whitepaper

Comparing SolarWinds® IP Address Manager to Windows Server® 2012 IP Address Management

By: Brien M. Posey

solarwinds

whitepaper

When Microsoft® released Windows® Server 2012, one new feature introduced was IP Address Management (IPAM). This new utility can help simplify some of the IP address management headaches and avoid the effort and mistakes associated with manual IP address management techniques.

Microsoft's IPAM utility is better than using a spreadsheet to keep track of IP addresses. However, it does take some work to deploy and configure. (http://technet.microsoft.com/en-us/library/jj878313.aspx). So, before you commit to using a native OS-level IP address management, it is worth considering whether it is better to use Microsoft's IPAM utility or if it would be more advantageous to invest in a 3rd-party IP address management solution, such as SolarWinds IPAM.

Examining the Existing Precedent

Before considering a 3rd-party alternative to Windows Server's native IP address management capabilities, take into account any existing precedents. In other words, is it normal to avoid using a built-in feature in favor of a 3rd-party solution?

There are a number of examples where 3rd-party software vendors have created products that are designed to provide more comprehensive functionality than what is provided by Microsoft's operating system utilities.

One of the best examples of 3rd-party software vendors augmenting the operating system's capabilities is the backup industry. Windows Server includes a native backup application called Windows Server Backup. Windows Server Backup is able to back up a full server (all volumes), selected volumes, the system state, or specific files or folders—and to create a backup that you can use for bare metal recovery in the event of a hard drive crash (http://technet.microsoft.com/en-us/library/cc772523.aspx). However, it lacks other common capabilities, such as the ability to back up cluster shared volumes. That being the case, countless vendors have developed backup products for Windows.

Of course, backup capabilities are not the only aspect of the Windows Server operating system that has been addressed by 3rd-party software vendors. There are 3rd-party solutions for everything from storage provisioning to logging and reporting. The point is that 3rd-party add-ons for Windows Server have become the norm. In fact, Microsoft has a program in place for certifying software to work with Windows Server (http://blogs.technet.com/b/in_the_cloud/archive/2014/04/08/the-application-certification-program-for-windows-server-2012-r2.aspx).

A Closer Look at Microsoft IPAM

Microsoft IPAM tends to be the most beneficial to smaller IT shops that are running homogenous Windows Server environments.

There are two primary advantages to using Microsoft IPAM. The first is the price. Microsoft IPAM is included with Windows Server 2012 and Windows Server 2012 R2. As such, your organization may already be fully licensed to use Microsoft IPAM.

The second advantage of Microsoft IPAM is that its capabilities are exposed through Microsoft's System Center Virtual Machine Manager. Organizations that use System Center Virtual Machine Manager 2012 or 2012 R2 to manage their Hyper-V® servers will find that IP address management for virtual networks is relatively straightforward.

Although Microsoft's IPAM has the basics covered, there are some limitations that you need to be aware of. The first is that Microsoft first introduced the IPAM utility with Windows Server 2012. Therefore, if you're running legacy versions of Windows Server, you will need to upgrade to Windows Server 2012 or 2012 R2 to use Microsoft IPAM.

The second limitation, as previously alluded to, is with the management console. The Microsoft IPAM console is a Windows client application and cannot connect to multiple IPAM instances or servers simultaneously (http://technet.microsoft.com/en-us/library/jj878313.aspx). This limitation can make managing the deployment of multiple IPAM servers tedious and time-consuming.

The reason why the IPAM management console does not accommodate distributed IPAM server deployments is because IPAM isn't technically a distributed application. A true distributed application is typically designed to be deployed across multiple servers, with each server performing a role that contributes to the application's overall functionality. With a true distributed or tiered application, all of the application servers can typically be managed through a centralized console. Unfortunately, this is simply not the case for Microsoft IPAM.

Although it is possible to deploy Microsoft IPAM on multiple servers and build a tiered architecture, the IPAM servers do not share a common database, making the consolidation of information difficult to achieve.

Tiered Microsoft IPAM server deployments require you to adopt one of two strategies (or a combination of the two strategies). One option is to configure each of the IPAM servers to use a unique scope. For example, an organization might deploy a separate IPAM server for each physical location or use a separate IPAM server for each Active Directory® domain.

