FSRM na fs01: limity, blokowanie plików, raporty i folder pułapka na ransomware

Poziom: średnio

Dotyczy: Windows Server 2022, fs01 (10.20.10.15), File Server Resource Manager

Czas: ~60 min

FSRM to wbudowany w Windows Server zestaw narzędzi, które pilnują serwera plików: ostrzegają, gdy dział zapycha dysk, nie wpuszczają programów tam, gdzie mają leżeć faktury, i co miesiąc mówią, kto trzyma najwięcej. Na tej stronie ustawiamy je na `fs01` i dokładamy folder pułapkę, który odcina od udziałów konto szyfrujące pliki. Wracamy tu przy alarmie z pułapki, przy prośbie o więcej miejsca i przy przeglądzie miesięcznym.

Skróty użyte na tej stronie (11)

Skrót	Co znaczy
ASR	Attack Surface Reduction: reguły redukcji powierzchni ataku w Defenderze, które blokują zachowania typowe dla złośliwego oprogramowania, na przykład uruchamianie plików z makr Office albo kradzież haseł z pamięci systemu; w Azure także Azure Site Recovery: replikacja maszyn do innego regionu i przełączenie po awarii
DFS	Distributed File System: usługa łącząca udziały z wielu serwerów pod jedną wspólną ścieżką sieciową
FSRM	File Server Resource Manager: rola Windows Server do pilnowania serwera plików, ustawia limity miejsca, filtry plików, raporty i akcje po zdarzeniach
GB	Gigabyte: miliard bajtów, jednostka pojemności pamięci i plików, tu najczęściej rozmiar modelu albo pamięci karty graficznej
S2D	Storage Spaces Direct: programowa macierz Windows Server z dysków wielu serwerów
SACL	System Access Control List: lista w zabezpieczeniach pliku, która mówi, które próby dostępu system ma zapisać w dzienniku audytu

Skrót	Co znaczy
SMB	Server Message Block: protokół udostępniania plików i drukarek w sieci Windows, na nim stoi zwykły udział sieciowy
USN	Update Sequence Number: rosnący licznik zmian w bazie Active Directory na danym kontrolerze domeny, używany do śledzenia postępu replikacji
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
VSS	Volume Shadow Copy Service: mechanizm Windows do tworzenia spójnych migawek danych mimo działających w tle usług, wykorzystywany też przy kopiach zapasowych kontrolera domeny
WSUS	Windows Server Update Services: firmowy serwer aktualizacji Windows

Fiszka

Komendy wykonujemy na `fs01` w PowerShellu uruchomionym jako administrator, chyba że przy fiszce napisano inaczej. Polskie placeholdery (`SciezkaUdzialu`, `NazwaGrupyPlikow`) podmieniamy na swoje, w przykładach stoją nazwy z Zielonej.

◫◫ ZMIENIA SYSTEM

Instalacja FSRM: Install-WindowsFeature FS-Resource-Manager

```
Install-WindowsFeature -Name FS-Resource-Manager -IncludeManagementTools
```

Instaluje usługę FSRM (`SrmSvc`) i konsolę „Menedżer zasobów serwera plików”. Restart serwera nie jest zwykle potrzebny, ale sprawdzamy to w wyniku polecenia (kolumna `Restart Needed`).

◫◫ **FSRM** = File Server Resource Manager: rola Windows Server do pilnowania serwera plików, ustawia limity miejsca, filtry plików, raporty i akcje po zdarzeniach

◫◫ ZMIENIA SYSTEM

Ustawienie poczty dla powiadomień: Set-FsrmSetting

```
Set-FsrmSetting -SmtpServer "NazwaSerweraSmtp" -AdminEmailAddress "AdresAdministratora"
-FromEmailAddress "AdresNadawcy"
Send-FsrmTestEmail -ToEmailAddress "AdresAdministratora"
```

W Zielonej: serwer `poczta.zielona.example`, administrator `it@zielona.example`, nadawca `powiadomienia@zielona.example`. Drugie polecenie wysyła wiadomość próbną. Zanim ustawimy powiadomienia pocztowe albo raporty, ustawienia poczty muszą być gotowe [3].

□□ ZMIENIA SYSTEM

Wyłączenie odstępu między uruchomieniami polecenia: Set-FsrmSetting -CommandNotificationLimit

```
Set-FsrmSetting -CommandNotificationLimit 0 -EventNotificationLimit 0
```

Te ustawienia mówią, ile minut musi minąć, zanim FSRM uruchomi ponownie akcję tego samego rodzaju [4]. Dla pułapki to ważne: przy domyślnym odstępie drugie zaszyfrowane konto w tej samej godzinie mogłoby nie zostać zablokowane. Czy wartość 0 całkiem wyłącza odstęp, sprawdzamy testem z dwoma kontami (do potwierdzenia), bo dokumentacja nie podaje wartości domyślnej.

