

A.K. TUMANYAN, A.H. HAMAZASPYAN, A.H. KOSTANYAN
IMPLEMENTATION OF MULTIPLICATION AND DIVISION
OPERATIONS IN THE RESIDUE NUMBER SYSTEM

A structure and an algorithm of modular multiplication based on correction of the sum of partial products and multiplicand in each cycle of multiplication are proposed. The algorithm of transition from the representation of the number in the RNS in the positional system and the division operation with the remainder scheme are also developed.

Keywords: modular multiplication, residue number system, modular division, Chinese remainder theorem.

ՀՏԴ 004.451.3

Լ.Գ. ԿԻՐԱԿՈՍՅԱՆ

ՏՎՅԱԼՆԵՐԻ ՕՔՅԵԿՏԱՅԻՆ ՊԱՀՊԱՆՄԱՆ ՀԱՄԱԿԱՐԳԵՐԻ
ՌԻՍՈՒՄՆԱՍԻՐՈՒԹՅՈՒՆ ԵՎ ԸՆՏՐՈՒԹՅՈՒՆ

Տվյալների կառավարումն առաջնային դեր ունի ամպի շահագործման ժամանակ: Հիշողությունը պետք է ոչ միայն լինի հուսալի և անվտանգ, այլև ունենա ընդլայնման հնարավորություն՝ չխաթարելով նախնական կառուցվածքը: Մեծածավալ տվյալների պահեստավորման, գրանցման/ընթերցման համակարգը պետք է հնարավորություն ունենա իր առջև դրված գործողություններն իրագործել արագ և առանց ընդհատումների: Վերլուծված են տվյալների պահպանման համակարգերը՝ Հայաստանի ազգային պոլիտեխնիկական համալսարանում ստեղծվող ամպային համակարգում կիրառելու տեսանկյունից:

Առանցքային բառեր. տվյալներ, տվյալների ընդլայնում, կառավարում, ceph, glusterfs, ֆայլային համակարգ:

Տվյալների օբյեկտային պահպանման համակարգեր: Տվյալների պահպանման ավանդական լուծումները չեն կարող ապահովել անհրաժեշտ հուսալիություն՝ ու անվտանգություն դրանք կիրառող համակարգերի թե՛ ծավալային, թե՛ սկզբունքային առանձնահատկություններից ելնելով: Տվյալների օբյեկտային պահպանման համակարգերն արդեն ծանոթ ֆայլային համակարգերից տարբերվում են նրանով, որ տվյալները պահպանում են որպես օբյեկտներ [1], ի տարբերություն ֆայլային համակարգերի, որտեղ այն գրանցվում է բլոկների մեջ [2]: Յուրաքանչյուր օբյեկտ պարունակում է տվյալ և նույնականացնող հատուկ համար: Տվյալների օբյեկտային պահպանման համակարգը կարող է կիրառվել մի շարք մակարդակներում, ինչպիսիք են, օրինակ՝ համակարգային կամ ինտերֆեյսային մակարդակները: Յուրաքանչյուր դեպքում համակարգի նպատակն է տրամադրել նոր միջոցներ, որոնք ֆայլային համակարգերն ընդունակ չեն տրա-

մադրելու: Դրանք կարող են լինել, օրինակ, ծրագրերով ուղիղ ծրագրավորվող ինտերֆեյսներ և այլն: Տվյալների օբյեկտային պահպանման համակարգերը լայն տարածում ունեն չկարգավորված տվյալների պահպանման համար: Դրանք լայնորեն կիրառվում են մեծ տվյալներ պահպանող ընկերությունների կողմից, ինչպիսիք են, օրինակ Facebook-ը, Dropbox-ը և այլն [3]: Տվյալների օբյեկտային պահպանման համակարգի ճարտարապետության հիմքում ընկած է ծրագրերով ցածր մակարդակների փակումը՝ այդպիսով տվյալները ցույց տալով որպես օբյեկտներ, ոչ թե բլոկներ: Համակարգի մեկ այլ կարևոր հատկանիշ է ինդեքսավորումը, երբ յուրաքանչյուր օբյեկտ պարունակում է իրեն յուրահատուկ կցված համարը, որը մեծ դեր ունի տվյալների գրանցման/ընթերցման արագության վրա: Համակարգը նաև առանձնացնում է տվյալները և դրանց մետատվյալները (անունը, ստեղծման ամսաթիվը, տիպը և այլն)՝ ապահովելով հետևյալ հնարավորությունները՝

