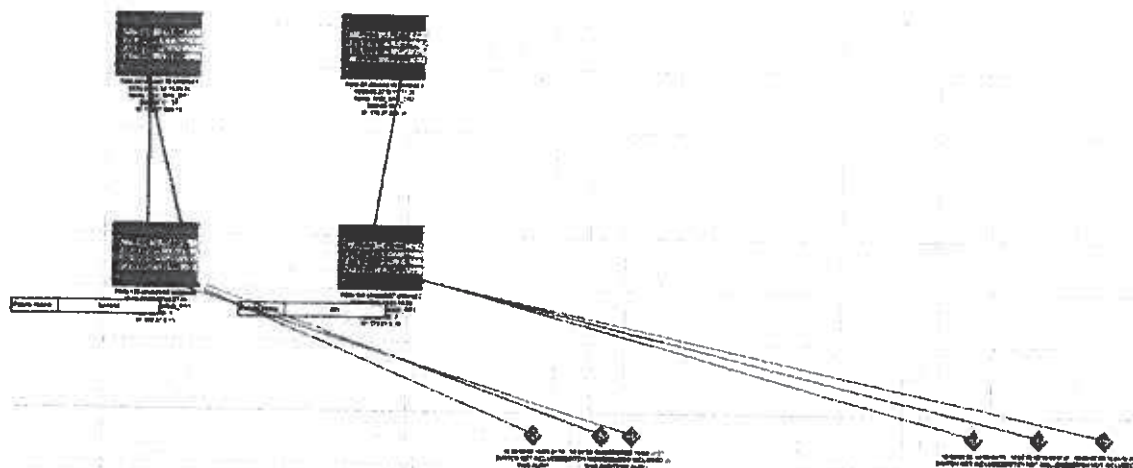
- **Thin provisioning** – Позволява дефинирането на повече пространство от реално използваното.
- **LDAP** удостоверяване.
- Миграция между две XIV системи с помощта на **IBM Hyper-Scale Mobility**.
- **Encryption** – Техника, използвана за криптирането на данни с криптиращ ключ (encryption key), като по този начин данните могат да бъдат прочетени само при наличие на декриптиращ ключ (decryption key).
- **Flash Caching** - Осигурява до 4,5 пъти подобрене на производителността при натоварвания.
- **IBM Real-time Compression** – Намалява до 5 пъти ефективния капацитет за всеки дял, без допълнителни хардуерни или смесени натоварвания.

4.2.4.5. SAN Комутатори

Банката е извършила консолидация на SAN комутаторите и в момента те са по една двойка комутатори от висок клас, обслужващи двата центъра за данни – ЦУ и КЦ. Комутаторите са базирани са от най-високия клас на Brocade, доставени като OEM от IBM. Преди около 3 години са обновени и сега са в поддръжка по договор за извънгаранционна поддръжка.

Архитектурата е базирана на 8 Gbps fabric с интересни модули с достатъчно запас като брой и скорост на интерфейси. Те могат да бъдат надградени с допълнителни модули, предвидени в листа от заданието.

Всички функции на управление на фабриките, зоните, виртуализация, комуникацията между сайтовете, защитата на данните, VSAN са съсредоточени в тях. Във всеки от комутаторите е инсталиран Crypto модул за защита на FC трафика.



В банката се експлоатират и още 6 SAN комутатора, които са вградени в blade chassis и представляват Access ниво за FC трафика от сървърите там. В предвид, че по-голямата част от новите сървърни приложения и виртуализация се изпълняват от rack сървъри, ролята им намалява.

Като цяло тази инфраструктура е надеждна и достатъчно производителна за текущите нужди.

Забележка: В списъка с изискваните модули за обновяване на комутаторите и свързаните с тях лицензи са предвидени модули, които са излезли от продажба в края на 2014 година, наследници на тези модули работят на 16 Gbps и са с подобрени функции за много-протоколна работа.

ПРЕМИНАВАНЕ КЪМ 16GBPS ПРЕНОС

Все повече сървъри и дискови масиви преминават към 16 Gbps интерфейси за комуникация през FC SAN. Ползите от този пренос са:

- Висока скорост на пренос – закъснението в SAN се намалява двойно и така освобождава по-бързо буферите на сървърните интерфейси. Приложенията изискващи голям трафик като DB репликация, backup & restore.
- Ниски закъснения при Roundtrip – типичен пример са закъсненията в рамките на няколко стотин micro sec. характерни за FlashSystems SSD дисковете. Ако времето за отговор се увеличава заради по-ниските скорости на обмен, ефекта от използването на подобни технологии се намалява и обезсмисля. Така седят неща и за отговорите от cache на дисковите масиви
- Виртуализация NPV – от появяването си в FC 8Gbps NPV става изключително използвано решение в Enterprise архитектурите. 16 GBps позволява много по-голяма плътност по брой интерфейсни дефиниции и на трафика през тях.



Предлагаме с навлизането на сървърната виртуализация от ново поколение да се премине към 16 Gbps за сървърите.

SVC и V7000 могат да бъдат доставени с по-бързи интерфейси, а и в тяхната роля е от съществено значение скоростта.

Дисковите масиви от висок клас малко „изостават“ и все още интерфейсите не са достатъчно достъпни, но в рамките на следващите една две години и там основния пренос ще бъде през 16 Gbps.

Заедно обновяването на сървърите и дисковите масиви предлагаме да се обновят поетапно модулите на комутаторите за да се премине към 16 Gbps пренос в рамките на DC. Между сайтове не се налага да се ангажира такъв капацитет и 4 x 8 Gbps ще бъде достатъчно и в бъдеще.

МНОГО-ПРОТОКОЛЕН SAN ДОСТЪП

Една характерна особеност на по-новото поколение адаптери е, че те могат да бъдат конфигурирани, тъй че да позволяват смяна на протокола от FC -> 10 GbE и обратно. SAN комутатора прави протоколна трансляция от FC към FCOE, протокол използван активно от сървърните платформи, за консолидиране на трафика към LAN и SAN в един Converged интерфейс и пренос.

SAN384B позволява FCOE трафика да бъде пренесен до дисковите масиви (обичайно работещи на FC), максимално ефективно.

Считаме, че с намаляване цената и изчистване на несъвместимостите между Converged адаптерите този тип трафик ще се увеличи и трябва да бъде предвиден за вграждане. Тъй като съществената част от консолидацията се пада на мрежовия пренос, а изискванията са jitters, загуби на пакети и закъснения са изключително високи, ние предвиждаме това да се случи съгласувано с изпълнение на мрежата стратегия за реализация на Active Active DC I стъпка 3.1.2.

При възникване на необходимост ще бъде извършена реконфигурация на съществуващите модули или ще бъде взето решение за закупуване на допълнителен модул в съществуващите комутатори като времето за имплементация е около 2 седмици след съгласуване с доставки и внедряване на FCOE оборудването и пренос.

РЕАЛИЗАЦИЯ НА DR САЙТ

Отдалечеността на DR сайта прави задачата за преноса на данни изисква винаги сериозно предварително планиране, защото алтернативните решения дават различни ползи.

При използване на вариант за DWDM или друг тип пренос от този тип ще трябва да се променят интерфейсите настройки да се дефинират по-големи буфери заради по-дългото трасе. Преимущество е, че и двете SAN фабрики ще бъдат видими и SAN ресурсите им ще бъдат достъпни през тях. SAN384 управлява добре трафика между сайтовете а в отдалечения сайт не предвиждаме голяма SAN среда тъй че може да се използват IBM System Storage SAN48B-5, с по-малкия footprint и брой портове.



При използване на IP не се налага да се изгражда алтернативен пренос за FC данните и може да се избегнат проблеми с преноса и настройките в бъдеще. Неудобството тук е, че ресурсите – дискови масиви, сървъри и лентови библиотеки не са в една и съща зона и трябва да се организира друг механизъм, който да ги обедини – например Storage Virtualization или да се използва директно Storage-Storage Replication.

Който и подход да бъде предприет, преноса на данните от дисковите масиви към DR е от изключителна важност и е в основата на проекта за отдалечен център за данни. Работата по реализацията е в зависимост от готовността на преноса към третия сайт и на останалото оборудване. Организирането, конфигурирането и пускането в експлоатация на SAN и пренос е около 2-3 месеца

4.3. Backup & Archiving

За осигуряване на нормалното функциониране на един съвременен център за данни, е необходимо да се обърне сериозно внимание, на методите за създаване на резервни копия и архивиране на данните. Политиките за архивиране и създаване на резервни копия също са много важна част, от едно решение за архивиране и създаване на резервни копия на данните. Съществуват два основни метода за съхранение на така създадените архиви и резервни копия – ленти и твърди дискове, всеки един от методите има своите предимства и недостатъци. За създаване на добре работещо решение е необходимо да бъдат използвани и двата метода. Текущото състояние на инфраструктурата за резервни копия разчита предимно на ленти за съхранение на данните. При архивирането и създаването на резервни копия има два много важни параметъра:

- RPO (Recovery point objective) – изразява „възрастта“ на файловете, които трябва да бъдат възстановени, за да може услугите и системите да бъдат приведени в нормално работно състояние;
- RTO (Recovery time objective) – изразява целевия интервал от време, в който услугите и системите трябва да бъдат възстановени в нормално работно състояние;

На база на тези параметри, решението за архивиране и създаване на резервни копия, трябва да бъде създадено така, че да осигурява едновременно минимално RTO и максимално RPO. Разглеждайки спецификата на текущото решение за архивиране и създаване на резервни копия, става ясно, че то не може да отговори на тези изисквания. За създаване на ефективно решение отговарящо на изискванията, трябва да се направят промени по текущото решение, като се запази максимално наличното оборудване.

Към съществуващото решение трябва да се добавят дискови системи, за създаване на резервни копия върху твърди дискове, които да се използват за кратковременно съхраняване на данните – максимум 60 дни. След това данните ще бъдат консолидирани в месечни архивни копия и ще бъдат копирани върху лентовите библиотеки и съхранявани там спрямо политиките за съхранение на архивни копия на данните. Данните от двата центъра за данни ЦУ и КЦ, ще се репликират помежду си, като и в двата центъра за данни, ще се съхраняват резервните копия на данните от другия център за данни. Тези данни ще бъдат репликирани в трети резервен

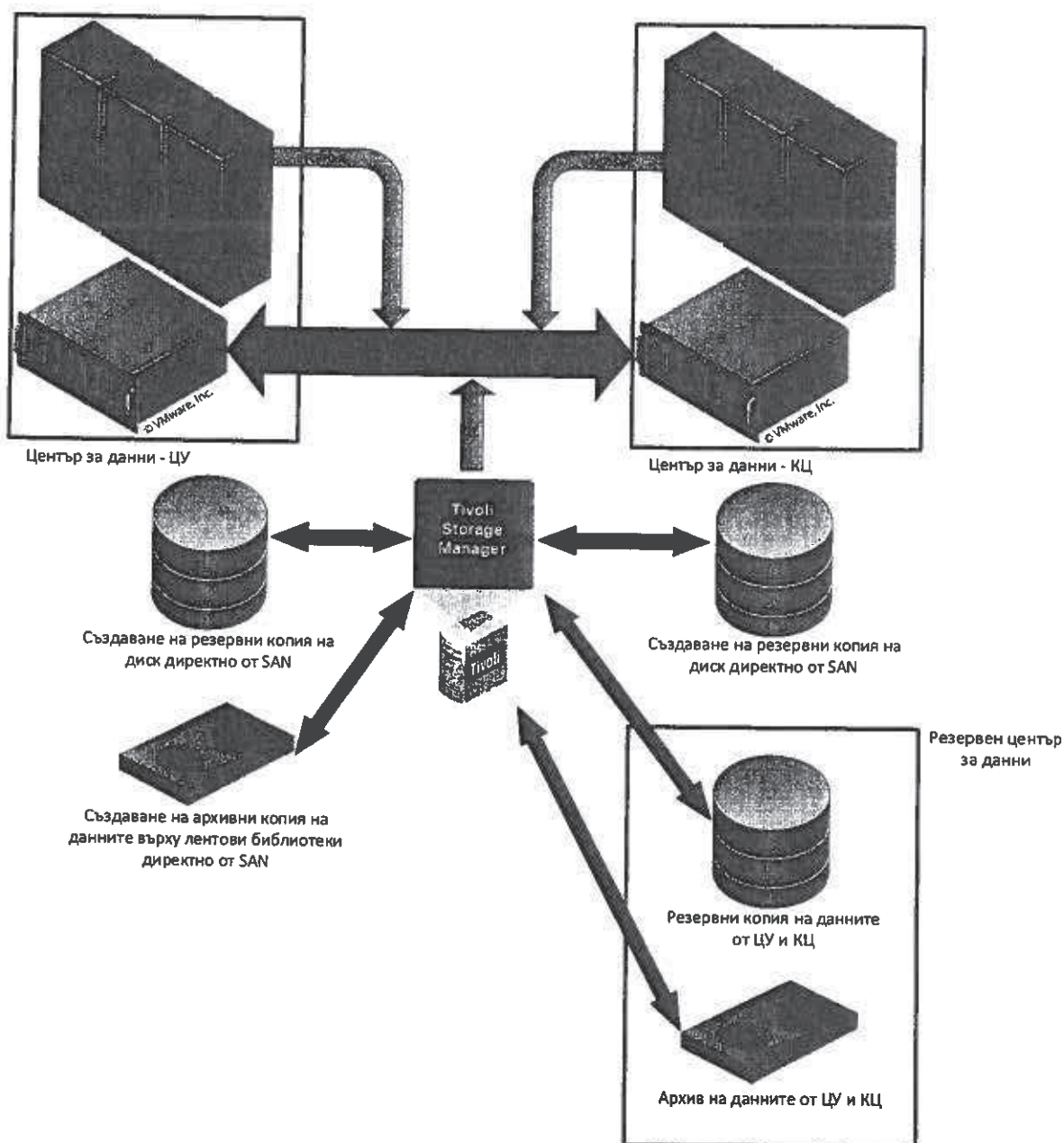


център за данни, където ще се съхраняват в случай на природно бедствие или авария в основните центрове за данни. Всички архивни данни от лентовите библиотеки в основния център за данни, ще бъдат репликирани върху лентовите библиотеки в резервния център за данни. По този начин резервните копия и архивните копия на данните ще се съхраняват минимум на две географски отдалечени локации.

С цел ускоряване на процеса по създаване на резервните копия и архиви, софтуера за създаването им Tivoli Storage Manager, ще копира данните директно от снимки (snapshots) на дисковите масиви и виртуализацията на дисковите масиви. По този начин времето за архивиране и създаване на резервни копия, значително ще се намали, като в същото време паразитното натоварване върху останалата част от инфраструктурата, също ще бъде намалено значително. За по-добро използване на дисковото пространство необходимо за съхранение на резервните копия, ще се използват технологии, като дедубликация и компресия на данните.

Софтуера ще използва интеграция с съществуващите приложения и по-този начин, ще осигури максимално удобство при управлението на резервните копия и архивните копия на данните.

С цел осигуряване на максимална вероятност за успешно възстановяване на данните, софтуера ще бъде настроен да прави проверка за възстановимост на данните, след създаване на резервните копия. По този начин, ще се гарантира, че данните могат да бъдат възстановени от резервните копия и архивните такива.



4.3.1. Лентови библиотеки

Банката експлоатира две лентови библиотеки TS3500 в DC в Централно управление и TS3310 в „Касов център“. Двете библиотеки са в експлоатация от отдавна и като цяло са с достатъчен капацитет за нуждите на банката.

Библиотеката в основния сайт е екипирана с LTO4 и LTO5 устройства и ленти, в „Касови център“ се библиотеката е екипирана с LTO5/LTO6 устройства.



