Подход за изграждане на високонадежден информационен център

Росен Радков, Иван Димитров, Петър Антонов

Approach to building high-reliable data center. *This article discusses some of the tasks to solve when building a data center. Attention is paid to the development of communications between elements of data center and reaction to failure of one of them. The main criteria are reliability and minimum time of incapacity The presented approach can be used to build a data center providing business continuity.*

Key words: *data center, disaster recovery, business continuity, virtualization*

ВЪВЕДЕНИЕ

Информационните центрове (data centers – дейта центрове) са ключов елемент от инфраструктурата [1], необходима за осигуряването на информационни услуги. Те придобиват все по-голямо значение не само при реализация на обществено достъпни услуги, а и тогава, когато се разгръща една корпоративна мрежа. Създаването на информационен център е сериозно предизвикателство, свързано с решаването на много задачи, част от които са:

- изграждане на добре изолирано и защитено помещение;
- организиране на контрола на достъп до него;
- осигуряване на система за пожароизвестяване и пожарогасене;
- изграждане на система за климатизация;
- осигуряване на непрекъсваемо електрозахранване;
- подбор и физическо разположение на сървърните шкафове;
- подбор на сървъри;
- избор на софтуерна платформа за виртуализация;
- подбор и изграждане на сторидж (storage) системата;
- изграждане на комуникационната и управляваща мрежа;
- осигуряване на надеждна свързаност към Интернет;

Основна цел е непрекъснатата работоспособност на дейта центъра. Тя трябва да бъде осигурена при отказ на който и да е негов елемент.

Целта на настоящия доклад е да се анализира задачата за изграждане на комуникационна и управляваща мрежа и да се предложи решение за нейната реализация като високонадежден корпоративен информационен център.

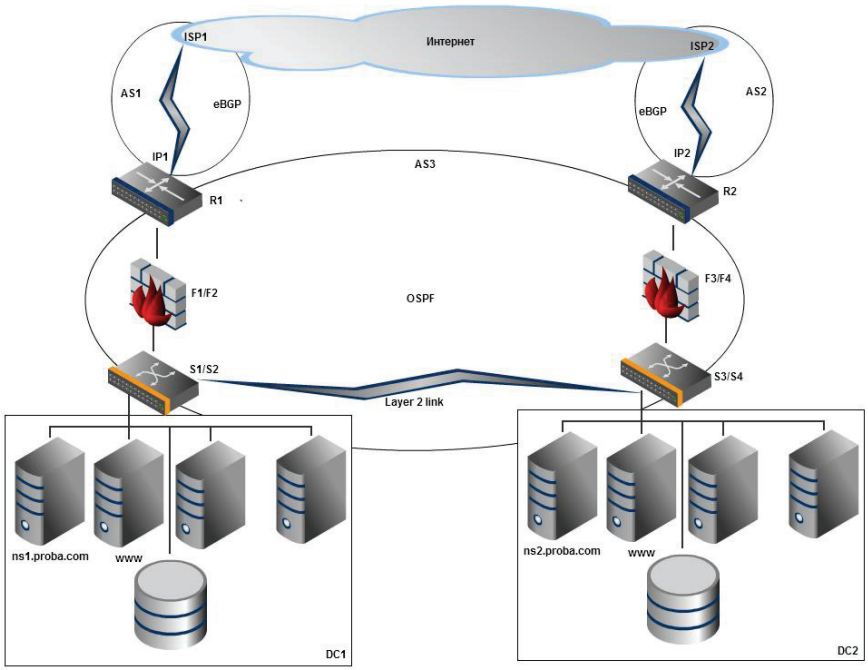
ПОСТАНОВКА НА ЗАДАЧАТА И СХЕМА НА ДЕЙТА ЦЕНТЪРА

Необходимо е изграждането на дейта център, отговарящ на изискването за време на неработоспособност, клонящо към нула. Предлаганата структура на дейта центъра е в състав и топологична свързаност (фиг.1), както следва:

1. Сървърни помещения (възли) – две отделни помещения (DC1 и DC2) на разстояние едно от друго минимум няколко стотици метра.
2. Сървъри – два комплекта, по един във всеки един от възлите.
3. Комутатори – два комплекта за двата възела (S1/S2 и S3/S4), по два комутатора във всеки комплект, конфигурирани в high-availability режим.
4. Защитни стени – два комплекта (F1/F2 и F3/F4), работещи в клъстер, с по две защитни стени, конфигурирани в high-availability режим, инсталирани във всеки един от възлите.
5. Маршрутизатори – по един за всеки възел (R1 и R2).
6. Доставчик на Интернет – два различни (ISP1 и ISP2), несвързани един с друг, за всеки един от възлите.
7. Свързаност на слой 2 от OSI модела между двата възела.

