IP FABRIC

Building a DORA-Compliant Network Resilience Practice

Building a DORA-Compliant Network Resilience Practice

IP FABRIC
AUTOMATED NETWORK ASSURANCE PLATFORM

Compliance through operational resilience - made clear for network teams.

The IP Fabric Automated Network Assurance Platform helps provide the controls and the evidence needed for resilient digital operations and therefore, regulatory compliance, including the EU's Digital Operational Resilience Act (DORA).

Translating hefty compliance regulations into practical steps for your IT network teams is no easy feat. With the enforcement of the DORA – taking effect on 17 January 2025 - it's time to act.

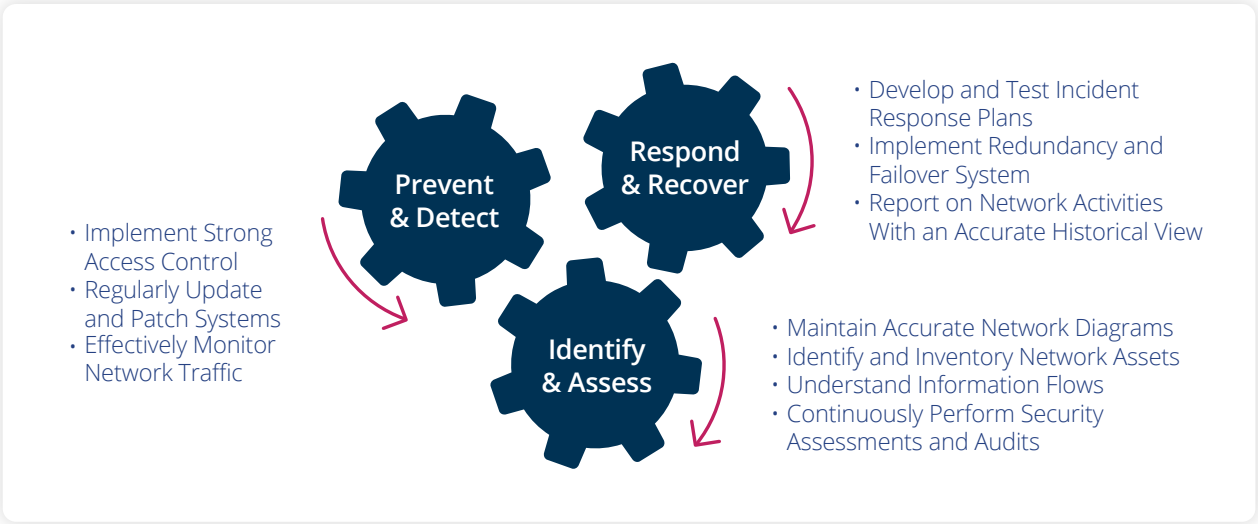
This document is intended to help you take steps today to assure that you (1) are compliant with critical controls outlined in DORA and (2) can produce necessary evidence for internal and external parties.

DORA has five pillars;

- ICT-risk management,
- reporting,
- testing,
- managing third-party risk, and
- information sharing.

10 DORA controls satisfied by IP Fabric to ensure operational resilience in your IT network

We've mapped, directly from the DORA text, ten necessary DORA controls that you can implement in your network today. With DORA's emphasis on proving resilience through surfacing and sharing actionable network insights, these 10 controls can be used as 10 steps to take that will help make your network more resilient and ensure you have the proof of compliance you need when auditors arrive. We've grouped the recommendations into three areas represented in IP Fabric's DORA-safe triad below. IP Fabric's Automated Network Assurance Platform has all of the capabilities needed for these ten requirements.



1. Maintain Accurate Network Diagrams (Article 8.4, Article 8.5)

Requirement: Keep up-to-date diagrams of the network's architecture, including all devices, connections, and configurations.

IP Fabric Provides:

- Automated Network Mapping: IP Fabric automatically generates detailed network maps, providing real-time visibility of all network devices and connections.
- Critical Infrastructure Mapping: Helps assess network functions and services to evaluate criticality, ensuring situational awareness.
- Risk Analysis: By keeping diagrams current, IP Fabric aids in identifying potential vulnerabilities and third-party borders, supporting risk assessments.

