ӘОК 004.056

ВИРТУАЛИЗАЦИЯ ҚҰРАЛДАРЫНА ЖҮРГІЗІЛЕТІН ШАБУЫЛДАРДАН БҰЛТТЫ ЕСЕПТЕУЛЕРДІ ҚОРҒАУ ӘДІСТЕРІ

Қали Айтханым
k.aithanym@mail.ru
Л.Н.Гумилев атындағы Еуразия ұлттық университеті, «Ақпараттық қауіпсіздік» кафедрасының
1 курс магистранты, Нұр-Сұлтан, Қазақстан
Ғылыми жетекшісі – Қоңырханова Ә.Ә.

Аңдатпа: Бұлтты есептеу қызметтері қазіргі таңда жақсы дамып, ақпараттық технологиялар саласына жақсы әсерін тигізіп жатыр. Дегенмен, бұлтты есептеулердегі қауіпсіздік мәселелері де барған сайын маңызды бола бастады, сонымен бірге бұлттық есептеулердің қауіпсіздігі маңызды факторлардың бірі болып саналады. Виртуализация технологиясы бұлтты есептеулердің негізгі технологияларының бірі болып табылады, сондықтан виртуалдандыру қауіпсіздігі де негізгі мәселе болып табылады. Бұл мақала виртуалдандырудың негізгі технологиясын таныстырады, бұлттық есептеулердегі виртуалдандырудың қауіпсіздік қауіптерін қарастырады және оларға қарсы шараларды ұсынады.

Кілттік сөздер: Виртуализация, қауіптер, шабуылдар, гипервизор, бұлтты есептеу,қорғау,осалдықтар.

Кіріспе

Бұлтты есептеу-қазіргі таңда өте қажетті IT саласының бір бөлігі болып саналады. Себебі, бұлтты есептеу технологиялары ірі және де ұсақ компанияларға деректерді, электрондық пошталарды және де басқа қосымшаларды виртуалды платформалар арқылы байланыстыра алады, және де кез-келген уақытта, кез-келген жерді қолжетімді болып саналады.Ең басты талабы – интернет жағдайы болса болғаны. Жалпы айтқанда, бұлтты есептеу тек қана компанияларға ғана пайдасын тигізіп қоймай, сонымен қатар IT бөліміне үлкен өзгеріс алып келді.

Бұлтты есептеуді әртүрлі мақсатта қолдануға болады. Бұлтты деректердің сақтық көшірмесін жасау, апаттарды қалпына келтіру, программалық жасақтаманы әзірлеу және тестілеу, үлкен деректерді талдау, бейнені электронды бейнелеу, виртуалды жұмыс үстелдері және тұтынушыларға бағытталған Интернет қосымшаларын қоса алғанда, әртүрлі мақсаттарда пайдалануға болады. Мысалы, денсаулық сақтау компаниялары бұлтты пациенттерді емдеу жоспарларын жекелендіру үшін пайдаланады. Ал, қаржы саласындағы компаниялар бұлтты алаяқтықты анықтау және алдын алу жүйелерінің негізі ретінде пайдаланады.

Негізгі бөлім. Виртуализация технологиясы

Кез келген бұлттық жүйе бірнеше типтік құрамдас бөліктерден тұрады, олардың арасында бұлтта жұмыс істейтін көптеген виртуалды машиналар (VM) жұмысын басқаратын және қолдайтын виртуализация құралдары ерекше орын алады. Виртуалды машина концепциясының көмегімен бұлт жүйедегі қолда бар аппараттық ресурстарды тиімді пайдалана отырып, көптеген пайдаланушылар үшін үзіліссіз және үнемді жұмысты қамтамасыз етеді.

Бұлтты орталар үшін негізгі технология виртуализация болып табылады. Ол жұмыс істеп тұрған қолданбаларды бір серверден екіншісіне көшіруге мүмкіндік беретін және бүкіл қолданбаның жұмысын тоқтатпай, бұлттарды сипаттайтын еркіндікті жасайды. Бұлтты жүйе әдетте бірнеше түйіндерден тұрады, олардың әрқайсысы әртүрлі деректер орталықтарында, соның ішінде басқа провайдерлердің орталықтарында орналасуы мүмкін. Бұлттық қызмет провайдерлерінің өздерінің деректер орталықтары (DPC) болмауы мүмкін, бірақ бірнеше желілік инфрақұрылым провайдерлерінен серверлерді немесе тіректерді жалға алады. Нәтижесінде нақты инфрақұрылымның элементтері өте әртүрлі болуы мүмкін. Бұлттық қызметтерді ұсынатын провайдердің желілік инфрақұрылымының екі элементі де, виртуализация ортасының өзі де шабуылға ұшырауы мүмкін.