□□ **FSRM** = File Server Resource Manager: rola Windows Server do pilnowania serwera plików, ustawia limity miejsca, filtry plików, raporty i akcje po zdarzeniach

□□ ZMIENIA SYSTEM

Limit miękki z ostrzeżeniem: New-FsrmQuota -SoftLimit

```
$poczta = New-FsrmAction -Type Email -MailTo "[Admin Email]" -Subject "fs01: [Quota Path] zajmuje [Quota Used Percent]% limitu" -Body "Folder [Quota Path] przekroczył próg [Quota Threshold]%."
$prog85 = New-FsrmQuotaThreshold -Percentage 85 -Action $poczta
$prog100 = New-FsrmQuotaThreshold -Percentage 100 -Action $poczta
New-FsrmQuota -Path "SciezkaUdzialu" -Size LimitGB -SoftLimit -Threshold @($prog85, $prog100) -Description "OpisLimitu"
```

Komendy można wykonać jako blok. Limit miękki niczego nie blokuje, tylko wysyła nam pocztę przy 85 i 100 procentach [5]. Zmienne w nawiasach kwadratowych podstawia FSRM; ich listę pokazuje przycisk „Wstaw zmienną” w oknie progu (nazwy w przykładzie do potwierdzenia na naszej wersji).

Przykład (dla działu wysyłek):

```
New-FsrmQuota -Path "D:\Dane\Wysylki" -Size 600GB -SoftLimit -Threshold @($prog85, $prog100) -Description "Wysylki: limit miekki, skany list przewozowych"
```

FSRM = File Server Resource Manager: rola Windows Server do pilnowania serwera plików, ustawia limity miejsca, filtry plików, raporty i akcje po zdarzeniach

ZMIENIA SYSTEM

Limit twardy dla folderu wspólnego: New-FsrmQuota

```
New-FsrmQuota -Path "SciezkaUdzialu" -Size LimitGB -Threshold @($prog85, $prog100) -
Description "OpisLimitu"
```

Bez `-SoftLimit` limit jest twardy: po jego osiągnięciu zapis kończy się błędem braku miejsca. Twardy limit stawiamy tylko na `D:\Dane\Wspolne` (100 GB), żeby wymusić porządki; działom zostawiamy miękkie, bo zatrzymany zapis faktury w zamknięciu miesiąca boli bardziej niż pełny dysk.

GB = Gigabyte: miliard bajtów, jednostka pojemności pamięci i plików, tu najczęściej rozmiar modelu albo pamięci karty graficznej

TYLKO ODCZYT

Odczyt limitów i zajętości: Get-FsrmQuota

```
Get-FsrmQuota | Format-Table Path, @{n='LimitGB';e={[math]::Round($_.Size/1GB)}},
@{n='ZajeteGB';e={[math]::Round($_.Usage/1GB)}}, SoftLimit
```

Przykład:

```
Path               LimitGB ZajeteGB SoftLimit
----               ------- -------- ---------
D:\Dane\Ksiegowosc     400      231      True
D:\Dane\Wspolne        100       88     False
D:\Dane\Wysylki        600      547      True
```

ZMIENIA SYSTEM

Utworzenie grupy plików wykonywalnych: New-FsrmFileGroup

```
New-FsrmFileGroup -Name "NazwaGrupyPlikow" -IncludePattern @("*.exe", "*.com", "*.scr",
"*.msi", "*.bat", "*.cmd", "*.ps1", "*.vbs", "*.js", "*.hta")
```

Grupa plików to lista wzorców nazw, na które patrzy filtr. W Zielonej grupa nazywa się `Wykonywalne Zielona`. Filtr patrzy na nazwy, a nie na zawartość, więc plik `faktura.pdf.exe` złapie, ale program przemianowany na `.pdf` przepuści.

□□ ZMIENIA SYSTEM

Filtr aktywny blokujący programy w udziale działu: New-FsrmFileScreen -Active

```
$zdarzenie = New-FsrmAction -Type Event -EventType Warning -Body "fs01: [Source Io
Owner] probowal zapisac [Source File Path] (grupa [Violated File Group])"
New-FsrmFileScreen -Path "SciezkaUdzialu" -IncludeGroup "NazwaGrupyPlikow" -Active -
Notification $zdarzenie
```

Filtr aktywny nie pozwala zapisać pliku z grupy i zapisuje zdarzenie w dzienniku Application, które agent wysyła do Grayloga [6]. Stawiamy go na każdym udziale działu poza `D:\Dane\IT`, gdzie leżą instalatory.

□□ **IT** = Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy

□□ ZMIENIA SYSTEM

Wyjątek od filtra dla jednego folderu: New-FsrmFileScreenException

```
New-FsrmFileScreenException -Path "SciezkaFolderuWyjatku" -IncludeGroup
"NazwaGrupyPlikow"
```

Wyjątek zwalnia jeden podfolder z filtra nadrzędnego. Przykład: pani Halina dostaje od dostawcy Optimy plik `.exe` z poprawką i potrzebuje folderu `D:\Dane\Ksiegowosc\Optima-poprawki` na czas aktualizacji; po aktualizacji wyjątek usuwamy.