Of course, large, enterprise-class environments prefer a centralized IPAM server that can provide IP address information for the entire organization. This is where the second strategy comes in. For example, if you use individual Microsoft IPAM servers to control various scopes, setting up a centralized IPAM server requires you to enable the retrieval of IP address data from the IPAM servers throughout the organization. Then you import that data into a centralized IPAM server. This is commonly accomplished by using a combination of task scheduling and PowerShell scripting.

As you know, the IPAM feature is designed to automate IP address management. By definition, an automated IP address management system needs to be able to communicate with the organization's DHCP and DNS servers. While Microsoft's IPAM feature does communicate with Microsoft DHCP and DNS servers, Microsoft IPAM is dependent on the Active Directory. IT does not allow for cross-forest IP address discovery, and it does not support multi-forest topologies (http://technet.microsoft.com/en-us/library/jj878312.aspx).

The Microsoft IPAM utility does well at communicating with Microsoft DHCP servers that have been registered in the Active Directory. In fact, almost all of the DHCP server functionality is exposed through the IPAM console. For example, the IPAM console can be used to create DHCP scopes, configure predefined DHCP options, create user and vendor classes, and more.

Even so, Active Directory registration tends to be a limiting factor. Rogue DHCP servers are not usually registered in the Active Directory. Similarly, many 3rd-party DHCP servers do not offer Active Directory registration. (http://www.windowsdevcenter.com/pub/a/windows/excerpt/securews_chpt11/ (http://www.experts-exchange.com/OS/Linux/Distributions/Q_23442499.html). These factors may result in a gap in DHCP server support.

Although Microsoft's IPAM server offers nearly comprehensive support for Microsoft DHCP servers, it provides no real DNS integration. Right-clicking on a DNS server displays a shortcut menu with options to either launch the Microsoft Management Console (MMC) or retrieve server data — no other options exist. As such, you can use the console to check on the status of host records or to monitor DNS zones, but for most other functionality, you are required to use the DNS management console.

While we are on the subject of DHCP and DNS integration, it is worth mentioning that the Microsoft IPAM utility was designed primarily to interact with Microsoft DNS and DHCP servers. In some cases, it is possible to import data from 3rd-party servers, but there is no direct support for things like BIND DNS servers or Cisco® DHCP servers.

Another potential limitation with Microsoft IPAM is the freshness of the data that is displayed through the IPAM console. One method of bringing DHCP lease information into an IPAM server involves using the Invoke-IpamDHCPLease cmdlet in PowerShell. The full command typically looks something like this:

Invoke - IpamDHCPLease – IPAMServerName <the name of your IPAM server> - DHCPServerFQDN <the name of your DHCP server> - Force

This command captures a static view of the current DHCP lease information. The IPAM console does not display fresh DNS lease information unless it is manually requested or scheduled. That being the case, many administrators add the –Periodic switch parameter to the command listed above. This causes a scheduled task to be created. It is then possible to use the Windows Task Scheduler to adjust the frequency at which fresh DHCP lease data will be retrieved.

What About a 3rd-Party Solution?

It goes without saying that Microsoft's IPAM does have some advantages over SolarWinds IPAM. Unlike Microsoft's IPAM utility, SolarWinds IPAM is not included with Windows Server, and it does not offer direct integration with System Center Virtual Machine Manager. Even so, SolarWinds IPAM offers a considerable amount of advantages over Microsoft's IPAM.

One advantage of SolarWinds IPAM is centralized management. SolarWinds IPAM makes use of the Orion® dashboard, which allows for organization-wide management of DHCP, DNS, and IP addresses. For example, if your organization has other licensed SolarWinds products, those products may also be exposed through the Orion dashboard. This dashboard does more than simply display a hierarchical view of the organization's DHCP and DNS servers. It provides a view of current issues that need to be addressed. One issue might be if an organization had a subnet that was running low on IP addresses, that issue would be conspicuously displayed on the dashboard, allowing the administrator to take action.

