efficient iP®

White Paper

Is Microsoft's DDI Good Enough ?

Evaluation criteria

- Increases network uptime and availability by eliminating human errors
- Reduces operating costs by automating administrator tasks
- Ensures Service Level Agreement (SLA) compliance with policy-based deployments
- Identifies unused network resources for capacity planning
- Enhances security and productivity through role-based delegation

The days of tracking IP addresses on spreadsheets are long gone, or rather should be. A true IP Address Management (IPAM) system is much more than just a way of tracking subnets and addresses. IPAM encompasses the ability to track and manage an IP environment regardless of the type of address, network, or architecture.

True IPAM is an integral part of the network and works cohesively with network devices to gather and organize device information. Additionally, the IPAM system should be the cornerstone of automation in planning and managing the IP space as well as integrating technologies such as DNS and DHCP. From risk mitigation and business continuity to virtualization, security, and mobility (BYOD), IPAM is a fundamental contributing solution to the critical challenges enterprises face today.

DDI, which stands for DNS, DHCP, and IP Address management reflects more closely the true direction of IP Address Management architecture. True DDI applications are able to manage the environment end-to-end providing unified management of DNS-DHCP and IP addresses with virtual LANs and device interfaces.

This holistic approach ensures global visibility, consistency control, and automated management of the IP infrastructures and services. Ultimately, DDI simplifies the processes of design, deployment, and management of the network through policy driven automation.

Is IP Address Management just about tracking IP addresses?

IP Address Management, in the modern world, is much more than just converting a spreadsheet into an eye popping GUI. IP Address Management is an integral part of a true DDI solution. IP Address Management encompasses the ability to have an end-to-end capability. This includes integrating with network devices to collect and track devices and relationships.

These relationships include tracking a device with a user and a MAC address or clientID with an IP address as well as port connections and VLAN affiliations to the network infrastructure. Tracking this detail is critical in dynamic environments enabling Network Security to identify when a device has received an IP address and where it was connected on the network. IPAM should then allow for the planning and design of an end to end architecture not only at the DNS and DHCP services level but also at the network topology level. Lastly, the IPAM system should be able to integrate seamlessly into the processes and systems that have been established within the environment.

This means an IPAM system must be extensible and have a mechanism to share data with other applications. Because an IPAM system contains information about all devices, it follows that IP addresses and other IP-related information, should be integrated with a firewall-rule system to enforce IP address blocks. The IPAM system should also integrate with an asset tracking system to associate a device with asset information.

Is Microsoft 2012 a DDI Solution?

With Server 2012, Microsoft has completely confused everyone with the new interface. Those that have never touched a Microsoft server might find the interface enjoyable, but the remaining population is going to spend their time trying to figure out where everything was hidden. Many of the GUI options, tools, and applications have been relocated and are more difficult and time consuming to find.

Interface changes aside, changes to Server 2012 include the DNS, DHCP, and IP Address (DDI) technologies. Examining these closer, you find that Microsoft has just refined their DNS and DHCP services and added a management console for DHCP that is referred to as IPAM. While it may be called IPAM and referred to as IP Address Management, it is not. It is also not a DDI solution. Care should be taken before making assumptions on its capability and value. After analyzing the different aspects of the Microsoft environment, it becomes very apparent that there is nothing to be gained by implementing the MS IPAM environment and in fact, may lead to more issues in the environment.

DNS Server

There were changes in the MS DNS server delivered with Server 2012. However, very little enhancements were added to ease the management of zones and the ability to enforce standardization. The management of MS DNS was not enhanced to provide for ease and consistency in an environment. This makes managing a large and diverse environment complex and tends to lead to errors that occur for example when zones are not set up on the appropriate slave servers or one server may restrict updates to certain ACL's while another server may not. Standardizing a DNS server configuration to enforce corporate standards should be a requirement for any environment looking to implement an IPAM system. The Microsoft DNS server also does not offer any tools for securing the environment and putting security at the fore front of the DNS architecture. For that, a DDI solution is the only option.

