KAPITEL 2

Entwerfen und Implementieren von Netzwerkinfrastrukturdiensten

Eine Netzwerkinfrastruktur besteht aus Basisdiensten wie DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System) und IP-Adressverwaltung (Internet Protocol). Windows Server 2012 stellt all diese Dienste zur Verfügung. Eine Neuerung in Windows Server 2012 ist ein Dienst namens IP-Adressverwaltung (IP Address Management, IPAM). Mithilfe von IPAM kann eine Organisation die Adressen ihres gesamten Netzwerks zentral verwalten und überwachen.

Prüfungsziele in diesem Kapitel:

Prüfungsziel 2.1: Entwerfen und Warten einer DHCP-Lösung

DHCP (Dynamic Host Configuration Protocol) stellt Geräten in einem Netzwerk IP-Adressen und andere Netzwerkkonfigurationsdaten zur Verfügung. Die meisten Clients und Clientgeräte in einem Unternehmen erhalten ihre Netzwerkdaten über DHCP.

Dieses Prüfungsziel behandelt die folgenden Themen:

- Entwurfsaspekte, zum Beispiel eine hoch verfügbare DHCP-Lösung mit geteiltem Bereich, DHCP-Failover, DHCP-Failovercluster, DHCP-Interoperabilität und DHCPv6
- Implementieren der DHCP-Filterung
- Implementieren und Konfigurieren eines DHCP Management Packs
- Warten einer DHCP-Datenbank

Entwerfen einer hoch verfügbaren DHCP-Lösung

DHCP ist ein wichtiger Dienst im Netzwerk einer großen Organisation. Ohne DHCP gelingt es Clients nicht, IP-Adressen und Daten wie die Adressen von DNS-Servern abzurufen. Aus diesem Grund wird DHCP in vielen Unternehmen hoch verfügbar bereitgestellt. Wenn ein Server ausfällt, übernimmt ein anderer seine Aufgaben. Dieser Abschnitt beschreibt, welche Aspekte beim Entwurf einer hoch verfügbaren Lösung für DHCP wichtig sind.

Weitere Informationen Terminologie und Grundlagen des DHCP-Entwurfs

Dieser Abschnitt konzentriert sich auf den DHCP-Entwurf in großen Organisationen und setzt voraus, dass Sie wissen, wie DHCP funktioniert, wie es bereitgestellt und verwaltet wird. Unter *http://technet.microsoft.com/library/dd283016* finden Sie weitere Informationen über DHCP, darunter eine Einführung in die Terminologie und den grundlegenden Entwurf.

Eine Lösung für hoch verfügbares DHCP verfolgt zwei Ziele:

- Der DHCP-Dienst soll ohne Unterbrechungen zur Verfügung stehen
- Wenn ein DHCP-Server ausfällt, sollen die Clients in der Lage sein, ihre Lease von einem anderen DHCP-Server verlängern zu lassen

Wenn Sie eine hoch verfügbare DHCP-Lösung entwerfen, haben Sie die Wahl zwischen geteilten DHCP-Bereichen und Failoverclustern.

Geteilte Bereiche

Bei einem geteilten DHCP-Bereich stellen zwei Server Adress- und Netzwerkdaten für einen Teil des Adressraums oder DHCP-Bereichs zur Verfügung. Wenn zum Beispiel eine Organisation ihren Clients Adressen aus dem Subnetz 192.168.100.0/24 zuweist, ist ein geteilter DHCP-Bereich sinnvoll, bei dem der eine Server 80 Prozent der Adressen vergibt und ein anderer Server die restlichen 20 Prozent. Das wird als »80/20-Regel« für die DHCP-

Bereichszuweisung bezeichnet. Manche Organisationen stellen den Server, der 80 Prozent des Bereichs vergibt, näher bei den Clients auf. Sie brauchen allerdings nicht die Zahl der Adressen auszurechnen, die bei der 80/20-Aufteilung zugewiesen werden müssen. Der *Assistent zur Konfiguration geteilter DHCP-Bereiche* enthält einen Schritt, in dem Sie die Aufteilung komfortabel konfigurieren können (Abbildung 2.1).

Abbildung 2.1 Konfigurieren eines geteilten Bereichs im *Assistenten zur Konfiguration geteilter DHCP-Bereiche*

Mit einem geteilten Bereich können Sie den Verkehr auf die beteiligten Server verteilen, aber dennoch Redundanz für den Fall sicherstellen, dass einer der beiden Server ausfällt. Die Clients übernehmen allerdings die erste DHCP-Antwort, die bei ihnen eintrifft, daher können Sie nicht garantieren, welcher Server einem Client seine DHCP-Daten zuweist. Wenn die Server in unterschiedlichen Subnetzen liegen, müssen Sie einen Router als DHCP-Relay-Agent konfigurieren und eine Verzögerung an dieser Stelle einbauen, damit der sekundäre Server nicht schneller antwortet als der primäre Server. Im *Assistenten zur Konfiguration geteilter DHCP-Bereiche* können Sie eine solche Verzögerung für einen der Server im geteilten Bereich einstellen (Abbildung 2.2).

Abbildung 2.2 Eine definierte Verzögerung für einen geteilten Bereich hilft sicherzustellen, dass die Clients Netzwerkdaten vom vorgesehenen Server erhalten

Stattdessen können Sie eine Verzögerung auch im Bereich selbst konfigurieren. Diese Einstellung nehmen Sie im Eigenschaftendialogfeld des Bereichs auf der Registerkarte *Erweitert* vor (Abbildung 2.3).

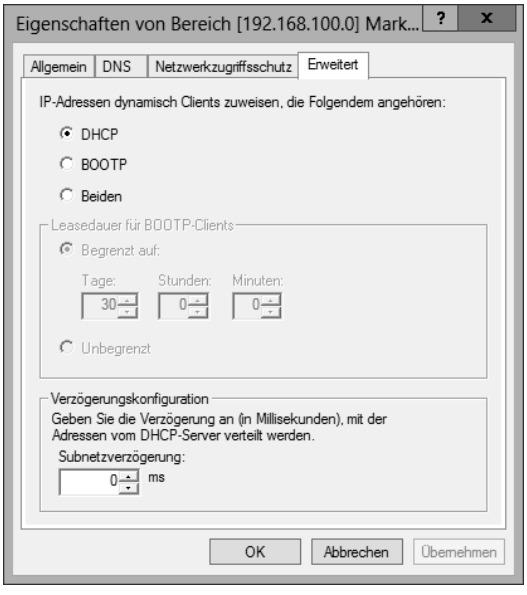

Abbildung 2.3 Konfigurieren einer Verzögerung für die Antwort eines DHCP-Servers in einem geteilten Bereich

Hinweis Geteilte Bereiche

Geteilte Bereiche stehen nur für IPv4 zur Verfügung.

DHCP-Failover

Beim DHCP-Failover, einer neuen Funktion in Windows Server 2012, werden zwei Server in derselben DHCP-Konfiguration eingerichtet. Windows Server 2012 stellt zwei DHCP-Failovermodi zur Auswahl: Hot-Standby und Lastenausgleich. Diese DHCP-Failovermodi unterscheiden sich von Failoverclustern, die weiter unten in diesem Prüfungsziel besprochen werden.

Hinweis Zwei Knoten

DHCP-Failover ist auf zwei Knoten beschränkt.

Jeder Server, der am DHCP-Failover beteiligt ist, verwaltet eine replizierte Version des gesamten Bereichs mit allen Leaseinformationen. Das bedeutet, dass jeder Server Adressen für den gesamten Bereich vergeben kann. Weil Bereichs- und Leasedaten repliziert werden, sind zwei Betriebsmodi möglich. Im Hot-Standby-Modus vergibt ein Server die DHCP-Daten, während der andere eine replizierte Version der DHCP-Leaseinformationen verwaltet und somit bereitsteht, beim Ausfall des primären Servers jederzeit dessen Aufgaben zu übernehmen. Im Lastenausgleichsmodus vergeben beide Server parallel DHCP-Daten an Clients und aktualisieren die gemeinsam genutzte Datenbank mit Leasedaten.

Der Hot-Standby-Modus eignet sich für Organisationen, die Remotestandorte mit DHCP-Clients haben. Diese Konfiguration wird oft als sternförmige Topologie (hub-and-spoke topology) bezeichnet. Der DHCP-Server im Remotestandort ist der primäre Server und ein Server im zentralen Rechenzentrum dient als Ersatz. Fällt der primäre Server im Remotestandort aus, übernimmt der sekundäre Server im Rechenzentrum seine Aufgaben. Die Einteilung in primären und sekundären Server geschieht auf Ebene des Subnetzes, nicht im Bereich selbst. Das bedeutet, dass ein Server gleichzeitig der primäre DHCP-Server für ein Subnetz und der sekundäre DHCP-Server für ein anderes Subnetz sein kann.

Der Lastenausgleichsmodus wird meist in Rechenzentren oder Szenarien mit zentralisiertem DHCP genutzt, wo zwei Server im selben Standort laufen. Im Lastenausgleichsmodus vergeben beide Server DHCP-Daten an Clients, wobei sie sich die Arbeit prozentual aufteilen. Den Prozentwert für die Lastverteilung legen Sie bei der Konfiguration fest (Abbildung 2.4).

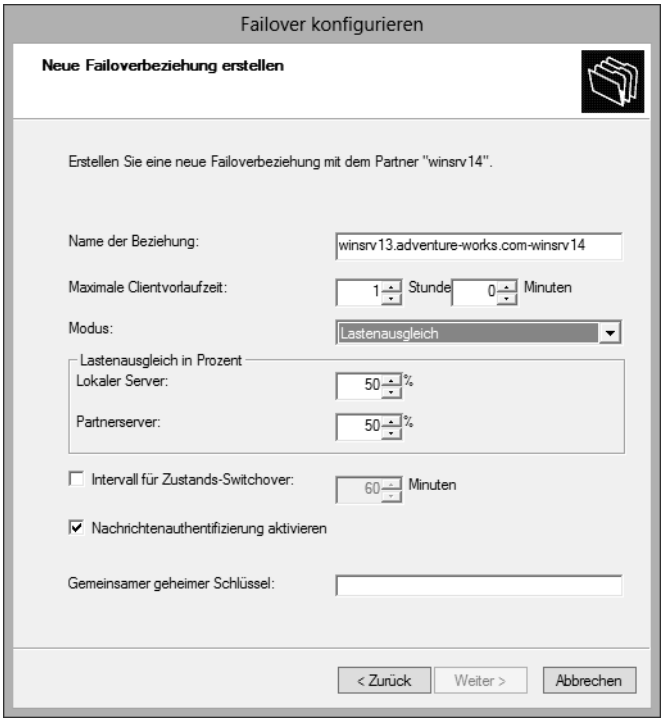

Abbildung 2.4 Konfigurieren des Prozentwerts für die Lastverteilung beim DHCP-Failover

Später können Sie den Prozentwert für die Lastverteilung jederzeit auf einem der Partnerserver ändern.

Hinweis Einschränkungen

DHCP-Failover ist auf IPv4-Bereiche und -Konfigurationen beschränkt.

DHCP-Failovercluster

Failovercluster sind eine Redundanzarchitektur, die bereits in älteren Versionen als Windows Server 2012 zur Verfügung stand. Bei einem Failovercluster vergibt der primäre DHCP-Server die DHCP-Daten, der sekundäre Server übernimmt beim Ausfall des primären Servers dessen Aufgaben. In diesem Fall greifen die DHCP-Server auf denselben Massenspeicher zu, daher kann bei einem Defekt des Massenspeichers das gesamte System lahmgelegt werden.

Weitere Informationen Failovercluster

Unter *http://technet.microsoft.com/library/ee405263* finden Sie weitere Informationen zu Failoverclustern.