2. Identify and Inventory Network Assets (Article 8.1, Article 8.4)

Requirement: Maintain an inventory of all network assets, including hardware and software components.

IP Fabric Provides:

- Automated Asset Discovery: Automatically discovers and inventories all network components, eliminating manual errors.
- Up-to-Date Asset Lists: Ensures that asset information is always current, aiding in accurate management and protection.

3. Understand Information Flows (Article 9.2, Article 11.5)

Requirement: Model data flows to identify critical paths and ensure security controls are in place.

IP Fabric Provides:

- End-to-End Path Analysis: Models data flows through the network to identify and secure critical data paths.
- Security Control Validation: Ensures that necessary controls protect data integrity and confidentiality, integrating seamlessly into operational processes like incident response.

4. Continuously Perform Security Assessments and Audits (Article 25)

Requirement: Conduct regular security assessments to identify vulnerabilities.

IP Fabric Provides:

- Automated Security Scans: Performs continuous vulnerability scans and audits, identifying security weaknesses with precision.
- Increased Frequency and Accuracy: Automation allows for more frequent and accurate assessments, ensuring timely remediation.

5. Implement Strong Access Control (Article 9.2, Article 9.4)

Requirement: Ensure only authorized access to network resources using RBAC and the principle of least privilege.

IP Fabric Provides:

- Access Policy Validation: Tests and validates access policies, ensuring compliance with network segmentation and access control protocols.
- Segmentation Analysis: Validates the enforcement of network segmentation policies to minimize exposure risks.

6. Regularly Update and Patch Systems (Article 9)

Requirement: Keep systems up-to-date to protect against vulnerabilities.

IP Fabric Provides:

- **Patch Management Oversight:** Tracks & validates the deployment of patches & updates across the network.
- **Configuration Standard Compliance:** Ensures policies, including hardening and encryption standards, are correctly implemented & enforced.

7. Effectively Monitor Network Traffic (Article 9.1)

Requirement: Observe network traffic for anomalies and potential threats.

IP Fabric Provides:

- Comprehensive Traffic Monitoring: Provides continuous traffic monitoring to detect unusual activities.
- IDS/IPS Integration: Supports integration with intrusion detection and prevention systems to mitigate potential threats

8. Develop & Test Incident Response Plans (Article 11.2-b)

Requirement: Define and regularly test incident response plans.

IP Fabric Provides:

- Incident Response Automation: Embeds network intelligence into incident response plans and service tickets.
- Regular Testing and Updates: Facilitates regular testing and updates to ensure the effectiveness of response strategies.

9. Implement Redundancy and Failover System (Article 11.4, Article 12)

Requirement: Ensure network resilience through redundancy in critical components.

IP Fabric Provides:

- Redundancy Planning: Assists in designing redundant architectures and validating backup systems.
- Failover Testing: Ensures networks can function as expected during business continuity and disaster recovery plans.

10. Report on Network Activities with an Accurate Historical View (Article 19)

Requirement: Document and maintain a historical view of network activities for troubleshooting and reporting.

IP Fabric Provides:

- Historical Data Access: Provides automated documentation of network changes over time, enabling retroactive analysis.
- Comprehensive Reporting: Ensures up-to-date understanding of network activities, enhancing transparency and accountability.

What to include in your DORA compliance reports

If the above network controls are successfully implemented, you should have the information you need to prove DORA compliance. We've clarified the outputs you'd want to include, to prove that your controls are effective, and they boil down to the following three buckets of evidence:

ASSETS	INTERDEPENDENCIES	TRAFFIC FLOWS
Discovery: Complete discovery of network assets to provide an inventory of known knowns and known unknowns. **Scope:** Establishing the boundaries of the network – identifying borders beyond which third parties, ISPs, etc manage adjacent infrastructure. **Lifecycle:** Show that you can determine when owned and managed assets are EOS, EOL, EOM. **Hardening:** Validate configuration standards are applied. **Vulnerabilities:** Demonstrate that you're checking against the NIST CVE database. **Backups:** Prove you're storing configuration backups for devices so they can be restored to new devices in case of failure.	**Map Topology:** Build a trustworthy view of the network that changes with it. **Segmentation:** Validate the extent of network segments and policy enforcement between them.	**Record Critical Service Paths:** Show that you understand how services are dependent on network infrastructure client to workload. **Validation Of Business Continuity:** Show that services will continue to function after DR invocation.

