Kopie bezpieczeństwa Windows serwer 2019

Cel ogólny lekcji: jest zapoznanie uczestników z procesem tworzenia kopii bezpieczeństwa w systemie Windows Server 2019 oraz zasadami ich przywracania, aby umożliwić skuteczną ochronę danych przed utratą i zapewnić ciągłość działania systemu. Zapoznanie uczniów z mechanizmem kopii bezpieczeństwa Windows serwer 2019 oraz narzędziem Kopia zapasowa systemu Windows Server (Windows Server Backup) do ochrony katalogu.

Cele szczegółowe lekcji:

1. Zapoznanie z podstawowymi pojęciami związanymi z tworzeniem kopii bezpieczeństwa w systemie Windows Server 2019.
2. Przedstawienie różnych metod tworzenia kopii bezpieczeństwa, w tym metod przy użyciu narzędzi wbudowanych w system.
3. Omówienie procesu przywracania kopii bezpieczeństwa w systemie Windows Server 2019.
4. Przedstawienie najlepszych praktyk związanych z tworzeniem kopii bezpieczeństwa i przywracaniem danych w systemie Windows Server 2019.
5. Zaznajomienie uczestników z procedurami testowania i weryfikowania kopii bezpieczeństwa w celu upewnienia się, że są one gotowe do użycia w przypadku awarii systemu.
6. Wyjaśnienie, jakie czynniki wpływają na wybór właściwej strategii tworzenia kopii bezpieczeństwa i jakie zagrożenia należy uwzględnić podczas tworzenia i przywracania kopii bezpieczeństwa.
7. Zapewnienie, że uczestnicy lekcji będą mieli wystarczające umiejętności i wiedzę, aby skutecznie tworzyć i przywracać kopie bezpieczeństwa w systemie Windows Server 2019.
8. Wyjaśnienie, czym jest mechanizm Kopie w tle folderów udostępnionych (Shadow Copies of Shared Folders) w systemie Windows 2019 oraz jak działa.
9. Omówienie możliwości odzyskiwania danych za pomocą Shadow Copies of Shared Folders oraz ich wpływu na wydajność działania woluminu.
10. Wyjaśnienie, jak konfigurować ustawienia kopii w tle dla poszczególnych woluminów oraz jakie harmonogramy można ustawić.
11. Omówienie problemów związanych z przestrzenią magazynową i maksymalnym rozmiarem kopii w tle.
12. Wyjaśnienie, jak korzystać z narzędzia Kopia zapasowa systemu Windows Server do ochrony katalogu oraz jakie są korzyści wynikające z takiego rozwiązania.
13. Porównanie korzyści i wad przywracania danych z kopii zapasowej oraz z kontenera z usuniętymi danymi.
14. Wyjaśnienie, jak przywracać dane z kopii zapasowej i jakie atrybuty są przywracane jednocześnie z danymi.
15. Omówienie ryzyk związanych z przywracaniem obiektów w AD DS i wyjaśnienie, jak uniknąć błędów podczas tej operacji.

Zalecam przypomnieć sobie materiał z klasy pierwszej z teorii dotyczący Typy kopii bezpieczeństwa, strategie tworzenia kopii bezpieczeństwa.

1. Kopia bezpieczeństwa w systemie Windows Server 2019.

Kopia bezpieczeństwa to proces tworzenia kopii danych z systemu w celu ochrony przed utratą danych w przypadku awarii sprzętu lub programów, ataków hakerskich lub innego rodzaju awarii systemu. W systemie Windows Server 2019 kopia bezpieczeństwa jest bardzo ważna, ponieważ zapewnia ochronę przed utratą danych biznesowych lub prywatnych.