□□ ZMIENIA SYSTEM

Przygotowanie folderu pułapki z wabikami

```
$pulapka = "SciezkaUdzialu\0-pulapka"
New-Item -Path $pulapka -ItemType Directory | Out-Null
Copy-Item -Path "C:\FSRM\wabiki\*" -Destination $pulapka
$folder = Get-Item $pulapka
```

```
$folder.Attributes = $folder.Attributes -bor [System.IO.FileAttributes]::Hidden
```

Komendy można wykonać jako blok, osobno dla każdego udziału działu. Wabiki to kilka zwyczajnie wyglądających plików (`Faktury_wzor.xlsx`, `Umowa_ramowa.docx`, `Zestawienie.pdf`) bez prawdziwych danych, przygotowanych raz w `C:\FSRM\wabiki`. Folder dziedziczy uprawnienia udziału, więc konto z prawem zapisu do działu może go zaszyfrować, a ukrycie zmniejsza szansę, że ktoś wejdzie tam przypadkiem. Wabiki kopiujemy przed założeniem filtra, bo inaczej sami uruchomimy pułapkę.

FSRM = File Server Resource Manager: rola Windows Server do pilnowania serwera plików, ustawia limity miejsca, filtry plików, raporty i akcje po zdarzeniach

PLIK KONFIGURACYJNY

Skrypt blokady konta: blokada-uzytkownika.ps1

```
param(
  [Parameter(Mandatory = $true)] [string]$Uzytkownik,
  [string]$Plik = ""
)
# Uruchamia FSRM jako LocalSystem, gdy ktos zapisze albo zmieni nazwe pliku w folderze pulapce.
# Konto dostaje odmowe na kazdym udziale, a jego sesje SMB sa zamykane.
$Zrodlo = "FSRM-Pulapka"
$Wyjatki = @("NT AUTHORITY\SYSTEM")

if (-not [System.Diagnostics.EventLog]::SourceExists($Zrodlo)) {
  New-EventLog -LogName Application -Source $Zrodlo
}

if ($Wyjatki -contains $Uzytkownik) {
  Write-EventLog -LogName Application -Source $Zrodlo -EventId 9001 -EntryType Warning -Message "Pulapka: zapis konta z listy wyjatkow $Uzytkownik, plik $Plik. Bez blokady."
  exit 0
}

$Udzialy = @(Get-SmbShare -Special $false)
foreach ($u in $Udzialy) {
  Block-SmbShareAccess -Name $u.Name -AccountName $Uzytkownik -Force | Out-Null
}
```

```
$Sesje = @(Get-SmbSession | Where-Object { $_.ClientUserName -eq $Uzytkownik })
$Sesje | Close-SmbSession -Force

Write-EventLog -LogName Application -Source $Zrodlo -EventId 9000 -EntryType Error -
Message "Pulapka: zablokowano $Uzytkownik na $($Udzialy.Count) udzialach, zamknieto
$($Sesje.Count) sesji. Plik: $Plik"
```

Plik zapisujemy jako `C:\FSRM\blokada-uzytkownika.ps1`, a folder `C:\FSRM` dostaje uprawnienia tylko dla `SYSTEM` i administratorów (skrypt uruchamiany jako LocalSystem, którego treść może zmienić zwykły użytkownik, byłby furtką do przejęcia serwera). `Block-SmbShareAccess` dopisuje do udziału wpis odmowy dla konta [7], a odmowa wygrywa z każdym zezwoleniem. Zdarzenie 9000 ze źródła `FSRM-Pulapka` to sygnał dla alarmu w Graylogu. Skrypt podpisujemy według strony Polityka wykonywania i podpisywanie skryptów, jeżeli na serwerach obowiązuje `AllSigned`.

FSRM = File Server Resource Manager: rola Windows Server do pilnowania serwera plików, ustawia limity miejsca, filtry plików, raporty i akcje po zdarzeniach · **NT** = pierwotnie kryptonim N-Ten, od procesora, dla którego system miał powstać; popularnie dziś odczytywane jako New Technology, choć to rozwinięcie nie jest oficjalne: rdzeń dzisiejszego Windows Server · **exit** = zakończ bieżącą powłokę albo skrypt z podanym kodem wyjścia

ZMIENIA SYSTEM

Filtr pasywny na pułapce z akcją polecenia: New-FsrmAction -Type Command

```
New-FsrmFileGroup -Name "Pulapka wszystkie pliki" -IncludePattern @("*")
$blokada = New-FsrmAction -Type Command -Command
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -CommandParameters '-
NoProfile -File C:\FSRM\blokada-uzytkownika.ps1 -Uzytkownik "[Source Io Owner]" -Plik
"[Source File Path]"' -WorkingDirectory "C:\FSRM" -SecurityLevel LocalSystem -
KillTimeOut 5 -ShouldLogError
$alarm = New-FsrmAction -Type Event -EventType Error -Body "PULAPKA fs01: [Source Io
Owner] zapisal [Source File Path] procesem [Source Process Image]"
$mail = New-FsrmAction -Type Email -MailTo "[Admin Email]" -Subject "PULAPKA fs01:
[Source Io Owner]" -Body "Zapis w folderze pulapce: [Source File Path]. Konto
zablokowane na udzialach."
New-FsrmFileScreen -Path "SciezkaUdzialu\0-pulapka" -IncludeGroup "Pulapka wszystkie
pliki" -Active:$false -Notification @($blokada, $alarm, $mail)
```

Komendy można wykonać jako blok. Grupę tworzymy raz, a ostatnią linię powtarzamy dla każdego udziału działu. Filtr pasywny niczego nie blokuje, tylko uruchamia akcje [8], więc szyfrujący program „myśli”, że mu się udało, a w tym czasie skrypt odcina konto. Zmienna `[Source Io Owner]` to konto, które wykonało zapis, `[Source File Path]` to ścieżka pliku, a `[Source Process Image]` nazwa programu [9]. Akcja polecenia działa z uprawnieniami `LocalSystem`, bo tylko takie konto może zmieniać uprawnienia udziałów [4].

