Infoblox Integrated IP Address Management Solution

“Built-in,” Appliance-based DNS/DHCP/IPAM for Real-time Data and Services Delivery

www.infoblox.com
An Introduction to IP Address Management

IP address management (IPAM) provides the ability to effectively manage, control, monitor, and assign the IP address space within a company. An IPAM solution reduces operations costs and improves network uptime by minimizing administrative effort and network downtime. To provide effective IP address management, it is essential to control the two key services within a company that provide the naming and delivery of IP addresses—which are DNS and DHCP—as well as to supply the feature sets necessary to generate and present reports detailing IP address information and usage. In this paper, we will explain the importance of IP address management, discuss the criteria for an ideal IP address management solution, and explain the features and advantages of the Infoblox IP address management solution.

Why Is IP Address Management Important?

Nearly all companies today, from the Fortune 500 to small and medium enterprises, rely on TCP/IP networking for core business services. At a minimum, their internal e-mail, web, network printing, and file storage infrastructure depends on the network. In most cases, the network also supports critical business applications, such as e-commerce, enterprise resource planning, customer management, and sales force automation. Increasingly, networked applications also link companies with their customers, suppliers, and partners.

The network has become such an essential corporate resource that an outage can have devastating effects, crippling a company’s ability to do business. Consequently, companies have invested substantially in network infrastructure, including routers and wide-area connections.

The criticality of TCP/IP networks continues to increase over time. The growth in mobile computing and the introduction of diverse IP-based devices such as IP telephones, cameras, and RFID readers means that soon virtually every business activity—from gaining access to a building to making a phone call—will be mediated by the IP network. In this light, IP network connectivity becomes as basic as electricity.

As the network takes on the role of a utility, like power and plumbing, the management of IP addresses and the data associated with them such as MAC, location operating system etc. becomes key. Organizations need tools to help allocate and track address space, from entire ranges to individual IP addresses. They need central control of and visibility into DHCP and DNS configuration, and central monitoring of the status of these services. And these tools need to be an integral part of the network, because change happens much more frequently as contractors and partners come and go, customers become part of the network, and mobile employees expect constant connectivity as they roam the halls, or the globe.

Regulatory compliance adds another dimension to the challenge. To comply with a subpoena, a company might need to produce a log of which computers had a particular IP address over a period of time. Even if not mandated by regulations, these are clearly vital functions necessary for an organization to detect and thwart attempts to misuse the network.
## Key Benefits of IP Address Management
### Ideal IPAM Solution Criteria

Administrators have a range of options available for IP address management. Most companies manually configure DNS and DHCP servers independently to provide names, IP addresses, and related configuration settings to devices, and use spreadsheets to keep track of these assignments. More advanced approaches use an overlay IP management application to manage DNS, DHCP and associated data e.g. location, device type, owner etc. In the overlay model, dedicated IPAM software uses a separate, external database to store IP address and host data, and generates and pushes configuration and data files to DNS and DHCP servers throughout a company. However, most of these approaches leave something to be desired when it comes to realizing all the benefits an IPAM system must offer. In the following paragraphs we will review some of the key criteria an IPAM system should satisfy in order to provide benefits discussed above.

| Lower IP Management and Monitoring Costs | An IPAM system makes it easy to assign static IP addresses. Without an IPAM system administrators need to manually maintain and keep updated a spreadsheet of IP addresses in use, resulting in higher administration costs. Additionally, an IPAM system provides alerts to administrators when IP addresses usage reaches unusually high or low mark, thus reducing the effort to constantly monitor the usage of IP space and minimize IP outages. |
| Reduced IP Related Helpdesk Calls | About 50% of network related helpdesk calls arise due to IP address outages. An IPAM system provides alerts when IP address usage is extremely high allowing administrators to take action before users start to experience outages. This results in fewer outages and helpdesk calls, saving effort and costs associated with processing and servicing helpdesk calls. |
| Enhanced Reporting for Forensics and Compliance | IPAM systems provide detailed reports about who is using a particular IP address currently and a historical account for who had an IP address in the past. This information is very useful in investigating criminal activity involving network usage. Sometimes regulatory authorities require organizations to produce records of IP address usage for forensic investigation. Without an IPAM solution it is hard or impossible to find such information. |
| Higher End user productivity | An IPAM system ensures that users do not experience IP address related outages and are thus able to perform their jobs rather than wait for an IP address related issue to resolve. This directly affects company revenues and profitability. |
INTEGRATION WITH DNS AND DHCP DATA