DHCP-Interoperabilität

Im Bereich von DHCP bezieht sich der Begriff *Interoperabilität* (interoperability) meist auf die Beziehung zwischen DHCP und anderen Microsoft-Technologien wie Routing und Remotezugriff, Netzwerkzugriffsschutz (Network Access Protection, NAP) oder Active Directory-Domänendiensten (Active Directory Domain Services, AD DS). Die Interoperabilität zwischen der Microsoft-DHCP-Implementierung und DHCP-Implementierungen anderer Hersteller ist damit seltener gemeint.

DHCP-Clients können bei der Adresszuweisung dynamisch DNS-Einträge registrieren. Damit das funktioniert, braucht der DHCP-Server Zugriff auf einen Domänencontroller. Außerdem muss der DHCP-Server autorisiert sein, solche Einträge in DNS zu erstellen. Sie konfigurieren diese Einstellungen auf der Registerkarte *DNS* im Eigenschaftendialogfeld eines Bereichs (Abbildung 2.5).

Abbildung 2.5 Einstellungen für dynamische DNS-Aktualisierungen in einem DHCP-Bereich

Der DHCP-Server kann sowohl die PTR- (Zeiger) als auch A-Einträge (Hostadressen) eines Clients aktualisieren. Für diese Aufgabe wird die DHCP-Option 81 (Client-FQDN) verwendet. Option 81 enthält den vollqualifizierten Domänennamen (Fully-Qualified Domain Name, FQDN) und andere Daten des Clients. Wie in Abbildung 2.5 zu sehen, können Sie den Server so konfigurieren, dass er die DNS-Einträge immer oder nur auf Anforderung des Clients aktualisiert. Ältere Clients, die die DHCP-Option 81 nicht senden, werden ebenfalls unterstützt, wenn Sie auf dieser Registerkarte das Kontrollkästchen *DNS-A- und -PTR-Einträge für DHCP-Clients, die keine Aktualisierung anfordern (z.B. Clients, die Windows NT 4.0 ausführen), dynamisch aktualisieren* aktivieren.

DHCP-Interoperabilität mit AD DS wird normalerweise genutzt, um zusätzliche DHCP-Server im Netzwerk zu erkennen und zu autorisieren. DHCP-Server, die unter Windows laufen, können in AD DS autorisiert werden. Sie können verhindern, dass unautorisierte Server IP-Adressen an Clients vergeben. Dieses Autorisierungsschema funktioniert aber nur bei DHCP-Servern, die unter Windows 2000 oder neuer laufen, also nicht für Linux-DHCP-Server oder Netzwerkgeräte.

DHCP kann mit NAP zusammenarbeiten, um den Clientzugriff einzuschränken, sofern der Client nicht bestimmte Voraussetzungen erfüllt. Abbildung 2.6 zeigt, wie Sie im Eigenschaftendialogfeld eines Bereichs die NAP-Konfiguration vornehmen.

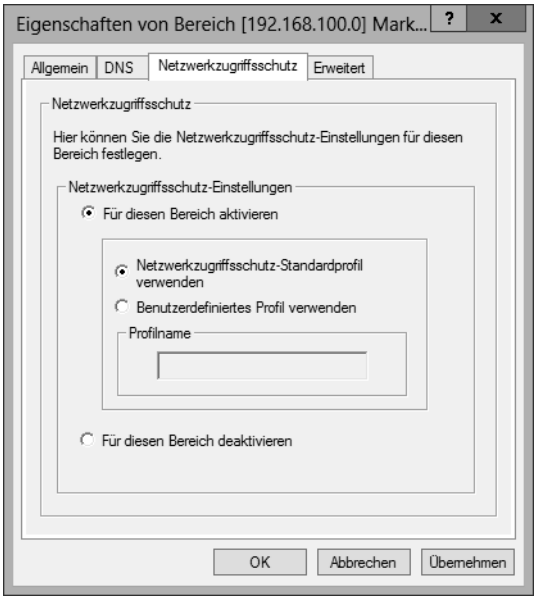

Abbildung 2.6 Einstellungen für den Netzwerkzugriffsschutz in einem DHCP-Bereich

Sie können NAP auf Ebene eines bestimmten Bereichs konfigurieren oder für alle Bereiche eines Servers.

Weitere Informationen Arbeiten mit NAP

Weitere Informationen über NAP finden Sie unter *http://technet.microsoft.com/de-de/library/cc730902*.

DHCPv6

DHCP für IPv6 kann in einem zustandslosen (stateless) oder in einem statusbehafteten (stateful) Modus arbeiten. Im statusbehafteten Modus erhalten die Clients sowohl ihre Adresse als auch zusätzliche Daten wie ihre DNS-Server vom DHCP-Server. Dagegen übernehmen die

Clients im zustandslosen Modus nur Daten wie die DNS-Server, während sie ihre Adresse über die automatische Konfiguration von IPv6 oder als statische IP-Adresse erhalten.

Implementieren der DHCP-Filterung

Mit der DHCP-Filterung, auch als *Verbindungsschichtfilterung* (link-layer filtering) bezeichnet, können Sie festlegen, welche Anforderungen nach Adress- und Netzwerkdaten der DHCP-Server beantwortet. Der DHCP-Server sendet die Daten dann nur an bekannte Clients oder verweigert bestimmten Clients die Daten. Das ist vor allem in Rechenzentren wichtig, wo Sie wahrscheinlich genau kontrollieren wollen, welche Geräte im Netzwerk erlaubt sind.

Die DHCP-Filterung arbeitet mit MAC-Adressen (Media Access Control), die der DHCP-Client zusammen mit seiner DHCP-Anforderung übermittelt. Windows Server 2012 bietet zwei Filtertypen an: Zulassen und Verweigern. Ein Zulassen-Filter sendet Netzwerkdaten nur an die Clients, die im Filter aufgelistet sind. Ein Verweigern-Filter verhindert dagegen, dass die aufgelisteten Clients Daten vom DHCP-Server erhalten.

Wenn Sie mit Zulassen-Filtern arbeiten, müssen Sie jede autorisierte MAC-Adresse in den Filter eintippen, andernfalls erhält der entsprechende Computer keine Daten vom DHCP-Server. Natürlich ist das kein Problem, wenn Sie dem Client eine statische Adresse zuweisen.

Windows Server 2012 ermöglicht die Filterung mit der vollständigen MAC-Adresse oder mit Platzhaltern. Alle folgenden Beispiele sind gültige Filter:

- 00-11-09-7c-ef-57
- 00-11-09-7c-ef-*
- 00-11-09-*-*-*
- 0011097cef57

Mithilfe von Platzhaltern können Sie eine Gruppe identischer Geräte oder alle Geräte eines bestimmten Herstellers zulassen oder verbieten. Sie brauchen dann nicht jede MAC-Adresse einzeln einzutippen, wenn eine ganze Gruppe von Geräten dasselbe MAC-Präfix hat.

Sie konfigurieren die DHCP-Filterung im MMC-Snap-In *DHCP*. Um eine gefilterte Adresse hinzuzufügen, klicken Sie mit der rechten Maustaste auf den Knoten *Zulassen* oder *Verweigern* (je nachdem, welchen Filtertyp Sie konfigurieren wollen) und geben dann die MAC-Adresse ein (Abbildung 2.7).

Abbildung 2.7 Erstellen eines DHCP-Filters

Wenn Sie die MAC-Adressen für Filter eingegeben haben, müssen Sie die Filter des jeweiligen Typs (Zulassen oder Verweigern) insgesamt aktivieren. Klicken Sie dazu im MMC-Snap-In *DHCP* mit der rechten Maustaste auf *Zulassen* beziehungsweise *Verweigern* und wählen Sie den Befehl *Aktivieren*. Sie können Filter auch auf der Ebene des Bereichs aktivieren.

Implementieren und Konfigurieren eines DHCP Management Packs

Das DHCP Management Pack ist in der Operations Manager-Komponente von Microsoft System Center 2012 enthalten. Es ermöglicht die erweiterte Protokollierung und Überwachung der DHCP-Umgebung. Zum Beispiel können Sie mit dem DHCP Management Pack die Verfügbarkeit des DHCP-Diensts, den Filterstatus und den Status von Bereichen überwachen, um zu verhindern, dass in einem Bereich die Adressen ausgehen.

Um ein DHCP Management Pack zu implementieren, brauchen Sie Microsoft System Center 2012. Das DHCP Management Pack wird in Operations Manager importiert. Es wird empfohlen, ein neues Management Pack zu erstellen, das Sie nach Ihren Wünschen individuell konfigurieren können, ohne die Originalversion des DHCP Management Packs verändern zu müssen.

Tabelle 2.1 beschreibt einige Szenarien für die Überwachung einer DHCP-Infrastruktur.

Tabelle 2.1 Szenarien für die DHCP-Überwachung

Überwachte Objekte	Beschreibung
Die Server selbst	Überwacht die Verfügbarkeit des Dienstes und erkennt unautorisierte DHCP-Server
DHCP-Bereiche	Überwacht, ob in einem Bereich die Adressen knapp werden
DHCP-Datenbank	Überwacht, ob bei der Datenbank Probleme auftreten
Leistung	Überwacht unter anderem, ob sehr viele Anforderungen eintreffen, die Warteschlange sehr lang wird oder viele Adressen vergeben sind

Weitere Informationen DHCP Management Pack

Unter *http://technet.microsoft.com/library/cc180306.aspx* finden Sie weitere Informationen über das DHCP Management Pack.

Warten einer DHCP-Datenbank

Zur Wartung einer DHCP-Datenbank gehört das Sichern und Wiederherstellen der Datenbank. Den Speicherort der Datenbank und ihrer Datensicherung konfigurieren Sie im Eigenschaftendialogfeld des DHCP-Servers (Abbildung 2.8).

Abbildung 2.8 Konfigurieren des Speicherorts für DHCP-Datenbank und der zugehörigen Datensicherung

Sie können die DHCP-Datenbank in der Konsole *DHCP* sichern oder wiederherstellen, indem Sie den Knoten des gewünschten Servers auswählen. Außerdem können Sie einstellen, in welchem Zeitabstand automatisch eine Datensicherung ausgeführt wird. Die Standardeinstellung sind 60 Minuten, aber Sie können den Wert *BackupInterval* im Registrierungspfad *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DHCPServer\Parameters* ändern.

Weitere Informationen Komprimieren mit Jetpack

Sie können die DHCP-Datenbank auch mit Jetpack komprimieren. Unter *http://technet.microsoft.com/library/hh875589* finden Sie weitere Informationen.

Falls bei den Clientadressen Inkonsistenzen zwischen der Zusammenfassung und den Detailinformationen auftreten, haben Sie die Möglichkeit, die Datenbank neu abzustimmen. Wählen Sie dazu auf Adresstypebene (*IPv4* oder *IPv6*) den Befehl *Alle Bereiche abstimmen* oder auf Bereichsebene den Befehl *Abstimmen*.

Gedankenexperiment Entwerfen einer DHCP-Topologie

Im folgenden Gedankenexperiment wenden Sie an, was Sie über dieses Prüfungsziel wissen. Die Antworten auf die Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Ein Remotestandort, der über WAN (Wide Area Network) angebunden ist, enthält 150 Clients, denen Adressdaten zugewiesen werden müssen. Ein zentrales Rechenzentrum liefert bereits DHCP-Daten für 350 Clients.

Beschreiben Sie, welche DHCP-Topologie sich für dieses Szenario eignet. Erläutern Sie, ob Sie eine Failoverarchitektur implementieren sollten und welchen Typ sie haben sollte.

