Challenge

Using Microsoft-native tools for DNS, DHCP, and IP tracking inhibits your ability to troubleshoot issues and outages quickly, automate workflows effectively, and secure with confidence.

Solution

BlueCat Micetro lets your operations teams continue to use Microsoft tools while centralizing visibility and control. Get the best of all worlds with granular access management, proactive alerting, and a one-stop shop for automation.

Benefits

- SSO/MFA with Active Directory, Entra ID, and Okta
- Granular Role-Based Access Control
- Proactive Alerting
- Scheduled and Triggered Events
- Reporting

Request a free trial

Why use Micetro in a Microsoft environment?

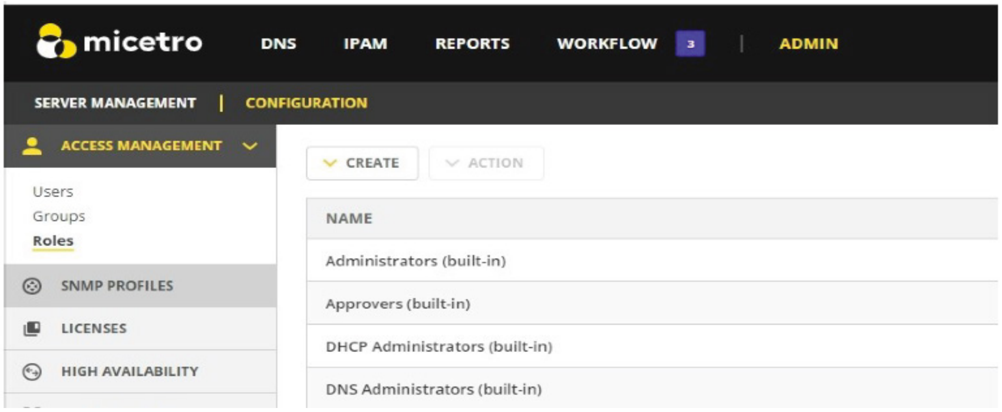
Sustainability is imperative, whether we're talking about energy and resource use or technical debt. By using an overlay solution like Micetro, you can enhance your current Microsoft offerings with a non-disruptive approach and abandon the forklift mentality that keeps organizations beholden to a single vendor.

Active Directory and Microsoft Entra ID integration

Micetro uses role-based access control (RBAC) to offer the most secure yet manageable access management solution. It ensures that permissions may only be granted to roles, and then users or groups can be assigned to those roles. These users and groups may come from Active Directory (AD), Microsoft Entra ID, other Lightweight Directory Access Protocol (LDAP) systems, or just defined directly in Micetro.

Permissions are ground zero when it comes to security. Having proper permissions will save you from accidental changes that may cause problems, not to mention intentional or malicious activity. It's already complex when only considering on-premises AD users, but when you add in multicloud factors with multiple access models, you can imagine how complex it becomes.

Creating the right roles that may be used across multiple platforms (in the cloud and on-premises) is the simplest and most secure way to ensure your users get the correct permissions. It also ensures that you can add new users with the correct permissions, and, more importantly, remove users from a role when they've left your organization.

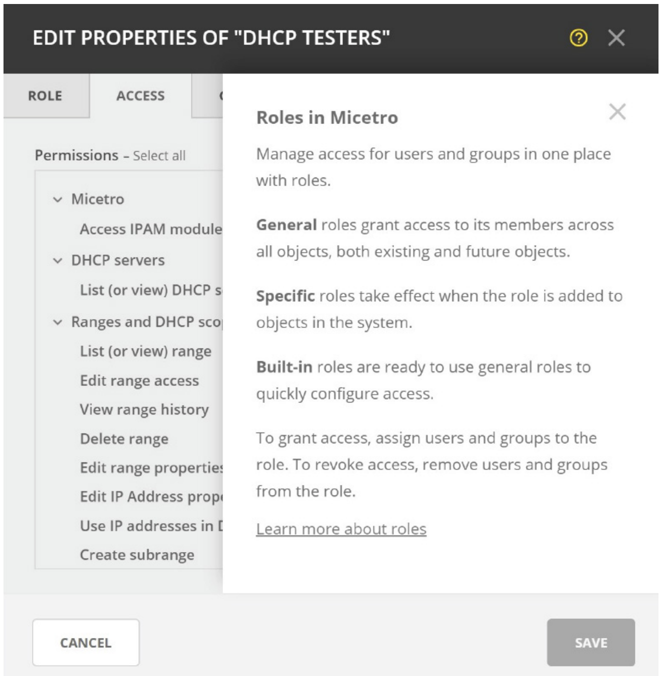


NAME
Administrators (built-in)
Approvers (built-in)
DHCP Administrators (built-in)
DNS Administrators (built-in)