2. Narzędzia i metody do tworzenia kopii bezpieczeństwa w systemie Windows Server 2019.

Aby utworzyć kopię bezpieczeństwa w systemie Windows Server 2019, można skorzystać z narzędzi wbudowanych, takich jak Windows Server Backup lub innych narzędzi dostępnych na rynku. Można wykorzystać także rozwiązania chmurowe, takie jak Azure Backup lub Amazon Web Services.

a) **Windows Server Backup** jest wbudowanym narzędziem do tworzenia kopii bezpieczeństwa na serwerach Windows Server 2019. Umożliwia ono tworzenie kopii zapasowych danych systemowych, plików, katalogów, dysków i woluminów. Można także ustawić harmonogram tworzenia kopii zapasowych i skonfigurować, gdzie mają być przechowywane kopie bezpieczeństwa.

Windows Server Backup pozwala na tworzenie kopii bezpieczeństwa danych systemowych, plików, katalogów, dysków i woluminów. Umożliwia ono wybór zarówno typu kopii zapasowej, jak i miejsca, w którym mają być przechowywane kopie. Narzędzie pozwala na automatyczne tworzenie kopii zapasowych według ustalonego harmonogramu.

Windows Server Backup oferuje kilka różnych sposobów tworzenia kopii zapasowych:

1. Kopie pełne zawierają wszystkie dane.
2. Kopie różnicowe zawierają zmiany od ostatniej kopii pełnej.
3. kopie przyrostowe zawierają zmiany od ostatniej kopii pełnej lub ostatniej kopii przyrostowej.

Windows Server Backup pozwala na:

1. tworzenie harmonogramów kopii zapasowych, dzięki czemu można ustawić regularne wykonywanie kopii według określonego harmonogramu (np. codziennie o określonej godzinie).
2. wykonywanie kopii na różne nośniki, takie jak dyski zewnętrzne, taśmy magnetyczne lub sieciowe urządzenia przechowujące dane.
3. umożliwia tworzenie kopii zapasowych na różnych nośnikach, takich jak dyski zewnętrzne, taśmy i napędy sieciowe.
4. skonfigurowanie backupu w chmurze.
5. szyfrowanie kopii zapasowych, aby zapewnić większe bezpieczeństwo danych.

Zastosowania Windows Server Backup:

1. zapewnienie ciągłości działania biznesu w przypadku awarii systemu lub utraty danych. Dzięki regularnym kopiom zapasowym można szybko przywrócić utracone dane i przywrócić normalne funkcjonowanie firmy.
2. migracja danych i systemu operacyjnego na nowy sprzęt.
3. dzięki backupowi można łatwo przenieść cały system operacyjny i dane na nowy serwer bez utraty żadnych informacji.

W skrócie, Windows Server Backup jest niezbędnym narzędziem dla administratorów serwerów, którzy chcą zapewnić bezpieczeństwo danych i ciągłość działania firmy. Narzędzie pozwala na tworzenie kopii zapasowych różnego typu i umożliwia automatyczne tworzenie kopii według harmonogramu.
Można także skonfigurować backup w chmurze, aby zapewnić większe bezpieczeństwo danych.

Kroki niezbędne do wykonania kopii bezpieczeństwa w systemie Windows Server 2019:

1. Uruchom konsolę Zarządzanie komputerem.
2. Kliknij na zakładkę Magazyn.
3. Kliknij na opcję Zarządzanie kopiami zapasowymi.
4. Wybierz opcję Utwórz zadanie kopii zapasowej.
5. Wybierz, czy chcesz wykonać pełną kopię systemu, czy tylko wybrane pliki i foldery.
6. Wybierz, gdzie chcesz zapisać kopię zapasową.
7. Wybierz harmonogram kopii zapasowej (np. codziennie, co tydzień itp.).
8. Skonfiguruj dodatkowe opcje kopii zapasowej, takie jak kryptowanie danych czy kompresja plików.
9. Uruchom kopię zapasową, klikając na przycisk Uruchom.
10. Monitoruj postęp kopii zapasowej i upewnij się, że została zakończona pomyślnie.

Po wykonaniu tych kroków będziesz miał kopię zapasową swojego systemu lub wybranych plików i folderów, co zwiększy poziom bezpieczeństwa Twoich danych i umożliwi ich odtworzenie w przypadku awarii.

b) Narzędzie zewnętrzne do tworzenia kopii bezpieczeństwa **Veeam Backup & Replication**, które oferuje zaawansowane funkcje, takie jak szyfrowanie danych, kopie bezpieczeństwa na poziomie aplikacji i odzyskiwanie wirtualnych maszyn.