Zusammenfassung des Prüfungsziels

- Die Rolle *DHCP-Server* in Windows Server 2012 bietet Redundanz durch geteilte Bereiche, Failover im Hot-Standby- oder Lastenausgleichsmodus und Failovercluster
- Beim Hot-Standby-Failover kann ein Server die Aufgaben eines ausgefallenen Partnerservers übernehmen
- Beim Lastenausgleich-Failover vergeben beide Server DHCP-Daten
- In einem Failovercluster sind beide Server in der Lage, DHCP-Daten zuzuweisen, weil sie auf dieselbe DHCP-Datenbank an einem freigegebenen Speicherort zugreifen
- Bei der DHCP-Filterung legen Sie mithilfe von Verbindungsschicht-MAC-Adressen fest, welchen Clients der Server antwortet
- Das DHCP Management Pack, eine Komponente im System Center Operations Manager, ermöglicht die Überwachung des DHCP-Dienstes und die Erstellung von Berichten
- Die DHCP-Datenbank wird im Dateisystem gespeichert und muss gelegentlich abgestimmt werden, um veraltete Einträge zu aktualisieren

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Themen überprüfen, die in diesem Prüfungsziel behandelt wurden. Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Sie konfigurieren einen geteilten DHCP-Bereich auf zwei Servern. Welche prozentuale Verteilung wird für diese DHCP-Konfiguration empfohlen?

   A. 60/40

   B. 70/30

   C. 80/20

   D. 50/50

2. Welches sind gültige MAC-Filter in Windows Server 2012? (Wählen Sie alle richtigen Antworten aus. Sie dürfen davon ausgehen, dass die MAC-Adressen selbst gültig sind.)
   A. 00-11-09-*-*-*
   B. 001109001111
   C. 00:11:09:09:11:09
   D. 00-11-09-7c-ef-%
3. Sie wollen die DHCP-Datenbank verschieben. Sie verwenden die Standardeinstellungen für Windows-Verzeichnisse und Programmpfade und haben den Pfad der DHCP-Datenbank bisher nicht geändert. In welchem Pfad liegt die DHCP-Datenbank in der Standardeinstellung?
   A. *C:\Windows\system32\dhcp*
   B. *C:\Program Files\Microsoft\DHCP\Data*
   C. *C:\Windows\system32\DHCP\Data*
   D. *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DHCP*
4. Sie implementieren einen geteilten Bereich. Nach einiger Zeit stellen Sie fest, dass der sekundäre Server auf viele DHCP-Anforderungen zuerst antwortet. Wie können Sie dieses Problem am besten lösen?
   A. Verändern Sie den Teilungsprozentsatz so, dass der sekundäre Server mehr IP-Adressen aus dem Bereich erhält.
   B. Legen Sie in der Konsole *DHCP* eine Verzögerung für DHCP-Angebote vom sekundären Server fest.
   C. Verringern Sie die Last des primären Servers, damit er schneller reagieren kann.
   D. Legen Sie den sekundären DHCP-Server in ein anderes Netzwerksegment, damit er später antwortet.

Prüfungsziel 2.2: Entwerfen einer Namensauflösungsstrategie

Die Namensauflösung arbeitet normalerweise mit DNS (Domain Name System), kann aber auch WINS (Windows Internet Name Service) umfassen. Dieses Prüfungsziel konzentriert sich auf den Entwurf einer Lösung, nicht auf die eigentliche Implementierung.

Dieses Prüfungsziel behandelt das folgende Thema:

- Entwurfsaspekte, zum Beispiel sichere Namensauflösung, DNSSEC, DNS-Socketpool, Cachesperrung, separate Namespaces, DNS-Interoperabilität, Migration auf Anwendungspartitionen, IPv6, Auflösung von DNS-Namen mit einer einzigen Bezeichnung, Zonenhierarchie und Zonendelegierung

Entwerfen einer Namensauflösungsstrategie

Wenn Sie eine komplexe Namensauflösungsstrategie für eine große Organisation entwerfen, gilt es mehrere Aspekte zu beachten. Sie sollten einerseits der Sicherheit einen hohen Stellenwert einräumen und andererseits eine zuverlässige und robuste Infrastruktur für Ihre Organisation bereitstellen. Windows Server 2012 stellt mehrere Funktionen zur Verfügung, die Ihnen helfen, eine robuste und zuverlässige Lösung zu entwickeln.

Neben den Funktionen, die Windows Server 2012 für eine robuste und zuverlässige Namensauflösung zur Verfügung stellt, sollten Sie für die Prüfung auch mit DNS vertraut sein. Dazu gehört, dass Sie Details des DNS-Protokolls kennen und die Tools und Konzepte beherrschen, mit denen DNS in einer großen Organisation implementiert wird. Viele dieser Tools und Konzepte sind schon älter und werden nicht direkt in den Prüfungszielen aufgelistet. Als Unternehmensadministrator wird von Ihnen aber erwartet, dass Sie mit wichtigen Protokollen wie DNS vertraut sind.

Weitere Informationen Informationsquellen

Tabelle 2.2 enthält Links auf TechNet-Seiten zu diesen Konzepten. Sie sollten aber zusätzliche Informationsquellen über DNS heranziehen, die über das hinausgehen, was in dieser Tabelle und den Prüfungszielen aufgeführt ist.

Tabelle 2.2 Informationsquellen für DNS-Konzepte

Konzept	Weitere Informationen
Bedingte Weiterleitung	*http://technet.microsoft.com/library/0104be3c-0405-4455-b011-6950875c0446*
DNS-Zonentypen	*http://technet.microsoft.com/library/cc771898*
Aufstellungsorte für DNS-Server	*http://technet.microsoft.com/library/cc737361*
Problembehandlung bei DNS	*http://technet.microsoft.com/library/cc753041*
Technische Referenz für DNS	*http://technet.microsoft.com/library/dd197461*

Sichere Namensauflösung

Um eine sichere Namensauflösung bereitzustellen, müssen Sie unter anderem den Namenserver und den DNS-Dienst selbst wirksam schützen. Die Registerkarte *Erweitert* im Eigenschaftendialogfeld eines DNS-Servers enthält mehrere Kontrollkästchen, die für eine sichere Namensauflösung relevant sind (Abbildung 2.9).

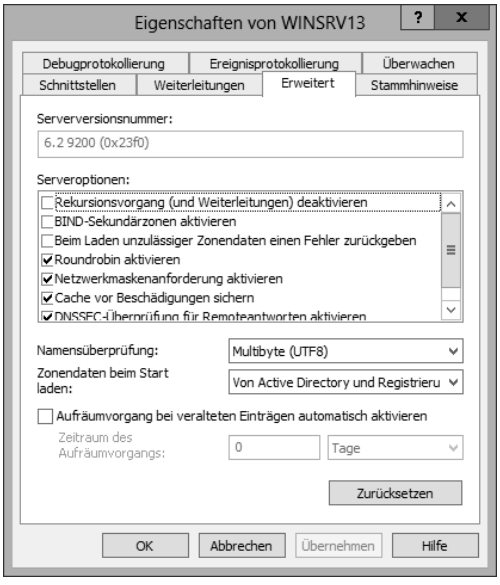

Abbildung 2.9 Erweiterte DNS-Eigenschaften für den DNS-Serverdienst

Eine der Optionen, die für die DNS-Sicherheit wichtig sind, ist *Cache vor Beschädigungen sichern*, die den Quellport für Anforderungen nach dem Zufallsprinzip auswählt, und *DNSSEC-Überprüfung für Remoteantworten aktivieren*, das im nächsten Abschnitt beschrieben wird.

Es gibt weitere Entwurfsaspekte, die Sie in Ihrer Namensauflösungsstrategie berücksichtigen sollten. Sofern Clients externe DNS-Namen auflösen, zum Beispiel Namen von Internethosts, können Sie eine Gruppe von DNS-Servern in der Gesamtstruktur-Stammdomäne so konfigurieren, dass sie Abfragen an externe DNS-Server oder mithilfe von Stammhinweisen weiterleiten. Dann konfigurieren Sie die Server in allen untergeordneten Domänen so, dass sie ihre Abfragen an die Server in der Gesamtstruktur-Stammdomäne weiterleiten.

Dieses Konzept machen Sie sich zunutze, wenn Sie auf einem untergeordneten DNS-Server die Rekursion deaktivieren. Sie können die Rekursion für DNS-Server deaktivieren, die für DNS-Zonen autorisierend sind, aber keine allgemeine DNS-Auflösung für Clients in ihrem Netzwerk zur Verfügung stellen. Ein gutes Beispiel ist ein Unternehmen, in dem die Domänencontroller von den DNS-Servern getrennt sind, die von den Clients für normale Internetnamensauflösung genutzt werden. In einem solchen Szenario sollte die Rekursion auf den Domänencontrollern deaktiviert werden. Wenn Ihre Domäne beide Typen der Namensauflösung nutzt, ist es wahrscheinlich sinnvoll, den DNS-Namespace zwischen externen und internen Server zu trennen.

Zonenübertragungen sollten Sie standardmäßig deaktivieren und nur für ausgewählte Hosts zulassen.

DNSSEC

Das in den RFCs 4033, 4034 und 4035 definierte DNSSEC (DNS Security Extensions) erweitert DNS um Sicherheitsfunktionen. Windows Server 2012 verbessert die Unterstützung für DNSSEC. DNSSEC definiert neue Ressourceneinträge und ermöglicht Datenintegrität, Ursprungsautorität und authentifizierte Angaben zur Nichtexistenz. DNSSEC basiert auf einer Kryptografie mit öffentlichen Schlüsseln. Die Clients erhalten dabei kryptographisch signierte Antworten auf ihre Abfragen. Eine Antwort ist mit dem öffentlichen Schlüssel des Servers signiert, daher kann der Client sicherstellen, dass die Antwort gültig ist und nicht manipuliert wurde.

DNSSEC kann auch gesamte Zonen signieren. Dazu dient in Windows Server 2012 das Tool *Dnscmd.exe*. In Windows Server 2012 ist es nun möglich, DNSSEC in Active Directory-integrierten Zonen mit dynamischen Aktualisierungen bereitzustellen. In älteren Windows-Versionen wurde diese Möglichkeit für DNSSEC nicht unterstützt.

DNSSEC baut eine Vertrauenskette auf, deren Ursprung, der sogenannte Vertrauensanker (trust anchor) in der Stammzone liegt. Damit wird eine Vertrauenskette erzeugt, die bestätigt, dass Antworten vertrauenswürdig sind. Wenn Sie den Einsatz von DNSSEC planen, müssen Sie daher die Position für den Vertrauensanker festlegen. Das bedeutet auch, dass Sie nicht nur die Gültigkeit einzelner Ressourceneinträge überprüfen, sondern auch den Server als den tatsächlich autorisierenden Server bestätigen können.

Eine signierte Zone enthält neben den normalen DNS-Einträgen für eine Zone RRSIG-, DNSKEY- und NSEC-Einträge. NSEC liefert authentifizierte Angaben zur Nichtexistenz für DNS. Windows Server 2012 unterstützt NSEC und NSEC3, eine erweiterte Version des Standards. NSEC3 hilft dabei, das Ausspähen einer Zone zu verhindern, bei dem Angreifer wiederholte Abfragen über eine Zone sendet, um potenzielle Ziele aufzuspüren.

Weitere Informationen Bereitstellen von DNSSEC

Eine Schritt-für-Schritt-Anleitung zum Bereitstellen von DNSSEC finden Sie unter *http://technet.microsoft.com/library/hh831411*.

DNS-Socketpool

Der DNS-Socketpool wechselt die Ports für Abfragen zufällig durch, um Cachevergiftungsangriffe zu erschweren. Das Sicherheitsupdate MS08-037 aktiviert diese Funktion als Standardeinstellung, in Windows Server 2012 ist sie ebenfalls standardmäßig aktiviert. Der DNS-Socketpool verwendet unterschiedliche Quellports für ausgehende Abfragen.