FSRM = File Server Resource Manager: rola Windows Server do pilnowania serwera plików, ustawia limity miejsca, filtry plików, raporty i akcje po zdarzeniach

TYLKO ODCZYT

Sprawdzenie filtrów i akcji: Get-FsrmFileScreen

```
Get-FsrmFileScreen | Format-Table Path, Active, IncludeGroup
```

Przykład:

```
Path                          Active IncludeGroup
----                          ------ ------------
D:\Dane\Handel                  True {Wykonywalne Zielona}
D:\Dane\Ksiegowosc              True {Wykonywalne Zielona}
D:\Dane\Ksiegowosc\0-pulapka   False {Pulapka wszystkie pliki}
D:\Dane\Magazyn                 True {Wykonywalne Zielona}
D:\Dane\Magazyn\0-pulapka      False {Pulapka wszystkie pliki}
```

ZMIENIA SYSTEM

Test pułapki kontem testowym

```
New-Item -Path "\\ad.zielona.example\pliki\NazwaUdzialu\0-pulapka\test-pulapki.txt" -
ItemType File
```

Wykonujemy na stacji testowej, zalogowani kontem testowym z prawem zapisu do działu (u nas `test.pulapka` w `GG_IT`, udział `IT` z pułapką na czas testu). Po kilku sekundach kolejne polecenie `Get-ChildItem` na tym udziale powinno zwrócić odmowę dostępu, a na `fs01` widzimy wpis `Deny` w `Get-SmbShareAccess` i zdarzenie 9000. Test to zmiana normalna we wtorkowym oknie, raz na kwartał i po każdej zmianie skryptu.

IT = Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy

ZMIENIA SYSTEM

Odblokowanie konta po wyjaśnieniu: Unblock-SmbShareAccess

```
Get-SmbShare -Special $false | ForEach-Object { Unblock-SmbShareAccess -Name $_.Name -
AccountName "ZIELONA\nazwa_usera" -Force }
```

Zdejmuje wpis odmowy ze wszystkich udziałów. Odblokowujemy dopiero wtedy, gdy stacja jest wyczyszczona albo przeinstalowana, a hasło konta zmienione. Pułapkę po teście sprzątamy: usuwamy `test-pulapki.txt`, żeby wabiki znów wyglądały jak nietknięte.

ZMIENIA SYSTEM

Miesięczny raport magazynu: New-FsrmStorageReport

```
$termin = New-FsrmScheduledTask -Time (Get-Date "06:00") -Monthly 1
New-FsrmStorageReport -Name "NazwaRaportu" -Namespace @("SciezkaDanych") -Schedule
$termin -ReportType @("LargeFiles", "DuplicateFiles", "FilesByOwner", "QuotaUsage") -
LargeFileMinimum 1GB -MailTo "[Admin Email]"
```

Komendy można wykonać jako blok. Raport powstaje pierwszego dnia miesiąca o 6:00 dla całego `D:\Dane` [10]: duże pliki, duplikaty, pliki według właścicieli i zajętość limitów. Z raportu „według właścicieli” korzysta przegląd kwartalny, a z „duplikatów” porządki w `Wspolne`.

KLIKAMY W INTERFEJSIE

Ustawienia w konsoli FSRM

```
Menedżer zasobów serwera plików → Zarządzanie osłanianiem plików → Osłony plików → wybór
osłony → Edytuj właściwości osłony pliku → zakładki Wiadomość e-mail, Dziennik zdarzeń,
Polecenie, Raport
```

To samo, co polecenia wyżej, w oknie. Nazwy w polskim interfejsie sprawdzamy na serwerze (w angielskim: File Screening Management, File Screens, Edit File Screen Properties).

ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: okno właściwości filtra `D:\Dane\Ksiegowosc\0-pulapka`, zakładka Polecenie z wpisaną ścieżką `powershell.exe`, argumentami ze zmienną `[Source Io`

`Owner]` i wybranym kontem Local System.

FSRM = File Server Resource Manager: rola Windows Server do pilnowania serwera plików, ustawia limity miejsca, filtry plików, raporty i akcje po zdarzeniach