Veeam Backup & Replication to oprogramowanie służące do tworzenia kopii bezpieczeństwa i replikacji danych w środowiskach wirtualizacyjnych. Pozwala na automatyczne tworzenie kopii bezpieczeństwa wirtualnych maszyn (VM) oraz odzyskiwanie danych w przypadku awarii lub utraty danych.

Jedną funkcjonalności Veeam Backup & Replication jest szyfrowanie danych, co zapewnia bezpieczeństwo przechowywanych kopii bezpieczeństwa. W przypadku krytycznych aplikacji, które wymagają wysokiego poziomu bezpieczeństwa, Veeam Backup & Replication oferuje opcję kopii bezpieczeństwa na poziomie aplikacji. Dzięki temu możliwe jest przywrócenie jednej konkretnej aplikacji bez konieczności przywracania całego środowiska.

Veeam Backup & Replication umożliwia tworzenie replikacji danych, co pozwala na szybkie przywracanie usług w przypadku awarii sprzętu lub oprogramowania.
Replikacja może odbywać się w czasie rzeczywistym lub z określonym opóźnieniem czasowym.

Oprogramowanie oferuje funkcję Instant VM Recovery, dzięki której możliwe jest szybkie przywrócenie wirtualnych maszyn bez konieczności oczekiwania na pełne przywrócenie danych.
Dzięki temu czas przywracania usług zostaje zminimalizowany.

Veeam Backup & Replication jest oprogramowaniem dedykowanym dla środowisk wirtualizacyjnych, w szczególności dla platformy VMware vSphere i Microsoft Hyper-V. Dzięki temu można łatwo zarządzać kopiami bezpieczeństwa i replikacją danych w całym środowisku wirtualizacyjnym z jednego miejsca.

c) rozwiązania chmurowe: Microsoft Azure Backup lub Amazon Web Services (AWS) Backup, które umożliwiają tworzenie kopii bezpieczeństwa w chmurze.

Azure Backup pozwala na tworzenie kopii bezpieczeństwa danych z serwerów w chmurze Microsoft Azure, a także na kopie bezpieczeństwa aplikacji, wirtualnych maszyn i bazy danych SQL Server.

Dzięki temu narzędziu można zapewnić ochronę danych przed utratą z powodu awarii sprzętu, ataków cybernetycznych, błędów użytkowników czy innego rodzaju zagrożeń. Azure Backup umożliwia łatwe przywracanie danych z kopii bezpieczeństwa, co pozwala na szybką i skuteczną reakcję w przypadku utraty danych. Dodatkowo, narzędzie to oferuje elastyczne opcje tworzenia harmonogramów kopii bezpieczeństwa oraz możliwość monitorowania statusu backupów w czasie rzeczywistym.

AWS Backup oferuje funkcje tworzenia kopii bezpieczeństwa dla różnych usług AWS, takich jak EC2, EBS, RDS, DynamoDB i Storage Gateway.

AWS Backup oferuje automatyczne zarządzanie cyklem życia kopii bezpieczeństwa, co umożliwia automatyczne usuwanie kopii, które są już niepotrzebne, a także automatyczne tworzenie nowych kopii zgodnie z określonym harmonogramem. AWS Backup pozwala na łatwe przywracanie kopii bezpieczeństwa w przypadku awarii, błędu ludzkiego lub innego problemu z systemem. Wszystkie kopie bezpieczeństwa są przechowywane w chmurze AWS, co zapewnia bezpieczeństwo i niezawodność procesu tworzenia kopii zapasowych.

d) Odzyskiwania danych

Warto zwrócić uwagę na to, że tworzenie kopii bezpieczeństwa to tylko jedna z części strategii zabezpieczeń danych. Ważne jest także **regularne testowanie odzyskiwania danych z kopii bezpieczeństwa**, aby upewnić się, że proces odzyskiwania działa prawidłowo w przypadku awarii systemu.

