ARCHIWIZACJA I ODZYSKIWANIE DANYCH W WINDOWS SERVER 2019 I WINDOWS 11

Skuteczne metody zabezpieczania i przywracania informacji

24/02/2025

Wprowadzenie i cele

ZAKRES PREZENTACJI I KONTEKST ćWICZEń CW39/CW40

Archiwizacja i odzyskiwanie danych

Prezentacja omawia kopie zapasowe i odzyskiwanie w Windows Server 2019, uwzględniając Windows 11 jako klienta.

Ćwiczenia laboratoryjne cw39 i cw40

Ćwiczenia obejmują konfigurację backupu, Shadow Copies, harmonogramy i odzyskiwanie kontrolera domeny.

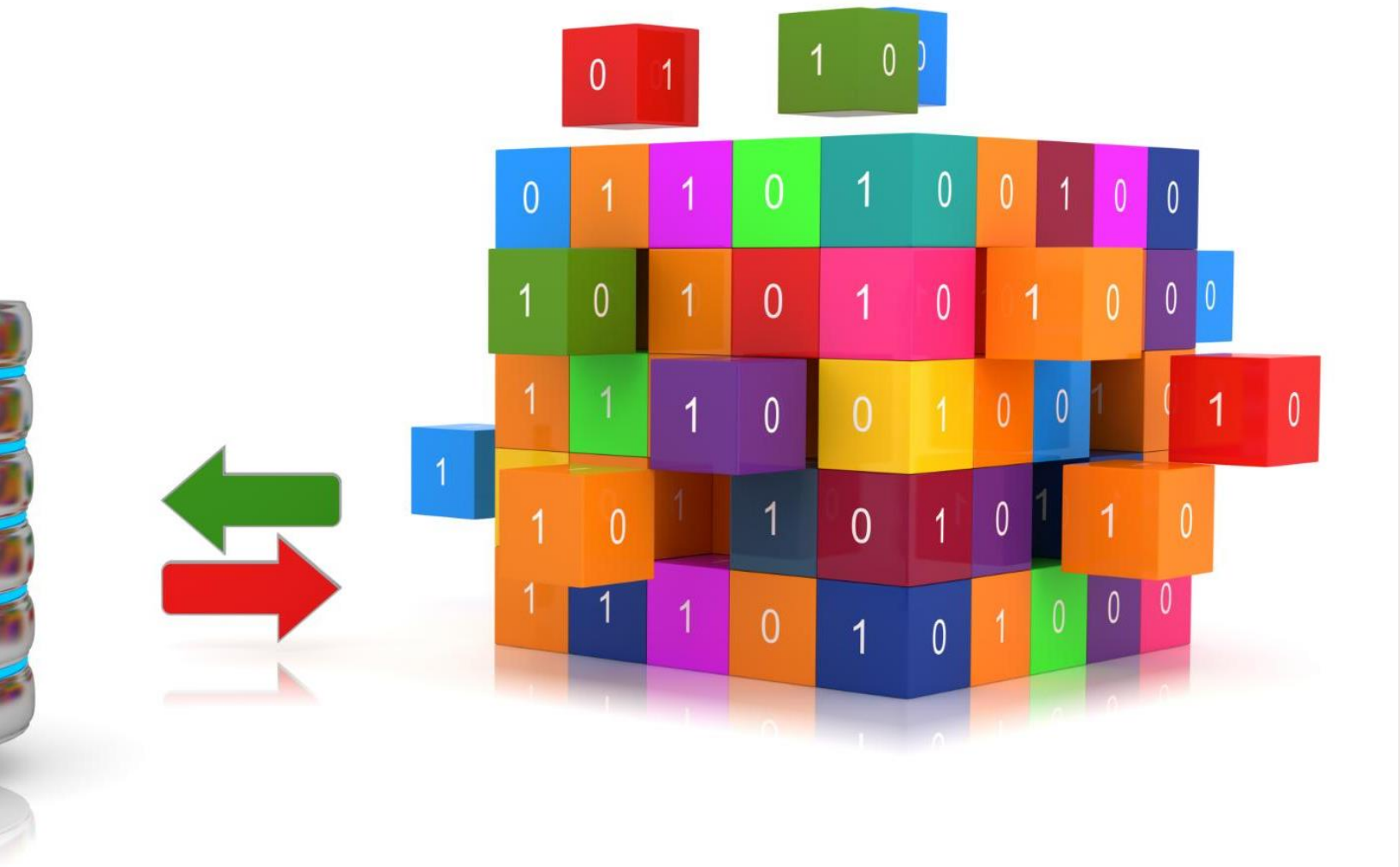
Zarządzanie Active Directory

Kładzie się nacisk na odzyskiwanie spójności bazy katalogowej w środowisku domenowym Active Directory.

