Vertiv™ Environet™ Alert

Installer/Admin Guide

The information contained in this document is subject to change without notice and may not be suitable for all applications. While every precaution has been taken to ensure the accuracy and completeness of this document, Vertiv assumes no responsibility and disclaims all liability for damages resulting from use of this information or for any errors or omissions. Refer to other local practices or building codes as applicable for the correct methods, tools, and materials to be used in performing procedures not specifically described in this document.

Technical Support Site

If you encounter any installation or operational issues with your product, check the pertinent section of this manual to see if the issue can be resolved by following outlined procedures.
Visit https://www.Vertiv.com/en-us/support/ for additional assistance.

TABLE OF CONTENTS

1 OVERVIEW

This document detaills the steps necessary to set up the Vertiv™ Environet™ Alert server.

This page intentionally left blank

2 INSTALLATION REQUIREMENTS

Before installing the Vertiv™ Environet™ Alert application, the following requirements must be met.

2.1 Permissions

Administrator permissions are required to install Vertiv Environet Alert files and Microsoft Windows services.

2.2 Server Requirements

REQUIREMENT	MINIMUM	RECOMMENDED
Operating System	Windows 10 (64-bit) Windows Server 2016 Windows Server 2019	Windows Server 2019
CPU (Intel or AMD)	4 CPU 2.0 GHz or Higher	(Intel or AMD) ≥6 CPU ≥2.2 GHz or Higher
RAM	8 GB	≥16 GB
Disk Space	100 GB	≥300 GB
Disk I/O	15 MBps read/write speed	≥200 MBps read/write speed
Network	10/100 MBps	≥1 GBps

2.3 Special Files and Directories

The following directories will be created by the installer and must not be altered.

- *C:\Environet*
  The default installation target, unless overridden.

IMPORTANT! The default Install Location (*C:\Environet*) will be specified in the instructions for the rest of this document. Substitute the actual Install Location if not using the default.

- *C:\snapshot*
  Used by the Environet Analytics service.
- *C:\Users\<User Account Running Installer>\Niagara<version>*
  Used by the Niagara application.
- *C:\Users\<User Account Running Installer>\AppData\Local\Temp*
  Setup Log <YYYY-MM-DD> #<Sequence Number>.txt
  - Installer logs contain details useful in troubleshooting installation problems.
  - The logs might be under a numeric subdirectory below Temp.

2.4 Network Port Requirements

The following dedicated network ports are used by the Vertiv™ Environet™ Alert.

2.4.1 Web Server

Windows Service Name: *EnvironetWeb*

Process Name: *httpd.exe*

PORT	PROTOCOL	PURPOSE
80	TCP	HTTP communication between web browser and application server
443	TCP	HTTPS communication between web browser and application server (disabled by default)

2.4.2 Application Server

Windows Service Name: *Environet Service*

Process Name: *environet-service.exe*

PORT	PROTOCOL	PURPOSE
8005	TCP	Used to start and shutdown the application
8009	TCP	Allows communication with a web connector using the AJP protocol

2.4.3 Niagara

Windows Service Name: *Niagara*

Process Name: *plat.exe*

Niagara Platform Server

Process Name: *niagarad.exe*

PORT	PROTOCOL	PURPOSE
3011	TCP	Niagara platform server local daemon port
5011	TCP	Niagara platform server local daemon SSL port

Niagara Station

Process Name: *station.exe*

PORT	PROTOCOL	PURPOSE
162	UDP	SNMP trap recipient port that SNMP devices can connect to
1911	TCP, UDP	Fox Service port that allows remote connections to a station
4911	TCP	Fox Service port that allows secure remote connections to a station (disabled by default)
5701	TCP, UDP	Hazelcast in memory shared cache between Environet Alert and Niagara
8443	TCP	HTTPS communications between Environet Alert and Niagara (disabled by default)
9000	TCP	HTTP communications between Environet Alert and Niagara

2.4.4 Database

Windows Service Name: EnvironetDB

Process Name: mariadbd.exe

PORT	PROTOCOL	PURPOSE
3306	TCP	Listening Port

2.4.5 MySQL

Microsoft Windows Service Name: *MySQLDB*

Process Name: *mysqld.exe*

PORT	PROTOCOL	PURPOSE
3306	TCP	Listening Port

2.4.6 Analytics Server

Windows Service Name: *Environet Analytics*

Process Name: *nssm.exe*

No port requirements.

