imagicle

Attendant Console and Desktop CTI failover using DNS SRV entries

Applies to:

Attendant Console or Desktop CTI clients rel. 2018.6.1 and above, regardless the UC Suite version.

Description:

This article explains how to enable the DNS mechanism that allows the Imagicle Attendant Console to automatically discover the list of the eligible UC Suite servers.

This mechanism allows to manage the scenarios having the Imagicle Attendant servers behind a NAT, that is a common scenario when clients need to reach the Imagicle UC Suite nodes on the Internet, without a VPN.
It also allows to expose on the Internet the Attendant Console Service of several Imagicle nodes using only one public IP address, as described below.

How it works

1. When logging in the Attendant Console client, the end-user specifies an a fully qualified domain name (FQDN) as Attendant server in place of an IP address or LAN hostname. For instance: *acme.com*
2. The client runs a DNS SRV query to discover the hostnames (DNS A entries) and TCP port numbers of the Imagicle servers associated to the invoked FQDN.
3. The DNS server replies the query sending to the client a weighted list of hostnames of available UC Suite servers. The one having the highest priority will be the first node the clients will try to reach.
4. The client process th SRV reply and collects the hostnames-ports list.
5. The client performs a DNS query (A query) to solve the hostname of the first server (the one with highest priority) and tries to connect to it.
6. The DNS server queries its A entries and replies sending the IPv4 of the first Imagicle server.
7. The client tries to connect to the returned IP address and TCP port
8. If failing, the client automatically escalate to the next server, accordingly with the (decreasing) priority of each server in the SRV list and repeats the procedure since point 5.

Single datacenter scenario:

Suppose you want to manage a scenario where:

- users of company "Acme Inc." wants to connect their Attendant Console clients to UC Suite over the Internet;
- the Imagicle servers (primary and backup node) run in the same remote datacenter with only **one public IP address** 123.100.100.100 that is known to the Internet as "acme.com"
- the Imagicle primary server has a private IP address 172.17.20.11 and the backup server has a private IP address 172.17.20.12.

Please find below how to manage such scenario with DNS discovery mechanism:

Unencrypted connection to UC Suite

1) In the datacenter create two NAT rules to expose the internal TCP port 51234 (default port used by Attendant Console) of each Imagicle server into a different port of the same public IP address, for instance:

- 123.100.100.100:28101 ==> 172.17.20.11:51234
- 123.100.100.100:28102 ==> 172.17.20.12:51234

2) In the DNS server used by the Attendant Console client workstations*, create the 2 following DNS SRV rules:

_service._proto.name.	TTL	class	SRV	priority	weight	port	target
_iac._tcp.acme.com.	86400	IN	SRV	10	100	28101	acme.com
_iac._tcp.acme.com.	86400	IN	SRV	8	80	28102	acme.com

* this can be either the internal organization DNS (for clients running inside the organization) or a public DNS server.

These entries will allow the client to discover the weighted list of hostnames and TCP port number of available UC Suite servers. Please notice that the prefix **_iac._tcp** cannot be changed.

3) The end-user runs the Attendant Console client on his workstation and specifies as server hostname: *acme.com*

4) The client will run a SRV query *_iac._tcp.acme.com*, getting from the DNS server the weighted list of Imagicle servers and related TCP ports.
The client tries to connect to the first SRV entry *acme.com* at tcp port 28101 (routed to the internal port 51234 of the first Imagicle server). In order to do that, the client will run a DNS "A" query to its DNS server, to solve the hostname *acme.com*.

5) If failing, it will automatically try to the second SRV entry *acme.com* at tcp port 28102 (routed to the internal port 51234 of the second Imagicle server).

Encrypted connection to UC Suite (2021.Winter.1 release and above)

1) In the datacenter create two NAT rules to expose the internal TCP port 51235 (default port used by Attendant Console) of each Imagicle server into a different port of the same public IP address, for instance:

- 123.100.100.100:28101 ==> 172.17.20.11:51235
- 123.100.100.100:28102 ==> 172.17.20.12:51235

2) In the DNS server used by the Attendant Console client workstations*, create the 2 following DNS SRV rules:

_service._proto.name.	TTL	class	SRV	priority	weight	port	target
_iacsec._tcp.acme.com.	86400	IN	SRV	10	100	28101	acme.com
_iacsec._tcp.acme.com.	86400	IN	SRV	8	80	28102	acme.com

* this can be either the internal organization DNS (for clients running inside the organization) or a public DNS server.