The principle of least privileges

According to the principle of least privileges, a user needs only the minimum access privileges necessary to perform a specific job and nothing more. If someone only needs to view DNS information, they should not have any change or remove privileges. Nor should they have any access to DHCP, for example. Very few users should have super admin privileges, and, even when they do, they shouldn't be using them for day-to-day work.

Therefore, granular RBAC is important. With Micetro, you can create roles that only have permissions for specific DNS, DHCP, and IP address management (together known as DDI) objects, such as a DNS zone or a DHCP scope. Micetro offers a level of granularity that is appropriate for an enterprise but also more sustainable and secure for admins to manage. In the case of needing even more granularity, Micetro offers an approval workflow capability called Workflow. For more information on how to create Workflows, view our blog post, Lockdown DNS Without Slowing Down Processes.



EDIT PROPERTIES OF "DHCP TESTERS"

Permissions - Select all

- Micetro
  - Access IPAM module
- DHCP servers
  - List (or view) DHCP s
- Ranges and DHCP sco
  - List (or view) range
  - Edit range access
  - View range history
  - Delete range
  - Edit range propertie
  - Edit IP Address prop
  - Use IP addresses in D
  - Create subrange

Roles in Micetro

Manage access for users and groups in one place with roles.

General roles grant access to its members across all objects, both existing and future objects.

Specific roles take effect when the role is added to objects in the system.

Built-in roles are ready to use general roles to quickly configure access.

To grant access, assign users and groups to the role. To revoke access, remove users and groups from the role.

Learn more about roles

For more information on how to configure access control in Micetro, please see Access Management in the Micetro Admin Guide.

Single sign-on and multi-factor authentication

BlueCat makes Micetro implementation open and easy to integrate with the third-party solutions you're already using in your environment. Micetro offers commonly used options for single sign-on (SSO) and multi-factor (MFA) or external authentication. You can use Active Directory, Microsoft Entra ID, and Okta to create a simple sign-in experience with an existing account (often called SSO). Several industries and regulations prioritize—or even require—MFA to achieve compliance. Industries like government, healthcare, and finance can require all their solutions and partners to use MFA to log in to services as well. In many cases, compliance standards like Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability (HIPAA), Defense Federal Acquisition Regulation Supplement (DFARS), and Payment Card Industry Data Security Standard (PCI DSS) require the use of MFA using at least two out of three factors (something you know, something you are, or something you have). Thanks to Micetro's third-party integration with Microsoft Entra ID and Okta, you can offer MFA when logging in to the Micetro user interface (UI).

Challenges using the snap-in for DNS

If you're already using Microsoft DNS via the Microsoft Management Console snap-in, you've likely become accustomed to logging in to several servers to locate—not to mention troubleshoot—specific DNS zones and records. Troubleshooting involves parsing system logs and there's no built-in alerting system. Building in automation is mysterious and not sustainable. Perhaps most importantly, access control is difficult because you can't assign granular permissions and often DNS servers are installed right on domain controllers. Giving everyone access to a domain controller is not good security hygiene, but often functionality wins when compromising best practices.

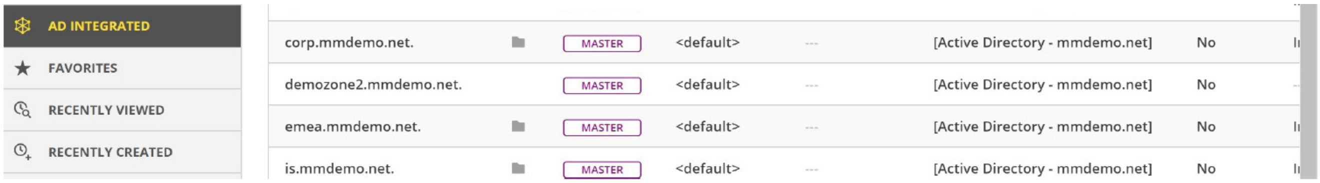
Microsoft DNS accomplishes the main objective of DNS, which is often internal DNS. However, it's more common to use externally managed DNS services or cloud DNS services to manage external DNS and cloud-based workloads. This means that admins must manage several different services in an inconsistent way. There may be different teams or people that manage these underlying services, which makes visibility and planning difficult and often contributes to network fragility.