Any IPAM solution is only as good as the underlying data. Most of the DNS and DHCP systems maintain their own data in configuration files or databases. Most commercial IPAM products use a separate, external database to store IP address and host data, and generate and push configuration and data files to DNS and DHCP servers throughout a network. This approach has the following shortcomings –

A separate database of the overlay IPAM solution is “once-removed” from the underlying DNS and DHCP data being served in the network and does not reflect the real-time network state. In the event of network slowdowns, the IPAM database can become significantly out of sync from actual DNS DHCP data and may lead to errors. In the case of disaster recovery, the entire IPAM solution may need to be rebuilt since the state of IPAM database will not reflect true state of the network. This process may take hours or even days to complete.

Customers are required to purchase and maintain separate IPAM hardware and software, in addition to their DNS and DHCP servers. This incurs significant additional costs, both in initial equipment for software and for ongoing management.

The general-purpose databases used by conventional IPAM systems are not optimized for real-time networking applications and do not lend themselves well to integration of additional network services protocols over time, such as TFTP, NTP, RADIUS, and LDAP. This will ultimately render them quite limited as administrators are challenged to be able to link users, devices, IP addresses and other data e.g. location asset information and other IPAM metadata together for planning, troubleshooting, and compliance purposes.

The better approach to IP address management is to build an entire system from the ground up that integrates IP management functionality into a DNS and DHCP appliance solution. By using a built-in, distributed database with real-time data updates across an Infoblox grid consisting of multiple, interconnected appliances, Infoblox is able to deliver an appliance-based IPAM solution that is unified with the underlying DHCP and DNS services. This reduces costs by eliminating the need for separate IPAM hardware and software, ensures that reports always reflect the immediate, real-time state of the network, and supports the ability to add more services and data over time to the same infrastructure.

EASE OF DEPLOYMENT AND DATA MIGRATION

As a key requirement, it should be relatively easy to implement IPAM in an existing network of any size and configuration. Introduction of IPAM tools presents problems in replicating the state of the network in the IPAM solution. An ideal IPAM product should provide capabilities for automatically discovering devices on the network and adding them to IPAM database, reconciling discovered devices with existing data in the IPAM system, as well as technologies to import data from existing IPAM systems (including spreadsheets) into its database.

EASE OF MANAGEMENT

Automation of frequent activities e.g. creation of a network identical to some other network, assignment of a static IP address, sharing of records between different networks etc. should be provided to ease management.
An IPAM system should allow easy upgrade of the system itself and underlying core network services devices. Any interruptions in service during upgrades may result in revenue losses therefore it is important that these upgrades are seamless and without any downtime.

IPAM systems typically store a lot of data about the state of the network. Storing this data requires a database management system to manage storage as well as manipulation of this data. If this database is external to the system it can add significant management effort and costs to purchase and manage a commercial database server. At times it may result in a dependency of networking group on a DBA to use the IPAM system. Therefore an ideal IPAM system should provide a built-in mechanism for data storage and manipulation with no expectation on administrators to manage a DBMS.

An appliance form factor for an IPAM system is highly desirable since patching and upkeep of a general purpose operating system based IPAM solution will add additional effort in managing the IPAM system.

EXPANDABILITY

It should be possible to add new networks to the IPAM deployment effortlessly. In the case of merger and acquisitions, several new networks may need to be added without requiring changes in IP address schemes which might contain overlapping ranges. It should be possible to manage overlapping IP address ranges with the IPAM solution. Additionally, IPAM solution should support overlapping address ranges e.g. two or more separate networks with identical IP address ranges. This is especially important when network architecture is a result of heavy merger and acquisition activity.

