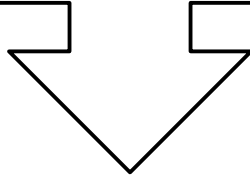


بِسْمِ اللّٰهِ الرَّحْمٰنِ الرَّحِیْمِ

عنوان تحقیق

IP Address Management (IPAM)



استاد محترم: جناب آقا مہندس منصور

نگارندہ: یوسف رشید

جہت درسی: MCSA 2016



مجمع فنی پھستان

## هدف کلی تحقیق

آشنایی کامل با (IPAM) IP Address Management

## اهداف جزئی

۱. آشنایی با پیش نیازها
۲. آشنایی با برخی قابلیت‌های IPAM
۳. آشنایی با برخی محدودیت‌های IPAM
۴. آشنایی با معماری سرویس
۵. آشنایی با سرورهای تحت مدیریت
۶. آشنایی با زمان بندی
۷. آشنایی با محل ذخیره سازی اطلاعات
۸. آشنایی با مدیریت سطوح دسترسی
۹. چرا باید سرویس IPAM را پیاده سازی کنیم

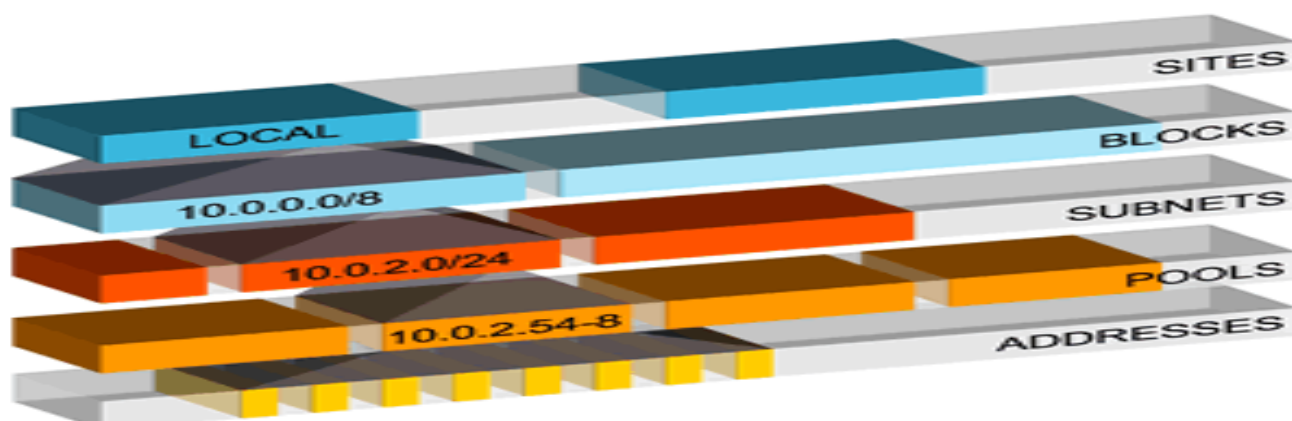
## هدف کاربردی

با استفاده از IPAM می توان به صورت متمرکز فضای آدرس‌های IP سازمان را مشاهده، مدیریت و پیکربندی کرد



## مقدمه:

امروزه مدیریت و نظارت بر **IP Address Space** در سازمان های بزرگ، سبب پیچیدگی های متعددی شده است. بسیاری از سازمان ها از فایل صفحه گسترده (Excel همانند **Spreadsheets**) جداگانه جهت مدیریت و نظارت بر وقایع زیرساخت های آدرس دهی سازمان ها استفاده می کنند. با گسترش شبکه های کامپیوتری و سرویس ها، پیچیدگی رهیافت فوق الذکر افزوده شده و علاوه بر آن سبب می گردد؛ جریان های کاری و فشار کاری افزایش یابد. با به کارگیری از سرویس **IP Address Management (IPAM)** در شبکه های مبتنی بر سرویس های مایکروسافت، این امکان حاصل می گردد تا ردگیری وقایع فضای آدرس های داینامیک در سازمان تسهیل شده، مدیریت و نظارت بر آدرس های منطقی دستی بهبود پیدا کرده و همچنین قابلیت یکپارچگی با زیرساخت های مجازی سازمان ایجاد گردد.