Nowoczesne narzędzia systemowe

Omówienie narzędzi Windows Server Backup, wbadmin.exe oraz metod przywracania po awarii.

Podstawowe pojęcia archiwizacji



RÓŻNICE MIĘDZY KOPIĄ ZAPASOWĄ A SHADOW COPIES

Kopia zapasowa – pełna ochrona

Kopia zapasowa służy do odzyskiwania danych po awariach sprzętu i systemu, często wymaga trybu offline.

Shadow Copies – szybkie przywracanie

Shadow Copies pozwalają użytkownikom szybko przywrócić wcześniejsze wersje plików bez przerywania pracy systemu.

Uzupełniające mechanizmy ochrony

Backup i Shadow Copies działają razem, zapewniając zarówno bezpieczeństwo danych, jak i wygodę użytkowników.

Windows Server Backup

MOŻLIWOŚCI NARZĘDZIA WINDOWS SERVER BACKUP

Tworzenie kopii zapasowych

Windows Server Backup umożliwia tworzenie jednorazowych i zaplanowanych kopii zapasowych na pliki, woluminy i cały system.

Odzyskiwanie danych

Narzędzie pozwala na odzyskanie danych na poziomie plików, woluminów oraz całego systemu, zapewniając elastyczność przy przywracaniu.

Elastyczność interfejsu

Windows Server Backup obsługuje zarówno interfejs graficzny, jak i wiersz polecenia, dostosowując się do różnych scenariuszy administracyjnych.

Wymagania instalacyjne

Narzędzie nie jest domyślnie zainstalowane i wymaga doinstalowania funkcji systemowej przed użyciem w środowisku Windows Server.

Kopia stanu systemu

ZAKRES SYSTEM STATE NA KONTROLERZE DOMENY

Zawartość kopii System State

Kopia System State kontrolera domeny obejmuje bazę danych Active Directory, folder SYSVOL, rejestr systemowy i pliki startowe systemu.

Dodatkowe komponenty kopii

System State może zawierać usługi certyfikatów oraz konfigurację IIS, jeśli są zainstalowane na serwerze.

Różnice w odzyskiwaniu danych

Odzyskiwanie System State przywraca strukturę usług katalogowych, nie całe woluminy, w trybie DSRM, unikając niespójności AD.

Zastosowanie System State i Bare Metal

Ćwiczenia uczą, kiedy używać System State, a kiedy pełnego odzyskiwania Bare Metal dla serwera.

Planowanie kopii zapasowych

HARMONOGRAM I ZACHOWANIE DYSKU DOCELOWEGO

Pierwsza konfiguracja dysku

Dysk docelowy jest formatowany tylko podczas pierwszego tworzenia harmonogramu kopii zapasowej.

Zarządzanie starszymi kopiami

Starsze kopie mogą być automatycznie usuwane, ale struktura dysku pozostaje zachowana.

Modyfikacja harmonogramu

Harmonogramy należy zmieniać tylko przez Windows Server Backup lub wbadmin, nie bezpośrednio w Harmonogramie zadań.

Weryfikacja kopii zapasowych

Polecenie wbadmin get versions umożliwia sprawdzenie istnienia wykonanych kopii zapasowych.

Nośniki kopii zapasowych

DOZWOLONE I NIEDOZWOLONE LOKALIZACJE BACKUPU

Dozwolone nośniki backupu

Windows Server Backup obsługuje lokalne dyski, dyski wymienne i wirtualne dyski twarde (VHD) jako miejsca kopii zapasowych.

Niedozwolone lokalizacje backupu

Mapowane napędy sieciowe oraz dysk systemowy i woluminy krytyczne nie mogą być używane jako lokalizacje kopii zapasowej.