Sie können sowohl die Zahl der verwendeten Quellports als auch ausgeschlossene Portbereiche für ausgehende Abfragen konfigurieren. Leider ist keine Möglichkeit vorgesehen, diese Funktion über die grafische Benutzeroberfläche zu steuern, daher müssen Sie für diese Konfiguration das Tool Dnscmd verwenden oder direkt die Registrierung bearbeiten.

Weitere Informationen Konfigurieren des DNS-Socketpools

Unter *http://technet.microsoft.com/library/ee649174.aspx* finden Sie weitere Informationen darüber, wie Sie den Socketpool konfigurieren.

Cachesperrung

Die Cachesperrung (cache locking) bietet eine weitere Möglichkeit, eine Cachevergiftung zu verhindern. Die Cachesperrung verhindert, dass zwischengespeicherte Antworten überschrieben werden, bevor ein bestimmter Teil ihrer TTL (Time to Live) abgelaufen ist. Sie konfigurieren die Cachesperrung als Prozentsatz der TTL. Wenn zum Beispiel die TTL 3600 Sekunden beträgt und Sie für die Cachesperrung 50 Prozent einstellen, können die zwischengespeicherten Werte die ersten 1800 Sekunden lang nicht überschrieben werden. Sie können die Cachesperrung im Registrierungsschlüssel *CacheLockingPercent* oder mit dem Tool Dnscmd konfigurieren.

Weitere Informationen Konfigurieren der Cachesperrung

Unter *http://technet.microsoft.com/library/ee649148.aspx* ist beschrieben, wie Sie die Cachesperrung konfigurieren.

Separate Namespaces

Bei einem separaten Namespace (disjoint namespace) unterscheidet sich die Active Directory-Domäne vom DNS-Domänensuffix. Zum Beispiel bilden das DNS-Suffix *corp.adventure-works.com* und die Active Directory-Domäne *int.corp.adventure-works.com* separate Namespaces. Domänenmitglieder registrieren Ressourceneinträge in der Domäne, in der sie Mitglied sind, im beschriebenen Beispiel also in *int.corp.adventure-works.com*. Der Domänencontroller registriert dann sowohl globale als auch standortsspezifische Diensteinträge (SRV) in der DNS-Domäne. Die SRV-Einträge werden ebenfalls in die *_msdcs*-Zone gelegt.

Separate Namespaces werden eingesetzt, wenn Geschäftsregeln vorschreiben, dass der Namespace getrennt werden muss. Sie sollten aber alle Anwendungen testen, die Sie in einem separaten Namespace nutzen wollen, denn möglicherweise setzen sie voraus, dass Domänen- und DNS-Suffix übereinstimmen. In einem solchen Fall könnte es zu Problemen kommen. Separate Namespaces verursachen außerdem höheren Administrationsaufwand, weil Sie die DNS- und die Active Directory-Informationen von Hand synchron halten müssen.

Die folgenden Konfigurationen unterstützen separate Namespaces:

- Eine Active Directory-Gesamtstruktur, die mehrere Domänen umfasst, aber nur einen DNS-Namespace oder eine DNS-Zone
- Eine einzelne Active Directory-Domäne, die in mehrere DNS-Zonen untergliedert ist

Dagegen funktioniert ein separater Namespace nicht in den folgenden Konfigurationen:

- Wenn ein Suffix einer Active Directory-Domäne in der aktuellen oder einer anderen Gesamtstruktur entspricht
- Wenn eine Zertifizierungsstelle, die Domänenmitglied ist, ihr DNS-Suffix ändert

DNS-Interoperabilität

Die Microsoft-Implementierung von DNS ist zu allen relevanten DNS-RFCs kompatibel, daher ist Interoperabilität mit anderen Servern möglich. Wenn Sie im Eigenschaftendialogfeld eines DNS-Servers auf der Registerkarte *Erweitert* das Kontrollkästchen *BIND-Sekundärzonen aktivieren* wählen, ermöglichen Sie die Zusammenarbeit zwischen dem Windows-DNS-Server und einem BIND-Namenserver. Abbildung 2.9 weiter oben in diesem Kapitel zeigt diese Registerkarte.

Migrieren auf Anwendungspartitionen

Anwendungspartitionen ermöglichen es, bestimmte Daten in unterschiedliche Partitionen aufzutrennen und zu replizieren. Mithilfe von Anwendungspartitionen können Sie den Replikationsumfang steuern, indem Sie beispielsweise nur bestimmte DNS-Zonen replizieren.

Sie erstellen eine Anwendungspartition mit dem Befehlszeilentool Dnscmd:

```
dnscmd <Servername> /CreateDirectoryPartition <FQDN>
```

Sobald die Partition erstellt ist, können Sie mit dem nächsten Befehl Server hinzufügen:

```
dnscmd <Servername> /EnlistDirectoryPartition <FQDN>
```

Wenn Sie eine Verzeichnispartition erstellt haben, können Sie die Zonenreplikation im Eigenschaftendialogfeld einer Zone ändern. Klicken Sie dazu im Eigenschaftendialogfeld der Zone auf der Registerkarte *Allgemein* in der Zeile *Replikation* auf die Schaltfläche *Ändern* (Abbildung 2.10).

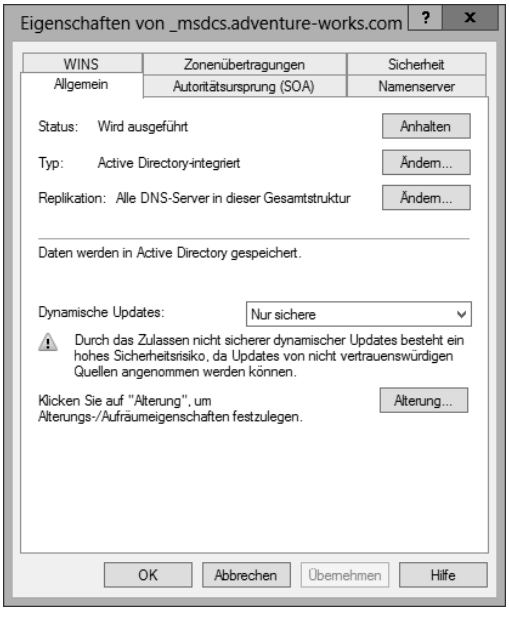

Abbildung 2.10 Sie konfigurieren die Replikation auf der Registerkarte *Allgemein* im Eigenschaftendialogfeld einer Zone

Nach dem Klick auf *Ändern* öffnet sich das Dialogfeld *Bereich der Zonenreplikation ändern* (Abbildung 2.11).

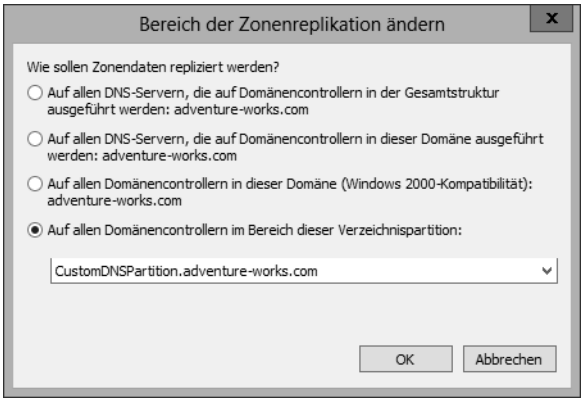

Abbildung 2.11 Replizieren einer Verzeichnispartition

IPv6

Windows Server 2012 unterstützt IPv6-DNS. IPv6-Adressen werden in AAAA-Einträgen angegeben statt in den A-Einträgen für IPv4. Beim Entwurf von IPv6-DNS müssen Sie üblicherweise eine Strategie entwickeln, die den Parallelbetrieb von IPv4- und IPv6-DNS im Netzwerk unterstützt.

Weitere Informationen Verwenden von IPv6 in Windows

Unter *http://technet.microsoft.com/network/bb530961.aspx* finden Sie weitere Informationen über den Einsatz von IPv6 in Windows.

Denken Sie beim Planen einer IPv6-Bereitstellung daran, dass WINS (Windows Internet Name Service) IPv6 nicht unterstützt. Sie können einen ISATAP-Router verwenden, um Umsetzungsdienste für WINS bereitzustellen.

Weitere Informationen Arbeiten mit ISATAP

Unter *http://technet.microsoft.com/library/dd379548* finden Sie weitere Informationen darüber, wie Sie ISATAP für diesen Zweck nutzen.

Namen mit einer einzigen Bezeichnung

In Domänennamen mit einer einzigen Bezeichnung (single-label names, auch als Kurznamen bezeichnet) fehlen die Domäne der obersten Ebene (Top-Level Domain, TLD) und der Punkt. Zum Beispiel lautet der normale Domänenname *adventure-works.com*, der Kurzname dagegen *adventure-works*.

Sie finden Namen mit einer einzigen Bezeichnung in Netzwerken, die das ältere WINS (Windows Internet Name Service) einsetzen. Da WINS allerdings als veraltet eingestuft ist,

müssen Administratoren Pläne entwickeln, wie sie die Namensauflösung für ältere WINS-basierte Anwendungen und wichtige Ressourcen zur Verfügung stellen. Windows hat eine GlobalNames-Zone (GNZ), die Sie nutzen können, um eine Namensauflösung für Kurznamen bereitzustellen. Sie können die GlobalNames-Zone in einer einzelnen Gesamtstruktur oder über mehrere Gesamtstrukturen hinweg bereitstellen, um eine statische Namensauflösung zu ermöglichen.

Die GlobalNames-Zone erleichtert die Übergangszeit beim Umstieg von WINS auf mehrteilige Standard-DNS-Zonen. Sie kann daher eine wichtige Komponente beim Planen einer Namensauflösungsstrategie sein. Sie sollten wissen, wie sich die GlobalNames-Zone von Domänensuffixen unterscheidet und wie sie die Leistung über mehrere Domänensuffixe hinweg verbessert, wenn Sie Kurznamen in einer Infrastruktur anbieten, die mehrere Domänen umfasst. Wenn Windows Server 2012 eine Abfrage nach einem Kurznamen empfängt, sucht es zuerst in der GlobalNames-Zone. Gibt es einen passenden Eintrag in der GlobalNames-Zone, kann der Eintrag nicht an dynamischen Aktualisierungen teilnehmen; Anforderungen nach einer dynamischen Aktualisierung des Eintrags werden dann einfach ignoriert.

Weitere Informationen Arbeiten mit der GlobalNames-Zone

Unter *http://technet.microsoft.com/library/cc794961.aspx* finden Sie weitere Informationen, darunter eine Auflistung aller Schritte, mit denen Sie eine GlobalNames-Zone konfigurieren. In *http://technet.microsoft.com/en-us/library/cc816610* werden Möglichkeiten beschrieben, die Namensauflösung durch eine GlobalNames-Zone zu unterstützen.

Zonenhierarchie und Zonendelegierung

Die Zonenhierarchie ist die baumförmige Struktur von DNS, in der der Stamm der Zone durch einen einzelnen Punkt (.) dargestellt wird. Oberhalb des Stamms befinden sich die Domänen der obersten Ebene (Top-Level Domains, TLDs), zum Beispiel *.com*, *.net* und *.org*. Die Baumstruktur verzweigt sich in private Domänen, von denen Ihnen viele vertraut sein dürften, etwa *microsoft.com* und *adventure-works.com*.

Die *Zonendelegierung* (zone delegation) ist die Fähigkeit, Abfragen für einen bestimmten Teil einer Zone autorisierend zu beantworten. Zum Beispiel sind im hierarchischen Aufbau von DNS die Stammserver für den Stamm der Zone verantwortlich, und sie delegieren die Autorität für TLDs an TLD-Server, die ihrerseits die Verantwortung für Domänen wie *adventure-works.com* an private Unternehmensnamenserver delegieren. Trifft eine Abfrage nach *www.adventure-works.com* ein, beginnt die Auflösung beim Stammserver, der die Abfrage an den Server weiterleitet, der für die TLD *.com* verantwortlich ist, und dieser Server wendet sich dann an den Server, der für die abgefragte Domäne zuständig ist.