3. Przywracanie dane z kopii bezpieczeństwa w systemie Windows Server 2019.

Aby przywrócić dane z kopii bezpieczeństwa w systemie Windows Server 2019, należy wybrać odpowiednią kopię, a następnie zainstalować system operacyjny na serwerze, na którym ma zostać przywrócona kopia. Po zainstalowaniu systemu należy skonfigurować jego ustawienia, a następnie przywrócić kopię danych.

W celu przywrócenia kopii bezpieczeństwa można wykorzystać wbudowane narzędzia systemowe, takie jak Windows Server Backup lub wbudowane narzędzie przywracania systemu.

Oto kroki, które należy wykonać:

1. Otwórz narzędzie Windows Server Backup lub wbudowane narzędzie przywracania systemu.
2. Wybierz opcję "Przywróć" lub "Restore" w zależności od używanego narzędzia.
3. Wybierz odpowiednią kopię bezpieczeństwa, która ma zostać przywrócona.
4. Wybierz dysk lub partycję, na której ma zostać przywrócona kopia.
5. Wybierz opcję "Przywróć" lub "Restore" i potwierdź operację.
6. Odczekaj, aż proces przywracania zostanie zakończony.
7. Skonfiguruj ustawienia systemu, jeśli jest to wymagane.
8. Przetestuj przywróconą kopię, aby upewnić się, że wszystkie dane zostały przywrócone poprawnie.

W przypadku większych lub bardziej skomplikowanych kopii bezpieczeństwa, warto rozważyć wykorzystanie specjalistycznego oprogramowania do przywracania danych.

4. Czynniki które uwzględnić podczas tworzenia i przywracania kopii bezpieczeństwa w systemie Windows Server 2019, takie jak

a) pojemność dysków,

b) prędkość i stabilność sieci,

c) a także czas potrzebny na tworzenie i przywracanie kopii bezpieczeństwa.

Proces tworzenia i przywracania kopii bezpieczeństwa może wpłynąć na wydajność systemu.

Dlatego ważne jest, aby wykonywać te czynności w dogodnym czasie dla użytkowników i w taki sposób, aby minimalizować wpływ na pracę systemu.

Podczas tworzenia kopii bezpieczeństwa należy także zadbać o odpowiednie przechowywanie danych. Najlepiej jest przechowywać kopie na osobnych dyskach lub w chmurze, aby zapewnić ochronę przed utratą danych w przypadku awarii systemu lub dysku.

Podczas przywracania kopii bezpieczeństwa należy pamiętać, że proces ten może spowodować utratę danych, które zostały zapisane od czasu utworzenia kopii. Dlatego przed przywracaniem kopii należy wykonać kopię aktualnych danych, aby móc je przywrócić w razie potrzeby.

Podsumowując, tworzenie i przywracanie kopii bezpieczeństwa w systemie Windows Server 2019 wymaga uwzględnienia wielu czynników i należy to robić w sposób odpowiedzialny i zgodny z zasadami bezpieczeństwa danych.

4. Najlepsze praktyki związane z tworzeniem i przywracaniem kopii bezpieczeństwa w systemie Windows Server 2019 oraz jak je wdrożyć.

Najlepsze praktyki związane z tworzeniem i przywracaniem kopii bezpieczeństwa w systemie Windows Server 2019 obejmują regularne tworzenie kopii zapasowych, przechowywanie kopii na różnych nośnikach, takich jak dyski zewnętrzne lub w chmurze, a także testowanie procesu przywracania kopii. Aby wdrożyć te praktyki, można skorzystać z automatyzacji procesu tworzenia kopii bezpieczeństwa i wykorzystać narzędzia, takie jak PowerShell.

Ważne jest, aby upewnić się, że kopie zapasowe są przechowywane w bezpiecznym miejscu i są zabezpieczone przed dostępem osób nieuprawnionych. W przypadku kopii zapasowych przechowywanych w chmurze, ważne jest, aby wybrać dostawcę, który oferuje wysoki poziom bezpieczeństwa i prywatności danych.