Библиотеките са в 4 годишен договор за поддръжка и се използват активно, както за запазване на данните, софтуера и операционните системи, така и за поддръжка на архивни данни и състояния на основните приложни системи в банката.

4.3.1.1. Концепция и стъпки за развитие

С течение на времето са се събрали значителен брой ленти особено от по-старите поколения LTO4, които не са ефективни заради капацитета и скоростта на работа. До края на експлоатацията (гарантирания брой записи) е добре да се продължи активното им ползване. Но обемите на архивите са достатъчно големи, а и банката често възстановява от ленти информация за системите и този процес е времеемък и трябва да се обърне внимание за подобряване на ефективността.

Ние предлагаме да се обновят устройствата, тъй че да се премине към LTO5-LTO6 и на база на тях да се търси решение за многото налични LTO4 ленти.

Наличната информация върху LTO4 ленти може да бъде консолидирана върху няколко пъти по-малък брой LTO6, а след това LTO4 да бъдат заменени устройствата с LTO6. По-старите устройства да бъдат изведени от експлоатация поетапно.

След изграждане на третия център за данни предлагаме той да бъде натоварен с задачата за създаване и поддръжката на архива на информационните системи.

4.3.1.2. Бекъп и възстановяване от дискове

В бъдеще се очаква данните да нарастват, допустимото време за възстановяване да намалява. Често данните, които биват търсени нови, а заявките разнообразни. Основните проблеми на лентовите библиотеки се дължат на тяхната технология – търсене и обновяване на каталози, подготовка на пакет за възстановяване, търсене и извличане на специфична информация или файл (за разлика от пълно възстановяване).

Компаниите имат решение в тази насока, които се свеждат до:

- Virtual Tape Library (VTL) – обикновено дисков масив емулиращ работата на библиотека, естествено се вписва в архитектурата на TSM и намалява значително времето за търсене и извличане на данни от библиотеката;
- Дедупликация и компресия – в комбинация с VTL допринасят за по-ефективното използване на дисковото пространство в устройствата, ефективно намалявайки операциите към и от дисковете и допълнително времената за търсене на информация;

Решението на IBM® ProtecTIER за дедупликация на данни подобряват архивиране и възстановяване след бедствие операции при намаляване на оперативните разходи и потребление на енергия. Данните могат да бъдат репликирани между центровете за данни и резервирани в случай на нужда и премахва нуждата от транспортиране на касети. В зависимост от типа на данни ефективността на алгоритъма може да стигне 10:1.



4.3.2. Tivoli Storage manager

Внедрен е софтуер TSM за Backup & Recovery с внедрени политики за архивиране на цялата инфраструктура. Политиката приложена за инфраструктурата е в съответствие в изискванията и добрите практики:

- Ежеседмичен пълен бекъп на бази данни, приложения и дялове на операционни системи
- Ежедневен частичен (incremental) бекъп на базите данни, приложения и др.
- Допълнителни backup сесии преди и след специализирани събития за част от информационните системи:
 - o Преди и след приключване на отчетен период
 - o Преди и след системни промени в софтуера, нови версии, Imports & exports
 - o Регулярни пълни архивни пакети за архивиране

TSM стои в основата на DR стратегията на банката, използват се възможностите му за резервиране на данните върху двата сайта и се извършва online репликация от единия сайт към другия, с цел всички данните да бъдат дублирани и в последно актуално състояние. Заедно с това се води архив, които според правилата на банката и регулациите в бранша е за сравнително дълъг период.

Ние считаме, че трябва да бъде ускорен процеса чрез подобрена интеграция на TSM с дисковите масиви и SAN и ползването им за по-бърз и ефективен начин за backup & restore.

4.3.2.1. Сървъри

TSM сървърите на банката са сравнително нови и отговарят на изискванията за бързи IO и сравнително големи натоварвания на паметта и процесора. В бъдеще, с увеличаване на капацитета и добавяне на услуги в TSM – за дедупликация и Server-less бекъп, натоварването и трафика през тях ще се увеличи, би могло да се планира преминаване към новата генерация сървъри S822 с конфигурация от типа:

P/N	Описание	Qty
8284-22A	Сървър за вграждане в сървърен шкаф - 4U -Процесор: 6-core 3.89 GHz POWER8 Processor Card 6x 1-core activation of #EPX1 - Памет: 2 x 16GB Memory DDR3 DIMMs, - Твърд диск: 6+6 storage backplane with split bay option, 146GB 15K RPM SFF3 SAS Disk Drive (AIX/Linux) - Софтуер: AIX Standard Edition PowerVM Enterprise edition с лицензи за всички ядра - 2 AC Power supply - 1400W	1
EPY1	One Processor Core Activation for #EPX1	1
EM83	16 GB DDR3 Memory	6
EN0B	PCIe2 LP 16Gb 2-port Fibre Channel Adapter	2
EN0L	PCIe2 LP 4-port(10Gb FCoE & 1GbE) SFP+Copper&RJ45	2



4.3.2.2. Server-less backup

За намаляване на бекъп прозореца да се използват snapshots от дисковите масиви и след фиксиране на данните, Backup сървърът извършва архивирането с максимална скорост, без да влияе на работата на основните машини.

Работата се подпомага от интегрирания Tivoli FlashCopy Manager софтуер, интегриран в базите данни и приложенията като SAP.

Backup се извършва в следните стъпки:

1. Инициране от TSM – на база регулярна политика или преди съществени системни събития
2. Извършва се архивиране на всички дялове от типа – RootVG, App. Volumes, през нормалния TSM агент през мрежата. Данните се съхраняват в областта за дедупликация, за по-бърз и ефективен достъп.
3. FlashCopy Manager иницира последователно преминаване на дяловете на базите данни (data, arch, logs) в hot backup, за да получи консистентно копие:
 - a. Превключване на съответния дял в Hot-backup, което изчиства буферите и прави дяла консистентен
 - b. Дисковия масив иницира разделяне на копията за създаване на snapshot
 - c. След приключване на т.б нормалната работа - R/W се възстановява
 - d. Преминва се към следващ дял.
4. След приключване на процеса, който не отнема повече от няколко секунди имаме консистентно състояние на базите и приложенията в дялове независими от основните данни
5. Прехвърляме данните върху друг сървър и извършваме бекъп. Това не е необходимо да бъде в извънработно време и се прави с максимална възможна скорост.
 - a. Възможно е да се иницира
6. Данните се разполагат в deduplication store, където се съхраняват само разликите.
7. След изтичане на времето определено за съхранение върху бърз архив (VTL или Deduplication Storage Pool) се прехвърля върху архив на ленти.

Възстановяване:

1. Инициране на възстановяване и уточняване на източника – лента или deduplication area
2. Подготовка на дисковия масив като се осигурява пространство в temp областите
3. Стартира се възстановяването на дяловете – бази данни, файлови системи или приложения (възможно е да се подготви и цялостно възстановяване)
4. При приключване на възстановяването на сървърът ще имаме консистентно копие на данните върху дисковия масив
5. „Прикачаме“ групата Snapshot на мястото на действащата до сега
6. Стартиране на машината или рестартиране на базата



4.3.2.3. Deduplication

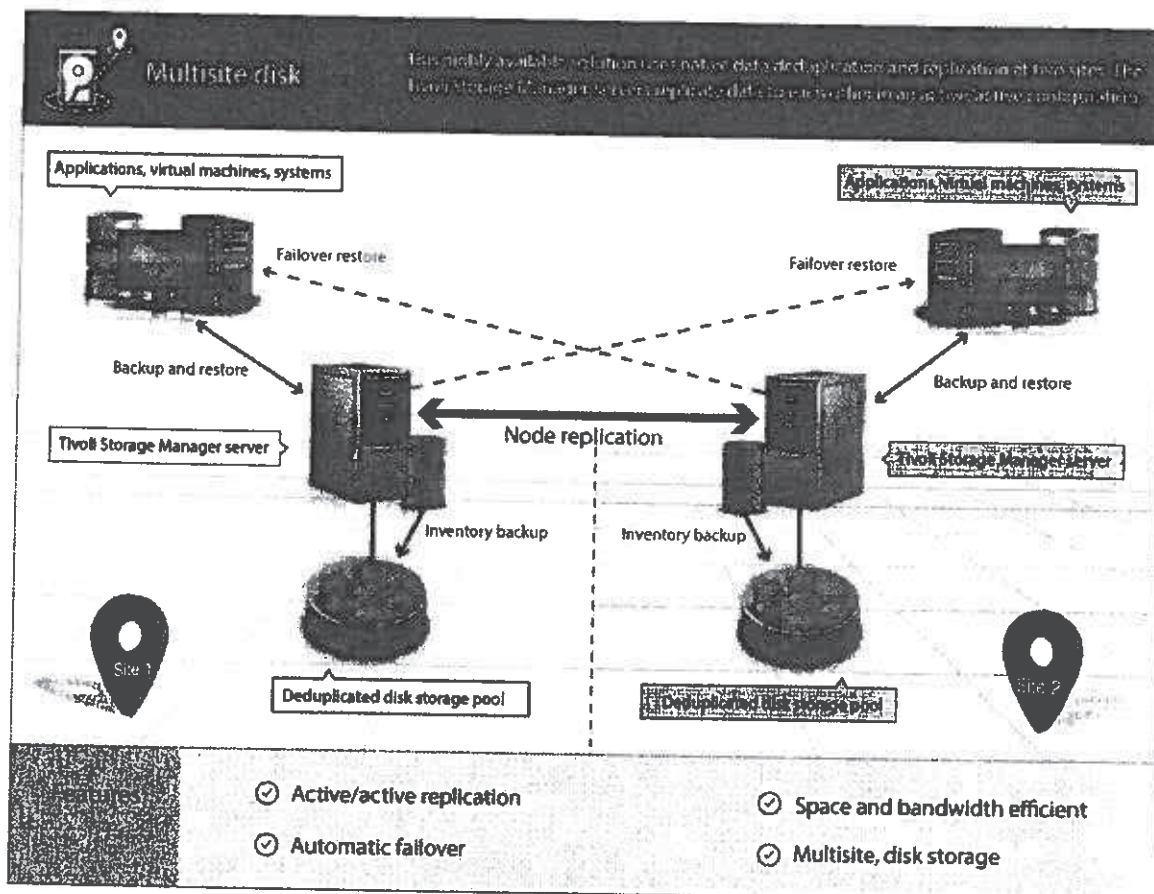
Дедупликацията решава един проблем, който се появява при използването на директен достъп до дисковете – невъзможност да се прави Incremental backup.

Агентите на TSM изготвят база данни на архивираните обекти и при извършване за нов incremental бекъп те следят да съхраняват само променените от последния бекъп обекти, драматично намалявайки времето и заетото пространство.

В случая с дисковия бекъп няма общ начин да се разбере, кои обекти в съответния дял са нови или променени. Дедупликацията работи със статистически алгоритми и разглежда данните от по-ниско ниво като търси повтарящи се части от данните, независимо от времето им за създаване.

Положителен страничен ефект на дедупликацията е, че за разлика от incremental backup времето за възстановяване е почти едно и също. Обичайно в края на седмицата се извършва пълен бекъп от които се стартира серия от incremental backups, които се извършват всяка нощ в работните дни като отразяват само промените от предишната нощ, до края на работната седмица. Така при възстановяване в петък, трябва да се възстанови пълния бекъп от последната неделя и последователно да се приложат всички incremental backup от понеделник до четвъртък. Процесът е трудоемък, бавен и зависи от това дали няколко поредни бекъп сесии са завършили успешно...

Вградената в TSM дедупликация може да се използва съвместно или алтернативно на предложеното по-горе решение базирано на IBM® ProtecTIER. Показано по-долу на графиката.



Ние предлагаме да се стартира с два дискови масива от типа V7000 конфигуриран за големи обеми от данни и висока скорост на последователни операции четене и запис например:

Part No	Description	Qty
2076-524	IBM Storwize V7000 SFF Control	1
5305	5m Fiber Cable (LC)	4
9730	Power Cord - PDU connection	1
AHB1	8Gb FC Adapter Pair	1
AHF4	1.8TB 10K 12GB SAS 2.5 Inch HDD	24

Те да предоставят капацитет около 35 TB след RAID и да служат на TSM сървърите за място, в което да се съхраняват данните за около 30-60 дни преди да бъдат архивирани. Функционалността на TSM за репликация за осигуряване на резервно копие ще продължи да се използва активно за DR.



4.3.2.4. IBM® ProtecTIER

При увеличаване на изискванията за обем и скорост на операциите, може да бъде необходимо преминаването към специализирано устройство IBM® System Storage® TS7650G ProtecTIER®, за да се освободят сървърите и дисковите масиви от тази задача. То предоставя следните:

- До 2,500 MBps или 9 TBph virtual tape library (VTL) постоянна бекъп производителност с дедупликация
- До 3,200 MBps или 11.4 TBph VTL постоянна скорост на възстановяване
- Капацитет увеличаващ се лесно до 25 PB
- File System Interface (FSI) за network-attached storage (NAS)-базирани среди, едновременна поддръжка на Network File System (NFS) v3 за UNIX клиенти и Common Internet File System (CIFS) за Microsoft Windows базирани среди.

4.4. Системен софтуер

4.4.1. Системи за наблюдение и управление на изчислителни ресурси

В момента се разчита на две основни платформи за наблюдение и управление на изчислителните ресурси TPC и VMWare Operations Center. От тях екипа на банката следи за наличните ресурси и трендовете за използването им и взема решения за бъдещото развитие.

Ние предлагаме този подход да бъде запазен и при реализация на проекта за частен облак БНБ да се възползва от новите средства за наблюдение и управление достъпни от там.

Използването на текущия софтуер паралелно с новите функции ще осигури плавно преход на екипа и пълен контрол върху процеса.

4.4.1.1. Tivoli Productivity Center

Tivoli Productivity Center е инсталирано в средата на банката с фокус върху наблюдението на SAN инфраструктурата, но то притежава функции, които го правят и за наблюдение на виртуална среда:

- Единна конзола за управление на всички типове данни на диск, флаш, файлове и обектни сториджи
- Опростен интерфейс на администратора включващ Web базиран интерфейс, VMware® vCenter™ plug-in и Cognos® Business Intelligence отчети
- Управление на масиви и устройства позволяващи бърза инсталация с agent-less управление
- Интегрирано управление на производителността с възможност да се наблюдава end-to-end – включвайки устройствата, SAN фабриките и дисковите масиви. С фокус към сторидж инфраструктурата, но с детайли към хостове и виртуални среди спомага за бързото разрешаване на проблеми



- Управление на репликация на данните позволява с поддръжка на Windows, Linux, UNIX и System z данни.

Като част от сървърната инфраструктура Power сървърите предоставят данни за заетите от тях ресурси в дисковите масиви, механизмите за репликация, изготвят се регулярни отчети необходими за планирането на IT.

4.4.1.2. VMware vSphere with Operations Management

vSphere with Operations Management предлага по-интуитивен потребителски интерфейс, отколкото vCenter сървър и подобрява възможности за мониторинг, чрез добавяне прогнозен анализ, за да помогнат с по-бързо откриване на проблеми и възстановяване, както и по-ефективно управление на ресурсите.

Unified Command Console показва ключови показатели за изпълнение в лесно идентифицируеми цветни значки и осигурява цялостен поглед в това, което е управление на настоящите и потенциалните проблеми бъдещо представяне и управление на капацитета.

Мониторинга на изпълнението и управлението на капацитета анализира vCenter данни на работата на сървъра и да установят динамични прагове, които предоставят интелигентни предупреждения за здравето разпадания, пречки за ефективната и недостиг на капацитет.