سرویس IP address management که یکی از Feature های جدید در Windows Server 2012 به شمار می آید، یک Framework مرکزی جهت مدیریت IP Address Space و سرویس های متناظر آن در سازمان همانند DNS و DHCP فراهم می آورد. IPAM با استفاده از قابلیت Auto Discovery در یک Forest فعال می گردد و با سطوح دسترسی Role-Based امکان نظارت، مدیریت و ردگیری وقایع را برای اپراتور ها فراهم می آورد.

## IPAM چیست و چگونه راه اندازی می شود

با یک مقاله دیگر از ویندوز سرور ۲۰۱۶ در خدمت شما هستیم همانطور که می دانید یکی از موارد مهم و اساسی در هر شبکه امکان کنترل و نظارت بر روی IP های استفاده شده می باشد. یکی از قابلیت های ویندوز سرور ۲۰۱۶ این است که با استفاده از IPAM می توان به صورت متمرکز فضای آدرس های IP سازمان را مشاهده، مدیریت و پیکربندی کرد. قطعاً برای شما هم پیش آمده است که بخواهید بر روی پروتکل های DNS و DHCP خود نظارت داشته باشید و آدرس های IP خود را مدیریت کنید، به طوری که امکان ردیابی آدرس های IP (هر IP قبلاً متعلق به کدام دستگاه بوده و در حال حاضر کجا مورد استفاده قرار گرفته) وجود داشته باشد.

## چرا باید سرویس IPAM را پیاده سازی کنیم؟

در سازمانهای بسیاری با این موضوع مواجه می شوند که چندین DNS Server و DHCP Server و یا حتی چندین NPS وجود داشته باشد و ما برای مدیریت آنها مجبور به ریموت زدن به سرورهای مختلف باشیم. علاوه بر این که ما با این کار دچار سردرگمی می شویم از نظر امنیتی هم کار زیاد جالبی نیست در ویندوز سرور ۲۰۱۲ به بعد مایکروسافت یک Feature رو اضافه کرده به نام IPAM (مخفف IP Address Management) که وظیفه این رول مدیریت متمرکز DNS , DHCP و NPS می باشد.

در صورتی که گزارش دقیقی از آدرس های IP موجود در شبکه خود نداشته باشید، ممکن است ساعت ها وقت، صرف عیب یابی شبکه خود که ناشی از تداخل IP است، کنید. فرض کنید به سیستمی که تازه وارد شبکه شده است، به اشتباه IP یکی از سرورهای خود را بدهید، اتفاقی که می افتد شاید تبدیل به یک فاجعه بزرگ شود. یکی از راه های مقابله با این مشکلات (IPAM (IP Address Manager است. همچنین برای تشخیص محدوده IP و Subnet ها، مدیریت IP های آزاد و بلاک شده، از بین رفتن پراکندگی IP و ... به کار می آید. مهم ترین کاربردهای سرویس IPAM به شرح زیر می باشد.

(۱) برنامه ریزی: جایگزینی IPAM با گزارش گیری های دستی و پراکنده سبب می شود امکان برنامه ریزی های دقیق تر حاصل گردد.

(۲) مدیریت و جریان های کاری: IPAM یک پلتفرم متمرکز جهت مدیریت آدرس های IP فراهم می آورد. این امر سبب می شود میز پشتیبانی (Help Desk) بتواند تغییرات مطلوب را (طی ایجاد دسترسی های متناسب بر اساس Role-Based Access Control) برای کلاینت های تحت پشتیبانی خود اعمال نماید.