Highcharts Export Server

Process Name: *highcharts-export-server-win.exe*

PORT	PROTOCOL	PURPOSE
7801	TCP	HTTP communications between Environet Alert and Analytics Server

PhantomJS

Process Name: *phantomjs.exe*

No port requirements.

2.5 Firewall Requirements

The following network ports must be open on the server firewall to allow network communication in and out of the server.

PORT	PROTOCOL	PURPOSE
80	TCP	Inbound HTTP requests from client computers to login and use Vertiv™ Environet™ Alert
161	UDP	Outbound SNMP calls from the server to monitored devices for getting point data
162	UDP	Inbound SNMP trap requests from monitored devices Outbound SNMP calls from the server to monitored devices for setting traps
443	TCP	Inbound HTTPS requests from client computers to login and use Environet Alert

2.6 Browser Requirements

The following web browsers are tested and supported with the current version of Vertiv™ Environet™ Alert. Other web browsers or versions of the browsers listed below may work, but are not necessarily tested and supported.

- Microsoft Edge (87.0.664.55)
- Firefox (83.0)
- Chrome (87.0.4280.88)

3 VERTIV™ ENVIRONET™ ALERT SETUP

WARNING! Do not install Vertiv Environet Alert on a server that is already running a newer version of Vertiv Environet Alert on it. Doing so will damage the existing installation.

3.1 Vertiv Environet Alert Installation Steps

IMPORTANT! If upgrading from Vertiv Environet Alert1.0.0, a different set of steps must be followed here: Vertiv™ Environet™ Alert 1.0.0 Upgrade Steps on page 23

1. Ensure that all Installation Requirements on page 3 steps above have been completed before continuing.
2. Obtain the latest Environet Alert installer zip file from authorized personnel
3. Unzip the Vertiv Environet Alert installer zip file.
4. Navigate to the extracted Environet-<version> folder.

NOTE: Be careful not to navigate into the zip file itself.

5. Launch the *Environet_setup_x64.exe* executable.
6. The Select Setup Language screen displays a list of the supported installer languages.

NOTE: Setup will determine the default language to use by checking the user's "UI language". The "UI language" is the language used in Windows' own dialogs. If Windows is configured with a multilingual user interface (MUI), then the default will be the currently selected UI language.

7. Accept the License Agreement and click *Next*.
8. Select an Install Location (default is *C:\Environet*) and click *Next*.

WARNING! If upgrading an existing Environet Alert installation, the Install Location must be kept the same so that all data from the previous install can be correctly migrated to the new install.

IMPORTANT! The default Install Location (*C:\Environet*) will be specified in the instructions for the rest of this document. Substitute the actual Install Location if not using the default.

9. Follow the instructions on the *Niagara License Files* page and click *Next*.

   These are the licensing instructions displayed:

   Obtaining Niagara License:

   a. Capture the Host Id (shown below) and License Key.

      <Host Id>

IMPORTANT! If you do not have a Host Id this means there is a space in the file path to the installer. Please exact the installation file to a location with no spaces in the path and rerun the installer.

b. On a machine with Internet, navigate to:

https://axlicensing.tridium.com/license/request

c. Complete the form including your email address.

d. If this computer has internet access, click *Next* and the license files will be automatically installed. Otherwise, complete the offline licensing instructions below before continuing with the install..

Offline Licensing Instructions:

a. The necessary licenses will be emailed to you after completing the Obtaining Niagara License steps.

b. Unzip the file with the Host Id that ends with (N4). Example: *Win-A3FE-1A02-4DEE-89B8(N4).zip*

c. Copy the license files (*DAC.license and Geist.license)* to the following directory on this computer: *<Installer Unzip Folder's "licenses" directory>*

10. On the Ready to Install page, click *Install* to start the installation.
11. On the Finished Installing page, click *Finish* to close the installer.

NOTE: At the end of the installation process, the installer will verify whether the Niagara license files where installed and valid. If they were not:

- **The Environet Windows Services will not be installed, and the application will not be started.**
- **The final screen of the installation will tell the user to rerun the installer and to verify that the instructions on the Niagara License Files screen are followed correctly.**

3.2 Post Installation Steps

3.2.1 Verify that Vertiv™ Environet™ Alert is Running

1. On a client computer, open a supported browser and navigate to the server's host name or IP address. Initially, the server only listens for HTTP requests (not HTTPS).

