

Implementacija naprednih mrežnih servisa



Algebra

visoka škola za
primijenjeno računarstvo

- Konfiguracija naprednih DHCP postavki
- Konfiguracija naprednih DNS postavki
- IPAM implementacija
- Upravljanje IP adresnim prostorom pomoću IPAM servisa



Algebra

visoka škola za
primijenjeno računarstvo

Konfiguracija naprednih DHCP postavki

- Pregled DHCP komponenti
- Konfiguracija interakcije DHCP s DNS
- Napredni DHCP dizajn raspona
- DHCP integracija s IPv6
- Što je DHCP zaštita imena?
- Što je DHCP Failover?



Algebra

visoka škola za
primijenjeno računarstvo

Pregled DHCP komponenti

DHCP komponente:

- Poslužiteljsko DHCP servis
- DHCP opcije
- DHCP konzola
- DHCP rasponi
- DHCP baza

Kada možemo koristiti DHCP:

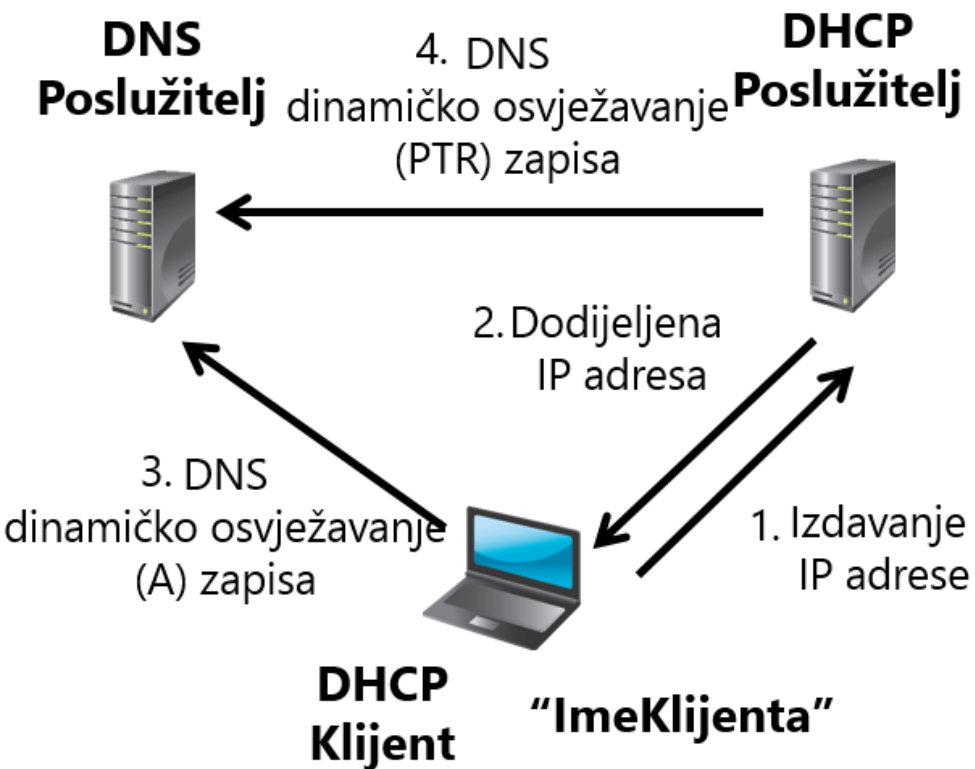
- Klijent traži IP konfiguraciju putem broadcast poruka
- IP adrese se dodjeljuju klijentima na određeno vrijeme i obnavljaju je
- DHCP poslužitelj mora biti autoriziran u AD servisu