Agentless operations

No one likes to deal with third-party agents on their servers, especially if those servers are domain controllers. As a close partner with Microsoft, we have minimized the necessity of connecting services via agents. With a Microsoft environment, you only need to install one agent on one DNS/DHCP server within your forest. You can then connect to all your other Microsoft DNS/DHCP servers without having to install any software on those servers. This limits your attack surface as well as minimizes the operational work necessary for maintaining those servers.

Micetro AD integrated zones

Micetro allows you to manage DNS internally and externally no matter which DNS services you're using in the underlay and no matter where your workloads reside. This means that you log into the same UI or API to have visibility and control of your entire DNS environment. Because Micetro is integrated with Microsoft every step of the way, there are built-in views and options specifically catering to Windows DNS.



corp.mmdemo.net.	MASTER	<default>	---	[Active Directory - mmdemo.net]	No	I
demozone2.mmdemo.net.	MASTER	<default>	---	[Active Directory - mmdemo.net]	No	--
emea.mmdemo.net.	MASTER	<default>	---	[Active Directory - mmdemo.net]	No	I
is.mmdemo.net.	MASTER	<default>	---	[Active Directory - mmdemo.net]	No	I

You can easily see which zones are coming from your Windows DNS and work with those as necessary, either individually or in bulk.

By clicking on the meatball menu, you'll see all the options available to you including:

- Editing zone properties: Add custom or built-in identification information about a DNS zone
- Editing zone transfer settings: Specify which servers for which zone transfers are allowed
- Editing zone notification settings: Specify which secondary servers to automatically notify when there are zone changes
- Adding an xDNS profile: Create multi-service DNS redundancy for 100% uptime even when a DNS service goes down
- Editing preferred servers: Change the order of domain controllers
- Adding to folders: Create a high level of flexible organization to help you more easily manage DNS
- Deleting zones: Delete individual or multiple zones
- Access control: See and modify access control for one or multiple zones
- View history: See when, how, who, and why a DNS object was modified or created

Micetro gives you the most accurate information within your zones as well. Every 15 minutes, by default, Micetro updates DNS content. You can change this value according to what works best in your environment. When clicking one level deeper into a zone to get information about DNS records, Micetro updates the content in real time so you can feel confident about the information you're viewing.

DNS redundancy

According to a recent report by Gremlin, the average cost of a website outage for the top five e-commerce sites in the U.S. is about $3.5 million USD per hour. Whether you're selling services over the public internet or relying on your website to build confidence and trust with your customers, you want to make sure your DNS services remain up and performant.

While DNS itself is a highly redundant protocol, the underlying infrastructure that provides it are often fragile and may go down for reasons such as human error, misconfigured router settings, or a DNS attack. Recent examples of major DNS outages include Dyn in 2016, CloudFlare in 2020, and Meta in 2021.

The xDNS capability, a unique offering from Micetro, allows you to build in DNS redundancy with two or more services. These services may be on-premises with Microsoft DNS or BIND and combined with other cloud or managed DNS service providers.

For more information on xDNS, view our whitepaper on xDNS for multiprovider redundancy and resilience.

Approval workflows

Another enhancement Micetro gives to a Microsoft environment is built-in workflow capability. Workflow is built into the web UI but may be accessed through APIs as well.