NOTE: If the browser connection times out, it may be that the server processes have not fully started yet. Wait a few minutes and try again. If after several minutes a connection cannot be made from the browser, see the troubleshooting section for help.

2. If this is a new installation the quickstart page will appear that provides a workflow for setting the initial admin account password and other settings. For upgraded systems, the default board should be present upon login.
3. If this is not a new install and the admin account password has already been set, the login page should appear. Sign in with your user credentials to start using the application

3.3 Configure HTTPS - Optional

Initially, Vertiv Environet Alert is set up to use HTTP only. To configure HTTPS communication between browsers and the server, follow the steps below.

3.3.1 Enabling HTTPS

To configure HTTPS communication between browsers and the server, login to the application and go to the System Admin (gear symbol) > System Settings > Security page.

When enabling HTTPS, you can choose between using the provided self-signed SSL certificate (created by the Environet Alert installer) or upload your own SSL certificate.

If using the provided self-signed SSL certificate, select that option on the Security page (mentioned above) and click SAVE, then skip to Configure Browser to Use Self-Signed Certificates on page 12. Otherwise, proceed to the next section.

3.3.2 User-Provided SSL Certificate Requirements

Take note of the following requirements for user-provided SSL certificates.

1. SSL certificate files must be in PEM format (i.e. Base64 ASCII encoded with plain text BEGIN and END headers and footers). Example of the private key file in PEM format:

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDC1akMRgokejYU
uX2ot3dWSnsWlkGRcMfdwZKK7YSvl6a0wyCxyhDa3gG38CBuU5a9zYStKxhyBWZN
[omitted for brevity]
FH9u2LbozzGa9XCqil4fKtb+6edhUkjzajGf4V1iDYfd9FBoW1L/7FzXIt+OEzqq
xsydXXOlXZFkOgEC5NchvS37
-----END PRIVATE KEY-----
```

2. Private Key: File name must end with .key extension.
3. Public Certificate: File name must end with .crt extension.
4. Intermediate Chain Certificate: File name must end with .crt extension.

NOTE: If the public certificate file contains the entire chain of certificates, this file can be omitted.

5. HINT: When downloading the SSL certificate from a Certificate Authority, choose the Apache web server format.

3.3.3 Generate a Public/Private Key Pair

The following steps will create a public/private key pair and store them in a new keystore. The application server will be configured in a subsequent step to use this keystore file.

1. Open a Microsoft Windows Command Prompt.
2. Change directory to *C:\Environet*.
3. Copy/paste or type the following command and click *Enter*.

```
jre\bin\keytool -genkeypair -alias environet -keyalg RSA -keysize 2048 -deststoretype pkcs12 -keystore
app\conf\environet.keystore
```

4. Type answers to each of the prompts and hit *Enter* after each.
   - Enter keystore password: *changeit* (Type this password)
   - Re-enter new password: *changeit*
   - What is your first and last name? (Must specify domain name)

NOTE: This must be set to the domain name used by the browser to reach the server. If a Trusted SSL Certificate will be used, this must be a fully qualified domain name (e.g., *example.com* or *subdomain.example.com*).

   - The remaining questions pertain to the customer's organization and are informational.
   - After the questions have been answered, you'll be shown your answers and asked if they are correct. If correct, type *y* or *yes* and click *Enter*. If any answer is incorrect, click *Enter* and you'll be asked the questions again. Click *Enter* when asked a question and the answer is already correct.

5. A keystore file will now exist at:

<Environet Alert Install Directory>\app\conf\environet.keystore

6. Make an external backup of your keystore file for safe keeping.

3.3.4 Trusted Certificate Setup

Trusted SSL Certificates are recommended for production environments. For test environments, a Self-signed SSL Certificate can be used. If using a Self-signed SSL Certificate, skip to Configure the Application Server for HTTPS on page 12.

IMPORTANT! If upgrading from Environet Alert 1.1.0 and a trusted SSL certificate was installed, a different set of steps can be followed here if you want to migrate the old certificate: Environet Alert 1.1.0 SSL Certificate Migration on page 21.

Generate a Certificate Signing Request:

Follow the steps below to generate a private key and certificate signing request (CSR). The private key is used to generate the CSR and the CSR is used to order an SSL certificate (public certificate). The public certificate is used to encrypt messages that only the private key can decrypt.

1. Open a Windows command prompt.
2. Change directory to somewhere outside of the Environet Alert install directory to create the private key and CSR.
3. Copy/paste or type the following command and hit Enter.