REPORTING

Reporting is a key functionality of IPAM systems and is helpful in –

1. Reporting on IP address Pool Usage Before an Outage Happens
   With an IPAM system in place the burden of constantly monitoring IP space usage should be transferred to the IPAM system. Any IPAM system should provide timely alerts via SNMP traps and email to ensure steps are taken to prevent an outage before it happens.

2. IP Address Use History for Forensic Investigation
   Sometimes when investigating security breaches and network misuse, it is important to know who had what IP address assigned at what time. An IPAM system must be capable of storing and displaying historical IP address assignment information to conclusively identify the offending machines.

3. Network Troubleshooting and Investigation
   The IPAM system should discover and provide current information on IP address assignments so network problems can be easily troubleshoot. An IPAM system that depends on a copy of data from underlying DNS and DHCP systems will typically fail to produce exact reports. Only a system that is tightly integrated with DNS and DHCP services using transactional data replication can satisfy this requirement.

4. Administrative Audit Reporting
   In a large network, several administrators are needed to manage core network services e.g. DNS and DHCP. Accurate reporting of changes enables IT organizations to hold individual administrators accountable for the system changes they make. This capability is also required for various compliance mandates.
It should be possible to easily pull relevant reports and also search IPAM database for keywords and regular expressions to find relevant data.

**ROLE BASED ADMINISTRATION**

Large networks typically require several administrators and groups, each responsible for different portions of the networks or different core network services. It should be possible to easily define administrative roles and add remove administrators to these roles.

**EXTENSIBILITY**

Each network is unique and therefore IPAM requirements vary and no one system may be able to accommodate all requirements. It should be possible to easily extend the functionality of an IPAM system using simple scripts and programming tools. An IPAM system should provide appropriate API and operating environment for executing custom programs based on this API to allow for simple extensions to be built.

**RELIABLE DATA BACKUP, RESTORE, AND DISASTER RECOVERY**

IPAM systems must provide backup and disaster recovery mechanisms to ensure that IPAM data are always available. Conventional IPAM systems, since they use a separate, dedicated IPAM database, typically implement an “out-of-band” model for backing up and restoring the dedicated IPAM data. Since the IPAM data in conventional systems is delayed in time from what’s actually being served in the network—and since the database copy operation is typically scheduled to only occur periodically—backup data rarely reflect the actual network state at the time of failover to a disaster recovery site. Plus, it can take hours or days to get the systems back in synch.

**Infoblox IPAM Details**

IPAM functionality is built-in to Infoblox NIOS software and includes a comprehensive suite of functions that support address allocation, management, and reporting. When used with the Infoblox grid module enabled by the DNSone® with Grid package, the IPAM functionality is greatly enhanced. Additionally, Grid provides benefits of centralized management, real-time distribution of data and services, with assured data integrity across a collection of distributed appliances.

**INTEGRATION WITH DNS AND DHCP DATA**

Infoblox manages the IPAM data as well as the DNS and DHCP server configurations using a distributed, real-time database. The DNS and DHCP protocol servers have been enhanced to directly read and write to the database so that all data are accurate and distributed in real time.

The Infoblox bloxSDB database, stores the IP address and DNS data in a structure known as a ‘Host object’, which models devices as they would exist on a network. Other systems treat IP address/DHCP data and DNS data as two separate entities. In most cases, an IP device has a hostname, IP address, MAC address, and may also have alias names for easier naming access. In order to identify devices by names instead of IP addresses—or to identify a
device name by an IP address—DNS forward records (A records) and DNS reverse records (PTR records) are configured on DNS servers. Furthermore, DHCP fixed addresses that are tied to a specific device are configured to always receive the same IP address based on the device MAC address. Since all this information is related to a single device, it is inefficient to designate the information that defines a unique IP address in multiple records. Doing so can lead to errors when the information stored in one record is modified but corresponding information stored in other records is not—such as may occur when dynamic DNS updates are allowed from clients on the network. The Infoblox Host object combines all the information about a single device into a single record, so all elements related to the object stay in sync.

For example, for an IP device defined with the following information,

The Infoblox Host object created in the Infoblox database includes all of the DNS, DHCP, and IPAM data related to the device, as shown below:

The Infoblox database creates a true representation of a host device. Instead of maintaining separate configurations where information is duplicated in DNS, DHCP, and IPAM device classifications, entries are only added once. This enables derived records, such as A, CNAME, and PTR records to be generated and maintained automatically by the system. When queried from DNS or DHCP, the database supplies the answer for the queried object by building it from the information in the Host model. This prevents any chance for data inconsistencies that occur when different instances of the same data are out of sync.

**EASE OF DEPLOYMENT AND DATA MIGRATION**

**Network Discovery**

Network Discovery allows administrators to search for active devices on their networks and populate the IPAM database with information discovered during the process. Depending on the method of discovery used, an administrator can take following actions upon completion of discovery.

**Add new devices to IPAM system** – Network discovery provides a quick mechanism to add unmanaged devices to the IPAM system without requiring administrators to manually input this information.
Resolve conflicts between the IPAM system and actual network state – If the IPAM system has one view of the system but actual IP address use on the network differs from this e.g. IPAM system as a fixed IP address with a MAC address however in reality it has a different MAC address, a network discovery will show this as a conflict that administrators can correct.

Discover unauthorized devices on the network – Periodically, administrators will discover devices on their network that ought not to be present there and may pose a security risk. Network discovery will show this as an unmanaged device in IPAM report.

Reclaim unused IP Addresses – Infoblox network discovery process reports when an IP was last discovered. This information helps in determining whether an IP address can be claimed back and reused.

Infoblox network discovery functionality allows administrators to run discovery process on networks that are remote or may be behind firewalls. This is a distinct benefit when compared to alternatives available in the market. Additionally, Infoblox network discovery process uses various discovering techniques including ICMP, TCP and NetBIOS enabling administrators to gather various pieces of information associated with the devices present on the network. Network discovery process reports IP Address, MAC Address, NetBIOS names, OS version and when an object was last seen on the network. Administrators can fully control which discovery methods are used and can easily start, pause and end the discovery process.

EASE OF MANAGEMENT AND AUTOMATION OF FREQUENT IP MANAGEMENT TASKS

Next Available IP
Next available IP feature produces the next unused IP address in a given network. This feature is extremely useful in assigning fixed IP addresses to network devices such as printers, security cameras etc. Availability of this feature reduces management effort in finding an unused IP address and assigning it to a device. Further the risk of future conflict with another device is reduced since IPAM system will not give out the same IP address for a different device.
Data Consistency Checking
The Infoblox software will automatically perform multiple levels of data consistency checking. With a “Host object,” the administrator can keep DNS forward and reverse zone records in sync to avoid inconsistent zone data. Infoblox also has a flexible hostname checking mechanism that allows administrators to develop custom templates for hostnames or choose from three defaults. The template is then applied to a zone so requirements can be customized for different zones. The software also performs data formatting checks for IP addresses and any other structured fields. Notably, the system prevents invalid data from being entered.

Dynamic Address Control
The Infoblox IPAM solution provides the ability to manipulate addresses and their status, such as converting a dynamically assigned DHCP lease to a DHCP fixed address or Infoblox Host object. For example, this allows administrators to deploy new devices on the network using a common workflow: Letting network devices such as servers, desktops, printers, and IP phones obtain IP address settings automatically using DHCP; Viewing the DHCP leases in the IP address management console, clicking on the entry, and then converting the lease to a DHCP fixed-address or Infoblox Host.
This saves time and prevents errors by allowing administrators to add devices into DNS and DHCP without having to worry about entering the wrong MAC address, IP address, or hostname. Furthermore, when a dynamic lease is converted to a fixed-address or Infoblox Host, administrators can assign IPAM data such as device classification information to these entries to make them easier to track.

In the figure above, right-clicking on a lease entry provides the option to convert the dynamic lease to a DHCP fixed-address, reserve it for later use, or convert it to an Infoblox Host record. The IP address and MAC address information are automatically populated into the fixed-address or host entry.

**Shared Record Groups**

Shared Record Groups (SRG) enable administrators to create groups of DNS records and then associate these groups with multiple views and zones. When a shared record is changed, it is dynamically updated in all associated views and zones. A unique icon identifies shared records both in the shared record group view and the regular DNS zone view and a unique icon identifies any zone with shared records. Using Shared Record Groups you can:

- Simplify and expedite the administration of resource records. When you create or update a shared record, the NIOS software automatically updates it in all associated zones.
- Reduce object count by using one shared record instead of creating the same record in multiple zones.
- Reduce configuration errors by reducing the need to manually update records in each view and zone.

**Name Server Group Templates**

With multi-appliance configuration and data entry from a single GUI interface, many operations are streamlined. For example, when adding a new DNS zone, it can be created, mapped to several appliances (as name servers), configured with specific zone parameters, and even have the contents imported from an existing DNS server—all through one dialog. This approach simplifies the initial configuration and the ongoing lifecycle management of a grid, rather than having to individually setup and administer each device independently.

The example below shows the creation of a name server group called “Primary 1.” This group selects a grid member “ns1.idblox.com” as the primary for zones, and it supplies a list of three grid members that will be secondary servers for the zones.
Once the name server group is created, it can be assigned to any zone which will inherit the primary and secondary server mappings. This saves time and prevents errors when creating zones with secondary sever assignments.

Network Templates

By using templates for networks, companies can automate and standardize the creation of DHCP configurations across their network. For example, if companies want the same configuration for each new branch or store, they can create a template that includes fixed addresses, DHCP ranges, exclusion ranges, DHCP options, and anything that can be configured for DHCP. When creating a new network, the administrator can pick a template and all the information for that network will be pre-populated according to the chosen template. Network templates can include any number of DHCP Range and DHCP Fixed Address templates.
Ranges and Fixed Address Templates
Ranges and fixed address templates further simplify DHCP administration. Users can create DHCP ranges and fixed addresses based on the pre-defined templates. This allows for a more homogenous use of IP address ranges throughout the enterprise, resulting in ease of troubleshooting network issues. For example, a standard Fixed Address template can be defined for printers with custom options and DHCP lease times. Or, a DHCP Range template can be defined for Voice Over IP phones with the correct custom DHCP options.

On-the-fly Assignment of Ownership
Using Infoblox grid technology, administrators can select an appliance within the grid to be primary or secondary for a DNS zone or the owner of a DHCP network and range. All data are automatically replicated to the appliances that serve the data.
In the example below, the secondary servers are chosen for the zone “idblox.com.” Once the member appliance is selected, the data will automatically be replicated to the appropriate members and they will have the capability to start serving data. No additional steps are required.

**Seamless Software Upgrades**

The upgrade process can be the “Achilles heel” of any large IT system. Upgrading some IPAM systems is a complex process that can involve upgrading the overlay IPAM application, the database, the server OS, the remote agent, and the DNS/DHCP server software. Upgrading all of these software components requires verifying that each specific version of each component is compatible. It also requires that the organization have access to all systems with the appropriate permissions to perform the upgrade. This can be daunting if the company has tens or hundreds of servers. In fact, because the upgrade process is so complex, some customers become stuck at the same release of software for years.

Inability to upgrade IPAM system and associated core network services devices may lead to security issues.

Infoblox appliances can be updated grid-wide to a new release of software with a simple two-step operation that distributes the code and then upgrades. It is also possible to roll-back appliances to prior releases, and to centrally backup and restore all data and configurations across an Infoblox grid.
EXPANDABILITY

Overlapping Networks
This is the capability of Infoblox IPAM system to manage two or more overlapping address ranges within the IPAM system. This is a key functionality of an IPAM system and is frequently required when managing networks created by heavy merger and acquisition activity. During M&A activity, IT departments typically do not re-architect the whole network; therefore, if the two merging entities were using same network address ranges in their networks they end up with same address used by multiple devices. The Infoblox IPAM system can handle this easily by using network views functionality. Using network views, administrators can keep two or more overlapping networks separate and still use Infoblox IPAM to manage these.

Split/Join Networks
As companies expand and grow either organically or through acquisition, they need to be flexible with their DHCP networking configuration. Split/Join networks allows a company to easily adjust to the dynamic nature of today’s networks. Split networks allows an administrator to quickly, easily, and accurately subdivide a network and have the resulting sub-networks inherit the configuration of the parent network. Join/Expand networks is unique in that it allows the administrator to combine smaller networks into a bigger network without losing any of the configuration including fixed addresses, dynamic ranges, etc.

IPAM REPORTING WITH INFOBLOX NIOS

Accurate reporting of IP address usage is of paramount importance to maintaining an auditable, secure and outage free network. A good IPAM solution should alert administrators when IP address usage thresholds are crossed so that action can be taken before an outage occurs. Additionally, an IPAM solution should provide reports including IP address lease history to enable administrators to examine security incidents and identify the users and devices involved. Finally, it should be possible to search and view devices by device type and other device attributes for quick troubleshooting and checking of device status.

Infoblox NIOS provides an array of reporting capabilities to provide an accurate picture of current network configuration as well as historical information. Following are the key reporting capabilities available in the NIOS solution.

Integrated IP Management Console
The IP address management console shows the power of running real-time DNS, DHCP, and IPAM services on the integrated Infoblox bloxSDB™ database.
Within the single screen above, administrators can search and sort through their IP networks based on a range of parameters—such as IP address, MAC address, usage status, device type, location, etc.—thereby simplifying many common IP management tasks. For example, modifying an IP address in the IP address management view gives the ability to associate, create, and modify Infoblox Hosts, DNS records, DHCP options, and device classification information associated with the IP address from one location. A simple sort on the status field helps administrators, in real-time, to find the next available IP address within a network to assign to a new device. And because the IPAM functions and DNS and DHCP services operate from the same database, all information is guaranteed to stay in sync even in the most dynamic environments. Reports can be easily exported to a CSV file for further analysis and integration with other reporting tools. Administrators can control what columns and data are exported.

**DHCP Lease History Tracking**

Administrators require the ability to collect and report historical information showing the IP assignments assigned by DHCP over time. This allows administrators to know which machine had a certain IP address at any time. As shown below, the Infoblox DHCP Lease History feature enables administrators to track and report on addresses based on a range of parameters, including User names, IP address status (dynamic, fixed, available, and reserved/disabled), hostnames, MAC Address, and DHCP Lease information including lease date/time, time left on lease, time of last renewal, and forced release of IP address. If the Infoblox NAC Foundation is used, administrators can produce a report of a specific user’s DHCP lease history and the device(s) they used to access the network. Tracking this information is imperative for security auditing and for meeting compliance regulations. The Infoblox solution stores up to 100,000 lease events locally before requiring archiving to an external server—which can be performed by a simple manual export process, or by an automated script.
**Administrator audit reporting**
A key requirement when delegating administration is the ability to track and report on changes by the administrators. All changes made by administrators are logged in a detailed centralized audit log. The audit log contains all the details of changes and addresses which can be searched and exported. Superusers can run reports on the audit log to obtain information such as: which administrator(s) made changes to a specific object and when the change was made or provide a list of all changes with dates and times and detailed change information for each administrator. This information is invaluable when performing any investigation for compliance.

**IPAM Extensible Attributes**
IPAM extensible attributes feature takes the anonymity out of IP networks by allowing organizations to fully describe their networks, zones and devices and to search and display them based on a wide range of criteria. Customers have a need to categorize and report on their networks and devices based on several criteria e.g. geographical locations, owners, department, asset class, building, campus, manufacturer, type etc. With IPAM extensible attributes, they can do exactly that. Administrators can define attributes on the fly and specify a data type (e.g. Date, E-Mail, Integer, Lookup list, String and URL) for the attribute. In addition they can also specify if this is a required field and if there are any object type restrictions e.g. if an attribute is valid only for network object types etc. Following diagram shows extensible attributes for a network object type.