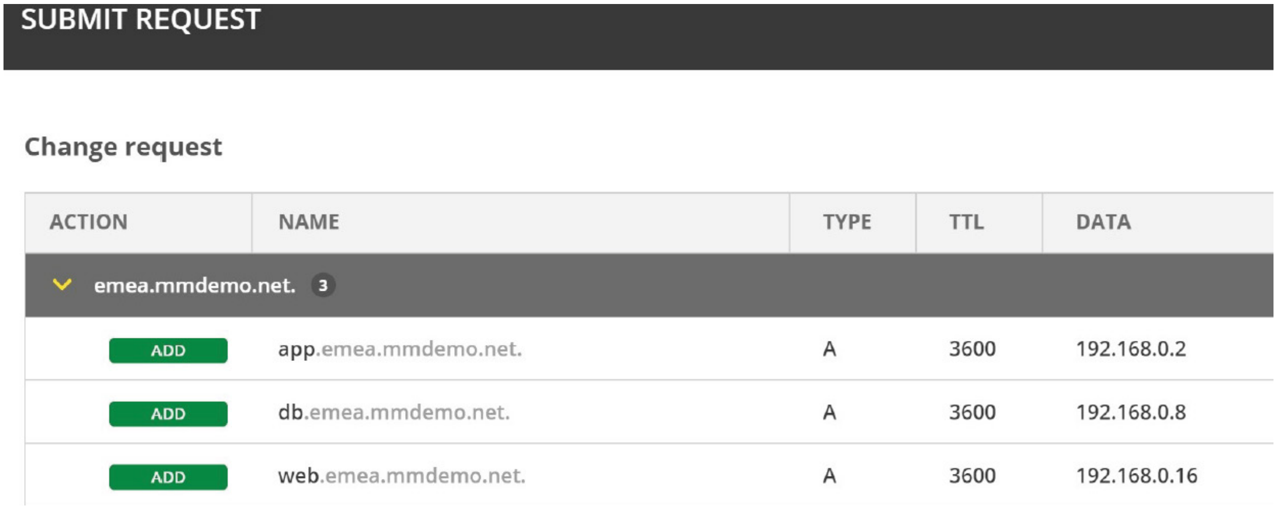
You can view DNS workflow as the flip side of the coin to granular access. It gives people in your organization requestor privileges that allow them to view specific environments and use the UI or APIs to make requests for DNS record creation or modification. It suggests the “next free IP” so that they can easily choose an appropriate IP address to use. If they’re trying to pick a specific IP, Micetro will let them know in the pop-up whether that IP address is available.

Furthermore, they can create multiple requests at the same time. When they’ve created their requests, they can submit them for approval and even suggest a scheduled time to enact the change. There’s also an area for leaving comments both by the requestor and approver to document everything as you move along this workflow.

Use case: DNS workflow

An application owner is ready to update a version of an app. At first, a developer will request IP addresses and DNS records for their development environment for every tier of this application. For the sake of simplicity, we’ll assume the app has three tiers, requiring an IP address and A record for each tier. A few weeks later, the QA test team creates a new request to deploy the app in the test environment so that they can continue testing. Then, one week later, the application owner requests new IP addresses and A records for the production environment. After deployment into production, you can reclaim the IP addresses and DNS records from the dev and test environments.

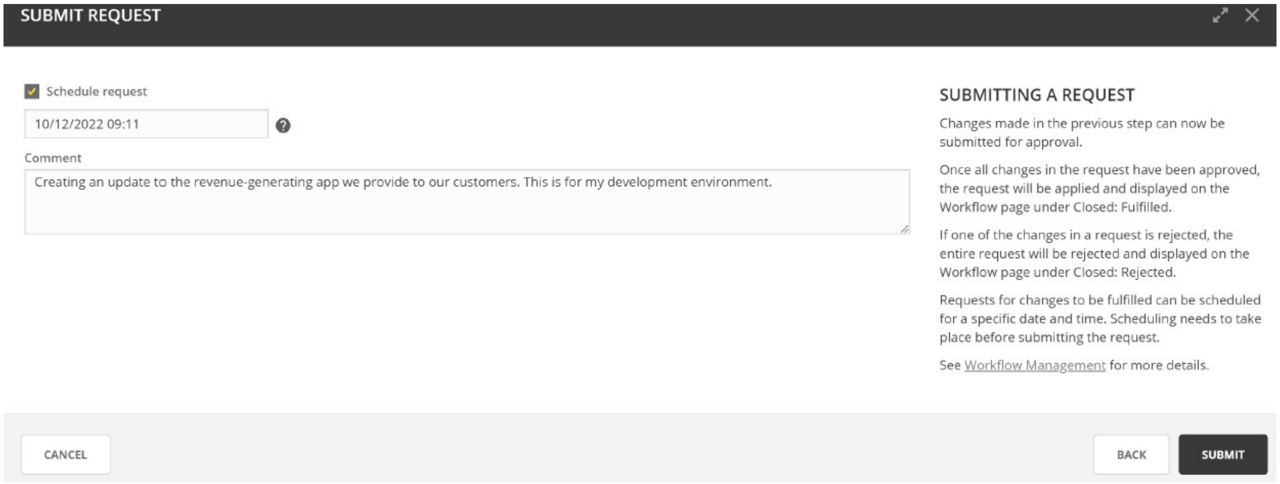
This very simple example consists of 18 different requests, from different teams, all involving the same app. Although these are very simple requests, submitting these tickets and making these changes in a Microsoft environment is a very manual process. Micetro’s Workflow capability removes the guessing, documentation, and reliance on manual tasks. This reduces the time spent on these types of tickets, and, more importantly, reduces the chances of human error in a production environment.



