Creating Content Packs in vCenter Log Insight 1.5

TECHNICAL WHITE PAPER
# Table of Contents

Introduction ................................................................. 4
Intended Audience ....................................................... 4
What’s New ................................................................. 4
Getting Started ........................................................... 4
  Instance ................................................................. 4
  User ................................................................ 5
  Events ................................................................. 5
  Authors ............................................................... 5
Queries ......................................................................... 5
  Saving Queries ....................................................... 6
  Message Queries .................................................... 7
  Field Queries ......................................................... 8
    Temporary Fields ................................................ 9
Aggregation Queries ..................................................... 10
  Bar Charts ............................................................ 10
  Line Charts ........................................................ 11
  Stacked Charts ..................................................... 11
  Multi-Colored Charts ............................................ 13
  Message Queries .................................................... 14
Alerts ........................................................................ 14
  Thresholds ............................................................ 14
Dashboards ................................................................. 15
  Dashboard Groups .................................................. 15
  Dashboard Widgets ................................................ 16
    Chart ............................................................... 17
    Query List ........................................................ 18
    Widgets ........................................................... 19
Content Packs ............................................................ 21
  View ................................................................. 21
  Export ............................................................... 22
  Import ............................................................... 23
  Edit ................................................................. 25
  Publish ............................................................. 25
Conclusions .................................................. 27
Getting Started ............................................. 27
User ............................................................... 27
Queries ........................................................... 27
Message Queries .............................................. 27
Field Extraction ............................................... 27
Aggregation Queries ........................................ 27
Alerts Queries .................................................. 27
Dashboards .................................................... 28
Dashboard Groups .......................................... 28
Dashboard Widgets ......................................... 28
Content Packs ................................................ 28
Resources ....................................................... 28
Acknowledgments .......................................... 28
About the Author ............................................. 28
Appendix ......................................................... 29
Orphaned Fields .............................................. 29
Introduction

Content packs are immutable, or read-only, plugins to vCenter™ Log Insight™ that provide pre-defined knowledge about specific types of events such as log messages. The goal of a content pack is to provide knowledge about a specific set of events in a format easily understandable by administrators, engineers, monitoring teams, and executives. A content pack should answer questions like, “Is the product/application healthy?” In addition, a content pack should create a greater understanding of how the product/application works.

A content pack is made up of information that can be saved from either the Dashboards or Interactive Analytics pages in Log Insight. This includes:

- Queries
- Fields
- Aggregations
- Alerts
- Dashboards

By default, the current version of Log Insight ships with the VMware - vSphere content pack, and other content packs can be imported as needed. Any Log Insight user can create a content pack for private or public consumption.

Intended Audience

This paper provides information about each piece of information that can be saved in a content pack as well as best practices for content pack creation. The information provided is specifically tailored to content pack authors using Log Insight 1.5. Content pack authors using Log Insight 1.0 are encouraged to upgrade to Log Insight 1.5 or refer to the Creating Content Packs in vCenter Log Insight technical white paper.

What’s New

Several enhancements have been made in regards to content pack creation and thus the reason for this updated technical white paper. Some changes to be aware of include:

- Query List widgets can be saved in content packs
- Editing a field now updates queries leveraging said field
- Orphaned fields are now called temporary fields and are no longer be contained in content packs
- Content packs can be imported into user space for editing
- Custom dashboards can be selectively exported into content packs
- Content pack objects can be selectively imported into custom dashboards

Given the enhancements in Log Insight 1.5, several best practices for content pack creation have been changed. Some changes to be aware of include:

- No longer need to save instance of Log Insight used to create a content pack, instead an exported content pack can be imported into any Log Insight instance for editing

Getting Started

Before explaining how to create a content pack, it is important to understand some concepts regarding the content pack workflow. The tips in this section will make creating and maintaining content packs easier.

Instance

Content pack files can be imported as a content pack by Log Insight admin users or imported into user space by any user. If a content pack is imported as a content pack then it cannot be edited. If a content pack is imported

---

1 Please note this information is different from Log Insight 1.0.
into user space then the objects contained within a content pack can be selectively imported under My Content for the given user. Importing a content pack into user space allows for content packs to be edited within a Log Insight instance. An exported content pack file is all that is needed to publish or modify a content pack.

**User**

Content packs are created in part from the content saved under Custom Dashboards, also known as user space, or more specifically either My Dashboards or Shared Dashboards on the Dashboards page. While objects from a custom dashboard can be selectively exported, it is recommended that every individual content pack be authored by a separate user entity in Log Insight to ensure a clean user space per content pack. For information on creating users in Log Insight, please refer to the Log Insight documentation.

**Events**

It is essential to collect relevant events before attempting to create a content pack to ensure that a content pack covers all relevant events for a product/application. One common way to collect relevant events is to ask quality assurance (QA) and/or support teams as these teams usually have access to, and knowledge about, common events. Attempting to generate events while creating a content pack will be time consuming and will likely result in missing important events. If QA and support teams are unable to supply events, simulated events may be used instead if product/application events are known and/or documented.

