Factsheet

Test Servers – On-net servers

On-net servers

On-net servers.

Many ISPs want to install test servers inside their network (hence "on-net") to allow them to segregate on-net and off-net performance. SamKnows provides a process to install, update, and monitor the SamKnows applications on these test servers.

Why use on-net?

The overwhelming majority of test servers used by SamKnows customers are off-net, i.e. hosted on the public internet in some fashion. We believe that reporting results to targets off an ISP's own network represents a "real world" experience for end users. However, we do recommend that ISPs install and test against on-net servers as well as off-net.

With both on-net and off-net servers in use, customers can see the difference between the performance of the ISP's own network and that of the public internet. The results can be used to troubleshoot peering links, routing issues, or simply rule out any capacity problems within the ISP's own network.

Requirements

On-net test servers can be either virtual machines or dedicated hardware. For dedicated servers, we strongly recommend that they only operate as test servers and are not used for any unrelated purpose (for example, as a web server or file server).

The minimum specification of a test server is as follows:

- CPU: Quad Core Xeon (2GHz+)
- RAM: 8GB
- Disk: 250GB
- Operation System: CentOS 7.x 64-bit or Redhat Enterprise Linux 7 64-bit
- Connectivity: Gigabit Ethernet connectivity, with 1Gbps upstream (10Gbps preferred)
- IPv4 connectivity

Measurement servers must be able to sustain 1Gbps throughput. Should your project involve testing connections of 500Mbps or faster, we strongly recommend provisioning 10Gbps servers to ensure there is no network contention. Additionally, if you wish to use Redhat Enterprise Linux, you must provide the appropriate Redhat License details for each server.

At a minimum, one publicly routable IPv4 address must be provisioned per server. The test server must not be presented with a NAT'd address. It is preferable for any new test servers to also be provisioned with an IPv6 address at installation time.

DNS records must be configured for each server before installation of SamKnows applications can proceed. We recommend using separate DNS records for IPv4 and IPv6, for example servername-v4.company.com and servername-v6.company.com to make it clear which protocol is being used at any time.

Server Management

SamKnows uses the popular agent-based management system "Puppet" to control and manage our server infrastructure. More details on Puppet can be found in the Methodology section of this documentation.

After the operating system has been installed by the customer, all documentation has been completed, and the installation instructions have been followed, then Puppet will download and install the SamKnows

applications on the server. Puppet will also ensure that the server is kept updated with the latest versions of the SamKnows applications, as well as ensuring that these applications are in a valid running state.

As part of the default on-net server installation, SamKnows will configure monitoring using our Nagios monitoring system. This involves a combination of active tests to the server, for example to ensure that services are listening on the correct port, and passive tests where the server checks its own process status and sends this information back to our monitoring system. We recommend that customers continue to run their own monitoring of the basics of connectivity, power, and network capacity.

The customer is responsible for ensuring the health of the operating system, the server hardware, and the local network.

Provisioning on-net test servers

ISPs are requested to complete an information form for each test server they wish to provision on their network. This will be provided by your SamKnows account manager. This will be used by SamKnows to configure the test server on the management system.

Additionally, if you have any special requirements - for example, the creation of an administration account on the server for your own use, or particular firewall rules that must be implement on the server - then please provide us with this information before installation.

Installation proceeds as follows:

1. Ensure that your test servers meet the minimum specifications.
2. Ensure your servers have the necessary firewall rules permitted.
3. Complete and return the test node installation form.
4. Await confirmation from your SamKnows account manager that the test servers have been configured on the SamKnows back-end.
5. Ensure that the results of the following commands are all correct:

(Please see page 4)

If the output for any of the above check commands do not concur with the expected result, please do not proceed until the issue has been resolved.

6. If the output for all of the above check commands is correct, you may proceed with the following commands to install & configure Puppet, which will then install the SamKnows applications and configure the server:

```
yum -y update && rpm -Uvh
https://yum.puppetlabs.com/puppet5/
puppet5-release-el-7.noarch.rpm

yum -y install puppet-agent

source /etc/profile

echo -e "[main]\nserver =
pm.samknows.com" >>
/etc/puppetlabs/puppet/puppet.conf

puppet agent --waitforcert 15 --test
```

If this process fails to complete successfully, it likely means that your server has not been provisioned on our systems. Please ensure you've followed the steps above, and if so, contact your SamKnows account manager with details of the error message.

Firewalling of on-net test servers

It is preferred that the test servers do not sit behind a hardware firewall or a network Access Control List as firewalling is usually managed on the testserver. If a firewall is used, then care must be taken to ensure it can sustain the throughput required above. Additionally, the following rules must be permitted at a minimum:

Inbound firewall rules required

Note: We recommend opening a range of TCP and UDP ports, 5000-7000, for proper operation of our services. We list the primary ports used by our applications for informative purposes.

(Please see page 4)

Outbound Firewall Rules

Note: These are only required if outbound access is denied by default.