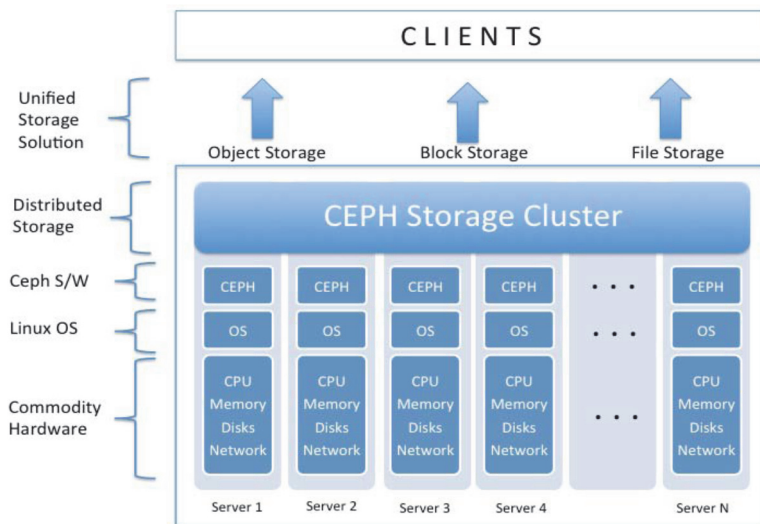
- ծրագրին կամ օգտատիրոջն անհրաժեշտ տվյալների կորզում բարելավված ինդեքսավորման համար,
- տվյալների կառավարման կանոնների ապահովում,
- նոդերի և տարբեր տվյալների պահպանման սերվերների կենտրոնացված կառավարում,
- մետատվյալների պահպանման օպտիմալացում:

Ինչպես նախապես նշվել է, տվյալների օբյեկտային պահպանման համակարգը ընձեռում է ծրագրավորման ինտերֆեյսների հնարավորություն, որոնց շնորհիվ ավելի ճկուն են դառնում տվյալների կառավարումն ու պահեստավորումը:

Տվյալների օբյեկտային պահպանման համակարգերը մեծ դեր ունեն ամպային տեխնոլոգիաների շահագործման մեջ: Հաշվի առնելով, որ ամպի հիմնական բաղադրիչը տվյալների ապահով պահպանումն է, պարզ է դառնում, որ ավանդական լուծումները չեն կարող տալ պահանջվող արդյունքը: Հայաստանի ազգային պոլիտեխնիկական համալսարանում մինչ ամպի կառուցումն ու շահագործումը, կատարվել է համեմատություն երկու տվյալների օբյեկտային պահպանման համակարգերի միջև՝ առկա խնդրի համար լավագույնն ընտրելու նպատակով: Վերոհիշյալ համակարգերն են՝ բաց ծրագրային կոդերով Ceph [4] և GlusterFS [5] համակարգերը: Ներկայացնենք դրանց հիմնական առանձնահատկությունները:

Ceph տվյալների օբյեկտային պահպանման համակարգ: Համակարգի հիմքում օբյեկտային պահպանման սկզբունքն է, որը կոչվում է Rados: Որպես օբյեկտային պահպանման համակարգ՝ Ceph-ը, տվյալները պահպանում է բինարային օբյեկտների տեսքով՝ անհրաժեշտության դեպքում դրանք ավելի փոք-

րացնելու հնարավորությամբ: Սովորական տվյալների պահպանման սարքերի խնդիրն այն է, որ երբ տվյալները գրանցվում են բլոկների մեջ, ապա այդ տվյալներն առաջիկայում ընթերցելու համար անհրաժեշտ է լինում ընթերցումը սկսել կոշտ սկավառակի առաջին իսկ բլոկից և այդ տվյալը գտնելուց հետո միայն ընթերցել այն: Այս գործընթացը բավականին երկար ժամանակ է խլում, ի տարբերություն օբյեկտային պահպանման եղանակի: Ceph-ը խուսափում է այս խնդրից՝ ավելացնելով մի մակարդակ, որը կառավարում է բլոկները: Այս մակարդակը կոչվում է RADOS: Այն բաղկացած է երկու մասից, որոնցից առաջինը Object Store Device (OSD)-ն է: Վերջինիս սկզբունքն այն է, որ յուրաքանչյուր սկավառակ պատկանում է տվյալների համակարգի կլաստերին (նկ. 1):