Once appropriate logs have been collected, they must be ingested into Log Insight. While not supported in the current version of Log Insight, it is possible to ingest events from the command line using the same process as the archive import process described in the Log Insight documentation. In short, any file, directory, tarball, or . ZIP can be ingested by copying the events to the Log Insight virtual appliance and running:

```
/usr/lib/loginsight/application/bin/loginsight repository import /path/to/events
```

While this process is not supported, it will work and is recommended when creating a content pack.

**Authors**

The authors of a content pack should have qualifications as outlined below.

- Experience using VMware vCenter Log Insight.
- Real world operating knowledge of the product/application.
- Understanding and ability to generate optimized regular expressions.
- Experience debugging multiple problems with product/application using logs.
- Support background, with exposure to a myriad of problems.
- System administrator background with previous syslog experience.

**Workflow**

The recommended approach for content pack creation is to start on the Interactive Analytics page and begin querying for specific types of events such as error or warning. Upon looking at the results of the queries, potential field candidates should be analyzed and extracted as appropriate. With some understanding of the types of events and useful pieces of information available in the events, relevant queries should be constructed and saved as appropriate. For queries that highlight an issue that should be acted on quickly, alerts should be created and saved. As queries are saved, they should be removed from the results list using a constraint to show other events that may be potential candidates for new saved queries. Once all relevant queries are saved, the queries should be organized and displayed in a logical manner on the Dashboards page. The process of constructing and saving queries as well as the minimum requirements for content packs are listed in the following sections.

**Queries**

Log Insight allows for queries to retrieve and summarize events. Queries can be created and saved from the Interactive Analytics page. A query is made up of one or more of the following:

- **Keywords**: Complete, or full-text, alphanumeric, hyphen, and/or underscore matches.
- **Globs**: Asterisk and/or question mark symbol used to match some quantity of keywords.
- **Regular expressions**: Sophisticated string pattern matching based on Java regular expressions.
Creating Content Packs in vCenter Log Insight 1.5

- **Field operations**: Keyword, regular expression, and pattern matches applied to extracted fields.
- **Aggregations**: Functions that are applied to one or more subgroups of the results.

Log Insight supports the following types of queries:

- **Message**: A query made up of keywords, regular expressions and/or field operations.
- **Regular expression or field**: A query made up of keywords and/or regular expressions.
- **Aggregation**: A query made up of a function, one or more groupings, and any number of fields.

Custom alerts can be defined in Log Insight and are triggered from scheduled queries of any type.

**Saving Queries**

Queries can be saved via one or more of the following:

- **Add to Dashboard**: Saves the last run query without time range as a chart widget in a dashboard group on the Dashboards page.
- **Save Current Query**: Saves the last run query with time explicit time range as a loadable query on the Interactive Analytics page. Queries saved using Save Current Query and exported as part of a content pack do not include any time range.

**Add Current Query to Dashboard**: Saves the last run query without time range as a chart widget or query list widget in a dashboard group on the Dashboards page.

The notes section is very important and should be populated for every query. Information added can be text, a link to documentation, a knowledge base article, or a forum. Information provided in the notes section should answer the following questions:

- Why is this widget important?
- What is a “good” and “bad” value?
- Where can more information be obtained?
It is highly recommended to provide enough information in the notes section to understand the importance of
the saved query in addition to providing a link to more information even if that means duplicating the information
available in the link. The goal is to provide as much value within the Log Insight product as possible and link to
additional information should the user want to learn more.

Message Queries
Message queries can be entered via one or more of the following:

• Search bar: The search bar is one way to refine the results returned given the existing events in a Log Insight
  instance. While a constraint can be used instead of the search bar, it is often easier to understand a query that
  leverages the search bar over an equivalent constraint. As such, the best practice is to use the search bar
  versus an equivalent constraint whenever possible.

• Constraints: A constraint allows for querying using a regular expression, a field, logical OR operation,
  or a combination of search bar and constraint queries.

While query building is outside the scope of this document, there are several important things to know about
the search bar and constraints when creating content packs. In general, the following best practices apply:

• Ensure queries are not environment specific. Public content packs should be generic to any environment
  and as such should not rely on environment specific information. Examples of environment specific information
  include source, hostname, and potentially facility if the facility uses local*.

• When constructing a query, use keywords whenever possible, when keywords are not sufficient use globs,
  and when globs are not sufficient use regular expressions. Keyword queries are the least resource intensive
  type of query. Globs are a simplified version of regular expression and are the next least resource intensive
  type of query. Regular expressions are the most intensive type of query.

