**№9 дәріс. ДЕРЕКТЕРДІ САҚТАУ ЖҮЙЕЛЕРІ**

Жоспары:

1. Желілерді басқару мен мониторингке кіріспе
2. Желіні басқарудың негізгі міндеттері мен функциялары
3. Желілерді бақылау технологиялары мен құралдары
4. Желіні басқарудағы қауіпсіздікті қамтамасыз ету әдістері
5. Желіні басқарудағы заманауи тенденциялар мен инновациялар
6. Қорытынды

**Желілерді басқару мен мониторингке кіріспе**

Желілерді басқару және бақылау желілік инфрақұрылымның денсаулығы мен қауіпсіздігін қамтамасыз етуде шешуші рөл атқарады. Цифрлық технологиялардың белсенді дамуы, желілерді масштабтау және берілетін деректер көлемінің ұлғаюы жағдайында желілерді тиімді басқару мен мониторингке қажеттілік артып келеді. Бұл процестер желінің тұрақтылығын, болжамдылығын және қауіпсіздігін қамтамасыз етуге, сондай-ақ проблемалар мен қауіптерді жедел анықтауға бағытталған.

Желілерді басқару және бақылау жүйелері желілік жабдықтар мен коммуникациялар жұмысының барлық аспектілерін бақылауды қамтамасыз ететін шаралар кешенін қамтиды: өнімділік пен өткізу қабілеттілігінен қауіпсіздік пен ақауларға төзімділікке дейін. Желіні басқарудың негізгі міндеттері-желілік жабдықты орнату және конфигурациялау, конфигурация мен қол жетімділікті басқару және қауіпсіздік саясатының сақталуын бақылау. Өз кезегінде, желіні бақылау желінің күйін нақты уақыт режимінде бақылауға, ақауларды тез анықтауға және ықтимал қауіптердің алдын алуға мүмкіндік береді.

Қазіргі заманғы желілер-бұл әртүрлі құрылғылар мен протоколдарды қамтитын күрделі жүйелер. Бұл желіні басқару жүйелері (Network Management Systems, NMS) және өнімділікті бақылау жүйелері (Performance Monitoring Systems) сияқты арнайы басқару және бақылау жүйелерін пайдалануды талап етеді. Осы жүйелер арқылы әкімшілер желіні басқара алады, қауіпсіздік саясатын реттей алады, кіруді басқара алады және желілік трафикті талдай алады. Желілерді тиімді басқару және бақылау Бизнестің өнімділігін арттыруға және тоқтап қалу қаупін азайтуға ықпал етеді.

**Желіні басқарудың негізгі міндеттері мен функциялары**

Желіні басқару желілік инфрақұрылымның оңтайлы жұмысын қамтамасыз етуге бағытталған көптеген міндеттерді қамтиды. Желіні басқарудың негізгі функцияларына конфигурацияны Басқару, қол жетімділікті конфигурациялау, ресурстарды пайдалануды бақылау және қауіпсіздік кіреді. Бұл тапсырмалар тоқтап қалу қаупін азайтуға, желі өнімділігін арттыруға және деректер қауіпсіздігінің жоғары деңгейін қамтамасыз етуге көмектеседі.

Желіні басқарудың негізгі міндеттерінің бірі-маршрутизаторларды, қосқыштарды және кіру нүктелерін конфигурациялау мен оңтайландыруды қамтитын желілік жабдықтың конфигурациясын басқару. Бұл ресурстарды пайдалануды оңтайландыруға және әртүрлі құрылғылар арасында тұрақты байланысты сақтауға мүмкіндік береді. Конфигурацияны басқару сонымен қатар ықтимал ақаулар мен ақаулардың себептерін тезірек табуға және шешуге мүмкіндік беретін өзгерістерді бақылауды қамтиды.

Желінің қауіпсіздігін басқару (Сурет 1) - бұл деректерді қорғауға және рұқсатсыз кірудің алдын алуға бағытталған тағы бір маңызды мүмкіндік. Бұған қауіпсіздік саясатын орнату, брандмауэрлерді орнату, шифрлау әдістерін қолдану және қауіп-қатерді үнемі талдау кіреді. Көп факторлы аутентификация және кіруді басқару сияқты заманауи қауіпсіздік әдістері Деректерді кибершабуылдар мен ағып кетулерден қорғауға көмектеседі.