Zwróć uwagę na czas trwania procesu tworzenia kopii zapasowych, aby uniknąć przeciążenia systemu i zapewnienia ciągłości działania usług. W przypadku systemów krytycznych, należy także rozważyć wdrożenie rozwiązań wykorzystujących replikację danych i automatyczne przełączanie na kopię zapasową w przypadku awarii.

Pamiętaj, że tworzenie i przywracanie kopii zapasowych jest jednym z najważniejszych elementów zapewnienia bezpieczeństwa systemu i danych. Regularne monitorowanie i aktualizowanie procesu tworzenia i przywracania kopii zapasowych jest kluczowe dla zapewnienia ciągłości działania systemu oraz szybkiego i skutecznego przywrócenia danych w przypadku awarii.

5. Kopie w tle folderów udostępnionych

Mechanizm Kopie w tle folderów udostępnionych (Shadow Copies of Shared Folders) w systemie Windows 2019 umożliwia łatwe odzyskiwanie danych, redukując konieczność interwencji administratora. Dzięki temu rozwiązaniu można odzyskać usunięte, zmienione lub uszkodzone pliki użytkownika bez konieczności używania dodatkowych narzędzi. Shadow Copies of Shared Folders wykonuje migawki plików przechowywanych w udostępnionych folderach, a czas tworzenia migawek określa harmonogram.

Domyślnie system Windows 2019 wykonuje kopie w tle we wszystkie dni powszednie o 07:00 rano i po północy, ale dla jednego woluminu możemy zastosować wiele harmonogramów. Możemy włączyć i wyłączyć Shadow Copies dla każdego woluminu oddzielnie oraz zmienić jego ustawienia.

Jeśli chcesz zmniejszyć wpływ funkcji Shadow Copies of Shared Folders na wydajność działania woluminu, możesz zapisywać kopię danych na oddzielnym woluminie. W przypadku woluminów, na których wykonywane są reglanie operacje zapisu i odczytu, takich jak udział, takie rozwiązanie może okazać się korzystne.

Jeśli na woluminie brakuje miejsca, usługa automatycznie usuwa najstarsze kopie, aby uwolnić miejsce. Niezależnie od wielkości dostępnej przestrzeni, na jednym woluminie nie będzie przechowywanych więcej niż 64 kopie w tle.

Podczas planowania harmonogramu musisz wziąć pod uwagę wpływ częstotliwości tworzenia kopii na okres przechowywania danych. W przypadku dostępnej odpowiedniej przestrzeni harmonogram tworzący kopie w każdy poniedziałek, środę i piątek przechowa je przez 21 tygodni. Domyślne ustawienia spowodują usuwanie najstarszych kopii w tle po 6 tygodniach od ich utworzenia.

Przy planowaniu wdrożenia funkcji Shadow Copies of Shared Folders w systemie Windows 2019 należy pamiętać, że ustawienia konfiguruje się osobno dla każdego woluminu.
Przestrzeń magazynowa, maksymalny rozmiar i harmonogramy dla różnych woluminów nie mają ze sobą nic wspólnego. Jeśli w danym środowisku jeden wolumin zawiera jeden udział, możesz zoptymalizować ustawienia kopii w tle w oparciu o sposób wykorzystywania danych, zamiast jednego kompromisowego rozwiązania dla różnych udziałów.

6. Wykorzystywanie narzędzia Kopia zapasowa systemu Windows Server (Windows Server Backup) do ochrony katalogu.

Korzystanie ze specjalnych narzędzi do uzyskiwania dostępu do usuniętych danych w katalogu, nie zawsze zapewnia najlepszą metodę odzyskiwania danych.
Obiekty przywracane z kontenera z usuniętymi danymi nie zawierają wszystkich swoich pierwotnych atrybutów. Należy wiedzieć, jaka zawartość atrybuty były przypisane do obiektu przed jego usunięciem, aby być w stanie przywrócić go do swojego pierwotnego stanu.
Gdy przywracamy dane z kopii zapasowej i ponownie przypisujemy je do katalogu, to przywracamy wszystkie atrybuty obiektu jednocześnie i nie musimy ponownie przypisywać atrybutów, takich jak członkostwa w grupach, itd. Oszczędza to czas po tym, jak obiekt zostanie przywrócony, ale wymaga bardziej skomplikowanej operacji do wykonywania przywracania.