Ähnlich wie Stammserver eine Abfrage an TLD-Server delegieren und diese dann wiederum an Unternehmensnamenserver, können Sie Teile Ihrer Unternehmensdomänen, zum Beispiel *adventure-works.com*, an andere Namenserver delegieren, damit sie für diesen Teil der Zone autorisierend werden. Zum Beispiel können Sie eine autorisierende Zone für *corp.adventure-works.com* erstellen, damit Abfragen nach Hosts dieser Domäne an einen anderen Server gesendet werden.

Sie konfigurieren die Zonendelegierung in der Konsole *DNS-Manager*, indem Sie mit der rechten Maustaste auf die Zone klicken und den Befehl *Neue Delegierung* wählen. Daraufhin wird der *Assistent zum Erstellen neuer Delegierungen* gestartet, in dem Sie den gewünschten Teil der Zone, zum Beispiel die Unterdomäne *corp* aus *corp.adventure-works.com*, delegieren können.

Weitere Informationen DNS-Hierarchie und -Delegierung

Unter *http://technet.microsoft.com/library/cc731879* finden Sie weitere Informationen über die Hierarchie- und Delegierungskonzepte von DNS.

Gedankenexperiment Problembehandlung für primäre und sekundäre Server

Im folgenden Gedankenexperiment wenden Sie an, was Sie über dieses Prüfungsziel wissen. Die Antworten auf die Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Sie haben in Ihrem zentralen Rechenzentrum einen sicheren primären DNS-Server bereitgestellt und darauf eine einzige Zone namens *contoso.com* konfiguriert. Nun stellen Sie einen neuen sekundären Server in einem Remotestandort auf. Bei diesem sekundären Server ist der DNS-Dienst konfiguriert, er erhält aber keine Aktualisierungen für die DNS-Zone *contoso.com*.

1. Beschreiben Sie, welche Problembehandlungsschritte Sie auf dem sekundären Server ausführen sollten und welche Konfigurationsänderungen Sie dort wahrscheinlich vornehmen müssen, um das Problem zu beseitigen.
2. Beschreiben Sie, welche Problembehandlungsschritte Sie auf dem primären Server ausführen sollten und welche Konfigurationsänderungen Sie dort wahrscheinlich vornehmen müssen, um das Problem zu beseitigen.

Zusammenfassung des Prüfungsziels

- Der DNS-Dienst unterstützt Funktionen, die die Sicherheit verbessern, zum Beispiel DNSSEC, DNS-Socketpool und Cachesperrung
- Der DNS-Socketpool wechselt die Quellports für DNS-Abfragen zufällig durch, und die Cachesperrung verhindert, dass zwischengespeicherte Antworten überschrieben werden, bevor ein bestimmter Prozentsatz ihrer TTL (Time to Live, Gültigkeitsdauer) abgelaufen ist
- Die Microsoft-DNS-Implementierung unterstützt separate Namespaces, bei denen sich das DNS-Namensuffix vom Active Directory-Domänennamensuffix unterscheidet
- Die Zonendelegierung macht einen anderen Server zum autorisierenden Server für eine Zone. Wenn Sie diese Technik mit Zonenhierarchien und Anwendungspartitionen kombinieren, können Sie komplexe Namensauflösungsarchitekturen für Ihre Organisation implementieren.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Themen überprüfen, die in diesem Prüfungsziel behandelt wurden. Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Für welche der folgenden Szenarien unterstützt Windows Server 2012 die Verwendung separater Namespaces? (Wählen Sie alle zutreffenden Antworten aus.)
   A. Wenn ein Suffix einer Active Directory-Domäne in der aktuellen oder einer anderen Gesamtstruktur entspricht.
   B. Eine Active Directory-Gesamtstruktur, die mehrere Domänen umfasst, aber nur einen DNS-Namespace oder eine DNS-Zone.
   C. Eine einzelne Active Directory-Domäne, die in mehrere DNS-Zonen untergliedert ist.
   D. Wenn eine Zertifizierungsstelle, die Domänenmitglied ist, ihr DNS-Suffix ändert.
2. Welcher Befehl erstellt eine Anwendungspartition?
   A. `dnscmd <FQDN> /CreateDirectoryPartition <Servername>`
   B. `dnscmd <Servername> /CreateApplicationPartition <FQDN>`
   C. `dnscmd <Servername> /CreateDirectoryPartition <FQDN>`
   D. `dnscmd <FQDN> /CreateApplicationPartition <Servername>`
3. Welche Funktion in der DNS-Implementierung von Microsoft erschwert eine Cachebeschädigung?
   A. DNS-Socketpool
   B. Cachesperrungspools
   C. Cachevergiftungsverhinderung
   D. DNS-Pool-Verwürfelung
4. Sie haben die Cachesperrung konfiguriert und erhalten Beschwerden, dass Clients veraltete Daten auf ihre DNS-Abfragen erhalten. Welchen Registrierungsschlüssel müssen Sie ändern, um zu konfigurieren, über welchen Prozentsatz der TTL ein Eintrag gesperrt bleibt?
   A. *TTLRatioPercent*
   B. *CacheResetValue*
   C. *TTLLockingValue*
   D. *CacheLockingPercent*

Prüfungsziel 2.3: Entwerfen und Verwalten einer IP-Adressverwaltungslösung

Windows Server 2012 führt mit der IP-Adressverwaltung (IP Address Management, IPAM) ein neues Feature ein, das Administratoren dabei hilft, ihre Infrastruktur und die Hosts im Netzwerk zu organisieren. IPAM ist ein leistungsfähiges Tool, mit dem Sie sowohl eine IPv4- als auch eine IPv6-Netzwerkinfrastruktur verwalten können. Es bietet außerdem die Möglichkeit, den IP-Adressraum zu überwachen.

Dieses Prüfungsziel behandelt die folgenden Themen:

- Entwurfsaspekte, darunter Techniken zur IP-Adressverwaltung (zum Beispiel IPAM, Gruppenrichtlinien und manuelle Bereitstellung) und den Unterschied zwischen verteilter und zentraler Anordnung
- Konfigurieren rollenbasierter Zugriffssteuerung
- Konfigurieren der IPAM-Überwachung
- Migrieren von IP-Adressen
- Verwalten und Überwachen mehrerer DHCP- und DNS-Server
- Konfigurieren der Datensammlung für IPAM

Entwurfsaspekte für die IP-Adressverwaltung

Beim Entwurf einer IP-Adresseninfrastruktur besteht Ihr Ziel darin, den Aufwand für die Administration des Adressraums möglichst gering zu halten. Viele Organisationen beschränken sich auf eine simple Tabelle, um ihren Adressraum zu verwalten. Bei einer solchen Technik ist schwierig nachzuvollziehen, wer Änderungen am Adressraum vorgenommen hat. Häufig anfallende Aufgaben müssen von Hand erledigt werden, wenn Sie zum Beispiel feststellen müssen, welches Gerät eine bestimmte IP-Adresse verwendet, und das Ergebnis dann dokumentieren wollen. Bei dieser umfangreichen Handarbeit im Bereich der IP-Adressverwaltung passieren Fehler und natürlich verursacht sie eine Menge Arbeit.

Im Idealfall würden sich die verwendeten IP-Adressräume möglichst weit selbst verwalten und die Administratoren müssten nur selten aktiv werden. Die IP-Adressverwaltung (IP Address Management, IPAM) in Windows Server 2012 nimmt Ihnen einige Verwaltungsarbeiten ab. Sie stellt dazu wichtige Funktionen zur Verfügung, zum Beispiel Gerätesuche, Überwachung, Berichterstellung und Überwachung.

IPAM ermöglicht die Verfolgung der IP-Adressen für Domänencontroller und Netzwerkrichtlinienserver, die unter Windows Server 2008 oder neuer laufen, die Konfiguration und Überwachung von DNS-Servern und die Bereichsüberwachung und -konfiguration von DHCP-Servern. IPAM sucht in regelmäßigen Abständen nach Domänencontrollern, DNS-Servern, DHCP-Servern und Netzwerkrichtlinienservern. Die Server können von IPAM verwaltet werden oder unverwaltet bleiben. Damit ein Server von der IPAM-Suche erkannt

wird, müssen die Firewalleinstellungen allerdings die Kommunikation vom IPAM-Server erlauben, außerdem müssen andere Sicherheitseinstellungen die Suche zulassen. Alle beteiligten Server müssen zur selben Active Directory-Gesamtstruktur gehören und Domänenmitglieder sein.

Wenn Sie eine IPAM-Lösung entwerfen, müssen Sie entscheiden, wo die Server aufgestellt werden. Sie können sie beispielsweise zentral versammeln oder jeweils einen IPAM-Server in einem Standort bereitstellen. IPAM-Server kommunizieren nicht miteinander und teilen sich keine Informationen, aber Sie können den Bereich jedes Servers so einschränken, dass er seine Suche auf den eigenen Standort beschränkt. Diese Entwurfsvariante bedeutet für die Praxis, dass Sie in einer Umgebung, die mehrere Standorte umfasst, bestimmte Bereiche definieren können, die jeweils von einem lokalen Team verwaltet werden. Für andere Umgebungen eignet sich ein zentralisierter Ansatz besser. Auf jeden Fall können Sie die IP-Adressverwaltung so aufteilen, dass die Anforderungen Ihrer Organisation optimal erfüllt werden.

Ein einzelner IPAM-Server kann höchstens die folgende Zahl von Elementen verwalten:

- 150 DHCP-Server
- 500 DNS-Server
- 6000 DHCP-Bereiche
- 150 DNS-Zonen

Nicht-Microsoft-Geräte, zum Beispiel Router und Switches, werden von IPAM nicht verwaltet oder überwacht.

Weitere Informationen Einführung in IPAM

Unter *http://technet.microsoft.com/library/hh831353* finden Sie einen Überblick über IPAM. Dort sind auch einige weitere Einschränkungen aufgeführt.

Wenn Sie den IPAM-Server installiert haben, können Sie ihn von Hand oder mit Gruppenrichtlinienobjekten (Group Policy Objects, GPOs) einrichten. Der Assistent zum Bereitstellen von IPAM (er trägt in der deutschen Version den etwas irreführenden Namen *Bereitstellungs-IPAM*) führt Sie durch den Bereitstellungsprozess (Abbildung 2.12). Nachdem Sie sich allerdings für eine Bereitstellungsmethode entschieden haben, können Sie sie nicht mehr ändern. Wenn Sie die Option *Gruppenrichtlinienbasiert* auswählen, ist es einfacher, mehrere Server als verwaltet zu markieren, und Sie brauchen die Gruppenrichtlinienobjekte nur zu entfernen, um Server wieder als unverwaltet zu markieren.