- Данни за производителността се абстрахира до здравни, рискови и ефективност мерки, които тя предоставя с операции видимост към ефективно идентифициране на развиващите се проблеми с производителността с по-малко време и усилия.
- Управлението на капацитета помага за разкриване на свободни ресурси или overprovisioned виртуални машини, за да си върне излишния капацитет и увеличи VM плътността.
- Възможности са еквивалентни на Standard edition на vRealize Operations Manager и достъпни като tool, който се инсталира в рамките на минути.
- vSphere Hardening проверява vSphere в областта на сигурността и прилага практики.

Повишена производителност и наличност на критични приложения чрез нови и подобрена функционалност дава по-голяма гъвкавост, ефективност и устойчивост при високи нива на обслужване за вашите ИТ среди.

4.4.2. Системи за наблюдение и управление на репликацията на данните

TPC for Replication предоставя следните предимства:

- Следене на състоянието на дяловете във всичките дискови масиви участващи в репликацията;
- Интеграция с AIX Basic HyperSwap for High Availability. Много важно предвид факта, че основните банкови системи работят върху AIX платформа.



- Координиране на Copy Service функциите (Metro Global Mirror and Multi Target PPRC (MM and GC).
- Единен софтуер за управление на всички масиви участващи в репликацията, предоставящ панели за графичен и команден ред на управление.
- SNMP известията при проблем/промяна в състоянието на репликацията.
- Конфигурация базирана на „стъпка по стъпка“ графичен панел.
- Всички репликрани дялове и тяхното състояние се съхранява в една база.
- Source / Target верификация.
- Поддръжка на голям набор от дискови масиви от IBM (ESS, DS6000, DS8000, XIV, SVC, Storwize Family).
- Следене на състоянието на всеки сайт.
- Опция за изграждане на High Availability Server Configuration- active and standby management server с цел резервиране на TCP конфигурацията и работоспособността.
- Лесно тестване на Disaster Recovery планове.
- Цялостно управление на планове при Disaster Recovery.

Използването на дискови масиви от висок клас DS8870 заедно със TPC for Replication предоставя редица предимства за защита на данните и автоматизация.

При изграждането на Active-Active връзката между 2-та „локални“ масива в София е необходимо всеки един от двата сайта да разполага с минимум 50% свободен капацитет с цел поемане на ресурсите от другият сайт при отпадане. Препоръчително е това пространство да бъде 50% + 20% заделено за локална репликация(snapshot).

В момента се използва TPC for Replication управление на текущата репликация. Изграждането на предложената репликация по горе, ще бъде лесна за имплементиране, понеже ще бъде нужен само ъпгрейд към версия 5.x(актуална в момента).

5. Планове за внедряване и обслужване

5.1. Процедури по управление на проекти

Ръководенето на проекти и контрола по изпълнението е част от възприетата от Телелинк методика за управление на проекти, описани в допълнителен документ.



5.2. Обучение

Инфраструктурата на БНБ представлява сложен комплекс от високо производителни и надеждни сървъри и дискови масиви, за да могат да изпълняват поставените им задачи, те трябва да бъдат конфигурирани и експлоатирани съобразно добрите практики и препоръките на производителите.

Телелинк разглежда обучението на потребителите и администраторите като съществен елемент от предоставянето на решение и за това го разделяме на две направления:

- **Knowledge transfer** – Екипите по инсталиране и миграция ще работи съвместно с експертите на Банката и ще предават знанията си и опита в инсталирането и конфигурирането на системи от висок клас. Така максимален кръг от ангажираните с експлоатацията на системата специалисти ще бъдат запознати със всички детайли от решението.
- **IBM Technical University** – Глобална серия от срещи на специалисти от IBM и основните ползватели на техниката. Предлагаме регулярно – веднъж в годината, специалисти на банката да участват в тези обучения, където да научат повече за направленията на развитие на IBM в областите на хардуерните платформи, сървъри и дискови масиви и на системния софтуер. А така също да придобият практически знания в Lab сесии.
- **Training** – за придобиване на по-задълбочени познания по отделните елементи на решението сме предвидили специализирана програма от обучения, специално пригодени за екипа специалисти, които ще обслужват решението в периода на договора

5.2.1. Обхват

Разделяме обучението на следните направления:

- **Power Servers & AIX** – екип от 2-3 човека
 - o Запознаване с Power архитектурата – Servers, HMC,
 - o Виртуализация – PowerVM, Power VC, VIOS, Pools, Partition mobility,
 - o OS – AIX (AIX Jumpstart Training) – процеси, LVM, памет, потребители и др.
 - o PowerHA, HyperSWAP
- **Storages** – 5 дни, екип от 2-3 човека
 - o Brocade SAN
 - o IBM SVC Technical Training – архитектура, възможности GUI,
 - o Storwize V7000
 - o DS8000
- **FlashCopy Manager**
- **TSM** – 5 дни, екип от 2-3 човека
 - o Backup & recovery with TSM – основно запознаване с архитектурата, възможностите и интеграция с DB2, SAP



- FlashCopy Manager – използване за създаване на копия на данните, интеграция с DB2, SAP, TSM
- Виртуализация
 -
- Облачни услуги

5.2.2. Планиране

РЕГУЛЯРЕН ПРЕГЛЕД

Всяко полугодие ще бъде извършван анализ и подготвяно за одобрение план за обучение на персонала на банката, в зависимост от конкретните проекти и общите теми набелязани по-горе

НОВИ ТЕМИ

Стратегическите инициативи трябва да бъдат осигурени от достатъчно по обхват и дълбочина обучения, за което ще бъде предвидено време при изпълнението им.

ОБУЧЕНИЯ ЗА СЪПЪТСТВАЩИ ТЕХНОЛОГИИ

При внедряване на проекти, за които е необходимо да се инсталира или експлоатира допълнителни системи, кореспондиращи с изграждането на решенията например VMWare VDI или Microsoft Infrastructure специалисти на ТелеЛинк ще извършват обучение за запознаване, съпровождане и администриране на изградените системи.

ТЕХНОЛОГИЧНИ ОБУЧЕНИЯ

Екипи на банката ще бъдат включени в специализирани семинари по по-обща теми, които да спомогнат за нови идеи и решения в областта на ИТ инфраструктурата ще бъдат. Тези семинари ще са на регулярна база. Включително с участие на производители и доставчици на оборудването и софтуера.

5.3. Процедури по извършване на гаранционно обслужване

Телелинк ще извършва услугите по гаранционно обслужване и разширена поддръжка, там където е необходимо. Гаранционното обслужване ще се осъществява от IBM България според изискванията на компанията да поддържа на оборудване от висок клас.

Телелинк ще използва създадената организация за обслужване на банката за извънгаранционно обслужване на IBM инфраструктурата и комуникационната техника. Нашите специалисти ще осъществяват първоначалната диагностика и troubleshooting до отстраняване на проблема на място.



5.3.1. Организация и структура на поддръжка

Система за регистриране на инциденти

Системата за регистриране и управление на инциденти има за цел да проследява прогреса по работата на всички активни инциденти и сервизни заявки, както и съхраняването им в единна централизирана база от данни. Системата притежава възможност за отдалечен ролеви достъп на потребители с различни права, както от страна на техническите специалисти на Телелинк така и от страна на Клиента.

Системата за регистриране и управление на инциденти е достъпна през web на адрес <http://support.telelink.bg>. Системата се достъпва след предварително направена регистрация с валиден имейл адрес и парола. Регистрацията се прави от Телелинк при необходимост или при поискване от страна на клиента. Системата функционира върху резервирани и географско раздалечени мрежови сървъри на Телелинк и нейният адрес е достъпен през интернет.

Основни функции на системата са:

- Автоматично генериране на уникален идентификатор на всеки инцидент (което дава възможност за проследяване на активни и вече затворени инциденти)
- Удобен, интуитивен web интерфейс
- Описание на статуса на всеки инцидент (In Progress, On hold, Fixed, Resolved, и др.)
- Записи и атрибути на инцидента, които не могат да бъдат променяни:
 - Отговори и обновявания на всеки запис
 - Времеви полета (timestamps)
 - Лог на промените
- Автоматично уведомление при административна ескалация

Компонентите са активни за избор след въвеждане на валиден e-mail адрес и парола в полето Login. Допълнително на началния екран са обявени телефоните за телефонна връзка с центъра за обслужване на клиенти и сервизни заявки на Телелинк.

При избиране на опцията **Регистриране на инцидент (Open a Ticket)**, системата предлага да се избере дали да се създаде Заявка за поддръжка (Support) или да се направи Заявка за промяна (Standard change request). При избор на един от двата варианта се отваря форма за въвеждане на заявката.

Системата показва всички Отворени (Open) и всички Затворени (Closed) заявки, заедно с техния номер, статус и дата на последна промяна. Чрез тази система, Клиентът може да проверява статуса на работата по създадената то него заявка, с какъв приоритет е, кой инженер е назначен по нея и т.н.

Ресурси за обслужване на поддръжката по проекта



Функционалните роли, свързани с процеса на управление и поддръжка на системите на клиента, съответно обособени в центъра за обслужване на клиенти са:

Хелпдеск оператор – основната цел на Хелпдеск операторите е да възстановят нормалната работа на услугите за клиентите колкото е възможно по-бързо. Това може да включва както отстраняване на техническа повреда, така и изпълнение на заявка за услуга или отговор на въпрос. Основно задължение на хелпдеск оператора е да регистрира и управлява всички активни инциденти.

Специфичните отговорности включват:

- Единствена точка за контакт при възникване на инцидент или сервизни заявки
- Наблюдение на управляваните с-ми, регистриране и управление на всички възникнали аларми и промени в състоянието на наблюдаваните обекти
- Регистриране на обажданията от клиентите и назначаването на правилните ресурси
- Извършване на първоначално изследване и диагностика на инцидента или първоначално обработване на заявката за обслужване
- Разрешаване на инцидентите, които могат да бъдат разрешени от тях
- Ескалиране на инциденти/заявки за услуга, които не могат да бъдат разрешени от тях в договорените времена
- Информиране на клиентите за прогреса на работата по даден инцидент
- Затваряне на всички разрешени инциденти

Първо ниво поддръжка – първо ниво техническа поддръжка поема всички случаи, които не са били разрешени от ниво Хелпдеск. Нивото е съставено от сертифицирани и квалифицирани инженери за работа със системите на клиента. Първо ниво поддръжка:

- Разрешават повечето софтуерни и хардуерни проблеми;
- Установяват дефекти в продуктите;
- Определят план за действие за търсене и разрешаване на проблеми;
- Използват външни програми за анализ, когато е нужно;
- Анализират признаците на проблемите и данните, когато е нужно;
- Провеждат тестове за възможност за работа и съвместимост с нови софтуерни и хардуерни версии;
- Провежда лабораторни симулации и възпроизвеждане на проблема;
- Създават алтернативни решения за хардуерни и софтуерни бъгове (там където настоящите или алтернативни функционалности го позволяват)
- В случай на ескалация до второ ниво поддръжка, посочват точните стъпки за възпроизвеждане на проблема.

Второ ниво поддръжка – Второ ниво поддръжка се счита за най-високото ниво по отношение на комплексност и често изисква директна връзка с разработчиците на софтуер и хардуер, когато причината за инцидента не е ясна. Второ ниво поддръжка:

- Създават алтернативни решения за хардуерни и софтуерни бъгове, които изискват познания и умения по-високи от тези на Хелпдеск или Първо ниво поддръжка;
- Възпроизвеждат проблема със сложни лабораторни симулации;
- Осигуряват или служат за връзка с инженерната поддръжка на продукта и/или софтуера за разрешаване на дефекти в продуктите.
- Идентифицират проблеми във взаимната работа, които могат да бъдат причинени от софтуер/хардуер от трети страни;
- Извършват дейности на процеса Управление на проблеми.

Регионални инженери по поддръжка на място – технически специалисти, разполагащи с необходимата експертиза, инструменти и инструкции, които отговарят за изпълнението на дейности по поддръжка на място на обекта на клиента. Основните им задължения са:

- Диагностика на проблем с дефектирало оборудване
- Подмяна на дефектирало оборудване
- Съдействие на инженер от Центъра за обслужване на клиенти, на обекта при диагностициране на проблем (Remote hands and eyes)



Фигура 1 Териториално разпределение на регионалните инженери

Функционалните роли, свързани с процеса на управление на проектите при обслужване и поддръжка са:

Ръководител Проект (РПр) – следи за цялостното изпълнение на проекта спрямо подписания договор с клиента. Това е дейност, която включва основно планиране и изпълнение на проекта, наблюдение, контрол и отчитане по отношение на процесите, свързани с обхвата, качеството, графика, рисковете, човешките ресурси, разходите и комуникациите по проекта.

Ръководителят проект при стартирането на един проект отговаря основно за:

- ✓ Създаване и администриране на проекта на вътрешно-фирмените портали и ERP системи
- ✓ Определяне на план на заинтересованите лица по проекта от страна на клиента и матрица на отговорностите на двете страни
- ✓ Създаване на план за управление на комуникациите
- ✓ Създаване на план на контролните точки и график на проекта
- ✓ Организиране на първоначална среща с клиента за запознаване с проекта и процедурите
- ✓ Съгласуване с клиента на горните

По време на изпълнение на проекта и в зависимост от обхвата му РПр следи и отговаря за:



- Планиране и контролиране на профилактични дейности, ако има такива
- Регулярен анализ на разходите
- Административно-финансови процеси и навременно изпращане на регулярните доклади
- Контрол над обхвата на проекта

Технически Ръководител Проект (ТРПр)

След инициирането проекта по поддръжка ТРПр, освен основните дейности описани по-горе за които съдейства на РПр, изпълнява и подготвя следните дейности:

- ✓ Организация, събиране и попълване на техническа информация на област на вътрешно-фирмения портал обособена за конкретния проект по поддръжка
- ✓ Подготовка и настройки на технически средства и инструменти необходими за контрол и проследяване на проекта като например Система за следене на инцидентите, Система за следене на промените в конфигурациите, Система за наблюдение на различни параметри и наличност на оборудването и други
- ✓ Организиране при необходимост на вътрешно-фирмени срещи и/или обучения с целия инженерен състав от всички нива на поддръжка за запознаване със съответния проект, процедури, специфики на обслужване и технологии за поддръжка
- ✓ Организиране и изчистване на процедурата по обслужване за конкретния клиент и проект, както и запознаване на всички заинтересовани лица от клиента с нея