SUBMIT REQUEST

Change request

ACTION	NAME	TYPE	TTL	DATA
emea.mmdemo.net. 3				
ADD	app.emea.mmdemo.net.	A	3600	192.168.0.2
ADD	db.emea.mmdemo.net.	A	3600	192.168.0.8
ADD	web.emea.mmdemo.net.	A	3600	192.168.0.16



☑ Schedule request

10/12/2022 09:11

Comment

Creating an update to the revenue-generating app we provide to our customers. This is for my development environment.

SUBMITTING A REQUEST

Changes made in the previous step can now be submitted for approval.

Once all changes in the request have been approved, the request will be applied and displayed on the Workflow page under Closed: Fulfilled.

If one of the changes in a request is rejected, the entire request will be rejected and displayed on the Workflow page under Closed: Rejected.

Requests for changes to be fulfilled can be scheduled for a specific date and time. Scheduling needs to take place before submitting the request.

See Workflow Management for more details.

Working with DHCP servers

Micetro works with several on-premises DHCP servers, which is invaluable as the workforce becomes more distributed and branch office operations offer another layer of complexity. To gain observability and manage all of your DHCP operations from one place, an overlay solution like Micetro is necessary.

As with DNS, Micetro will work with your Microsoft DHCP servers without having to install an agent on every server in your AD forest. Because Micetro is an overlay, it will take on the features of the underlying service. For example, Microsoft offers the ability to reconcile DHCP scopes. Therefore, you can also reconcile Microsoft DHCP scopes from Micetro. This function also fixes any inconsistencies found between the Microsoft registry and DHCP database.

Micetro gives you a quick view of all your DHCP scopes along with helpful information like at-a-glance utilization. Within the IP address management (IPAM) tab, you can click on the meatball menu next to one or multiple DHCP scopes to take the following actions:

- Open network: View the scope and see which IPs have been used, scope range, exclusions, etc.
- Edit network properties: Modify the custom properties providing built-in documentation, such as identification characteristics of those scopes
- Convert to network: Change the DHCP scope into an IP range at the click of a button
- Set AD site: Assign the scope to a Microsoft Active Directory site
- Add to folder: Add the scope into a folder for organizational purposes
- Set discovery schedule: Enable a discovery schedule and set the frequency for discovery
- Set subnet monitoring: Trigger a script to run when thresholds meet a specified metric
- Manage DHCP pools: Set the range for DHCP pools inside your scopes
- Manage scope instances: Set which servers are enabled for a scope
- Edit scope options: Set DHCP options and dynamic DNS options. Here, you can set up the DHCP server to automatically update authoritative DNS servers with the host (A) and pointer (PTR) records of DHCP clients.
- Reconcile DHCP scopes: Fix inconsistencies between the DHCP registry and database
- Delete network: Remove the scope entirely from all server instances
- Access: Set access control for a specified DHCP scope or multiple scopes
- View history: See when, how, who, and why a DHCP object was modified or created

Using DHCPv6

IPv6 offers its own way of dynamically allocating IPv6 addresses to devices (known as SLAAC). But many enterprises prefer to use DHCPv6 because they're still using IPv4 and DHCP and want operational consistency. There are also other benefits to using DHCPv6, such as specifying DHCP options and dynamic DNS options and policies. For more information on dynamic allocation methods, view our blog post, Planning IPv6 Address Assignment.