Критериите, следвани при проектирането са:

1. Осигуряване на клонящо към нула време на неработоспособност на комуникационната мрежа в дейта центъра.
2. Балансирано използване на оборудването в дейта центъра.



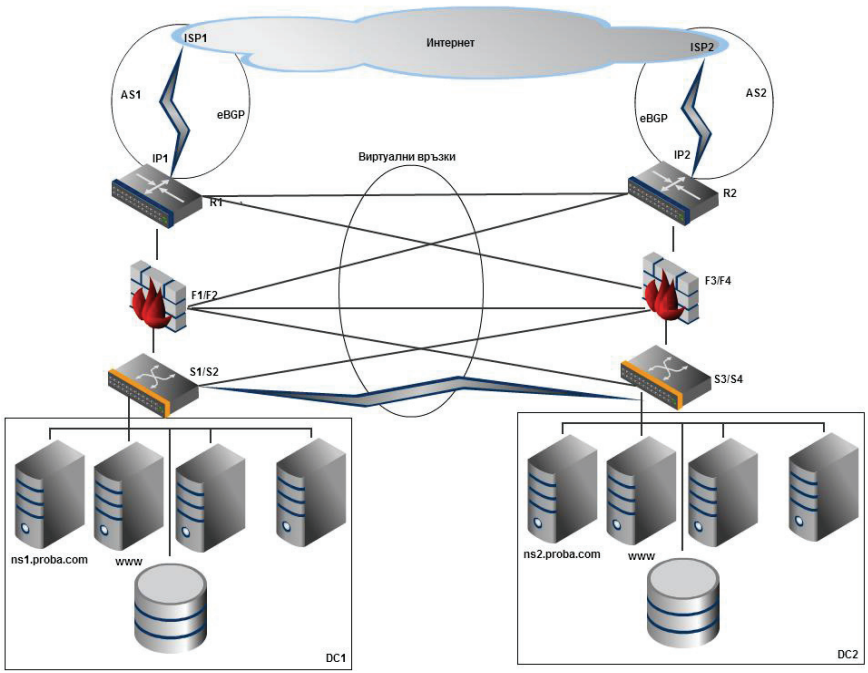
Фиг.1. Топология на дейта центъра

ОПИСАНИЕ НА РАБОТАТА НА СХЕМАТА И АНАЛИЗ НА НАДЕЖДНОСТНИТЕ ХАРАКТЕРИСТИКИ.

Информационните услуги, предоставяни от дейта центъра, се ползват от произволни компютри, намиращи се в Интернет пространството. Регламентирането на достъпа им до информацията в дейта центъра не е предмет на настоящия доклад.

Конфигурирането на схемата включва дефиниране на три автономни системи: AS1 за връзка с първия доставчик на Интернет ISP1, AS2 за връзка с втория доставчик на Интернет ISP2 и AS3, която обхваща устройствата в двата възела. Информационните услуги, предоставяни от центъра ще бъдат достъпни чрез един домейн proba.com. За целта, в описанието на зоната proba.com, се обявява, че два сървъра за имена, ns1.proba.com и ns2.proba.com, отговарят за този домейн. В DC1 се разполага ns1.proba.com, а в DC2 - ns2.proba.com. Адресите, чрез които те са достъпни са съответно IP1 и IP2. Чрез протокол за маршрутизация eBGP [2], маршрутизаторите R1 и R2 обменят информация със своите съседи (маршрутизатори на доставчиците на Интернет). От друга страна R1 и R2 имат помежду си VPN свързаност, което дава възможност взаимно да следят състоянието си. Чрез свързването на защитните стени F1/F2 и F3/F4, две по две в high availability режим и двата комплекта в клъстер, четирите устройства функционират като една единствена защитна стена с уникална ARP таблица и филтриращи правила. Клъстер