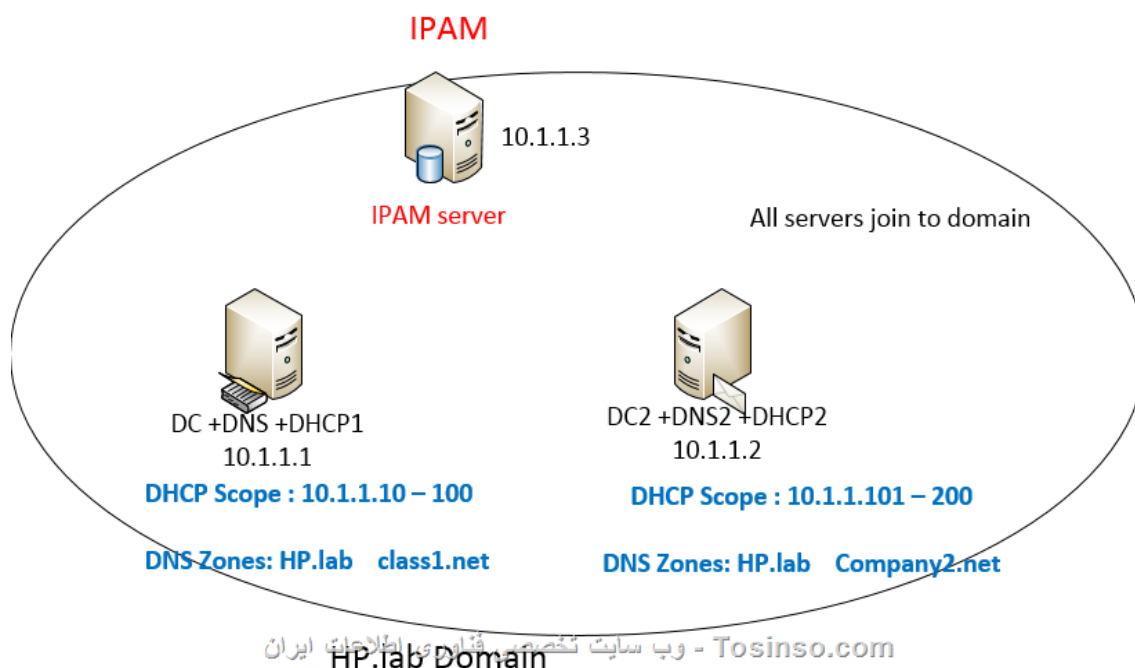
(۳) ردگیری و بازبینی: IP address management یک ابزار یکپارچه جهت ردگیری آدرس های lease شده و همچنین تنظیمات روی سرور های تحت نظارت خود ایجاد می کند.

IP Address Management یا به اختصار IPAM یک راهکار Agentless جهت Discovery، مانیتورینگ، نظارت و مدیریت IP Address Space است. با استفاده از این Feature در ویندوز امکان نظارت و مدیریت یکپارچه سرور های DHCP، DNS و NPS ایجاد می گردد. IPAM به صورت خودکار می تواند زیرساخت های IP Address Space (با استفاده از فرآیند Provisioning) را دیسکاور کند و یک رابط مرکزی برای مدیریت این امر فراهم می آورد.

آخرین نسخه ویندوز سرور ۲۰۱۶ با قرار دادن یک Feature امکان دسترسی به IPAM را برای شما فراهم کرده است.

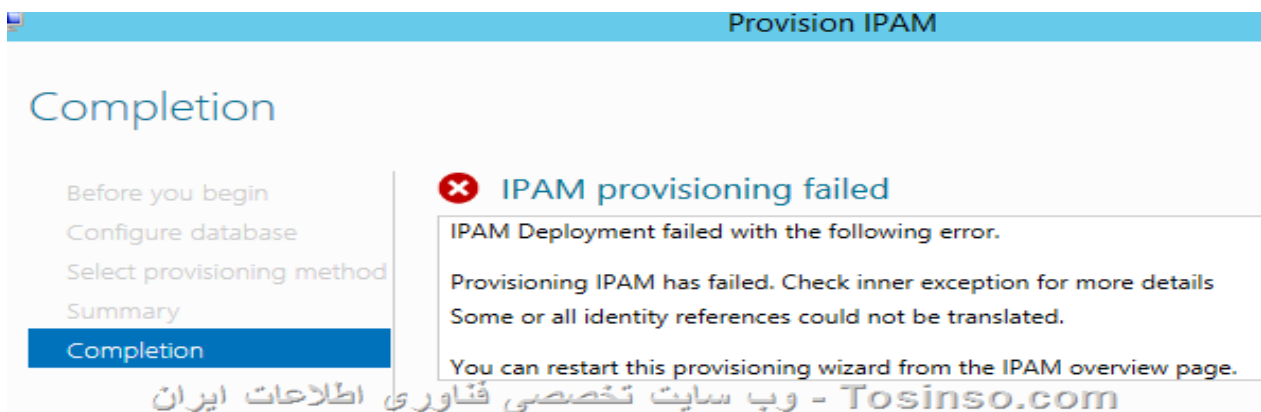
## برخی قابلیت‌هایی که با استفاده از IPAM می‌توانید در شبکه داشته باشید

