Cisco Catalyst WAN Automation with Ansible

A Comprehensive 5-Lab Training Series

5-Lab Training Series Presentation

Title Slide

Cisco Catalyst WAN Automation with Ansible A Comprehensive 5-Lab Training Series

- Environment: Cisco Catalyst WAN v20.10
- Platform: **https://sandbox-sdwan-2.cisco.com**
- Approach: Read-Only Monitoring & Analysis
- Tools: Ansible + REST APIs

Presented by: [Instructor Name] Date: [Current Date]

Training Objectives

What You Will Learn

By the end of this training, you will be able to:

- Connect to Catalyst WAN vManage via REST API using Ansible
- Monitor Catalyst WAN fabric health and performance
- Analyze policies and configuration templates
- Generate automated compliance and security reports
- Implement network monitoring workflows
- Troubleshoot Catalyst WAN environments using automation

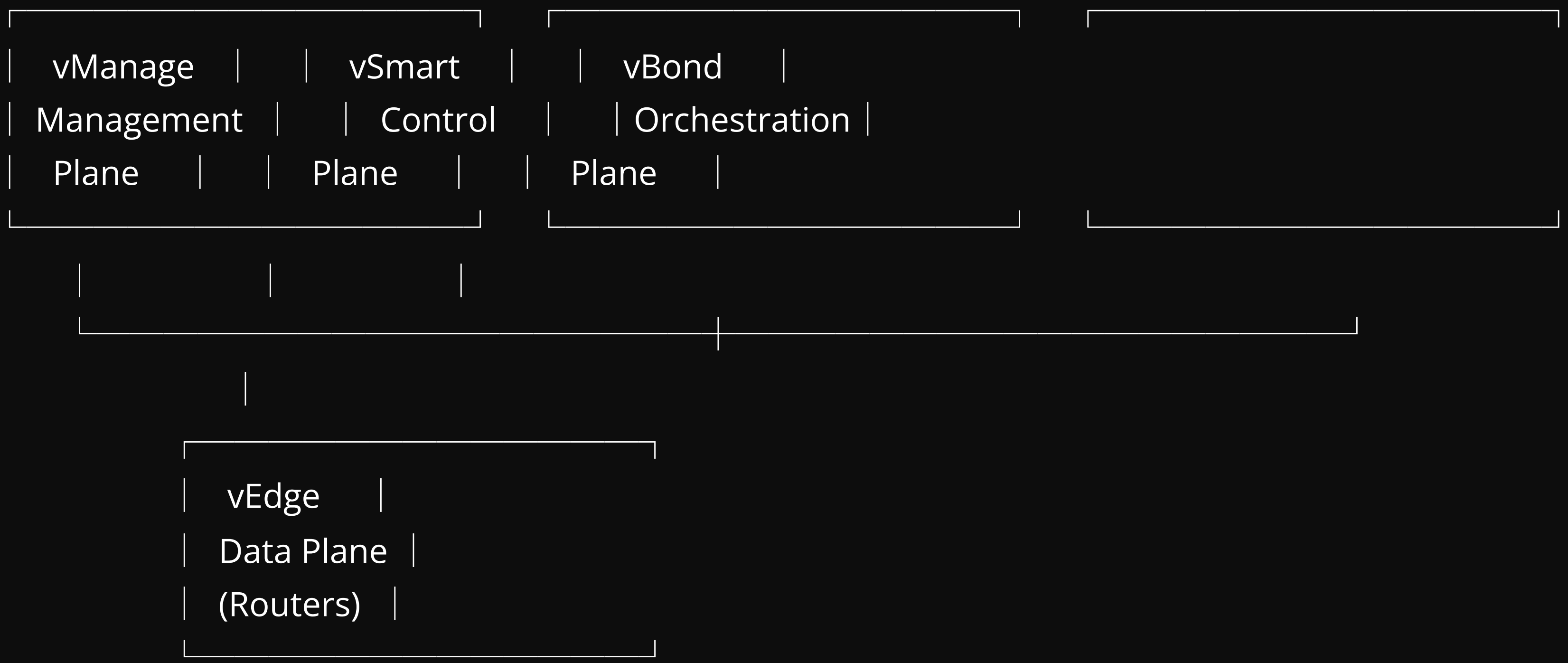
Lab Series Overview

5 Progressive Labs

Lab	Topic	Focus
Lab 1	Basic Connectivity & Device Discovery	API fundamentals, device inventory
Lab 2	Catalyst WAN Fabric Health Monitoring	Control/data plane status
Lab 3	Policy & Template Analysis	Configuration management
Lab 4	Network Performance Monitoring	Metrics and optimization
Lab 5	Security & Compliance Reporting	Audit and compliance

Catalyst WAN Architecture Overview

Understanding the Catalyst WAN Components



vManage Management Plane

vSmart Control Plane

vBond Orchestration Plane

vEdge Data Plane (Routers)

Key Components:

- vManage: Centralized management and monitoring
- vSmart: Control plane policy distribution
- vBond: Device orchestration and onboarding
- vEdge: Data plane routing and forwarding

Lab Environment Setup

Sandbox Environment Details

Environment Specifications:

- URL: **https://sandbox-sdwan-2.cisco.com**