The IP Fabric Automated Network Assurance Platform produces a complete data model of your network, all its components, relationships, and dependencies. The data are used in a few ways to support a DORA compliance program

- Data regarding the observed state of the network is compared to your "intent" and differences are flagged in our dashboard or pushed to users or to other systems;
- Specific "maps" can be drawn for each of your critical services as evidence that you have proper controls in place for each, or you can map the network holistically;
- Data can be pushed into other systems such as CMDB, configuration management, automation, firewall policy management, network monitoring, etc. This assures that every tool that helps you operate a secure and resilient environment has all the information needed to work as intended. Nothing is missed.

For teams managing large and complex network environments, achieving the above manually is unreasonable; you simply can't measure, visualize, and validate what you don't know is there. With ICT-Risk Management playing such a huge role in DORA, proceeding without this baseline of network knowledge is futile.

Automated network assurance offers day one peace of mind by automatically gathering and analyzing the network data to provide understanding, visibility, and control; the exact ingredients you need to proactively achieve DORA compliance.

Talk to the IP Fabric team to learn more about how we help you achieve digital operational resilience and provide the evidence needed for DORA compliance.

Mock DORA Compliance Report Output Example

Produced by IP Fabric	16.05.2024 9:05
IP Fabric URL	https://demo2.eu.ipfabric.io
Snapshot ID	40e3426f-877e-46ee-a48d-18868b51262d

Applications

Name	Client	Endpoint	Protocol	Destination Port	URL	Comments
Internal-app	172.16.12.60/31	172.16.31.60	TCP	443	https://app.internal/	Internal app for use by users inside network
External-app	172.16.21.0/24	172.16.32.60	TCP	443	https://app.external.com/	External-facing app for use by users coming in over VPN

Checks

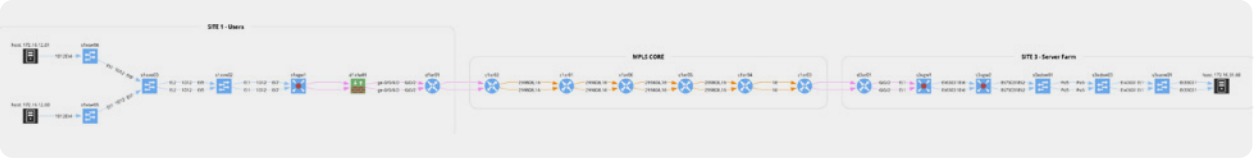
Border	Unmanaged neighbors present
Hardware EOL	Self explanatory - no longer supported by vendor
AAA	Authentication intent check
NTP	Time protocol intent check
SNMP	Monitoring protocol intent check
Management Access	Method of access to device
CVEs	Cross-reference vendor, platform, OS version w/ NIST CVE database
Backups	Configuration backups stored