```
"C:\Environet\web\bin\openssl.exe" req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr -config
"C:\Environet\web\conf\openssl.cnf"
```

4. Type answers to each of the prompts and hit Enter after each one. Note the following special field requirements:
   a. The Common Name field must be set to the fully qualified domain name (e.g. example.com).
   b. A challenge password must not be set. Just hit Enter on this prompt.
5. The following files will now exist in your current directory.
   - server.csr
   - server.key

IMPORTANT! Make an external backup of the files above for safe keeping.

Order a Trusted SSL Certificate:

NOTE: The following instructions are for DigiCert. If the customer has another preferred certificate authority, the instructions may differ slightly but will generally apply.

1. Go to the DigiCert (formerly Symantec) website: https://www.digicert.com/compare-and-buy-ssl-certificates/
2. Choose the SSL certificate product that fits the customer's needs.
3. On the Select Product step:
   a. Pick the pricing options.
   b. Under the Name(s) to Secure section, click the checkbox next to (Optional) I would like to provide my CSR and auto-fill names now.
   c. On the dialog window that pops up, select *Apache* in the *Select Server Software* box.

d. In the Upload a CSR or Paste one below box, copy and paste in the entire contents of the server.csr file you created in the previous steps.
e. Click *Continue* and the dialog window will close.
f. Click *Continue*.

4. On the Organization Information page:
   a. Some of the organization details will be populated from the CSR file you copied and pasted in the previous step.
   b. Fill in the remaining form fields.
   c. Click *Continue*.
5. On the Payment page, enter payment details and complete the purchase.

Upload the Trusted SSL Certificate:

1. Once the certificate authority creates the certificate, login to your DigiCert account and download the intermediate certificate file (DigiCert.crt) and your public certificate file (your_domain_name.crt).
2. Login to Environet Alert and go to the *System Admin* (gear symbol) > *System Settings* > *Security page*
3. Make sure the check box next to *Enabled* is checked.
4. Under Manage Certificates select *Upload Certificate*.
5. Under Private Key, load the private key file (e.g. server.key).
6. Under Public Certificate, load the public certificate file (e.g. your_domain_name.crt).
7. Under Intermediate Chain Certificate, load the intermediate certificate file (e.g. DigiCert.crt).

NOTE: If the public certificate file contains the entire chain of certificates, this file can be omitted.

8. Click *SAVE* to upload the certificate files.
9. The Web Server will be restarted automatically so that the uploaded certificate files can be activated. If a failure occurs, the Web Server will be reverted to its previous state.

This completes trusted SSL certificate setup.

Install the Trusted SSL Certificate

1. Once the certificate authority creates the certificate, download the certification file package. This should be a file with an extension of *.p7b*
2. Rename the file to your site name. For example, if your site name is example.com, the file should be called *example.com.p7b*
3. Put the renamed certificate package file in the following directory:
   Environet\app\conf
4. Open a Windows Command Prompt.
5. Change directory to *C:\Environet*.
6. Type the following command (replacing *your_site_name* with your actual site name) and click *Enter*.

   *niagara\jre\bin\keytool -import -trustcacerts -alias environet -file app\conf**your_site_name**.p7b -keystore app\conf\environet.keystore*
7. If prompted for the keystore password, type: *changeit*.
8. You should get a confirmation that the *Certificate reply was installed in keystore*.
9. If you are prompted to trust the certificate, type *y* or *yes*.

3.3.5 Configure the Application Server for HTTPS

Now that the keystore has been created and populated with the public/private key pair (and trusted SSL Certificate, if chosen), the Application Server can be configured to use the keystore.

To configure HTTPS,

1. Open the following file in a text editor:

   Environet\app\conf\server.xml
2. Locate the section that starts with *<Connector port="443"...*
   a. Initially this section will be commented out. Uncomment the section by removing the surrounding tags:

      <!-- and -->
   b. Add in the following keystore attributes between *sslProtocol="TLS" and />*:

      keyAlias="environet" keystoreFile="conf/environet.keystore"

Redirect HTTP to HTTPS

1. Open the following file in a text editor:

   Environet\app\conf\web.xml
2. Add the following lines just before the closing *</web-app>* line at the bottom of the file:

```
<security-constraint>

   <web-resource-collection>
      <web-resource-name>Protected Context</web-resource-name>
      <url-pattern>/*</url-pattern>
   </web-resource-collection>
   <user-data-constraint>
      <transport-guarantee>CONFIDENTIAL</transport-guarantee>
   </user-data-constraint>
</security-constraint>
```

IMPORTANT! The Application Server must be restarted for these settings to take effect. Restart the Application Server by opening the Windows Services panel and restarting the service named *Environet Service*.

3.3.6 Configure Browser to Use Self-Signed Certificates

A security exception must be added to the web browser if using a Self-signed SSL Certificate.

Browse to the server using: *https://<domain name>*

If you see a page indicating that the site is not secure or that your connection is not private:

1. Look for an Advanced button and click it.
2. Then scroll down until you see a link or button that says something like "details", "accept" or "proceed" and click it.
3. You should now see the Environet Alert Login page.

This page intentionally left blank

4 BACKUP AND RESTORE VERTIV™ ENVIRONET™ ALERT

Vertiv Environet Alert should be backed up regularly as part of a larger disaster recovery process. Backup and restore functions are available through the Environet Alert UI.

This page intentionally left blank

5 UNINSTALLING VERTIV™ ENVIRONET™ ALERT

5.1 Uninstalling Geist Environet Alert

To completely uninstall the Vertiv Environet Alert application and all associated data,

1. In Windows *File Explorer*, navigate to *C:\Environet*.
2. Launch the uninstaller: *unins000.exe*.
3. Follow the prompts.

NOTE: If after the uninstall completes, a dialog box says that some files could not be removed, this indicates that the Niagara station took longer than expected to shut down. In this case, restart the server and then manually remove the *C:\Environet*.

This page intentionally left blank

6 TROUBLESHOOTING

6.1 Finding the Vertiv™ Environet™ Alert Version Number

The Vertiv Environet Alert version number is stored *C:\Environet\version.txt*.

6.2 Resolving Installation Errors

The most common reason for general errors is overlooking or incorrectly following a step in this document. The easiest way to resolve such issues is to start from the beginning and perform each step carefully.

If the error still exists, contact technical support. The installer log files will be needed by technical support to troubleshoot the error. See Special Files and Directories on page 3 for the location of the installer logs.

6.3 Port Conflicts

If a port in the Network Port Requirements on page 4 is in use by another application, determine which application is listening on that port using the *Windows Resource Monitor*.

To start Windows *Resource Monitor* do one of the following:

- In the Windows *Search field*, type *resmon* and hit *Enter*.
- Or, launch Windows *Task Manager* and on the *Performance* tab, click *Open Resource Monitor*.

In *Resource Monitor*:

1. Click on the *Network* tab.
2. Expand the *Listening Ports* section.
3. Sort by the *Port* column.
4. Locate the application by finding the row containing the conflict port number.

6.4 Connection Issues

If after Vertiv™ Environet™ Alert installation or server reboot, the browser can't connect to the server, try the following steps:

1. Ensure the server is running.
2. Ensure the host name or IP address is correct.
3. Ensure your computer is on the same network as the server.
4. Ensure the server firewall is configured correctly per the Firewall Requirements section.

NOTE: If you can't connect from a remote browser, try connecting from a browser running on the server to determine if the problem is a firewall issue.

5. Ensure the Windows Services are all in a Running state. See the Network Port Requirements section for the service names.

IMPORTANT! On a slower server, the Niagara service may not be able to start up within the time allotted by Windows. If that happens, you can start it manually from the Services application. You can then change the Startup Type to Automatic (Delayed Start) which will tell Windows to wait to start the service until Windows is fully initialized (on server reboot).

6. If you turned HTTPS off in Environet Alert, you'll need to re-type the URL to the server with the http:// prefix.

IMPORTANT! If you turn HTTPS off, the browser will likely have issues since it doesn't like the session cookie changing from being flagged as secure to non-secure. This can cause odd behavior such as being redirected to the login page over and over. To solve this problem, clear the browser cache and restart the browser.

7 ENVIRONET ALERT 1.1.0 SSL CERTIFICATE MIGRATION

Beginning with Environet Alert 1.2.0, SSL Certificate Management is done through the application UI. Before that, SSL was configured manually in the application directory.

If upgrading from a 1.1.0 install that had a trusted SSL certificate configured, you can migrate the SSL certificate files to the new format and then upload them into the application UI on the new version of Environet Alert.

1. Upgrade to the latest version of Environet Alert. The keystore file from Environet Alert 1.1.0 will be preserved so that the SSL certificate files can be exported from it. After a successful upgrade, proceed to the next step.
2. Open a Windows command prompt.
3. Change directory to somewhere outside of the Environet Alert install directory to export the SSL certificate files to.
4. Copy/paste or type the following command and hit Enter. Then type in the keystore password (changeit) and hit Enter.