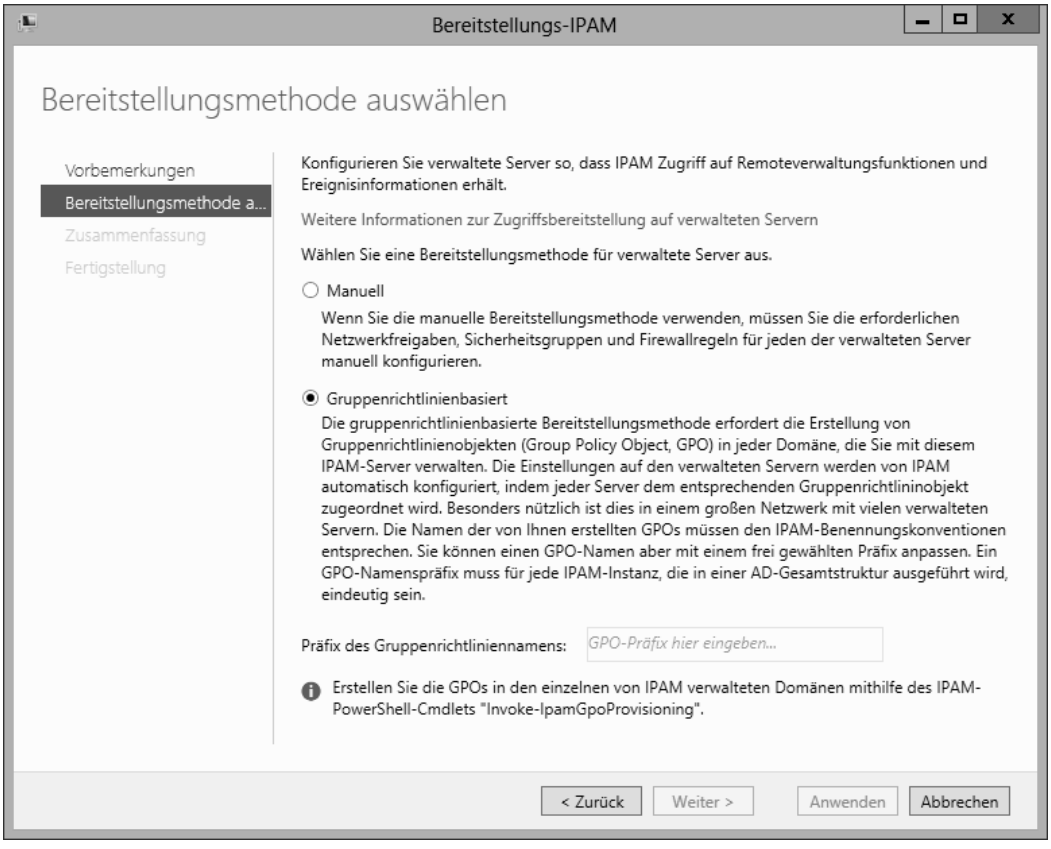

Abbildung 2.12 Konfigurieren der IPAM-Bereitstellungsmethode

Mithilfe von Gruppenrichtlinienobjekten können Sie eine Aufgabe zur Serverermittlung (Serversuche) in die Aufgabenplanung eintragen. Sie können die Suche aber auch von Hand auf der Seite *IPAM* im Server-Manager starten. Abbildung 2.13 zeigt, nach welchen Servertypen Sie suchen können.

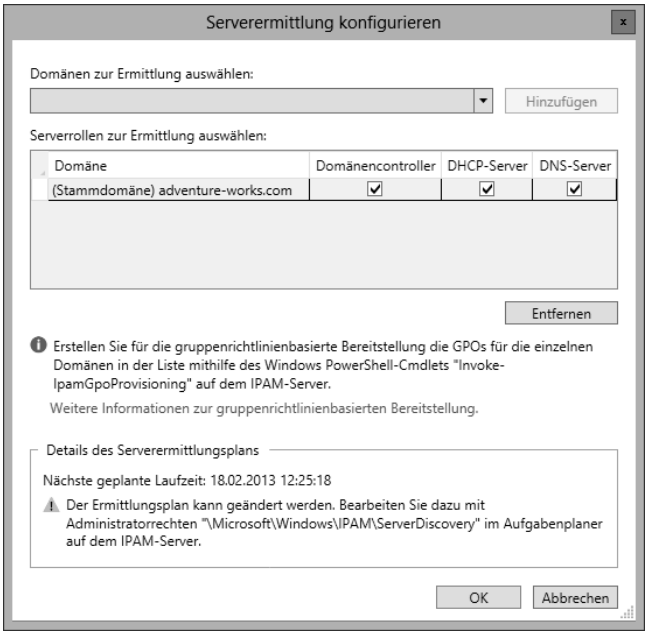

Abbildung 2.13 Konfigurieren der Servertypen, die von IPAM gesucht werden

Wenn Server gefunden werden, wird ihr IPAM-Zugriffsstatus als »Blockiert« angezeigt und ihr Verwaltbarkeitsstatus ist »Nicht angegeben« (Abbildung 2.14).

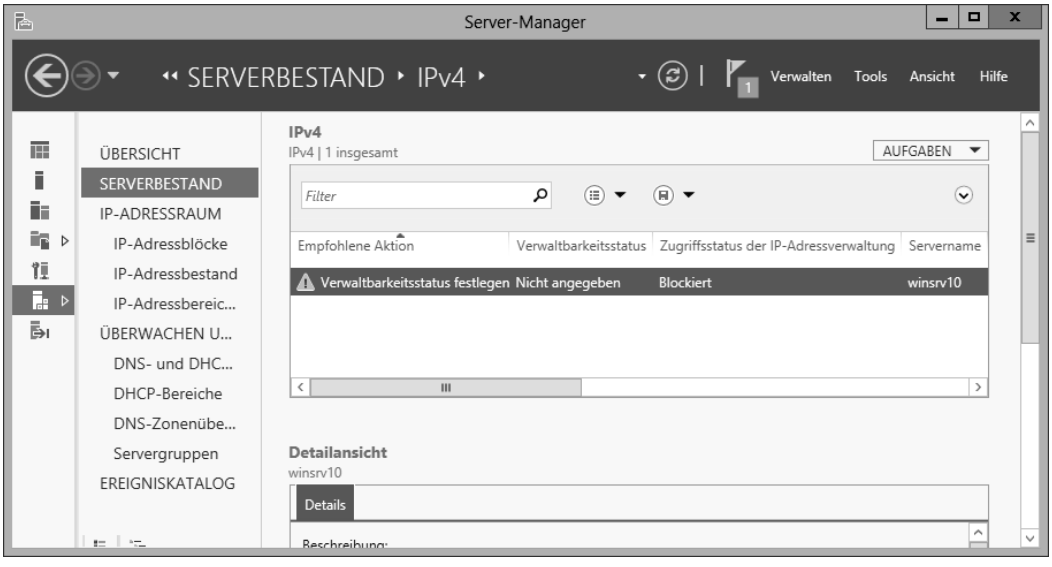

Abbildung 2.14 Sie müssen den Verwaltbarkeitsstatus eines neu erkannten Servers ändern, damit Sie ihn verwalten können

Sie konfigurieren den Server als verwaltet, indem Sie ihm die entsprechenden Gruppenrichtlinienobjekte zuordnen. Dazu können Sie auf dem IPAM-Server den folgenden PowerShell-Befehl (als Administrator) ausführen:

```
Invoke-IpamGpoProvisioning -Domain <Domäne> -GpoPrefixName <Präfix> -IpamServerFqdn <IPAM-Servername>
```

Dieser Befehl erstellt drei Gruppenrichtlinienobjekte. Wenn Sie zum Beispiel bei der Bereitstellung von IPAM das GPO-Namenspräfix *IPAM1* angeben, können Sie in der Gruppenrichtlinienverwaltung sehen, dass die folgenden Gruppenrichtlinienobjekte erstellt werden:

- IPAM1_DC_NPS
- IPAM1_DNS
- IPAM1_DHCP

Anschließend müssen Sie auf jeden Server, der verwaltet werden soll, diese Gruppenrichtlinienobjekte anwenden. Führen Sie dazu auf dem jeweiligen Server den folgenden Befehl aus:

```
gpupdate /force
```

Und schließlich müssen Sie noch den Verwaltbarkeitsstatus des Servers auf *Verwaltet* setzen. Klicken Sie dazu mit der rechten Maustaste auf den Server, wählen Sie den Befehl *Server bearbeiten* und ändern Sie den Eintrag in der Zeile *Verwaltbarkeitsstatus* auf den Wert *Verwaltet*.

Konfigurieren der rollenbasierten Zugriffssteuerung

Bei der Installation legt IPAM fünf Sicherheitsgruppen an, die in Tabelle 2.3 beschrieben sind. Diese Gruppen werden während der IPAM-Bereitstellung hinzugefügt und sie können wie jede andere Windows-Sicherheitsgruppe verwendet werden. Wenn Sie beispielsweise Benutzer zu einer dieser Gruppen hinzufügen, können sie die IPAM-Aufgaben ausführen, die durch die Berechtigungen der jeweiligen Gruppe erlaubt werden.

Tabelle 2.3 Von IPAM erstellte Sicherheitsgruppen

Sicherheitsgruppe	Beschreibung
IPAM-Benutzer	Diese Benutzer dürfen sich Informationen über die verschiedenen Bereiche ansehen, die von IPAM verwaltet werden. Eine Ausnahme sind die Daten zur IP-Adressverfolgung.
IPAM-MSM-Administratoren	Umfasst alle Privilegien der Gruppe *IPAM-Benutzer* und zusätzlich die Fähigkeit, den IPAM-Server zu verwalten
IPAM-ASM-Administratoren	Umfasst alle Privilegien der Gruppe *IPAM-Benutzer* und zusätzlich die Fähigkeit, den IP-Adressraum und den Server zu verwalten
IPAM-IP-Überwachungs-administratoren	Umfasst alle Privilegien der Gruppe *IPAM-Benutzer* und zusätzlich die Fähigkeit, Daten zur IP-Adressverfolgung anzuzeigen
IPAM-Administratoren	Eine administrative Gruppe, die alle IPAM-Aufgaben ausführen darf

Konfigurieren der IPAM-Überwachung

Sie können IPAM für Überwachungsaufgaben einsetzen. Es liefert Ihnen Informationen über die Adressennutzung, Richtlinieneinhaltung und spezifische andere Daten zum jeweiligen Servertyp, der von IPAM verwaltet wird. Sie konfigurieren die IPAM-Überwachung im Ereigniskatalog (Abbildung 2.15). Die IP-Adressüberwachung von IPAM sammelt Benutzerinformationen zusammen mit IP-Adresse, Hostname und Clientkennung (MAC-Adresse für IPv4 oder DUID für IPv6). Diese Daten stammen von verwalteten DHCP-Servern, Domänencontrollern und Netzwerkrichtlinienservern.

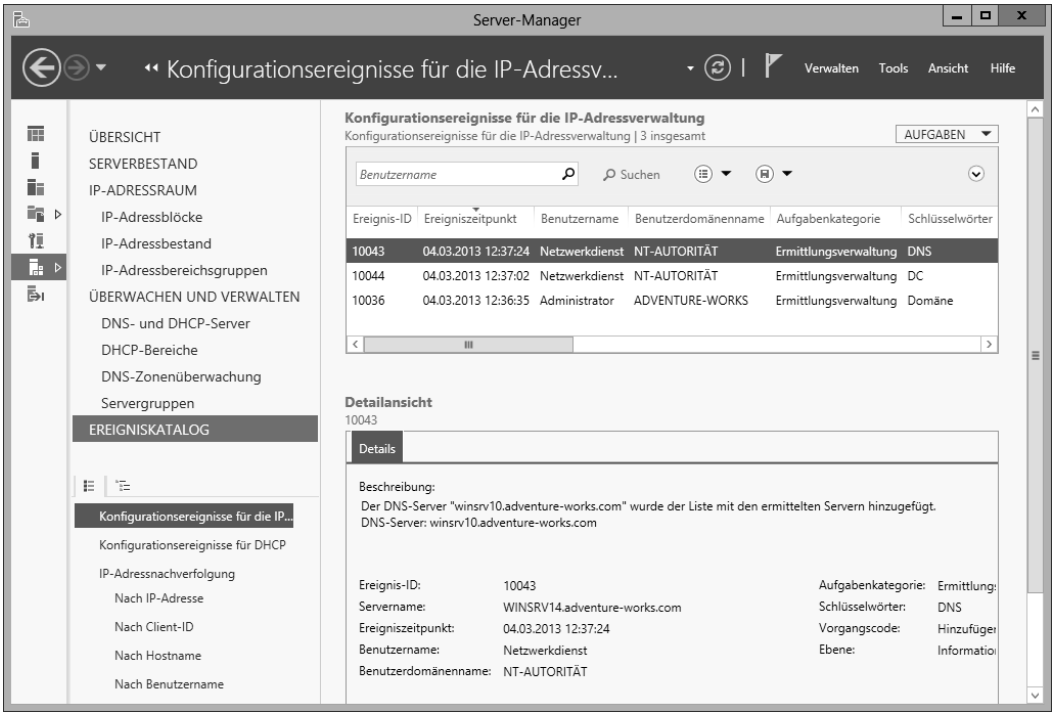

Abbildung 2.15 Der Ereigniskatalog in IPAM

In der Standardeinstellung werden IPAM-Konfigurationsereignisse aufgelistet, Sie können aber auch andere Ereignisse anzeigen und Berichte aus den aufgezeichneten Daten erstellen. Der Ereigniskatalog stellt Abfragetools und ein Suchfeld zur Verfügung, mit denen Sie festlegen können, welche Ereignisse angezeigt werden. Sie haben auch die Möglichkeit, Kriterien zu einem Abfragefilter hinzuzufügen (Abbildung 2.16).

