AWS EFT Usage Instructions

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT v7 and later

DISCUSSION

You don't need to have your own infrastructure and server hardware to deploy an enterprise-level managed file transfer (MFT) server. Instead, you can build and scale EFT in the cloud using Amazon EC2 instances in Amazon Web Services (AWS). This article describes how to get started with this type of cloud-based deployment.

Prerequisites

To run EFT on AWS, you need the following:

- An Amazon AWS account
- A license key if you plan to use EFT past the 30-day evaluation period

Licensing

The EFT image includes a fully functional, preconfigured copy of EFT that will operate without a license for 30 days. After the evaluation period is over you will need to provide a license key in order to continue using the software. The license key is not restricted to an EFT running in the cloud, but is restricted based on the number of servers licensed. For more information on licensing please refer to EFT's End User License Agreement or contact Globalscape sales.

Obtaining the Image

If you haven't done so already, log on to your AWS account and visit the AWS marketplace and search for "Globalscape". Locate Globalscape EFT server offering and select it, following Amazon's One-Click setup process to create and launch an instance of that image. We recommend you select the default options, but do require that RDP be available (so you can login and perform administrative tasks in EFT), and HTTPS (so you can login as a user and upload/download files to EFT using the web client application).

AWS EFT Usage Instructions

Quick Test

If you used the One-Click setup, then an instance of EFT image is both created and launched in a single step. Give the instance a few minutes so that the machine password will be available and so that EFT can finish configuring itself. After 5 minutes or so do the following:

1. In your web browser, type https://<this_instance_ip_address> . If the connection fails then you should either try again in a few minutes, or double check the Security Group (EC2 Dashboard > Network & Security > Security Groups) assigned to this image, ensuring that HTTPS is added and that your IP address is allowed.
2. If you get a security warning in your browser, select the option to proceed. The browser is simply alerting you to the fact that the SSL certificate used by the site is unsigned (self-signed), and thus untrusted. More on SSL certificates below.
3. On the login page, type in the user account credentials as follows:

   Username: User

   Password: <The_Instance_ID>

4. The instance ID is shown in your EC2 Dashboard for this instance. This is a unique value that was generated when you created the instance from the EFT image. When the instance was launched for the first time, a script was run that generated this test account and retrieved the instance ID, and thus dynamically setting the password. Even though it is unique, we recommend you change the test user account credentials at the earliest opportunity, as both the testuser and EFT administrator account are assigned the instance ID as their respective password.
5. If the login fails, then please contact our support team or RDP in and use EFT's administration interface to manually configure EFT (in the rare case that the script failed)
6. If login succeeds then EFT's Web Transfer Client (WTC) interface will load, and you will be able to transfer files from/to the EFT server, using the intuitive controls provided. The web client represents a tiny sub-set of EFT's functionalities, and in fact isn't necessary if purely automated transactions will be conducted between systems; however, it is a good way to test that the server is running and is useful when person-to-business or person-to-person transfers are also needed.

EFT Administration

AWS EFT Usage Instructions

To take full advantage of EFT you will need to configure it beyond the preconfigured settings. This includes security settings that meet your internal policies, user provisioning, and creation of workflows that depend on triggers such as files being uploaded, files deposited into a "hot" folder, or recurring scheduled events.

1. Establish a remote desktop session to the running instance (if you are reading this then you are likely already connected). Instructions for RDPing and for obtaining the uniquely generated administrator password for this instance are available on Amazon's website.
2. Once logged in to Windows, click on the EFT administrator shortcut locate on the desktop.
3. When the administrator interface appears, you will be asked which server you want to administer. Select Local server and click OK or next.
4. On the next screen, enter your administrator credentials as follows:

   Admin username: Administrator

   Password: <The_Instance_ID>

5. As with the test user account, the admin account also uses the instance ID as the password. We highly recommend that you change the default password, which can be done from the Administrators dialog (tab), displayed when the Server icon is selected in the upper left corner of the administrator interface.
6. You can now configure the server to your liking, which could include things like adding more users to the default Site, creating a new Site (which is like a virtual host that can have its own unique authentication mechanism, protocol, and security settings), changing default settings, or start experimenting with EFT's automation capabilities, which includes the Event Rules and Advanced Workflows features.
7. The complete documentation on EFT administration can be found on our support website.

AWS EFT Usage Instructions

log4cplus.logger.Cloud.AWS=OFF

Next steps

1. First, don't forget to change your EFT administrator and User account passwords in EFT.
2. If you haven't done so already, you should change your Windows Administrator password.
3. Enable additional protocols in EFT (FTPS, SFTP, AS2) as desired, remembering to update your AWS Security Group values as necessary, so that connections can be established from outside of AWS.
4. EFT was preconfigured with Amazon's SMTP server values; however, you will need your SES (http://docs.aws.amazon.com/ses/latest/DeveloperGuide/Welcome.html) SMTP credentials if you want to leverage EFT's email notification capabilities.
5. If you plan on using this EFT in a production environment, and assuming it's been licensed, then do not forget to replace the test SSL certificate that was generated for EFT with a CA signed certificate. Please note that the test certificate private key password was also the instance ID.
6. If you plan on using this EFT in a production environment, then you will probably want to audit to a separate SQL server, rather than the provided SQL Server Express 2014 edition. In order to both change EFT's audit settings AND create the schema on the target SQL server you will need to re-run the installer, choose Modify, and then follow the instructions when prompted to set EFT auditing and reporting. Alternatively, you can contact our support team for assistance.
7. The instance will default to the UTC time zone. Instructions for changing the time zone here: http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/windows-set-time.html
8. You can join this instance to your AWS domain within your Virtual Private Cloud (VPC) by following these instructions: http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2-join-aws-domain.html Note that EFT supports an authentication mode that lets you point to an AD controller, using native Windows calls (for full impersonation), using LDAP, if authentication alone is needed (with EFT controlling authorization).

Do not hesitate to contact our sales team if you would like to see a demo or have specific questions you would like answered.

See also https://kb.globalscape.com/KnowledgebaseArticle11229.aspx.

GlobalSCAPE Knowledge Base

AWS EFT Usage Instructions

https://kb.globalscape.com/Knowledgebase/11237/AWS-EFT-Usage-Instructions-