Network Inventory

Hostname		Serial Number	Login IP	Vendor	Family	Platform	Model	Version	Type	Border	Hardware EOL	AAA	NTP	SNMP	Management Access	CVEs	Backups
c1xr01		303ef2beb338	192.168.1.101	juniper	junos	vsrx		21.3R1.9	router	Y	N	Y	Y	Y	SSH	142	Y
c1xr02		daaa27594ff5	192.168.1.102	juniper	junos	vsrx		21.3R1.9	router	Y	N	N	N	N	SSH	142	Y
c1xr03		eab19849667b	192.168.1.103	juniper	junos	vsrx		21.3R1.9	router	N	N	Y	Y	N	SSH	142	Y
c1xr04		5bc8d7731a2d	192.168.1.112	juniper	junos	vsrx		21.3R1.9	router	N	N	Y	Y	N	SSH	142	Y
c1xr05		291575d76603	192.168.1.113	juniper	junos	vsrx		21.3R1.9	router	N	N	Y	Y	Y	SSH	142	Y
c1xr06		0cc6e8184696	192.168.1.114	juniper	junos	vsrx		21.3R1.9	router	N	N	Y	Y	N	SSH	142	Y
d1xfw01		42c18111c48f	192.168.1.106	juniper	junos	vsrx		21.3R1.9	fw	N	N	Y	Y	N	SSH	142	Y
d1xr01		a000004	192.168.1.104	cisco	ios	vios	IOSv	15.6(2)T	router	N	N	Y	Y	N	SSH	63	Y
d1xr02		a000005	192.168.1.105	cisco	ios	vios	IOSv	15.6(2)T	router	N	N	Y	Y	N	SSH	63	Y
d2xfw01	ht	e7ad6ce97d43	192.168.1.107	juniper	junos	vsrx		21.3R1.9	fw	Y	N	Y	Y	Y	SSH	142	Y
d3xr01		a000008	192.168.1.108	cisco	ios	vios	IOSv	15.6(2)T	router	N	N	Y	Y	Y	SSH	63	Y
d3xr02		a000009	192.168.1.109	cisco	ios	vios	IOSv	15.6(2)T	router	N	N	Y	Y	N	SSH	63	Y
d4xr01		a00000a	192.168.1.110	cisco	ios	vios	IOSv	15.6(2)T	router	N	N	Y	Y	Y	SSH	63	Y
d4xr02		a00000b	192.168.1.111	cisco	ios	vios	IOSv	15.6(2)T	router	N	N	Y	Y	N	SSH	63	Y
s1xgw1		D59DF0117331E56E9AD	192.168.1.115	arista	eos	lab	vEOS-lab	4.27.0F	l3switch	N	N	Y	Y	Y	SSH	10	Y
s1xgw2		B59D046ECD68B12E98(	192.168.1.116	arista	eos	lab	vEOS-lab	4.27.0F	l3switch	N	N	Y	Y	Y	SSH	10	Y
s1xsw01		04EBF26CE8D30151E09	192.168.1.117	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s1xsw02		4C3BCD87D9B5D51985	192.168.1.118	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s1xsw03		CA86EAAE3A09DBA6BA(	192.168.1.119	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s1xsw04		1AEC44D7BEC7301D98:	192.168.1.120	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s1xsw05		48D5AA877626622C2BC	192.168.1.121	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s1xsw06		7F41ADA9A64A2D4D272	192.168.1.122	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s2xgw1	ht	FF5EC10DACCD4D0121	192.168.1.125	arista	eos	lab	vEOS-lab	4.27.0F	l3switch	N	N	Y	Y	Y	SSH	10	Y
s2xsw01	ht	5171A617C468E8EAD8F	192.168.1.126	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s3xasw01		E1EB311F49EACCB01CI	192.168.1.134	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s3xasw02		AA758CCE35D59BBA61(	192.168.1.135	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s3xasw03		7198377790A03F428E1(	192.168.1.136	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s3xasw04		F7962F589B50A7431A5(	192.168.1.137	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s3xdsw01		4237F4D2E10890AAE1E	192.168.1.130	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s3xdsw02		F3D6908E2AF5EC86B67	192.168.1.131	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s3xdsw03		EEC4ECE5090A9E39AB5	192.168.1.132	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s3xdsw04		D249D8090EA37136274	192.168.1.133	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s3xgw1		300F1478C6CBE5021E9	192.168.1.128	arista	eos	lab	vEOS-lab	4.27.0F	l3switch	N	N	Y	Y	Y	SSH	10	Y
s3xgw2		34DD1F8A41D640616421	192.168.1.129	arista	eos	lab	vEOS-lab	4.27.0F	l3switch	N	N	Y	Y	Y	SSH	10	Y
s4xsw01		A782C7E99EF451909BA	192.168.1.140	arista	eos	lab	vEOS-lab	4.27.0F	l3switch	N	N	Y	Y	Y	SSH	10	Y
s4xsw02		72606E0653E2447A9A5:	192.168.1.141	arista	eos	lab	vEOS-lab	4.27.0F	l3switch	N	N	Y	Y	Y	SSH	10	Y
s4xsw03		BC8EC0CA486DF930502	192.168.1.142	arista	eos	lab	vEOS-lab	4.27.0F	l3switch	N	N	Y	Y	Y	SSH	10	Y
s4xsw04		1ACC4C10A9256A440B(	192.168.1.143	arista	eos	lab	vEOS-lab	4.27.0F	l3switch	N	N	Y	Y	Y	SSH	10	Y
s4xsw05		6EFDE9E0EFF5C2BCD1(	192.168.1.144	arista	eos	lab	vEOS-lab	4.27.0F	l3switch	N	N	Y	Y	Y	SSH	10	Y
s4xsw06		FFA802927CEBA097720	192.168.1.145	arista	eos	lab	vEOS-lab	4.27.0F	l3switch	N	N	Y	Y	Y	SSH	10	Y
s4xsw07		03B74C53392A877190F	192.168.1.146	arista	eos	lab	vEOS-lab	4.27.0F	l3switch	N	N	Y	Y	Y	SSH	10	Y
s5xr01		a000031	192.168.1.149	cisco	ios	vios	IOSv	15.6(2)T	router	N	N	Y	Y	N	SSH	63	Y
s5xr02		a000032	192.168.1.150	cisco	ios	vios	IOSv	15.6(2)T	router	N	N	Y	Y	N	SSH	63	Y
s5xr03		a000033	192.168.1.151	cisco	ios	vios	IOSv	15.6(2)T	router	N	N	Y	Y	N	SSH	63	Y
s5xr04		a000034	192.168.1.152	cisco	ios	vios	IOSv	15.6(2)T	router	N	N	Y	Y	N	SSH	63	Y
s5xr05		a000035	192.168.1.153	cisco	ios	vios	IOSv	15.6(2)T	router	N	N	Y	Y	N	SSH	63	Y
s5xr06		a000036	192.168.1.154	cisco	ios	vios	IOSv	15.6(2)T	router	Y	N	Y	Y	N	SSH	63	Y

Internal - App

Hostname	Site	Serial Number	Login IP	Vendor	Family	Platform	Model	Version	Type	Border	Hardware EOL	AAA	NTP	SNMP	Management Access	CVEs	Backups
s1xsw06	SITE 1 - Us	7F41ADA9	192.168.1	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s1xsw05	SITE 1 - Us	48D5AA87	192.168.1	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s1xsw03	SITE 1 - Us	CA86EAAE	192.168.1	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s1xsw02	SITE 1 - Us	4C3BCD87	192.168.1	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s1xgw1	SITE 1 - Us	D59DF011	192.168.1	arista	eos	lab	vEOS-lab	4.27.0F	l3switch	N	N	Y	Y	Y	SSH	10	Y
d1xfw01	SITE 1 - Us	42c18111	192.168.1	juniper	junos	vsrx		21.3R1.9	fw	N	N	Y	Y	N	SSH	142	Y
d1xr01	SITE 1 - Us	a000004	192.168.1	cisco	ios	vios	IOSv	15.6(2)T	router	N	N	Y	Y	N	SSH	63	Y
c1xr02	MPLS COR	daaa2759	192.168.1	juniper	junos	vsrx		21.3R1.9	router	Y	N	N	N	N	SSH	142	Y
c1xr01	MPLS COR	303ef2be	192.168.1	juniper	junos	vsrx		21.3R1.9	router	Y	N	Y	Y	Y	SSH	142	Y
c1xr06	MPLS COR	0cc6e818	192.168.1	juniper	junos	vsrx		21.3R1.9	router	N	N	Y	Y	N	SSH	142	Y
c1xr05	MPLS COR	291575d7	192.168.1	juniper	junos	vsrx		21.3R1.9	router	N	N	Y	Y	Y	SSH	142	Y
c1xr04	MPLS COR	5bc8d773	192.168.1	juniper	junos	vsrx		21.3R1.9	router	N	N	Y	Y	N	SSH	142	Y
c1xr03	MPLS COR	eab19849	192.168.1	juniper	junos	vsrx		21.3R1.9	router	N	N	Y	Y	N	SSH	142	Y
d3xr01	SITE 3 - Se	a000008	192.168.1	cisco	ios	vios	IOSv	15.6(2)T	router	N	N	Y	Y	Y	SSH	63	Y
s3xgw1	SITE 3 - Se	300F1478	192.168.1	arista	eos	lab	vEOS-lab	4.27.0F	l3switch	N	N	Y	Y	Y	SSH	10	Y
s3xgw2	SITE 3 - Se	34DD1F8A	192.168.1	arista	eos	lab	vEOS-lab	4.27.0F	l3switch	N	N	Y	Y	Y	SSH	10	Y
s3xdsw01	SITE 3 - Se	4237F4D2	192.168.1	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s3xdsw03	SITE 3 - Se	EEC4ECE5	192.168.1	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s3xasw01	SITE 3 - Se	E1EB311F	192.168.1	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y