Gesammelte Daten können Sie in Form einer CSV-Datei (Comma-Separated Values, das heißt, die Einträge sind durch Kommas voneinander getrennt) exportieren.

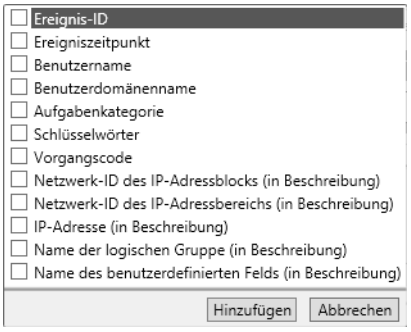

Abbildung 2.16 Zusätzliche Filterkriterien für die IPAM-Überwachung

Migrieren von IP-Adressen

IPAM hilft Ihnen dabei, die IP-Adressen in einem Netzwerk zu verwalten. Sie können IPAM einsetzen, um die Verwendung von IP-Adressen in einem bestimmten Standort zu verfolgen. Auf diese Weise können Sie sicherstellen, dass für die Clients in diesem Standort genug Adressen zur Verfügung stehen. IPAM definiert IP-Adressbereiche als Gruppen aufeinanderfolgender IP-Adressen, und IP-Adressblöcke als Gruppen von IP-Adressbereichen.

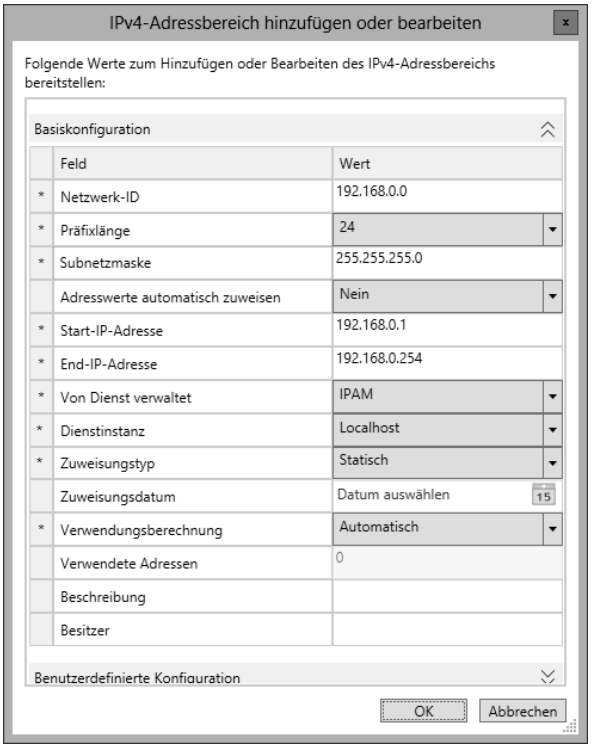

Abbildung 2.17 Hinzufügen und Bearbeiten eines IP-Adressbereichs in IPAM

Wenn Sie IP-Adressen migrieren, um sie durch IPAM verwalten zu lassen, können Sie die Adressen von Hand als Adressbereich, Adressblock und einzeln eintippen. Sie können die IP-Adressen aber auch aus einer CSV-Datei in IPAM importieren. Abbildung 2.17 zeigt das Dialogfeld *IPv4-Adressbereich hinzufügen oder bearbeiten*.

Das Kombinationsfeld *Von Dienst verwaltet* ist für die Migrationsplanung sehr nützlich. Hier konfigurieren Sie, wie der jeweilige Adressblock oder -bereich verwaltet wird. Zur Auswahl stehen Optionen wie IPAM (in Abbildung 2.17 ausgewählt), eine Nicht-Microsoft-DHCP-Lösung, Microsoft Virtual Machine Manager oder eine andere Methode. Wenn Sie hier die passende Einstellung konfigurieren, können Sie den IP-Adressraum bereits in IPAM importieren, während Sie die Adresszuweisung vorerst noch über die bisherige Methode durchführen lassen. Sobald alles bereit ist, können Sie die IP-Adressen der IPAM-Verwaltung unterstellen.

Verwalten und Überwachen mehrerer DHCP- und DNS-Server

IPAM kann Server zu logischen Gruppen zusammenfassen, um ihre Konfiguration, Überwachung und Verwaltung zu erleichtern. Das ist nützlich, wenn Sie mehrere Server verwalten, die beispielsweise im selben Remotestandort stehen oder andere gemeinsame Eigenschaften haben, die für ihre Verwaltung und Überwachung in IPAM wichtig sind. Servergruppen konfigurieren Sie auf der Server-Manager-Unterseite *IPAM* im Abschnitt *Überwachen und verwalten*.

Auf der IPAM-Unterseite *Servergruppen* können Sie eine Servergruppe im Dialogfeld *Servergruppe hinzufügen* (Abbildung 2.18) hinzufügen.

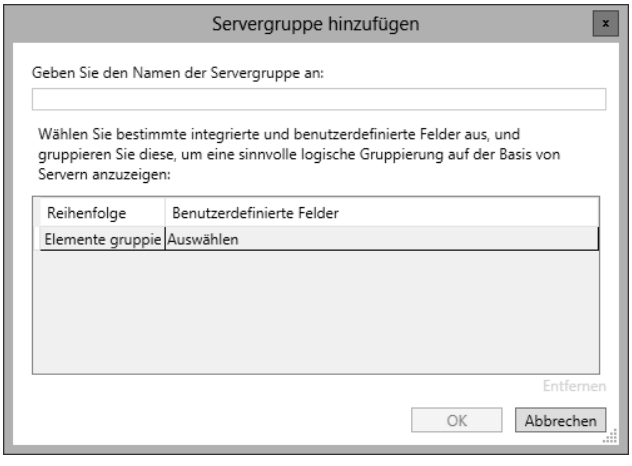

Abbildung 2.18 Hinzufügen einer Servergruppe in IPAM

Wie in Abbildung 2.18 zu sehen, können Sie die Server anhand verschiedener Kriterien auswählen. Abbildung 2.19 zeigt die verfügbaren Kriterien.

Abbildung 2.19 Verfügbare Kriterien für die Auswahl von Servergruppen in IPAM

Es steht eine mehrstufige Filterung zur Verfügung, daher können Sie zuerst eine Gruppierung anhand eines Kriteriums durchführen und die Gruppe dann auf Basis anderer Kriterien weiter einschränken.

Sobald Sie eine Servergruppe erstellt haben, wird sie auf der IPAM-Unterseite *Servergruppen* aufgeführt. Wie bei anderen Bereiche können Sie auch Servergruppen durchsuchen und ihre Reihenfolge ändern, um eine bestimmte Gruppe verwalteter Server auszuwählen.

Konfigurieren des Datenabrufs

Die Datenabrufprozesse von IPAM werden in der Aufgabenplanung verwaltet und in regelmäßigen Abständen ausgeführt. Welche Daten gesammelt werden, hängt davon ab, welche Elemente Sie in IPAM konfiguriert haben. Wenn Sie IPAM beispielsweise einsetzen, um IP-Adressen zu verwalten, wird im Rahmen des Datenabrufs die Nutzung aller verwalteten IP-Adressen überprüft. Auch wie lange das Abrufen dieser Daten dauert, hängt vom Typ der gesammelten Daten ab.

Die Datenabrufaufgaben werden in der Aufgabenplanungsbibliothek im Zweig *Microsoft/Windows/IPAM* konfiguriert. Tabelle 2.4 listet die Namen der Aufgaben und ihr Standardintervall auf.

Tabelle 2.4 Standardzeitpläne für Aufgaben in der Aufgabenplanung

Aufgabenname	Intervall
AddressExpiry	1 Tag
AddressUtilization	2 Stunden
Audit	1 Tag
ServerAvailability	15 Minuten
ServerConfiguration	6 Stunden
ServerDiscovery	1 Tag
ServiceMonitoring	30 Minuten

Welche Daten von einem Server abgerufen werden, hängt vom Typ dieses Servers ab. Zum Beispiel werden von einem DHCP-Server keine DNS-Zonen abgerufen. Im Dialogfeld *Server*

hinzufügen oder bearbeiten (Abbildung 2.20) können Sie konfigurieren, welche Daten gesammelt werden. Wählen Sie hier die Kontrollkästchen der gewünschten Servertypen aus, um einzustellen, welche Daten abgerufen werden.

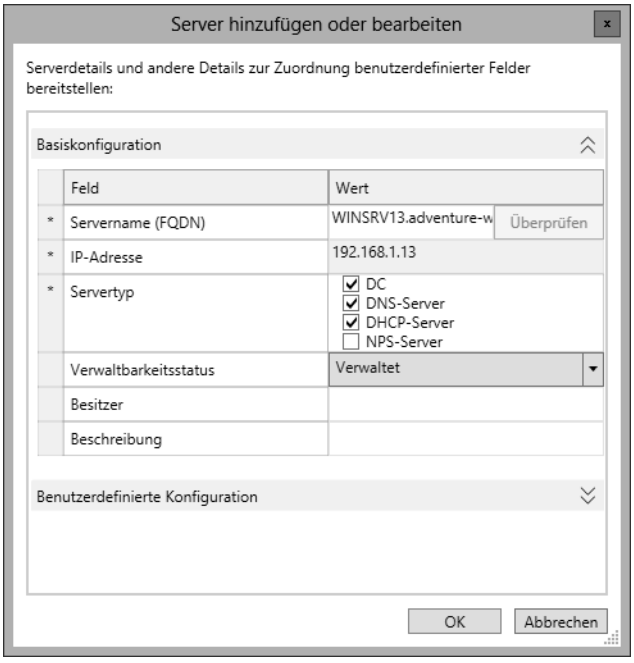

Abbildung 2.20 Im Dialogfeld *Server hinzufügen oder bearbeiten* konfigurieren Sie den Servertyp für IPAM

Weitere Informationen Konfigurieren von IPAM

Unter *http://technet.microsoft.com/library/hh831622* finden Sie weitere Informationen zum Konfigurieren von IPAM.

Gedankenexperiment Konfigurieren von Servern für IPAM

Im folgenden Gedankenexperiment wenden Sie an, was Sie über dieses Prüfungsziel wissen. Die Antworten auf die Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Sie haben das Feature *IP-Adressverwaltungsserver (IPAM-Server)* auf einem zentralen Server installiert und die gruppenrichtlinienobjektbasierte Suche konfiguriert. Nachdem Sie eine Serverermittlung ausgeführt haben, werden zwei Server aufgelistet, die Sie verwalten können.

Beschreiben Sie, mit welchen Schritten Sie diese Server unter IPAM-Verwaltung stellen.