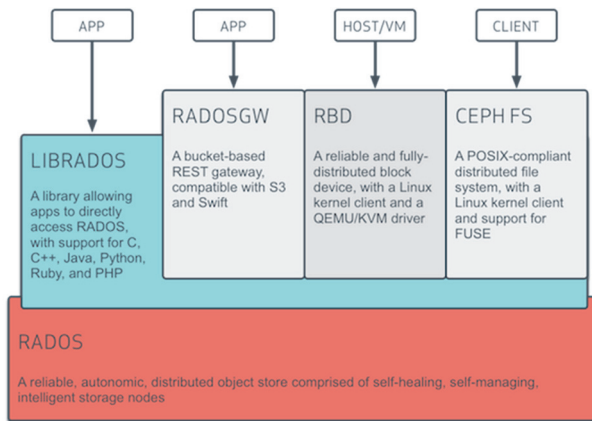
Նկ. 1. Ceph-ի կլաստերային համակարգը [6]

Երբ օգտատերն ընթերցում կամ գրանցում է որևէ տվյալ, ամբողջ գործառույթն իրականացվում է այս մասի միջոցով: Երկրորդ մասը մոնիթորինգի համակարգն է, որը կառավարում է OSD-ները: Գաղափարը շատ պարզ է. նշանակություն չունի, թե քանի սերվեր կամ կոշտ սկավառակ է կիրառվում տվյալների պահպանման համար: Օգտատերը տեսնում է միայն դրա ինտերֆեյսը, որը միշտ նույնն է:

Բացի կենտրոնացված սերվեր ունենալու անհրաժեշտությունից, անհրաժեշտ է, որ Ceph կլիենտները տեղադրված լինեն հիպերվայզերների վրա, որպեսզի այն կարողանա գրանցել/ընթերցել ցանցային տվյալների պահպանման համակարգից: Հիպերվայզերի վրա տվյալներ գրանցել/ընթերցելու ժամանակ Ceph-ի կենտրոնական սերվերը դիմում է վերոհիշյալի վրա տեղադրված իր

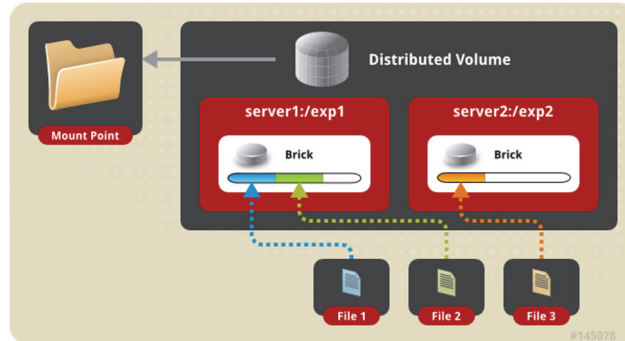
կլիենտին, հաստատում կապ, որից հետո միայն կատարում անհրաժեշտ փոփոխությունները: Համակարգում բոլոր փոփոխությունները կատարվում են front-end-ում՝ առանց ֆիզիկական մասերի հետ աշխատելու կարիքի:

Այսպիսով, համակարգի ծրագրային կառավարման հիմքն ապահովում է մեծ ճկունություն տեղադրողների համար: Ի տարբերություն այլ համակարգերի՝ Ceph-ը կախված չէ ֆիզիկական սարքավորումներից և կարող է տեղադրվել ցանկացած տիպի կոշտ սկավառակ ունեցող համակարգչի վրա (նկ. 2): Համակարգը տրամադրում է կենտրոնացված կառավարման սերվեր, որը ևս բավականին հեշտացնում է դրա հետագա շահագործումը [7]:



Նկ.2. Ceph-ի ճարտարապետությունը [8]