۱. پیدا نمودن تمام فضای آدرس IP و بررسی در دسترس بودن آنها
۲. پیدا نمودن یک IP جدید و ثبت آن در DNS
۳. بررسی وضعیت پر بودن DHCP Scope ها در شبکه و...
۴. مدیریت یکپارچه‌ی فضای دینامیک و استاتیک IP آدرس
۵. تشخیص و مدیریت ناسازگاری‌ها، همپوشانی‌ها، و تکرارهای فضای آدرس بین سیستم‌ها
۶. نمای فهرست‌وار فضای IP آدرس با قابلیت سفارشی‌سازی بالا
۷. مانیتورینگ متمرکز و گزارش از نحوه به کار گیری آدرس‌ها
۸. پشتیبانی از مانیتورینگ بهره‌وری آدرس برای IPv4
۹. کشف خودکار دامنه‌ی IP آدرس از محدوده‌های DHCP
۱۰. پشتیبانی از وارد و خارج کردن IP آدرس‌ها و دامنه‌های IP آدرس
۱۱. هشدارهای میزان مصرف IP آدرس و اخطارهایی با آستانه‌های تعیین شده
۱۲. تشخیص و تخصیص IP آدرس‌های موجود
۱۳. IPAM می‌تواند با یک سرور DHCP 150 و 6000 Scopes را مدیریت نماید.
۱۴. IPAM می‌تواند به صورت همزمان 500 DNS و 1500 Zone را مدیریت نماید.



## برخی محدودیت های IPAM

۱. IPAM تنها میتواند اطلاعات کامپیوترهایی را به دست آورد که دارای نسخه ویندوز سرور ۲۰۰۸ به بالا باشند.
۲. IPAM یک سرویس اختصاصی مایکروسافت بوده که تنها از سیستم عاملهای این شرکت پشتیبانی میکند.
۳. IPAM نمی تواند روی Domain Controller ها فعال شود.
۴. Address Utilization صرفا روی IPv4 عمل می کند.
۵. IPAM نمی تواند IP Address consistency را روی network router و switch ها بررسی کند.
۶. IPAM امکان auditing را برای IPv6 فراهم نمی آورد.
۷. یک IPAM Server تنها در یک Forest می تواند عمل کند.
۸. IPAM تنها از Windows Server 2012 R2 امکان اتصال به SQL Server را دارد
۹. IPAM تنها از Windows Server 2012 R2 امکان Role-Based Access Control را به صورت مناسبی دارا می باشد.
۱۰. IPAM از سیستم های غیر مایکروسافتی جهت Management و Configuration پشتیبانی نمی کند. امکان Import کردن اطلاعات برای دیوایس های غیر مایکروسافتی وجود دارد.
۱۱. جهت Provisioning لازم است ۳ سیاست گروهی مختلف روی اشیاء معینی اعمال گردد.
۱۲. IPAM Server لازم است یک Member Server باشد.
۱۳. جهت مدیریت IPAM Server اکانت دامین با دسترسی مناسب لازم می باشد.
۱۴. IPAM روی دومین کنترلر قابل نصب نیست و با پیغام زیر مواجه میشیم.



تصویر زیر به عنوان یک مثال میزان Address Utilization را در یک شبکه نمایش می دهد.

The screenshot shows the Server Manager IPAM interface. On the left, there is a navigation pane with categories like OVERVIEW, SERVER INVENTORY, IP ADDRESS SPACE, and MONITOR AND MANAGE. The main area displays a table of IP Address Ranges. One range is highlighted in blue, and a context menu is open over it. Below the table is a 'Details View' for the selected range, which includes a 'Utilization Trend' graph showing the percentage of address space used over time.