Z życia wzięte

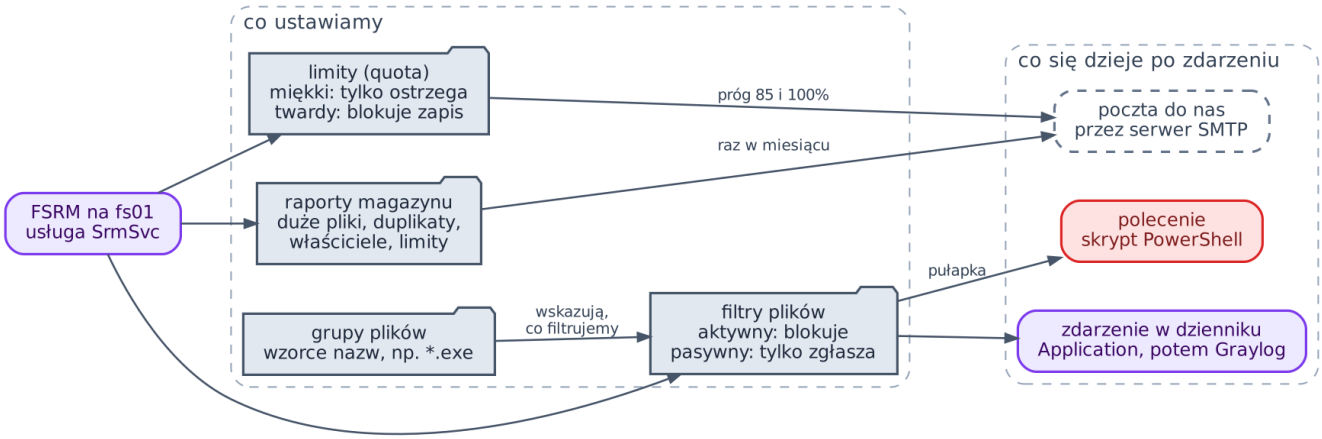
Z ŻYCIA WZIĘTE

Czwartek, 10:52. Laptop handlowca, który od rana pracował w hotelowej sieci, zaczyna przez VPN zmieniać nazwy plików na `\\ad.zielona.example\pliki\Handel` na `*.lockd`. Program idzie po kolei i trzeci plik, jaki zmienia, leży w `0-pulapka`. Po czterech sekundach konto jest odcięte od wszystkich udziałów, sesja SMB zamknięta, a Tomek dostaje alarm z Grayloga. W `Handel` zaszyfrowane są 23 pliki z jednego folderu, które odtwarzamy z poprzednich wersji z 7:00, bez sięgania do `bkp01`.

Jak to działa

Rozwiń: jak to działa pod spodem

Pojęcie: FSRM (File Server Resource Manager). Rola Windows Server do zarządzania danymi na serwerze plików. Umie pięć rzeczy: limity miejsca, filtry plików, raporty magazynu, klasyfikację plików i zadania zarządzania plikami [1]. W Zielonej używamy pierwszych trzech; klasyfikacja i zadania zostają na później.



Rysunek 1. Elementy FSRM na fs01: limity, filtry z grupami plików i raporty, a po zdarzeniu poczta do nas, zdarzenie w dzienniku dla Grayloga albo polecenie, które uruchamia skrypt (kliknięcie otwiera pełny rozmiar)

FSRM jest w Windows Server 2025, 2022, 2019 i 2016 [1]. Na liście funkcji usuniętych i nierozwijanych w Windows Server (strona aktualizowana 24.09.2025, sprawdzona 26.10.2026) nie ma FSRM, przestrzeni nazw DFS, replikacji DFS ani kopii w tle [2]. Usługa FSRM zakłada na wolumenach dziennik zmian (dziennik USN), który zajmuje trochę miejsca; da się go wyłączyć wpisem w rejestrze, ale wtedy przestaje działać klasyfikacja w czasie rzeczywistym [1].

Limity

> **Pojęcie: limit (quota).** Granica miejsca dla folderu. Limit twardy nie pozwala zapisać więcej, limit miękki tylko raportuje i uruchamia progi [5]. Limit FSRM liczy rozmiar folderu, a nie właściciela plików, więc pasuje do udziału działu.

Udział	Limit	Rodzaj	Uzasadnienie
`Ksiegowosc`	400 GB	miękki	zamknięcie miesiąca nie może stanąć przez pełny limit
`Kadry`	100 GB	miękki	mało danych, dużo wrażliwości
`Magazyn`, `Wysylki`	200 GB, 600 GB	miękki	skany rosną szybko, chcemy wiedzieć wcześniej
`Handel`, `Zarzad`	150 GB, 100 GB	miękki	jak wyżej

Udział	Limit	Rodzaj	Uzasadnienie
`IT`	300 GB	miękki	instalatory i obrazy systemów
`Wspolne`	100 GB	twardy	wymiana, nie archiwum; twardy limit wymusza sprzątanie

Liczby to propozycja do zatwierdzenia przez właścicieli, dobrana do dysku `D:` 2 TB. Suma limitów może przekraczać dysk, bo limit miękki niczego nie rezerwuje; pilnujemy wolnego miejsca na `D:` osobno w Zabbixie.

