opentext™

OpenText Software Delivery Management Secure Deployment and Configuration Guidelines

1 Welcome to this Guide

Welcome to the OpenText Software Delivery Management Secure Deployment and Configuration Guide. This document is designed to help you deploy and manage OpenText Software Delivery Management instances in a secure manner in the modern enterprise. Our objective is to help you make well-informed decisions about the various capabilities and features that OpenText Software Delivery Management provides to meet modern enterprise security needs.

Security requirements for the enterprise are constantly evolving and this guide should be viewed as OpenText's best effort to meet those stringent requirements. If there are additional security requirements that are not covered by this guide, please open a support case with the OpenText support team to document them and we will include them in future editions of this guide.

2 Introduction

OpenText Software Delivery Management stores sensitive data with encryption AES-256 algorithm with shared secret symmetric key. This key is used for both encryption and decryption. The keys are generated automatically.

To ease installation Software Delivery Management is not fully hardened by the automatic install process. It is important to follow this guide in order to better secure the installation. This document describes how to secure the server.

3 Common Security Considerations

- Thoroughly review the trust boundaries between OpenText Software Delivery Management components (OpenText Software Delivery Management servers, exchange servers, database servers, LDAP servers, and other integrating servers) to minimize the number of communication opportunities between the components.

- When there is a firewall between any OpenText Software Delivery Management deployment components, ensure the proper configuration according to the vendor recommendation.

- Run periodic trusted root Certificate Authority certificate updates on your clients and servers to ensure that the publisher certificates used in digital code signing are trusted.

- Always change the default passwords provided by vendors (for example DB schema password, key store password etc.)

- If OpenText Software Delivery Management is deployed with other web applications on the same domain, OpenText Software Delivery Management data from browser storage will be available to these other web applications.

4 Software Delivery Management Practice

The OpenText Software Delivery Management application server installation supports a secure connection via TLS.

OpenText encourages the customer to always configure a secure connection which is not done automatically. By not implementing this configuration you may exposing the system to increased security risks. You understand and agree to assume all associated risks and hold OpenText harmless for the same. It remains at all times the Customer's sole responsibility to assess its own regulatory and business requirements. OpenText does not represent or warrant that its products comply with any specific legal or regulatory standards applicable to Customer in conducting Customer's business.

Ensure OpenText Software Delivery Management installed only on supported environments, for details see System Requirements.

In addition, it is expected and recommended that the front end server (load balancer or reverse proxy) will be configured to require secure connection. The demonstration web applications and demo projects are not necessarily secure and should not be deployed on production servers.

5 Installation Security

Read System Requirements for supported web and application servers.

5.1 Make sure RPM has a proper digital signature.

This procedure is necessary for the digital signature verification of the RPM package, to make sure the file has not been tampered with, and the code was indeed signed by the trusted entity (OpenText).

All of the OpenText Software Delivery Management packages generated by OpenText are signed using GnuPG. RPM has a built-in mechanism to verify both the checksum of the downloaded file and the authenticity of the file as it was signed.

Verifying the rpm package before installing it is highly recommended to make sure that the file was not corrupted during download or tampered with. To verify the file perform the following steps:

1. Install the public key

- Download the following file:
  - https://admhelp.microfocus.com/documents/octane/security/Micro_Focus_Group_Limited%20RSA-2048-3-RPM.zip
- Unzip the file
- Import the public key using the following command:
  ```
  rpm --import public_key_Micro_Focus_Group_Limited_RSA-2048-3-RPM.ASC
  ```

2. Verify the RPM package

Verify the authenticity of the file by running:

```
rpm --checksig <name of rpm package>
```

The response should look like this:

```
<name of RPM package>: rsa sha1 (md5) pgp md5 OK
```

3. Troubleshooting

If you receive an unexpected result:

- The file may have been corrupted on download. Download the package again.
- The signature may not have imported correctly. Try to import the key again and make sure that RPM does not report any errors.
- Check the key installed by running:
  ```
  rpm -q gpg-pubkey --qf '%{NAME}-%{VERSION}-%{RELEASE}\t%{SUMMARY}\n'
  ```

  You should see:
  ```
  gpg-pubkey-9ce117a7-5b69da19    gpg(OpenText Group Limited RSA-2048-3-RPM)
  ```
  among the results.

5.2 Install with the proper user.

To install OpenText Software Delivery Management, use a user that has the following access:

Folder	Permission	Default value
Installation folder	Read, write, execute	linux: /opt/octane windows: c:\octane
Log folder	Read, write	linux: /opt/octane/log windows: c:\octane\log

For Linux:

OpenText Software Delivery Management should be installed with a user that can run the **rpm** command and can install a new service. It is recommended not to use **root** user.

For Software Delivery Management:

OpenText Software Delivery Management should be installed with a user that can run the **exe** command and can install a new service.

5.3 Modify permissions of the OpenText Software Delivery Management user.

Make sure the user that runs the OpenText Software Delivery Management service has only the following folder permissions:

Folder	Permission	Default value
Installation folder	Read	linux: /opt/octane windows: c:\octane
Log folder	Read, write	linux: /opt/octane/log windows: c:\octane\log
Repository folder	Read, write	linux: /opt/octane/repo windows: c:\octane\repo

For Linux:

By default, OpenText Software Delivery Management installation on Linux creates a new group called **octane**, and a user in this group called **octane.** OpenText Software Delivery Management also supports the option to use predefined users and groups using the OCTANE_GROUP and OCTANE_USER variables. See the Linux Installation Guide for details.

5.4 Network permission of OpenText Software Delivery Management server user.

Make sure that the OpenText Software Delivery Management user has network access to the following:

- Shared repository folder (if exists on network)
- Database server
- Elasticsearch server

Target	Default ports
Files repository	n/a
Oracle	TCP 1521 (Oracle SQL*Net Listener)
MSSQL	TCP 1433
Elasticsearch	9200 (HTTP interface) 9300 (Binary interface)

It is recommended to change default ports to other ports.

5.5 Project file repository and installation folder.

Make sure that only the OpenText Software Delivery Management user has read and write access to the repository. No other user should have read or write access to the files repository or the installation folder.

OpenText encourages the Customer to use anti-virus, which is not provided by OpenText. By not running anti-virus on uploaded files you may exposing the system to increased security risks. You understand and agree to assume all associated risks and hold OpenText harmless for the same. It remains at all times the Customer’s sole responsibility to assess its own regulatory and business requirements. OpenText does not represent or warrant that its products comply with any specific legal or regulatory standards applicable to Customer in conducting Customer's business.

Full Disk Encryption (FDE)

Full disk encryption (FDE) is supported for all system components, including database, server, repository server, and client machines. Implementation of FDE can have an impact on system performance. For details, contact the vendor providing encryption.

6 Secure configuration and deployment

6.1 HTTPS in production

In production systems, only secure configuration (HTTPS) is supported. In staging, we do not recommend using non-secure configuration.

Using HTTPS requires a pair of a public certificate and a private key. We recommend that the public certificate will be signed by a known CA (Certificate Authority).

The most common public certificate files have *.crt or *.cer extensions. Note that these files store only the public certificate, and these alone are not enough to configure the HTTPS connection.

There are several formats that can store both a public certificate and a private key: JKS, PKSC12, PFX, DER, PEM. (The files in these formats can be converted to one another.) OpenText Software Delivery Management supports either JKS or PKSC12 (*.p12 file extension) format.

6.2 Securing access to LDAP

For secure access to LDAP read SetUp LDAP

6.3 SSL termination

OpenText Software Delivery Management supporт SSL termination on Jetty. See “Securing access to OpenText Software Delivery Management Application Server (Jetty)” below.

OpenText Software Delivery Management also supports external SSL termination. See KM03286744 – “Wrong redirection in SSL offloading in OpenText Software Delivery Management ”.

6.4 Protect the network by closing ports.

Close all ports that are not needed.

By leaving ports open, you are disabling or bypassing security features, thereby exposing the system to increased security risks. By using this option, you understand and agree to assume all associated risks and hold OpenText harmless for the same.

See list of needed ports in above section “Network permission of OpenText Software Delivery Management server user”.

On the OpenText Software Delivery Management server node open only SSL port and SSH port.

6.5 Securing access to OpenText Software Delivery Management Application Server (Jetty)

Note: OpenText Software Delivery Management supports secure connections using TLS 1.2. In addition, TLS 1.3 is supported in OpenText Software Delivery Management versions 16.0.400 and later.

To configure secure connection to the OpenText Software Delivery Management server:

1. Obtain a server certificate in java keystore (.jks) or PKCS12 format, issued to the fully qualified domain name of the OpenText Software Delivery Management server. If you are not sure how to do this, see How to create JKS to enable SSL.
2. Enter the keystore details in your **octane.conf** file, in the **server-binding** section. For details, refer to the How to enable secure connection (SSL/HTTPS).
3. Restart the service: *Service octane restart*

Distributed Denial of Service attack protection

Consider implementing DDoS attack protection on servers hosting OpenText Software Delivery Management web client, only in cases where your OpenText Software Delivery Management web client is exposed to the public internet. In most production environments, deploying OpenText Software Delivery Management web client on the public internet are rare, so carefully consider if this best practice applies to your specific deployment.

A few DDoS attacks such as Slowloris may be mitigated by implementing third-party protections such as the following:

- mod_reqtimeout – applicable if using Apache HTTP server
- mod_qos – applicable if using Apache HTTP server
- F5BigIPLTM iRule – applicable if using F5 hardware load balancer in front of the OpenText Software Delivery Management web client

Note: Due to the nature of these attacks, it is not possible to implement application-specific fixes or enhancements to prevent these types of attacks.

For more information, refer to the following:

- https://en.wikipedia.org/wiki/Denial-of-service_attack
- https://httpd.apache.org/docs/trunk/mod/mod_reqtimeout.html
- https://bz.apache.org/bugzilla/show_bug.cgi?id=54263

Note:

OpenText Software Delivery Management includes a built-in DoS protection filter based on Jetty DoSFilter. This DoS filter is capable of partially mitigating flood-based DoS attacks. By default, the OpenText Software Delivery Management server's DoS protection filter is disabled because the filter may have negative impact on system performance.

We recommend that you use a dedicated product which provides DoS protection, as described above.

However, if you want to enable the OpenText Software Delivery Management built-in DoS protection filter, see Appendix B.

6.6 Redirect non-secure access to secure port (http to https)

In the OpenText Software Delivery Management Installation Guide, refer to the section "Advanced OpenText Software Delivery Management server configuration" for details on how to redirect http request to https.

Establishing trust to Certificate Authority

This procedure is necessary when OpenText Software Delivery Management connects to any other server over a secure channel, such as database server, LDAP server, etc.

For details refer to the section "Configure secure database access" in the OpenText Software Delivery Management Installation Guide.

SSL Offloading

SSL offloading configuration defines external node as the SSL termination node. The protocol from the given node to Jetty is HTTP. OpenText Software Delivery Management still needs to send links to clients with HTTPS in their protocol.

For details on how to configure external proxy server as SSL termination server, see KM03286744.

In addition, see "Advanced OpenText Software Delivery Management server configuration" in the OpenText Software Delivery Management Installation Guide.

SSL Enforcement

In OpenText Software Delivery Management 15.1.90, we added reinforcement for on-premises environments working with HTTPS. If OpenText Software Delivery Management is defined in **octane.conf > app-url** as using HTTPS protocol, users trying to access OpenText Software Delivery Management with HTTP will now be blocked.

To enable HTTP when SSL is defined in OpenText Software Delivery Management:

In some cases, you may want to use HTTP protocol to access OpenText Software Delivery Management despite defining your environment as secure (for example for an internal tool). In this case, add the parameter **allow-http-requests-if-ssl-enabled** to the **octane.conf > server-binding** section, and define its value as **true**. This enables usage of HTTP in a secure environment.

To enable HTTP when SSL is defined via reverse proxy:

If you are working with SSL offloading, the **X-Forwarded-Proto** header must be defined in a reverse proxy. If you have not defined this header, you will no longer be able to connect to OpenText Software Delivery Management via a load balancer. To resolve this you can either define the header as described in KM03286744, or choose one of the following options:

- Add the **octane.conf** parameter **allow-http-requests-if-ssl-enabled** as described above.
- Edit the value of the site parameter **ENABLE_SECURED_CONNECTION_VALIDATION** to **false** to disable the new HTTPS filter when using SSL offloading.

6.7 Configuration steps

From http://secureitnetworks.net/index.php/2015/08/21/how-to-insert-http-header-x-forwarded-proto-for-ssl-traffic-of-f5-ltm:

1. Log in to F5 LTM GUI.
2. Open Local Traffic menu.
3. Choose Profiles > Services > HTTP.
4. Click “Create.”
5. Enter the new profile’s name.
6. Under the new profile make sure that Parent Profile is “http.” Select “Custom” on the right hand side.
7. In “Request Header Erase” insert X-Forwarded-Proto.
8. In “Request Header Insert” enter X-Forwarded-Proto: https
9. Click “Finished” to save the profile.
10. Go to VIP for SSL traffic (listening on port 443) and add the profile created under “HTTP Profile.”

For an example of defining a new HTTP profile, see Appendix A.

7 Securing access to the database

7.1 Securing access

OpenText Software Delivery Management creates two schemas in first server start: one for site administration and one for the first shared space. To do this it gets a username and password for a strong enough user.

OpenText Software Delivery Management installation supports using predefined schemas instead of creating them during OpenText Software Delivery Management server start. In this case, the "SiteAction" in setup.xml should be "FILL_EXISTING". See installation guide for more information.

OpenText Software Delivery Management supports SSL connection to database. See "Configure secure database access" in the OpenText Software Delivery Management Installation Guide.

7.2 Transparent Data Encryption (TDE)

OpenText Software Delivery Management supports Transparent Data Encryption (TDE) for Microsoft SQL and Oracle databases. Implementation of TDE can have an impact on system performance. For details, contact the vendor providing encryption.

OpenText Software Delivery Management Encryption

OpenText Software Delivery Management crypto capability is used to encrypt sensitive system data and store it encrypted in the database. Examples of sensitive data include credentials to the database server OpenText Software Delivery Management uses, credentials to the LDAP and SMTP servers with which OpenText Software Delivery Management integrates, and credentials for CI CD servers and other integration components that contain user data.

OpenText Software Delivery Management crypto implementation uses the following security configuration:

LW crypto source, Symmetric block cipher, AES engine, 256 key size.

Password Encryption

User passwords are never stored, only the hash versions are stored hashed by algorithm SHA 256.

7.3 Data Integrity

Data integrity is a critical security requirement. The data backup procedure is an integral part of this requirement. OpenText Software Delivery Management does not provide backup capabilities. Following are some important considerations:

- Backup is especially important before critical actions such as project upgrade.
- Backup files should be stored properly according to the industry best practices to avoid unauthorized access.
- Since data backup consumes lots of resources, it is strongly recommended to avoid running backups during peak demand times.

Note: When backing up the database, ensure that the file repository is backed up at the same time to reflect the same system state.

8 Elasticsearch

8.1 Securing access to Elasticsearch

It is recommended to use the authentication plugin called X-Pack to define username and password for accessing the data.

By not doing this, you are disabling or bypassing security features, thereby exposing the system to increased security risks. By using this option, you understand and agree to assume all associated risks and hold OpenText harmless for the same.

It is recommended to follow Elasticsearch security guidelines in Configuring security in Elasticsearch.

Ensure that the latest version of X-Pack is deployed, and all security patches of Elasticsearch are installed.

9 OpenText Software Delivery Management Security Settings

This chapter contains reference to some of the OpenText Software Delivery Management settings that are relevant to security.

9.1 Secure OpenText Software Delivery Management Storage

OpenText Software Delivery Management allows users to upload files to the server. This allows users to upload attachments, save automation scripts and test run results, and so on. All files uploaded to the server must be validated, since they can contain viruses, malicious code, or Trojan horses that could infect the entire system. An attacker or a malicious user can upload malicious files from one account and then download them to diverse clients.

The site administrator can limit the types of files that can be uploaded to OpenText Software Delivery Management by using the ATTACHMENTS_FILE_EXTENSION_BLACK_LIST site parameter, which filters unwanted file types by extension. However, the attachment files can contain dangerous content. As a result, a downloaded file must still be opened with caution. It is strongly recommended to implement proper antivirus protection for the file storage allocated for the OpenText Software Delivery Management repository.

9.2 Configure site parameters according to security guidelines.

The following parameters affect security of OpenText Software Delivery Management.

Group	Parameter	**Description**
Storage	ATTACHMENTS_FILE_EXTENSION_BLACK_LIST	This parameter defines a list of not permitted extensions of storage file
	ATTACHMENTS_FILE_EXTENSION_WHITE_LIST	This parameter defines a list of the permitted extensions of MQM storage files
	ATTACHMENTS_URL_DOMAIN_WHITE_LIST	This parameter defines a list of the permitted domains of NGA attachments URLs

	ATTACHMENTS_URL_ENABLE_DOMAIN_WHITE_LIST	This parameter defines if the domain white list validation of attachment url is enabled
	EXTENSION_TO_MIME_TYPE	This parameter defines mapping of custom extension to mime type to be used for validation of uploaded files
	FILE_EXTENSION_WHITE_LIST_DOWNLOAD	The value is the semicolon delimited string with the file extensions that are allowed to be downloaded via open attachments, REST API, or FTP Explorer
	FILE_EXTENSION_WHITE_LIST_UPLOAD	The value is the semicolon delimited string with the file extensions that are allowed to be uploaded via open attachments, extended storage, REST API, or FTP Explorer
	VALIDATE_MIME_TYPE_MATCH_TO_EXTENSION	This parameter defines whether to enable the validation of file extension and content relevancy
Authentication	SUPPORTS_BASIC_AUTHENTICATION	Define whether shared space supports basic authentication. Note: Basic authentication is not secured. Turning this parameter on reduces the security level of OpenText Software Delivery Management.
	AUTHENTICATION_DELAY_ACTIVE	Activates a brute-force attack prevention mechanism during sign-in
	AUTHENTICATION_DELAY_SECONDS	Time frame which starts at first authentication failure. Reaching AUTHENTICATION_MAX_ATTEMPTS within this period will cause blocking further attempts until it ends.

		Applying a new value, requires a restart.
	AUTHENTICATION_MAX_ATTEMPTS	Number of allowed failed authentication attempts (with same user or from same address) before being delayed
	MINUTES_UNTIL_GLOBAL_SESSION_TIMEOUT	The maximum number of minutes that the session lasts even if the session is in use. Default global timeout is 1440 minutes (24 hours).
	MINUTES_UNTIL_IDLE_SESSION_TIMEOUT	The maximum number of minutes that the session lasts while the session is not in use. Default idle timeout is 180 minutes (3 hours).
Logs	SEND_UI_LOGS_TO_SERVER	Control if client sends error logs to server
Security	ENABLE_STRICT_TRANSPORT_SECURITY_HEADER	Defines whether Strict-Transport-Security header is added to response. Default: true. For details, see https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security.

For details on each parameter see https://admhelp.microfocus.com/octane/en/latest/Online/Content/AdminGuide/params.htm

If you select unsecured options of site parameters or undocumented parameters, you are disabling or bypassing security features, thereby exposing the system to increased security risks. By using this option, you understand and agree to assume all associated risks and ho

10 Logs

There are several types of logs provided on the OpenText Software Delivery Management server:

- Client logs
- Audit logs

- Site administration logs

In addition, the history of changes to existing objects (defects, tests, requirements, and so on) are stored in the database as history. This information remains as long as the object itself is not deleted.

Recommendations:

- Pay attention to the log level and do not leave the level at Debug.
- Pay attention to log rotation.
- Restrict access to the log directory.

11 Product Security

Product is ISO 27001:2013 certified

For details refer to Certificate

12 Learn more.

Question

Where can I view security bulletins?

Answer

Via the following link: Security Bulletin Archive

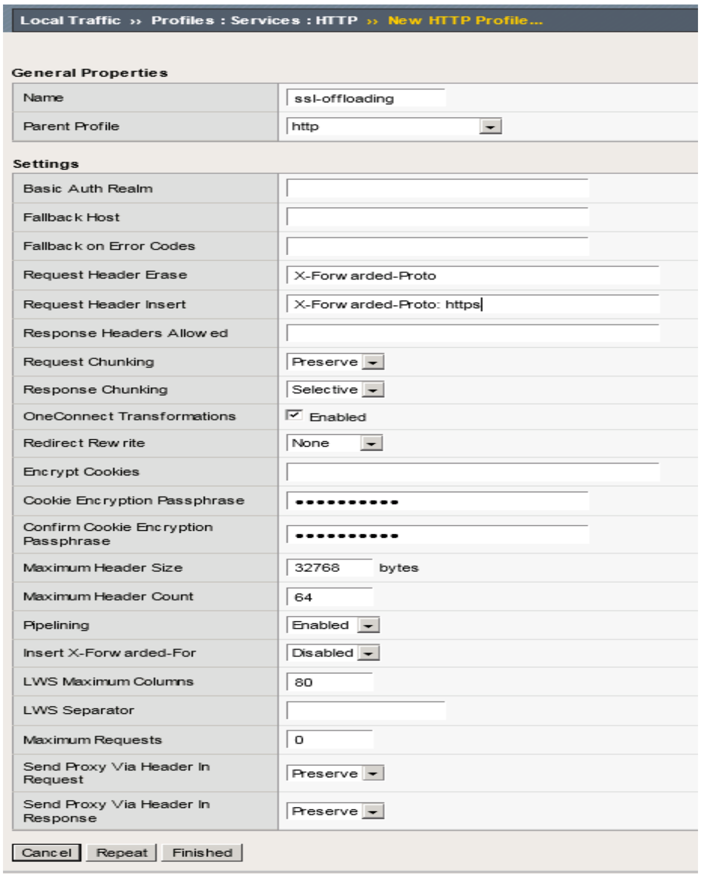
Question

Where can customers obtain the latest information regarding security vulnerabilities?

Answer

You can register for security vulnerability alerts via the following: Register for e-mail notification

Appendix A: Define a new HTTP profile



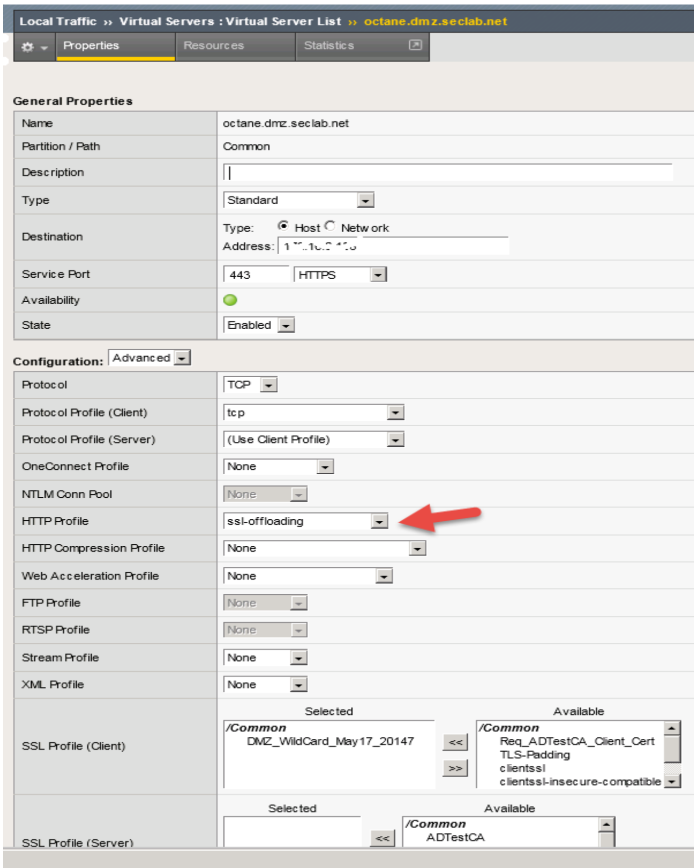
Local Traffic ›› Profiles : Services : HTTP ›› New HTTP Profile...

General Properties

Name	ssl-offloading
Parent Profile	http

Settings

Basic Auth Realm	
Fallback Host	
Fallback on Error Codes	
Request Header Erase	X-Forwarded-Proto
Request Header Insert	X-Forwarded-Proto: https
Response Headers Allowed	
Request Chunking	Preserve
Response Chunking	Selective
OneConnect Transformations	☑ Enabled
Redirect Rewrite	None
Encrypt Cookies	
Cookie Encryption Passphrase	●●●●●●●●●●●
Confirm Cookie Encryption Passphrase	●●●●●●●●●●●
Maximum Header Size	32768 bytes
Maximum Header Count	64
Pipelining	Enabled
Insert X-Forwarded-For	Disabled
LWS Maximum Columns	80
LWS Separator	
Maximum Requests	0
Send Proxy Via Header In Request	Preserve
Send Proxy Via Header In Response	Preserve



Local Traffic ›› Virtual Servers : Virtual Server List ›› octane.dmz.seclab.net
Properties
Resources
Statistics

General Properties

Name	octane.dmz.seclab.net
Partition / Path	Common
Description	
Type	Standard
Destination	Type: ● Host ○ Network Address: [illegible]
Service Port	443 HTTPS
Availability	🟢
State	Enabled

Configuration: Advanced

Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
OneConnect Profile	None
NTLM Conn Pool	None
HTTP Profile	ssl-offloading
HTTP Compression Profile	None
Web Acceleration Profile	None
FTP Profile	None
RTSP Profile	None
Stream Profile	None
XML Profile	None
SSL Profile (Client)	Selected: /Common DMZ_WildCard_May17_20147 Available: /Common Req_ADTestCA_Client_Cert TLS-Padding clientssl clientssl-insecure-compatible
SSL Profile (Server)	Selected: Available: /Common ADTestCA

Appendix B: Enabling the built-in DoS protection filter in production

OpenText Software Delivery Management includes a built-in DoS protection filter based on Jetty DoSFilter. This DoS filter is capable of partially mitigating flood-based DoS attacks. By default, the OpenText Software Delivery Management server's DoS protection filter is disabled because the filter may have negative impact on system performance.

We recommend that you use a dedicated product which provides DoS protection, as described earlier in the section "Distributed Denial of Service attack protection".

However, if you want to enable the OpenText Software Delivery Management built-in DoS protection filter, use the following instructions.

Enable the built in DoS protection filter

1. Edit the **wrapper-parameters-for-customer-site.conf** file, and add a custom configuration as follows:
   - If this is the first configuration in this file, add the following:
     wrapper.java.additional.200=-Dcom.hp.mqm.rest.infra.jetty_dos_filter_enable=true
   - If this is not the only configuration in this file, instead of 200 use the next available unique configuration ID greater than 200.

2. You can control other aspects of this filter as explained in Jetty DoSFilter Guide > **Configuring DoS Filter Parameters,** using the following parameters:
   - com.hp.mqm.rest.infra.jetty_dos_filter_max_requests_per_second to set maxRequestsPerSec, default is 25.
   - com.hp.mqm.rest.infra.jetty_dos_filter_delay_millis to set delayMs, default is 100.
   - com.hp.mqm.rest.infra.jetty_dos_filter_max_request_timeout_millis to set maxRequestMs, default is 10 minutes.

   For example, these parameters can be configured as:

   wrapper.java.additional.201=-Dcom.hp.mqm.rest.infra.jetty_dos_filter_max_requests_per_second=25

   wrapper.java.additional.202=-Dcom.hp.mqm.rest.infra.jetty_dos_filter_delay_millis=100

   wrapper.java.additional.203=-Dcom.hp.mqm.rest.infra.jetty_dos_filter_max_request_timeout_millis=600000

3. Repeat the above configuration in each OpenText Software Delivery Management server node.
4. After the configuration has been changed, restart the OpenText Software Delivery Management node.

opentext™

About OpenText

OpenText enables the digital world, creating a better way for organizations to work with information, on-premises or in the cloud. For more information about OpenText (NASDAQ/TSX: OTEX), visit opentext.com.

Connect with us:

OpenText CEO Mark Barrenechea's blog

Twitter | LinkedIn