Zusammenfassung des Prüfungsziels

- IPAM weist einige Einschränkungen bezüglich der Zahl der verwalteten Server auf. Es kann höchstens 150 DHCP-Server, 500 DNS-Server, 150 DNS-Zonen und 6000 DHCP-Bereiche verwalten.
- Welche Server ein IPAM-Server verwaltet, können Sie von Hand oder mithilfe von Gruppenrichtlinienobjekten festlegen
- IPAM-Server können so verteilt werden, dass die Anforderungen der Organisation am besten erfüllt werden
- IPAM erstellt mehrere Sicherheitsgruppen, mit denen Sie eine rollenbasierte Zugriffssteuerung für die verschiedenen IPAM-Funktionen implementieren können
- IP-Adressen können in IPAM verwaltet und überwacht werden. Sie können in IPAM außerdem IP-Adressen definieren, die von anderen DHCP-Servern verwaltet werden.
- Servergruppen erleichtern die Verwaltung mehrerer Server in IPAM. Dazu fassen die Administratoren Server zu logischen Gruppen zusammen.
- Die Aufgabenplanung enthält mehrere Aufgaben, die Daten für IPAM sammeln. Sie können den Datenabruf auch von Hand starten.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Themen überprüfen, die in diesem Prüfungsziel behandelt wurden. Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Sie wollen ausgewählten Benutzern erlauben, sich IPAM-Überwachungsinformationen anzusehen. Zu welcher Gruppe sollten Sie diese Benutzer hinzufügen, damit sie nur die Berechtigungen erhalten, die Sie tatsächlich für diese Aufgabe brauchen?

   A. *IPAM-Benutzer*

   B. *IPAM-IP-Adressüberwachungsadministratoren*

   C. *IPAM-Administratoren*

   D. *IPAM-IP-Überwachungsadministratoren*

2. Sie haben bei der Bereitstellung von IPAM die gruppenrichtlinienobjektbasierte Suche konfiguriert. Sie wollen nach Servern suchen und sie in IPAM als verwaltete Server konfigurieren. Welchen Befehl müssen Sie direkt auf einem Server ausführen, der verwaltet werden soll?

   A. `Invoke-IpamAudit /server <IPAM-Servername> /domain`

   B. `gpupdate /reset`

   C. `Invoke-IpamAudit /server <IPAM-Servername> /configure`

   D. `gpupdate /force`

3. In welchem Intervall wird die Datenabrufaufgabe *ServerDiscovery* standardmäßig ausgeführt?

   A. 3 Tage

   B. 8 Stunden

   C. 1 Tag

   D. 1 Stunde

4. Welches der folgenden Kriterien steht *nicht* zum Filtern von Ereignissen zur Verfügung (vorausgesetzt, Sie verwenden kein benutzerdefiniertes Kriterium)?

   A. Schlüsselwörter

   B. Ereignisregion

   C. Benutzername

   D. Benutzerdomänenname

5. Wann tauschen IPAM-Server Informationen über die Server aus, die sie jeweils verwalten?

   A. Wenn sie in einem verteilten Szenario konfiguriert sind.

   B. Nie. IPAM-Server tauschen untereinander keine Informationen aus.

   C. Wenn sie mit System Center 2012 konfiguriert sind.

   D. Wenn sie für die Verwendung von DNS konfiguriert sind.

Zusammenfassung des Kapitels

- Die Windows Server 2012-Rolle *DHCP-Server* bietet Redundanz durch geteilte Bereiche, Failover im Hot-Standby- oder Lastenausgleichsmodus und Failovercluster
- In einem Failovercluster sind beide Server in der Lage, DHCP-Daten zuzuweisen, weil sie auf dieselbe DHCP-Datenbank an einem freigegebenen Speicherort zugreifen
- Bei der DHCP-Filterung legen Sie mithilfe von Verbindungsschicht-MAC-Adressen fest, welchen Clients der Server antwortet
- Das DHCP Management Pack, eine Komponente im System Center Operations Manager, ermöglicht die Überwachung des DHCP-Diensts und die Erstellung von Berichten
- Der DNS-Dienst unterstützt Konfigurationen, die die Sicherheit verbessern, zum Beispiel DNSSEC, DNS-Socketpool und Cachesperrung
- IP-Adressen können in IPAM verwaltet und überwacht werden. Sie können in IPAM auch IP-Adressen definieren, die von anderen DHCP-Servern verwaltet werden

Antworten

Dieser Abschnitt enthält die Lösungen zu den Gedankenexperimenten und den Lernzielkontrollfragen dieses Kapitels.

Prüfungsziel 2.1: Gedankenexperiment

Am besten eignet sich wahrscheinlich eine Hot-Standby-Failoverkonfiguration mit zwei Servern. Der Server im zentralen (primären) Standort bedient normalerweise Clients in der Zentrale und ein sekundärer Server im Remotestandort beantwortet die Anforderungen im Remotestandort. Wenn in einer Hot-Standby-Konfiguration einer dieser Server ausfällt, bedient der andere die Anforderungen.

Prüfungsziel 2.1: Lernzielkontrolle

1. **Richtige Antwort:** C
   A. **Falsch:** Diese Aufteilung wird nicht empfohlen.
   B. **Falsch:** Diese Aufteilung wird nicht empfohlen.
   C. **Richtig:** Für geteilte DHCP-Bereiche wird eine Aufteilung von 80 zu 20 Prozent empfohlen, wobei der primäre Server 80 Prozent der Adressen erhält und der sekundäre Server 20 Prozent.
   D. **Falsch:** Diese Aufteilung wird nicht empfohlen.
2. **Richtige Antworten:** A und B
   A. **Richtig:** 00-11-09-*-*-* ist ein gültiger Filter, der mithilfe von Platzhaltern auf mehrere MAC-Adressen zutrifft.
   B. **Richtig:** 001109001111 ist ein gültiger MAC-Filter.
   C. **Falsch:** 00:11:09:09:11:09 ist kein gültiger MAC-Filter. Doppelpunkte sind nicht als Trennzeichen erlaubt.
   D. **Falsch:** 00-11-09-7c-ef-% ist kein gültiger MAC-Filter. Ein Prozentzeichen ist nicht als Platzhalter erlaubt.
3. **Richtige Antwort:** A
   A. **Richtig:** Der Pfad *C:\Windows\system32\dhcp* ist der Standardspeicherort für die Datenbank. Er wird im Eigenschaftendialogfeld des DHCP-Servers konfiguriert.
   B. **Falsch:** Den Pfad *C:\Program Files\Microsoft\DHCP\Data* gibt es nicht.
   C. **Falsch:** Den Pfad *C:\Windows\system32\DHCP\Data* gibt es nicht.
   D. **Falsch:** Der Registrierungsschlüssel *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DHCP* enthält nicht die DHCP-Datenbank.

4. **Richtige Antwort:** B

   A. **Falsch:** Wenn Sie den Verteilungsprozentsatz so ändern, dass der sekundäre Server mehr IP-Adressen aus dem Bereich erhält, erreichen Sie lediglich, dass der sekundäre Server mehr Adressen vergeben kann. Sie beseitigen damit nicht das Problem, dass der sekundäre Server Adressen an Clients zuweist, die vom primären Server bedient werden sollten.

   B. **Richtig:** Wenn Sie in der Konsole *DHCP* eine Verzögerung für DHCP-Angebote vom sekundären Server festlegen, beseitigen Sie das Problem, weil der primäre Server dann zuerst antwortet und der sekundäre Server erst nach der eingestellten Wartezeit. Weil DHCP-Clients die Daten aus der ersten Antwort übernehmen, ist das Problem damit gelöst.

   C. **Falsch:** Wenn Sie die Auslastung des primären Servers so verringern, dass er schneller antwortet, verringert das unter Umständen das Ausmaß des Problems. Aber weil in der Aufgabe nicht erwähnt wird, dass der primäre Server überlastet ist, antwortet der sekundäre Server vielleicht aus anderen Gründen schneller als der primäre.

   D. **Falsch:** Wenn Sie den sekundären DHCP-Server in ein anderes Netzwerksegment legen, damit seine Antworten später eintreffen, lösen Sie nicht das geschilderte Problem. Außerdem treten dadurch möglicherweise Verbindungsprobleme für die DHCP-Antworten auf.

Prüfungsziel 2.2: Gedankenexperiment

1. Stellen Sie auf dem sekundären Server zuerst sicher, dass der primäre Server erreichbar ist. Dafür reicht ein simpler Ping-Befehl, sofern ICMP-Echoanforderungen und -Echoantworten nicht durch eine Firewall blockiert werden. Sie können auf dem sekundären Server auch Nslookup starten und beim primären Server Daten zur Domäne *contoso.com* abfragen.

2. Prüfen Sie auf dem primären Server, ob die Netzwerkverbindung zum sekundären Server funktioniert und vor allem, ob Zonenübertragungen zum sekundären Server erlaubt sind. Diese Einstellung nehmen Sie im Eigenschaftendialogfeld der Zone auf der Registerkarte *Zonenübertragungen* vor. Außerdem sollten Sie sicherstellen, dass die Firewall eingehenden Verkehr über die UDP- und TCP-Ports 53 zulässt.

Prüfungsziel 2.2: Lernzielkontrolle

1. **Richtige Antworten:** B und C.

   A. **Falsch:** Diese Konfiguration wird von Microsoft nicht unterstützt.

   B. **Richtig:** Diese Konfiguration wird unterstützt.

   C. **Richtig:** Diese Konfiguration wird unterstützt.

   D. **Falsch:** Diese Konfiguration wird nicht unterstützt.

2. **Richtige Antwort:** C
   A. **Falsch:** Die Syntax dieses `dnscmd`-Befehls ist falsch.
   B. **Falsch:** Die Syntax dieses `dnscmd`-Befehls ist falsch.
   C. **Richtig:** Dies ist die richtige Syntax für die beschriebene Aufgabe.
   D. **Falsch:** Die Syntax dieses `dnscmd`-Befehls ist falsch.
3. **Richtige Antwort:** A
   A. **Richtig:** Der DNS-Socketpool wechselt die Quellports für DNS-Abfragen zufällig durch.
   B. **Falsch:** Eine solche Funktion gibt es nicht.
   C. **Falsch:** Eine solche Funktion gibt es nicht.
   D. **Falsch:** Eine solche Funktion gibt es nicht.
4. **Richtige Antwort:** D
   A. **Falsch:** Dies ist kein gültiger Registrierungsschlüssel.
   B. **Falsch:** Dies ist kein gültiger Registrierungsschlüssel.
   C. **Falsch:** Dies ist kein gültiger Registrierungsschlüssel.
   D. **Richtig:** Das ist der richtige Registrierungsschlüssel.

Prüfungsziel 2.3: Gedankenexperiment

Zuerst müssen Sie mit dem Cmdlet `Invoke-IpamGpoProvisioning` die Gruppenrichtlinienobjekte anlegen. Führen Sie dann auf den Servern, die Sie verwalten wollen, den Befehl `gpupdate /force` aus. Zuletzt müssen Sie die Server in IPAM auf den Status *Verwaltet* setzen.

Prüfungsziel 2.3: Lernzielkontrolle

1. **Richtige Antwort:** D
   A. **Falsch:** *IPAM-Benutzer* ist eine gültige Gruppe, aber sie gewährt nicht die Berechtigung, Überwachungsinformationen anzuzeigen.
   B. **Falsch:** Eine solche Gruppe gibt es nicht.
   C. **Falsch:** Die Gruppe *IPAM-Administratoren* verfügt zwar über die erforderlichen Privilegien, sie gewährt aber mehr Berechtigungen, als für diese Aufgabe tatsächlich gebraucht werden.
   D. **Richtig:** Die Gruppe *IPAM-IP-Überwachungsadministratoren* gewährt nur die Privilegien, die für die Aufgabe tatsächlich gebraucht werden.