Сурет 1. Желінің қауіпсіздігін басқару

Қол жеткізуді басқару пайдаланушы құқықтары мен желі ресурстарына кіруге рұқсаттарды орнатуды қамтиды. Бұл құпия деректерге қол жеткізуді шектеуге және желіні бақылауды сақтауға көмектеседі. Қол жеткізуді тиімді басқару әсіресе көптеген қызметкерлер мен қосылған құрылғылар қатаң бақылауды қажет ететін ірі ұйымдар үшін өте маңызды.

Желіні басқарудың осы міндеттерінің әрқайсысы желінің қауіпсіздігі мен өнімділігін сақтауда маңызды рөл атқарады, бұл бизнестің тұрақты жұмыс істеуіне және ақаулық қаупін азайтуға ықпал етеді.

**Желілерді бақылау технологиялары мен құралдары**

Желілерді бақылау үшін әкімшілерге нақты уақыт режимінде желінің күйі мен өнімділігін бақылауға мүмкіндік беретін әртүрлі технологиялар мен құралдар қолданылады. Бұл құралдар ақаулықтарды жедел анықтауды, желілік трафикті талдауды қамтамасыз етеді және желінің қауіпсіздігін арттыруға

көмектеседі. Мониторинг құралдарының негізгі санаттары өнімділікті бақылау жүйелері (Network Performance Monitoring, NPM) және қауіптерді анықтау жүйелері (Intrusion Detection Systems, IDS) болып табылады.

Өнімділікті бақылау жүйелері (NPM) өткізу қабілеттілігі, кідірістер, пакеттің жоғалуы және ресурстарды пайдалану сияқты желі параметрлерін бақылайды. NPM құралдары желінің өнімділігін бақылауға және трафиктің өзгеруіне жедел жауап беруге мүмкіндік береді. Танымал NPM жүйелерінің мысалдарына SolarWinds Network Performance Monitor және PRTG Network Monitor кіреді, олар егжей-тегжейлі аналитиканы қамтамасыз етеді және әкімшілерге өнімділік мәселелерін болжауға көмектеседі.

Қауіпті анықтау жүйелері (IDS) желіге рұқсатсыз кіру немесе кіру әрекеттері сияқты күдікті әрекеттер мен шабуылдарды анықтауға мүмкіндік береді. IDS құралдары желілік трафикті талдайды және қауіптер анықталған кезде ескертулер жасайды, бұл әкімшілерге уақтылы әрекет етуге мүмкіндік береді. Snort және Suricata сияқты кейбір заманауи IDS жүйелерінде қауіп-қатерді талдау және басқа қауіпсіздік жүйелерімен интеграциялау мүмкіндігі жоғары.

Wireshark сияқты желілік трафикті талдау құралдары әкімшілерге желі арқылы өтетін деректер пакеттерін егжей-тегжейлі зерттеуге көмектеседі. Бұл талдау ақаулардың немесе ықтимал шабуылдардың себептерін түсінуді жақсартатын ауытқулар мен күдікті әрекеттерді анықтауға мүмкіндік береді. Желілік трафикті талдау технологиялары желінің қауіпсіздігін едәуір жақсартуға және деректердің жоғалу қаупін азайтуға мүмкіндік береді.

Желілік трафикті бақылау және талдау құралдары желілік инфрақұрылымның қауіпсіздігі мен тұрақтылығын сақтауда маңызды рөл атқарады, бұл әсіресе қауіпсіздік талаптарының жоғарылауы жағдайында маңызды.

**SNMP (қарапайым желіні басқару протоколы)**

SNMP (Simple Network Management Protocol) — бұл желілік құрылғыларды басқаруға және бақылауға арналған стандартты протокол. Ол маршрутизаторлар, коммутаторлар, серверлер және тіпті жұмыс станциялары сияқты желілік компоненттердің күйі мен өнімділігі туралы ақпарат жинау үшін қолданылады. SNMP клиент-сервер моделі бойынша жұмыс істейді, онда басқарылатын құрылғылар (агенттер) деректерді басқару жүйелеріне (менеджерлерге) жібереді.