Filtry plików

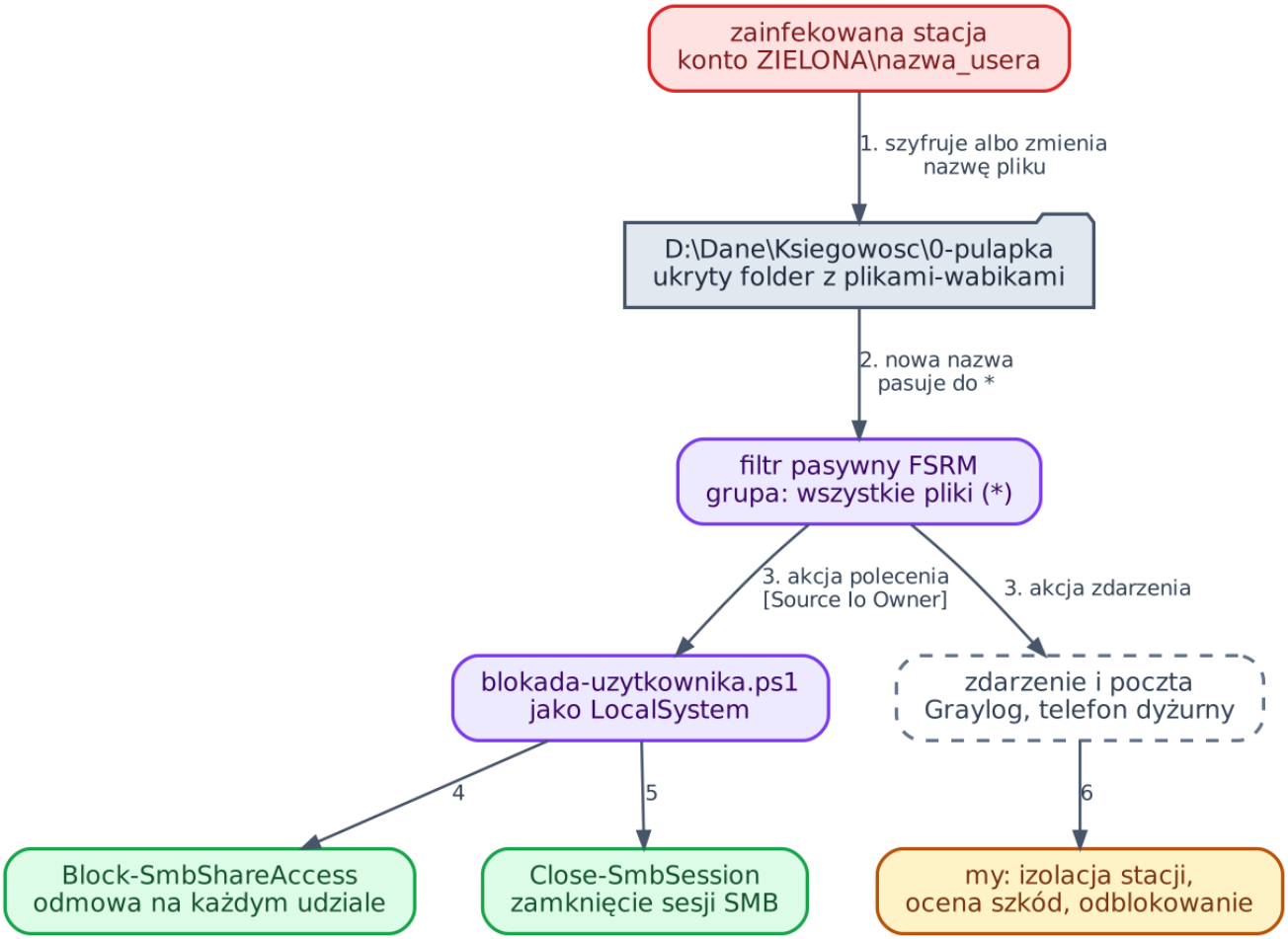
> **Pojęcie: filtr plików (file screen).** Reguła, która patrzy na nazwy zapisywanych plików w folderze. Filtr aktywny nie pozwala zapisać pliku pasującego do grupy, filtr pasywny pozwala, ale uruchamia powiadomienia [8].

> **Pojęcie: grupa plików (file group).** Nazwana lista wzorców nazw, na przykład `*.exe` i `*.msi`, z możliwością wykluczeń [11]. Filtr wskazuje jedną albo kilka grup.

Filtry na rozszerzenia znane z ransomware (`*.locky`, `*.crypt` i setki innych) mają ograniczoną wartość. Listy trzeba stale uzupełniać, a nowsze programy szyfrujące używają losowych rozszerzeń albo w ogóle nie zmieniają nazw. Dlatego zamiast długiej listy rozszerzeń stawiamy pułapkę: folder, w którym żaden człowiek nie ma powodu niczego zapisywać.

Folder pułapka

> **Pojęcie: folder pułapka (honeypot folder).** Folder z plikami-wabikami, którego nikt nie używa, więc każdy zapis w nim jest podejrzany. Program szyfrujący przechodzi przez udział i trafia na wabiki tak samo jak na prawdziwe pliki. FSRM widzi nową nazwę w folderze, uruchamia skrypt, a skrypt odcina konto.