These entries will allow the client to discover the weighted list of hostnames and TCP port number of available UC Suite servers. Please notice that the prefix **_iacsec._tcp** cannot be changed.

3) The end-user runs the Attendant Console client on his workstation and specifies as server hostname: *acme.com*

4) The client will run a SRV query *_iacsec._tcp.acme.com*, getting from the DNS server the weighted list of Imagicle servers and related TCP ports.
The client tries to connect to the first SRV entry *acme.com* at tcp port 28101 (routed to the internal port 51235 of the first Imagicle server). In order to do that, the client will run a DNS "A" query to its DNS server, to solve the hostname *acme.com*.

5) If failing, it will automatically try to the second SRV entry *acme.com* at tcp port 28102 (routed to the internal port 51235 of the second Imagicle server).

Dual datacenter scenario:

Suppose you want to manage a scenario where:

- users of company "Acme Inc." wants to connect their Attendant Console clients to UC Suite over the Internet;

- the Imagicle servers (primary and backup node) run in **2 different remote datacenters**, each one with its own public IP address:
  - Primary DC: 123.100.100.100, known to Internet as *dc1.acme.com*
  - Backup DC: 123.200.100.100, known to Internet as *dc2.acme.com*
- the Imagicle primary server has a private IP address 172.17.20.11 and the backup server has a private IP address 172.18.20.11.

Here how to manage such scenario with DNS discovery mechanism:

1) In each datacenter create a NAT rule to expose the internal TCP port 51234 (or 51235 in case of encrypted connection) of each Imagicle server into a TCP port of the corresponding public IP address, for instance:

- Primary DC: 123.100.100.100:21234 ==> 172.17.20.11:51234 (or 51235 for TLS 1.2)
- Backup DC: 123.200.100.100:21234 ==> 172.18.20.11:51234 (or 51235 for TLS 1.2)

Please, notice that the 2 public TCP ports can be different on the 2 datacenters.

2) In the DNS server used by the Attendant Console client workstations*, create the 2 following DNS SRV rules:

Unencrypted connection:

_service._proto.name.	TTL	class	SRV	priority	weight	port	target
_iac._tcp.acme.com.	86400	IN	SRV	10	100	21234	dc1.acme.com
_iac._tcp.acme.com.	86400	IN	SRV	8	80	21234	dc2.acme.com

Encrypted connection (2021.Winter.1 release and above):

_service._proto.name.	TTL	class	SRV	priority	weight	port	target
_iacsec._tcp.acme.com.	86400	IN	SRV	10	100	21234	dc1.acme.com
_iacsec._tcp.acme.com.	86400	IN	SRV	8	80	21234	dc2.acme.com

* this can be either the internal organization DNS (for clients running inside the organization) or a public DNS server.

These entries will allow the client to discover the weighted list of hostnames and TCP port number of available UC Suite servers. Please notice that the prefix "_iac._tcp" cannot be changed.

3) The end-user runs the Attendant Console client on his workstation and specifies as server hostname: *acme.com*

4) The client will run a SRV query *_iac._tcp.acme.com* (or *_iacsec._tcp.acme.com* for TLS connection), getting from the DNS server the weighted list of Imagicle servers and related TCP ports.
The client tries to connect to the first SRV entry *acme.com* at tcp port 21234 (routed to the internal port 51234 or 51235 of the first Imagicle server). In order to do that, the client will run a DNS "A" query to its DNS server, to solve the hostname *dc1.acme.com*.

5) If failing, it will automatically try to reach the second SRV entry *dc2.acme.com* at tcp port 21234 (routed to the internal port 51234 or 51235 of the second Imagicle server). In order to do that, the client will run a DNS "A" query to its DNS server, to solve the hostname *dc2.acme.com*.

Notes

- if the SRV query run by client fails, the client automatically falls back to the regular login mechanism, trying to connect to the hostname *acme.com* on TCP port 51234 (or 51235 for TLS 1.2). This will involve a DNS "A" query to solve such hostname into a valid IPv4 address.
- if the SRV query gets answered, the private IP addresses of the Imagicle servers are not considered at all by the client.