*1. SNMP жұмыс принциптері*

SNMP протоколы үш негізгі компоненттен тұратын архитектураны қолданады:

SNMP менеджері: бұл құрылғының күйі және оның параметрлері туралы ақпарат алу үшін агенттерге сұраныстар жіберетін жүйе.

SNMP агенті: бұл құрылғының күйі туралы деректерді жинайтын және сақтайтын басқарылатын құрылғыға орнатылған бағдарламалық жасақтама.

Агент менеджердің сұрауларына жауап береді, сонымен қатар оқиғалар немесе күй өзгерістері туралы хабарламалар (траппалар) жібере алады.

Басқару дерекқоры (MIB): MIB (Management Information Base) — бақылауға болатын басқарылатын нысандар туралы ақпаратты қамтитын құрылымдық дерекқор. Ол қандай параметрлерді бақылауға болатындығын және оларды қалай ұйымдастыруға болатындығын анықтайды.

*2. SNMP артықшылықтары мен қолданылуы*

SNMP әкімшілерге нақты уақыт режимінде желінің өнімділігі мен күйі туралы деректерді алуға мүмкіндік береді. Бұл мәселелерді тез анықтауға және шешуге, сондай-ақ желілік ресурстарды оңтайландыруға көмектеседі. SNMP қолдану әсіресе қолмен бақылау тиімсіз болатын көптеген құрылғылары бар үлкен желілерде маңызды.

**NetFlow**

NetFlow-бұл Cisco компаниясы желілік трафикті бақылау және талдау үшін жасаған хаттама. Ол өткізу қабілеттілігін талдауға, кедергілерді анықтауға және трафиктегі ауытқуларды анықтауға мүмкіндік беретін желілік құрылғылар арқылы өтетін деректер ағындары туралы ақпарат береді.

*1. NetFlow жұмыс принциптері*

NetFlow кіріс және шығыс пакеттері туралы ақпарат негізінде желілік ағындар туралы деректерді жинайды. Әрбір ағын көздің IP мекенжайы, тағайындалған IP мекенжайы, порттар және протоколдар сияқты параметрлердің бірегей комбинациясымен анықталады. NetFlow ағындар туралы ақпаратты біріктіреді және оны әрі қарай өңдеу үшін аналитикалық жүйелерге жібереді.

*2. NetFlow қолданудың артықшылықтары*

NetFlow көмегімен әкімшілер желілік трафиктің терең талдауын ала алады, соның ішінде:

Өткізу қабілеттілігін пайдалануды бақылау: желіні жүктеуді талдау оңтайландыруды қажет ететін ресурстарды анықтауға мүмкіндік береді.

Өнімділікті талдау: NetFlow желідегі кедергілерді анықтауға және әртүрлі қолданбалардың желілік ресурстарды қалай пайдаланатынын бағалауға көмектеседі.

Ауытқуларды анықтау: ағымдағы ағындарды тарихи деректермен салыстыру қауіпсіздікті немесе өнімділікті көрсетуі мүмкін трафиктің ерекше үлгілерін анықтауға мүмкіндік береді.

**Желілік бақылау жүйелері**

*1. Nagios*

Nagios-бұл желілік құрылғылардың, серверлердің және қосымшалардың күйін бақылауға мүмкіндік беретін танымал бақылау жүйесі. Nagios пайдаланушыға әртүрлі бақылау параметрлерін және жүйенің күйі туралы хабарландыруларды теңшеу мүмкіндігін береді.

Функционалдылық: Nagios қол жетімділікті, өнімділікті және ресурстарды пайдалануды бақылауды қолдайды. Жүйе проблемалар туындаған кезде хабарламалар жібереді және күй туралы есептер береді.

Модульдік архитектура: Nagios функционалдылықты кеңейтуге және басқа жүйелермен біріктіруге мүмкіндік беретін көптеген плагиндерді ұсынады.

*2. Zabbix*

Zabbix-бұл желі мен серверлерді басқарудың жан-жақты тәсілін қамтамасыз ететін тағы бір қуатты бақылау жүйесі.