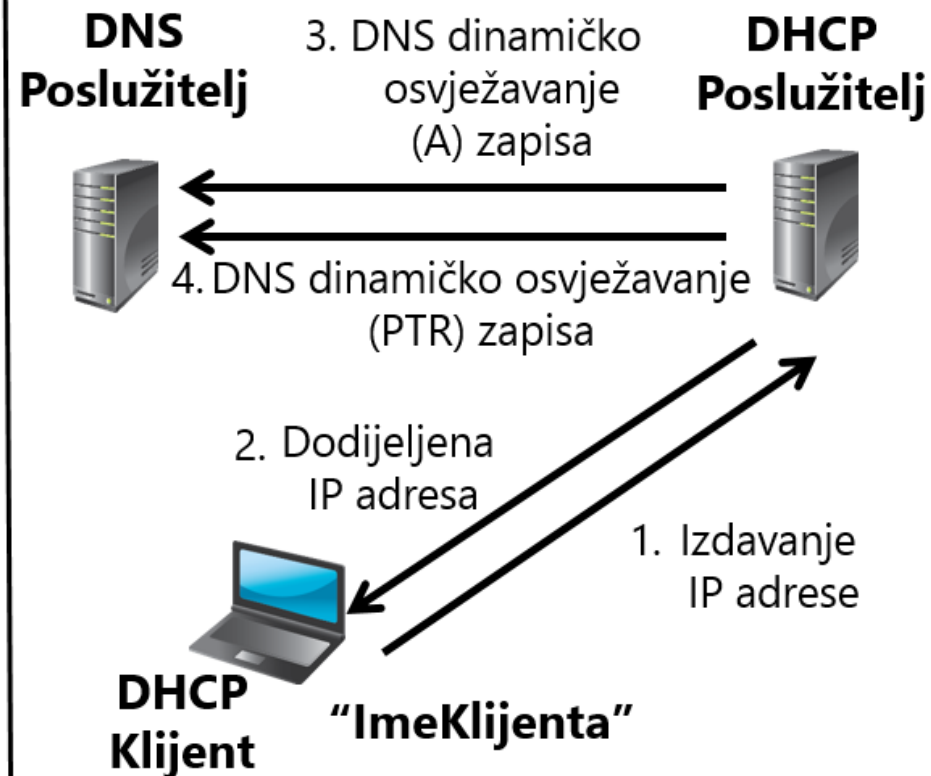
Konfiguracija interakcije DHCP s DNS

Konfiguracija opcije 081 omogućava DHCP poslužitelju da registrira A i PTR zapise za klijenta

Opcija 081 nemodificirana



Opcija 081 modificirana



Napredni DHCP dizajn raspona

Superscope

- Podrška za više VLAN-ova na jednom fizičkom segmentu mreže
- Olakšava prelazak na drugu IP konfiguracijsku shemu
- Zahtjeva postojanje usmjernika između VLAN-ova

Multicast

- Koristi klasu D 224.0.0.0/3
- Koriste ga aplikacije koje zahtijevaju simultanu komunikaciju s više klijenata
- Koristi se skupa s standardnom IP adresom klijenta



Algebra

visoka škola za
primijenjeno računarstvo

DHCPv6 podržava stateful i stateless konfiguracije

DHCPv6 također podržava raspone koje možemo konfigurirati s sljedećim svojstvima:

- Ime i opis
- Preferanse
- Valid i Preferred vrijednosti trajanja
- Prefiks
- Izuzetci
- DHCP opcije



Što je DHCP zaštita imena?

DHCP Name Protection:

- Onemogućava da ime Windows operativnog sustava bude prebrisano DNS ime od strane ne Windows operativnog sustava s istim imenom
- Koristi DHCID zapis pomoću kojeg prati računala koja su originalno zatražila DNS ime
- Može se konfigurirati na razini mrežnog protokola ili raspona



Algebra

visoka škola za
primijenjeno računarstvo

Što je DHCP Failover?

DHCP failover:

- Omogućava da dva DHCP poslužitelja nude IP adrese i opcionalne konfiguracije istoj pod mreži ili rasponu
- Failover odnos mora imati unikatno ime
- Podržava hot standby i load sharing način rada

Kada koristimo DHCP failover:

- MCLT određuje kada failover partner preuzima kontrolu nad pod mrežom ili rasponom
- Auto state switchover interval određuje kada se smatra da je failover partner nedostupan
- Autentifikacija poruka može potvrditi failover poruke
- Pravila vatrozida se automatski konfiguriraju na DHCP poslužitelju