External - App

Hostname	Site	Serial Number	Login IP	Vendor	Family	Platform	Model	Version	Type	Border	Hardware EOL	AAA	NTP	SNMP	Management Access	CVEs	Backups
d2xfw01	SITE 2 - Ma	e7ad6ce97	192.168.1	juniper	junos	vsrx		21.3R1.9	fw	Y	N	Y	Y	Y	SSH	142	Y
c1xr01	MPLS COR	303ef2beb	192.168.1	juniper	junos	vsrx		21.3R1.9	router	Y	N	Y	Y	Y	SSH	142	Y
c1xr06	MPLS COR	0cc6e818	192.168.1	juniper	junos	vsrx		21.3R1.9	router	N	N	Y	Y	N	SSH	142	Y
c1xr05	MPLS COR	291575d7	192.168.1	juniper	junos	vsrx		21.3R1.9	router	N	N	Y	Y	Y	SSH	142	Y
c1xr04	MPLS COR	5bc8d773	192.168.1	juniper	junos	vsrx		21.3R1.9	router	N	N	Y	Y	N	SSH	142	Y
c1xr03	MPLS COR	eab19849	192.168.1	juniper	junos	vsrx		21.3R1.9	router	N	N	Y	Y	N	SSH	142	Y
d3xr01	SITE 3 - Se	a000008	192.168.1	cisco	ios	vios	IOSv	15.6(2)T	router	N	N	Y	Y	Y	SSH	63	Y
s3xgw1	SITE 3 - Se	300F1478	192.168.1	arista	eos	lab	vEOS-lab	4.27.0F	l3switch	N	N	Y	Y	Y	SSH	10	Y
s3xgw2	SITE 3 - Se	34DD1F8A	192.168.1	arista	eos	lab	vEOS-lab	4.27.0F	l3switch	N	N	Y	Y	Y	SSH	10	Y
s3xdsw01	SITE 3 - Se	4237F4D2	192.168.1	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s3xdsw03	SITE 3 - Se	EEC4ECE5	192.168.1	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y
s3xasw02	SITE 3 - Se	AA758CCE	192.168.1	arista	eos	lab	vEOS-lab	4.27.0F	switch	N	N	Y	Y	Y	SSH	10	Y

IP FABRIC

AUTOMATED NETWORK ASSURANCE PLATFORM

Support & Documentation
https://docs.ipfabric.io

HQ Office Boston
98 North Washington St.
Suite 407
Boston, MA 02114
United States

+1 617-821-3639

IP Fabric UK Ltd.
Gateley Legal,
1 Paternoster Square,
London,
England EC4M 7DX

+420 720 022 997

IP Fabric s.r.o.
Kateřinská 466/40
Praha 2 - Nové Město,
12000
Czech Republic

+420 720 022 997

ipfabric.io