NetBrain Device Discovery

Pre-Requisites

The most critical element of any NetBrain project is readiness of the customer to onboard devices to the NetBrain platform and take the first steps to creating the Digital Twin of the physical network. NetBrain Service Engineers have identified the most critical device discovery pre-requisites to minimize complications and device discovery timeline.

Key Resources for Discovery Success

- ☐ Identify the Network Administrators in your organization that can support ACL updates, creation of Service Accounts, and that control device access credentials (SNMP & SSH)

Network Security

- ☐ Update Firewall ACLs to support required IP connectivity between NetBrain Windows Front Server and the target devices on commonly used ports 161 (SNMP), 22 (SSH), 443/8443/8080 (API)
- ☐ Confirm connectivity (Ping, SNMP, SSH) from Windows Front Server IP Address to all network devices. If a Jumpbox is required to access your network, consult the Jumpbox Configuration Guide for additional requirements.

Standard Devices (Switches, Routers, Load Balancers, etc.)

- ☐ Collect all SNMP v1/2c community strings
- ☐ Collect all SNMP v3 usernames, passwords, and authentication credentials
- ☐ Collect all SSH username/passwords
- ☐ *(Recommended)* Create and deploy Service Account for NetBrain across all network devices
- ☐ *(Optional)* Collect all privilege login credentials (enable password), for devices where service accounts may not have sufficient privileges to retrieve configuration and data tables

Cisco ACI

- ☐ *(Recommended)* Create and deploy a new Service Account for NetBrain and assign to all Security Domains with a minimum of **readPriv** privilege applied
- ☐ Validate that Service Account is assigned to all available system tenants in the Security Domain, including any manually created tenants
- ☐ Validate that Service Account role has all available privileges (admin not required)
- ☐ Collect the IP Address, Username, Password of all APICs in the network
- ☐ Confirm the NetBrain Windows Front Server can successfully access each APIC using the Port Verification Utility

Amazon AWS

- ☐ Review the NetBrain AWS Quick Setup Guide
- ☐ Confirm Access type to be used for discovery: Key-Based, Role-Based, Combined
- ☐ Complete the documented pre-requisites to support AWS discovery

Microsoft Azure

- ☐ Review the NetBrain Azure Quick Setup Guide
- ☐ Confirm that Custom Role(s) have been created
- ☐ Confirm that the Custom role is attached to the subscription

VMware vCenter

- ☐ *(Recommended)* Create and deploy a new Service Account for NetBrain with role type Read-only is created and available for use by NetBrain
- ☐ Identify the URL of the VMware vCenter Controller
- ☐ Gather the Username and Password of the read-only user account

VMware NSX-V

- ☐ All pre-requisites for VMware vCenter
- ☐ *(Recommended)* Create and deploy a new Service Account for NetBrain with role type "Auditor" and it is enabled in vCenter where the NSX Manager is registered
- ☐ Gather the Username and Password of the "Auditor" user account
- ☐ Identify the URL of the NSX Manager

Meraki

- ☐ Identify the URL of the Meraki Cloud Controller
- ☐ Identify the Meraki API Key
- ☐ *(Recommended)* Gather the admin account credentials (or an account with administrator privileges)

If there are questions or clarifications required prior to project kickoff, please contact your NetBrain Account Executive and they can connect you with a representative from the Customer Success Team or open a support case with our Technical Support Team at our Customer Portal or by emailing us at support@netbraintech.com.

NetBrain

+1 (800) 605-7964 | info@netbraintech.com | www.netbraintech.com facebook.com/netbraintech twitter.com/NetBrainTechies