

## БӨЛІМ: ЖАҢА ТЕХНОЛОГИЯЛАР

## Кәсіпорындағы құрылғылар үшін Microfost Server жалпы және жеке қауіпсіздік саясатын пайдаланудың артықшылықтары.

ЖАРИЯЛАНДЫ  
23.03.2023СІЛТЕМЕ  
<https://bilimger.kz/135246/>

Әлім Әлішер

Бұл мақалада жергілікті құрылғыда немесе шағын немесе орташа өлшемді ұйымда қауіпсіздік саясатының параметрлерін басқарудың әртүрлі әдістері қарастырылады.

Ұйымдағы Домен контроллерлерінің, серверлердің, клиенттік құрылғылардың және басқа ресурстардың қауіпсіздігін қамтамасыз ету үшін қауіпсіздік саясатының параметрлерін жалпы қауіпсіздікті іске асыру шеңберінде пайдалану керек.

Қауіпсіздік параметрлері саясаттары-бұл құрылғыда немесе желіде ресурстарды қорғау үшін құрылғыда немесе бірнеше құрылғыларда конфигурацияланатын ережелер. «Жергілікті топтық саясат редакторы» жабдығының қауіпсіздік параметрлерін кеңейту (Gpedit.msc) объектінің бөлігі ретінде қауіпсіздік конфигурацияларын анықтауға мүмкіндік береді топтық саясат (GPO). Топтық саясат нысандары сайттар, домендер және бөлімшелер сияқты Active Directory контейнерлерімен байланысты және әкімшілерге доменге қосылған кез келген құрылғыдан бірнеше компьютердің қауіпсіздік параметрлерін басқаруға мүмкіндік береді.

Қауіпсіздік параметрлері келесі параметрлерді басқара алады:

- \* Желіде немесе құрылғыда пайдаланушының түпнұсқалығын тексеру.
- \* Пайдаланушыларға кіруге рұқсат етілген ресурстар.
- \* Пайдаланушы немесе топ әрекеттерін Оқиғалар журналына жазу керек пе.
- \* Топқа мүшелік.

Бірнеше компьютердің қауіпсіздік конфигурацияларын басқару үшін келесі опциялардың бірін пайдалануға болады:

- \* Топтық саясат объектісінде белгілі бір қауіпсіздік параметрлерін өзгерту.

\* Қауіпсіздік шаблондарын қолдану үшін қауіпсіздік саясатын қамтитын қауіпсіздік шаблонын жасау үшін қолданыңыз, содан кейін қауіпсіздік шаблонын объектіге импорттаңыз топтық саясат. Қауіпсіздік үлгісі-бұл қауіпсіздік конфигурациясын білдіретін файл. Оны топтық саясат объектісіне импорттауға немесе жергілікті құрылғыға қолдануға немесе қауіпсіздікті талдау үшін пайдалануға болады.

«Жергілікті қауіпсіздік саясаты» жабдығын пайдалану

«Жергілікті қауіпсіздік саясаты» (Secpol.msc) Жергілікті саясат объектілерін ұсынуды келесі саясаттар мен функциялармен шектейді:

- Тіркелу саясаты
- Жергілікті саясаткерлер
- Жоғары қауіпсіздік режимінде Windows брандмауэрі
- Желілік тізім менеджерінің саясаты
- Ашық кілт саясаты
- Бағдарламаларды шектеулі пайдалану саясаты
- Қолданбаларды басқару саясаты
- Жергілікті компьютердегі IP мекенжайларының қауіпсіздік саясаты
- Аудит саясатының кеңейтілген конфигурациясы
- Егер компьютер доменге қосылған болса, жергілікті түрде берілген саясаттарды қайта жазуға болады.
- Secedit пәрмен жолы бағдарламасын пайдалану

Secedit пәрмен жолы бағдарламасы қауіпсіздік үлгілерімен жұмыс істейді және алты негізгі мүмкіндікті ұсынады:

- Конфигурация параметрі дұрыс емес серверге дұрыс қауіпсіздік үлгісін қолдану арқылы құрылғылар арасындағы қауіпсіздік сәйкессіздіктерін жоюға көмектеседі.
- Талдау параметрі сервердің қауіпсіздік конфигурациясын таңдалған шаблонмен салыстырады.
- Импорттау параметрі бар шаблон негізінде мәліметтер базасын құруға мүмкіндік береді. Бұл клондау конфигурация және қауіпсіздікті талдау құралы арқылы да орындалады.
- Export параметрі параметрлерді дерекқордан қауіпсіздік параметрлері үлгісіне экспорттауға мүмкіндік береді.