Utilization	Overlapping	Network	Start IP Address	End IP Address	Managed by Service	Assigned Addresses	Utilized Addresses	Assignment Type
Optimal	No	10.86.50.0/26	10.86.50.3	10.86.50.62	MS DHCP	60	34	Dynamic
Optimal	No	10.86.15.0/26	10.86.15.3	10.86.15.62	MS DHCP	60	35	Dynamic
Optimal	No	10.86.4.0/24	10.86.4.6	10.86.4.254	MS DHCP	249	70	Dynamic
Optimal	No	10.72.206.0/24	10.72.206.6	10.72.206.254	MS DHCP	244	145	Dynamic
Over	No	10.72.144.0/22	10.72.144.3	10.72.144.254	MS DHCP	1000	1020	Dynamic
Under	No	10.72.132.0/22	10.72.132.3	10.72.132.254	MS DHCP	0	0	Dynamic
Under	No	10.67.64.0/19	10.67.64.6	10.67.64.254	MS DHCP	0	517	Dynamic
Under	No	10.67.25.0/24	10.67.25.4	10.67.25.254	MS DHCP	0	2	Dynamic
Under	No	10.67.24.0/24	10.67.24.4	10.67.24.254	MS DHCP	0	1	Dynamic
Under	No	10.67.23.0/24	10.67.23.4	10.67.23.254	MS DHCP	0	0	Dynamic
Under	No	10.67.22.0/24	10.67.22.4	10.67.22.254	MS DHCP	0	0	Dynamic

Annotations in the image point to:

- IP Address Range along with Utilization Statistics (points to the table row)
- IP Address Block hierarchy (points to the left navigation pane)
- Utilization trend Graph of IP Address Range (points to the graph in the details view)

## معماری سرویس

سرویس IP address management سه معماری متمایز را به شرح زیر پشتیبانی می کند:

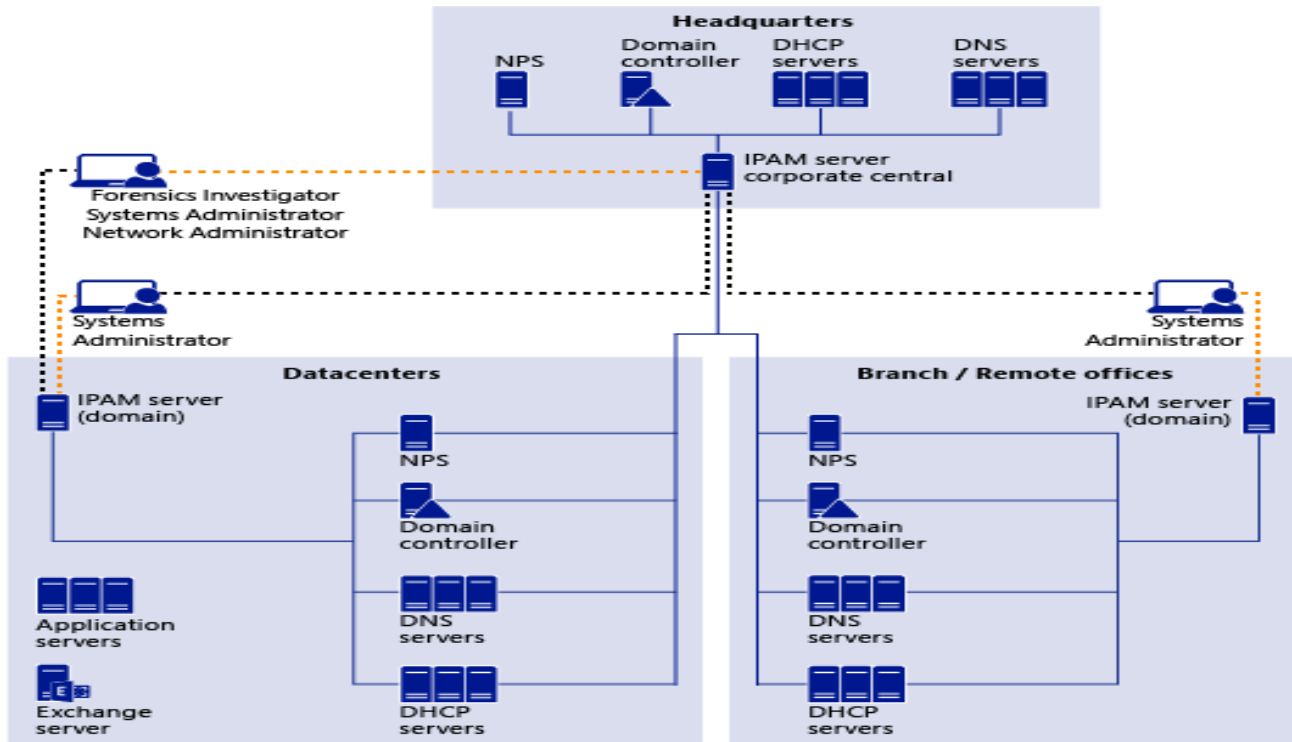
(۱) Distributed: در هر یک از سایت های فیزیکی یک IPAM Server مجزا ایجاد می گردد.

