FORTINET

Release Notes

FortiSIEM 6.6.0

FORTINET®

01/30/2023
FortiSIEM 6.6.0 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
07/26/2022	Initial version of FortiSIEM 6.6.0 Release Notes.
07/27/2022	Added Known Issue.
08/15/2022	Two known issues added to 6.6.0 Release Notes.
08/17/2022	Known issue workaround added to 6.6.0 Release Notes.
09/16/2022	Added/Updated Known Issues to FortiSIEM 6.6.1 and 6.6.0 Release Notes.
09/20/2022	Updated Known Issue #1 in FortiSIEM 6.6.1 and 6.6.0 Release Notes.
10/25/2022	Added Known Issue to 6.4.0-6.6.2.
12/06/2022	Added Key Enhancement for 6.4.0 Release Notes.
01/30/2023	Added Known Issue to 6.6.0-6.7.0 Release Notes.

What's New in 6.6.0

- New Features
- Key Enhancements
- New Device Support
- Bug Fixes and Minor Enhancements
- Known Issues

New Features

- Scale Out ClickHouse Cluster
- Generic REST API Based Event Collection
- Watchlist REST API for FortiGate Threat Feed and 3rd Party Devices

Scale Out ClickHouse Cluster

In this release, you can set up a Scale Out ClickHouse Cluster using Supervisor and Worker nodes. All operations can be done from FortiSIEM GUI. The first step is to add storage to the FortiSIEM nodes for storing events. Then you configure the Cluster by specifying the number of shards and choosing the Keeper Cluster members and Server Cluster Replicas. Insertion, Replication and Queries are distributed to Supervisor and Worker nodes resulting in a redundant scale out and architecture.

For understanding concepts see Background Information.

For adding storage to Worker nodes, see Initial Configuration.

For configuring ClickHouse Cluster, see ClickHouse Configuration.

For configuring a ClickHouse retention policy, see Creating a ClickHouse Online Event Retention Policy.

For sizing guide on how to achieve high insert and query efficiency with ClickHouse, see the 6.6.0 Sizing Guide.

For ClickHouse Index Design and Query Optimization, see ClickHouse Usage Notes in the Appendix.

Generic REST API Based Event Collection

Increasingly Cloud Applications such as Cisco Umbrella, Microsoft Defender for Endpoint, WorkDay, Box.com, etc. are providing events and alerts via HTTPS based API. Rather than develop application by application support, this release provides a generalized way to configure an HTTPS based access method and pull data via that access method. A customer just needs to write a specific log parser for the application. This approach can cover all HTTPS based logging applications without requiring a new FortiSIEM release.

This release includes built in support for Cisco Umbrella Activity API and Microsoft Defender using Graph API using this Generalized HTTPS Access Method.

For details on configuring HTTPS API, see Generic Log API Poller HTTPS Advanced Integration from the External Systems Configuration Guide.

For details on creating HTTPS Credential for Cisco Umbrella Activity API, see Cisco Umbrella Configuration from the External Systems Configuration Guide.

For details on creating HTTPS Credential for Microsoft Defender API, see Windows Defender for Endpoint Configuration from the External Systems Configuration Guide.

Watchlist REST API for FortiGate Threat Feed and 3rd Party Devices

This list provides a simplified Watchlist Read REST API that FortiGate Firewalls or any other 3rd party device can use to download a FortiSIEM Watchlist and take blocking action. The REST API returns a list containing IP, Domain or Hash values that appear in FortiSIEM Watchlist.

Set Up

1. In FortiSIEM, set up a Watchlist and associate the Watchlist to one or more rules.
2. In FortiGate, define the Watchlist REST API as a threat feed.
   - See FortiGate/FortiOS Cookbook Threat feed for details on configuring FortiGate threat feed.
   - See Read APIs for Integration with FortiGate Firewalls for the FortiSIEM Watchlist Read API for FortiGates.

How it Works

1. A threat detection rule triggers in FortiSIEM and dynamically populates a Watchlist.
2. FortiGate periodically pulls the Watchlist as a threat feed.
3. FortiGate takes mitigating action.

Consider the scenario where the IP ages out from Watchlist in FortiSIEM because the rule stops triggering or other reasons.

1. FortiGate periodically pulls the Watch List again (that entry would be missing)
2. FortiGate undoes the mitigating action.