Przywracanie obiektów w AD DS było ryzykowną operacją w poprzednich wersjach systemu Windows Server, ponieważ:

- niemożliwe było przeglądanie obiektów w zestawie danych z kopii zapasowej przed jej przywróceniem,
- było i nadal pozostaje niemożliwe przywracanie różnych zestawów kopii zapasowych do różnych kontrolerów domeny i podglądanie zawartych w nich danych.

System Windows Server 2019 zawiera narzędzie montowania bazy danych AD DS, dzięki któremu można podejrzeć zestaw danych kopii zapasowej przed operacją przywracania.
To narzędzie może zaoszczędzić czas, gdy należy przywrócić obiekt i pomóc w odzyskaniu właściwej wersji obiektu.

Tworzenie i przywracanie kopii zapasowej Active Directory, umożliwia:

- wykonanie kopii zapasowej całego serwera, w tym jego systemu operacyjnego,
- wykonanie kopii zapasowej tylko danych o stanie systemu, które zawierają dane konfiguracyjne serwera, jak magazyn katalogu Ntds.dit,
- przywracanie danych nieautorytatywnych - dane, które będą dodane do kontrolera domeny, ale zostaną zaktualizowane przez replikacje z wieloma wzorcami, gdy kontroler domeny zostanie z powrotem przyłączony do sieci,
- przywracanie danych nieautorytatywnych - dane, które będą dodane do kontrolera domeny, ale będą aktualizować dane na wszystkich innych kontrolerach domeny przez replikację z wieloma wzorcami, gdy kontroler domeny zostanie z powrotem przyłączony do sieci,
- wykonanie konfigurowania kontrolerów domeny przez instalowanie z nośnika, które opiera się na kopii bazy Ntds.dit z innego kontrolera domeny w celu ograniczania replikacji wymaganej do utworzenia kontrolera domeny podczas instalacji.

Sposoby wykorzystywania zestawów danych kopii zapasowych podczas pracy z kontrolerami domeny w systemie Windows Server 2019:

- Kopie zapasowe są wykonywane przez program Kopia zapasowa systemu (Windows Server Windows Server Backup) lub odpowiadające mu narzędzie wiersza polecenia Wbadmin.exe. Oba te narzędzia są funkcjami systemu Windows Server 2019 i muszą zostać dodane do serwera, aby stały się dostępne. Nie są instalowane domyślnie.

- Kopie zapasowe nie są rozczłonkowane, przechwytują krytyczne woluminy w całości.
  Na kontrolerze domeny do krytycznych woluminów należą:

  Wolumin systemowy.
  Wolumin rozruchowy.
  Wolumin przechowujący udział SYSVOL.
  Wolumin przechowujący bazę danych AD DS.
  Wolumin przechowujący dzienniki AD DS.

- Kopie zapasowe mogą być zautomatyzowane lub ręczne.

- Kopie zapasowe nie mogą być wykonywane na napędach taśmowych albo woluminach dynamicznych, a tylko na napędach sieciowych, wymiennych dyskach twardych skonfigurowanych jako woluminy podstawowe albo na płytach DVD i CD.

- Nie można tworzyć kopii zapasowych pojedynczych plików. Program Windows Server Backup (Kopia zapasowa systemu Windows Server) obsługuje tylko tworzenie kopii zapasowych pełnych woluminów.

- Jeśli chcemy zabezpieczyć tylko dane o stanie systemu, musimy użyć narzędzia wiersza polecenia Ntdsutil.exe.

- Operatorzy kopii zapasowych nie mogą tworzyć zaplanowanych kopii zapasowych tylko członkowie lokalnej grupy Administratorzy (Administrators) mają ten przywilej w systemie Windows Server 2019. W większości przypadków oznacza to bycie członkiem grupy Administratorzy domeny (Domain Admins) na kontrolerach domeny.

