Administering vRealize Log Insight

12-OCT-2017

vRealize Log Insight 4.5

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Administering vRealize Log Insight

Administering vRealize Log Insight provides information about administering VMware® vRealize™ Log Insight™, including how to manage user accounts and how to integrate Log Insight Agents with other VMware products. It also includes information about managing product security and upgrading your deployment.

The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

Updated Information for *Administering vRealize Log Insight*

Administering vRealize Log Insight is updated with each release of the product or when necessary.

This table provides the update history of *Administering vRealize Log Insight*.

Revision	Description
10-OCT-2017	■ Removal of note about deprecation of support for Active Directory. ■ Minor bug fixes.
05-SEP-2017	■ Clarification of hardware requirements.
002541-1	■ Revisions provide clarification of support status for external load balancers and native Active Directory use. See Working with an Integrated Load Balancer and Chapter 3 Configuring Authentication.
002541-0	Initial release.

1 Upgrading vRealize Log Insight

Depending on the current version of vRealize Log Insight, you can upgrade to a newer version.

This section includes the following topics:

vRealize Log Insight Upgrade Path

The upgrade path and procedure to follow varies with the installed version of vRealize Log Insight that you want to upgrade.

You can also check supported upgrade paths using the **Upgrade Path** feature on the VMWare Product Interoperability Matrixes site.

vRealize Log Insight upgrades are incremental. You must upgrade to each intermediate release.

Table 1-1. Supported Upgrade Paths

Upgrade from	Upgrade to	Procedure
vRealize Log Insight 4.3	vRealize Log Insight 4.5	See Upgrade to vRealize Log Insight 4.5
vRealize Log Insight 4.0	vRealize Log Insight 4.3	See Upgrade to vRealize Log Insight 4.3
vRealize Log Insight 3.6	vRealize Log Insight 4.0	See Upgrade to vRealize Log Insight 4.0.
vRealize Log Insight 3.3	vRealize Log Insight 3.6	See Upgrade to vRealize Log Insight 3.6.

Upgrade to vRealize Log Insight 4.5

You can automatically upgrade a cluster to vRealize Log Insight 4.5.

Upgrading vRealize Log Insight must be done from the master node's FQDN. Upgrading using the Integrated Load Balancer IP address is not supported.

During the upgrade, the master node is upgraded first, and restarts. Then each of the cluster nodes is upgraded sequentially. You can see the current status of the rolling upgrade seen on the **Admin > Cluster** page. If the integrated load balancer is configured, its IPs are migrated among the cluster nodes so cluster services, including UI, API, and ingestion of incoming events, remain available throughout the rolling upgrade. Low-level details are written to the `upgrade.log` file on each individual node. A system notification is sent when upgrade completes successfully.

If an issue is encountered affecting one or more of the nodes during the upgrade process, the entire cluster is automatically rolled back to the original, working version. Because configuration changes performed after the upgrade started might be inconsistent or invalid, the configuration is reverted to a known-good state captured before upgrade. No ingested events are lost. Progress is written to `rollback.log` file on each individual node. A system notification is sent when rollback finishes. After the issue is investigated and fixed, you can retry the upgrade.

Prerequisites

- Verify that you are applying the upgrade for a supported upgrade path. See vRealize Log Insight Upgrade Path.
- Create a snapshot or backup copy of the vRealize Log Insight virtual appliance.
- Obtain a copy of the vRealize Log Insight upgrade bundle `.pak` file for the release you are upgrading to.
- Verify that you are logged in to the vRealize Log Insight*portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is https:///*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Management, click **Cluster**.
3. Click **Upgrade from PAK** to upload the `.pak` file.
4. Accept the new EULA to complete the upgrade procedure.

What to do next

After the master node upgrade process is complete, you can view the remaining upgrade process which is automatic.

Check for the email sent to the Admin to confirm the upgrade completed successfully.

Upgrade to vRealize Log Insight 4.3

You can automatically upgrade a cluster to vRealize Log Insight 4.3.

Upgrading vRealize Log Insight must be done from the master node's FQDN. Upgrading using the Integrated Load Balancer IP address is not supported.

During the upgrade, the master node is upgraded first, and restarts. Then each of the cluster nodes is upgraded sequentially. You can see the current status of the rolling upgrade seen on the **Admin > Cluster** page. If the integrated load balancer is configured, its IPs are migrated among the cluster nodes so cluster services, including UI, API, and ingestion of incoming events, remain available throughout the rolling upgrade. Low-level details are written to the `upgrade.log` file on each individual node. A system notification is sent when upgrade completes successfully.