Rysunek 2. Pułapka na ransomware: zainfekowana stacja zmienia plik w folderze pułapce, filtr pasywny FSRM uruchamia skrypt jako LocalSystem, który blokuje konto na każdym udziale i zamyka sesje SMB, a zdarzenie i poczta trafiają do nas (kliknięcie otwiera pełny rozmiar)

Nazwa `0-pulapka` zaczyna się od cyfry, więc w kolejności alfabetycznej stoi przed folderami działu. Część programów szyfruje po kolei, część równolegle albo losowo, więc na kolejność nie liczymy: pułapka skraca szkodę, ale jej nie zeruje. Dlatego obok niej stoją trzy inne warstwy:

1. poprzednie wersje z migawek VSS do szybkiego cofnięcia kilkudziesięciu plików (strona Migawki VSS i poprzednie wersje na fs01: harmonogram, miejsce na różnice i dlaczego to nie jest kopia),
2. kopia w repozytorium tylko do dopisywania na `bkp01` (strona Kopia fs01: restic z migawką VSS do repozytorium pliki i test odtworzenia pliku oraz całego udziału),
3. audyt zapisu na wabikach w Graylogu, który łapie też szyfrowanie bez zmiany nazwy (strona Audyt dostępu do plików na fs01 i kwartalny przegląd uprawnień z właścicielami działów),

4. reguły ASR i ochrona stacji ze strony Polityki ochrony: ochrona nowej generacji, zapora, reguły ASR i kontrolowany dostęp do folderów.

Kontrolowany dostęp do folderów z tej ostatniej strony chroni lokalne foldery stacji (Dokumenty, Pulpit). Szyfrowanie udziału przez zainfekowaną stację dociera do `fs01` jako zapis przez sieć, więc na udziały ta funkcja nie działa tak samo (zachowanie na serwerze plików do potwierdzenia w dokumentacji Defendera).

Czego pułapka nie łapie. Filtr patrzy na nazwy plików, bo grupy plików to wzorce nazw [11]. Pewnie zadziała, gdy program utworzy nowy plik albo zmieni nazwę wabika; czy zadziała przy zapisie nowej treści do istniejącego wabika bez zmiany nazwy, sprawdzamy testem (do potwierdzenia), a na wszelki wypadek łapie to audyt zapisu na wabikach. Skrypt blokuje konto, a nie komputer: jeśli napastnik ma hasło innego konta, pracuje dalej z nim. Odcięcie stacji od sieci i dalsze kroki należą do planu reagowania, który powstanie w książce o wykrywaniu i reagowaniu.

Raporty

> **Pojęcie: raport magazynu (storage report).** Zestawienie zawartości folderów: największe pliki, duplikaty, pliki według właściciela, według grupy plików, najdawniej i najczęściej używane, zajętość limitów [10]. Raport może powstawać według harmonogramu, w odpowiedzi na zdarzenie albo od ręki.

W Zielonej raport miesięczny idzie do nas, a fragmenty trafiają do właścicieli działów przy przeglądzie kwartalnym. Raport „najdawniej używane” traktujemy ostrożnie: na serwerach Windows aktualizacja czasu ostatniego dostępu bywa wyłączona, więc daty mogą być nieaktualne (sprawdzamy `fsutil behavior query disablelastaccess`).

Odpowiednik bez Microsoftu

Funkcja FSRM	Bez Microsoftu	Uwagi
Limity folderów	`quota` i `refquota` na zbiorach danych ZFS, jeden zbiór na dział	limit twardy; ostrzeżenie robimy w Zabbixie z `zfs get used,quota`
Filtry plików	opcja Samby `veto files` dla udziału, na przykład `veto files = /*.exe/*.msi/`	blokuje bez powiadomień; zgłoszenia trzeba zbudować z logów

Funkcja FSRM	Bez Microsoftu	Uwagi
Pułapka z akcją	moduł `vfs_full_audit` Samby wysyła zapisy do sysloga, a reguła w Graylogu na ścieżkę pułapki uruchamia skrypt (na przykład zablokowanie konta w FreeIPA albo w AD)	pętla przez Grayloga trwa dłużej niż akcja FSRM na tym samym serwerze
Raporty	`du`, `ncdu`, raporty Zabbixa, `zfs list -o space`	bez gotowego raportu duplikatów
Nextcloud	limit miejsca na użytkownika i grupę, aplikacje do ochrony przed ransomware w sklepie Nextcloud (stan aplikacji do sprawdzenia przy wdrożeniu)	dotyczy plików w Nextcloud, nie udziałów SMB

Częste błędy

Objaw	Przyczyna	Co robimy
Pułapka uruchomiła się w trakcie jej zakładania	wabiki skopiowane po założeniu filtra	kopiujemy wabiki przed `New-FsrmFileScreen`, a nasze konto odblokowujemy `Unblock-SmbShareAccess`
Drugie konto w tej samej godzinie nie zostało zablokowane	odstęp między uruchomieniami akcji polecenia	`Set-FsrmSetting -CommandNotificationLimit 0` i test z dwoma kontami
Skrypt się nie uruchamia, w dzienniku błąd akcji	zła ścieżka, polityka wykonywania albo brak `-SecurityLevel LocalSystem`	`-ShouldLogError` pokazuje kod błędu w dzienniku, uruchamiamy skrypt ręcznie jako SYSTEM (`psexec -s` albo zadanie zaplanowane)
Pani Halina nie może zapisać poprawki Optimy	filtr aktywny na `*.exe` w `Ksiegowosc`	wyjątek dla jednego folderu na czas aktualizacji, potem usuwamy
Antywirus albo kopia uruchamia pułapkę	narzędzie zapisuje w folderze (plik tymczasowy, strumień)	konto narzędzia na listę `$Wyjatki` w skrypcie, po sprawdzeniu, że naprawdę zapisuje
Limit pokazuje 100%, a nikt nie dostał poczty	brak ustawień SMTP albo poczta odrzucona	`Send-FsrmTestEmail`, sprawdzamy przekazywanie na serwerze pocztowym

□□ Ćwiczenia

1. Dlaczego na pułapce stoi filtr pasywny, a nie aktywny, skoro chcemy zatrzymać szyfrowanie?

Odpowiedź

Bo zatrzymujemy konto, a nie jeden plik. Filtr aktywny zablokowałby tylko zapis w pułapce, a program szyfrujący poszedłby dalej do prawdziwych folderów. Filtr pasywny pozwala na zapis, a jego akcja polecenia odcina konto od wszystkich udziałów naraz.