Key Enhancements

- Custom Image Upload Endpoint
- Performance Improvements
- Update Glassfish CA Certificate store with Java CA Cert Store
- System Upgrades
- Added Support for Elasticsearch 7.17

Custom Image Upload Endpoint

During Collector/Agent/Content upgrades, the Upgrade URL for Collectors and Agents is automatically generated by the App Server based on the Supervisor host name or IP in the GUI. However this approach does not work when there are

Load Balancers in front of Supervisor node. This release provides an option for the user to specify a Load Balancer Host Name or IP and Supervisor will use it to create the custom endpoint for Collectors and Agents. If you use Load Balancer Host Name, it must be resolvable by Agents and Collectors. The Load Balancer is an easier choice.

For details on Setting up Custom Image Upload Endpoint, see Custom Update.

Performance Improvements

The following performance improvements have been made in 6.6.0.

- Incident Handling Performance Improvement
- IdentityWorker Performance Improvement
- ReportWorker and RuleWorker Performance Improvement
- QueryMaster Memory Usage Improvement

Incident Handling Performance Improvement

App Server on Supervisor post-processes Incidents to add meta data, update risk scores, stores in PostGRESQL database and then executes notification policies and external integrations. FortiSIEM Manager aggregates Incidents from all Supervisors and stores them in local PostGRESQL database for display in FortiSIEM Manager GUI. Therefore, fast incident handling is critical for the system to work correctly at high loads.

This release contains extensive Incident handling performance optimizations. FortiSIEM Manager can handle about 1500 Incidents/sec from FortiSIEM Supervisors.

IdentityWorker Performance Improvement

This is achieved by making IdentityWorker multi-threaded while getting events from shared buffer.

ReportWorker and RuleWorker Performance Improvement

This is achieved by optimizing IN Group query handling code

QueryMaster Memory Usage Improvement

This is achieved by frequently calling memory release operations in Google tcmalloc library.

Update Glassfish CA Certificate store with Java CA Cert Store

Many Java based external integrations required users to import root CA certificates, as the Glassfish CA store was not populated after migrating to Glassfish V5 in an earlier FortiSIEM release. In this release, during migration and upgrade process, the Glassfish CA store is populated with valid certificates from the Java CA cert store. With this change, Java based external integrations should work more seamlessly.

System Upgrades

Upgrade to Rocky Linux 8.6 with patches released on May 16, 2022. See https://docs.rockylinux.org/release_notes/8_6/ and https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/8.6_release_notes/bug_fixes#bug-fix_securityfor more information.

Added Support for Elasticsearch 7.17

Support has been added for Elasticsearch 7.17.

New Device Support

- Cisco Umbrella Activity API - done via Generalized HTTPS based Event Collection methodology
- Microsoft Defender for end point using Graph API - done via Generalized HTTPS based Event Collection methodology

Bug Fixes and Minor Enhancements

Bug ID	Severity	Module	Description
822029	Minor	Anomaly	Exclude network logon events from UEBA AI engine.
824268	Minor	App Server	IPS to CVE validation does not work correctly.
821804	Minor	App Server	Restarting App Server sometimes gives heap error and it is not fixed by re-deploying.
816715	Minor	App Server	Org id in the device maintenance table did NOT get deleted when customer deletes the org.
816492	Minor	App Server	Older open SAML library causes login failure to OKTA authentication portal.
815696	Minor	App Server	When user changes org scope, create this event PH_AUDIT_USER_CHANGE_ORG_SCOPE instead of PH_AUDIT_USER_SUED.
815025	Minor	App Server	Specifying Reporting device group and Event type Group does not work correctly for Event forwarding, Event Dropping and Retention Policy and Org mapping.
813642	Minor	App Server	HTTP Error page reveals App Server name and version.
811630	Minor	App Server	If you change the priority of a system rule, after FortiSIEM upgrade, the rule's priority is incorrectly reset to its default priority.

Bug ID	Severity	Module	Description
821813	Minor	Data	Time Stamps are not parsed properly for Falcon Data Replicator.
821585	Minor	Data	SystemShutdown event group has some incorrect event types.
817295	Minor	Data	WinOSPull parser has incorrect function definition.
814834	Minor	Data	Update BarracudaCloudGenFW parser format recognizer.
814409	Minor	Data	Update FortiSIEM Claroty CTD parser.
811907	Minor	Data	Reduce parser test events down to 10 for ease of cloning and testing.
811224	Minor	Discovery	AWS credentials are included in aws-phgetflowlogs.php in clear text.
821427	Minor	ElasticSearch	Add 7 day allowance to write data to Elasticsearch to cover data buffering more than 2 days.
818548	Minor	Event Pulling	AWS Kinesis fails to sync shards and leases on connection.
817081	Minor	Event Pulling	AWS Kinesis buffer size are incorrect and causes event pull failure.
821263	Minor	GUI	Ticket Note not saved in Incident Ticket.
820583	Minor	GUI	Show proper error codes returned by FortiSOAR executing playbook or connectors.
814430	Minor	GUI	GUI does not allow dot in user name field.
810866	Minor	GUI	When you disable a Device in Pull Events with a search filter, a different device in the global list is disabled.
816499	Minor	Parser	Increase TCP/UDP buffer from 16KB to 24KB to handle large events up to 24KB.
814318	Minor	Report	For ClickHouse Storage, Incident CSV export does not contain result for incident status and resolution.
809386	Enhancement	App Server	The events PH_DEV_MON_LOG_DEVICE_DELAY_LOW and PH_DEV_MON_LOG_DEVICE_DELAY_HIGH do not generate reliably.
802322	Enhancement	App Server	Changing Supervisor IP may lead to two Supervisor entries showing up in Cloud Health.
801605	Enhancement	App Server	Users who have Read only admin permission on Super Global but have Full Admin on Org, cannot edit credentials in the Org after switching to that Org.
804904	Enhancement	App Server,GUI	New Dashboard folders may not appear in the drop-down in the dashboard folder section.
810382	Enhancement	Data	Some generic events from FortiGate need to be further parsed.

Bug ID	Severity	Module	Description
809024	Enhancement	Data	Event Type generated from Windows logs received via Epilog is incorrect and very long.
803091	Enhancement	Data	Update FortiGate parser to support Bandwidth Delta values.
802247	Enhancement	Data	Update MSDefender AdvancedHunting parser.
797026	Enhancement	Data	Update Nginx event parser.
792333	Enhancement	Data	Update FortiAI parser to handle new log format and relabeling of product to FortiNDR.
779162	Enhancement	Data	Update Claroty parser to accommodate year timestamp in syslog header and new event.
774819	Enhancement	Data	Update FortiMail log parser.
684254	Enhancement	Data	Update Extreme switch log parser.
807886	Enhancement	Data Manager	A log from Elasticsearch event insert code contains password.
801973	Enhancement	Data Manager	Online data is not removed when defining online retention policies for all events.
807102	Enhancement	Discovery	SNMP V3 Trap support causes Auth Password and Priv Password directly in snmptrapd.conf on Collectors.
796086	Enhancement	Discovery	Support more HP switches for discovery, performance and availability metrics via SNMP.
775692	Enhancement	Discovery	Test connectivity results sometimes display Windows OMI text password in GUI.
644096	Enhancement	Discovery, Perf Monitoring	Enable AES256 and SHA256 for SNMP V3.
809387	Enhancement	ElasticSearch	Limit the number of dynamically allocated shards.
795638	Enhancement	Event Pulling	Sophos logs via API are polled very frequently; thereby quickly reaching API limit.
810548	Enhancement	GUI	System notifications are unreadable and overlaps with page information.
783383	Enhancement	Rule	Suppress excessive PH_REPORT_PACK_FAILED events.

Known Issues

1. Currently, Policy based retention for EventDB does not cover two event categories: (a) System events with phCustId = 0, e.g. a FortiSIEM External Integration Error, FortiSIEM process crash etc., and (b) Super/Global customer audit events with phCustId = 3, e.g. audit log generated from a Super/Global user running an adhoc query. These events are purged when disk usage reaches high watermark.

2. When retention policies are defined, there is a memory corruption issue in Parser module that can cause Parser module to crash or consume high memory. This may not always happen. This may result in event parsing being delayed, events being missed or Supervisor GUI being slow. From the Cloud Health page, you can see `phParser` process is down or has high CPU for any node. This issue has been resolved in release 6.6.2.
3. On hardware appliances running FortiSIEM 6.6.0 or earlier, FortiSIEM `execute shutdown` CLI does not work correctly. Please use the Linux `shutdown` command instead.
4. If you are running FortiSIEM 6.6.0 or earlier and have a Malware IOC group with 750K entries or more, then restarting the application server or rebooting of FortiSIEM Super node may fail. If this issue occurs, take the following steps:
   a. ssh into the Supervisor as root user.
   b. Run the following command to back up your copy of the domain.xml file.

      ```
      cp -a /opt/glassfish/domains/domain1/config/domain.xml
      /opt/glassfish/domains/domain1/config/domain.xml.backup
      ```

   c. Run the following command to modify the domain.xml file.

      ```
      vi /opt/glassfish/domains/domain1/config/domain.xml
      ```

   d. Find the following on line 220 and 221 (based off of default domain.xml file):

      ```
      <jvm-options>-Xmx5120m</jvm-options>

      <jvm-options>-Xms5120m</jvm-options>
      ```

      and change to:

      ```
      <jvm-options>-Xmx10G</jvm-options>

      <jvm-options>-Xms10G</jvm-options>
      ```

   e. Save the changes and exit.
   f. Run the following command.

      ```
      ps -ef | grep glassfish5
      ```

      Example output:

      ```
      admin 2993 1 85 Aug15 ? 1-16:43:25 /opt/Java/bin/java -cp
      /opt/glassfish5/glassfish/modules/glassfish.jar -XX:+UnlockDiagnosticVMOptions -
      XX:+UseParNewGC -XX:+CMSConcurrentMTEnabled -XX:+CMSParallelRemarkEnabled -
      XX:+LogVMOutput -XX:MaxPermSize=384m -XX:+UseConcMarkSweepGC -
      XX:ReservedCodeCacheSize=128m -XX:NewRatio=2 -
      XX:LogFile=/opt/glassfish5/glassfish/domains/domain1/logs/jvm.log -
      XX:+UseCompressedOops -XX:+DisableExplicitGC -XX:+UseCMSInitiatingOccupancyOnly -
      XX:CMSInitiatingOccupancyFraction=30 -Xmx5120m -Xms5120m -server -
      javaagent:/opt/glassfish5/glassfish/lib/monitor/flashlight-agent.jar -
      Djavax.net.ssl.trustStore=/opt/glassfish5/glassfish/domains/domain1/config/cacerts.j
      ks -Dfelix.fileinstall.dir=/opt/glassfish5/glassfish/modules/autostart/ -
      Dcom.sun.aas.installRoot=/opt/glassfish5/glassfish -Dfelix.fileinstall.poll=5000 -
      Djava.endorsed.dirs=/opt/glassfish5/glassfish/modules/endorsed:/opt/glassfish5/glass
      fish/lib/endorsed -
      Djava.security.policy=/opt/glassfish5/glassfish/domains/domain1/config/server.policy
      -Dcom.sun.enterprise.server.logging.max_history_files=20 -
      Dosgi.shell.telnet.maxconn=1 -Dfelix.fileinstall.bundles.startTransient=true -
      Dcom.sun.enterprise.config.config_environment_factory_
      class=com.sun.enterprise.config.serverbeans.AppserverConfigEnvironmentFactory -
      Dfelix.fileinstall.log.level=2 -
      ```

```
Djavax.net.ssl.keyStore=/opt/glassfish5/glassfish/domains/domain1/config/keystore.jks
-
Djava.security.auth.login.config=/opt/glassfish5/glassfish/domains/domain1/config/lo
gin.conf -Dfelix.fileinstall.disableConfigSave=false -
Dorg.owasp.esapi.resources=/opt/phoenix/config -
Dfelix.fileinstall.bundles.new.start=true -
Dcom.sun.aas.instanceRoot=/opt/glassfish5/glassfish/domains/domain1 -
Dosgi.shell.telnet.port=37401 -Dgosh.args=--nointeractive -
Dcom.sun.enterprise.security.httpsOutboundKeyAlias=s1as -
Dosgi.shell.telnet.ip=127.0.0.1 -DANTLR_USE_DIRECT_CLASS_LOADING=true -
Djava.awt.headless=true -
Djava.ext.dirs=/opt/Java/lib/ext:/opt/Java/jre/lib/ext:/opt/glassfish5/glassfish/dom
ains/domain1/lib/ext -Djdbc.drivers=org.apache.derby.jdbc.ClientDriver -
Djava.library.path=/opt/glassfish5/glassfish/lib:/opt/phoenix/lib64:/opt/phoenix/lib
32:/usr/local/lib:/usr/java/packages/lib/amd64:/usr/lib64:/lib64:/lib:/usr/lib
com.sun.enterprise.glassfish.bootstrap.ASMain -upgrade false -domaindir
/opt/glassfish5/glassfish/domains/domain1 -read-stdin true -asadmin-args --
host,,,localhost,,,--port,,,4848,,,--secure=false,,,--terse=false,,,--echo=false,,,--
interactive=false,,,start-domain,,,--verbose=false,,,--watchdog=false,,,--
debug=false,,,--domaindir,,,/opt/glassfish5/glassfish/domains,,,domain1 -domainname
domain1 -instancename server -type DAS -verbose false -asadmin-classpath
/opt/glassfish/lib/client/appserver-cli.jar -debug false -asadmin-classname
com.sun.enterprise.admin.cli.AdminMain
```

Note: The Process id is 2993 from the example.

g. From step f, note the Process id (PID) and kill it, by running the following command, and substituting <*PID*> with your actual PID.

```
kill -9 <PID>
```

Example command:

```
kill -9 2993
```

h. Wait for `AppServer` to restart.

5. FortiSIEM 6.5.0 ran ClickHouse on a single node and used the Merge Tree engine. FortiSIEM 6.6.0 onwards runs Replicated Merge Tree engine, even if Replication is not turned on. So after upgrading to FortiSIEM 6.6.0, you will need to do the following steps to migrate the event data previously stored in Merge Tree to Replicated Merge Tree. Without these steps, old events in 6.5.0 will not be searchable in 6.6.0. Once you are on post 6.5.0 release, you will not need to do this procedure again.

   To upgrade your FortiSIEM from 6.5.0 to 6.6.0 or later, take the following steps.

   a. Navigate to **ADMIN >Settings > Database > ClickHouse Config**.

   b. Click **Test**, then click **Deploy** to enable the ClickHouse Keeper service which is new in 6.6.0.

   c. Migrate the event data in 6.5.0 to 6.6.0 by running the script `/opt/phoenix/phscripts/clickhouse/clickhouse-migrate-650.sh`.

6. Sometimes App Server may not come up properly after upgrading to 6.6.0. This is rare and Fortinet has only seen it occur in Azure, although the hypervisor platform has very little to do with it. If this issue occurs, you will see that the backend ph processes will be down and there will not be any upgrade errors in ansible. In this situation, use the following workaround to get the system up and running.

   a. Download `gf_admin-keyfile` and `deploy-fresh.sh`.

   b. Copy the file `gf_admin-keyfile` to Fortisiem Supervisor node under `/opt/phoenix/deployment/jumpbox`.

   c. Login to FortiSIEM Super console and run the following command.

   ```
   cp /opt/phoenix/deployment/deploy-fresh.sh /opt/phoenix/deployment/deploy-
   ```

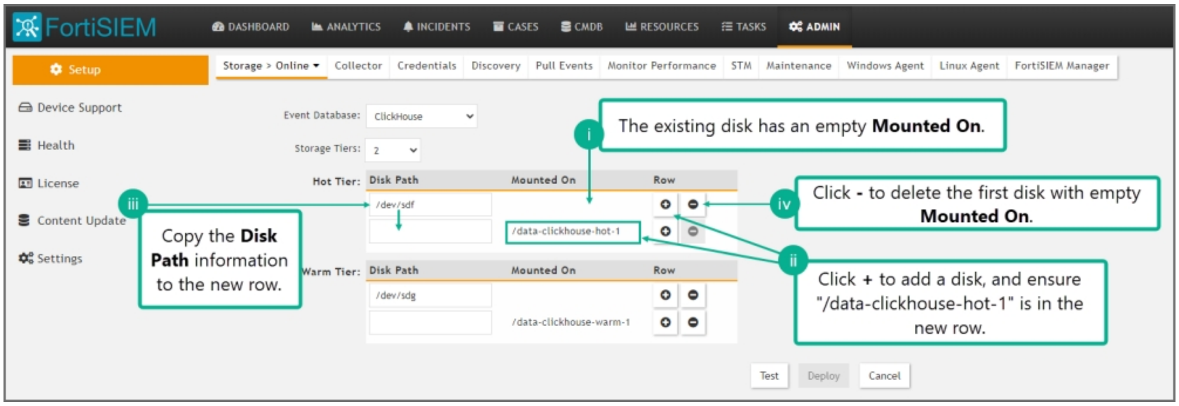
```
fresh.sh.orig
```

d. Copy the file `deploy-fresh.sh` to FortiSIEM Super under `/opt/phoenix/deployment`.

e. Login to the Supervisor console and run the following commands.

```
chmod +x /opt/phoenix/deployment/deploy-fresh.sh
su - admin
/opt/phoenix/deployment/deploy-fresh.sh /opt/phoenix/deployment/phoenix.ear
```

7. If you are running ClickHouse and upgrade from 6.5.0 to 6.6.0 and go to Storage > Online Settings and click **Test**, it will fail. Fortinet introduced a new disk attribute called "Mounted On" to facilitate disk addition/deletion that was not present in 6.5.0. Follow these steps to fix the problem.
   a. Go to **ADMIN > Setup > Storage > Online**. ClickHouse should be the selected database.
   b. For Hot tier and for every configured disk within the tier, do the following:
      i. The existing disk should have empty Mounted On.
      ii. Click + to add a disk. For the new disk, Disk Path should be empty and Mounted On set to /data-clickhouse-hot-1.
      iii. Copy the Disk Path from the existing disk into this newly disk. The new disk should have the proper Disk Path and Mounted On fields.
      iv. Delete the first disk with empty Mounted On.



Event Database: ClickHouse

Storage Tiers: 2

Hot Tier: /dev/sdf; /data-clickhouse-hot-1

Warm Tier: /dev/sdg; /data-clickhouse-warm-1

i The existing disk has an empty **Mounted On**.

iv Click - to delete the first disk with empty **Mounted On**.

iii Copy the **Disk Path** information to the new row.

ii Click + to add a disk, and ensure "/data-clickhouse-hot-1" is in the new row.

Do this for all disks you have configured in 6.5.0. After your changes, the disks should be ordered /data-clickhouse-hot-1, /data-clickhouse-hot-2, /data-clickhouse-hot-3 from top to bottom.

   c. Repeat the same steps for the Warm tier (if one was configured in 6.5.0), except that the Mounted On fields should be /data-clickhouse-warm-1, /data-clickhouse-warm-2, /data-clickhouse-warm-3 from top to bottom.
   d. When done, click **Test**, then click **Deploy**.

8. In Elasticsearch based deployments, queries containing "IN Group X" are handled using Elastic Terms Query. By default, the maximum number of terms that can be used in a Terms Query is set to 65,536. If a Group contains more than 65,536 entries, the query will fail.

   The workaround is to change the “max_terms_count” setting for each event index. Fortinet has tested up to 1 million entries. The query response time will be proportional to the size of the group.

   Case 1. For already existing indices, issue the REST API call to update the setting

```
PUT fortisiem-event-*/_settings
{
  "index" : {
    "max_terms_count" : "1000000"
  }
}
```

Case 2. For new indices that are going to be created in the future, update fortisiem-event-template so those new indices will have a higher max_terms_count setting

a. `cd /opt/phoenix/config/elastic/7.7`

b. Add `"index.max_terms_count": 1000000` (including quotations) to the “settings” section of the `fortisiem-event-template`.

   Example:

   ...

```
  "settings": {
    "index.max_terms_count": 1000000,
```

   ...

c. Navigate to **ADMIN > Storage > Online** and perform **Test** and **Deploy**.

d. Test new indices have the updated terms limit by executing the following simple REST API call.

   `GET fortisiem-event-*/_settings`

9. If you set up Disaster Recovery (DR) on FortiSIEM 6.5.0, then upgrading the Secondary to 6.6.0 will fail. If you set up DR on older versions, this issue does not occur. The following workarounds are available, depending on your situation.

   If you have not started the upgrade to 6.6.0 on DR yet, take the following steps:

   Instructions before Upgrading Secondary in DR Configuration

   a. Step 1: Back up Primary Glassfish Key into Secondary

      i. ssh into the Primary Supervisor as root.

      ii. Run the following command.

```
phLicenseTool --showDatabasePassword
```

      iii. Note the password.

      iv. Run the following command.

```
cat /opt/glassfish/domains/domain1/config/admin-keyfile
```

      v. Note the output.

   b. Step 2: Insert into Secondary before Upgrade

      i. Log into the Secondary Supervisor as root.

      ii. Run `phsecondary2primary`

      Note: This disables disaster recovery for the time being.

      iii. Run the following command to modify the `admin-keyfile` file.

```
vi /opt/glassfish/domains/domain1/config/admin-keyfile
```

      iv. Paste the output from Step 1 v. to the `admin-keyfile` file, replacing the current entry and save.

   c. Step 3: Verify that the Key has Taken Effect on Secondary Supervisor

      i. Run the following commands.

```
su - admin; /opt/glassfish/bin/asadmin stop-domain
/opt/glassfish/bin/asadmin start-domain
/opt/glassfish/bin/asadmin login
```

      For user name, enter admin

      For password, enter the password from Step 1 iii.

