VMware Global Network Identities

vmware®

Table of contents

Overview

VMware Global Network Identities™ is a network services platform that provides unified visibility, control and governance of network identities. It offers connectors to orchestrate DNS, DHCP, and IP address management (IPAM) capabilities into existing enterprise, public cloud, and managed solutions. It simplifies the management of network identities and provides a framework for Zero Trust.

Core components

- Resource manager – Utilize the customizable resource management system with flexible structures, fields, permissions, and workflow integration, all driven by API. Create a global source of truth for network identifiers, from virtual machines (VMs) to cloud to branches, all in one place. Implement enterprise-wide Zero Trust security via the common resource framework.
- Global permissions structure – Create groups and user accounts for each object. You can also set permissions down to each object.
- IPAM – Handle everything from subnet allocation management to host-level assignments to devices with complete IPv4/IPv6 support; comes with import tools to get up and running quickly. Enable support for advanced field validation and features, such as IPv6 sparse allocation, virtual routing and forwarding (VRF), and multi-domain VLANs.
- DNS controller – Integrate multiple DNS servers with different DNS technologies and users out of the box with a variety of DNS providers and platforms, giving you the flexibility to work with your current infrastructure as is and ease DNS migration(s) in the future, as needed. Easily support duplicate zones and even the most complicated DNS environments with DNS groups. Utilize built-in support for role-based permissions and approval workflows at the DNS group, DNS zone, and DNS record levels.
- DHCP controller – Take advantage of one-stop configuration management for DHCP scopes. Enable easy integration and use by provisioning teams via API or UI.
- REST API – Enable simple integration into current environments without sacrificing support for future environments via an API-first approach. No more having to question if a feature in the UI has an API.

General architecture

VMware Global Network Identities was designed to unify existing DNS/DHCP/IPAM (DDI) solutions while providing a path to standardized architectures, multi-cloud systems, and public managed DNS providers. Many organizations have various solutions deployed depending on specific requirements and the environment augmented by homegrown network admin tools, spreadsheets and wikis. While many traditional DDI solutions seek to provide all-in-one solutions tied to DNS/DHCP appliances, VMware Global Network Identities offers architecture flexibility along with turnkey, standards-based solutions, focusing on automation, workflows, and a flexible resource system that serves as a foundation for Zero Trust frameworks.

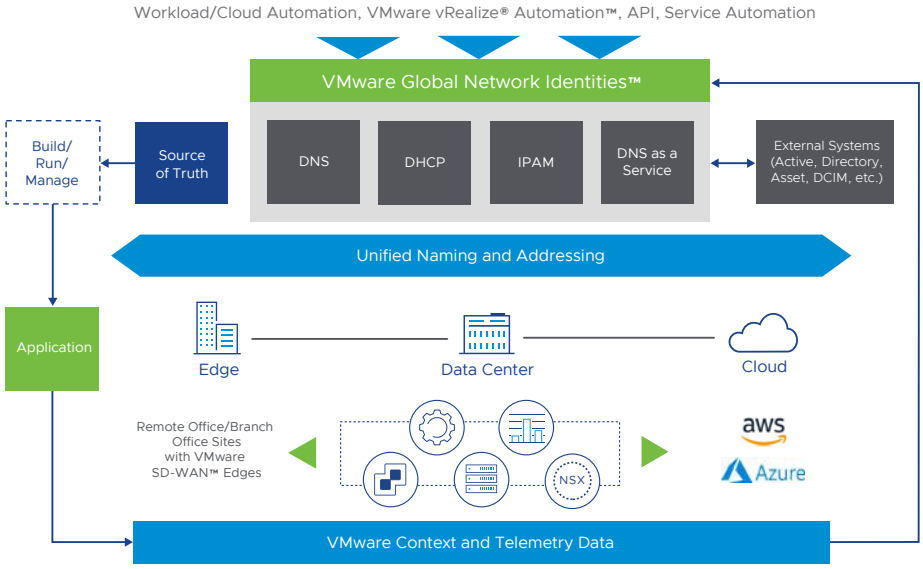

FIGURE 1: The VMware Global Network Identities vision.

Connectors

VMware Global Network Identities offers a wide range of built-in connectors, and provides an extensible framework to quickly deliver additional connectors and even custom connectors specific to environments.