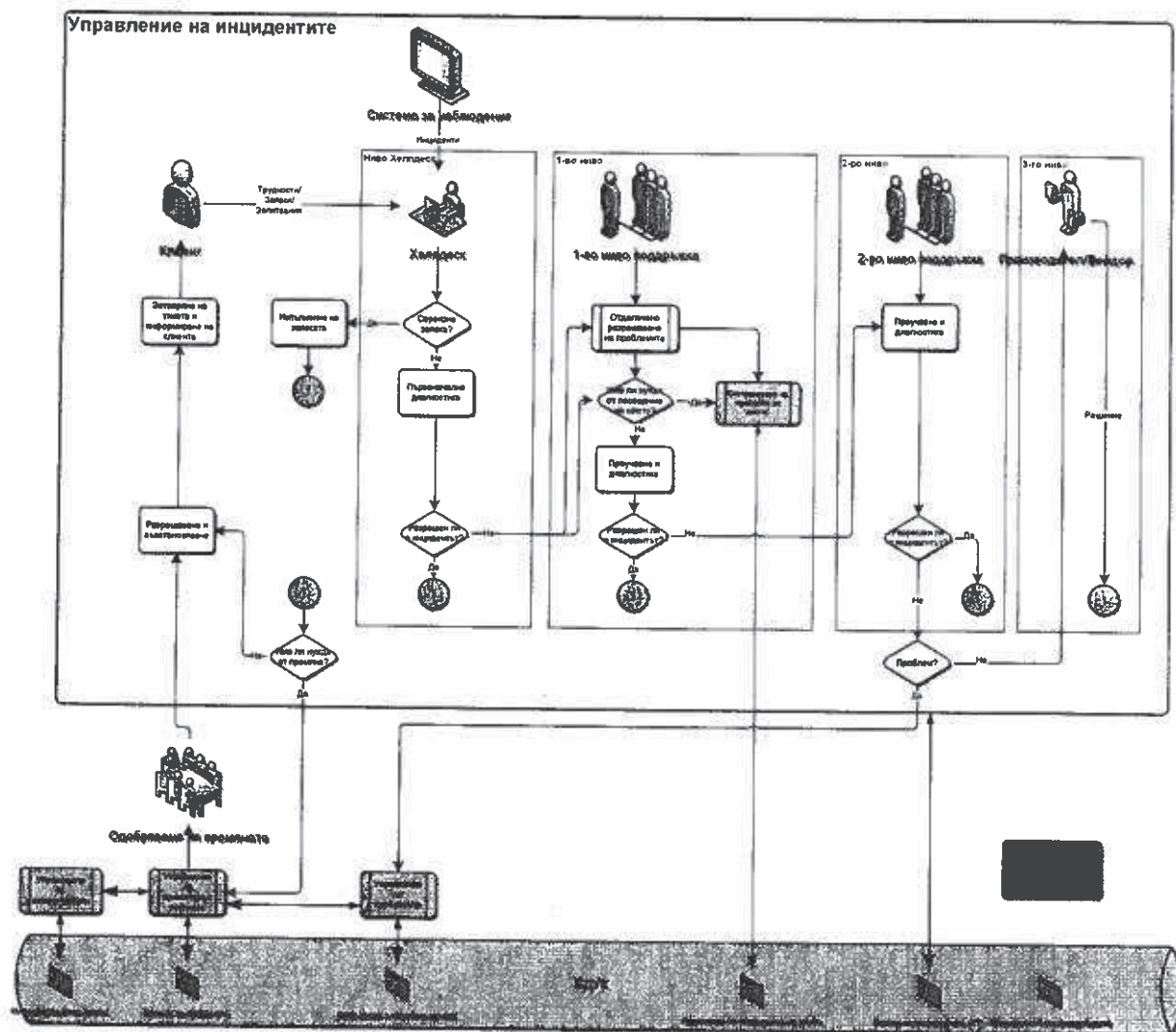
По време на изпълнение на проекта и в зависимост от обхвата, технологията и решението на обслужване и поддръжка ТРПр следи и отговаря за следните параметри:

- Регулярна проверка (минимум 1 път в месеца) за актуалност на техническата информация на вътрешно-фирмения портал
- Изготвяне и анализ на периодични доклади към клиента
- Точка на ескалация при нарушаване на договорените времена за наличност и реакция
- Техническа точка за контакт от страна на клиента при ескалация
- Единствена точка за контакт вътре в компанията при необходимост от информация
- Необходимост от периодични опреснителни обучения и/или срещи с инженерите от всички нива на поддръжка



Описание на процеси и дейности по управление и поддръжка на мрежата на клиента

Всички инциденти и проблеми свързани с функционирането на клиентската мрежа се регистрират, анализират и отстраняват съобразно утвърдената процедура за управление на инциденти показана на следващата схема.



Телелинк се може да поеме ангажимент за ежедневните процеси по поддръжка и експлоатация – Управление на инцидентите, Управление на проблемите, Управление на конфигурациите, Управление на промените и Управление на версиите, както и процедури за Отстраняване на проблемите на място и Отдалячено диагностициране.



Телелинк Хелпдеск осигурява единствена, централна точка за контакт за всички системи и под-системи на проекта, обработвайки всички инциденти, клиентски заявки и запитвания. Това звено осигурява интерфейс към всички други процеси по поддръжка.

Процесът Управление на инциденти управлява всички инциденти от регистрирането им до разрешаването и затварянето им. Целта на процеса е връщането на услугата към нормално състояние, колкото е възможно по-скоро и с минимално прекъсване за бизнеса на клиента.

Целта на процеса Управление на проблеми е да намали до минимум неблагоприятния ефект на инцидентите и проблемите върху бизнеса. За да постигне това този процес подпомага Управление на инциденти чрез управление на всички критични инциденти и проблеми, старайки се да запише всички алтернативни решения и „бързи решения“ като Известни грешки, когато това е подходящо и иницирайки промени, които да внедрят постоянното решение. Управление на проблеми също анализира тенденции при инцидентите и проблемите, за да може про-активно да предотврати появяването им.

Промените са внимателно управлявани през цялото време на техния жизнен цикъл от инициране и записване, през филтриране, оценяване, категоризиране, одобряване, назначаване на време за имплементиране, изграждане, тестване, имплементиране и тяхното преглеждане и затваряне. Един от основните резултати е одобрението на Промяната, което дава началото на действителното и имплементиране.

Управление на конфигурации осигурява основата за успешно управление на услуги и подпомага всички останали процеси. Основният продукт на процеса е базата данни за управление на конфигурациите (БДУК), състояща се от една или повече интегрирани бази данни, които описват в детайли ИТ инфраструктурните компоненти на организацията и всички други важни ИТ активи. Тези активи осигуряват услугите и се наричат конфигурационни единици.

Управление на инциденти

Главната цел на процеса Управление на инциденти е възстановяване на нормалната работа на услугата колкото е възможно по-скоро и намаляване до минимум на неблагоприятния ефект върху бизнес операциите, като по този начин се осигуряват най-добрите възможни нива на качеството и достъпност на услугата.

Инцидент се дефинира като:

- Всяко събитие, което не е част от стандартната работа на услугата, което причинява или може да причини прекъсване или намаляване на качеството на услугата.

Един инцидент може да възникне по някой от следните начини:

- Заявка от страна на клиента през web базираното приложение
- Телефонно обаждане от страна на клиента
- E-mail до Телелинк поддръжка

Обработката на клиентската заявка от неговата регистрация в Телелинк Хелпдеск системата до неговото изпълнение преминава през различни етапи:



Регистриране на инцидент

Всички инциденти се записват със съответната дата и час на регистрация, без значение от начина на инициране (телефон, e-mail, web интерфейс) – отваря се Trouble Ticket.

Генериране на автоматично съобщение от Телелинк Хелпдеск приложението, че заявката е регистрирана и приета и се изпраща до заявителя.

Ако сервизната заявка е получена по телефона, Хелпдеск операторът ръчно отваря ТТ от името на клиента, като описва в подробности разговора, отбелязва името и e-mail на лицето, което е направило заявката (Заявител). Регистрацията на нова заявка предполага назначаване на Хелпдеск оператора на смяна като собственик на този случай.

В някои случаи, в зависимост от важността, ТТ може да бъде отворен автоматично от мониторинг системата, поради ограничено време за реакция при отпадане на елемент от основната мрежа. По този начин се намалява първоначалното време за отваряне на ТТ, така че Хелпдеск операторът да премине директно към първоначална диагностика на проблема.

Проверка за оторизация

Преди да се пристъпи към обработката на нова заявка, Хелпдеск операторът се уверява, че лицето, което изпраща сервизната заявка е оторизирано от компанията-клиент. Ако той/тя не е в съгласувания списък с оторизирани служители, Хелпдеск операторът се свързва с основното лице за контакт от страна на клиента и изисква потвърждение за валидността на заявката и добавяне на нов контакт в листата с оторизирани лица.

Приоритизация на инцидента

Всеки инцидент се приоритизира съгласно възприетите Дефиниции на приоритетите. Клиента получава писмено уведомление за назначеното ниво на приоритет на неговия инцидент, съответно получава и нотификации при следващи промени на приоритета.

Първоначална диагностика

След получаване на по-детайлна информация от клиента по определена заявка, Хелпдеск операторът пристъпва към извършване на всички необходими и възможни действия за отдалечена диагностика, отстраняване на повреди и възстановяване на функционалността, съгласно съответната оперативна процедура за поддръжка на клиентската инфраструктура. Резултатите от всички действия се записват в ТТ от Хелпдеск оператора.

На този етап от процеса Хелпдеск операторът може да бъде способен да разреши инцидента, без да отнася въпроса към други екипи по поддръжка чрез следването на подходящи стъпки за отстраняване на инцидента или чрез съпоставянето на инцидента към Известна грешка и даването на подробности на клиента за разрешаването му. В този случай инцидентът трябва да бъде свързан към Известната грешка, така че всички засегнати клиенти да могат да бъдат идентифицирани, когато се намери постоянно решение.

Ескалация на случая към 1-во/2-ро ниво поддръжка

В случай, че проблемът не може да бъде разрешен от Хелпдеск оператора или в съответната оперативна процедура е указано незабавно назначаване на по-високо ниво инженер поддръжка или на регионален инженер (в случай на поддръжка на място), съответният ТТ се трансферира/ескалира към агент поддръжка от 1-во ниво (или респективно 2-ро ниво, за най-



високо приоритетни инциденти). Новоназначеният инженер предприема всички възможни действия за разрешаване/изпълнение на сервизната заявка и отбелязва в ТТ стъпка по стъпка целия процес, включително и странична кореспонденция с клиента. В случай на интервенция на обекта, извършените действия се регистрират в ТТ или от Хелпдеск оператора или от самия изпълнител, в зависимост от важността и приоритета на заявката.

Всяко посещение на обект на клиента се отразява в попълнен и подписан от Телелинк инженера и представител на клиента Протокол за посещение на обект. В него се описват всички действия предприети на обекта и, ако има, допълнителни забележки по експлоатацията на оборудването или възникнали проблеми (напр. неподходяща за работата на оборудването околна среда, липса на материали и т.н.).

При работа директно на обект на клиента често се налага подмяна на комуникационно оборудване на клиента с резервно/алтернативно. Това винаги се осъществява с Приемопредавателен протокол, подписан от Телелинк инженера и представител на клиента.

Ескалация към мениджър или производител/вендор

Тази ескалация се прилага при неизпълнение на сервизната заявка от техническите лица на Телелинк в договорените времеви рамки.

Ескалация към производител се прави изключително от инженер поддръжка 2-ро ниво с най-добри познания в дадена технологична област в следните случаи:

Ескалацията към производителя се извършва след:

- Инженерите на Телелинк са опитали да разрешат проблема, използвайки всички възможни алтернативни решения и източници на информация
- Проблемът е свързан с хардуерен или софтуерен дефект
- Проблемът е свързан с мрежови дизайн или функционалност на устройство
- Клиентът заявява разрешаването на софтуерен бър
- Проблемът е извън компетенцията и опита на Телелинк
- Трябва да се вземе бързо решение и няма време за анализ

Мениджърската ескалация е автоматизиран процес, извършван от Хелпдеск системата и базирано на съответния SLA. При активиране на този процес клиентът получава уведомление за ескалация на ТТ до мениджърския екип на Телелинк.

Проучване и диагностика

Всяко от по-високите нива на поддръжка може да установява отдалечена връзка (при възможност за такава) към засегнатото устройство/система, проучва и диагностицира инцидента. Всички тези дейности (включително подробности за действията, предприети за разрешаването или пресъздаването на инцидента) трябва да бъдат напълно документирани в ТТ, така че да бъде поддържан пълен хронологичен запис.

Следните действия е вероятно да бъдат изпълнени по време на изследването:

- Установяване какъв точно е проблемът и какви са очакванията на клиента



- Разбиране на точната хронологична последователност на събитията
- Потвърждаване на пълното въздействие на инцидента, включително броя и обхвата на засегнатите клиенти/системи
- Идентифициране на всички събития, които биха могли да са провокират инцидента (напр. скорошна промяна, някое действие на клиента и т.н.)
- Търсене за предишни инциденти/проблеми в базата данни с Известни грешки или в базите на производителите/доставчиците

Разрешаване и възстановяване

Когато се намери потенциално решение, то трябва да бъде приложено и тествано. Специфичните действия, които могат да бъдат предприети и хората, които са свързани с дейностите по възстановяване са различни, в зависимост от същността на повреда, но могат да включват:

- Инструктиране на клиента за определени действия със засегнатото оборудване
- Имплементиране на решението от Хелпдеск оператора отдалечено (напр. рестартиране на устройство), използвайки софтуер за отдалечен достъп до оборудването на клиента
- Имплементиране на специфично решение от специализирани екипи на поддръжката (напр. реконфигуриране на маршрутизатор)
- Разрешаване на проблема от доставчик или трета страна.

Провеждат се обстоятелни тестове дори когато е намерено решение, за да се потвърди, че действията по възстановяване са изпълнени докрай и че услугата е напълно възстановена.

Независимо от предприетите действия, записът за инцидента трябва да се актуализира с цялата свързана информация, така че да се поддържа пълен хронологичен запис.

Ако групата, която разрешава инцидента е различна от Хелпдеск звеното, то тя трябва да предаде инцидента обратно към Хелпдеск оператора за затваряне.

В конкретни случаи имплементирането на „решението“ може да е обект на процедура по управление на промените. Съответно трябва имплементирането трябва да се съобрази с правилата за съответния клиент.

Затваряне на инцидента

Преди затварянето (разрешаване) на даден случай, трябва да бъде получено потвърждение от клиента за успешно изпълнение на сервизната заявка и отказ от наблюдение на съпътстващи събития. Затварянето на ТТ в Хелпдеск системата автоматично ще генерира уведомление към клиента, че случаят е приключен и няма да бъде видим в списъка с активните заявки.

Управление на проблеми



Целта на Управление на проблеми е да се намали до минимум неблагоприятния ефект на проблемите върху бизнес процесите на клиента, които са причинени от грешки в IT инфраструктурата, и да предотврати повторната поява на инциденти, свързани с тези грешки. За да постигне тези цели Управление на проблеми се стреми да намери причината за възникване на инцидентите и да започне дейности по подобряване или поправяне на ситуацията.

Процесът Управление на проблеми има реактивна и проактивна страна. Реактивната страна се занимава с разрешаването на проблеми в отговор на един или повече инциденти. Проактивната страна се занимава с идентифицирането на проблеми и Известни грешки до възникването на инциденти.

Проблем се дефинира като:

- Неизвестната причина за поява на един или повече инциденти

Известна грешка се дефинира като:

- Инцидент или проблем, за който причината е известна или за когото е намерено временно решение или постоянна алтернатива. Възможно е инициране на заявка за промяна, ако съществува бизнес изискване за това, но се идентифицира като Известна грешка освен, ако не е разрешена за постоянно от имплементирана Промяна.

Алтернативно решение се дефинира като:

- Намаляване или елиминиране на въздействието на инцидент или проблем, за който все още няма крайно решение.

Управление на конфигурации

Целите на процеса Управление на конфигурации са:

- Описване на всички IT активи и конфигурации на управляваните услуги
- Осигуряване на точна информация за конфигурациите и тяхната документация, за да се поддържат всички други процеси по управление на услугите
- Осигуряване на стабилна основа за процесите Управление на инциденти, Управление на проблеми, Управление на промени и Управление на версии
- Сравняване на конфигурационните записи срещу действителната инфраструктура и коригиране на всякакви несъответствия.

Обхватът на процеса Управление на конфигурации включва всички компоненти, които са счетени за важни за доставката на управлявани услуги.

Конфигурационна единица се дефинира като:

- Компонент от инфраструктурата, който е под контрола на процеса Управление на конфигурации. Това включва хардуер, софтуер и свързаната документация. Може също да включва и заявки за промяна, договори с



гарантирани параметри на услугата, процедури и всякакви други елементи, които трябва да бъдат контролирани. Информацията за конфигурационните единици се държи в база данни за управление на конфигурациите (БДУК).

Управление на промени и Управление на версии

Целта на Управление на промени е да се осигури използването на стандартизирани методи и процедури за ефективно и бързо обработване на всички промени. По този начин се намалява ефекта на заявките, свързани с промени и се подобрява доставянето на услуги на клиента.