      Example success login:

```
/opt/glassfish/bin/asadmin login
Enter admin user name [Enter to accept default]> admin
Enter admin password>
Login information relevant to admin user name [admin] for host [localhost] and
admin port [4848] stored at [/opt/phoenix/bin/.gfclient/pass] successfully.
Make sure that this file remains protected. Information stored in this file will
be used by administration commands to manage associated domain.
Command login executed successfully.
```

Note: Step 3 must work in order to proceed to Step 4.

d. Step 4: Upgrade to 6.6.0 on Secondary

  i. Follow the Upgrade Guide.

e. Step 5: Add Secondary Back into the System

  i. Log into the Primary Supervisor’s GUI.

  ii. Navigate to **ADMIN > License > Nodes**.

  iii. Select the Secondary entry in the GUI and click on **Edit**.

  iv. Click on **Save** to re-establish connection to the Secondary.

Instructions if you are Already in a Failed State in the Secondary

a. Step 1: Grab the Supervisor's DB Password

  i. Log into the Primary Supervisor as root.

  ii.

```
Run the following command.
phLicenseTool --showDatabasePassword
```

  iii. Note the password.

  iv. Run the following command.

```
cat /opt/glassfish/domains/domain1/config/admin-keyfile
```

  v. Note the output.

b. Step 2: Update the Glassfish Password on Secondary to Continue with the Upgrade

  i. Log into the Secondary Supervisor as root.

  ii. Run the following commands to modify the `admin-keyfile` file.

```
cd /opt/glassfish/domains/domain1/config/
```

```
cp -a admin-keyfile admin-keyfile.bad
```

```
vi /opt/glassfish/domains/domain1/config/admin-keyfile
```

  iii. Paste the output from Step 1 v. to the `admin-keyfile`, replacing the current entry and save.

c. Step 3: Deploy `appserver` Manually after Admin Passkey has Changed

  i. Run the following command.

```
vi /opt/phoenix/deployment/deploy-fresh.sh
```

  ii. Replace the password with the password from Step 1 iii by finding the following line, and making the password replacement there.

```
echo "AS_ADMIN_PASSWORD="$dbpasswd > $DEPLOYMENR_HOME/glassfish-pwd.txt
```

Example:

```
echo ‘AS_ADMIN_PASSWORD=ad1$dnsk%’ > $DEPLOYMENR_HOME/glassfish-pwd.txt
```

Note: The use of single quote character (‘) in the replacement vs the double quote character (“).

iii. Save the file `deploy-fresh.sh`.

iv. Run the following commands.

```
su - admin
```

```
/opt/phoenix/deployment/deploy-fresh.sh /opt/phoenix/deployment/phoenix.ear
```

d. Step 4: Modify Ansible Playbook to Finish Upgrade

i. Run the following command.

```
vi /usr/local/upgrade/post-upgrade.yml
```

ii. Remove only the following:

```
 - configure
    - update_configs
    - fortiinsight-integration
    - setup-python
    - setup-node
    - setup-clickhouse
    - setup-zookeeper
    - setup-redis
    - migrate-database
    - appserver
```

iii. Save the modification.

iv. Resume the upgrade by running the following command.

```
ansible-playbook /usr/local/upgrade/post-upgrade.yml | tee -a
/usr/local/upgrade/logs/ansible_upgrade_continued.log
```

v. Reboot the Supervisor if system does not reboot itself.

10. FortiSIEM uses dynamic mapping for Keyword fields to save Cluster state. Elasticsearch needs to encounter some events containing these fields before it can determine their type. For this reason, queries containing `group by` on any of these fields will fail if Elasticsearch has not seen any event containing these fields. Workaround is to first run a non-group by query with these fields to make sure that these fields have non-null haves.

FORTINET®

www.fortinet.com