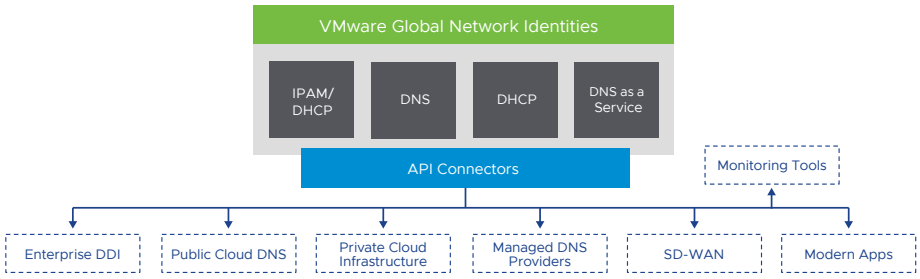

FIGURE 2: VMware Global Network Identities connectors.

Resource system as a foundation for Zero Trust

The resource management system is a key component of VMware Global Network Identities. This system supports a variety of hierarchies and metadata. The resource system acts as a networking source of truth across multiple domains along with a flexible automation framework. The system is delivered with a multitenant foundation along with permissions, constraints, and approval workflows as granular as a single object. Each resource creates an API endpoint, allowing easy integration with automation frameworks or configuration management databases (CMDBs), such as ServiceNow.

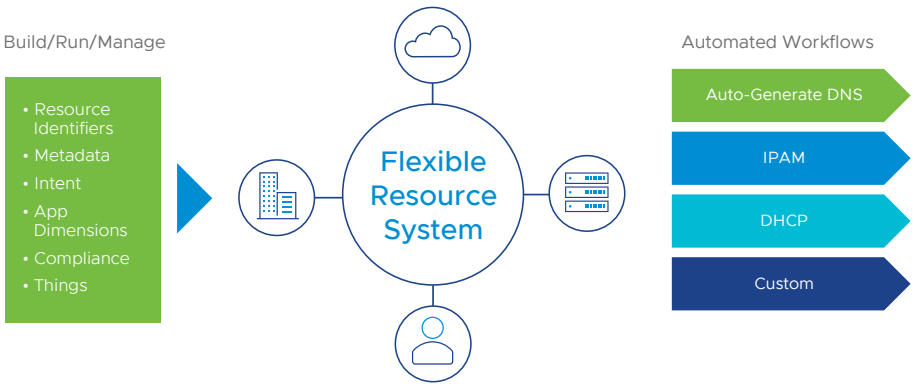

FIGURE 3: The VMware Global Network Identities resource system.

For example, a VM resource can have customizable metadata assigned that can hold any information from environment, universally unique identifiers (UUIDs), owners, compliance information, locations, or anything else. Those fields can then help form DNS entries based on constraints and automated through DNS auto-generation gadgets associated with the resource and IP address assignments based on IPAM smart assign, direct assign, or manual assign (smart browse). This can be done for any other resource as well, such SD-WAN edges (e.g., VMware SD-WAN™ Edges), containers, routers, switches, and the like. The system is completely customizable.

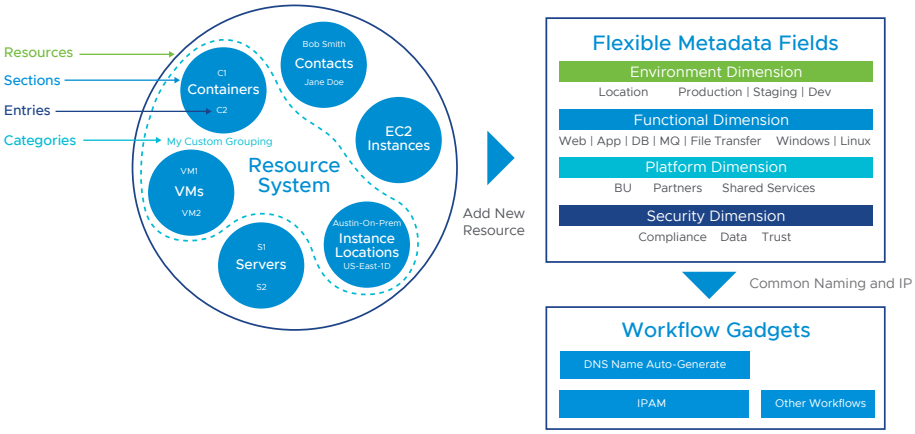

FIGURE 4: VMware Global Network Identities resource system example flow.

Operational considerations

VMware Global Network Identities was built on a multitenant foundation. You have the ability to create groups and user accounts, and can also set permissions down to each object. There is also flexible monitoring and reporting systems built across users, resources, DNS, DHCP and IPAM systems.