Zalety wirtualnych dysków VHD

Wirtualne dyski VHD są przenośne i mogą być łatwo przechowywane oraz transportowane na nośnikach zewnętrznych.

Znaczenie prawidłowej konfiguracji

Zrozumienie zasad wyboru lokalizacji backupu zapobiega błędom i zapewnia bezpieczeństwo danych w Windows Server 2019.

DSRM

DIRECTORY SERVICES RESTORE MODE I JEGO ROLA

Cel trybu DSRM

DSRM umożliwia odzyskanie usług Active Directory bez aktywnej bazy danych, zapobiegając konfliktom replikacyjnym i niespójnościom.

Metody uruchomienia DSRM

Najlepszą metodą wejścia w DSRM jest polecenie bcdedit /set safeboot dsrepair, szczególnie w środowiskach UEFI i wirtualnych maszynach.

Znaczenie hasła DSRM

Hasło DSRM jest kluczowe dla bezpieczeństwa i powinno być okresowo zmieniane, aby chronić kontroler domeny.

Przywrócenie normalnego trybu

Po zakończeniu odzyskiwania należy przywrócić standardowy tryb uruchamiania systemu kontrolera domeny.

Bare Metal Recovery

ODZYSKIWANIE CAŁEGO SERWERA

Procedura Bare Metal Recovery

Odzyskiwanie całego serwera po awarii dysku lub odbudowie maszyny od podstaw.

Środowisko odzyskiwania WinRE

Windows Server 2019 używa WinRE z nośnika instalacyjnego do przeprowadzenia odzyskiwania.

Metody odzyskiwania

Odzyskiwanie można wykonać przez interfejs graficzny lub polecenie wbadmin w wierszu polecenia.

Różnica między odzyskiwaniem systemu

Bare Metal Recovery przywraca cały serwer, różniąc się od odzyskiwania stanu systemu, które nie odtwarza woluminów.

Weryfikacja po odzyskiwaniu

SPRAWDZANIE ACTIVE DIRECTORY PO RESTORE

Weryfikacja jednostek organizacyjnych i użytkowników

Użycie poleceń dsquery ou i dsquery user pozwala potwierdzić obecność jednostek i kont użytkowników w Active Directory po przywróceniu.

Interpretacja wyników restore

Brak nowych obiektów po backupie wskazuje na prawidłowe odtworzenie systemu do stanu z momentu kopii zapasowej.

Kontrola usług katalogowych i replikacji

Należy sprawdzić, czy usługi katalogowe działają poprawnie i nie występują błędy replikacji w środowisku domenowym.

Znaczenie analitycznego podejścia

Proces uczy analizy konsekwencji przywracania danych i rozumienia działania środowiska Active Directory po restore.

Windows 11 jako klient

ROLA WINDOWS 11 W SCENARIUSZACH TESTOWYCH

Rola klienta systemu Windows 11

Windows 11 pełni rolę stacji klienckiej, nie wykonując kopii zapasowych serwera.

Testowanie dostępu i wersji plików

System testuje dostęp do udziałów sieciowych, Shadow Copies i funkcji „Poprzednie wersje” plików.

Samodzielne przywracanie plików

Użytkownicy mogą sami przywracać pliki bez udziału administratora, wzmacniając ochronę danych.

Testy odzyskiwania Active Directory

Windows 11 umożliwia testowanie odzyskiwania Active Directory z perspektywy klienta w środowisku domenowym.

Wnioski i pytania

WNIOSKI UCZNIÓW I PYTANIA KONTROLNE

Przywracanie stanu systemu

Przywracanie systemu odtwarza stan z momentu wykonania kopii zapasowej, bez przywracania późniejszych obiektów.

Różnice między backupem a Shadow Copies

Backup i Shadow Copies to różne mechanizmy, każde z odmiennego zastosowania w ochronie danych.

Tryb DSRM i odzyskiwanie Active Directory

Tryb DSRM jest niezbędny do bezpiecznego przywrócenia kontrolera domeny Active Directory.

Pytania kontrolne i utrwalenie wiedzy

Pytania kontrolne utrwalają wiedzę o Shadow Copies, DFSR, obsłudze kont i audycie zmian katalogowych.