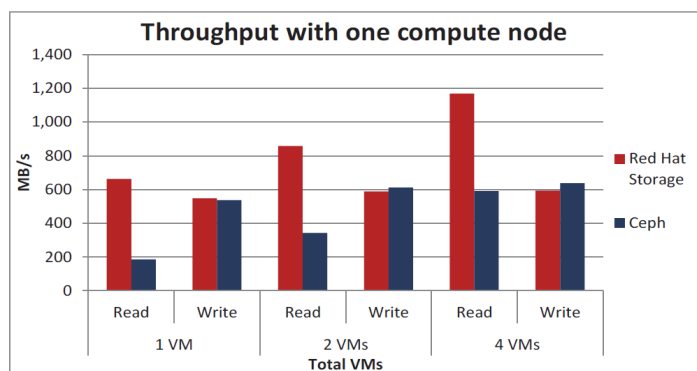
GlusterFS տվյալների օբյեկտային պահպանման համակարգ (նկ. 3): Ինչպես Ceph-ը, GlusterFS-ը նույնպես բաց ծրագրային կողով համակարգ է: Համակարգը նման է NAS-ին (Network Attached Storage՝ ներկայացնում է ցանցով հասանելի տվյալների պահպանման գրադարան) նրանով, որ կապում է ցանցում գտնվող տվյալների պահպանման սերվերները մեկը մյուսին՝ ստեղծելով տվյալների պահպանման մեկ ընդհանուր համակարգ, որտեղ յուրաքանչյուր սերվեր հանդիսանում է իր volume-ներից մեկը: Համակարգը ևս ունի կլիենտներ, որոնք տեղադրվում են առանձին տվյալների պահպանման սերվերների վրա, իսկ կենտրոնացված կառավարման սերվերն ապահովում է կլիենտների կարգավորումները և դրանց ընդհանրացված, ամբողջական աշխատանքը: GlusterFS-ի աշխատանքի սկզբունքն ընկած է ֆայլային mirroring-ի, stripping-ի և replication-ի վրա: Համակարգն ունի նաև հզոր load balancing-ի բաղադրիչ, որը կարգավորում է համակարգում ծանրաբեռնվածությունները:



Նկ. 3. GlusterFS-ի ճարտարապետությունը [9]

Համակարգի հիմնական գործառնություններն իրականացնում են, այսպես կոչված, «թարգմանիչները», որոնք տեղակայված են կլիենտների վրա, որոնք կառավարում են սերվերի վրա տեղադրված տվյալները: Համակարգը, ի տարբերություն Ceph-ի, որը կիրառում է մետատվյալներ տվյալների պահպանման ժամանակ, աշխատում է հեշինգի ալգորիթմի հիման վրա:

Ceph-ի և GlusterFS-ի համեմատական վերլուծությունը: Կարևոր է պարզել, թե երկու համակարգերից որն է ապահովում ավելի մեծ թողունակություն: Թեստավորումների ժամանակ պարզ է դառնում, որ երկու համակարգերն էլ ունեն իրենց առավելություններն ու թերությունները, և կախված առկա խնդրից՝ պետք է որոշել, թե որն է առավել նպատակահարմար կիրառել: Մեկ սերվերով աշխատելիս GlusterFS-ը ցուցաբերում է ավելի բարձր թողունակություն գրանցել/ընթերցելու ժամանակ, սակայն Ceph-ի թողունակության ցուցանիշներն ավելի բարձր են, երբ համակարգերը թեստավորվում են 4-ից ավելի վիրտուալ մեքենաների շահագործելիս (նկ. 4):



Նկ. 4. Համակարգերի ընթերցելու/գրանցելու համեմատական արդյունքները [10]

Եզրակացություն: Տվյալների օբյեկտային պահպանման համակարգերը հսկայական դեր ունեն ամպային տեխնոլոգիաների զարգացման բնագավառում, քանի որ ապահովում են տվյալների պահպանման ճկունություն՝ առանց ֆիզիկական սարքերից կախվածության մեջ լինելու: Ուսումնասիրված երկու տվյալների օբյեկտային պահպանման համակարգն էլ ունեն իրենց առավելությունները, սակայն վերը նշված թեստավորման արդյունքներից ելնելով և հաշվի առնելով, որ Հայաստանի ազգային պոլիտեխնիկական համալսարանում կառուցվող ամպը շահագործվելու է 4-ից ավելի վիրտուալ մեքենաների կիրառմամբ, որպես տվյալների պահպանման համակարգ ընտրվել է Ceph ծրագրային բաց կոդով տվյալների օբյեկտային պահպանման համակարգը:

ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

1. **Mesnier, Mike; Gregory R. Ganger; Erik Riedel** Object-Based Storage (PDF)
// IEEE Communications Magazine. - August, 2003. – P. 54-90.
2. **Porter De Leon, Yadin; Tony Piscopo.** Object Storage versus Block Storage: Understanding the Technology Differences. - Druva. August, 2014.
3. **Chandrasekaran, Arun, Dayley, Alan** Critical Capabilities for Object Storage: Gartner Research. - 11 February, 2014.
4. <http://ceph.com/>
5. <https://www.gluster.org/>
6. Learning Ceph, Karan Singh, Page 11
7. Learning Ceph, Karan Singh, Page 23
8. <http://docs.ceph.com/docs/hammer/architecture/>
9. <http://gluster.readthedocs.io/en/latest/Quick-Start-Guide/Architecture/>
10. http://www.principledtechnologies.com/Red%20Hat/RedHatStorage_Ceph_1113.pdf,
Page 5

Л.Г. КИРАКОСЯН

ИССЛЕДОВАНИЕ И ВЫБОР ОБЪЕКТНЫХ СИСТЕМ ХРАНЕНИЯ ДАННЫХ

Управление данными имеет приоритетную роль при использовании облака. Хранение данных должно быть не только надежным и безопасным, но и иметь возможность масштабирования, не искажая исходную архитектуру. Система хранения, чтения/записи больших данных должна иметь возможность выполнения задач быстро и без прерываний. В данной работе проанализированы системы хранения данных с точки зрения их использования в облачной системе Национального политехнического университета Армении.

Ключевые слова: данные, расширение данных, управление, ceph, glusterfs, файловая система.

L.G. KIRAKOSYAN

RESEARCH AND SELECTION OF OBJECT STORAGE SYSTEMS

Data management is the highest priority when distributing a cloud system. Storage should not only be reliable and secure, but also have the ability of scaling, while not causing problems with already established architecture. Big data storage, read/writing systems should be able to provide all the necessary tasks at high speeds without any interruptions. The document provides an analysis of storage systems for implementation in National Polytechnic University of Armenia cloud system.

Keywords: data, data scaling, management, ceph, glusterfs, file system.

ՀՏԴ 004.22:004.421

Բ.Գ. ԱԹԱՅԱՆ

ՏՎՅԱԼՆԵՐԻ ԱՄՊԱՅԻՆ ՊԱՀՈՒՍՏԱՎՈՐՄԱՆ ՀԱՄԱԿԱՐԳՈՒՄ ՏԱՐԲԵՐԱԿՆԵՐԻ ԵՐԱՇԽԱՎՈՐՎԱԾ ՀԵՌԱՅՈՒՄԸ

Ներկայացվում է տվյալների պահուստավորման ամպային պաշտպանված համակարգ, որը գործում է որպես անվտանգության լրացուցիչ մակարդակ այսօրվա ամպային ծառայությունների օգտագործման պայմաններում: Տվյալների պահուստավորման ամպային համակարգում իրագործված է դրանց բազմակի պահուստավորման գործընացի լավարկման արդյունավետ վերապահուստավորման ալգորիթ, որի օգտագործման շնորհիվ բացառվում է տվյալների պահուստների մի քանի տարբերակների ստեղծման արդյունքում առաջացած ավելցուկային տվյալների պահուստը համակարգում: Համակարգը ապահովում է նաև տվյալների պահուստների գաղտնագրային պաշտպանություն, մասնավորապես, պահուստների տարբեր տարբերակներում ընդգրկված տվյալների անվտանգ հեռացումը: Համակարգը հնարավորություն է տալիս օգտագործողներին հեռացնել պահուստների որոշակի տարբերակները և դարձնել դրանք անվերականգնելի, իսկ պահուստների այն տարբերակները, որոնք պարունակում էին ընդհանուր մասեր հեռացված տարբերակի հետ, կմնան հասանելի:

Առանցքային բաներ. ամպային պահուստավորում, երաշխավորված հեռացում, վերապահուստավորում, տարբերակների վերահսկում, բազմաշերտ գաղտնագրում:

Ամպային տեխնոլոգիաների զարգացման շնորհիվ ներկայումս այդ ոլորտում գործող ամպային ծառայությունները տրամադրում են հարմարավետ գործիքներ ֆիզիկական անձանց և կազմակերպություններին, ծախսելով քիչ գումարներ, պահպանել իրենց տվյալների պահուստային օրինակները ամպում: Սակայն ամպային ծառայության օգտագործողները պետք է ունենան ամպում պահվող տվյալների անվտանգության երաշխիքներ: Ամպում պահպանվող տվյալների անվտանգության ապահովման կարևորագույն խնդիր է երաշխավորված հեռա-