DHCP Server

One of the biggest weaknesses with Microsoft's tools, especially with DHCP, was the fact that every server had to be set up and managed independently. There wasn't, and in reality, still isn't, a cohesive view of what was happening in the environment, how servers were set up and which server was responsible for what configuration. The management of the DHCP configuration is discussed further in the IPAM discussion later in this paper. The focus of this section is the importance of the performance and scalability of the DHCP service itself.

As long as your needs are basic, then MS DHCP server will meet that need. If the environment is a highload environment or a distributed environment, then MS DHCP server will probably not be reliable enough.

To provide the level of support, additional Microsoft servers would need to be implemented and thus increase the cost basis. As a basic DHCP server, the service itself is stable. However, when needing to scale, the limitations become evident. Based on Microsoft's testing, average transactions per second averages about 645 and this will vary based on the CPU speed and the number of DHCP scopes.

A transaction is either a new address (lease) acquisition or a renew of an existing address. Each packet between a DHCP server and a DHCP client contain a transaction ID to identify the conversation.

The performance capability of a DHCP server is very important. For example, in a Voice over IP (VoIP) environment, the phone expects a timely response from the DHCP server when it is booting. If the response is not received in the expected timeframe, the phones will not boot.

IP Address Management – IPAM

One of the most touted improvements to Server 2012 is the inclusion of an IPAM feature. This capability allows for the deploying, managing and monitoring of the IP address infrastructure by automatically discovering the IP address infrastructure. Evaluating the new IPAM capability, it is obvious very quickly that the goal is to simplify the management of Microsoft DHCP rather than a full IPAM solution. Environments that have a mixed platform architecture will quickly realize that the IPAM feature is not really designed for diverse environment. Microsoft's IPAM only supports domain joined DHCP, DNS and NPS servers in a single forest.

Each category described identifies some of the major areas of emphasis that should be evaluated before attempting to implement Microsoft's IPAM solution as an IPAM solution.

Data Configuration and Tracking

The auto discovery feature of MS IPAM 2012 requires access to Active Directory to discover network infrastructure servers. This discovery is necessary to enable IPAM services. Discovery allows administrators to identify servers running Windows Server® 2008 or later with the DNS Server, DHCP Server and AD DS role services installed.

This discovery process is extremely slow and typically, the Microsoft configuration guide recommends kicking it off and let it run overnight. What is being discovered are DHCP scopes that have been defined in Active Directory along with DNS domains that have been defined on a MS DNS server.

An MS IPAM server can monitor and manage multiple domains as long as they are part of the same Active Directory forest as the IPAM server. In large, distributed environments, there may be multiple forests and thus multiple IPAM systems would need to be implemented. And, these MS IPAM systems would contain different data and would not have a view into each other's data.

The multi-server management feature of the MS IPAM interface enables an administrator to edit and configure key properties of multiple DHCP servers and scopes across the organization. Please note, key properties can be managed, not all properties. While Microsoft states that the IPAM system facilitates monitoring and tracking of DHCP service status and utilization of DHCP scopes, this information is only as valid as the tasks are scheduled to run. The data within the IPAM system, from utilization to monitoring, is updated based on tasks. For example, the address utilization task collects IP address space usage data from DHCP servers to display current and historical utilization. By default, this task runs every 2 hours.

That means the data is only as valid as the last time the task ran. Ideally, all of the DHCP information should be updatable in real time to have a true reflection of the environment. Real-time updates allow for a more reflection of the current status of the DHCP scopes and allow for better tracking for security in which device has what address.

A quality IPAM solution should include an auto discovery of more than just DHCP servers. As an IP Address Management solution should be tracking all addresses in the environment, it should also be able to track the relationship between these addresses. This includes querying network devices such as switches and routers and integrating in Level 2 and Level 3 information.

This strategy offers a better and more comprehensive understanding of the address environment: switch port occupancy rate, reclaim unused port/IPs/device over a period of time and device and IP address mobility on the network to name a few. Simply, the Microsoft IPAM tool does not deliver any of these capabilities.