технологиите дават възможност да се постигне минимално време за корегиране на пътищата при дефектиране на устройство. Аналогично е свързването на комутаторите S1/S2 и S3/S4. Устройствата, включени в AS3, комуникират помежду си с OSPF протокол [3], като комуникацията е от тип „всеки с всеки“ (full mesh). При така проектираната и конфигурирана схема, на базата на физическите връзки, представени на фиг. 1, се получава логическо свързване на устройствата, представено на фиг. 2. Идеята, която е вложена, при създаването на виртуалните връзки се състои в „заобикаляне“ на дефектиралия елемент от схемата и минимални промени в режима на работа на устройствата. В DC1 и DC2 се разполагат два еднакви комплекта сървърно оборудване. Върху физическите сървъри, използвайки виртуализация, се създават необходимия брой виртуални машини, които предоставят информационните услуги. С цел балансиране на натоварването на хардуера, една част от машините, които предоставят услуги, са активни в DC1, а другата част - в DC2 (например: www и mail сървърите са в DC1, а сървърът за приложенията и терминалния сървър - в DC2). За да се използват пълноценно и двата Интернет доставчика, част от услугите (www, SMTP и IMAP) се ползват през IP1, а останалите - през IP2. Изчислителната мощност на хардуера във всеки един комплект трябва да бъде оразмерена, така че да поема цялото натоварване при необходимост.



Фиг. 2. Схема на логическите връзки между устройствата

За описание на процеса на работа на представения дейта център, по-долу в качеството на пример е взета реализацията на www услугата.

Нека сайтът **www.proba.com** да е хостван на сървър www, работещ в DC1, означен като DC1www. Сървърите за имена са конфигурирани така, че в ns1.proba.com е описано, че **www.proba.com** е достъпен през IP1, а в ns2.proba.com,

че е достъпен през IP2. При генериране на обръщение от произволен компютър в Интернет към **www.proba.com**, в нормален режим на работа комуникационният път към www сървъра е R1-F1-S1-DC1www.

При дефектиране на някои основни елементи от схемата, комуникационните пътища ще бъдат както следва:

1. Отпадане на линка към ISP1 или дефект на маршрутизатор R1.
При опит за достъп до **www.proba.com**, отговор на DNS запитването „Кой е IP адреса на **www.proba.com**?" ще бъде даден от ns2.proba.com, тъй като ns1.proba.com не е достъпен. Следователно за компютъра, който е отправил запитването, IP адресът на **www.proba.com** е IP2. Комуникацията се извършва по IP2-F1-S1-DC1www.

2. Дефектиране на защитна стена F1.
Тъй като F1 и F2 са конфигурирани в high-availability режим при отпадане на една от двете защитни стени, работата не се нарушава. Комуникацията се извършва по пътя IP1-F2-S1-DC1www.

3. Дефектиране на двойката защитни стени F1/F2.
Комуникацията ще се осъществи по веригата IP1-F3-S1-DC1www.

4. Дефектиране на комутатор S1.
Комутаторите S1 и S2 са конфигурирани в high-availability режим и при отпадане на единия от двата, работата няма да се наруши. Комуникацията се извършва по IP1-F1-S2-DC1www.

5. Дефектиране на двойката комутатори S1/S2 или DC1www.
В този случай, хостът, който управлява виртуализацията, ще стартира виртуалната машина DCwww. Комуникацията ще се реализира по маршрута IP1-F1-S3-DC2www.

ЗАКЛЮЧЕНИЕ

Представеният подход за изграждане на надежден дейта център е приложим при всеки един случай, където се изисква много висока надеждност и клонящо към нула време за неработоспособност. Конкретните параметри са в зависимост от настройките на устройствата. Направените от нас експерименти показват резултати, които удовлетворяват поставените цели.

ЛИТЕРАТУРА

[1] Kant, K. Data center evolution. //Computer Networks, 2009, 53, pp. 2939 - 2965.

[2] Rekhter, Y., T. Li, S. Hares. RFC 4271. A Border Gateway Protocol 4 (BGP 4). IETF 2006.

[3] Coltun, R., D. Ferguson, J. Moy, A. Lindem. RFC 4271 OSPF for Ipv6. IETF 2008.

За контакти:

гл. ас инж. Росен Радков, катедра "Компютърни науки и технологии", Технически университет - Варна, тел.: 052 383 403, e-mail: rossen@actbg.bg.

инж. Иван Димитров, IT мениджър, тел.: 0889 257137, e-mail: ivan@dimitrov.ws.

доц. д-р инж. Петър Антонов, катедра "Компютърни науки и технологии", Технически университет - Варна, тел.: 052 383 320, e-mail: peter.antonov@ieee.org.

Докладът е рецензиран.