```
"C:\Environet\web\bin\openssl.exe" pkcs12 -in "C:\Environet\app\conf\environet.keystore" -nodes -nocerts -out server.key
```

5. Copy/paste or type the following command and hit Enter. Then type in the keystore password (changeit) and hit Enter.

```
"C:\Environet\web\bin\openssl.exe" pkcs12 -in "C:\Environet\app\conf\environet.keystore" -nokeys -out server.crt
```

6. The following files will now exist in your current directory.
   - server.crt
     Public certificate file that should contain the entire certificate chain.
   - server.key
     Private key file.

IMPORTANT! Make an external backup of the files above for safe keeping.

7. Now you can login to the application and upload the cert files. See the Upload the Trusted SSL Certificate subsection under the Trusted Certificate Setup on page 10 section for details.

This page intentionally left blank

8 VERTIV™ ENVIRONET™ ALERT 1.0.0 UPGRADE STEPS

Since the release of Environet Alert 1.0.0, significant changes were made to the architecture which make it impossible to automatically upgrade to newer versions.

IMPORTANT! Follow the steps in the sections below in the order shown to perform the upgrade from 1.0.0 to 1.1.0. Do not attempt to upgrade from 1.0.0 to any other version.

8.1 Backup and Uninstall Vertiv Environet Alert1.0.0

Backing up the Vertiv Environet Alert 1.0.0 data involves backing up the database, Niagara station, and file store.

WARNING! Changes to Vertiv Environet Alert should not be made during the backup process. This prevents inconsistencies between the database, Niagara station, and file store backups. Follow the steps in the sections below in the order shown to ensure consistency between the backups.

8.1.1 Backup Vertiv Environet Alert 1.0.0

Backup Location

Determine a central location to store backups for the database, Niagara station, and file store. This location will be referred to as ***backup_location*** in the steps below.

WARNING! The backup location must be outside the Environet Alert install path.

Database Backup

To perform a full backup of the Vertiv Environet Alert database, follow these steps:

1. Open a Windows Command Prompt.
2. Change directory to ***backup location***.
3. Type the following command (replacing ***DATE-TIME*** with the current date and time. e.g. 20200319-1438) and hit *Enter*. ***Only use numbers and dash for the DATE-TIME. Do not use any spaces in the file name***.

   *"C:\MySQL\MySQL Server 8.0\bin\mysqldump" -u root -p environet > environet-**DATE-TIME**.sql*

NOTE: If MySQL was installed to a different drive, the drive letter may need to be changed from *C:* to the actual drive letter in the command above.

4. You will be prompted for the password. Enter the password you created for the root database user (when MySQL was installed) and hit *Enter*.

NOTE: Depending on the size of the database, the backup could take several minutes. When the Command Prompt is displayed again, the backup has completed.

5. Verify that the database was backed up correctly.
   a. Verify that the files appears with the name you gave it above and ends with *.sql*
   b. Verify that the file size is not *zero* bytes.

IMPORTANT! If any errors were displayed during backup or if the verification above failed, rerun the database backup setups, ensuring the steps are followed correctly. If it still fails, contact technical support.

Niagara Station Backup

1. In Windows *File Explorer*, navigate to:

   C:\Environet\niagara\bin
2. Launch the Vertiv Supervisor *(wb.exe)* application.
3. In the left nav bar, expand the *My Host* tree node to see its immediate child nodes. If you do not see a *Station (Environet Base Station)*, then right-click on *My Host* and click *Open Station*.
   a. On the *Open Station* dialog window, select *Station Connection* from the *Type* drop-down menu and click *OK*.
   b. Enter the following credentials and click *OK*.

      Username: *admin*

      Password: *(this was configured as part of the post-install steps for Environet Alert 1.0.0)*
4. In the left navigation bar, expand the *Station (Environet Base Station)* tree node, navigate to *Config>Services*.
5. Right-click on *BackupService* and choose *Views>Property Sheet*.
6. Ensure the properties are set as follows then click *Save*:
   a. Enabled: *true*
   b. Exclude Files: **.lock*
   c. Exclude Directories: *<none>*