Нуждата от промени възниква както проактивно, така и реактивно поради редица причини:

- Проактивно – например, търсейки ползи за бизнеса като намаляване на цените, подобряване на услугите или повишаване на ефективността на поддръжката.
- Реактивно - като средство за разрешаване на грешки или адаптиране към променящи се обстоятелства.

Промяна се дефинира като:

- Всяко добавяне, модификация или премахване на одобрена, планирана или поддържана услуга или компонент на услугата и свързаната с нея документация.

Целта на Управление на версии е да въвежда нови версии на конфигурационните единици в експлоатационна среда.

Версия се дефинира като:

- Съвкупност от хардуер, софтуер, документация, процеси или други компоненти нужни за имплементация на една или повече одобрени промени на услугите.

Следните кодове се използват, за отразяване статуса на Заявката за Промяна:

- Отворена: Заявката е приета, но все още не е назначена.
- В прогрес: Заявката е приета, одобрена и има назначен отговорник. Работи се по изпълнението на Промяната.
- Одобрена: Бизнес и техническата оценка са завършени, промяната е одобрена и предадена за изпълнение.
- Отхвърлена: Промяната е отхвърлена и ще бъде върната към Заявителя с описание за отказа и препоръки за по-нататъшни действия.
- Затворена: Заявката е затворена
- Отменена: Заявката е отменена.

Отстраняване на проблеми на място

Това са услугите, свързани с посещение на място като хардуерна поддръжка, подмяна, конфигуриране инсталация на ново оборудване. Телелинк осигурява 2-часов (или по-добър) отговор за посещение на място от времето на получаване на заявката за съдействие на място.

Достъп за отдалечено отстраняване на проблеми

Тази процедура описва възможностите на Телелинк да достъпва отдалечено клиентските мрежи или чрез използването на канал за управление от потребителската мрежа или чрез използването на отделна мрежа за управление.

Управление на сигурността

Управлението на сигурността се простира върху всички процеси и дейности по поддръжка и осигурява конфиденциалността, интегритета и достъпността на активите, информацията, данните и услугите на Телелинк и клиентите на Телелинк.

Компанията е сертифицирана по стандарта за информационна сигурност ISO27001.

Непрекъсваемост на услугите/Възстановяване от бедствие

Непрекъсваемостта на услугите цели, в случай на бедствие или загуба на Центъра за управление на мрежата, възстановяване на нужните технически и сервизни устройства (включително компютърни системи, мрежи, приложения, телекомуникации, техническа поддръжка и Хелпдеск звено) в договорени времеви интервали. За да се постигне това, Телелинк има на разположение резервирано местоположение за Центъра за управление на мрежата, изнесени резервни сървъри и приложения за наблюдение, както и план за непрекъсваемост на бизнеса в условия на бедствие.

5.3.2. Административна ескалация

С цел предоставяне на ефективни и надеждни услуги по поддръжка, Телелинк гарантира навременното отстраняване на проблеми. В случай на забавяне от договорените времена, всеки инцидент подлежи на автоматична административна ескалация по долу посочената схема.

Инцидентът който бъде административно ескалиран, автоматично се назначава на посоченият в таблицата контакт, който наблюдава случая до неговото трайно разрешаване и осигурява необходимият ресурс за това.

Първоначално време	Ескалация 1	Ескалация 2	Ескалация 3	Ескалация 4
1-час	Ръководител отдел Поддръжка			



Минимално време	Приоритет 1	Приоритет 2	Приоритет 3	Приоритет 4
4-часа	Директор Системна Интеграция Ескалация към производител	Ръководител отдел Поддръжка		
24-часа	Изпълнителен Директор	Директор Системна Интеграция Ескалация към производител		
48-часа		Изпълнителен Директор	Ръководител отдел Поддръжка	
72-часа			Директор Системна Интеграция Ескалация към производител	Ръководител отдел Поддръжка

5.3.3. ON-LINE система (OTRS) за приемане и обработване на сервизни заявки

Системата за регистриране и управление на инциденти има за цел да проследява прогреса по работата на всички активни инциденти и сервизни заявки, както и съхраняването им в единна централизирана база от данни. Системата притежава възможност за отдалечен ролеви достъп на потребители с различни права, както от страна на техническите специалисти на Телелинк така и от страна на Клиента. Телелинк използва специализиран софтуер за работа с регистриране и управление на инциденти – OTRS (Open Technology Real Services).

Системата за регистриране и управление на инциденти е достъпна през web на адрес <https://support.telelink.bg/otrs/customer.pl> Системата се достъпва след предварително направена регистрация с валиден имейл адрес и парола. Регистрацията се прави от Телелинк при необходимост или при поискване от страна на клиента. Системата функционира върху резервирани и географско раздалечени мрежови сървъри на Телелинк и нейният адрес е достъпен през Интернет.

Основни функции на системата са:


- Автоматично генериране на уникален идентификатор на всеки инцидент (което дава възможност за проследяване на активни и вече затворени инциденти)
- Удобен, интуитивен web интерфейс
- Описание на статуса на всеки инцидент [Open, Pending (Customer, Telelink, Third Party), Closed (with workaround)]

- Записи и атрибути на инцидента, които не могат да бъдат променяни:
 - Отговори и обновявания на всеки направен запис
 - Времеви полета (timestamps)
 - Лог на промените
- Автоматично уведомление при административна ескалация

Основни компоненти на системата са:

- Начален екран
- Регистриране на инцидент (създаване на сервизна заявка)
- Преглед на историята на инцидентите (преглед на отворени и/или затворени сервизните заявки)
- Моят профил (персонални настройки на профила за достъп до системата).

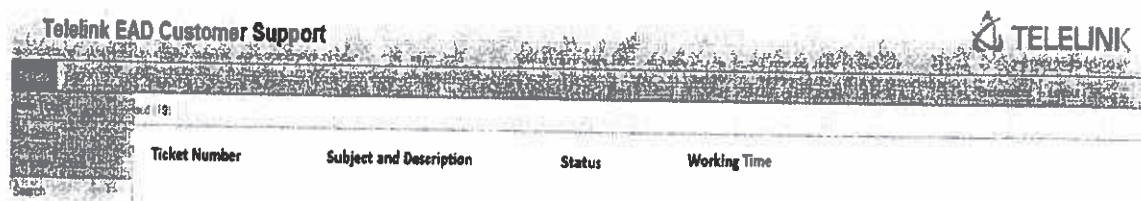
За достъп до системата трябва да е въведено потребителско име и парола в полето ВХОД. Само Телелинк, може да създава акаунти на клиентите си.



ФИГУРА 2: НАЧАЛЕН ЕКРАН – СТРАНИЦА ЗА ВЛИЗАНЕ В СИСТЕМАТА

Началният екран, показан на следващата фигура предоставя следните възможности за избор при работа със системата:

- Регистриране на инцидент – *New Ticket*
- История на инцидентите – *My Tickets and Company Tickets*
- Търсене на сервизни заявки в базата данни – *Search*



ФИГУРА 3: ОСНОВЕН ПРОЗОРЕЦ – КЛИЕНТСКИ ИЗГЛЕД

Системата показва всички Отворени (Open) и всички Затворени (Closed) заявки, заедно с техния номер, статус и дата на последна промяна. Чрез този екран, Клиентът може да проверява статуса на работата по създадената то него заявка, с какъв приоритет е, кой инженер е назначен по нея и т.н.

При избиране на опцията **Регистриране на инцидент (New Ticket)**, системата предлага да се избере какъв тип да бъде заявката:

Incident:

- Заявка за инцидент в мрежата на клиента;

Problem:

- Заявка за проблем в мрежата на клиента;

IMAD:

- Заявка за инсталация на ново оборудване;
- Заявка за миграция на съществуващо оборудване;
- Заявка за премахване/демонтиране на съществуващо оборудване;
- Заявка за добавяне на модули на съществуващо оборудване;

Като всичко се отнася само за съществуващо оборудване, което е в обхвата на проекта

Change:

- Промяна на конфигурация на съществуващо оборудване;
- Всяка промяна, която не е дефинирана в IMAD (например: смяна на IOS, смяна на повреден кабел, описване на порт и т.н.);

Other:

- Заявка за консултация/съвет към Телелинк;
- Заявка за нова оферта към Телелинк;
- Всичко останало, което не е дефинирано в предишните типове.

При избор на един от типовете се отваря форма за въвеждане на заявката, показана на следващата фигура:



TELELINK

150 Sofia Bulgaria • Business Park Sofia • Building 12A Floor 3
Tel: +359 2 970 40 40 • Fax: +359 2 970 40 43 • www.telelink.com

Telelink EAD Customer Support

TELELINK

Preferences Logout

*Type: [dropdown]
*T: [dropdown]
Service: [dropdown]
SLA: [dropdown]
*Subject: [text field]
*Text: [text area]
Attachment: [Choose File] No file chosen
Submit

ФИГУРА 4 СЪЗДАВАНЕ НА НОВА ЗАЯВКА

Полетата отбелязани с * са задължителни, като винаги в полето TO се поставя SERVICE DESK от падащото меню. Автоматично става избора при полето SERVICE в зависимост от договора на клиента с Телелинк. В полето SLA се дефинира приоритета на заявката (P1,P2 или P3) като се появява и допълнително описание за наличността на услугата (24x7, 8x5 или друга).

Формата предоставя възможност за въвеждане на тема и детайлно описание, както и за прикачване на файлове.

За търсене в системата заявки както по клиент така и тези които са били създадени от дадения потребител, се избира Tickets->Search и се появява нов прозорец в който може да се дефинират различни параметри за търсене. За улеснение на търсенето може да се дефинират шаблони. При търсенето, клиента вижда и може да търси само заявки за неговия проект, и не може да вижда други заявки на клиентите на Телелинк.



Tickets

FAD

Profile

Search template



Select

Delete

Search

TT#

TT#

e.g. 1012155 or 1095157

CustomerID

Fulltext search in tickets (e. g. "John*n" or "WiFi*")

From

To

Cc

Subject

Text

Services:

Types:

Extended Support

Generic

Managed Services

Service Relay Point

Support



11/11

Change

IMAD - Installation/Move/Add/Disposal

Incident

Other

Problem

Priority:

State:

Priority 1

Priority 2

Priority 3



closed

closed with workaround

merged

new

open



Time restrictions

All

Only tickets created

within the last ...

1

day(s)

Only tickets created between

11

13

2013

and

12

13

2013

11

Save search as template?

Save as Template?



Template Name

Search

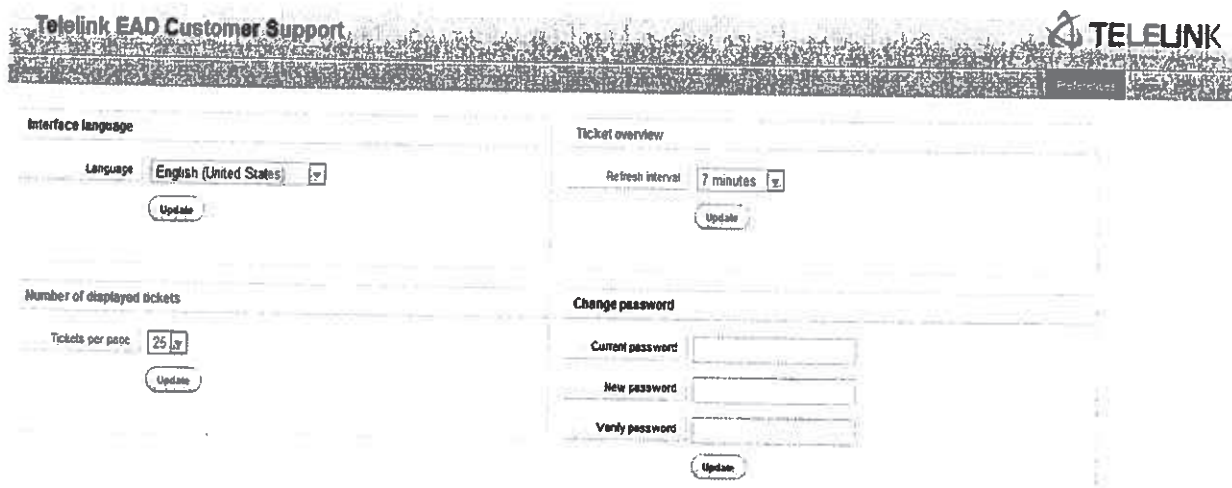
Output to

Normal



ФИГУРА 5 ТЪРСЕНЕ В БАЗАТА ДАННИ НА СЕРВИЗНИТЕ ЗАЯВКИ

При избиране на опцията Preferences от началния екран, системата показва персонални настройки за профила за достъп до системата, визуализацията на клиентския интерфейс на системата, както и възможност за промяна на паролата.



ФИГУРА 6 НАСТРОЙКИ НА ПРОФИЛА НА КЛИЕНТСКИЯ ИНТЕРФЕЙС.

План за обучение

1. Обхват

Документът описва начина за провеждане на обучение на екип от специалисти на Възложителя, като целта на провежданите занятия е аудиторията да бъде запозната със съвременните технологии, оборудване и системи, използвани при изграждането на по отделните елементи на решението.

Обучението е фокусирано върху технологиите, оборудването и системите, които ще изградят комуникационната инфраструктура и нейните специфични функционалности. След завършване на обучението, екипът, който ще бъде обучаван, ще има познания за дизайна, конфигурацията, функционалността и услугите, както и за процедурите по експлоатация и начина на работа с различните компоненти и системи.

Предвиденото обучение е с техническа насоченост, ще се проведе на годишна база в рамките на 4 години съгласно предварително подготвени и съгласувани в Възложителя конкретни графици и теми.

2. Документация за обучение

Изпълнителят се ангажира с осигуряването и разпространението на всички материали, които са необходими за провеждане на обучението. Материалите за обучението бъдат осигурени от Изпълнителя, като те ще включват материали и ръководства на оборудването, както и специфично изготвени за обучението презентации, примерни сценарии и упражнения, където е възможно.

Допълнителна информация относно обучението:

- Занятията на обучението ще се проведат в помещения на Възложителя;
- Обучението ще бъде проведено на български език;
- В настоящия документ е включен примерен график обучението, който ще бъде съгласуван допълнително с Възложителя.

3. Методология

Занятията на обучението ще се провеждат под формата на семинари, които ще съдържат последователност от лекции и упражнения при използване на следните техники:

- Презентации – концептуално представяне на възможностите и функциите на комуникационното оборудването, което ще се използва в проекта, като също така ще се

наблегне на конкретните конфигурационни шаблони за различните типове услуги и функционалността на отделните компоненти;

- Демонстрации – ще се проиграт типични сценарии, като се демонстрират стъпки от процеса на експлоатация на комуникационното оборудване;
- Самостоятелни упражнения – курсистите ще имат възможност самостоятелно да се запознаят с възможностите на отделните компоненти на оборудването и начина на работа с мрежата;
- Обобщения – в края на всеки учебен ден се прави обобщение на ключовите знания, необходими за работа;
- Въпроси и отговори – лекциите и упражненията протичат интерактивно, като основна задача на всеки лектор е да придобие увереност, че преподавания материал е усвоен от курсистите. Стремежът е максимално пълно да се отговори на всички възникнали въпроси по време на обучението.

Използвайки комбинацията от всички горни описание методи се гарантира осигуряването и получаването на необходимите теоретични и практически знание по поддръжката и експлоатацията на изградените решения.

4. Стратегия

Техническото обучение на екипа на Възложителя е ключов момент при експлоатацията на IT инфраструктура, като основната цел е провеждането на качествени и ефективни занятия, които да запознаят специалистите с работата с мрежовите устройства, дизайна на мрежата и системите за наблюдение и управление.

Основната задача на Изпълнителя е провеждането на качествено обучение, чрез лектори, които са специалисти с опит и познания в дадената област и предварително подготвени учебни материали и упражнения.