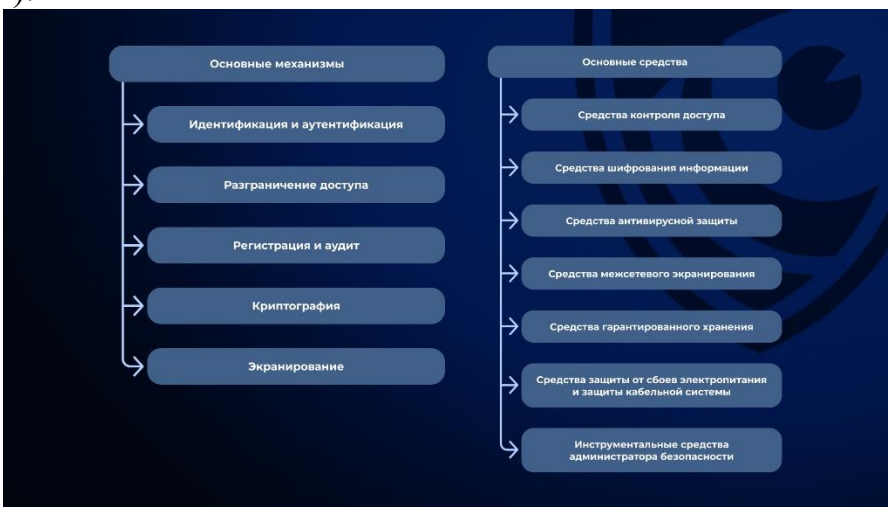
Әмбебаптық: Zabbix серверлерді, желілік құрылғыларды және виртуалды машиналарды қоса алғанда, әртүрлі құрылғыларды бақылауды қолдайды.

Деректерді жинау: Zabbix деректерді SNMP, IPMI, JMX және басқа протоколдар арқылы жинай алады, бұл егжей-тегжейлі есептер мен визуализациялар жасауға мүмкіндік береді.

Масштабтау: Zabbix көптеген нысандарды басқару мүмкіндігінің арқасында ірі кәсіпорын желілері үшін жақсы жұмыс істейді.

**Желіні басқарудағы қауіпсіздікті қамтамасыз ету әдістері**

Желіні басқарудағы қауіпсіздік желілік инфрақұрылым мен деректерді рұқсатсыз кіруден және шабуылдардан қорғау бойынша шаралар кешенін қамтиды. Қауіпсіздікті қамтамасыз етудің негізгі әдістері-шифрлау, аутентификация, қол жетімділікті басқару және желілік белсенділіктің тұрақты аудиті (Сурет 2).




Сурет 2. Қауіпсіздікті қамтамасыз етудің негізгі әдістері

Деректерді шифрлау желі арқылы тасымалдау кезінде ақпаратты қорғауға мүмкіндік береді. Желіні басқарудың заманауи жүйелері әртүрлі деңгейдегі деректерді қорғау үшін симметриялы және асимметриялық шифрлауды қолданады. Шифрлау құпия ақпаратты рұқсатсыз кіруден қорғауға көмектеседі және деректердің бұзылу қаупін азайтады.

Пайдаланушының аутентификациясы желілік инфрақұрылымды қорғауда маңызды рөл атқарады. Көп факторлы аутентификацияны (MFA) пайдалану пайдаланушылардан құпия сөзді енгізуді ғана емес, сонымен қатар мобильді құрылғы немесе басқа тексеру арқылы жеке басын растауды талап ету арқылы

қорғауды күшейтуге көмектеседі. Бұл желі ресурстарына рұқсатсыз қол жеткізу мүмкіндігін азайтады.

Қол жетімділікті басқару және қауіпсіздік саясатын құру — бұл тек уәкілетті пайдаланушылар үшін деректер мен желілік ресурстарға қол жетімділікті шектейтін желі қауіпсіздігінің маңызды аспектілері. Рөлдік қол жетімділікті басқаруды (RBAC) енгізу жұмыс міндеттеріне байланысты қол жетімділікті бөлуге мүмкіндік береді, бұл басқаруды жеңілдетеді және қауіпсіздікті арттырады.

Желілік белсенділіктің тұрақты аудиті және журналдарды талдау күдікті әрекеттер мен ықтимал қауіптерді уақтылы анықтауға көмектеседі. Аудит рұқсат етілмеген кіру әрекеттерін анықтауға және пайдаланушылардың әрекеттерін талдауға мүмкіндік береді, бұл желіні қорғаудың алдын алу шараларын қабылдауға көмектеседі.