As IoT devices—and especially IoT devices deployed with IPv6 addresses—proliferate our data centers and campuses both on premises and in the cloud, we especially need the ability to automatically assign IP addresses and DNS names and to attach policies to these devices. For more information on IoT and DHCPv6, see our blog post, The IoT Use Case for DHCPv6.

Spreadsheet-based IPAM

Generally, admins using a Microsoft-based IPAM solution are using an Excel spreadsheet or some other manually updated spreadsheet to keep track of their IP addresses. While this is a tried-and-true method of asset management, it has its downsides.

Five reasons to move to a modern IPAM solution

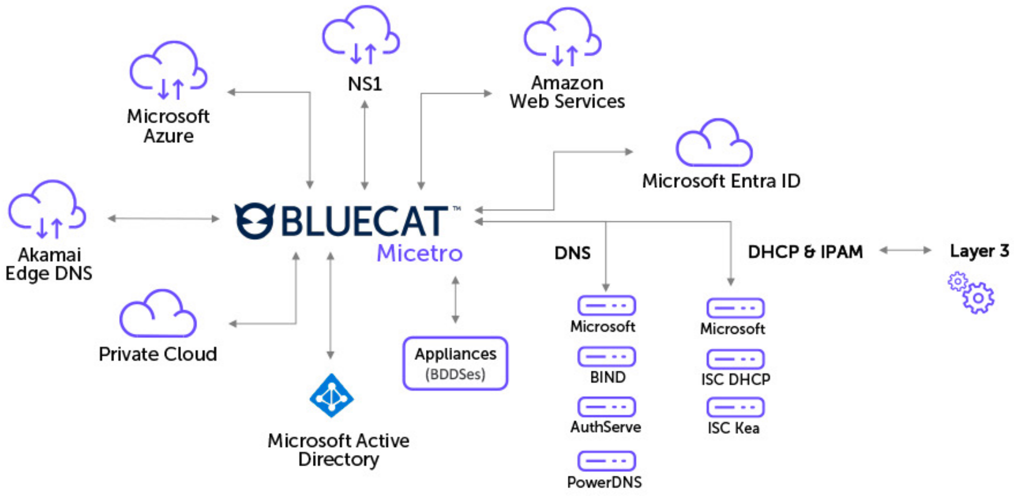
- You have more than one person or team managing your network. This can lead to inconsistencies, confusion, and missing information.
- You have more than one site and/or hundreds or thousands of IP addresses to track. At some point it just becomes too much to track manually.
- You find yourself missing history and audit information. If you're spending too much time tracking down compliance information or locating information for troubleshooting, modern IPAM is already necessary in your environment.
- You keep track of DNS, DHCP, and IP addresses in multiple places. Easily seeing contextual information linking DNS, DHCP, and IP addresses will only help you in your planning, deploying, migrating, and troubleshooting practices.
- It takes days or weeks to deploy new apps and services due to planning for IP addressing and DNS information. With a modern IPAM solution, you can avoid being the bottleneck for deploying and updating revenue-generating services.

Multicloud asset management and custom properties

As multicloud and Secure Access Service Edge (SASE) architectures become the norm, having built-in documentation and asset management becomes even more complex and necessary. We may not be able to physically touch the racks and servers in the public cloud, but we still must pay for those resources. As a result, tracking is a huge part of planning and budgeting.

Micetro, which not only connects to all parts of your multicloud infrastructure but also to every app, service, and device, is an integral part of asset management. This is true whether your workloads are in Azure, on-premises, or in any other cloud. With Micetro, you can also provide even more context to your objects to feed your asset management engine by using custom properties.

Micetro indexes custom properties, so they're searchable and accessible through open APIs. Armed with contextual DNS, DHCP, and IP address information, as well as identity information for your entire enterprise, you can more confidently prove compliance, save on cost, and easily migrate when it's time.