Konfiguracija naprednih DNS postavki

- Upravljanje DNS servisom
- Optimizacije DNS imenske rezolucije
- Što je GlobalNames zona?
- Opcije za implementaciju DNS sigurnosti
- Kako radi DNSSEC
- Nove DNSSEC mogućnosti u Windows Server 2012



Algebra

visoka škola za
primijenjeno računarstvo

Upravljanje DNS servisom

Da bi upravljali DNS servisom:

- Delegirajmo DNS administraciju kroz članstvo u DNS Admins grupi
- Pregledajmo DNS zapise u Event Viewer
- Omogućimo DNS debug logging u DNS konzoli
- Omogućimo aging i scavenging da bi izbrisali zastarjele zapise

Metode sigurnosnih kopija DNS baze ovise o tome kako je baza implementirana:

- Active Directory-integrirane zone možemo backupirati pomoću system state sigurnosne kopije, korištenjem dnscmd komande ili Windows PowerShell
- Ne integrirane primarne zone su tekstualne datoteke koje možemo jednostavno kopirati ili backupirati pomoću backup alata

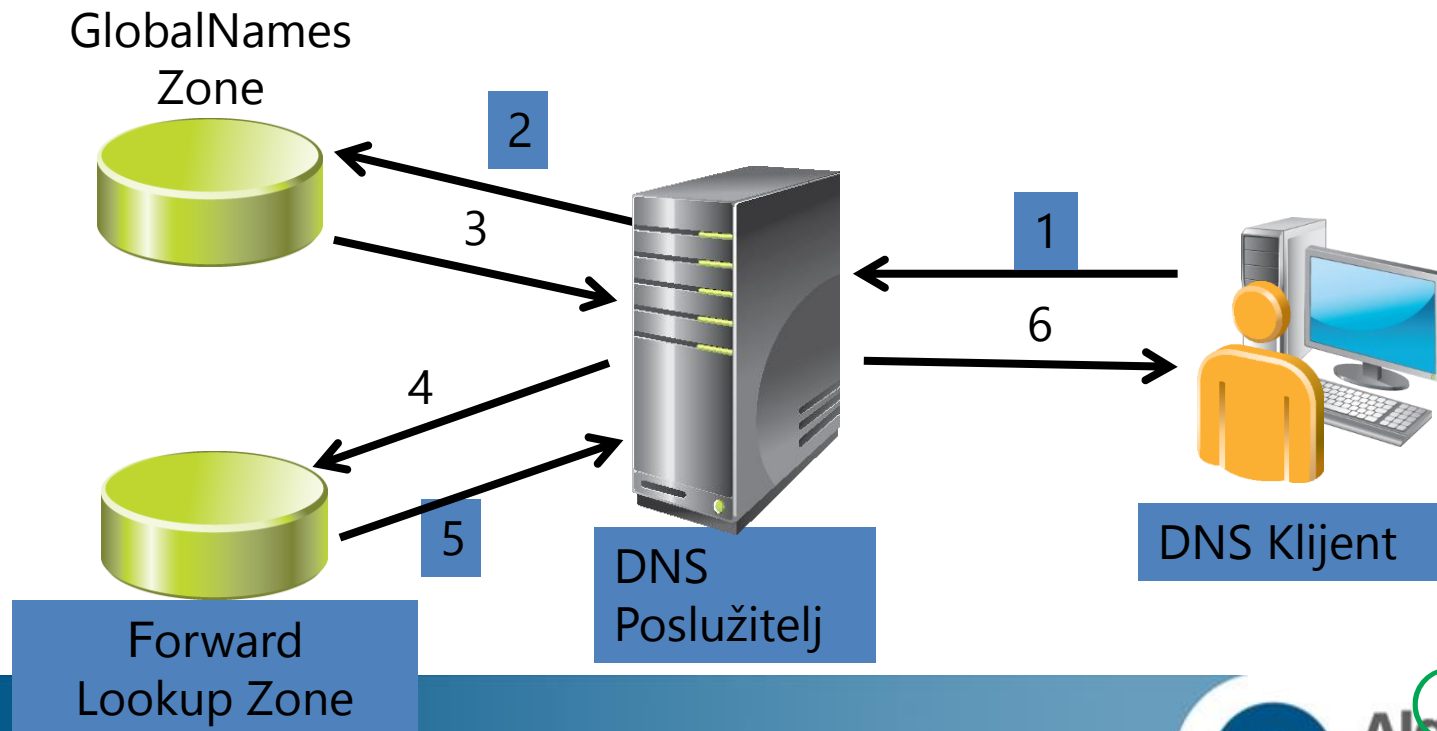


Optimizacije DNS imenske rezolucije

Opcija	Opis
Prosljeđivanje	Prosljeđuje DNS zahtjeve koji se ne mogu lokalno riješiti drugim DNS poslužiteljima
Uvjetno prosljeđivanje	Prosljeđuje upite za specifične DNS sufikse specifičnim DNS poslužiteljima
Stub zone	Replicirana kopija određenih DNS zapisa koji identificiraju autoritativne DNS poslužitelje za specifične DNS domene
Slaganje prema mrežnim maskama	Odgovara s adresom računala koje je blizu na osnovu IP adrese klijenta

Što je GlobalNames zona?

GlobalNames zona omogućava da se jednostavna imena mapiraju u više DNS domenskih okruženja



Opcije za implementaciju DNS sigurnosti

Opcija	Opis
DNS cache locking	Onemogućava prebrisivanje unosa u cache zapisima dok ne istekne TTL
DNS socket pool	Randomizira izvorišni port koji se koristi za zadavanje DNS upita Uključeno automatski u Windows Server 2012
DNSSEC	Omogućava kriptografsko potpisivanje DNS zapisa tako da klijenti mogu potvrditi dobivene odgovore

DNSSEC funkcionira kako slijedi:

- Ako je zona digitalno potpisana, odgovor na upit će sadržavati digitalni potpis
- DNSSEC koristi trust anchors, to su specijalne zone koje čuvaju javne ključeve koji su povezani s digitalnim potpisima
- Oni koji šalju upite koriste trust anchors da bi dohvatili javne ključeve i izgradili lanac vjerovanja
- DNSSEC zahtjeva da trust anchors budu konfigurirani na svim DNS poslužiteljima koji sudjeluju u DNSSEC
- DNSSEC koristi NRPT, koja sadrži pravila koja kontroliraju ponašanje klijenta koji traži informaciju i dobiva odgovor



Nove DNSSEC mogućnosti u Windows Server 2012

DNSSEC poboljšanja za Windows Server 2012 :

- Jednostavnija DNSSEC implementacija
- DNSSEC Zone Signing čarobnjak koji nas vodi kroz konfiguraciju digitalnog potpisivanja i ostalih DNSSEC partnera
- Novi zapisi:
 - DNSKEY
 - DS
 - RRSIG
 - NSEC



IPAM implementacija

- Što je IPAM?
- IPAM komponente
- IPAM zahtjevi za implementaciju
- IPAM upravljanje i nadgledanje
- IPAM topologije implementacije
- Planiranje IPAM kapaciteta
- Integracija IPAM i VMM
- Upravljanje virtualnim adresnim prostorima iz IPAM
- IPAM RBAC



Algebra

visoka škola za
primijenjeno računarstvo

- IPAM funkcionalnosti su podijeljene u četiri grupe:
 - IPAM otkrivanje
 - Upravljanje IP adresnim prostorom
 - Nadgledanje i upravljanje s više poslužitelja
 - Nadgledanje i praćenje korištenja IP adresa
- Nove mogućnosti koje Windows Server 2012 R2 donosi:
 - Poboljšan RBAC
 - Upravljanje virtualnim adresnim prostorom
 - Poboljšano upravljanje DHCP poslužiteljima
 - Podrška za vanjske baze
 - Podrška za nadogradnje i migraciju
 - Napredna Windows PowerShell podrška



IPAM komponente

IPAM se sastoji od tri glavne komponente:

- IPAM poslužitelj
- IPAM klijenti
- Poslužitelji kojima upravljamo



Algebra

visoka škola za
primijenjeno računarstvo

IPAM zahtjevi za implementaciju

Da bi imali uspješnu IPAM implementaciju mrežna infrastruktura tvrtke mora zadovoljiti nekoliko uvjeta:

- IPAM poslužitelj ne smije biti DC
- IPAM poslužitelj ne bi trebao imati nijednu drugu ulogu instaliranu
- Za upravljanje IPv6 adresnim prostorima, uključimo IPv6 na IPAM poslužitelju
- Prijavimo se na IPAM poslužitelj s domenskim vjerodajnicama
- Moramo biti član ispravne IPAM lokalne sigurnosne grupe na IPAM poslužitelju
- Uključimo praćenje account logon događaja za praćenje IP adresa i nadgledanje
- IPAM mora zadovoljiti ostale hardverske i softverske preduvjete



Algebra

visoka škola za
primijenjeno računarstvo

IPAM upravljanje i nadgledanje

Pomoću IPAM možemo:

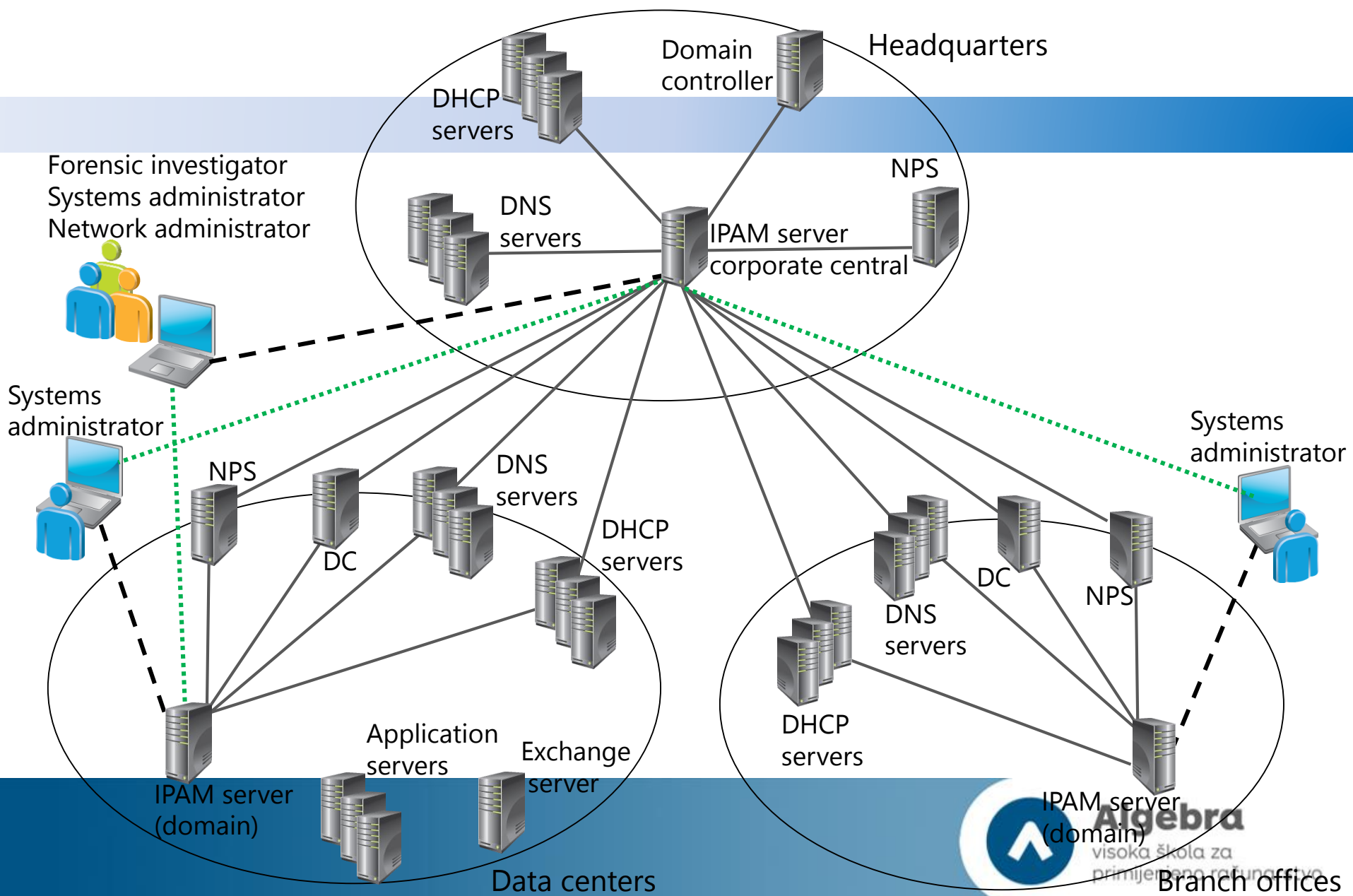
- Nadgledati iskorištavanje IP adresnog prostora
- Nadgledati DNS i DHCP ispravnost i stanje
- Konfigurirati razne DHCP postavke i vrijednosti iz IPAM konzole
- Koristiti katalog događaja da bi na jednom mjestu vidjeli sve konfiguracijske promjene koje su se dogodile