• Avoid regular expressions whenever possible. If the query can be written without regular expressions
  then it should be written without regular expressions primarily because, from a resource perspective,
  regular expressions are the most expensive type of query. Leverage globs instead of regular expressions
  when keywords are not sufficient.
• **Provide as many keywords as possible.** When using regular expressions or fields, be sure to include as many keywords as possible. Any keywords should be outside of any regular expressions including a logical OR like: (this|that). Regular expressions use a lot of resources. Keyword queries are the least resource intensive type of query and Log Insight is optimized to perform keyword queries prior to regular expressions to minimize regular expression overhead.

Field Queries
Fields are a powerful way to add structure to unstructured events and allow for the manipulation of both the textual and visual representation of data. Fields are one of the most important items in a content pack as they can be used in multiple ways including:

• **Aggregations:** Allow for functions and groupings to be applied to fields.
• **Constraints:** Allow for operations to be performed against fields.

Any part of a log message that might be applicable to a query or aggregation should be extracted. Fields are a type of regular expression query and are especially useful for complex pattern matching so the user does not need to know, remember, or learn complicated regular expressions.

• **Regex before value:** This field should include as many keywords as possible. If this field is empty or only contains special characters, then the **Regex after value** must include keywords.
• **Regex after value:** This field should include as many keywords as possible. If this field is empty or only contains special characters, then the **Regex before value** must include keywords.
• **Name:** Only use alphanumeric characters. Ensure all characters are lower case and use underscores instead of spaces as this makes fields easier to view. Important: Names for content pack fields and user fields can be the same though content pack fields will have a namespace in parenthesis to the right of the field name. It is recommended to prefix content pack fields with an abbreviation (e.g. vmw_ _) to avoid confusion.

In addition to the various components that make up a field, several best practices must be considered. These include:

• **Only create fields for regular expression patterns.** If a field can be queried using keyword queries, or will only ever return a single value, then keyword queries should be used instead of a pre-defined field. If a field will only return two values then consider constructing individual queries instead of extracting a field. Fields are meant to add structure to unstructured data as well as provide a way to query over specific parts of an event.

![Figure 9](image1.png) An example of two different ways to construct the same query. The first constraint is a regular expression while the second is a keyword, comma separated, logical OR match. The second constraint is always preferred over the first.

![Figure 10](image2.png) An example of two different ways to query for the same field. The first constraint is generic and only contains two keywords. The second constraint is very specific and has five keywords. The second constraint is always preferred over the first.

![Figure 11](image3.png) An example of an extracted field definition with multiple keywords.

![Figure 12](image4.png) The recommended way to query for keyword matches. Information entered into the search bar or a constraint can also be saved for future usage by selecting the menu drop-down next to the Search button and selecting Save Current Query...
• Only create fields for regular expression patterns that return a fraction of the total events. Fields that will match most events and/or return a very large number of results are not a good candidate for field extraction because the regular expression will need to be applied to a large quantity of events resulting in a resource-intensive operation. If additional keywords can be added to reduce the number of results returned then the additional keywords should be added to optimize the query.

• If a field contains keywords within regular expression syntax then such keywords should be added as a constraint without regular expression syntax. For example, if the value or the context of a field contains keywords within regular expression syntax such as (this|that) then the keywords should be added as a text constraint to optimize the query like text contains this, that.

Temporary Fields
Starting with Log Insight 1.5, orphaned fields are now referred to as temporary fields. A temporary field is a field that exists as part of a query, but is not saved globally within a Log Insight instance or as part of an installed content pack. Log Insight 1.5 reduces the chances of creating a temporary field by automatically updating the query that relies on a field being modified.

In Log Insight 1.5, if a field that a saved query relies on is deleted then the saved query will contain a temporary field.

---

2 This information only applies to Log Insight 1.5 and greater.
3 For more information on orphaned fields and how they functioned in Log Insight 1.0 please see the appendix.
Temporary fields are noticed when running a saved query on the Interactive Analytics page and a field used in the saved query contains the namespace Temporary to the right of the field name.

It is common for queries to contain one or more fields. For saved queries created in Log Insight 1.5, it is important to note that the field definition used when a query is saved will be modified if the field is modified. Field modifications would include:

- The value of the field is changed
- The regex before value and/or the regex after value of the field is changed
- The name of the field is changed
- The field is deleted

When exporting a content pack in Log Insight 1.5, Log Insight ensures that all temporary fields are converted to content pack fields. This means that content packs created in Log Insight 1.5 will not contain temporary fields. If a temporary field is seen for an imported content pack in Log Insight 1.5 then that means either the content pack was created in Log Insight 1.0 and exported with orphaned fields or the content pack was manually edited.

**Aggregation Queries**

Log Insight allows for visual manipulation of events through the use of aggregation queries. An aggregation query is made up of two distinct attributes:

- Functions
- Groupings

In content packs, groupings are the most important consideration, but both functions and groupings will be addressed as they impact how charts are displayed. An aggregation query requires one function and at least one grouping.

**Bar Charts**

By default, the Interactive Analytics page of Log Insight displays a count of events over time in the overview chart. If the count function is used in conjunction with the time series grouping, then a bar chart is created.
If the count function is used in conjunction with a single field grouping instead of time series, then a bar chart is created with quantities listed from greatest to least.

