5nine Cloud Security
Installation Prerequisites

INSTALLATION PREREQUISITES

5nine Cloud Security is installed into the Hyper-V environment to protect virtual machines from attacks, unauthorized traffic and malware (agentless antivirus scans, agentless real-time traffic screening and agent-based active protection of virtual machines) and to shield the environment on the Hyper-V virtual switch level (virtual firewall protection).

The product should be installed into the properly prepared environment that meets the following general prerequisites (please refer to the product QSG to find the detailed system requirements):

1. All networks/connections in the environment should be set up and work in a stable manner.
2. All servers, hosts and clusters (whatever applicable) that are involved into the installation must be fully set and work in a stable manner. Windows updates/patches should be done prior to the installation, if applicable. Ensure there are no issues related to those updates.
3. User(s) shall be created in AD (for domain environments) and meet system requirements: management service user should have administrative privileges on SQL server (sysadmin) if Windows auth is used, host user should have local administrative privileges and "Logon as a service" privilege. If the same account is used for both management and host services, then it should have all required permissions for both.
4. Management server (in most cases – either dedicated or shared VM with other service like SCVMM management service) should be set and accessible and have all required TCP ports opened (TCP ports 8183, 8534, 8789, 8790 and 8939).
5. All hosts that are supposed to be protected by 5nine Cloud Security should have necessary ports opened as per System requirements (TCP ports 8533 and 8788).
6. Hosts must be ready for reboot to install and set 5nine filtering extension and properly set in maintenance mode or paused-drained (applicable to cluster nodes). Not all environments tolerate reboot actions smoothly on Hypervisors, and this is not caused by 5nine and shall not be considered as a 5nine-dragged issue. Alerts/warnings may appear if SCVMM is used to manage the environment, until all reboots/refreshes of the hosts are done and it can take significant time and repetitive attempts to fix the issues in SCVMM. There is no way to avoid it.
7. SQL data source must be available, accessible and set up. If TCP port is different than default one (1433) then connection string must be specified in format:
   `sql-server\instance, port`.
8. All Hyper-V virtual switches must be set on all protected hosts.
9. If a logical SC VMM switch(es) are used, a compliance plugin will be installed as a part of the product to ensure compliant state on logical switches. If there are hosts that are not supposed to have 5nine Cloud Security installed, but using the same logical switch with those who are, the idle driver will be installed onto those for compliance. It does not affect hosts' functioning, but is necessary to maintain compliant state of logical switch. Alternate way is to have separate logical switches for those hosts that are protected by 5nine and those that are not. This depends on customer's approved networking/SCVMM structure and does not depend on 5nine.
10. If Azure Pack is used and 5nine Cloud Security installs as a part of admin and tenant portals (extension), a principal user that 5nine Cloud Security backend service is connected with the main application (service user) must be added to Azure pack admins.
11. Any changes during/after installation of 5nine Cloud Security result in involving additional resources/maintenance and WILL BE SUBJECT FOR AN EXTRA CHARGE FROM 5NINE ON PER HOUR BASIS. These changes include, but are not limited by, the following possible actions:
    - Any networking changes (MAC, IP addressing scheme, VLANs etc).
    - DNS/AD changes including users or users' privileges, specifically those that are used for 5nine services or function.
    - SQL data source changes: migrating SQL server to another cluster, removing/changing privileges of the database user, change in the database/instance name, network address etc. that will make database vFirewall inaccessible and, therefore, management service failure.
    - SCVMM configuration changes, including manual enabling/disabling extensions, specifically 5nine filtering extension, or their order and enabling/disabling 5nine compliance plugin on hosts/clusters groups.
    - Hyper-V configuration changes, including manual enabling/disabling extensions, specifically 5nine filtering extension or their order.
    - Uninstallation of 5nine components/request to do so on hosts/servers, which have been already set up.
    - Azure Pack configuration changes (if applicable).
12. Visual C++ Redistributable for Visual Studio 2012 x86 should be installed on Management Server.
13. Cloud Security WAP plugin requires to allow PUT/DELETE operations in IIS configuration.

CONTACT US

Sales:

Phone US: + 1 561 898 1100
Phone EU: + 44 20 7048 2021
Email: sales@5nine.com
Fax: + 1 732 203 1665

Technical Support:

Phone US/Canada Toll Free: + 1 877 275 5232
Phone: + 1 561 898 1100 Ext.3
Email: techsupport@5nine.com
Fax: + 1 732 203 1665

01/21/2017

Microsoft Partner
Gold Datacenter