Algebra

visoka škola za
primijenjeno računarstvo

IPAM topologije implementacije



Planiranje IPAM kapaciteta

- Svaki IPAM poslužitelj može upravljati s do:
 - 150 DHCP poslužitelja
 - 500 DNS poslužitelja
 - 6000 DHCP raspona
 - 150 DNS zona
 - 20000 IP adresnih raspona (za IPv4 i IPv6 svaki)
- IPAM baza uključuje:
 - Objekte baze. Ne zahtjeva više od 1 GB
 - Podatke o utilizaciji. Oko 1 GB mjesečno za svakih 10000 IP adresnih raspona
 - Podaci kataloga događaja. Oko 0.6 GB za svakih milijun događaja



Algebra

visoka škola za
primijenjeno računarstvo

IPAM integracija s VMM

Da bi integrirali VMM i IPAM, napravimo sljedeće korake:

1. Provjerimo da su satovi na VMM poslužitelju i IPAM poslužitelju sinkronizirani
2. Dodajmo IPAM poslužitelj u VMM tkanje (fabric) kao mrežni servis
3. Definirajmo Run As račun za poslužitelj u VMM koji je dio IPAM ASM Administrators uloge i Remote Management Users grupe



Algebra

visoka škola za
primijenjeno računarstvo



OVERVIEW
SERVER INVEN...
IP ADDRESS SP...
IP Address Bl...
IP Address In...
IP Address R...
VIRTUALIZED I...
MONITOR AN...
DNS and DH...
DHCP Scopes
DNS Zone M...
Server Groups

IPv4

Provider IP Ad...

Customer IP A...

IPv6

Provider IP Ad...

IPv4

IPv4 | 3 total

Current view: IP Address Spaces

Filter

+ Add criteria

Utilization	Name	Type of IP address space	Access Scope	Percentage Utilized	Owner	Description
Under	Security Department	Customer IP Address Space	\Global	0.00		Security Department Network
Under	Default IP Address Space	Provider IP Address Space	\Global	0.00		Default Provider IP Address Space
Under	AdatumHQ	Provider IP Address Space	\Global	0.00		Adatum HQ Datacenter

Details View

Security Department

Configuration Details Event Catalog

Description:

Security Department Network

Name: Security Department

Type of IP address space: Customer IP Address Space

Owner:

Access Scope: \Global

Isolation Method: NVGRE

Utilization: Under

Percentage Utilized: 0.00

Provider IP address space: AdatumHQ

Is Inherited Access Scope: Yes



IP ADDRESS SPACE

IP Address Blocks

IP Address Inventory

IP Address Range Groups

VIRTUALIZED IP ADDRESS SPACE

MONITOR AND MANAGE

DNS and DHCP Servers

DHCP Scopes

DNS Zone Monitoring

Server Groups

EVENT CATALOG

ACCESS CONTROL

Roles

Access Scopes

Access Policies

Roles

Roles | 8 total

TASKS ▾

Add User Role...

Export...