Permissions

The permissions structure in VMware Global Network Identities is designed to give you as much flexibility as you need to accommodate most use cases. When mapping out the permissions structure for your organization, keep in mind who you want to access the application:

- Internal users and roles (admins, read only, etc.)
- Partners related to multiple specific resources/accounts
- Customers/departments with a limited view to only their respective resources/accounts

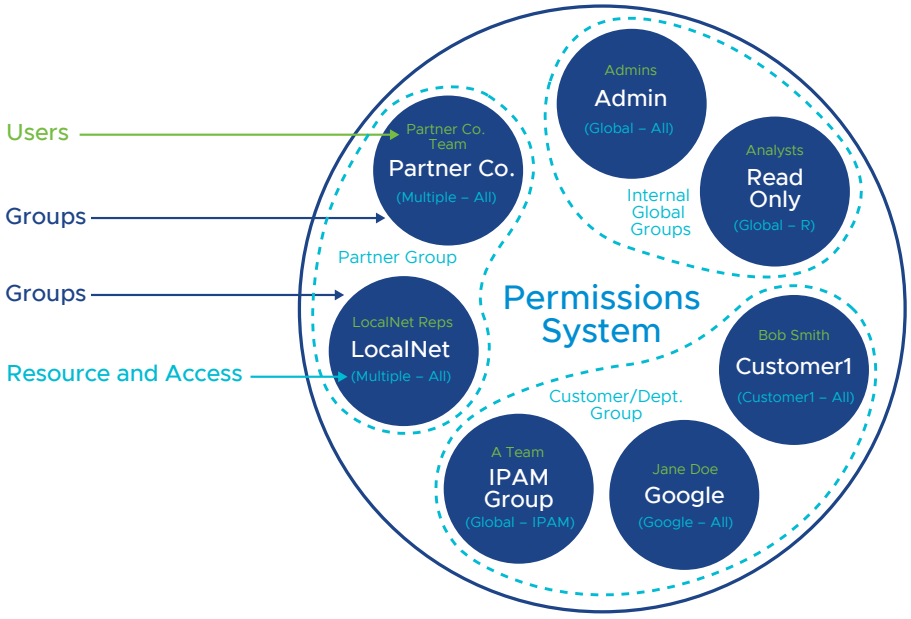

FIGURE 5: The VMware Global Network Identities permissions system.

Figure 5 shows groups for each of those scenarios: internal groups, partner groups, and customer groups. Each of these groups has access to different resources, permission levels, and users assigned to them.

The components of the permissions system include:

- Users – A user is a single login account that accesses VMware Global Network Identities. Users are assigned to groups.
- Groups – A group is a set of permission conditions that apply to selected users. Allowed resources and access levels (C/R/U/D permissions) are set inside the group.
- Resources and access – Inside a group, resource access may be set to global (applies to all resources) or to the resource level (applies to only the selected resources). For each resource selected, access permissions can be set with C/R/U/D permissions under each VMware Global Network Identities functional area (IPAM,

DNS, resource).

As a whole, this makes up the VMware Global Network Identities permissions system. The permissions system allows you to fine-tune access to resource data to be as detailed as you need.

Approvals

The approvals module stores and queues DNS actions made by selected user groups, and sends those actions to a pending changes list for administrative review. Later, an administrator (or combination of administrators) can approve or reject these stored actions.

Currently, approvals are available only for DNS-related actions as we gather feedback and use cases to inform possible future updates.

The VMware Global Network Identities approvals system gives administrators an additional layer of flexibility and oversight to manage which changes are allowed to DNS items by users.

With approvals, administrators can set group permission rules requiring that certain types of DNS changes made by a user are either automatically denied or approved by an administrator. In the latter case, one or more admin groups must be assigned to approve those action types.

Reporting

Reporting contains reports for five VMware Global Network Identities modules: IPAM, DNS, users, resources and DHCP.

Default reports are available for each module, and users can create their own customized report from existing templates. Once created, reports can be exported on demand, or exports can be scheduled to be sent to a user at regular intervals.

Reporting features include:

- Default system reports for IPAM, DNS, users, resources and DHCP
- Customizable user-created reports
- IPAM utilization and runout
- Export reports to .csv and/or .pdf
- Schedule reports to be emailed at selected intervals
- Safely view existing reports and apply filters without overwriting saved report settings, or chose to permanently save changes
- Copy existing reports to use as editable templates
- IPAM reports include integration with IPAM metadata and IPAM column settings

In reporting, any admin user can view, manage and edit an individual report. Default reports will display with “System” as the owner and can be viewed, edited and copied, but they are not deletable.

User-created reports will display with the creator’s username in the owner field and can be viewed, deleted, edited and copied. Report ownership, as a concept, only extends to displaying the creator of the report; there are no report actions that are locked to any specific user or access restrictions in place per report, outside of the normal viewing permissions.

Although it is possible to edit and save both default reports and reports created by other users, it is recommended to either coordinate the changes with the report’s owner or create a new copy of the existing report to use for modifications.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Item No: 970581aq-wp-vmw-glbl-ntwk-ids-a4 6/21