**Line Charts**

All functions, except the count function, are mathematical and require a field to apply the equation against. When performing a mathematical function on a field and grouping by time series, a line chart is created.

**Stacked Charts**

By default, the overview chart on the Interactive Analytics page of Log Insight is a count of events over time. If one field is added to the time series grouping, then a stacked chart is created.
If grouping by time series plus a field and any function except count is used, a stacked line chart is created.

![Stacked Line Chart Example](image1)

**Figure 21.** An example of a stacked line chart using average of a field over time grouped by a field.

Stacked charts are powerful when attempting to find anomalies for an object. Consideration needs to be taken based on the number of objects that could be returned. In general, the following best practices apply:

- If the number of objects per bar returned will be <10, then stacked charts are encouraged.
- If the number of objects returned per bar is or could be 10-20, then stacked charts can be good, but consideration must be taken when visually representing the chart in a content pack.
- If the number of objects returned per bar is or could be >20, then stacked charts are discouraged.

![Stacked Bar Chart Example](image2)

**Figure 22.** An example of a stacked line chart with a small number of objects. The chart is easy to read and understand.

The reason for the above recommendations is because more objects mean more resources necessary to parse and display information. In addition, there are a fixed number of colors or primary colors, 9 in the current version, and even with the different shades available, distinguishing between objects may become challenging depending on the number of objects returned.

![Bar Chart Example](image3)

**Figure 23.** An example of a stacked bar chart with a large number of objects. The chart is hard to read and understand.
Multi-Colored Charts

If a grouping is created using more than one field and time series, then a multi-colored chart is created. The chart will consist of two colors that interchange. Each interchange represents a new time range. Multi-colored charts can be hard to interpret so the value of such a chart should be considered before including it in a content pack.

When grouping by multiple fields, consider removing the series, listed as over time, for a more easily understood bar chart.

If multiple fields are important given a time range, then multiple charts could be created for each field individually over the time range. The charts could then be displayed in the same column of a dashboard group in a content pack.

Figure 24. An example of a multi-colored bar chart using count of events over time grouped by two fields.

Figure 25. An example of a multi-field grouping bar chart using count of events grouped by two fields.

Figure 26. An example of two similar charts stacked. Notice how one red alarm in blue matches mostly pink sources.
**Message Queries**

When constructing an aggregation query, the message query should only return results relevant to the aggregation query. This makes analyzing easier and ensures only relevant fields are shown. To ensure the message query returns the same results as the aggregation query, ensure that constraints using the `exists` operator are added for each field used in the aggregation query.

![Figure 27](image1.png) An example of an aggregation query without a message query. This is not recommended.

![Figure 28](image2.png) An example of an aggregation query with a message query. This is recommended.

**Alerts**

Alerts provide a way to trigger a reaction when a certain type of event is seen. Log Insight supports two different types of alerts natively:

- Email
- vCenter Operations Manager

Alerts can only be saved in user space and as such, all content pack alerts are disabled by default. If an enabled alert is created and then exported as part of a content pack, then the alert will be disabled in the content pack. This means that email and/or vCenter Operations Manager settings are not contained and cannot be added to a content pack.

**Thresholds**

It is important to understand how thresholds work to ensure that, if enabled, a content pack alert does not unintentionally spam a user. When considering a threshold, there are two things to keep in mind:

- **How frequently to trigger the alert**: Log Insight comes with pre-defined frequencies. Alerts will only trigger once for a given threshold window.

![Figure 29](image3.png) An example of an alert. The threshold has been set to trigger when one red vCenter Server alarm for any type is seen in the last hour. The query runs every 10 minutes and if the alert triggers, it will not run again for one hour.
Creating Content Packs in vCenter Log Insight 1.5

- **How often to check if an alert state has occurred:** An alert is triggered by a query. Alerts, just like queries, are not real-time in the current version. For each threshold window, a pre-determined query frequency has been allocated. Changing the threshold will change the query time.

**Dashboards**

**Dashboard Groups**

A content pack is made up of one or more dashboard pages known as dashboard groups.

A dashboard group can be created in the following ways:

- **Dashboards page**
  - Select *New Dashboard* option in one of the custom dashboards

- **Interactive Analytics**
  - Select *Add to Dashboard*
  - Select *Add Current Query to Dashboard* from the menu drop-down next to the search button

Dashboard groups can be reordered by dragging and dropping the handle widget to left of the dashboard.

**Figure 30.** The vSphere content pack. In the left navigation bar, below the name of the content pack, are the dashboard groups.