Бұлттық есептеулердегі виртуализацияға қатысты қауіпсіздік қатерлері. Осы уақытқа дейін ірі бұлттық сервистерге шабуыл жасалған болатын. Мысалға келтіретін болсақ, 2009-жылдың желтоқсанында белгісіз шабуылдаушылар Amazon Elastic Compute Cloud қоғамдық бұлттық қызметіне, сондай-ақ оны басқару үшін жабық консольге рұқсатсыз кіру мүмкіндігіне ие болды. Шабуылшылар бастапқыда Amazon сервисінің өзін емес, оның нысандарында орналасқан сайттардың бірін бұзды және бұзылған сайт арқылы олар Amazon сервисінің өзіне қол жеткізді. Бұзылғаннан кейін операциялық жүйенің виртуалды данасы жасалды, онда ботнеттерді құруға және басқаруға арналған Zeus бағдарламалық құралы орналастырылды. Ал 2013-жылдың сәуірінде Associated Press-тің Twitter аккаунты бұзылып, нәтижесінде АҚШ-тың Ақ үйіне жасалған шабуыл туралы жалған ақпарат тарады.

Бұлттық есептеулердегі виртуализацияға қатысты қауіпсіздік қатерлерінің негізгі түрлеріне тоқталайық:

-Виртуалдық машинаны миграциялау.

Виртуалды машинаны миграциялау виртуалды машинаны өшірмей, виртуалды машинаны басқа физикалық машинаға жіберу арқылы жүзеге асырылады. Ақаулыққа төзімділікті сақтау немесе жүктемені теңдестіру үшін миграциялау орындалады. Миграциялау кезінде виртуалды машина желіге әсер етеді, бұл деректердің құпиялылығын жоғалтуға әкелуі мүмкін.

-Виртуалды машинадан шығу

Виртуалды машиналардың көмегімен пайдаланушылар хост ресурстарын бөлісе алады және өзара оқшаулауға қол жеткізе алады. Ең дұрысы, виртуалды машинада жұмыс істейтін бағдарлама басқа виртуалды машиналарға әсер етпеуі керек. Алайда, техникалық шектеулерге және виртуализация бағдарламалық жасақтамасындағы кейбір кемшіліктерге байланысты, кейбір жағдайларда виртуалды машинаның жергілікті желісінде жұмыс істейтін бағдарламалар оқшаулау шектеулерін айналып өтіп, virtual machine escape деп аталатын хост машинасында тікелей іске қосылады. Виртуалды машинаға шабуыл сәтті болған кезде, бұл гипервизор үшін де, хост үшін де үлкен қауіп төндіреді.

- *Қызмет көрсетуден бас тарту шабуылы*

Виртуалды машиналардарғы ақпарат барлық физикалық машиналарда бірдей қолданылады. Егер шабуылдаушы хост-машинаның барлық ресурстарын алу үшін бір виртуалды машинаны қолданса, басқа виртуалды машиналардың ресурстары да бұзылады немесе тіпті қол жетімді ресурстардың жоқтығынан сәтсіздікке ұшырайды, бұл виртуалды ортада қызмет көрсетуден бас тартуға әкеледі.

-Виртуалды машина мониторының мәселесі

Виртуалды машина мониторы виртуализацияның негізгі модулі болып табылады. Виртуалды машина мониторы виртуалды машиналарды басқаруға да, оқшаулауға да, виртуалды ресурстарды құруға немесе басқаруға да жауап береді. Егер VM мониторы бұзылса, шабуылдаушы барлық VM IT менеджерлерін басқарады, ал VM мониторы арқылы VM метадеректерін сақтау шабуылдаушыға қол жетімді болады.

-Виртуализация платформаларына шабуылдарды болдырмау

Дәстүрлі жұмыс ортасында бір осалдық тек жүйелік осалдығы бар физикалық машинаға шабуыл жасай алады, ал шабуыл аймағы өте тар және шектеулі екенің білеміз. Бұлтты есептеу виртуализация платформасына негізделген бірнеше жалдауға алған пайдаланушылар бүкіл жүйе туралы ақпарат алмасып, содан кейін бір виртуалды машинаның көмегімен бүкіл виртуалды осалдық платформасына шабуыл жасай алады.