Задача на Възложителя е изборът на точния екип от специалисти, които са пряко свързани с процеса по експлоатация и поддръжка на комуникационната инфраструктура.

5. Учебна база

Учебната зала, в която ще се провежда обучението трябва да бъде оборудвана с мултимедиен проектор, LAN мрежа, Интернет достъп, както и с отдалечен достъп до оборудването на изградената IT инфраструктура. За всеки инженер участващ в обучението трябва да има работно място с компютър. За целите на обучението ще бъдат демонстрирани възможностите на оборудването в комуникационната система на Възложителя и/или свободно оборудване от лабораторията на Изпълнителя.



6. Учебна програма, график и предмет на обучението

След успешното приключване на курса, те ще имат придобити знания за изградената система, структурата, компонентите и работните ѝ възможности. След края на курса ще бъде подписан протокол и ще бъдат издадени персонални удостоверения за преминат курс на обучение.

Обучението ще бъде съобразено с доставеното оборудване и софтуер, техните конфигурации и функционалност.

В следващата част от документа са описани по-подробно темите в отделните модули на обучението, което ще бъде проведено според нуждите и плана за внедряване:

№	Обучение	Съставни Модули	Обща продължителност
1.	Power Servers & AIX	Запознаване с Power архитектурата – Servers, HMC; Виртуализация – PowerVM, Power VC, VIOS, Pools, Partition mobility; OS – AIX (AIX Jumpstart Training) – процеси, LVM, памет, потребители и др; PowerHA, HyperSWAP	5 дни
2.	Storages	Brocade SAN IBM SVC Technical Training – архитектура, възможности GUI Storwize V7000 DS8000	5 дни
3.	FlashCopy Manager	Запознаване с използвания софтуер Добри практики	5 дни
4.	TSM	Backup & recovery with TSM – основно запознаване с архитектурата, възможностите и интеграция с DB2, SAP FlashCopy Manager – използване за създаване на копия на данните, интеграция с DB2, SAP, TSM	5 дни
5.	Виртуализация	Запознаване с внедрения софтуер VMware Добри практики	2 дни
6.	Облачни услуги	Запознаване с технологиите - Openstack	1 ден

Допълнително по желание на възложителя може да се организира IBM Technical University – Глобална серия от срещи на специалисти от IBM и основните ползватели на техниката. Предлагаме регулярно – веднъж в годината за 1 седмица, специалисти на банката да участват в тези обучения, където да научат повече за направленията на развитие на IBM в областите на хардуерните платформи, сървъри и дискови масиви и на системния софтуер. А така също да придобият практически знания в Lab сесиите.

7. Списък от курсисти

Преди началото на всеки курс Възложителя трябва да предостави списък с предвидените участниците във курса, както и да гарантира за тяхното присъствие, което ще бъде удостоверявано по време на обученията чрез попълване на Присъствен лист.

Изпълнителят ще осигури възможност за обучение на от 4 до 6 служители на Възложителят.

8. Организация

За провеждане на ефективно и качествено обучение трябва да се създаде организация, която да включва специалисти със следните роли:

- Лектори от страна на Изпълнителя, които ще водят учебните занятия;
- Координатор на учебните занятия от страна на Изпълнителя;
- Координатор на учебните занятия от страна на Възложителя;
- Курсисти;

9. Оценка на преподавателя

В края на провежданото обучение всички курсистите попълват Анкетна карта, в която изразяват своето мнение за качеството и ефективността на проведеното обучение и на получените учебни и помощни материали.

Процедури по управление на проекти по обслужване на клиенти и внедряване на нови решения

Дейността по Управлението на проекта цели осигуряването на съответствие на изхода на проекта с изискванията, посочени в Договора и конкретния обхват на възложената поръчка и работа. Това е дейност, която включва основно планиране и изпълнение на проекта, наблюдение, контрол и отчитане по отношение на процесите, свързани с обхвата, качеството, графика, рисковете, човешките ресурси, разходите и комуникациите по проекта. За да постигнем това следваме най-добрите практики, които са се доказали от натрупания опит до сега.

Процесите за управление на проекти в Телелинк се базират основно на международния стандарт и методология на PMI (Project Management Institute®) като през годините непрекъснато се адаптират и подобряват към променящата се бизнес среда в България и според различните нови технологии и решения, които предлагаме на нашите клиенти. Също така Телелинк разполага с Ръководители проекти сертифицирани до най-високо ниво от PMI - PMPro (Project Management Professional).

В този документ ще намерите детайлно описание и информация по отношение на:

1. Процедура по управление на проекти при внедряване на нови решения
2. Процедура по управление на проекти при обслужване и поддръжка
3. Описание на дейностите по изпълнение в проекта

1. Процедура по управление на проекти при внедряване на нови решения

Телелинк ще организира внедряването на новите решения в един или няколко проекта в зависимост от времевите рамки и технологичните области, които бъдат възложени от БНБ според предложените фази за концептуално развитие. За всеки един от проектите ще бъде назначен основен екип от Ръководител Проект (РП) и Технически Ръководител Проект (ТРП), който ще отговаря за цялостното управление и изпълнение на проекта. Допълнително всеки един проект има и допълнителен екип, който не се променя по време на изпълнението на проекта, съставен от Търговски представител (ТП), Инженер пред-продажби (ИП), Архитекти на решението (А). Допълнителния екип носи пряка отговорност за успешното завършване на проекта, но бива координиран и свикван за определени задачи от основния екип по проекта.

Всеки един проект за внедряване (вкл. ре-дизайн, дизайн) в Телелинк преминава през следните основни етапи и процеси:

Инициране

Планиране

Изпълнение

Наблюдение и контрол

Приключване

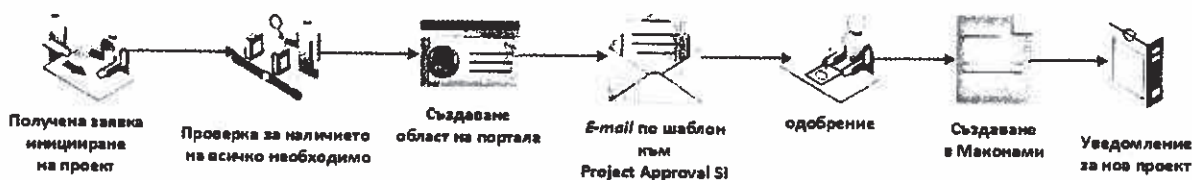
Инициране

Иницирането води своето начало от Търговския представител (ТП), който има ангажимент да пусне заявка за нов проекта към звено Бизнес Процеси (БП). БП екипа преглежда входната информация (минимум обхват на работа и количествено стойностна сметка) и стартира процес по избор на основен екип по проекта.

След назначаването на основния екип, който се подбира според необходимите професионални умения и нужди за конкретния случай, РП и ТРП имат грижата да се запознаят в детайли с основната част от бъдещия проект - бюджет, обхват и срокове, като за тази цел преглеждат подготвените от предпродажбения екип документи, събрани оферти от доставчици, както и се срещат с него, за да се запознаят със спецификите и разяснят най-важните моменти и детайли от решението, което трябва да се внедри. След като основния екип се увери, че цялата информация е налична и всички компоненти в бюджета са заложили коректно и отговарят на това, което е поръчано от клиента задвижват вътрешно-фирмена процедура по инициране на нов проект, която включва следните стъпки:

- ✓ Изпращане на заявка към звено Бизнес Процеси за създаване на нов проект съдържаща бюджет с остойностено необходимото оборудване и дейности за изпълнение на проекта, както и официална поръчка от клиента
- ✓ Звено Бизнес Процеси проверява за цялост на заявката и създава област на вътрешно-фирмения портал където ще бъде обособено място за разработване, организиране и съхранение на цялата документация по съответния проект
- ✓ След което се изпраща заявка към ръководството на компанията за одобрение за създаване на проект и отпускане на бюджетна рамка на екипа по проекта с която да го за изпълни
- ✓ След получаване на съответните необходими нива на одобрение проекта получава своя уникален номер и се създава в ERP системата на Телелинк със заложен бюджет и срок

SI Services



Планиране

Фазата на планиране е една от най-важните фази в един проект, тъй като по време на нея се анализират и изготвят необходимите реквизити за управление на проекта или т.нар. План на проекта, който съдържа всички или част от следните компоненти:

График на проекта

РПр и ТРПр извършват по-задълбочен анализ на заложените дейности по съответния проект и спрямо бюджета и необходимите ресурси изготвят първоначален график за изпълнение, който съдържа най-важните и основни дейности с поставени вече по-конкретни времеви рамки, за да може да се изпълнят заложените срокове и очаквания към клиента.

Матрица на основните заинтересовани лица

РПр и ТРПр изготвят план на основните заинтересовани лица включващ роли и отговорности по проекта, както и план на необходимите човешки ресурси. ТРПр е необходимо да направи по-задълбочен анализ според внедряваните технологии и заложените дейности в обхват на проекта какъв тип и ниво на квалификация инженерен екип ще му бъде необходим. Ако е необходимо може да поиска предварително назначаване на т.нар. Архитект на решение (Solution Architect) за съдействие за изготвяне и разбивка на дейностите и необходимия ресурс. В рамките на проекта Solutions Architect ще бъде отговорен за дизайна и проектирането на дадената технология, както и успешното и внедряване при клиента. По един проект може да има няколко Архитекта в зависимост от обхвата му и броя решения и технологии, които се преплитат. Задачата на ТРПр ще бъде да контролира и организира тяхната работа така, че да бъде в синхрон както помежду им, така и с изискванията и очакванията по договор с клиента.

Примерна матрица на основните заинтересовани лица по проекта, като при стартиране на проекта трябва да бъде допълнена с конкретни имена на лица и контакти за връзка:

Организация	Роля	Отговорности	Отчет за действията към
Телелинк	Ръководител договор (РД)	Ще следи периодично за общото качество на предоставените услуги и изпълнение на проекта. Ще бъде точка за ескалация при нужда от страна на Възложителя. Одобрява промени по договора при нужда.	Директор Системна Интеграция - Телелинк
Телелинк	Ръководител проект (РПр)	Управление и координиране на всички дейности по време на изпълнение на проекта от страна на Телелинк. Отговорен за изпълнение на обхвата на проекта според договорения график, бюджет и качество. РПр е точка за контакт за комуникация за Възложителя по време на изпълнението на проекта за административни въпроси.	РД Телелинк; Директор Системна Интеграция - Телелинк

Организация	Роля	Отговорности	Отчет за действията към
Телелинк	Технически Ръководител проект (ТРПр)	Отговорен за внедряването на техническото решение и изпълнение, както и следи за качеството на всички технически дейности според необходими стандарти и процедури за това. Отговорен за координация между техническите лица работещи по проекта; възлагане на задачи на всички технически лица; контролиране на прогреса по изпълнение на възложените задачи; техническото досие и документация на проекта. ТРПр е точка за контакт за комуникация за Възложителя по време на изпълнението на проекта.	РПр Телелинк
Телелинк	Архитект на решение Х	Изготвяне на дизайна на решението и необходимата техническата документация, както и следене и контрол на успешното и внедряване при клиента. Води техническа комуникация с екипа на клиента по изясняване на детайли и въпроси за съответното решение.	ТРПр Телелинк
Телелинк	Експертен технически екип	Помага при изпълнението на специфични технически задачи.	ТРПр Телелинк
Телелинк	Технически екип по места (ТЕМ)	Експерти и специалисти, които ще изпълнят монтажа на оборудването, захранване и инсталационни приемни изпитания по места, както и конфигурация и въвеждане в експлоатация на решението.	ТРПр Телелинк
Възложител	Ръководител проект (РПр)	Управление и координиране на проекта от страна на Възложителя. Оказване на съдействие на Телелинк за успешното приключване на проекта.	Мениджмънт - Възложител
Възложител	Експертен технически екип	Упълномощени експерти и специалисти на Възложителя, които да съдействат по време на разработване на дизайна на решението за събиране на необходимата предварителна техническа информация и съобразяване с текущите стандарти и политики на Възложителя	РПр Възложител
Възложител	Технически екип по места (ТЕМ)	Упълномощени експерти и специалисти на Възложителя, които по време на работа по обектите да съдействат за достъпа до съответните помещения за работа и да придружават техническите екипи на Телелинк, както и да подписват необходимите протоколи за извършените доставки и дейности по обектите	РПр Възложител



Забележка:	Описаните роли и отговорности от страна на Възложителя са минималните необходими функционални роли за успешното изпълнение и приключване на проекта. Подробно разпределение на ролите и отговорностите се очаква да бъде предоставено от Възложителя допълнително след подписване на договора и стартиране на проекта.
-------------------	--

План за управление на комуникациите

Предварителна уговорка за начин на комуникация между различните страни и роли според типа на информация, както и времевите рамки и интервали. Предварително се договарят или описват очакванията на клиента така, че да бъде навременно информирана всяка заинтересована страна от клиента, в необходимия размер и честота с цел ефективност.

Примерен план за управление на комуникациите:

Документ/Описание	Вид	Получател	Средство	Честота на изпращане	Оповорно лице
Цялостен преглед, контрол и наблюдение на проекта	Задължителен	РПр Възложител	Среща	Всеки месец	РПр Телелинк
Отчет за статуса на проекта към Възложителя	Задължителен	РПр Възложител	e-mail	всяка седмица	РПр Телелинк
Заявка за промени	Извънредно Двустранно	РПр Телелинк РПр Възложител	Официално писмо (хартиен носител)	при необходимост	РПр Възложител РПр Телелинк
Необходимост от допълнителна информация	Извънреден	РПр Възложител	e-mail	при необходимост	РПр Телелинк
Уведомления за започване на работа по конкретни обекти – план за работа за последваща седмица	Задължителен	РПр Възложител	e-mail	Предходната седмица на седмицата предвидена за работа	РПр Телелинк

Документ/Описание	Вид	Получател	Средство	Честота на изпращане	Отговорно лице
Одобрение и потвърждение на план за работа за последващата седмица	Задължителен	РПр Телелинк	e-mail	Предходната седмица на седмицата предвидена за работа	РПр Възложител
Предоставяне на всички технически документи за одобрение	Задължителен	РПр Възложител	Официално писмо (хартиен носител)	по график	ТРПр Телелинк
Одобрение на всички технически документи	Задължителен	ТРПр Телелинк	Официално писмо (хартиен носител)	при необходимост	РПр Възложител
Промени в графика на проекта	Извънредно Двустранно	РПр Телелинк РПр Възложител	Двустранно подписано допълнително приложение към договора	при необходимост	РПр Възложител РПр Телелинк
Протоколи от срещи между двете страни	Задължителен	РПр Възложител	Хартиен носител	след всяка среща	РПр Телелинк

План за управление на риска

Преди да започне проекта РПр, ТРПр и Архитектите е необходимо да помислят по-задълбочено какви рискове биха могли да излязат по време на решението от всякакво естество – техническо, административно, организационно и други, с цел да планират предварително по-добре дейностите и да се опитат да избегнат тяхното появяване, на кои дейности да се отдели повече време или допълнителен ресурс, или да се включат евентуално допълнителни дейности и стратегии в плана на проекта, които да въздействат върху предотвратяване на риска или дейности, които да минимизират шанса от случване на съответният риск.