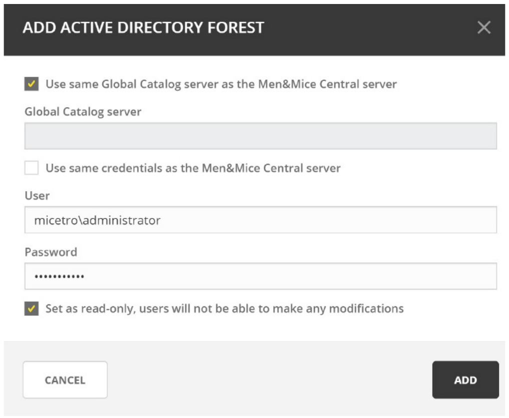


Active Directory sites and subnets

Many DDI solutions have AD users and groups integration. But Micetro takes it a step further by offering AD sites and subnet integration. Organizational structure is key to a healthy DDI environment, but you shouldn't have to reinvent the wheel with every solution you use. By adding in AD sites, you'll gain observability of your Microsoft AD forests, sites, and subnets quickly for better planning, deployment, and troubleshooting, provided you're running Micetro on a Windows server.

After adding in the AD forests, you can navigate based on the AD forest structure to find information about specific networks within that site.

With this functionality, you can also easily move subnets between sites by selecting the IP range in the IPAM grid, selecting "Set AD Site," and then picking the correct site.


ADD ACTIVE DIRECTORY FOREST

☑ Use same Global Catalog server as the Men&Mice Central server

Global Catalog server

□ Use same credentials as the Men&Mice Central server

User

micetro\administrator

Password

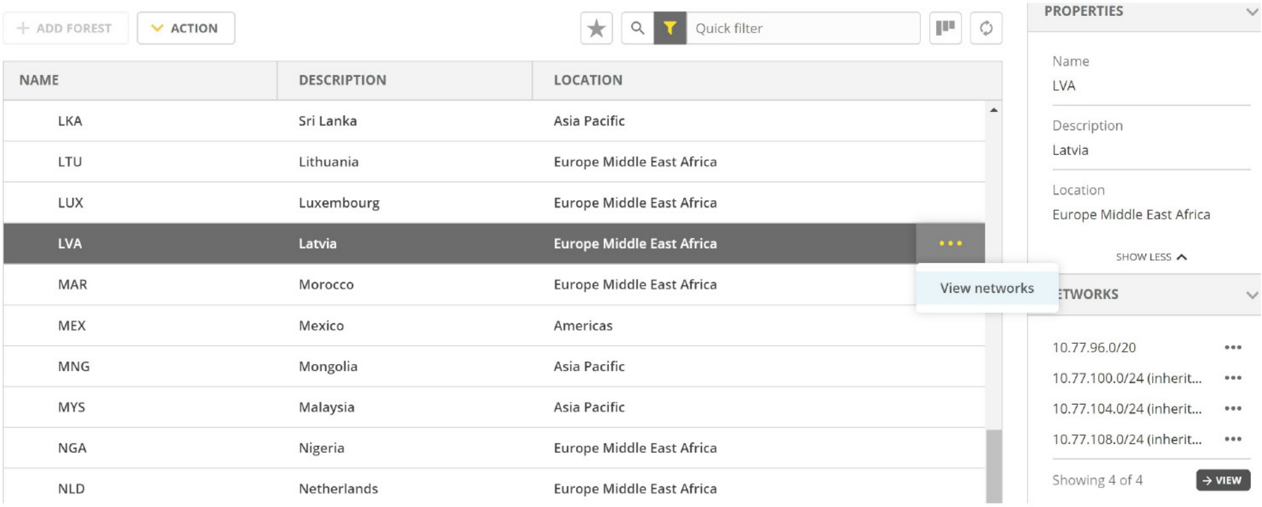
•••••••••••

☑ Set as read-only, users will not be able to make any modifications

Use case: Mergers and acquisitions

Mergers and acquisitions are the norm for many enterprises, leaving IT teams to figure out how to combine networks while keeping everything up and running. By using Micetro, IT can add the new organization's AD forest and select to "Set as read-only, users will not be able to make any modifications." This lets them see everything from both organizations in a centralized view, while guaranteeing that no changes will be made until it's necessary.

In addition to adding new forests for read-only or write, Micetro includes the Address Spaces function, which allows you to manage overlapping IP ranges from the same place without causing IP conflicts or requiring multiple management solutions.



NAME	DESCRIPTION	LOCATION
LKA	Sri Lanka	Asia Pacific
LTU	Lithuania	Europe Middle East Africa
LUX	Luxembourg	Europe Middle East Africa
LVA	Latvia	Europe Middle East Africa
MAR	Morocco	Europe Middle East Africa
MEX	Mexico	Americas
MNG	Mongolia	Asia Pacific
MYS	Malaysia	Asia Pacific
NGA	Nigeria	Europe Middle East Africa
NLD	Netherlands	Europe Middle East Africa

Name
LVA

Description
Latvia

Location
Europe Middle East Africa

10.77.96.0/20
10.77.100.0/24 (inherit...
10.77.104.0/24 (inherit...
10.77.108.0/24 (inherit...