(Please see pages 5-6)

Provisioning on-net test servers

Check command	Expected result	Potential problem if not correct
hostname	servername	Puppet SSL certificate DN will not match
hostname -f	servername.company.com	Puppet SSL certificate DN will not match
grep search /etc/resolv.conf	search company.com	DNS/Reverse DNS lookups may fail
(echo > /dev/tcp/pm.samknows.com/8140) > /dev/null 2>&1 && echo "OK"	OK	Unable to contact the SamKnows Puppet master server(s)

Inbound firewall rules required

Source IP	Protocol	Port	Purpose
77.89.189.17/32	TCP & UDP	ALL	Remote management from the office (Main IP)
89.105.103.193/32	TCP & UDP	ALL	Remote management from the office (Backup IP)
2a00:f18:33::/48	TCP & UDP	ALL	Remote management from the office (IPv6)
83.142.229.43	TCP	22	Remote management from Bastion Server
ALL	TCP	80 & 443	Test HTTP(S) Traffic (nginx)
ALL	TCP & UDP	5000-7000	Test Traffic (SamKnows Applications)
ALL	TCP	8080	Test Traffic (skhttp_server)
ALL	TCP	8443	Test Traffic (skhttp_server)
ALL	UDP	8444	Test Traffic (skhttp_server)
37.220.21.130	TCP	5666	Nagios NRPE Active Monitoring Traffic (lnman1.samknows.com)
2a02:2658:101d::2	TCP	5666	Nagios NRPE Active Monitoring Traffic (lnman1.samknows.com)

Outbound Firewall Rules

Destination IP	Protocol	Port	Purpose
159.69.58.62	TCP	8140	Puppet Management Traffic (eupm1.samknows.com)
2a01:4f8:231:981::2	TCP	8140	Puppet Management Traffic (eupm1.samknows.com)
23.92.20.243	TCP	8140	Puppet Management Traffic (newpm1.samknows.com)
2600:3c03::f03c:91ff:fe24:b483	TCP	8140	Puppet Management Traffic (newpm1.samknows.com)
139.162.246.10	TCP	8140	Puppet Management Traffic (lonpm1.samknows.com)
2a01:7e00::f03c:91ff:fe24:f8e4	TCP	8140	Puppet Management Traffic (lonpm1.samknows.com)
213.52.128.57	TCP	389	LDAP Data Access (ldap1.samknows.com)
2a01:7e00::f03c:91ff:fe1f:3ab	TCP	389	LDAP Data Access (ldap1.samknows.com)
172.104.131.94	TCP	389	LDAP Data Access (ldap2.samknows.com)
2a01:7e01::f03c:91ff:fefb:de27	TCP	389	LDAP Data Access (ldap2.samknows.com)
172.104.139.223	TCP	80 & 443	SamKnows managed repository mirrors (mirror.samknows.com)
2a01:7e01::f03c:91ff:fe80:ea3e	TCP	80 & 443	SamKnows managed repository mirrors (mirror.samknows.com)
23.92.16.59	TCP	80 & 443	SamKnows managed repository mirrors (mirror.samknows.com)
2600:3c03::f03c:91ff:feb6:8902	TCP	80 & 443	SamKnows managed repository mirrors (mirror.samknows.com)
139.162.9.228	TCP	80 & 443	SamKnows managed repository mirrors (mirror.samknows.com)
2400:8901::f03c:91ff:feb6:26e6	TCP	80 & 443	SamKnows managed repository mirrors (mirror.samknows.com)
8.8.8.8	UDP	53	Google DNS
2001:4860:4860::8888	UDP	53	Google DNS
8.8.4.4	UDP	53	Google DNS

Destination IP	Protocol	Port	Purpose
2001:4860:4860::8844	UDP	53	Google DNS
139.162.167.123	UDP	123	NTP Service (ntp.samknows.com)
2a01:7e01::f03c:91ff:fe2a:4c03	UDP	123	NTP Service (ntp.samknows.com)
151.236.222.193	UDP	123	NTP Service (ntp.samknows.com)
2a01:7e00::f03c:91ff:fe78:b004	UDP	123	NTP Service (ntp.samknows.com)
66.228.32.104	UDP	123	NTP Service (ntp.samknows.com)
2600:3c03::f03c:91ff:fe2a:ad71	UDP	123	NTP Service (ntp.samknows.com)
139.162.33.192	UDP	123	NTP Service (ntp.samknows.com)
2400:8901::f03c:91ff:fe2a:4c8a	UDP	123	NTP Service (ntp.samknows.com)
37.220.21.130	TCP	42217	Netstat RRD Traffic Monitoring (lnman1.samknows.com)
2a02:2658:101d::2	TCP	42217	Netstat RRD Traffic Monitoring (lnman1.samknows.com)
37.220.21.130	TCP	5667	Nagios NSCA Passive Host Monitoring (lnman1.samknows.com)
2a02:2658:101d::2	TCP	5667	Nagios NSCA Passive Host Monitoring (lnman1.samknows.com)