Кешендегі бұл әдістер деректердің қауіпсіздігі мен желінің тұрақтылығын қамтамасыз ететін көп деңгейлі қорғаныс жүйесін жасайды, бұл әсіресе өсіп келе жатқан киберқауіптер жағдайында маңызды.

**Желіні басқарудағы заманауи тенденциялар мен инновациялар**

Желілер күрделене түсуде және жаңа технологиялар басқару мен бақылауға инновациялық тәсілдерді енгізуді талап етеді. Соңғы жылдары желілерді автоматтандыру, бағдарламалық қамтамасыз етумен анықталған желілер (SDN) және желілік деректерді талдау үшін жасанды интеллектті қолдану сияқты бағыттар белсенді дамып келеді.

Желілік процестерді автоматтандыру желіні басқаруды жеңілдетуге және жұмыс тиімділігін арттыруға мүмкіндік береді, әсіресе үлкен және күрделі инфрақұрылымдарда. Автоматтандыру жүйелері конфигурацияларды орнату және басқару сияқты күнделікті тапсырмаларды орындауға көмектеседі, бұл уақытты үнемдейді және қателерді азайтады.

Бағдарламалық жасақтамамен анықталған желілер (SDN) - бұл желіні басқару аппараттық құралдан бөлінген архитектура. Бұл желіні орталықтан басқаруға және маршруттар мен ресурстарға қол жетімділікті икемді түрде реттеуге мүмкіндік береді. SDN икемділікті арттыруға және желіні басқаруды жеңілдетуге көмектеседі, сонымен қатар трафиктің өзгеруіне және пайдаланушылардың талаптарына тез бейімделуге мүмкіндік береді.

Жасанды интеллект және машиналық оқыту желілік деректерді талдауда және ақауларды болжауда белсенді қолданылады. AI негізіндегі жүйелер үлкен көлемдегі деректерді талдай алады, үлгілерді анықтай алады және ықтимал ақауларды болжай алады, бұл әкімшілерге алдын алу шараларын қабылдауға мүмкіндік береді. Бұл желінің тұрақтылығын арттыруға және кибершабуылдан қорғауды жақсартуға көмектеседі.

Бұл тенденциялар желіні басқаруды икемді, болжамды және тиімді етеді. Жаңа технологияларды енгізу компанияларға басқару шығындарын азайтып

қана қоймай, сонымен қатар желінің қауіпсіздігі мен өнімділігін жоғары деңгейде қамтамасыз етуге мүмкіндік береді.

**Қорытынды**

Желілерді басқару және бақылау заманауи цифрлық инфрақұрылымның ажырамас элементтері болып табылады. Олардың маңыздылығы деректердің өсіп келе жатқан көлеміне, технологиялардың дамуының жеделдеуіне және қосылған құрылғылар санының артуына байланысты. Басқару жүйелері желілердің үздіксіз жұмыс істеуіне, конфигурацияларды басқаруға, ресурстарға қол жеткізуді бақылауға және өзгерістерге жылдам жауап беруге мүмкіндік береді, бұл әсіресе корпоративтік және қоғамдық желілердің қарқынды өсуі жағдайында маңызды. Мониторинг, өз кезегінде, трафикті талдау және ауытқуларды анықтау арқылы желінің күйін үнемі бақылауды қамтамасыз етеді, бұл ықтимал қауіптер мен бұзылуларға жедел жауап беруге мүмкіндік береді.

Желілерді тиімді басқару мен бақылаудың негізгі аспектісі-процестерді автоматтандыру, бағдарламалық жасақтамамен анықталған желілер (SDN) және жасанды интеллект сияқты инновациялар. Бұл технологиялар желіні басқару тәсілін өзгертеді, жүйе әкімшілерінің жұмысын жеңілдетеді, тоқтап қалудан аулақ болуға және адами факторды азайтуға мүмкіндік береді. Автоматтандыру басқару процестерін икемді етеді және олардың орындалуын тездетеді, ал SDN желіні орталықтандырылған басқаруды қамтамасыз етеді, оны орнатуды және оңтайландыруды жеңілдетеді. Жасанды интеллект желілік трафиктегі ауытқуларды анықтауға, ықтимал ақауларды болжауға және тіпті оларды автоматты түрде шешуге көмектеседі.