   d. Offline Exclude Files: **.lock*
   e. Offline Exclude Directories: *<none>*
7. Double-click on *BackupService*.
8. Click on the *Backup* button at the bottom of the right frame.
9. On the *File Chooser* window, navigate to the ***backup_location*** using *My File System* in the left nav.
10. Click the *Save* button.
11. The *File Chooser* window will close, and you should see a new entry in the *Backups* table in the right frame.
12. Close Vertiv Supervisor by clicking the *X* in the upper-right corner.

File Store Backup

1. In Windows *File Explorer*, navigate to *C:\Environet*
2. Copy the *filestore* directory.
3. Navigate to your ***backup_location*** and paste the folder there.
4. Rename the pasted *filestore* folder to include a date and time (e.g. *filestore-20200319-1438*)

8.1.2 Unistalling Vertiv™ Environet™ Alert 1.0.0

To completely uninstall the Vertiv Environet Alert 1.0.0 application and all associated data, follow these steps:

Vertiv Environet Alert 1.0.0 Uninstall Steps

1. In Windows *File Explorer*, navigate to *C:\Environet*
2. Launch the unistaller: *unins000.exe*.

3. Follow the prompts.

NOTE: It may appear that the uninstall is stuck, but it is waiting for various Windows Services to stop. This can take several minutes.

4. Verify that *C:\Environet* has been removed.

IMPORTANT! If after the uninstall completes, *C:\Environet* still exists, this indicates that a process still holds a lock on one or more files. In this case, restart the server and then manually remove *C:\Environet*.

MySQL Uninstall Steps

To completely uninstall MySQL from the server, follow these steps:

1. To remove MySQL and all data stored in the database:
   a. Go to *Start > MySQL > MySQL Installer - Community*.
2. If presented with *Optional MySQL Installer Upgrade Available*, click *No*.
3. On the *MySQL Installer* window, click *Remove...* on the right side of the page.
4. On the *Select Products to Remove page*:
   a. Select *all* products.
   b. Click *Next*.
5. On the *Remove Server* page:
   a. Ensure the box next to *Remove* the *data directory* is checked.
   b. Click *Next*.
6. On the *Remove Selected Products* page:
   a. You should see server and workbench products listed.
   b. Click *Execute*.
   c. After product removal has completed. You should see *Status of Complete* for both products.
   d. Ensure the boxes next to the following are checked:
      i. *Yes, unistall MySQL Installer*
      ii. *Yes, reboot when done*
   e. Click *Finish*.
7. A dialog will popup asking to restart your system. Click *OK*.
8. Manually delete any leftover files (this is important to prevent issues during installation if MySQL is reinstalled). To do so, delete the MySQL directories if they exist in any of these places:
   - *C:\MySQL*
   - *C:\Program Files\MySQL*
   - *C:\Program Files (x86)\MySQL*
   - *C:\ProgramData\MSQL (ProgramData is hidden folder)*

8.2 Install Vertiv™ Environet™ Alert Alert 1.1.0

Perform the steps in Vertiv™ Environet™ Alert Setup on page 7 to install the Vertiv Environet Alert 1.1.0.

8.3 Restore Backed Up Data to Environet Alert 1.1.0

The next sections will guide you through restoring the database, Niagara station, and file store.

WARNING!

1. **The restoration process will replace all existing data in Environet Alert.**
2. **Ensure that the backup files to be used for restore are from Environet Alert 1.0.0.**
3. **Follow the steps in the sections below in the order shown to ensure a consistent restoration.**

8.3.1 Shutdown Environet Alert Application

Before restoring the data, the Environet Alert application must be stopped to ensure no data is modified, file locks are removed, and the in-memory cache is replaced.

1. Launch the Windows *Services* application.
2. Right-click on the following services (in the following order) and click *Stop*:
    a. *Environet Service*
    b. *Niagara*
3. The Status column for the above services should be empty (i.e., no longer be *Running*).
4. Launch Windows *Task Manager* and click on the *Details* tab to view the process list.
5. Sort the process list by *Name* and look for the following processes:
    a. *environet-service.exe*
    b. niagarad.exe
    c. station.exe
6. After the processes above have disappeared from the process list, you can continue with the restore process. This could take several minutes depending on the size of the station.