Although SolarWinds IPAM works with the Active Directory, it does not have a direct Active Directory dependency. This gives SolarWinds IPAM the flexibility to work with DHCP and DNS servers that are not Active Directory registered. This includes some common 3rd-party infrastructure components, such as Cisco DHCP Services (including ASA devices, ISC, DHCP, and DNS).

This brings up an interesting point. As previously mentioned, the SolarWinds dashboard provides centralized management capabilities. This includes the ability to manage DHCP and DNS servers across the organization. Microsoft IPAM provides DHCP management capabilities, but its DNS functionality is very limited. For example, while it is possible to use the Microsoft IPAM console to create a DHCP scope, it cannot be used to manually create a DNS record. Right-clicking on a DNS server reveals only the options to launch MMC or to retrieve server data. As you recall, SolarWinds IPAM is designed to be a multi-vendor solution. The management console is designed to allow you to manage DHCP and DNS servers in a consistent manner regardless of which vendor's DHCP and DNS servers are being used.

SolarWinds IPAM also differs from Microsoft IPAM in how it discovers network resources. As stated earlier, SolarWinds does not require DHCP servers to be registered within Active Directory. Therefore, SolarWinds performs a true network discovery rather than relying only on Active Directory queries. This allows SolarWinds IPAM to detect rogue DHCP servers and also avoid any problems related to inaccurate or outdated Active Directory data.

The SolarWinds network discovery engine provides the added benefit of automated IP address conflict detection. SolarWinds IPAM automatically detects and helps you troubleshoot IP address conflicts. To troubleshoot an IP address conflict, single-click to access the IP address history, which shows the systems that used the address most recently. A second click launches the User Device Tracker (UDT). This helps you to determine which switch port the offending device is connected to as well as relevant details such as the operating system, machine vendor, etc. Once this information is known, you can reconfigure the offending system or take it offline.

Microsoft makes it possible to create custom IPAM reports through using PowerShell scripting, but SolarWinds IPAM delivers rich reporting capabilities through a point-and-click interface that does not require writing any code. In fact, SolarWinds is able to detect a device's vendor by examining the device's MAC address. Not only is this information reported, it can be useful when trying to physically locate devices that are using conflicting IP addresses.

Both the Microsoft and SolarWinds IPAM products log historical IP usage data, which can be useful in a variety of situations. For example, you could conceivably use historical data to track the way an IP address space is used over time. By tracking past usage patterns, you can predict when IP address depletion for the address space is likely to occur.

Similarly, historical information is useful for security purposes. For example, suppose that a server logs an attempted security breach and the server's audit logs list the IP address from which the attack was launched. Assuming that the IP address is internal to your network, you could use an IPAM system's historical data to determine which computer was leasing the IP address at the time of the attack.

In addition to IP address usage reports, SolarWinds IPAM also has a built-in alert mechanism. The software can use alerts to notify administrators of pressing issues. For example, you might receive an alert indicating that a DHCP scope is running low on IP addresses that can be leased to client devices. Microsoft's IPAM also provides alerts, but these alerts focus primarily on reserved IP addresses that are about to expire (http://technet.microsoft.com/en-us/library/hh831622.aspx).

One more advantage is that SolarWinds IPAM provides support for legacy operating systems. Microsoft IPAM is included with Windows Server 2012 and 2012 R2 and is able to manage DHCP servers running on Windows Server 2008, 2008 R2, 2012, and 2012 R2. However, many organizations still have legacy Windows Servers and may also have 3rd-party systems that need to be managed. SolarWinds IPAM works with the latest Windows Server releases, but it also supports older versions of Windows.

Important Business Considerations

Information Technology is now more bottom-line focused than it has perhaps ever been. The relentless emphasis on cost savings may make it tempting to deploy Microsoft's IPAM utility since it is included with the Windows Server operating system. However, as with any software, it is critical to examine the total cost of ownership rather than considering only the licensing costs. The "free" solution may not really be free after all.