Примерен план за управление на риска

Прогнозен											Реален			
№	1	2	3	4	5	6	7	8	9	10	11			
	Идентификация на Риск	Възникване на риск	Възможност за възникване на риск	Възможност за възникване на риск	Превенционни мерки за предотвратяване на риска	Стратегия/Корективни действия	Отговорник за риска	Дата на настъпване	Предприети действия/стратегия	Въздействие	Участници			
1	Неизпълнение на изискванията към обектите/помещенията	Средна	График Качество	н/а	Уведомяване на Възложителя за рисковете при инсталация в такива помещения/обекти. Предвидено време за отстраняване на забележките в графика. Предвидени огледи на помещенията	Удължаване на крайния срок на проекта. Подписване на Официално писмо удостоверяващ съгласието на Възложителя да се инсталира при предоставените от тях условия.	РПр Възложител	-	-	-	-			
2	Забавяне на доставките на оборудването от договорения срок с доставчика	Средна	График Бюджет	Смяна на дата за изпращане на оборудването от доставчика	Регулярни прегледи и проследяване на оборудването	Преразглеждане на графика и сроковете в договора	РПр Телелинк	-	-	-	-			

№	Прогнозен					Реален					
	1	2	3	4	5	6	7	8	9	10	11
	Идентифицирани Рискове	Варов-Риск	Въздействие в/у	Град на извършване	Предварителни мерки за предотвратяване на риска	Стратегия/Корективни действия	Отговорник за риска	Дата на настъпване	Предприети действия/стратегия	Въздействие в/у	Участници
3	Увеличаване на обхвата на проекта	Ниска	График Обхват	н/а	Съгласуван обхват на работа към договора с Възложителя	Подписване на допълнително приложение към договора за допълнителна поръчка. Промяна на план на проекта	РПр Телелинк РПр Възложител				
4	Непълно запознаване на екипа с проекта от страна на Телелинк	Ниска	Бюджет	Некоректно внедрен обект	Предварително изпращане на необходимата информация за работа и потвърждение за запознаване с нея от страна на екипа Пълно проследяване на работата на екипа по време на изпълнение на дейностите от назначени ТРПр	Допълнително посещение на обектите за корективни действия Допълнително изпращане на необходимата информация	ТРПр Телелинк				
5	Липса на свободен квалифициран персонал	Ниска	График Бюджет	н/а	Предварително уведомяване на ресурсните мениджъри за планирания график на работа и запазване на необходимите ресурси	Промяна в графика	РПр Телелинк				

Прогнозен						Реален					
№	1	2	3	4	5	6	7	8	9	10	11
	Идентификация Рисков	Вирител- ност	Въздей- ствие В/У	Степен на въздействие	Предвидени мерки за предотвратяване на риска	Стратегия/Корективни действия	Отговор- ник за риска	Дата на настъп- ване	Пред- приети действия/страт- егия	Въздей- ствие В/У	Участ- ници
6	Нереалистично определени продължителност на действията в графика или пропуснати/не планирани дейности	Средна	График Бюджет	н/а	Изготвяне на детайлен графика с участие на всички заинтересовани лица от двете страни. Получаване на максимално пълна информация от Възложителя	Ангажиране на допълнителен ресурс за изпълнение на графика Официална промяна на графика.	РГр Телелинк РГр Възложител	-	-	-	-
7	Забавяне на одобрение на Детайлния дизайн на проекта	Средна	График	н/а	Съгласуван график между двете страни. Явно описани задължения на двете страни в договора.	Удължаване на крайния срок на графика.	РГр Телелинк РГр Възложител	-	-	-	-
8	Промяна на крайната дата за приключване на проекта от Възложителя - закъснение или избързване	Средна	График	н/а	Съгласуван график от двете страни, включен към договора	Промяна в графика за сметка на някоя от другите дейности. Официална промяна на графика.	РГр Телелинк РГр Възложител	-	-	-	-
9	Забавяне (или непълна) на исканата информация от страна на Възложителя	Ниска	График	н/а	Явно изразен план за комуникация. Съгласуван от двете страни график.	Преразглеждане на графика	РГр Телелинк РГр Възложител	-	-	-	-

№	Прогнозен					Реален					
	1	2	3	4	5	6	7	8	9	10	11
	Идентифицирани Рискове	Вероят- ност	Въздей- ствие в/у	План за нама- вяване на риска	Предвидени мерки за предотвратяване/пoлoвa на риска	Стратегия/корективни действия	Отговор- ник за риска	Дата на настъп- ване	Пред- приети действи- я/страт егия	Въздей- ствие в/у	Участ- ници
10	Закъсняване на отговори от Възложителя към Телелинкa при необходимост от разясняване и изчистване на въпроси/проблеми	Средна	График	н/а	Навременно изпращане на цялата писмена комуникация. Ясна изразителност на всички необходими въпроси за разясняване и изчистване. Навременна ескалация на проблемите от двете страни.	Удължаване на крайния срок на проекта	ТРПр Телелинк РПр Възложител				
11	Проблемна комуникация м/у Възложител и Телелинк	Ниска	График Качество	Регулярно изоставане от графика	Редовни отчети за статуса на проекта и срещи със заинтересованите лица. Съгласуван официален План за управление на комуникации.	Преразглеждане на плана за управление на комуникациите	РПр Телелинк РПр Възложител				



План за контрол на качеството

Телелинк гарантира качествено изпълнение на доставките и услугите със създаване на стриктна организация за изпълнение на всеки договор документирайки План за изпълнение и управление на проекта в съответствие с конкретния обхват на договора.

Наръчник по качеството (НК) е основен документ на Системата за Управление на Качеството (СУК) за Телелинк, който документира политиката и целите по качеството на дружеството и дава описание на основните процеси, същността и обхвата на СУК. Наръчникът по качеството определя принципите, основните правила, взаимоотношенията и отговорностите при осъществяване на процесите по управление на качеството в съответствие с изискванията на БДС EN ISO 9001:2001. В това число НК служи като ръководство за дейността на персонала на дружеството по управление на качеството по време на изпълнение на възложените договори на Телелинк.

Контрол на документите – Телелинк има установени норми за създаване на документи, тяхното одобрение и съхранение. Компанията има установени процедури за контрол на документите. Всички административни и технически документи се преглеждат от съответния представител на екипа.

Осигуряване качество на доставка – оборудването трябва да е фабрично опаковано с не нарушена цялост на опаковката. Всички артикули в пратката – като документи, кабели или други допълнителни материали включени в комплекта – трябва да са налични.

Осигуряване качеството на услугите – конкретните дейности и услуги за дадения договор се контролират чрез разработването на План спрямо обхвата на дейностите както следва:

Цел	Методи за постигане
Всички дейности да бъдат изпълнени по график	Отчет за статуса на проекта към Възложителя всяка седмица.
	Предварително предотвратяване на грешки в дизайн и евентуални проблеми по време на Функционалните тестове в лабораторни условия.
	Внедряване на пилотни обекти.
	Предварителна подготовка и конфигуриране на оборудването преди доставка по обектите.
	Всички грешки и проблеми да бъдат ескалирани на момента.

Цел	Методи за постигане
Високо качество на изпълнение при внедряване	Проблемите установени при Оглед на обектите да бъдат ескапирани на време към Възложителя и коригирани от Възложителя преди инсталация.
	Техническите екипи да бъдат запознати предварително с обхвата на проекта, изискванията на Възложителя и процедурите и стандартите за инсталация за конкретния проект.
	Наличен План за имплементация за всеки тип обект.
	Работата на обект се изпълнява със съответната необходима документация.
	Правят се снимки след всяка инсталация и всяко посещение на обект и се изпращат от обекта за проверка към Технически Ръководител Проект.
	Всички инсталации се контролират и проверяват от Технически Ръководител Проект
	Внедряването и пускането в експлоатация на всяка точка се следи от ТРПр и/или съответния Архитект на решението

Цел	Методи за постигане
Високо качество на документацията	Всички документи се изготвят по установени образци и бланки от Телелинк съобразени с добри практики от предходни подобни проекти и препоръки на производителите на оборудването.
	Всички технически документи се преглеждат и контролират от ТРПр.

Цел	Методи за постигане
Висока удовлетвореност на клиента	Двустранно съгласуван, одобрен и подписан План на проекта и Детайлен дизайн. Стриктно спазване от двете страни на дейностите и отговорностите в План на проекта.





Цел	Методи за постигане
	Всички внедрени технологии и решения се разясняват детайлно на техническия състав на Възложителя.

Фазата на планиране завършва с организирането на следните две срещи:

- Вътрешна среща за стартиране на проекта, на която се представя общ план на проекта, включените дейности и технологии и очакваните срокове на изпълнение и ангажираност на необходимите екипи пред ресурсните ръководители и звено Бизнес Процеси. Целта на тази среща е екипа по проекта да запознае ръководството с какви бъдещи дейности и срокове сме ангажирани по коректния проект както и да получи обратна връзка и съвети от експертен екип с дългогодишен опит по отношение на плана на проекта
- Организиране на първа среща с клиента, с цел запознаване на членовете на основния екип от двете страни, запознаването и определянето на ролите на всеки един от тях. Както и представянето на предварително подготвените планове за цялостното изпълнение на проекта. На срещите се решава как и колко често по време на проекта ще се осъществява комуникация, докладване и други компоненти по управлението на самия проект. Целта на срещата е да се съгласуват всички компоненти от Плана на проекта с клиента, за по-добра организация и комуникация по време на изпълнението на проекта.

След приключване на тези срещи се допълва и/или коригира там където е необходимо Плана на проекта според договорените и допълнените дейности и уговорки.

Изпълнение

Всички дейности по проекта се планират, управляват и контролират от основния екип по проекта - РГП и ТРГП. На база предварително изготвения и съгласуван график с клиента се изготвя по детайлна разбивка на работата на ниво задачи според която на седмична база се ангажират необходимите ресурси от РГП.

ТРГП има грижата да постави конкретните параметри и изисквания на всяка една задача към съответния инженерен ресурс, както и очаквания резултат, неговия формат и срок на изпълнение. За тази цели се използва автоматизирана система за поставяне на задачи, която спомага за организацията на всеки един инженер по отношение на поставените му задачи на седмична база като в нея има зададени минимални реквизити за изисквана информация за стартиране на една задача.

ТРГП има отговорността да следи своевременно как се справя всеки с всяка поставена задача, дали е срещнал затруднения и съответно дали се очаква приключване в срок. При откриване на проблем ТРГП има отговорността да предприеме необходимите действия за справяне с проблема като ангажира допълнителен ресурс за съдействие или да ескалира навременно към РГП и/или клиент в зависимост от естеството на проблема.



Наблюдение и Контрол

Прилагане на практика и непрестанна актуализация на описаните начини за контрол на административно-организационните и технически дейности към проекта, включващи:

- ✓ Детайлен график за изпълнение на дейностите
- ✓ План за управление на комуникациите
- ✓ Матрица на основните заинтересовани лица и отговорности
- ✓ План за управление на риска
- ✓ Управление на обхвата и промените по проекта

Също така съществуват следните вътрешно-фирмени контроли и практики за проектите:

Среща за отчет на финансовите параметри

Всеки РГПр изготвя и представя финансов доклад към ръководството на дирекцията съдържащ статус на бюджета към момента спрямо прогнозния, очаквани крайни резултати и отклонения към момента, както и има ли налични промени в обхвата на проекта, графика и очаквани рискове, които биха повлияли на горното. Крайната цел е да се проследи основно финансовите резултати на всеки един проект и прогноза как ще приключи с идеята, ако може да се вземат мерки превантивно при нужда и да се представи общ статус на проекта.

Срещата се провежда 1 път в месеца и основните участници са всички РГПр и ръководния екип на дирекцията.

Актуален статус на проектите

Всеки ТРГПр представя обобщен статус за свършената работа и дейност за всеки активен проект и какво остава да се изпълни. Имаме ли проблеми и рискове с проекта от техническо естество. Целта е да се проследи прогреса и проблемите по оперативното изпълнение на проекта, както и ТРГПр да взаимодействат добри практики един от друг.

Срещата се провежда на всеки 2 седмици и основните участници са всички ТРГПр и Ръководител отдел Управление на проекти като се пада всеки един ТРГПр да говори 1 път в месеца

Обща дискусия РГПр и ТРГПр

Обща дискусия за добри практики, идеи, проблеми и коментари по ежедневната работа на един проект, дискутиране и разрешаване на казуси. Целта на срещата е да се подобрява работата между РГПр и ТРГПр да се извлича нужда от оптимизация/корекция на процеса по Управление на проекти и оперативната ежедневна работа.

Срещата се провежда на всеки 3 месеца и основните участници са всички РГПр и ТРГПр заедно с Ръководител отдел Управление на проекти.

Актуализация регистър на активните проекти

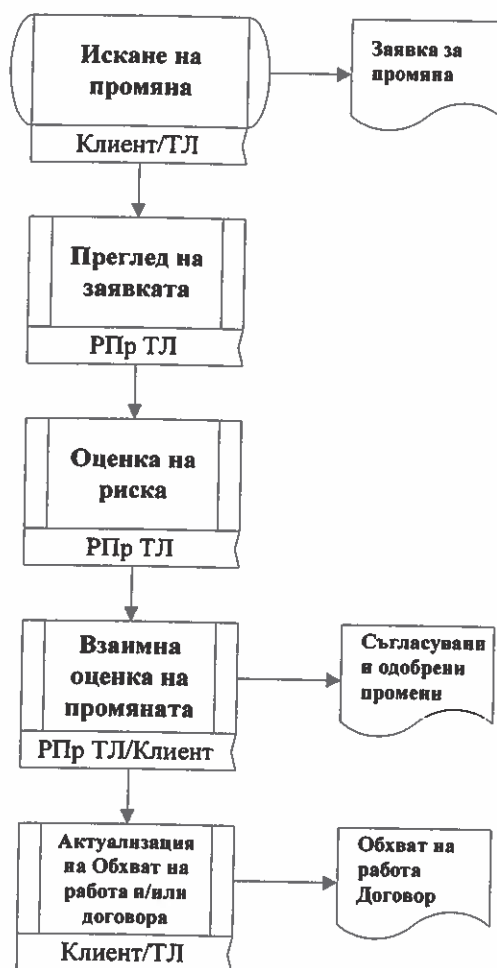
Звено Бизнес процеси 1 път в месеца прави преглед на изтичащите срокове на проектите и изпраща напомнящи е-маили към всички РГПр за приключване, актуализиране на статуса и/или удължаване



на срока на проектите. Целта е да разполагаме във всеки един момент с актуален регистър на активните проекти и очакваните срокове на вътрешно-фирмения портал.

Процедура за управление на промените

Без влияние в/у обхвата, графика и цената на проекта	РПр и ТРПр Телелинк (ТЛ)
Влияние върху обхвата	РПр ТЛ, ТРПр ТЛ, Оперативен директор ТЛ, Клиент
Влияние върху графика	РПр ТЛ, ТРПр ТЛ, Оперативен директор ТЛ, Клиент
Влияние върху крайната цена на проекта	РПр ТЛ, Оперативен директор ТЛ, Изпълнителен директор ТЛ, Клиент
Влияние върху качеството	РПр ТЛ, ТРПр ТЛ, Клиент



- Всеки, който желае да инициира промяна попълва Заявка за промяна (не се допуска одобрение на промяна, без налична заявка) и я предава на съответния Ръководител проект. Заявка за промяна и одобрение, които не са в писмен вид са неприемливи.
- Заявката трябва да съдържа причината за промяната, както и очакваното въздействие върху обхвата, графика, бюджета или качеството. Включването на всякаква допълнителна налична информация е силно препоръчително.
- Ръководителят на проекта оценява същността на заявката и определя вида и влиянието на промяната. Извършва се оценка на риска и резултатите се предоставят на двете страни.
- Заявката за промяна се разглежда съвместно от представители на двете страни с цел постигане на съгласие относно промените по резултатите, услугите и допълнителните разходи, ако е приложимо. Промените по проекта и промените на договора (ако има такива) трябва да бъдат потвърдени от двете страни в срок от 10 работни дни.
- Впоследствие промените се включват официално в Обхвата на работа и/или Договора (ако е приложимо).
- В случай на противоречие между първоначалния Обхват на работа и последвала Заявка за промяна, предимство има последната одобрена промяна.