Showing 4 of 4

Microsoft database backend

If you're a Microsoft shop, Micetro supports the use of Microsoft SQL as a database backend, although other types of databases are supported as well. As with every part of Micetro, we want our customers to continue taking advantage of what they already have on their network. It is likely you already have security and access control policies, database health monitoring, and high availability set up in your database farms. You can continue using what you already have due to the flexibility Micetro offers. For a complete list of Micetro supports, please see our system requirements.

Build DDI automation into your workflows

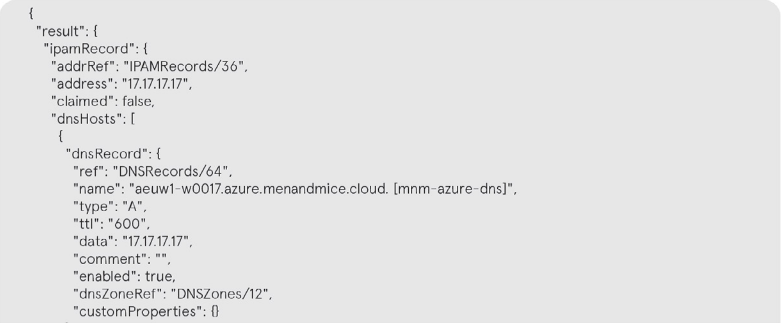
Finally, Micetro gives you open APIs to build DDI automation into all your workflows. When you consider the number of tasks and devices DNS, DHCP, and IP addressing touches, it's clear why open APIs in your DDI solution are paramount. Micetro has built APIs in from the beginning. This not only means that everything is accessible from the APIs, but that anything done from a third-party through API integration will also be logged in the same place as where it would be logged if done from the UI. Again, this gives you a centralized view of your history and audit trails.

As a Microsoft partner, Micetro supports Powershell scripts, which our customers use regularly. Micetro also supports and has up-to-date plug-ins for Ansible and Terraform.

Let's look at an example Powershell script to find information on an IPAM record (17.17.17.17) in Azure:

```
$cred = Get-Credential
Invoke-RestMethod -Method GET -Cred $cred -Uri “https://<your_host>/mmws/api/
IPAMrecords/17.17.17.17” | ConvertTo-Json -Depth 5
```

This results in the following JSON, which gives you contextualized information not only about the IP address but DNS information, DHCP information, custom properties, and other information attached to that IP:



```
{
 "result": {
  "ipamRecord": {
   "addrRef": "IPAMRecords/36",
   "address": "17.17.17.17",
   "claimed": false,
   "dnsHosts": [
    {
     "dnsRecord": {
      "ref": "DNSRecords/64",
      "name": "aeuw1-w0017.azure.menandmice.cloud. [mnm-azure-dns]",
      "type": "A",
      "ttl": "600",
      "data": "17.17.17.17",
      "comment": "",
      "enabled": true,
      "dnsZoneRef": "DNSZones/12",
      "customProperties": {}
```

```
          },
          "ptrStatus": "Unknown",
          "relatedRecords": []
        }
      ],
      "dhcpReservations": [],
      "dhcpLeases": [],
      "discoveryType": "None",
      "lastSeenDate": "",
      "lastDiscoveryDate": "",
      "lastKnownClientIdentifier": "",
      "device": "",
      "interface": "",
      "ptrStatus": "Unknown",
      "extraneousPTR": false,
      "customProperties": {},
      "state": "Assigned",
      "usage": 4
    }
  }
}
```

No-risk installation

Micetro is a non-disruptive DDI solution that you can install in less than an hour in your environment. Since you don’t have to change anything on your endpoint devices for Micetro to start working, it’s a no-risk install.

Corporate Headquarters

4100 Yonge St. 3rd Floor, Toronto, ON, M2P 2B5
1-416-646-8400 | 1-866-895-6931

bluecat.com

Next steps

Use an overlay and orchestration solution to regain network visibility and control.

Request a free trial