Although Microsoft's IPAM utility is not subject to any feature-specific licensing requirements, an organization may need to purchase additional Windows Server licenses prior to deploying it (a valid Windows Server 2012 or 2012 R2 license is required). If Microsoft IPAM is installed onto a dedicated virtual machine, the virtual machine's operating system must also be licensed. Although Microsoft does not technically require the IPAM utility to run on a dedicated server, Microsoft IPAM cannot be installed on a domain controller nor can it be installed onto a DHCP server that needs to be managed through IPAM (the utility installation succeeds on a DHCP server, but IPAM is unable to discover the DHCP server) (http://technet.microsoft.com/en-us/library/hh831353.aspx).

Licensing the IPAM server is far from being the only business consideration that needs to be taken into account. It is also important to determine whether Microsoft IPAM will meet your current and future business needs. As previously explained, Microsoft IPAM is limited to managing Microsoft DNS and DHCP servers (http://technet.microsoft.com/en-us/library/hh831353.aspx). This means that organizations using 3rd-party DNS or DHCP servers must choose to either relinquish their previous investment in favor of Microsoft servers or have a blind spot in their management framework if they want to use Microsoft IPAM.

Another consideration that must be taken into account is Microsoft's operational boundaries for IPAM. Microsoft IPAM cannot extend beyond the Active Directory forest boundary (http://technet.microsoft.com/en-us/library/hh831353.aspx). This can be a problem for organizations with multiple Active Directory forests or for organizations that make use of certain types of cloud services.

Outside of licensing, the most significant cost associated with using Microsoft IPAM is likely the administrative cost. Microsoft IPAM is designed to simplify and automate IP address management. However, large organizations are likely to find that Microsoft IPAM's

inability to replicate data or to share databases between IPAM servers can increase complexity since PowerShell scripts are commonly required in order to make Microsoft IPAM work in the desired manner. For example, Microsoft IPAM does not automatically add DHCP leases to the IPAM databases as IP addresses, but the task can be manually performed through the IPAM client console and the task can be automated through PowerShell (http://technet.microsoft.com/en-us/library/jj878303.aspx).

Feature Comparison

The chart below provides a feature-by-feature comparison between Microsoft IPAM and SolarWinds IPAM.

Feature	SolarWinds IP Address Manager	Microsoft Windows Server IPAM Utility
Support for Windows Server prior to 2012	Yes	No
Seamlessly manage IPAM, DHCP, and DNS services across two or more Active Directory Forests	Yes	No
Integrated management of Microsoft DNS services	Yes	No
Natively manage multi-vendor DHCP and DNS services	Yes	No
Management console offers user-defined data refresh options without the need to build custom pollers	Yes	No
Uses active network discovery to find and verify IP address status	Yes	No
Uses active network discovery to find subnets	Yes	No
Able to detect and alert on IP conflicts	Yes	No
Able to maintain IP address history	Yes	Yes
Support for System Center Virtual Manager	No	Yes
Able to associate MAC and IP address with switch and switch port	Yes, with IP Control Bundle	No
Able to associate devices to vendor	Yes	No
View pre-built reports	Yes	No
Build custom reports	Yes	Yes
Monitor IP Resources	Yes	Limited

whitepaper

Conclusion

The transition from manual to automated IP address management is not a task to be taken lightly. There are numerous IP address management solutions available, and these solutions can vary widely in terms of cost, functionality, and complexity. It is important to choose a solution that will accommodate your organization's current and future needs, without introducing unnecessary complexity, being excessively expensive, or forcing the organization to abandon its existing investment in DHCP and DNS.

To learn more about how SolarWinds IPAM can help you manage your DHCP, DNS, and IP addresses, please visit: solarwinds.com/ip-address-manager.aspx.

About the Author

Brien Posey is a freelance technology author with over two decades of IT experience, and has received Microsoft's MVP award 13 times for his work with Windows Server, IIS, Exchange Server, and File Systems / Storage. Posey has authored dozens of books and many thousands of articles, and routinely speaks at various international IT events. Prior to going freelance, Brien served as CIO for a national chain of hospitals and healthcare facilities. Previously, he served as a Network Engineer for the United States Department of Defense at Fort Knox. He has also worked as a Network Administrator for some of the nation's largest insurance companies.