1. Marek prosi o więcej miejsca, bo dostał pocztę o 85% limitu `Wysylki`. Co sprawdzamy, zanim podniesiemy limit?

Odpowiedź

Raport duplikatów i największych plików dla `D:\Dane\Wysylki` (czy nie leżą tam kopie tych samych skanów), wolne miejsce na `D:` i w puli S2D (strona o pojemności puli) oraz to, czy stare skany nie powinny trafić do archiwum według okresu przechowywania. Limit miękki niczego nie blokuje, więc nie ma pośpiechu.

1. Program szyfrujący zmienia zawartość plików, ale zostawia ich nazwy. Która warstwa go zauważy, skoro filtr pułapki nie zareaguje?

Odpowiedź

Audyt zapisu na wabikach: lista SACL na folderze pułapki zapisuje zdarzenie 4663 z dostępem do zapisu, a reguła w Graylogu podnosi alarm. Do tego Defender na stacji i kopia tylko do dopisywania na `bkp01`, z której odtworzymy pliki.

1. Dlaczego folder `C:\FSRM` ze skryptem blokady ma uprawnienia tylko dla `SYSTEM` i administratorów?

Odpowiedź

Bo FSRM uruchamia skrypt jako LocalSystem. Ktoś, kto mógłby zmienić treść skryptu, a potem zapisać plik w pułapce, wykonałby dowolny kod z najwyższymi uprawnieniami na serwerze plików.

Powiązane: fs01 od środka: maszyna na hvclu01, wolumeny, udziały działów i przestrzeń nazw DFS · Migawki VSS i poprzednie wersje na fs01: harmonogram, miejsce na różnice i dlaczego to nie jest kopia · Audyt dostępu do plików na fs01 i kwartalny przegląd uprawnień z właścicielami działów

· Polityki ochrony: ochrona nowej generacji, zapora, reguły ASR i kontrolowany dostęp do folderów · Graylog: codzienna praca z logami · Zakres i ryzyko w Zielonej: rejestr aktywów, macierz ryzyka i plan postępowania · MailCow: codzienna praca z domenami, skrzynkami i spamem

Źródła (stan na 26.10.2026):

1. learn.microsoft.com: File Server Resource Manager (FSRM) overview (Windows Server 2025, 2022, 2019, 2016; pięć funkcji; dziennik USN i wpisy `SkipUSNCreationForSystem`, `SkipUSNCreationForVolumes`)
2. learn.microsoft.com: Features removed or no longer developed in Windows Server (aktualizacja 24.09.2025; brak FSRM, DFS i kopii w tle na liście; WSUS i WebDAV Redirector nierozwijane)
3. learn.microsoft.com: Create a File Screen Template (Windows Server 2016 do 2025; ustawienia poczty przed powiadomieniami, zakładki E-mail, Dziennik zdarzeń, Polecenie, Raport)
4. learn.microsoft.com: Set-FsrmSetting (`-SmtpServer`, `-AdminEmailAddress`, `-FromEmailAddress`, `-CommandNotificationLimit`, `-EventNotificationLimit`) oraz New-FsrmAction (`-Type Command`, `-SecurityLevel`, `-KillTimeOut`, `-ShouldLogError`, `-RunLimitInterval`)
5. learn.microsoft.com: New-FsrmQuota (`-Size`, `-SoftLimit`, `-Threshold`) i New-FsrmQuotaThreshold
6. learn.microsoft.com: New-FsrmAction, typ `Event` z `-EventType`
7. learn.microsoft.com: Block-SmbShareAccess (wpis odmowy w deskryptorze udziału) i Unblock-SmbShareAccess
8. learn.microsoft.com: New-FsrmFileScreen (`-Active` jako przełącznik, filtr pasywny `-Active:$false`) i opis filtrów aktywnych oraz pasywnych na stronie Create a File Screen Template
9. learn.microsoft.com: [MS-FSRM] File Screen Macros (`[Source Io Owner]`, `[Source File Path]`, `[Source Process Image]`, `[Violated File Group]` i pozostałe)
10. learn.microsoft.com: New-FsrmStorageReport i New-FsrmScheduledTask (typy raportów, `-Schedule`, `-Monthly`, `-MailTo`)
11. learn.microsoft.com: New-FsrmFileGroup (`-IncludePattern`, `-ExcludePattern`)

Revision #2
Created 2026-10-26 14:05:46 UTC by Tomasz Konieczny
Updated 2026-10-26 14:07:12 UTC by Tomasz Konieczny