**Figure 31.** New Dashboard button.

**Figure 32.** Add to Dashboard dialog box with New Dashboard selected.

**Figure 33.** Add Current Query to Dashboard dialog box with New Dashboard selected.

**Figure 34.** Example of dashboard group reordering.
When creating dashboard groups, the following best practices apply:

- Content packs commonly contain a minimum of 3 dashboard groups. The best practice is to start with an overview dashboard group to provide high-level information about the events for a particular product or application. In addition to the overview dashboard group, dashboard groups should be created based on logical groupings of events. The logical groupings are product-specific or application-specific, but some common approaches are: performance, faults, and auditing. It is also common to create dashboard groups per component like disk and controller. With the component approach, it is important to note that it is only effective if queries can be constructed to return results from specific components. If this is not possible, then the logical approach is recommended.

- When naming dashboard groups, make the title generic and avoid adding product-specific or application-specific names unless being used in a component-specific fashion. For example, in the VMware - vSphere content pack, there is a dashboard group called ESX/ESXi instead of VMware ESX/ESXi.

- A dashboard group should contain a minimum of 3 dashboard widgets and a maximum of 6 dashboard widgets. With any less than 3 dashboard widgets the amount of knowledge that can be attained by the dashboard group is minimal. In addition, having a lot of dashboard groups with only a limited amount of dashboard widgets requires a user to switch between different pages and does not provide information in a coherent way. Conversely, any more than 6 dashboard widgets per dashboard group can result in the following:
  - Too much information: A user may not know where to start or what is most important.
  - Resource intensive: Each widget is a query that needs to be run against the system.

When exceeding 6 dashboard widgets in a dashboard group, separate information and create multiple dashboard groups. If a dashboard widget is applicable to one or more dashboard groups, it is recommended to create the widget in each applicable dashboard group.

Dashboard Widgets

There are two different types of dashboard widgets in the current version of Log Insight:

- **Chart**: contains a visual representation of events with a link to a saved query.
- **Query List**: contains title links to saved queries.

---

**Figure 35.** An example of a chart widget.

**Figure 36.** An example of a query widget.
Chart

A dashboard chart widget contains a visual representation of events. A chart can either be represented as a bar or line chart and either can be displayed in a stacked fashion. The following best practices apply:

• Charts can contain a lot of information so avoid having more than two chart widgets per row. In some rare cases, three chart widgets can be used effectively, but more than three is strongly discouraged. When determining whether chart widgets are readable or not, be sure to use the minimum resolution supported by Log Insight (1024 x 768) as one cannot assume that users of the product will have a better resolution.

• If any row except the last row has a single chart widget, then it is recommended to make that widget full-width.

• When naming a chart widget, use a descriptive title and avoid cryptic field names. For example, an extracted field is called vmw_error_message. Instead of calling a chart Count of vmw_error_message, call it Count of error messages.
Similar charts can be saved and stacked in the same column of a dashboard group for visual comparison. Examples of such charts include:

- Average X of events over time + Maximum X of events over time. Given the different functions used, it is possible that the Y-axis of the charts will not be the same scale.
- Count of events over time grouped by X + Count of events over time grouped by Y.

Query List

A dashboard query list widget contains one or more links to a pre-defined query. Query list widgets can be used for a variety of reasons including:

- When a chart widget does not provide significant value, but the underlying query does
- To save complex queries such as those using regular expressions
- To use different aggregations on the same underlying query within a dashboard group

---

4 Please note this information is different from Log Insight 1.0.
Widgets

Widgets can be modified in a variety of ways including:

• **Rename**: To rename a widget, select the name of the widget. When naming a chart widget, use a descriptive title and avoid cryptic field names.

• **Resize**: To resize a widget, hover over the right edge of a widget’s contents.

• **Reorder**: Query list widget links can be reordered within a query widget by dragging and dropping a link. Links cannot be moved between query list widgets.

• **Move**:
  - **Within a dashboard group**: To move a widget within a dashboard group, select between the title and the action buttons and drag to the new location. It is not possible to create a new row between two existing rows.

  Instead, move the widget to the left-most position of the row below the row desired and move all widgets after the new widget down.

---

5 Please note this information is different from Log Insight 1.0.
- **Between dashboard groups:** To move a widget between dashboard groups, select the gear action button followed by *Move to Dashboard*.

- **Clone:** To clone a widget, select the gear action button followed by *Clone*. When cloning a chart widget, any fields the chart relies on are not cloned. Instead, cloned chart widget fields are defined by the cloned source. For this reason, cloned widgets should not be used in content packs as they may cause content packs to be dependent on other content packs.

- **Edit Information:** To edit the notes section of a widget, select the i button followed by *Edit*.
The notes section is very important and should be populated for every dashboard widget. Information added can be text, a link to documentation, a knowledge base article, or a forum. Information provided should answer the following questions:
- Why is this widget important?
- What is a “good” / “bad” value?
- Where can more information be obtained?

The underlying query for a widget cannot be modified. In order to change the underlying query, a new widget needs to be created and the old widget needs to be deleted. For chart widgets, the directions are:
- Go to the widget on the Dashboards page.
- Select the Open in Interactive Analytics arrow button within the widget.
- Modify the query as desired.
- Select the Add to Dashboard button on the Interactive Analytics page.
- Select the Delete button from the gear button within the old widget from the Dashboards page.

Content Packs

With an understanding of what makes up a content pack and the best practices when performing each operation, it is now time to view, export, import, edit, and publish the content.

View

To view saved content:
- Navigate to the Content Packs section by selecting the gear icon in the navigation bar and selecting Content Packs.
• Select where the content was saved. For content pack authors, content is saved under *Custom Content* and, if following the best practices in the Getting Started section of this document, saved content will appear under *My Content*.

In general, a content pack should have:

• 3+ Dashboards (dashboard groups)
• 3+ Queries (chart widgets) per dashboard (9+ total)
• 5+ Alerts
• 20+ Extracted Fields

**Export**

To export saved information within a particular set of content:

• Select the content, select the gear icon to the right of the content name, and select *Export*.
• Select what objects to export.
• Enter a name for the content pack. The recommended format is: `<Company> - <Product> [<VersionsSupported>]` (e.g. VMware - vSphere).
• If this content pack is for public consumption:
  - Enter a namespace for the content pack. The recommended format is: `<Ext>.<Domain>.<Product>` (e.g. com.vmware.vsphere).
  - Enter author information. It is recommended to enter the company name here.
  - Enter URL information. It is recommended to enter the company URL here.
  - Enter a description as to what the content pack contains and how it brings value.
  - Upload a logo for the content pack
• If the content pack is for private consumption:
  - Entering a namespace for the content pack is optional.
  - Entering author information is optional.
  - Entering a URL is optional.
  - Entering a description is optional.
  - Uploading a logo is optional.
• Select **Export**.

Once done, a file ending in VLCP, which stands for **vCenter Log Insight Content Pack**, will be downloaded.

---

**Figure 55.** How to export a content pack.

---

**Import**

- Select the **Import Content Pack** button in the bottom of the left navigation bar.
- Select **Browse...** to specify the location of the VLCP file.

---

**As Content Pack**

Only **Admin Users** can import a content pack as a content pack. To import a content pack as a content pack:

- Select **Install as content pack**.
- Select **Import**.

---

**To User Space**

Any user can import a content pack into user space. To import a content pack into user space:

- Select **Import into My Content**.
- Select **Import**.

---

Please note this information is different from Log Insight 1.0.
• Select what objects to import. Please note that field dependencies are automatically selected to ensure no temporary fields exists.

Errors/Warnings
When importing a content pack, some warning/error events can occur. These include:

• **Upgrade:** An Upgrade means that another content pack is installed in the system that has the same namespace. In this case, the options are to either choose Upgrade to replace the existing content pack or Cancel to keep the existing content pack.

• **Invalid Format:** Invalid Format means that the VLCP file was manually edited and contains syntax errors. The syntax errors need to be fixed before the content pack can be imported. As VLCP files should not be manually edited, there is no easy way to locate and fix syntax errors.

• **Newer Version:** Newer Version means that this content pack was created and is only supported on a newer version of Log Insight. As of Log Insight 1.5 this feature has not been implemented so seeing this error message means that the VLCP file was manually edited.

• **Unrecognized Version:** Unrecognized Version means that the VLCP file was manually edited and contains syntax errors. The syntax errors need to be fixed before the content pack can be imported. As VLCP files should not be manually edited, there is no easy way to locate and fix syntax errors.

7 Please note this information is different from Log Insight 1.0.
Edit

Content packs imported as content packs are immutable, or read-only. It is possible to clone content pack dashboard widgets to custom dashboards, also known as user space, however the cloning operation does not clone extracted fields. The recommended way to edit content pack is to import them into user space.

Publish

Once a content pack has been created, it can be published on the Log Insight marketplace, which is located on VMware Solution Exchange. The requirements for content pack publishing are as follows:

- **Content pack**: A VLCP file.
- **Events**: Appropriate events necessary to validate content pack.
- **Overview**: A one-paragraph overview of the content pack.
  
  An example from the VMware vSphere content pack:

  The VMware vSphere content pack provides deep knowledge of vSphere logs and powerful insight, allowing for informed and proactive decisions within an environment.

- **Highlights**: Three bullets that highlight the value of the content pack.
  
  An example from the VMware vSphere content pack:

  - Proactive monitoring of vSphere environment
  - Change tracking and auditing
  - Additional information and context

- **Description**: A one or more paragraphs describing the value of the content pack.
  
  An example from the VMware vSphere content pack:

  The vSphere content pack provides you with important information about your vSphere environment from ESX/ESXi logs, vCenter Server logs, and vCenter Server events, tasks, and alarms. The content pack enables:

  Proactive monitoring of your vSphere environment

  Quickly identify issues and drill down to determine the root cause with powerful visualizations of your data and targeted queries.

  Change tracking and auditing

  Track user-initiated changes and automated vSphere actions. Understand how your environment is being used.