Приключване

След приключване на дейностите по проекта и финалното приемане на работата от клиента РПр и ТРПр отделят време да направят подробен анализ на случилото се за:

- ✓ срещнати проблеми и начините за справяне с тях
- ✓ анализ на графика - изпреварвания и закъснения, и причини за това
- ✓ реално изразходван бюджет по съответните пера спрямо планирания
- ✓ използвани добри практики и иновативни подходи в работата на екипа по проекта

Всичкото това имат грижата да бъде описано в т.нар. база данни с научени уроци (Lessons Learned) след което се организира финална среща по проекта на която се събират екипа по проекта, екипа, който е работил по предпродажбената фаза и ръководството за разглеждане на анализи с цел взимане на полезни изводи и по-добра подготовка и организация при следващ подобен проект.

2. Процедура по управление на проекти при обслужване и поддръжка

Управлението на проектите по обслужване и поддръжка е организирано по подобен начин във основните 5 фази - Инициране, Планиране, Изпълнение, Наблюдение и Контрол, и Приключване, както и отново се назначава основен екип по проекта в ролята на РПр и ТРПр.

След одобрението и иницирането на един проект във фазата на Планиране, освен основните дейности описани по-горе по отношение на отговорници, план за комуникации и график се подготвят и изпълняват следните дейности от ТРПр:

- ✓ Организация, събиране и попълване на техническа информация на област на вътрешно-фирмения портал обособена за конкретния проект
- ✓ Подготовка и настройки на технически средства и инструменти необходими за контрол и проследяване на проекта като например Система за следене на инцидентите, Система за следене на промените в конфигурациите, Система за наблюдение на различни параметри и наличност на оборудването и други
- ✓ Организиране при необходимост на вътрешно-фирмени срещи и/или обучения с целия инженерен състав от всички нива на поддръжка за запознаване със съответния проект, процедури, специфики на обслужване и технологии за поддръжка
- ✓ Организиране и изчистване на процедурата по обслужване за конкретния клиент и проект, както и запознаване на всички заинтересовани лица от клиента с нея

По време на изпълнение на проекта и в зависимост от обхвата, технологията и решението на обслужване и поддръжка ТРПр следи и отговаря за следните параметри:

- Регулярна проверка (минимум 1 път в месеца) за актуалност на техническата информация на вътрешно-фирмения портал
- Изготвяне и анализ на периодични доклади към клиента
- Точка на ескалация при нарушаване на договорените времена за наличност и реакция
- Техническа точка за контакт от страна на клиента при ескалация
- Единствена точка за контакт вътре в компанията при необходимост от информация

- Необходимост от периодични опреснителни обучения и/или срещи с инженерите от всички нива на поддръжка

Повече информация за начина, организацията и средствата за обслужване може да намерите в отделен документ наречен „Описание на структурата и методиката за обслужване на клиенти“.

3. Описание на дейностите по изпълнение в проект

В зависимост от нуждите и конкретния обхват на решението и технологията, която ще се внедрява може да се включат следните основни дейности, които ще бъдат извършени и подробно документирани от Телелинк:

- ✓ Изготвяне на пълния набор от техническа документация за основните дейности;
- ✓ Валидиране изискванията на клиента;
- ✓ Оценка на готовността на обектите;
- ✓ Оценка на готовността на мрежата;
- ✓ Анализ на изискванията за сигурност;
- ✓ Концептуални тестове;
- ✓ Разработване на детайлен дизайн;
- ✓ Функционални тестове;
- ✓ Тестове за фабрични дефекти;
- ✓ Подготовка и предварителна конфигурация на оборудването;
- ✓ Доставка, физическа инсталация и оживяване
- ✓ Приемни изпитания на обект,
- ✓ Миграция;
- ✓ Приемни изпитания на решението;
- ✓ Изготвяне на екзекутивна документация;
- ✓ Обучение на персонала на Възложителя;

Всяка от тези дейности се извършва от Телелинк, като предварително се съгласува с Възложителя и едновременно с това се документира, за да се сведат до минимум проблемите и грешките при извършването ѝ. Цялата документация се съгласува и предоставя на Възложителя.

Валидиране изискванията на клиента

След разговор и дискусия с клиента, анализ на неговите изисквания и въз основа на предходното предложено решение, Телелинк разработва документ Доклад за валидиране изискванията на клиента. Неговата цел е да предостави:

- Подробна информация за изискванията на клиента по отношение на текущия проект;
- Концептуална архитектура и оценка на капацитета, необходими за определяне на хардуерно, софтуерно и инфраструктурното осигуряване за изграждане на решението;

- Анализ на съществуващата спецификация на оборудването и препоръки за промени, необходими, за да бъдат изпълнени изискванията на клиента;
- Пропуски в изискванията и рискове по отношение на решението;

Оценка на готовността на обектите

Оценка на готовността на обектите се извършва след потвърждение от клиента, че обектите са подготвени съгласно Спецификация на изискванията към обектите, разработена и предоставена предварително от Телелинк. Всеки обект ще бъде посетен от представител на Телелинк съгласно предварително подготвен и одобрен от двете страни график. При оценката на обекта се попълва Протокол за оглед на обекта, подготвен от Телелинк.

След приключване на огледите на всички обекти Телелинк ще подготви Доклад за готовност на обектите, който представлява обобщени резултатите от всички огледи. При констатирани разлики спрямо изпратените изисквания, Телелинк ще уведоми клиента за тях и ще изчака тяхното отстраняване преди да започне инсталацията на обектите.

Оценка на готовността на мрежата

Целта на оценка на готовността на мрежата е чрез подробно проучване да получи пълна характеристика на съществуващите технологии и решения при клиента във връзка с предложеното решение. Тази оценка може да включва целия инсталиран и оперативен хардуер и софтуер, както и протоколите, изграждащи мрежата на клиента.

Процесът за оценка на готовността на мрежата има три фази. Първа фаза включва документиране на съществуващото положение свързано с обхвата на проекта. През втора фаза се извършва техническа оценка на готовността на мрежата във връзка с предложеното решение. Трета фаза включва идентифициране и документиране на пропуски, които трябва да се вземат под внимание.

Анализ на изискванията за сигурност

Целта на процеса по анализ на изискванията за сигурност е чрез подробно проучване да получи пълна характеристика на съществуващите политики и процедури на клиента във връзка с предложеното решение и управлението на целия проект.

Процесът на анализ на изискванията за сигурност има три фази. Първа фаза включва документиране на съществуващите политики и процедури за сигурност, свързани с обхвата на проекта. През втора фаза се извършва техническа оценка на изискванията за сигурност, свързани с предложеното решение. Трета фаза включва идентифициране и документиране на пропуски, които трябва да се вземат под внимание.

За тази цел клиента трябва да предостави информация за съществуващите процедури по сигурност и съществуващите политики по сигурност;

Концептуални тестове

Телелинк ще проведе тестове, които да докажат специфични части от дизайн концепцията, за да се провери дали съпадат с изискванията на клиента. Концептуалните тестове се провеждат съгласно

процедура, подготвена от Телелинк и одобрена от клиента предварително. По време на тестовите ще се използва само част от оборудването, необходимо за симулиране на реалната мрежова среда. Всяка технология, използвана при дизайна, ще се тества в Лаборатория Телелинк заедно с оторизиран представител на клиента.

Разработване на Детайлен дизайн

Детайлният дизайн включва подробно описание на решението на клиента, включително специфичните компоненти и взаимодействието между тях, за да отговаря на нуждите на клиента за създаване на пълно решение. Преди започване разработването на дизайна клиентът трябва да потвърди всички изисквания и да определи финалните параметри на необходимото решение на среща или по e-mail. Детайлният дизайн се разработва от екип опитни експерти, като се вземат предвид спецификите в бизнеса на клиента, техническите изисквания, информацията, предоставена по време на работните срещи, както и последващи ревизии на дизайна. Детайлният дизайн подлежи на преглед, коментари ако е необходимо и одобрение от клиента преди да се пристъпи към следващите дейности по проекта.

Функционални тестове

Телелинк ще проведе тестове, които да докажат специфични части от функционалностите на дизайна (описани в документа Детайлен дизайн). Функционалните тестове се провеждат съгласно процедура, подготвена от Телелинк и одобрена от клиента предварително. По време на тестовите ще се използва само част от оборудването, необходимо за симулиране на реалната среда. Всяка технология, използвана при дизайна, ще се тества в Лаборатория Телелинк заедно с оторизиран представител на клиента или може да се направи при клиента с пилотна постановка без да засягат текущите услуги.

Тестове за фабрични дефекти

Тестове за фабрични дефекти на цялото необходимо оборудване се извършва преди физическата инсталация по обектите. Клиентът предоставя оборудването за отговорно пазене и временно ползване на Телелинк преди доставката му по обекти. Тестовите за фабрични дефекти се провеждат, за да се потвърди, че хардуера и софтуера функционират коректно и да се гарантира правилното функциониране на комуникационното оборудване след доставката му от производителя, следвайки предварително подготвена процедура. Тестовите се изпълняват в Лаборатория Телелинк и само при нужда и по специфични изисквания от страна на клиента.

Подготовка и предварителна конфигурация на оборудването

Подготовката и предварителната конфигурация на цялото необходимо оборудване се извършва преди физическата инсталация по обектите при нужда. Клиентът предоставя оборудването за отговорно пазене и временно ползване на Телелинк преди доставката му по обекти. Оборудването се конфигурира съгласно Процедура за подготовка и конфигурационните образци произлезли от документа Детайлен дизайн, който трябва да бъде завършен преди тези дейности. Предварителната подготовка и конфигурация се извършва в Лаборатория Телелинк.

Телелинк ще извърши физическа инсталация, окабеляване и свързване на оборудването съгласно приетата дизайн документация, изискванията на производителите и План за имплементация, подготвен предварително от Телелинк. Инсталационните дейности ще започнат само след одобрение на документа Детайлен дизайн на решението и съгласно предварително подготвен двустранно приет график.

- Разопаковане на оборудването;
- Опис на серийните номера и сверяване с документите по доставката;
- Подписване на двустранен Приемо-предавателен протокол за доставката на оборудването;
- Физическа инсталация на комуникационното оборудване в шкафове/кабинети
- Инсталация на захранващи и заземителни кабели на комуникационното оборудване вътре в шкафа/кабинета
- Проверка дали модулните карти са поставени в правилните слотове;
- Окабеляване на комуникационното оборудване;
- Окабеляване между комуникационното оборудване на обекта само в помещението, където ще се инсталира оборудването;
- Поставяне етикети на оборудването и всички кабели;
- Включване на захранването на оборудването;
- Почистване на обекта – изхвърляне на всички опаковъчни материали;

Дейностите по физическата инсталация се извършват, следвайки и потъпвайки Контролен лист от инсталация. Идеята на контролния лист е да осигури по-добро предаване на информацията между отделните екипи, както и цялостен контрол на качеството. В края на тази дейност се правят подробни снимки, които се изпращат за преглед от Техническия Ръководител Проект - отново за постигане на предварително дефинираното ниво на качество.

Оживяването включва конфигуриране и настройки на оборудването според документацията за дизайн на решението.

Приемните изпитания на обектите се провеждат от Телелинк след приключване на физическата инсталация и оживяване на системата, за да се удостовери, че инсталацията е коректна и според стандартите. Тестът се провежда пред упълномощен представител на клиента за всеки обект съгласно Процедурата за приемни изпитания, подготвена предварително от Телелинк и одобрена от клиента. Резултатите от тестовете се записват в Констативен протокол за приемане, подготвен предварително от Телелинк и одобрен от клиента, и се подписва от двете страни след успешно преминаване на тестовете на всеки обект.



Миграция

Телелинк ще изпълни необходимите дейности описани в Миграционната процедура подготвена предварително от Телелинк и одобрена от клиента. Всичките дейности ще бъдат изпълнени според одобрен предварително от двете страни график и след потвърждение, че всички дейности по подготовка за миграция са приключили.

Миграционната процедура включва:

- всички възможни компоненти, които ще се мигрират
- техническо описание на услугите/ системата преди и след миграцията
- миграционна процедура стъпка по стъпка за всяка услуга/ система
- процедура за връщане в първоначално състояние, ако е приложима
- екип за миграцията – неговите роли и отговорности
- времеви график/ интервал за миграцията
- методология за тестване
- дефинирани критерии за успех, приемане и констативен протокол

Приемни изпитания на решението

Приемни изпитания на решението се провеждат след успешна Инсталация и Приемни изпитания на всички обекти / Миграция. Процедура за приемни изпитания на решението се подготвя от Телелинк и одобрява от Клиента предварително. Тестовите се провеждат в присъствието на упълномощени представители на Телелинк и Клиента и покриват всички аспекти и функционалности на интегрираното решение. След успешно преминаване на тестовете се подписва двустранен Констативен протокол за приемане.

Изготвяне на екзекутивна документация

След успешното приключване на Приемни изпитания на обектите / Приемни изпитания на решението / Миграцията Телелинк отговаря за актуализиране на документа Детайлен дизайн и План за имплементация, съгласно реално извършената инсталация по обектите, при необходимост.

Обучение на персонала

Обучението ще се проведе според изискванията на клиента и описаните параметри, план и продължителност, които са описани подробно в отделен документ План за обучение.



ДЕКЛАРАЦИЯ ЗА СРОК ЗА ИЗПЪЛНЕНИЕ

по чл. 8, ал. 3 от проекта на договор за обособена позиция № 1 при участие в открита процедура за възлагане на обществена поръчка по чл. 16, ал. 8 от ЗОП с предмет:

„Доставка и гаранционна поддръжка на компютърно оборудване, компютърни компоненти за него, софтуерни продукти и услуги по инсталиране и конфигуриране”

От: **“ТЕЛЕЛИНК” ЕАД**
(наименование на участника)

1. Предлагаме време за реакция при възникнали дефекти в срока по чл. 8, ал. 1 от проекта на договор и стартиране на процедура за отстраняване им до *1/12 (5 минути)* часа, считано от момента на уведомяването ни.
2. Задължаваме се да спазваме времето за реакция по т.1 за целия срок на договора.

ДАТА: 08.06.2015 г.

ПОДПИС и ПЕЧАТ: ...

ЛЮБОМИР ПЕТРОВ
(име и фамилия)

Търговски директор, Продажби публичен
сектор и пълномощник на
Цветан Димитров Мутафчиев, Изпълнителен
директор на „Телелинк” ЕАД
(длъжност на представляващия участника)

ДЕКЛАРАЦИЯ

за информационна сигурност

Долуподписаният,
(име, ЕГН, за чуждестранните физически лица, други данни за самоличност, постоянен и
настоящ адрес), в качеството ми на (длъжност), в/на.....
(наименование, правноорганизационна форма, ЕИК, седалище на юридическото лице), във
връзка с изпълнението на сключения между
(наименование, правноорганизационна форма) и Българската народна банка (БНБ) Договор
№..... на основание т..... от Корпоративната политика за сигурност на информационните
системи на БНБ

ДЕКЛАРИРАМ, ЧЕ:

1. Запознат/а съм Корпоративната политика за сигурност на информационните системи на БНБ (април 2005г.) и свързаните с нея специфични политики за сигурност и процедури, както следва:

- Процедурата за управление на движението и унищожаването на преносимите информационни носители (януари 2008 г.)
- Процедура за управление на промени в информационните системи на БНБ (май 2010г.)
- Процедура за управление правата на достъп (февруари 2011г)
- Процедура за образуване и ползване на потребителски имена и пароли (октомври 2011г.)

2. Ще спазвам изискванията за сигурност, установени в Политиката за сигурност на информационните системи и свързаните с нея специфични политики за сигурност и процедури.

Известно ми е, че за нарушение на установените изисквания за сигурност на информационните системи и свързаните с нея специфични политики за сигурност и процедури нося наказателна, гражданска или дисциплинарна отговорност в съответствие с българското законодателство.

София,.....2015 г.

Декларатор: