Secant

WHITE PAPER

SMTP NOTIFICATIONS

Publication No. 102

Version: November 28, 2011

SMTP Notifications

INTRODUCTION

Simple Mail Transport Protocol (SMTP) notifications are one of the most common built in notification methods for applications and devices. Many applications and devices support sending SMTP notifications directly from the application/device to an SMTP server. This approach to notifications has a number of limitations but is still considered worthwhile for many devices and applications particularly when other more sophisticated monitoring methods are not already being used. For example, one limitation to monitoring backups with this approach is that if the backup services are not working at all, then the service can't send an alert to notify someone that the backups are not working. Thus, the recommended approach to monitoring and alerting involves using a combination of strategies including more sophisticated monitoring solutions. Secant offers several more sophisticated monitoring and alerting solutions.

BACKGROUND

When using SMTP notifications the SMTP server must be configured to allow relaying (no authentication) from the source server/device. When using SMTP notifications keep in mind that SMTP itself is not a secure protocol and thus using authenticated SMTP is not recommended because the password will be sent in cleartext (unless a transport security protocol is also being used).

In many existing environments email alerts are configured to send notifications to only one individual's email address. This is not the preferred approach for several reasons. Sending notifications to an individual address results in limited visibility. If the individual being notified is not available to respond to the alert, then the next responsible person does not have visibility of the notification. If the individual being notified leaves the organization, then all applications and devices configured for SMTP notifications need to be reconfigured.

It is critical that the SMTP notifications configured in an environment do not generate too many messages too frequently, particularly for minor issues, because this leads to notifications simply being ignored eventually. It's important to find the right balance with notifications. If a certain device or application sends too many alerts, it should be adjusted accordingly. In some cases SMTP filtering software may be able to be applied to filter unwanted alerts based on rules if the source application/device does not offer granular configuration of alerts. It's also critical that the right people are being notified. Periodically reviewing and testing the notification process is important to maintaining a healthy environment.

APPLICATIONS/DEVICES

The following types of applications/devices should be considered for configuration of SMTP notifications.

- Server-based Applications
  - Backup applications
  - Network/systems monitoring applications
  - Security-related applications
  - Anti-virus applications
  - Patch management applications
  - VMware vCenter Server
- Devices
  - Managed power devices including UPS units with network cards, managed power strips, etc.
  - Environment sensor devices
  - SAN equipment
  - NAS devices
  - Appliance devices that provide a critical service

GUIDELINES

Applications/devices that are configured for SMTP notifications should be configured per the following guidelines.

- SMTP notifications should be sent to a distribution group address rather than any individual mailbox addresses. Each organization should start with a minimum of one distribution group with the address **alerts@domain.com**. Each distribution group's member list should include a shared account for centralized and historical reference. This group should be populated with the shared mailbox and a list of the individuals that are responsible for maintaining the technology infrastructure. Additional distribution groups should be added to provide the appropriate amount of visibility where needed. Each distribution group is then populated with an appropriate list of individuals that should have visibility of the alert type. For example, environment sensor alerts should be sent not only to system administrators but also to facilities managers.

- Notifications should only be sent for warnings/errors and other important/critical events. Informational events generally do not require notifications. For example, backup job notifications should only occur when a backup job fails.
- For critical alerts like power and environment alerts, alerts should be sent to both internal and external recipients to ensure greater visibility.
- If using a hosted email solution, refer to documentation or technical support regarding SMTP relaying. In many cases, the hosted solution will not allow for unauthenticated email relaying or will not allow for SMTP email relaying at all. If this is the case, an alternative SMTP alerting service may be required to support SMTP notifications.
- A DNS CNAME record should be created named **smtp** within the internal DNS zone and should resolve to the FQDN of the preferred SMTP server.
- The SMTP server address, sender email address, and the recipient email address(es) should be configured as specified below.

MAIL SERVER CONFIGURATION

The following is a summary of the configuration changes required on the organization's mail server(s).

1. Allow email relaying from the appropriate IP address ranges that include the servers and devices sending SMTP notifications.
2. Create the appropriate distribution groups that will receive SMTP notifications.
3. Configure optional settings on each distribution group.
4. Populate the distribution groups with the appropriate recipients.

Exchange Server 2010 Configuration Details

Relay Configuration - Configure the relay settings.

1. From the Exchange Management Console open **Server Configuration** > **Hub Transport**. Open the Properties of the **Relay** Receive Connector (created under the Exchange Server 2010 standard).
2. Open the **Network** tab. Under the **Receive mail from remote servers that have these IP addresses** section add the appropriate IP address ranges (Example: 10.6.0.0/16, etc.). Click **OK**.
3. Note: Exchange Server should already be configured to allow relayed messages to be delivered to external recipients if the server was configured by Secant. If that is not the case, then refer to the Exchange Server 2010 standard or contact Secant for additional assistance.

Mail Contacts - Create and configure contacts for all external recipient email addresses including text messaging addresses and pager addresses.

1. From the Exchange Management Console open **Recipient Configuration** > **Mail Contact**.
2. Create a new contact for each recipient address and specify an appropriate alias and external e-mail address. (Example alias: JohnDoe.Text, e-mail address: 2695555555@vtext.com)
3. Open the Properties of the contact and select **Hide from Exchange address lists**.
4. Open the **E-mail Addresses** tab. Deselect **Automatically update e-mail addresses based on e-mail address policy**. Remove any SMTP addresses besides the address previously specified. Click **OK**.
5. Repeat for all additional external recipient addresses required.

Distribution Groups - Create and configure distribution groups.

1. From the Exchange Management Console open **Recipient Configuration** > **Distribution Group**.
2. Create a new distribution group with name and alias **alerts**.
3. Open the Properties of the distribution group. Open the **Advanced** tab and select H**ide group from Exchange address lists**.
4. Open the **Mail Flow Settings** tab and open the **Message Delivery Restrictions** Properties. Deselect the **Require that all senders are authenticated** option. Click **OK**.
5. Open the **Members** tab. Add the **Administrator** recipient (or an alternate shared account if desired). Add the appropriate recipients. Click **OK**. Click **OK**.
6. Repeat for all additional distribution groups using the name and alias format **alerts-type**, etc.

APPLICATION/DEVICE CONFIGURATION

SMTP Server Address

For all applications and devices, the SMTP server address should be specified as an IP address rather than a DNS name to avoid the dependency on DNS name resolution. This helps ensure applications and devices are configured consistently and notifications are as reliable as possible in the event of a service outage.

Sender Email Address

Sender email addresses should be configured to describe the source of the notification. Specifying the source in this manner helps clarify the source of notifications and also allows for email rules to be configured based on different types of notifications if needed. The sender email address should also not be a valid destination email address. This helps mitigate the possibility of creating an email loop.

For devices, the hostname or device name should be used as part of the sender email address. For example, a NAS device in the environment named NAS1 should use nas1@*domain.com* as the sender email address. For applications, the application name should be used as part of the sender email address. The following are recommended sender email addresses for specific applications.

Application	Sender Email Address
CA ARCserve Backup	arcserve@*domain.com*
HP SIM	hpsim@*domain.com*
HP MSA	hpmsa@*domain.com*
Sophos Endpoint Security	sophos@*domain.com*
Symantec Backup Exec	backupexec@*domain.com*
Veeam Backup & Replication	veeam@*domain.com*
VMWare vCenter Server	vcenter@*domain.com*
Microsoft WSUS	wsus@*domain.com*

Recipient Email Address(es)

Recipient email addresses should be specified as a distribution group address rather than any individual mailbox address. Each distribution group's member list should include a shared account for centralized and historical reference. The shared mailbox used for centralized reference could be the domain "Administrator" mailbox in Active Directory environments.

Each organization should start with a minimum of one distribution group with the address alerts@*domain.com*. This group should be populated with the shared mailbox and a list of the individuals that are responsible for maintaining the technology infrastructure.

Additional distribution groups should be added when more granularity is needed. Each distribution group is then populated with an appropriate list of individuals that should have visibility of the alert type. For example, environment sensor alerts should be sent not only to system administrators but also to facilities managers.

The following are recommended distribution groups that should be used anywhere that further granularity is needed.

Description	Distribution Group / Recipient Address
Backup applications	alerts-backup@*domain.com*
Facility environment (sensors)	alerts-environment@*domain.com*
Facility power	alerts-power@*domain.com*
Server systems	alerts-systems@*domain.com*
Storage infrastructure	alerts-storage@*domain.com*
Network devices	alerts-network@*domain.com*
Critical alerts requiring broader visibility	alerts-critical@*domain.com*

If different sites are managed by different technology staff, then a site identifier should be inserted into the address as well. For example, a company that has a New York site and a Detroit site would use distribution groups like alerts-newyork@*domain.com*, alerts-detroit@*domain.com*, alerts-newyork-backup@*domain.com*, etc.

Secant Managed Services

In cases where Secant holds a managed contract on a service/device, then SMTP alerting to Secant may be required. Secant will configure the appropriate settings where necessary.

800.875.4222 | SECANTCORP.COM