Administrator Management

One of the first tasks to implementing the Microsoft IPAM service is to identify a provisioning method. Once one is chosen, it is permanent and the only way to change is to uninstall and reinstall the IPAM server. Provisioning is the process of enabling required permissions, file shares, and access settings on managed servers so that the IPAM server can communicate with them.

The Group Policy based method is the recommended method as manually trying to set everything will guarantee at least one if not two re-installations.

Once provisioning is configured, administrators are defined based on Microsoft IPAM Security groups. There are 5 pre-defined administrator roles. Users are then associated with one or more of these administrator roles. This provides a very limited flexibility in administration and delegation of those privileges. In addition, Administrator accounts are limited to those admins that have an account in Active Directory.

An IPAM solution should provide flexibility in administrative delegation that can accommodate a corporation's environment. Privileges should be able to be defined based on not just a Server but be able to split up who has permission to which subnet and address or DNS zones and DHCP scopes.

If you want to restrict the Email administrators with permission to manage just email servers that are scattered throughout the environment, you should be able to do that without have to give those admins permissions to everything. Microsoft IPAM's administration does not offer that flexibility. It is ridged and restricted to the predefined notions.

Application Flexibility

Many critical applications within an environment key off of critical information such as hostname, MAC address, or IP address. The ability to integrate with these applications should be a requirement for all businesses. Security monitoring and asset tracking are just two examples where integration is advantageous. This integration should be automatic and seamless. With MS IPAM, the only way to share information is to use PowerShell to push or pull data. There is not a way to integrate an external application automatically.

For example, if you would like to block an IP address, you would like to document the block within the IPAM database. When a block is set, that information should automatically be sent to the firewall or security database to update that a block was enabled. All of this communication should occur when a block is entered and not require an additional step of having to send an email or run a script to pull that information.

Ideally, the IPAM solution should allow for an action to be triggered on an event. If a field, be it an address, a user defined field, subnet, network any data element is changed, then the capability should exist to trigger on that event. Microsoft's IPAM solution cannot do this.

Customizations should also include the ability to add User Defined Fields (UDF) and apply corporate policies. These UDF's should be flexible enough to track any type of data from plain text fields to validated addresses. Ideally, flexibility should exist to provide the ability to set up a pre-defined value for a UDF or hostname based on its location.

For example, if the Subnet Name is Denver, then the corpo- rate standard is the hostname begins with den. If the class is a Workstation, when the Class is set, the hostname now changes to denw. If the class is really Server, then as the class is updated, the hostname changes to dens. These are all very valuable capabilities that an IPAM solution should provide.

Unfortunately, this is another area where the MS IPAM solution does not provide Naming Convention Management.

DHCP Management

An IPAM system should be able to manage the configuration of a DHCP server as well as manage all aspects of the DHCP server. This includes DHCP options, server options, and debugging settings.

Of course, this ability should be available for managing multiple servers at the same time, meaning that the administration is not limited to a server-to-server basis. In addition, the IPAM solution should extend the management to the next level.

Being able to set up a DHCP server or architecture template so that all DHCP servers are configured the same way is a minimal requirement. Unfortunately, Microsoft's IPAM solution does not include any of this. Key properties are managed through the IPAM interface, but not all elements and it is not possible to enforce standardization of neither the server nor architecture configuration.

This is when the value of a DDI system comes to light. The ability to manage a mixed DHCP environment through one standard interface is crucial and what should be expected from a true IPAM interface.

DNS Management

As with DHCP management, DNS management with an IPAM tool should be able to manage all aspects of a DNS server from its configuration to the zone files. Microsoft's IPAM solution does not deliver these features and in fact has very little capability for managing DNS servers or zones.

This is yet another clear indication that the MS IPAM solution is not really an IPAM solution. One more clear dis- tinction is that Microsoft's IPAM system is limited to 350 zones that will prove to be very restrictive for many companies.

Network Information Management

As mentioned previously, the goal of a DDI system is to manage the environment from end to end. This includes the ability to manage the network topology. Microsoft's IPAM solution does not even attempt to support this aspect of an IPAM solution.