(۲) Centralized: استفاده از یک IPAM Server در سازمان.

(۳) Hybrid: ترکیبی از حالات فوق.

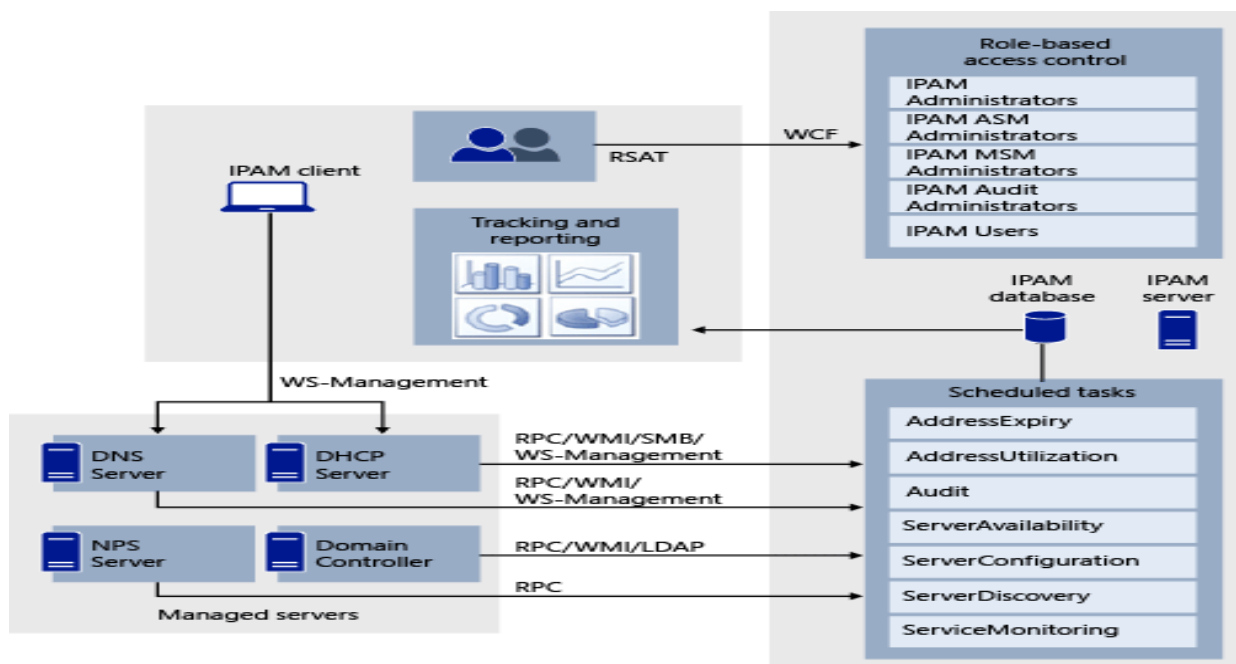


تصویر زیر یک معماری Hybrid را نمایش می دهد.



### سرور های تحت مدیریت

IPAM به صورت متناوب، جهت دیسکاور سرور های DNS, DHCP, NPS در سایت خود اقدام می کند و لازم است پس از دیسکاور شدن، به عنوان Managed Server معرفی گردند. تصویر زیر به صورت شماتیک ارتباطات فوق الذکر را نمایش می دهد.

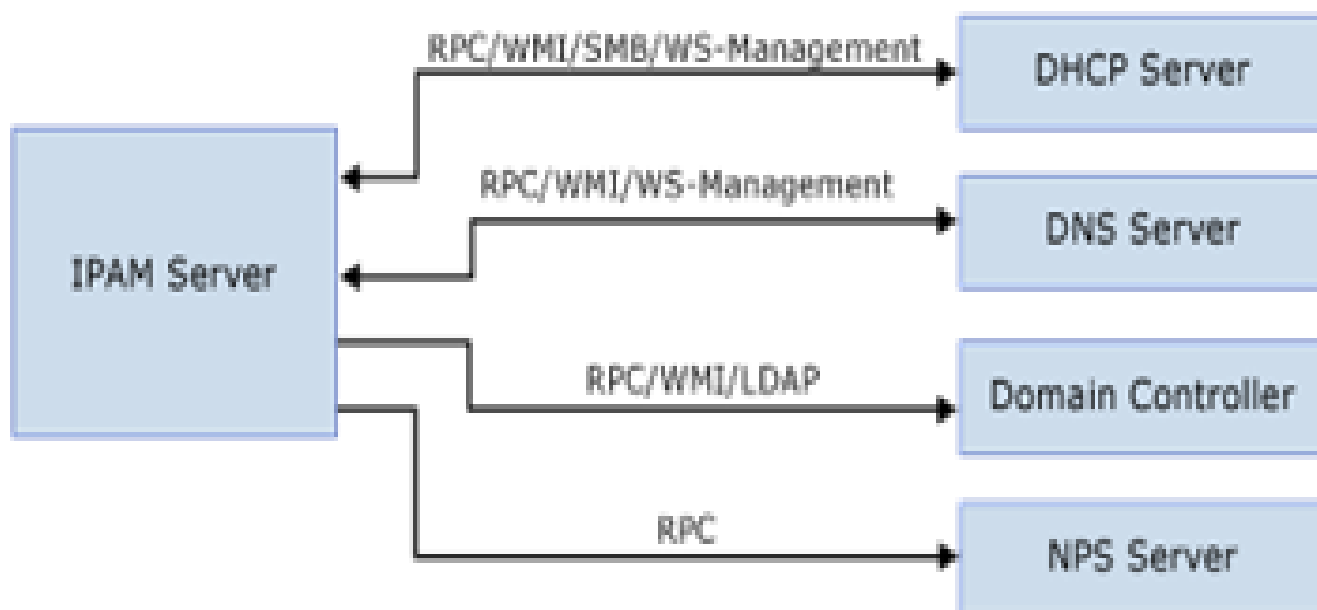


Windows Management Instrumentation .Remote Procedure Call (RPC) از IPAM Web Services for Management WS- و Server Message Block SMB.(WMI) Management برای جمع آوری اطلاعات و نظارت بر سرور های تحت مدیریت خود استفاده می کند.

جدول زیر به صورت مشروح این مورد را نشان می دهد.

فعالیت ها	متد ارتباطی	سرور تحت مدیریت
Monitor: IP address utilization Monitor: Service status Configure: Servers and scopes Audit: IP address lease events Audit: DHCP configuration events	RPC, WMI, SMB, WS- Management	DHCP
Discover: DNS servers Monitor: DNS zone health Configure: DNS zones	RPC, WMI, WS- Management	DNS
Discover: DNS and DHCP servers Validate: Managed servers Audit: User and device logon events	RPC, WMI, LDAP	Domain Controller
Audit: User and device logon events	RPC	NPS

تصویر زیر اطلاعات جدول فوق را به اختصار نمایش می دهد.



## زمان بندی

سرویس IPAM دارای تعدادی Scheduled Task است که جهت جمع آوری اطلاعات اجرای می گردند. زمان بندی پیشنهادی به شرح زیر است.

نام وظیفه	زمان بندی	بازه
Address Expiry	1day	Indefinite
Address Utilization	2hours	Indefinite
Audit	1day	Indefinite
Server Availability	15minutes	Indefinite
Server Configuration	6hours	Indefinite
Server Discovery	1day	Indefinite
Service Monitoring	30minutes	Indefinite

## محل ذخیره سازی اطلاعات

IPAM با استفاده از Lightweight Directory Access Protocol LDAP به دیسکآوری DHCP Server ها پرداخته و با استفاده از SMB برای یافتن اطلاعات Lease ها عمل می کند. در Windows Server 2012 تنها امکان استفاده از Windows Internal Database جهت ذخیره سازی اطلاعات IP address management وجود دارد. در Windows Server 2012 R2 این امکان حاصل شده است تا SQL Server نیز به عنوان Database استفاده گردد. استفاده از SQL Server امکانات جدیدی را به IPAM اضافه نمی کند با این وجود به صورت عمومی مزایای زیر را به همراه دارد:

۱. مقیاس پذیری بیشتر

۲. استفاده از راهکارهای Disaster Recovery

## مدیریت سطوح دسترسی

در Windows Server 2012 R2 امکان افزودن Custom Role جهت Role-Based Access Control ایجاد شده است؛ با این وجود گروه های کاربری پیش فرض IP address management، در اکثر سناریو ها پاسخگوی نیاز های طراحی شده است.

سطوح دسترسی پیش فرض به شرح زیر است.

شرح	نام	نوع
DNS Resource Record ها در مدیریت	DNS record administrator	Role
IP address ها به استثنای IP Address مدیریت spaces ranges blocks و subnets	IP address record administrator	Role
IPAM مدیریت تمام اشیاء و تنظیمات در	IPAM administrator	Role
ها IP Address مدیریت کامل روی	IPAM ASM administrator	Role
ها DHCP Server مدیریت کامل	IPAM DHCP administrator	Role
ها Reservation مدیریت	IPAM DHCP reservations administrator	Role
DHCP های Scope مدیریت	IPAM DHCP scope administrator	Role
DHCP و DNS مدیریت کامل	IPAM MSM administrator	Role
به صورت پیش فرض، تمام اشیاء موجود در IPAM در یک Scope به این نام قرار می گیرند.	Global	Role

بدیهی است، تنظیم سطوح دسترسی و حوزه متناسب برای کاربران سرویس IPAM از اهمیت بسیار بالایی برخوردار است.

## پیش نیازها

جدول زیر، پیش نیازهای سرویس IPAM را نشان می دهد.

ابزار یا ویژگی	شرح
Remote Server Administration Tools	جهت مدیریت سرویس های تحت نظارت
Windows Internal Database	جهت ذخیره سازی اطلاعات IPAM
Windows Process Activation Service	IIS process model عمومی سازی
Group Policy Management	جهت مدیریت سیاست های گروهی که در ایجاد می گردد Provisioning فرآیند
.NET Framework 4.5 Features	Framework اجرایی .Net

## مراحل نصب IPAM

برای نصب IPAM از قسمت Features اقدام می کنیم

Select one or more features to install on the selected server.

Features	Description
<input type="checkbox"/> BitLocker Network Unlock	<p>IP Address Management (IPAM) Server provides a central framework for managing your IP address space and corresponding infrastructure servers such as DHCP and DNS. IPAM supports automated discovery of infrastructure servers in an Active Directory forest. IPAM allows you to manage your dynamic and static IPv4 and IPv6 address space, tracks IP address utilization trends, and supports monitoring and management of DNS and DHCP services on your network.</p>
<input type="checkbox"/> BranchCache	
<input type="checkbox"/> Client for NFS	
<input type="checkbox"/> Data Center Bridging	
<input type="checkbox"/> Direct Play	
<input type="checkbox"/> Enhanced Storage	
<input type="checkbox"/> Failover Clustering	
<input type="checkbox"/> Group Policy Management	
<input type="checkbox"/> IIS Hostable Web Core	
<input checked="" type="checkbox"/> Ink and Handwriting Services (Installed)	
<input type="checkbox"/> Internet Printing Client	
<input type="checkbox"/> IP Address Management (IPAM) Server	
<input type="checkbox"/> iSNS Server service	
<input type="checkbox"/> LPR Port Monitor	
<input type="checkbox"/> Management OData IIS Extension	

Tosinso.com - وب سایت تخصصی فناوری اطلاعات ایران

ویا از طریق پاورشل با دستور زیر

```
PS C:\> Get-WindowsFeature *ipam* | install-WindowsFeature
```

Or

```
PS C:\> install-WindowsFeature IPAM -includeAllSubfeature
```

پس از نصب IPAM وارد Server Manager شده و با انتخاب گزینه IPAM , شش مرحله به ما نمایش داده می شود که باید کانفیگ شود تا راه اندازی این Feature انجام شود.

باتشکر فراوان از توجه شما استاد عزیز