- Username: devnetuser
- Password: [Provided by instructor]
- Version: Cisco Catalyst WAN v20.10
- Access: Read-Only (monitoring and analysis only)

Prerequisites:

- Ansible installed with cisco.catalystwan collection
- Network connectivity to sandbox environment
- Basic understanding of REST APIs
- Familiarity with YAML syntax

Lab 1 - Basic Connectivity & Device Discovery

Establishing Foundation

Objectives:

- Test API connectivity to vManage
- Discover all Catalyst WAN devices in the fabric
- Categorize devices by type and role
- Generate device inventory reports

Key Concepts:

- Catalyst WAN REST API authentication
- Device hierarchy (controllers vs edges)
- System IP addressing in Catalyst WAN
- Ansible httpapi connection plugin

Deliverables:

- Device inventory report
- Understanding of fabric topology
- Working API connectivity

Lab 1 - Technical Implementation

API Connection Methods

Method 1: CLI Ad-hoc Commands

```
ansible vmanage1 -i ansible-collection-sdwan/inventory.ini -m cisco.catalystwan.devices_info -a '{"manager_credentials": {"url": "https://10.10.20.90:443", "username": "admin", "password": "C1sco12345"}, "device_category": "controllers"}'
```

Method 2: YAML Playbook

```
- name: Discover Catalyst WAN devices
  cisco.catalystwan.devices_info:
    manager_credentials:
      url: "https://{{ inventory_hostname }}:443"
      username: "{{ ansible_user }}"
      password: "{{ ansible_password }}"
    device_category: controllers
  register: all_devices
```

Key Learning Points:

- Inventory file configuration for httpapi
- Device categorization and filtering
- Error handling for sandbox limitations
- Report generation and analysis

Lab 2 - Catalyst WAN Fabric Health Monitoring

Monitoring Control and Data Planes

Objectives:

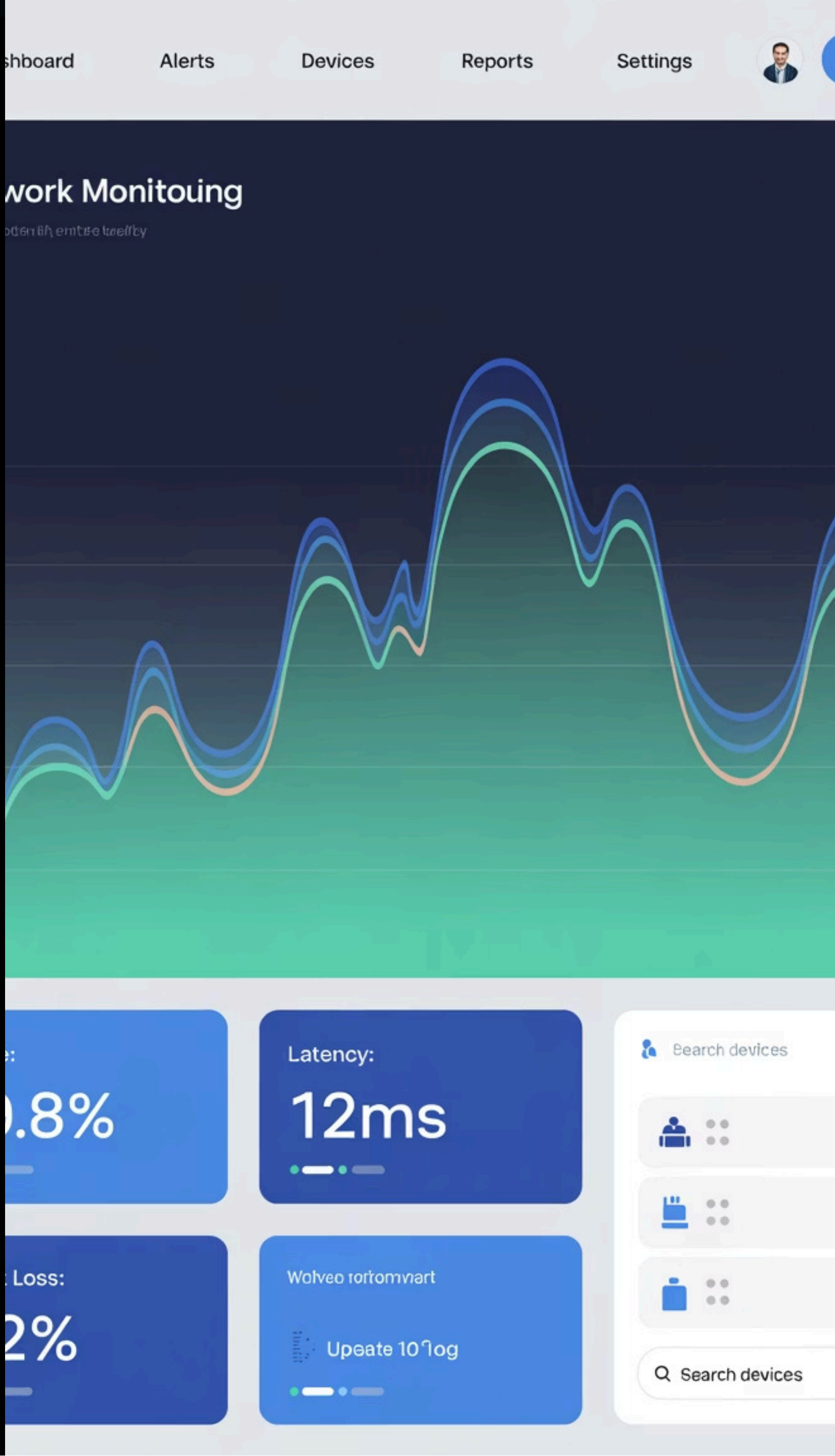
- Monitor control plane connections (vEdge ↔️ vSmart)
- Check BFD session health and statistics
- Analyze OMP peer relationships
- Examine IPsec tunnel status and performance

Key Concepts:

- Control plane vs data plane separation
- BFD (Bidirectional Forwarding Detection)
- OMP (Overlay Management Protocol)
- Tunnel establishment and maintenance

Deliverables:

- Fabric health score calculation
- Connection status dashboard
- Performance trend analysis



Lab 2 - Health Monitoring Metrics

Key Performance Indicators

Control Plane Health:

- vEdge to vSmart connections: UP/DOWN status
- Control connection count and stability
- Authentication and certificate validation

Data Plane Health:

- BFD session establishment and maintenance
- IPsec tunnel count and throughput
- Packet loss and latency measurements

Health Score Calculation:

Overall Health = (Control Plane % + Data Plane % + BFD %) / 3

Alert Thresholds:

- 🟢 Healthy: >95%
- 🟡 Warning: 80-95%
- 🔴 Critical: <80%

Lab 3 - Policy & Template Analysis

Configuration Management at Scale

01

Inventory centralized policies and their status

02

Analyze device templates and feature templates

03

Examine security policies and access controls

04

Generate policy compliance reports

Key Concepts:

- Centralized vs localized policy enforcement
- Template hierarchy and inheritance
- Policy precedence and conflict resolution
- Configuration drift detection

Deliverables:

- Policy inventory documentation
- Template usage analysis
- Compliance gap assessment

Lab 3 - Policy Architecture

Catalyst WAN Policy Framework

```
Centralized Policies
├── Application-Aware Routing
│   ├── Traffic Engineering
│   └── Path Selection
├── Security Policies
│   ├── Access Control Lists
│   ├── Firewall Rules
│   └── URL Filtering
└── QoS Policies
    ├── Traffic Classification
    └── Bandwidth Allocation

Device Templates
├── System Templates
├── Interface Templates
└── Routing Protocol Templates
```

Policy Types:

- **Control Policies:** Route advertisement and filtering
- **Data Policies:** Traffic forwarding and security
- **Application Policies:** App-aware routing decisions

Lab 4 - Network Performance Monitoring

Optimizing Network Performance

Collect interface utilization and error statistics

Monitor application-aware routing effectiveness

Analyze tunnel bandwidth and latency metrics

Generate performance optimization recommendations

Key Concepts:

- Interface utilization thresholds and alerting
- Application response time monitoring
- Quality of Experience (QoE) measurements
- Performance baselines and trending

Deliverables:

- Performance dashboard
- Bandwidth utilization reports
- Application performance analysis

Lab 4 - Performance Metrics

Comprehensive Network Visibility

Interface Metrics:

- Bandwidth utilization (RX/TX)
- Packet error rates and discards
- Interface availability and status

Application Metrics:

- Response time and latency
- Throughput and loss measurements
- Application classification accuracy

Tunnel Performance:

- IPsec tunnel utilization
- Path quality measurements
- Failover and recovery times

Performance Thresholds:

Interface Utilization:

- Green: <70% - Normal operation
- Yellow: 70-85% - Monitor closely
- Red: >85% - Capacity planning needed

Lab 5 - Security & Compliance Reporting

Ensuring Security Posture

Audit certificate status and expiration dates

Analyze security policy configurations and enforcement

Monitor authentication and authorization events

Generate comprehensive compliance reports

Key Concepts:

- PKI certificate lifecycle management
- Zero-trust security architecture
- Audit logging and compliance tracking
- Security policy effectiveness measurement

Deliverables:

- Security posture assessment
- Certificate management reports
- Compliance gap analysis

Lab 5 - Security Framework

Catalyst WAN Security Architecture

Security Layers:

```
┌─────────────────────────────────────────────┐
│        Application Layer       │ ← URL Filtering, App Control
├─────────────────────────────────────────────┤
│         Network Layer          │ ← Firewall, ACLs, IPS
├─────────────────────────────────────────────┤
│        Transport Layer         │ ← IPsec, TLS Encryption
├─────────────────────────────────────────────┤
│      Authentication Layer      │ ← PKI Certificates, AAA
└─────────────────────────────────────────────┘
```

Identity

Certificate-based device authentication

Segmentation

Micro-segmentation and VPN isolation

Policy

Centralized security policy enforcement

Visibility

Comprehensive logging and monitoring

Ansible Integration Benefits

Why Ansible for Catalyst WAN Automation

Key Advantages:

- **Agentless:** No additional software on Catalyst WAN devices
- **REST API Native:** Direct integration with vManage APIs
- **Idempotent:** Safe to run multiple times
- **Scalable:** Handles large Catalyst WAN deployments
- **Readable:** YAML playbooks are self-documenting

Use Cases:

- **Monitoring:** Automated health checks and reporting
- **Compliance:** Regular configuration audits
- **Troubleshooting:** Systematic data collection
- **Documentation:** Dynamic inventory and topology
- **Integration:** Connect with ITSM and monitoring tools

Real-World Applications

Beyond the Labs

Network Operations:

- Automated daily health reports
- Performance trending and capacity planning
- Proactive alerting for threshold breaches
- Change management validation

Security Operations:

- Certificate expiration monitoring
- Security policy compliance checking
- Audit trail generation for compliance
- Incident response data collection

Business Operations:

- SLA monitoring and reporting
- Cost optimization through utilization analysis
- Vendor management and performance metrics
- Risk assessment and mitigation planning

Best Practices & Lessons Learned

Implementation Guidelines

Development Best Practices:

- Start with read-only operations in production
- Implement proper error handling and logging
- Use version control for playbooks
- Test thoroughly in sandbox environments
- Document all custom modules and roles

Operational Best Practices:

- Schedule regular automated health checks
- Establish performance baselines and thresholds
- Implement graduated alerting (info → warn → critical)
- Maintain audit trails for all automation activities
- Regular review and optimization of automation workflows

Troubleshooting Common Issues

Solutions to Typical Challenges

API Connectivity Issues:

```
# Problem: SSL certificate validation errors
# Solution: Set validate_certs=false in sandbox environments

# Problem: Authentication timeouts
# Solution: Check credentials and network connectivity
```

Data Collection Issues:

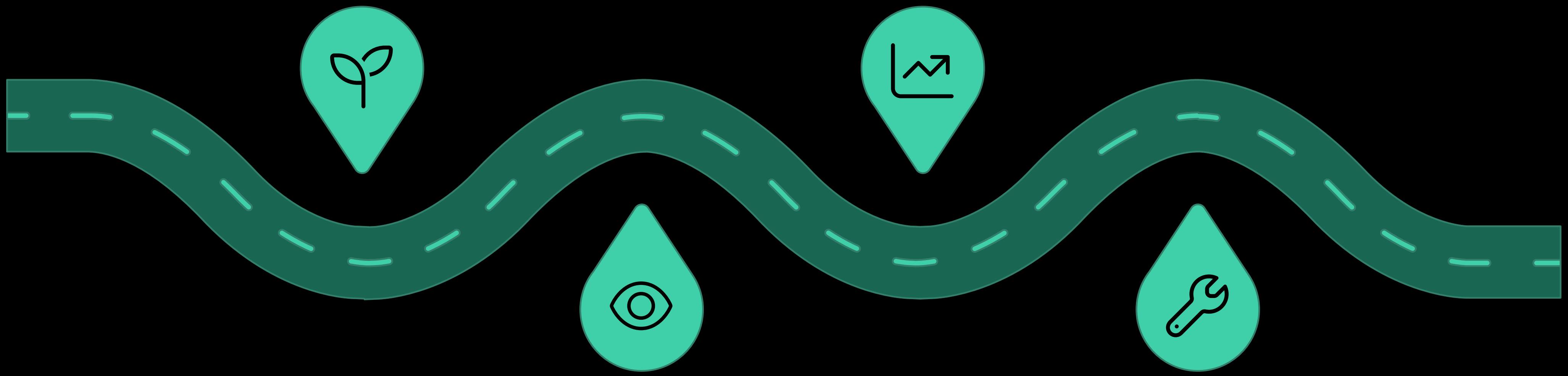
- **Empty Responses:** Some sandbox environments have limited data
- **Rate Limiting:** Implement delays between API calls
- **Large Datasets:** Use pagination and filtering
- **Version Compatibility:** Check Catalyst WAN software versions

Playbook Optimization:

- Use ignore_errors: yes for optional data collection
- Implement proper variable defaults with | default('N/A')
- Group related API calls to minimize round trips

Lab Progression & Skills Building

Learning Path Structure



Lab 1

Foundation — Beginner: API connectivity

Lab 2

Monitoring — Intermediate data collection

Lab 3

Analysis — Intermediate complex analysis

Lab 4

Optimization — Advanced automation

Skills Progression:

- **Beginner:** API connectivity and basic data collection
- **Intermediate:** Complex data analysis and reporting
- **Advanced:** Custom automation and integration workflows

Extension Opportunities

Beyond the Core Labs

Advanced Topics:

- Custom dashboard creation with collected data
- Integration with monitoring tools (Grafana, Splunk)
- Automated remediation workflows
- Multi-tenant Catalyst WAN management
- CI/CD pipeline integration for network changes

Integration Projects:

- **ITSM Integration:** Automatic ticket creation for issues
- **ChatOps:** Slack/Teams integration for network status
- **Reporting:** Executive dashboards and KPI tracking
- **Alerting:** PagerDuty/Opsgenie integration
- **Documentation:** Auto-generated network documentation

Industry Impact & Career Benefits

Professional Development Value

Market Demand:

- Catalyst WAN adoption growing at 25% annually
- Network automation skills in high demand
- DevOps practices expanding to network operations
- Cloud-first networking strategies driving automation needs

Career Advancement:

- **Network DevOps Engineer:** Automation-focused network roles
- **Site Reliability Engineer:** Infrastructure automation expertise
- **Solutions Architect:** End-to-end automation design
- **Technical Consultant:** Customer automation implementations

Skill Transferability:

- Ansible knowledge applies across IT infrastructure
- REST API skills valuable for cloud platforms
- YAML/JSON data formats universal in modern IT
- Automation mindset applicable to any technology stack

Resources & Next Steps

Continuing Your Learning Journey

Official Resources:

- Cisco Catalyst WAN Documentation Portal
- Ansible Network Automation Documentation
- Cisco DevNet Learning Labs and Sandboxes
- Catalyst WAN REST API Reference Guide

Community Resources:

- Ansible Network Automation Community
- Cisco Catalyst WAN Reddit Community
- DevNet Community Forums
- GitHub Catalyst WAN Automation Projects

Certification Paths:

- Cisco DevNet Associate/Professional
- Red Hat Certified Specialist in Ansible Automation
- Network Automation certifications from various vendors

Lab Completion & Assessment

Validation & Recognition

Lab Completion Criteria:

- ✅ Successfully complete all 5 labs
- ✅ Generate required reports from each lab
- ✅ Demonstrate understanding of key concepts
- ✅ Troubleshoot common issues independently

Assessment Methods:

- Practical lab execution and validation
- Report quality and analysis depth
- Understanding of Catalyst WAN concepts
- Ability to modify playbooks for custom requirements

Recognition:

- Certificate of completion
- Digital badge for LinkedIn/resume
- Reference materials for future use
- Access to advanced automation resources

Q&A and Lab Environment Access

Getting Started

Environment Access:

- URL: https://sandbox-sdwan-2.cisco.com
- Credentials: [Provided during session]
- Lab Files: Available in course materials
- Duration: Sandbox access for [X] days

Support Resources:

- Lab instruction guides for each exercise
- Sample playbooks and inventory files
- Troubleshooting guides and FAQs
- Instructor office hours schedule

Questions & Answers Session

Ready to begin your Catalyst WAN automation journey? Let's start with Lab 1: Basic Connectivity & Device Discovery!

Appendix - Quick Reference

Command Cheat Sheet

Essential Ansible Commands:

```
# Test connectivity
ansible vmanage1 -i ansible-collection-sdwan/inventory.ini -m ping

# Run device discovery
ansible-playbook -i ansible-collection-sdwan/inventory.ini SDWAN-lab1-device-discovery.yml

# Check playbook syntax
ansible-playbook --syntax-check playbook.yml

# Run with verbose output
ansible-playbook -vvv playbook.yml

# Dry run (check mode)
ansible-playbook --check playbook.yml
```

Useful REST API Endpoints:

- /dataservice/device - Device information
- /dataservice/device/control/connections - Control plane status
- /dataservice/template/policy/vedge - Centralized policies
- /dataservice/certificate/stats - Certificate information