Жоғарыда айтылып өткен қауіп қатерлерге қарсы төмендегідей шаралар жүргізуге болады:

-Гипервизорды қорғауға арналған қауіпсіздік. Қазіргі уақытта Xen, VMware және KVM сияқты виртуализацияның негізгі бағдарламалық жасақтамалары бар, олар гипервизордың тұтастығы мен қорғанысын бұзуы мүмкін, гипервизордың қауіпсіздігі виртуализация платформасының қауіпсіздігі үшін өте маңызды. Қазіргі уақытта гипервизордың қауіпсіздігін арттырудың үш негізгі аспектісі бар, біріншісі-жеңілдетілген

гипервизор құру, екіншісі - сенімді есептеу технологиялары негізінде гипервизордың тұтастығын қорғау, үшінші әдіс - виртуалды брандмауэрді орнату және хост ресурстарын ұтымды бөлу арқылы гипервизордың қорғаныс қабілетін арттыру.

-Виртуалды машинаның қауіпсіздігін оқшаулау

Виртуалды машиналардың оқшау орналастырылған қорғаныс механизмінің арқасында тұтынушулардың виртуалды машиналары өздігінен жұмыс істейді және бір-біріне кедергі жасамайды. Ол негізінен екі аспект бойынша жүзеге асырылады: біріншіден, SM қауіпсіздік жадын басқару моделі SMM контроллері арқылы жадты шифрлау үшін қолданылады, екіншіден, SON қауіпсіздік енгізу-шығару басқару моделі Dom0 forse-ді босату үшін қолданылады.

-Virtual machine access control (Виртуалды машинаға кіруді бақылау)

Skype, Chinese wall және BLP сияқты қауіпсіздік модельдері виртуалды машина жүйесіндегі жасырын ақпарат ағымының қаупін азайту үшін, сондай-ақ жүйенің қауіпсіздігін арттыру үшін виртуалды машина ішіндегі ресурстарды пайдалану мен оқиғалардың әрекетін бақылау үшін қолданылады.

-Виртуалды машинаның қауіпсіздігін бақылау

Әрбір виртуалды машинаның үздіксіз жұмыс істеуін қамтамасыз ету үшін виртуалды машиналардың қауіпсіздігін бақылау қажет.Виртуалды машиналардың қауіпсіздігін бақылаудың екі негізгі архитектурасы бар: бақылау модулін гипервизорға орналастыратын және басқа виртуалды машиналарды VM интроспекция технологиясымен анықтайтын VM интроспекция технологиясына негізделген бақылау архитектурасы, екіншісі - виртуализацияға негізделген белсенді қауіпсіздікті бақылау архитектурасы, ол жүйенің күйін өзгертуге кедергі келтіреді, бақыланатын қондырғыға қосылудың кейбір функцияларын енгізеді.

Қорытынды

Виртуализация технологиясының жетілгендігі мен кең қолданылуы бұлтты есептеулерді түрлендіруге және дамытуға ықпал етті. Виртуализация технологиясы бұлтты есептеулерді дамытудың негізгі факторы болып табылады деп айтуға болады. Дегенмен, виртуализация технологиясының көптеген қауіпсіздік қаупі бар. Бұлтты есептеулердегі виртуалдандыру технологиясының қауіпсіздік мәселесі де бұлтты есептеулердің дамуын шектейтін маңызды мәселе болып табылады. Сондықтан, виртуализация технологиясына төнетін қауіптер-қатерлерді зерттеу және оларды талдау арқылы қорғауды күшейту өте маңызды болып саналады.

Қолданылған әдебиеттер тізімі

1.Junaid S, Kashif B. Data Center Energy Efficent Resource Scheduling. Cluster Computing,2014,17, pp. 1265–1277.

2.Игнатович Р.О., Савицкая Д.Г., Мигалевич С.А., Марков А.Н.Внедрение облачных решений в образовательный процесс / Игнатович Р.О., Савицкая Д.Г., Мигалевич С.А., Марков А.Н. // Центр молодежных инноваций минский городской технопарк – Минск: 2018, с.67.

3. Савицкая Д.Г., Мигалевич С.А., Основные угрозы безопасности виртуализации / Савицкая Д.Г., Мигалевич С.А. // Электронный научный журнал «Вестник современных исследований». – Омск: Научный центр «Орка»

4. Dallas K. The Internet of Things is Here URL – http://blogs.msdn.com/b/windows-embedded/archive/2013/09/06/the-internet-of-things-is-here.aspx (11.12.2018)

5. Amazon S3 URL – https://ru.wikipedia.org/wiki/Amazon_S3 (18.12.2018)

ӘОК 004.85

КОМПЮТЕРЛІК КӨРУ НЕГІЗІНДЕГІ ТЕХНОЛОГИЯЛАР ТЕНДЕНЦИЯЛАРЫ