

Cisco Stealthwatch Host Group Automation Service



Benefits

- Tackle dynamic server behavior that consistently changes IP addresses. Host Group Automation is necessary to dynamically configure Cisco Stealthwatch to apply policies to these automated, dynamic, host groups.
- Proactively manage integrations with third-party threat feeds. Constantly changing IP addresses need updating in real time so you can mitigate erroneous alarms when communicating to malicious hosts.
- When your system interacts with third-party application servers with dynamic IP addresses, you need Host Group Automation Services to maintain their proper configuration.
- Optimize Cisco® Stealthwatch performance and reduce operational overhead to lower operating costs while reducing errors and superfluous alerts and job notifications.
- Automate host-group updating, which keeps Stealthwatch operating at maximum efficiency for optimal protection against wide-ranging threats.

Automate Host Group Creation for Granular Visibility

The Stealthwatch Host Group Automation Service gives customers a logical means of categorizing network assets for improved visibility and control. Use this service to:

- Optimize Stealthwatch system performance and automatically manage your specific address IP pool.
- Reduce excess consumption of your team's resources by decreasing overall cost to operate Stealthwatch and by decreasing false positive alarms. Security teams can have a high degree of confidence that when an alarm fires it warrants investigation.
- Automate host group synchronization. When you do you can maintain accurate groupings, so you're assured that users are assigned correctly for compliance with corporate policy.

Being able to segment your network and users by logical work groups, geographies, organizations, job functions, and many other ways allows forward-thinking organizations to closely monitor network traffic to each individual group. For instance, grouping critical corporate assets can enable Stealthwatch to monitor traffic to and from those assets and sound an alarm on any anomalous activity. Automating your host groups provides a regular and repeatable method to report back any anomalies occurring within your host group environment.

Automate Host Groups for Precise Stealthwatch Customization

Cisco Stealthwatch Host Group Automation Service periodically updates Stealthwatch host groups with data from your authoritative IP address management system. The service is delivered as a set of customizable tools and scripts that our professional services engineers will tailor to your unique environment. Keeping Stealthwatch host groups synchronized with your network infrastructure can reduce overhead and contribute to optimized Stealthwatch operation.

Automating host groups is an ideal way to keep Stealthwatch operating at its best, and that your network and security personnel receive timely, error-free data. All of this goes to reducing operational overhead and to preventing false-positive alarms that consume the security team's time. It permits them to receive more accurate alarming so there is a high degree of confidence that alarms are meaningful events.

Next Steps

To learn more about Cisco Security Services and how our Stealthwatch deployment services can benefit your business, contact your local account representative or authorized Cisco reseller. For more information on how Cisco can help you protect your organization from today's dynamic threats, visit www.cisco.com/go/services/security.