Network Information Management includes the ability to identify networks that are being used in the environment as well as how those networks are broken down into subnets as defined in the network infrastructure. As these are very rarely static definitions, IPAM solutions should support the ability adjust and change the subnet and network definitions.

Microsoft cannot track multiple IP addresses with a single device. Each view is independent of the other nor can they represent the state of the network.

Reporting and Monitoring

While Microsoft's IPAM interface allows for searching and sorting on most of the fields, it does not support compound searching nor does it support generating reports in any format other than CSV. SOLIDserver has the ability to generate reports in HTML or PDF format. Integrated into the interface is the ability to generate a graphical view of a DNS server's usage and DHCP server's usage as well as statistics such as DNS or DHCP traffic, memory usage and disk usage.

Business Continuity Management

Business Continuity Management can take many forms. It is not just a hardware failure but the abili- ty to bring a service back online quickly. Key to bringing a service online quickly is the ability to access the data and configuration information to perform that action.

The Microsoft IPAM solution is not integrated with Active Directory so data is not replicated. Consequently, care must be taken to backup the system. Having a data backup does not mean a server can be rebuilt easily. If a Microsoft DNS or DHCP server fails, that server must be rebuilt. All software must be installed, and configured before it can be reintegrated with the IPAM software. This is obviously not ideal.

Since the data is not integrated into Active Directory, the backup of the data is only as good as the last backup. If a backup only occurs once a day, then recovery is only as valid as that point in time.

Application and Operating System Security

Security should be an overriding focus of any architecture and application that is implemented. This includes not just focusing on the configuration of DNS and DHCP, but also the underlying hardware and network.

IPv6 Management

Everyone is familiar with IPv4 addresses. These are the 32-bit addresses consist of 4 octets separated by a dot ([0-255].[0-255].[0-255].[0-255]). The network ID is the left most portion and the host ID is the right most portion.

This addressing scheme provides for approximately 4.3 Billion addresses. When IPv4 was initially developed, 4.3 Billion IP addresses seemed like it would be more than enough. However, time has proven that theory wrong. Therefore, the next generation of IP Addressing was developed – IPv6.

IPv6 addresses are 128-bits which will provide approximately 340 undecillion. An IPv6 address consists of eight 16-bit sets of hexadecimal characters separated by a colon (:). For example, and IPv6 address might look like:

fd41:929c:c5b0:0001:0020:abc3:12ab:1212

As with IPv4, the network prefix is the left-most sets while the right most is the Interface ID. The characters used in an IPv6 address are case-insensitive.

As the IPv6 addresses are more complex, the management of IPv6 addresses should be simplified by the IPAM solution. Microsoft has yet to achieve this goal.

Summary

With Windows Server 2012, Microsoft has integrated a new IPAM capability. As described, "IPAM provides a built-in framework for discovering, monitoring, auditing, and managing IP address space and infrastructure servers on a corporate network". A closer look though reveals that the IPAM feature really focuses on a centralization of Microsoft DHCP configuration and not a full, feature-rich IP Address Management system.

There are so many features and capabilities that are crucial to a comprehensive understanding and management of an IP Infrastructure that is only available from commercial solutions such as SOLIDserver.

A true DDI solution must offer comprehensive and integrated management of DNS/DHCP/IPAM and VLANs with devices and their network interfaces in a single process.

It should be able to define and manage the relationships between all these IP related resources to ensure high availability, security and automation to guarantee that your network infrastructure will actively support your business imperatives.

EfficientIP provides a comprehensive suite of features that intelligently simplify and automate design, deployment and management of IP network infrastructure:

- Unified and integrated management of IPAM, DNS, DHCP with VLANS/VRF organizations and network device interfaces repository
- Native capacity to integrate Enterprise policies automating best practices enforcement
- Enterprise provisioning process modeling and automation
- Holistic reconciliation management of the network infrastructure

efficient iP®

REV: C-150616

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
60 Paya Lebar Road #11-47
Paya Lebar Square SINGAPORE 409051
+65 6678 7752