  Additional information and context

  Each dashboard widget includes information about the widget with links to documentation, knowledge base articles, or any other information that might be applicable.

---

8 Please note this information is different from Log Insight 1.0.

9 Please note this information is different from Log Insight 1.0.
• **Tech Specs:** The minimum requirements to use the content pack. An example from the VMware vSphere content pack:

*The following are the prerequisites for using the VMware vSphere content pack:*  

- VMware vCenter Log Insight  
- VMware ESX/ESXi 4.x or newer  
- VMware vCenter Server 4.1 or newer  
- VMware vCenter Server integration

• **Video:** Example of how the content pack brings value (e.g. YouTube video).  

• **White Paper:** How to configure the product/application to forwards logs to Log Insight

The content pack itself must meet the following requirements:

• **Content**  
  - Minimum of three dashboard groups  
  - Minimum of three dashboard widgets per dashboard group  
  - Maximum of six dashboard widgets per dashboard group  
  - Maximum of three dashboard widgets per row  
  - Minimum of five alerts  
  - Minimum of 20 extracted fields

• **Quality**  
  - Every query has at least one full-text keyword and ideally three or more keywords  
  - Queries are not based on environment specific attributes like source, hostname, or local*  
  - Every field has at least one full-text keyword and ideally three or more keywords  
  - Fields are specific to product/application and will not return results for other product/application logs  
  - Every dashboard widget must contain information/links on what the chart shows and why it is important

• **Standards**  
  - Content pack name format: `<Company> - <Product>`  
  - Content pack namespace format (content pack must be exported with namespace): `<Ext>.<Domain>.<Product>`  
  - Extracted field format: `<Prefix> _ <Field> _ <Name>`

Once all the information to publish a content pack has been collected, perform the steps below to submit the content pack on VMware Solution Exchange:

• Go to [http://solutionexchange.vmware.com](http://solutionexchange.vmware.com)  
  - If you already have a username and password, click the Log In Now link in the top right corner of the page. Enter your username and password and click the Log In Now button.  
  - If you do not have a username and password, click the Register Now button and select Register Now under the Partner Registration Request section. Fill out the required information within the Partner Registration Request and submit. You will receive a notification email if your login request is approved.

• Once logged in you will be able to update or add new listing by clicking on Administration. This will take you to the Administration menu where you will be able to make changes to your personal account information, your company profile information, and add/edit a solution on your VSX profile.

• Choose Manage Solutions from the Administration menu.  
  - Find the solution that you are looking to edit, choose Edit under Actions and proceed to edit your solution.  
  - If your solution is not listed, click Add Solution to begin a new listing. Make sure to use the Save Draft button frequently, just to make sure that you do not lose any of your work. Once you have completed your solution listing, click Submit For Approval. This will send your solution listing to the VSX Alliance Team to be reviewed for approval. You will receive an email regarding the approval of your solution, or information about why your solution may have been declined, along with information about what changes need to be made in order to get it approved.
• For more information about completing a solution listing:
  - Select the Partner Corner link on the top of the site.
  - If you are unable to find the information that you need within this Getting Started site please feel free to contact VSXAlliance@vmware.com with any questions.

Conclusions
Content packs are a powerful way to extend the knowledge contained within Log Insight. When creating a content pack, several best practices must be considered as outlined below.

Getting Started
User
• Use a separate content pack author user on Log Insight for every content pack being created.

Queries
Message Queries
• Use keyword queries whenever possible.
• If keyword queries are not sufficient use globs.
• Use regular expressions only if keywords and globs are not sufficient. When using regular expressions, provide as many keywords as possible. All queries should contain at least one keyword and ideally at least three keywords.
• Make queries as specific as possible. Content pack queries should only match events applicable to the product/application for which the content pack was designed.

Field Extraction
• Minimize the amount of regular expressions used whenever possible.
• Confirm that the regular expression value will match every applicable log message (e.g. IP and FQDN).
• Provide as much pre-keyword and/or post-keyword context as possible with at least one keyword and ideally at least three keywords.
• If keywords are contained within regular expression syntax then a constraint querying for the keywords without regular expression syntax should be used.
• When naming a field:
  - Use the following naming standard: <prefix> _ <field> _ <name>
  - Use underscore instead of space.
  - Use all lowercase letters.
  - <prefix> = something applicable to the content pack.

Aggregation Queries
• When grouping by time series, do not add more than one field.
• Do not group by time series and one field if the number of unique fields is or could be over 20.
• When grouping by more than one field and time series, ensure the time series adds value.
• If the time series is important for more than one field, consider creating individual charts per field and per time series and save charts in the same column of a dashboard group.
• When constructing aggregation queries, ensure message queries return equivalent results.

Alerts Queries
• Create alerts primarily for critical events.
• Limit alerts using thresholds. In general, the user should not get more than 6 alerts per hour.
• Any saved alerts will be disabled once exported as part of a content pack. Email and/or vCenter Operations Manager definitions will not be included in a content pack.
• Be sure to enter descriptive information about the alert so the user will know why it is important.
Creating Content Packs in vCenter Log Insight 1.5

Dashboards

Dashboard Groups
- Consider starting with an overview dashboard group.
- Create dashboard groups based on a specific type of message (e.g., overview, performance, etc.) and not based on a specific type of component (e.g., compute, network, storage).
- It is recommended to duplicate the same dashboard widget in multiple dashboard groups if the dashboard widget is applicable in each dashboard group.
- Target at least 3 dashboard groups in a content pack.
- Dashboard groups and query list widget links can be reordered; dashboard widgets can be moved.

Dashboard Widgets
- Target at least 3 dashboard widgets per dashboard group.
- Do not put more than 3 dashboard widgets in the same row.
- Do not put more than 6 dashboard widgets in a dashboard group.
- When displaying similar information in different formats, ensure each format brings value.
- Stack related dashboards together for easier viewing.
- Give the dashboard widgets descriptive names. Do not use field names in widget titles.
- Include notes for every dashboard widget. Ensure the notes answer questions such as, “Why is the widget important?” and “Where can additional information be found?”
- The query definition of a dashboard widget cannot be modified. Instead, a new widget needs to be created and the old widget needs to be removed.

Content Packs
- A content pack should contain a minimum of 3 dashboards, 9 total widgets, 5 alerts, and 20 fields.
- When exporting a content pack use the naming format: `<Company> - <Product>`
  Ideally, the content pack name should be under 30 characters to prevent word wrapping.
- When exporting a content pack for publishing, export with a namespace in format: `<Ext>.<Domain>.<Product>`

Resources
More information about Log Insight and Log Insight content packs can be found using the links below.
- VMware vCenter Log Insight documentation: http://pubs.vmware.com/log-insight-15/index.jsp
- VMware vCenter Log Insight communities: http://loginsight.vmware.com
- VMware vCenter Log Insight marketplace: https://solutionexchange.vmware.com/store/loginsight

Acknowledgments
The author would like to thank the following individuals for their technical review of this white paper:
Jon Herlocker, Spiros Xanthos, Chengdu Huang, Chris Blinn, and Chris Todd.

About the Author
Steve Flanders is a Senior Solutions Architect at VMware. He has an extensive background in designing and implementing cloud solutions with focuses on ensuring scalability and promoting a cloud vision. Steve has helped architect several cloud offerings including VMware’s Cloud Foundry, AT&T’s Synaptic Storage as a Service, and EMC’s Atmos Online. Steve is the author of SFlanders.net, a technology-centric weblog focusing on a variety of topics including cloud computing, virtualization, and system administration.
Appendix

Orphaned Fields

An orphaned field is a field that exists as part of a query, but is not saved globally within a Log Insight instance or as part of an installed content pack. If a field that a saved query relies on is modified in Log Insight 1.0 then the query will contain an orphaned field. Orphaned fields are noticed when running a saved query on the Interactive Analytics page and a field used in the saved query is opened in a green dialog box under the Fields section.

It is common for queries to contain one or more fields. For saved queries created in Log Insight 1.0, it is important to note that the field definition used when a query is saved is always maintained. This means if a query is saved with a field and that field is later modified, then the query will not be modified. Field modifications would include:

- The value of the field is changed
- The regex before value and/or the regex after value of the field is changed
- The name of the field is changed
- The field is deleted

It is critical that saved queries that leverage a field be recreated if the field is modified. If a previously saved query is not updated when a field it relies on is modified, then the saved query will contain an orphaned field. An orphaned field is a field that exists in a saved query, but does not exist as an available field. Orphaned fields are apparent when running a saved query in the Interactive Analytics page, as a green field dialog box will be open under the Fields section. Important: Saving, deleting, closing, or modifying the open dialog box will result in any use of the orphaned field being removed from the query.

Figure 65. An example of a keyword field. Since this query can be constructed without a regular expression, it is not a good candidate for field extraction.

Figure 66. An example of running a saved query with an orphaned field. Notice how the overview chart is grouped by security_host and the security_host field definition is open under the Fields section. This means the field does not exist in the Log Insight instance, but does exist as part of a chart widget or saved query.

Figure 67. An example of what happens when an orphaned dialog box is closed. Notice how the search bar remains the same, but the overview chart is no longer grouped by security_host. In addition, security_host is not listed under the Fields section.

10 This information only applies to Log Insight 1.0.
Ensure that content pack queries do not contain orphaned fields. If an orphaned field is found, recreate the saved query and delete the old saved query to remove the orphaned field. To remove an orphaned field from a chart widget:

- Go to the widget on the Dashboards page.
- Select the *Open in Interactive Analytics* arrow button within the widget.
- Modify the field(s) used.
- Select the *Add to Dashboard* button on the Interactive Analytics page.
- Select the *Delete* button from the gear button of the old widget from the Dashboards page.