Желіні басқару мен бақылаудың тиімді әдістерімен ұйымдар жабдықтың тоқтап қалуына байланысты шығындарды азайтып, кибершабуыл қаупін азайтып, желінің өнімділігін арттыра алады. Цифрлық ортада белсенді дамып келе жатқан компаниялар үшін мұндай технологиялар қажет болады, өйткені олар бизнестің тұрақты дамуын және нарықтағы тұрақты өзгерістерге бейімделуді қолдайды. Желінің жылдамдығы мен қауіпсіздігіне үнемі өсіп келе жатқан талаптарды ескере отырып, басқару мен бақылауға инвестиция салатын компаниялар жоғары сапалы қызмет көрсете алады және пайдаланушылардың үміттерін қанағаттандыра алады.

Автоматтандыруды, бұлттық қызметтермен интеграцияны және жасанды интеллекттің өсуін қоса алғанда, желіні басқарудың заманауи тенденциялары масштабтауға және нақты тапсырмаларға бейімделуге қабілетті күрделі және икемді желілерді құруға мүмкіндік береді. Желілердің сенімділігі мен қауіпсіздігін сақтау үшін технологияларды енгізу ғана емес, сонымен қатар тұрақты аудит, осалдықтарды талдау және қорғаныс механизмдерін жаңарту қажет екенін есте ұстаған жөн. Болашақта желілерді басқару мен бақылау тек жетілдіріліп, жаңа сын-қатерлерге тиімді жауап беруге және цифрлық экожүйелердің қауіпсіз және тұрақты жұмысын қамтамасыз етуге мүмкіндік береді деп күтуге болады.

**Бақылау сұрақтары:**

1. Деректерді сақтау жүйесі дегеніміз не және оның негізгі Функционалы қандай?
2. Деректерді сақтау жүйелерінің өнімділігіне қандай факторлар әсер етеді?
3. NAS (сетевое хранилище) или SAN (сеть хранения данных) жүйелерінің негізгі айырмашылықтарын сипаттаңыз.
4. Сақтау жүйелерінің қауіпсіздігін қамтамасыз ету үшін қолданылатын шифрлау әдістері мен технологииларын түсіндіріңіз.
5. Бұлттық сақтау жүйесі дегеніміз не және ол дәстүрлі сақтау жүйелерінен қалай ерекшеленеді?
6. Деректерді архивтеу мэн резервтік көшіру арасындағы айырмашылықты түсіндіріңіз. Қайсысы деректер қауіпсіздігін қамтамасыз ету үшін маңыздырақ?
7. Таратылған сақтау жүйелелерінің (распределенные системы хранения) артықшылықтары мен кемшіліктерін сипаттаңыз.
8. Деректерді сақтауда өнімділік пени сенімділік арасында қандай теңгерімдер болады?

**Ұсынылған әдебиеттер:**

*Негізгі әдебиеттер*:

1. Смирнов, И. Н. Управление и мониторинг сетей: учебное пособие. М.: Академия, 2022.
2. Сидоров, А. Б. Основы управления сетевой инфраструктурой. СПб.: Питер, 2021.
3. Котов, М. С. Защита и управление сетями. М.: ФОРУМ, 2020.
4. Олифер, Н., & Олифер, V. Computer Networks: Principled, Technologies and Protocols. New York: John Wiley & Sons, 2019.
5. "Тенденции автоматизации управления сетями." Журнал "Информационные технологии", 2023.
6. "Мониторинг и безопасность сетей." Вестник сетевых технологий, 2021.

*Қосымша әдебиеттер:*

7. Cisco. Network Management Basics. Available online: https://www.cisco.com/c/en/us/solutions/.
8. Gartner. Network Monitoring and Automation Market Guide. Available online: https://www.gartner.com/en/documents/.
9. Microsoft. Network Monitoring and Diagnostics. Available online: https://docs.microsoft.com/en-us/network/.
10. Juniper Networks. Network Management and Security. Available online: https://www.juniper.net/.