- Validate параметрі қауіпсіздік үлгісіне жасалған немесе қосылған әрбір немесе кез келген мәтін жолдарының синтаксисін тексеруге мүмкіндік береді. Бұл тексеру шаблон синтаксисті қолдана алмаса, шаблондағы мәселе болмайды.
- Generate Rollback параметрі сервердің ағымдағы қауіпсіздік параметрлерін қауіпсіздік үлгісіне сақтайды, осылайша оны сервердің көптеген қауіпсіздік параметрлерін белгілі күйге келтіру үшін пайдалануға болады. Ерекшелік-қолдану кезінде кері қайтару үлгісі соңғы қолданылған шаблонмен өзгертілген файлдардағы немесе тізілім жазбаларындағы кіруді басқару тізімінің жазбаларын өзгертпейді.

### Қауіпсіздікті орнату және талдау

Қауіпсіздікті конфигурациялау және талдау-бұл жергілікті жүйенің қауіпсіздігін талдауға және конфигурациялауға арналған ММС қондырғысы.

### Қауіпсіздікті талдау

Құрылғыдағы амалдық жүйе мен қосымшалардың күйі динамикалық. Мысалы, әкімшілік немесе желі мәселелерін дереу шешу үшін қауіпсіздік деңгейлерін уақытша өзгерту қажет болуы мүмкін. Алайда, бұл өзгеріс жиі өзгермеуі мүмкін. Өзгерістердің бұл күйі компьютер енді корпоративтік қауіпсіздік талаптарына сәйкес келмеуі мүмкін дегенді білдіреді.

Тұрақты талдау корпоративтік тәуекелдерді басқару бағдарламасының бөлігі ретінде әрбір компьютерде қауіпсіздіктің жеткілікті деңгейін бақылауға және қамтамасыз етуге мүмкіндік береді. Сіз қауіпсіздік деңгейлерін реттей аласыз және ең бастысы жүйеде уақыт өте келе туындауы мүмкін барлық қауіпсіздік кемшіліктерін анықтай аласыз.

Конфигурация және қауіпсіздік талдауы қауіпсіздікті талдау нәтижелерін жылдам қарауға мүмкіндік береді. Ол жүйенің ағымдағы параметрлерімен қатар ұсыныстарды ұсынады және ағымдағы параметрлер ұсынылған қауіпсіздік деңгейіне сәйкес келмейтін аймақтарды бөлектеу үшін көрнекі жалаушаларды немесе жазбаларды пайдаланады. Конфигурация және қауіпсіздік талдауы сонымен қатар талдау арқылы анықталған сәйкессіздіктерді жоюға мүмкіндік береді.

### Қауіпсіздік конфигурациясы

Конфигурация мен қауіпсіздікті талдауды жергілікті жүйенің қауіпсіздігін тікелей реттеу үшін де пайдалануға болады. Жеке мәліметтер базасын қолдана отырып, қауіпсіздік шаблондарымен жасалған қауіпсіздік шаблондарын импорттауға және сол шаблондарды жергілікті компьютерге қолдануға болады. Бұл қауіпсіздік үлгілері үлгіде

көрсетілген деңгейлермен жүйенің қауіпсіздігін бірден реттейді.

### Қауіпсіздік үлгілері

Басқару консоліне (Microsoft) арналған «қауіпсіздік үлгілері» құралының көмегімен құрылғы немесе желі үшін қауіпсіздік саясатын жасауға болады. Бұл жүйелік қауіпсіздіктің толық спектрін ескеруге болатын бірыңғай кіру нүктесі. Қауіпсіздік шаблондары жаңа қауіпсіздік параметрлерін енгізбейді, ол қауіпсіздікті басқаруды жеңілдету үшін барлық қолданыстағы қауіпсіздік атрибуттарын бір жерде ұйымдастырады.

Қауіпсіздік үлгісін объектіге импорттау топтық саясат Домен немесе бөлім үшін қауіпсіздікті бір уақытта реттеу арқылы доменді басқаруды жеңілдетеді.

Қауіпсіздік үлгісін жергілікті құрылғыға қолдану үшін қауіпсіздік конфигурациясы мен талдауын немесе secedit пәрмен жолы бағдарламасын пайдалануға болады.

Қауіпсіздік үлгілерін анықтау үшін пайдалануға болады:

- Тіркелу саясаты
- Пароль саясаты
- Есептік жазбаны бұғаттау саясаты
- Керберос Саясаты
- Жергілікті саясаткерлер
- Аудит саясаты
- Пайдаланушы құқықтарының мақсаты
- Қауіпсіздік параметрлері

\* Оқиғалар журналы: қолданба, жүйе және қауіпсіздік оқиғалары журналы опциялары

- Шектеулі топтар: қауіпсіздікке сезімтал топтарға мүшелік
- Жүйелік қызметтер: жүйелік қызметтер үшін іске қосу және рұқсаттар
- Тізілім: тізілім бөлімдеріне рұқсаттар
- Файлдық жүйе: қалталар мен файлдарға рұқсаттар

Әрбір үлгі мәтіндік INF файлы ретінде сақталады. Бұл файл шаблонның кейбір немесе барлық атрибуттарын көшіруге, қоюға, импорттауға немесе экспорттауға мүмкіндік береді. Интернет протоколының қауіпсіздік саясаты мен ашық кілттерді қоспағанда, барлық қауіпсіздік атрибуттары қауіпсіздік үлгісінде болуы мүмкін.

Қауіпсіздік параметрлерін кеңейту топтық саясат

Бөлімшелер, домендер мен сайттар объектілерімен байланысты топтық саясат.

Қауіпсіздік параметрлері құралы объектінің қауіпсіздік конфигурациясын өзгертуге мүмкіндік береді топтық саясат, өз кезегінде бірнеше компьютерлерге әсер етеді. Қауіпсіздік параметрлері арқылы көптеген құрылғылардың қауіпсіздік параметрлерін қай объектіге байланысты өзгертуге болады топтық саясат сіз доменге қосылған бір құрылғыдан өзгертесіз.

Қауіпсіздік немесе қауіпсіздік саясатының параметрлері-бұл құрылғыда немесе желіде ресурстарды қорғау үшін құрылғыда немесе бірнеше құрылғыларда конфигурацияланған ережелер. Қауіпсіздік параметрлері келесі параметрлерді басқара алады:

- Пайдаланушылар желіде немесе құрылғыда аутентификациядан қалай өтеді
- Пайдаланушыларға қандай ресурстарды пайдалануға рұқсат етіледі
- Пайдаланушы немесе топ әрекеттері Оқиғалар журналына жазыла ма
- Топқа мүшелік

Бірнеше компьютердегі қауіпсіздік конфигурациясын екі жолмен өзгертуге болады:

- Қауіпсіздік үлгілері бар қауіпсіздік үлгісін пайдаланып қауіпсіздік саясатын жасаңыз, содан кейін үлгіні қауіпсіздік параметрлері арқылы импорттаңыз нысан топтық саясат.
- Қауіпсіздік параметрлерін пайдаланып бірнеше таңдау опцияларын өзгертіңіз.
- Жергілікті қауіпсіздік саясаты

Қауіпсіздік саясаты-бұл құрылғыдағы қауіпсіздікке әсер ететін қауіпсіздік параметрлерінің жиынтығы. Жергілікті құрылғыдағы тіркелгі саясаттары мен жергілікті саясаттарды өзгерту үшін жергілікті қауіпсіздік саясатын пайдалануға болады.

Жергілікті қауіпсіздік саясатының көмегімен келесі параметрлерді басқаруға болады:

- Сіздің құрылғыңызға кім жүгінеді
- Пайдаланушылар сіздің құрылғыңызда қандай ресурстарды пайдалануға құқылы
- Пайдаланушы немесе топ әрекеттері Оқиғалар журналына жазыла ма

Егер сіздің жергілікті құрылғыңыз доменге қосылған болса, сіз қауіпсіздік саясатын Домен саясатынан немесе сіз мүше болып табылатын кез келген бөлімшенің саясатынан ала аласыз. Егер сіз саясатты бірнеше көздерден алсаңыз, қақтығыстар келесі басымдық тәртібімен шешіледі.

- Бөлімше саясаты

- Домен саясаты
- Сайт саясаты
- Жергілікті Компьютер саясаты

**ҚМ АА** Күәлік нөмірі: **KZ45VPY00102718** — ҚР Мәдениет және Ақпарат министрлігі

© 2026 **Bilimger.kz** Ақпараттық-танымдық білім порталы. Барлық мазмұн авторлық құқықпен қорғалған.