- Jeśli serwer jest wyłączony, należy skorzystać z lokalnej kopii środowiska Windows Recovery Environment (WinRE) do przywrócenia systemu. Środowisko WinRE może być albo zainstalowane lokalnie, albo można je znaleźć na nośniku instalacyjnym systemu Windows Server 2019.

Rekomendacje przy budowaniu kontrolerów domeny, aby były łatwiejsze do odzyskiwania:

- Uruchamiać kontrolery domeny jako osobne serwery i nie dodawać do nich innych ról, z wyjątkiem roli DNS Server (Serwer DNS).

- Uruchamiać kontrolery domeny jako maszyny wirtualne przy użyciu techniki Hyper-V w systemie Windows Server 2019. Kontrolery domeny są idealnymi kandydatami do użycia w Hyper-V, ponieważ przede wszystkim wymagają przepustowości sieciowej i możliwości przetwarzania do zarządzania logowaniami. Nawet jeśli domena zawiera tysiące użytkowników i charakteryzuje się dużym użyciem procesora podczas głównych okresów logowania, na przykład rano i po przerwie obiadowej, można je wirtualizować i przypisywać im więcej zasobów.

- Nie przechowywać żadnych innych danych na kontrolerze domeny, można zastosować osobne woluminy dla bazy danych i dzienników kontrolera domeny.
  Jeśli baza danych AD DS zawiera dużą liczbę obiektów.

- Przekształcić nośnik instalacyjny systemu Windows w plik ISO i udostępnić go hostom Hyper-V, tak aby był dostępny, gdy należało będzie przywrócić kontroler domeny.

Jeśli nie, to należy zainstalować WinRE na każdym tworzonym kontrolerze domeny.
W tym celu potrzebny nam będzie dostęp do zestawu Windows Automated Installation Kit (WAIK).

- Wykonywać regularne, zautomatyzowane kopie zapasowej swoich kontrolerów domeny.
  Mogą być one tworzone na dedykowanym woluminie podstawowym albo mapowanym napędzie sieciowym.

- Dobrze chronić hasło trybu odzyskiwania usług katalogowych. To hasło musi być używane do przywracania danych w kontrolerze domeny, a ponieważ jest hasłem uprzywilejowanym, to musi być cały czas chronione.

7. Praca z stanem systemu

Na serwerze, na którym działa rola AD DS, do danych o stanie systemu należą następujące dane:

- rejestr,
- baza rejestracji klas com+,
- pliki rozruchowe,
- pliki systemowe, które są objęte ochroną zasobów systemu Windows,
- baza danych usług active directory domain services (usługi domenowe w usłudze active directory),
- katalog sysvol.

Gdy inne role serwera są zainstalowane w systemie, stan systemu będzie zawierał pierwsze cztery wymienione wcześniej obiekty i następujące pliki:

- dla roli Uslugi certyfikatów w usłudze Active Directory (Active Directory Certificate Services): bazę danych AD CS,
- dla funkcji klastra pracy awaryjnej: informacje o usłudze klastra,
- dla roli serwera WVWV: Pliki konfiguracyjne IIS.

Informacje o stanie serwera są ważne, nie mogą być przechwytywane przez program Kopia zapasowa systemu Windows Server (Windows Server Backup). Mogą być przywracane, ponieważ Kopia zapasowa systemu Windows Sewer (Windows Server Backup) obsługuje trzy tryby przywracania:

- pełne przywracanie serwera,
- przywracanie tylko stanu systemu,
- przywracanie pojedynczego pliku lub foldera.

Każdy tryb umożliwia odzyskanie potrzebnych w danym momencie informacji.

Kopie zapasowe generowane przez program Kopia zapasowa systemu Windows Server (Windows Server Backup) są zawsze tworzone do tego samego pliku i dodawane do zawartości pliku w miarę wykrywania zmian w systemie źródłowym.

Za każdym razem, gdy generowana jest kopia zapasowa, tworzony jest nowy plik katalogu.

Ten plik katalogu jest używany do wyszukiwania danych dla określonej kopii zapasowej.