Extensible attributes once defined can be displayed in the tree view as following. The column values of extensible attribute can be sorted just like ordinary attributes. Additionally, extensible attributes data is available to perspective and local searches. This enables administrators to issue flexible search queries e.g. show all the printers in the Boston office etc.
Advanced Search Capabilities with “Live” Results

This feature allows users to edit services and data based on search strings which can be simple text searches or complex Regular Expressions. The search results panel shows data from a search through the entire database. Results are dynamic objects that allow editing and viewing results displayed by the search. In this example, all the DNS zones that the corporate group manages have the “Corporate” tag in the Comment field. Using the search functionality, an administrator from the corporate office enters a search string “Corp” to find records with this tag. The results of the search display all the zones with “Corp” in the name or comment field. By clicking on any of the search results the administrator can view all the resource records and can modify the zone properties as well, the same as if the administrator were administering from the Infoblox Views panel itself.

![Advanced Search Capabilities with “Live” Results](image-url)
IPAM Statistics Viewer and DHCP Threshold Alerts

The IPAM statistics viewer enables administrators to allocate IP address ranges more efficiently and effectively by displaying the number of static and dynamic IP addresses in use and the percent utilization for each network assigned to each Infoblox appliance.

If DHCP threshold limits are exceeded, alerts can be sent using e-mail and SNMP traps so that administrators can take preventive action, such as re-allocating networks. “Low water” thresholds are also useful for detecting network anomalies. For example, if a network that is normally fully populated with IP phones suddenly passed a low-water DHCP threshold, it would indicate that phones were not renewing their leases and that there was likely a problem with the phones or the IP telephony network.

Role based administration with delegation

Role based administration allows alignment of real world job responsibilities of the administrators with the permissions to carry out tasks on Infoblox appliances. Infoblox NIOS allows creation of administrative roles and assignment of different administrators to these roles. An administrative role can be defined based on flexible criteria e.g. DHCP administrators in the Phoenix data center or Printer administrators worldwide etc. Once the role has been defined, administrator accounts can be added to specific roles.

IPAM features on NIOS recognize permissions associated with these roles and function accordingly e.g. if an administrator with permission to assign static IP addresses uses “Next available IP” function in order to allocate an IP address to a printer, the IP address returned will be compliant with the permissions of the role of the administrator. Next when the administrator assigns the new printer a name and IP address, host name syntax checking will be activated to ensure that the name complies with the naming rules as specified by the central administrator.

Extensibility

bloxTools environment

bloxTools environment provides a way to extend the capabilities of Infoblox IPAM system by providing a way to create custom applications (called snapins) using Infoblox provided API and a virtual environment on Infoblox appliances to run these snapins. Using bloxTools, customers can integrate Infoblox IPAM system with their other IT systems if required. Additionally, bloxTools developer community provides an array of innovative snapins free of charge. Some examples of these community supported snapins include, GeoViewer snapin that allows administrators to locate all of their Infoblox devices on a map and see status of these devices in real time, operator console snapin that allows helpdesk personnel to easily allocate IP addresses to users without impacting network administrators etc. For more details on bloxTools community and snapins please visit www.bloxtools.com.
Reliable Data Backup, Restore, and Disaster Recovery

IPAM data in Infoblox grids is exactly the same data being served in the network at any given time. In addition, the backup devices in Infoblox grids, known as “master candidates,” always contain an exact replica of the authoritative data on the grid master. A failover to a disaster recovery site simply involves “promoting” a master candidate to become the grid master. Member appliances automatically “re-home” to the new master with none of the manual, client-side intervention required with conventional systems. The process takes seconds, synchronization is nearly immediate, and services continue to run on remote servers at all times. This unique, nonstop approach to real-time data backup and restore and seamless failover enables Infoblox to provide the fastest time-to-recovery of any system available. Locally, Infoblox appliances can be configured in high-availability (HA) pairs to ensure continued service delivery even if an appliance should fail.

Summary

IP address management functions have become essential on modern corporate networks. However, the cost and complexity of traditional IPAM software has prevented many companies from deploying such solutions. Infoblox has taken a “built-in” vs. “built-on” approach to delivering IPAM as part an appliance-based solution fully integrated with DNS and DHCP services. This results in powerful IPAM functionality, greater resiliency and robustness, more accurate and real-time data, and lower cost of deployment and ownership.
For More Information:
+1.408.625.4200
1.866.463.6256
(toll-free, U.S. and Canada)
info@infoblox.com
www.infoblox.com