FireScope DDM FAQ

How does DDM discover a business service?

FireScope DDM listens to the URLs being requested by users to discover service endpoints. It can also listen for specific protocols or port traffic, such as LDAP or Oracle applications, to discover infrastructure service endpoints. From either starting point, the solution analyzes aggregate network traffic between virtual and physical servers to follow transactions through their downstream dependencies. Additional virtualization, storage and network discovery scans complete the picture by mapping the virtual and physical dependencies.

Do I have to open ports or enable remote administrative privileges to make it work?

No. A widely raised security concern for many discovery tools is the requirement that RPC ports must be opened and remote administrative privileges granted. With FireScope's approach, this is not necessary.

## What do I need to know about my Services before beginning discovery?

In short, nothing. For many competing solutions, you have to tell the solution where to start with each service (e.g. provide a url or server) and know a significant amount about the application's architecture. FireScope DDM can detect which urls are being requested by users, providing you a list of what we have automatically identified as potential services. Once you select the services you care about discovering, the solution does the rest.

Is this Application Dependency Discovery (ADDM)?

Application dependency discovery is limited to applications and the servers they run on, with little to no visibility into other dependencies that are just as critical such as at the network, storage and virtualization layers. FireScope DDM supports the complete picture, telling you which applications on which vms are depending on another, which physical hosts and data stores those vms are running on, and which routers and switches they are plugged into. This is absolutely critical for effective change impact analysis, as a failed switch can have a larger impact on the business than a failed server.

How are changes tracked? Can FireScope DDM track service dependencies that may be utilized infrequently or after hours, such as scheduled jobs or after hours data processing?

FireScope continually analyzes aggregate network traffic; which servers are communicating with other servers over specific ports or protocols. Once a service baseline has been created, all traffic is compared with this baseline to identify new connections as they happen or when connectivity between two assets has stopped for extended periods of time. As this is running continuously, there's no need to worry about what might me missed with schedule-based discovery.
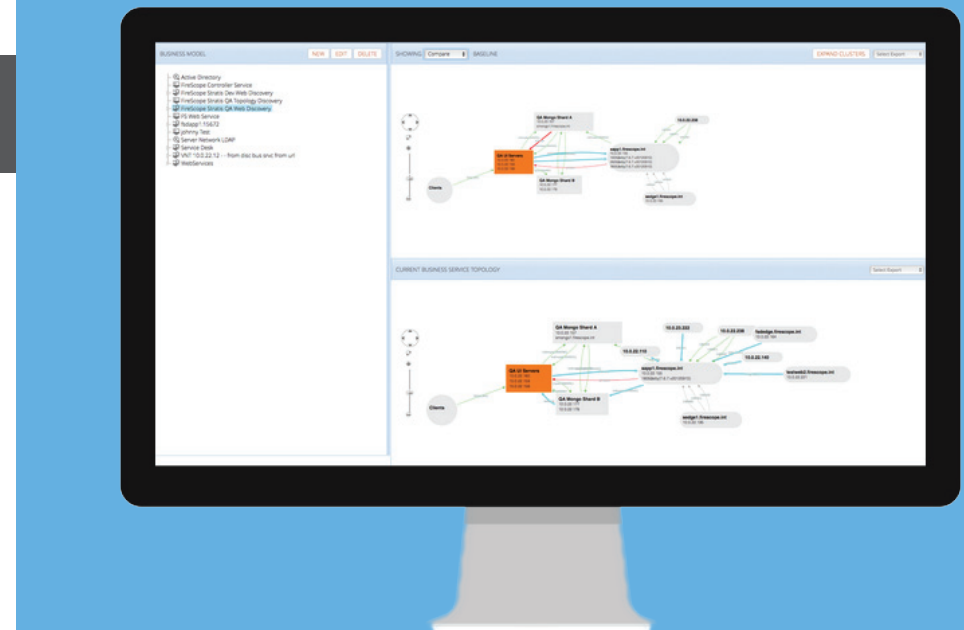
What if I don't/can't have the network team involved in this project?

FireScope DDM includes a host of options to discover service dependencies. If access to network devices is unavailable, the solution can utilize optional sensors running on vms or servers.

What if I don't/can't have the server team involved in this project?

Discovery can still be performed by using port mirroring or NetFlow/sFlow from network devices. Additionally, the network discovery can identify OS, DNS name, running network applications (e.g. Apache, MySQL, Oracle) without the use of an agent. Agents do provide much deeper system configuration details, but are not required or could be rolled out at a later date.

Can FireScope DDM map my custom applications?

Absolutely! At the network level, application architecture becomes moot. Web servers talk to application servers, application servers talk to database servers, regardless of whether they are written in Java, .Net or any other language. Because FireScope is looking at how different systems are communicating with each other, this allows it to discover any service topology, regardless of platform, architecture or whether they are commercial or custom.

Can I leverage existing repositories of configuration data?

Absolutely. Just a few of the more common scenarios are described below:

- Spreadsheets – We often run into customers with considerable data in spreadsheets, which can be imported and mapped to attribute data.

- SCOM, Solarwinds, asset management or monitoring tools – Leveraging FireScope DDM's Enterprise Service Bus and other methods, the solution can directly query these solutions for asset data. This data can then be verified and gaps filled in using FireScope DDM's native discovery capabilities.