8.3.2 Database Restore

To restore the Vertiv™ Environet™ Alert database from a backup file, follow these steps:

1. The database backup file must first be modified to be compatible with the new database server.
    a. In Windows *File Explorer*, navigate to your ***backup_location***.
    b. Find the database backup file (i.e. environet-***DATE-TIME***.sql **where** ***DATE-TIME*** represents the date/time you specified) that you created in the backup steps above.
    c. Before modifying the backup file, make a copy of it in case something goes wrong.
        i. Copy the database backup file and paste into the same directory. The copy will automatically have " - *Copy*" added to the name.
        ii. The copy will contain the original database backup data in case something goes wrong.
    d. Launch *Notepad*.
    e. Go to *File>Open…*, then navigate to the ***backup_location*** and change the drop-down menu on the bottom right from *Text Documents* to *All Files*. Then select the backup file (i.e. environet-***DATE-TIME***.sql).
    f. Click on *Edit>Replace…*, enter the following parameters, and click *Replace All*:

        Find what: *utf8mb4_0900_ai_ci*

        Replace with: *utf8mb4_unicode_ci*

    g. Save the file and exit *Notepad*.
2. Open a Windows Command Prompt.
3. Change directory to your ***backup_location***.
4. Type the following command (replacing ***DATE-TIME*** with the date/time you specified in the file name) and hit *Enter*.

    ```
    C:\Environet\db\bin\mysql -u root -p environet < environet-DATE-TIME.sql
    ```

5. You will be prompted for the password.
    Enter the password *environet1* and hit *Enter*.

NOTE: If any errors occur, contact technical support.

NOTE: Depending on the size of the file, the restore could take several minutes. When the Command Prompt is displayed again, and if no errors were encountered, the database is now restored, and you can proceed to the next step. If any errors were displayed, contact technical support.

8.3.3 Niagara Station Restore

1. In Windows File Explorer, navigate to:

    C:\Environet\niagara\bin
2. Launch the Niagara console *(console.exe)* application.
3. In the console application, change directory your ***backup_location***.
4. Run the following command (replacing ***DATE-TIME*** with the date/time in the file name) to migrate the station to the new Niagara version and output to the stations folder:

    ```
    n4mig -o backup_Environet_Base_Station_DATE-TIME.dist -t:c
    C:\Environet\niagara\daemonhome\stations\Environet_Base_Station
    ```

NOTE: Depending on the size of the file, the station migration could take several minutes. When the Command Prompt is displayed again, you should see the words "Completed Migration" near the bottom of the output.

IMPORTANT! If any errors were displayed, capture the console output and contact technical support with that information before proceeding with the next steps.

5. Exit out of the console application by typing *exit* and hitting *Enter*.

8.3.4 File Store Restore

1. In Windows File Explorer, navigate to your ***backup_location***.
2. Copy the *filestore-**DATE-TIME*** directory to be restored (***DATE-TIME*** is a placeholder for the date/time in the actual folder name).
3. Navigate to *C:\Environet*.
4. Remove the old *filestore* directory.
5. Paste the *filestore-**DATE-TIME*** directory in *C:\Environet*.
6. Rename the pasted *filestore-**DATE-TIME*** directory to *filestore*.

8.3.5 Start Environet Alert Application

After restoring the data, the Environet Alert application must be started back up.

1. Launch the Windows Services application.
2. Right-click on the following services (in the given order) and click *Start*:
   a. *Niagara*
   b. *Environet Service*
3. The *Status* column for the above services should be *Running*.

NOTE: It may take several minutes for the application to come back up.

8.4 Verify Upgrade

1. Verify that Environet Alert is running by following the steps in Verify that Vertiv™ Environet™ Alert is Running on page 8
2. Verify that your Boards, Groups, Equipment, Reports, Alarms, Histories look correct.
3. If any data appears to be missing or corrupt, contact technical support with the relevant details.

Vertiv.com | Vertiv Headquarters, 1050 Dearborn Drive, Columbus, OH, 43085, USA

SL-09007_REV2_01-21