Name	Built-in Role
DNS Record Administrator Role	Yes
IP Address Record Administrator Role	Yes
IPAM Administrator Role	Yes
IPAM ASM Administrator Role	Yes
IPAM DHCP Administrator Role	Yes
IPAM DHCP Reservations Administrator Role	Yes
IPAM DHCP Scope Administrator Role	Yes
IPAM MSM Administrator Role	Yes

Upravljanje IP adresnim prostorom pomoću IPAM servisa

- Korištenje IPAM-a za upravljanje IP adresama
- Dodavanje adresnih prostora u IPAM
- Uvoženje i promjene u adresnim prostorima
- Pronalaženje, alociranje i povrat IP adresa
- Održavanja inventara IP adresa u IPAM-u
- Nadgledanje IPAM

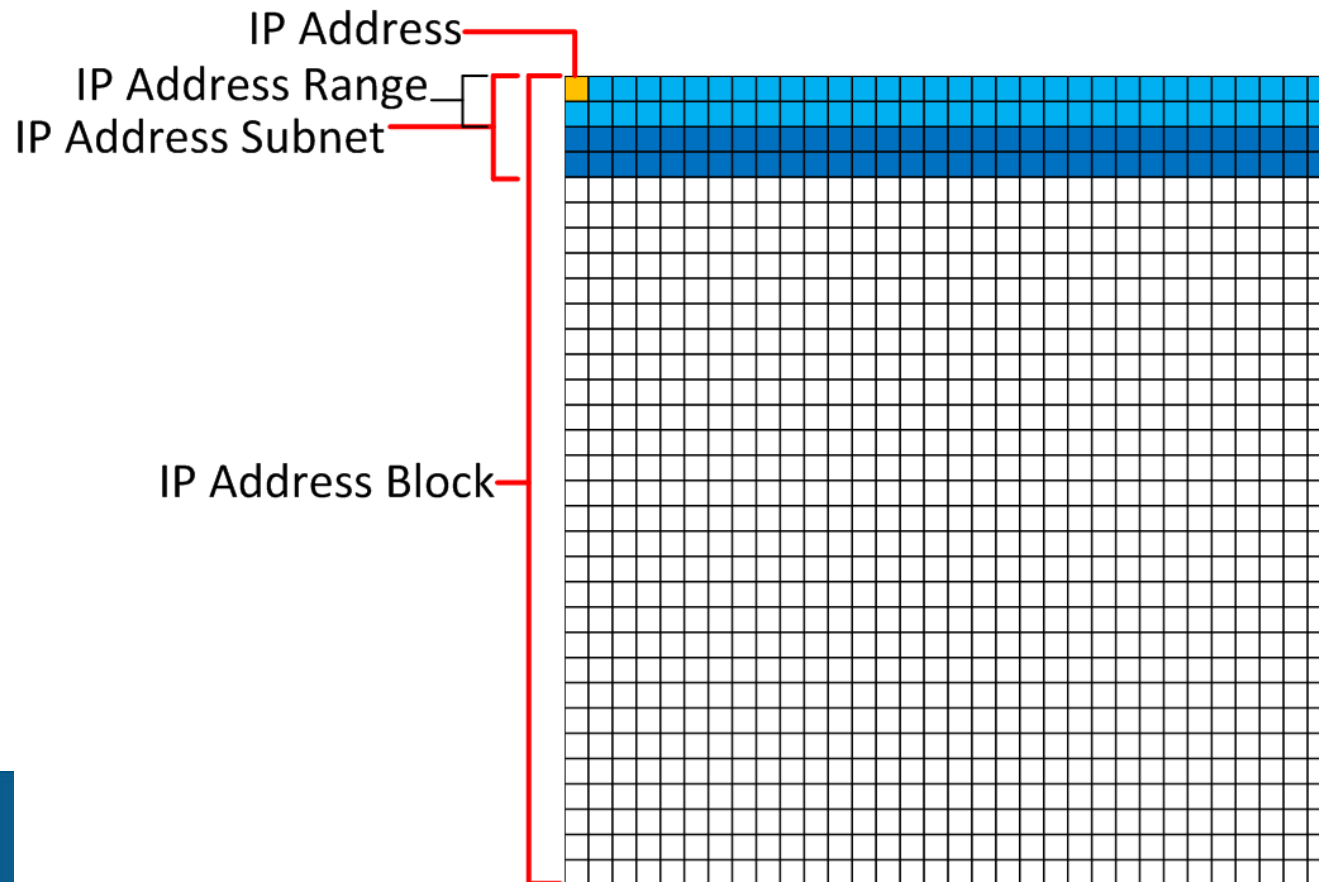


Algebra

visoka škola za
primijenjeno računarstvo

Korištenje IPAM-a za upravljanje IP adresnim prostorima

IP adresni prostor je podijeljen u blokove, pod mreže, raspone, i pojedine adrese:



IP adresni prostor možemo vidjeti i upravljati njime pomoću sljedećih alata u konzoli:

- IP address blocks
- IP address ranges
- IP addresses
- IP inventory
- IP address range groups

IP adresni prostor možemo nadgledati pomoću sljedećih alata u konzoli :

- DNS and DHCP servers
- DHCP scopes
- DNS zone monitoring
- Server groups



Dodavanje adresnih prostora u IPAM

Edit IP Address Subnet

Edit IPv4 Address Subnet

Show All

- General -
- Virtualization +
- Custom Configura... +

IP Address Subnet Properties

Modify the values to update the IPv4 address subnet:

* Name:

* Network ID:

* Prefix length (22 - 32):

VLAN ID:

Owner:

Description:



Uvoženje i promjene u adresnim prostorima

- Za uvoz pojedinačnih IP adresa koristimo tekstualne datoteke
- Obvezna polja za uvoz IP adresa su:
 - IP Address
 - Managed by Service
 - Service Instance
 - Device Type
 - IP Address State
 - Assignment Type
- Koristimo tekstualne datoteke za uvoz ili promjene raspona IP adresa
- Obvezna polja za uvoz blokova IP adresa su:
 - Network
 - Start IP address
 - End IP address
 - RIR



Algebra

visoka škola za
primijenjeno računarstvo

Pronalaženje, alociranje i povrat IP adresa

Reclaim IP Addresses

Select IP addresses to reclaim

☒ Delete DNS resource records ☒ Delete DHCP reservation

Select IP addresses to reclaim from the identified IP address range

Select addresses to reclaim

Summary

Selected IP address ranges:

Network	Percentage Utilized	Reclaim Last Run	Start IP Address	End IP Address	Managed by Service	Service Instance	Assigned Addresses	Utilized Addresses
192.168.30.0/24	1.57		192.168.30.1	192.168.30.254	IPAM	Localhost	254	4

Select IP addresses to be reclaimed:

	Expiry Status	Expiry Date	IP Address	MAC Address	Managed by Service	Service Instance	Device Name	Device Type	IP Address State
<input type="checkbox"/>	Not expired		192.168.30.1		IPAM	Localhost		Host	In-Use
<input type="checkbox"/>	Not expired		192.168.30.2		IPAM	Localhost		Host	In-Use
<input type="checkbox"/>	Not expired		192.168.30.3		IPAM	Localhost		Host	In-Use
<input type="checkbox"/>	Not expired		192.168.30.4		IPAM	Localhost		Host	In-Use

Select all Unselect all

Reclaim

Cancel




IPv4
IPv4 | 1 total

Current view: IP Addresses

Filter

Duplicate Expiry Status IP Address MAC Address Managed by Service Service Instance Access Scope IP Range Virtualized

No	 Not expired	192.168.30.1	IPAM	Localhost	\Global	192.168.30.1-192.168.30.254	No
----	---	--------------	------	-----------	---------	-----------------------------	----

Details View
192.168.30.1

Configuration Details Event Catalog

- Edit IP Address...
- Create DHCP Reservation
- Create DNS Host Record
- Create DNS PTR Record
- Delete DHCP Reservation
- Delete DNS Host Record
- Delete DNS PTR Record
- Delete



Nadgledanje IPAM-a

Pomoću IPAM možemo:

- Nadgledati iskorištenje IP adresnog prostora
- Nadgledati stanje DNS i DHCP servisa
- Konfigurirati razna DHCP svojstva i njihove vrijednosti iz IPAM konzole
- Koristiti event katalog kao centralni repozitorij za sve promjene konfiguracije koje su se dogodile



Algebra

visoka škola za
primijenjeno računarstvo



Algebra

visoka škola za
primijenjeno računarstvo