If an issue is encountered affecting one or more of the nodes during the upgrade process, the entire cluster is automatically rolled back to the original, working version. Because configuration changes performed after the upgrade started might be inconsistent or invalid, the configuration is reverted to a known-good state captured before upgrade. No ingested events are lost. Progress is written to `rollback.log` file on each individual node. A system notification is sent when rollback finishes. After the issue is investigated and fixed, you can retry the upgrade.

Prerequisites

- Verify that you are applying the upgrade for a supported upgrade path. See vRealize Log Insight Upgrade Path.
- Create a snapshot or backup copy of the vRealize Log Insight virtual appliance.
- Obtain a copy of the vRealize Log Insight upgrade bundle `.pak` file for the release you are upgrading to.
- Verify that you are logged in to the vRealize Log Insight*portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is https:///*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Management, click **Cluster**.
3. Click **Upgrade from PAK** to upload the `.pak` file.
4. Accept the new EULA to complete the upgrade procedure.

What to do next

After the master node upgrade process is complete, you can view the remaining upgrade process which is automatic.

Check for the email sent to the Admin to confirm the upgrade completed successfully.

Upgrade to vRealize Log Insight 4.0

You can automatically upgrade a cluster to vRealize Log Insight 4.0.

Upgrading vRealize Log Insight must be done from the master node's FQDN. Upgrading using the Integrated Load Balancer IP address is not supported.

During the upgrade, the master node is upgraded first, and restarts. Then each of the cluster nodes is upgraded sequentially. You can see the current status of the rolling upgrade seen on the **Admin > Cluster** page. If the integrated load balancer is configured, its IPs are migrated among the cluster nodes so cluster services, including UI, API, and ingestion of incoming events, remain available throughout the rolling upgrade. Low-level details are written to the `upgrade.log` file on each individual node. A system notification is sent when upgrade completes successfully.

If an issue is encountered affecting one or more of the nodes during the upgrade process, the entire cluster is automatically rolled back to the original, working version. Because configuration changes performed after the upgrade started might be inconsistent or invalid, the configuration is reverted to a known-good state captured before upgrade. No ingested events are lost. Progress is written to `rollback.log` file on each individual node. A system notification is sent when rollback finishes. After the issue is investigated and fixed, you can retry the upgrade.

Prerequisites

- Verify that you are applying the upgrade for a supported upgrade path. See vRealize Log Insight Upgrade Path.
- Create a snapshot or backup copy of the vRealize Log Insight virtual appliance.
- Obtain a copy of the vRealize Log Insight upgrade bundle `.pak` file for the release you are upgrading to.
- Verify that you are logged in to the vRealize Log Insight*portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is https:///*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Management, click **Cluster**.
3. Click **Upgrade from PAK** to upload the `.pak` file.
4. Accept the new EULA to complete the upgrade procedure.

What to do next

After the master node upgrade process is complete, you can view the remaining upgrade process which is automatic.

Check for the email sent to the Admin to confirm the upgrade completed successfully.

Upgrade to vRealize Log Insight 3.6

You can automatically upgrade a cluster to vRealize Log Insight 3.6.

Upgrading vRealize Log Insight must be done from the master node's FQDN. Upgrading using the Integrated Load Balancer IP address is not supported.

During the upgrade, the master node is upgraded first, and restarts. Then each of the cluster nodes is upgraded sequentially. You can see the current status of the rolling upgrade seen on the **Admin > Cluster** page. If the integrated load balancer is configured, its IPs are migrated among the cluster nodes so cluster services, including UI, API, and ingestion of incoming events, remain available throughout the rolling upgrade. Low-level details are written to the `upgrade.log` file on each individual node. A system notification is sent when upgrade completes successfully.

If an issue is encountered affecting one or more of the nodes during the upgrade process, the entire cluster is automatically rolled back to the original, working version. Because configuration changes performed after the upgrade started might be inconsistent or invalid, the configuration is reverted to a known-good state captured before upgrade. No ingested events are lost. Progress is written to `rollback.log` file on each individual node. A system notification is sent when rollback finishes. After the issue is investigated and fixed, you can retry the upgrade.

Prerequisites

- Verify that you are applying the upgrade for a supported upgrade path. See vRealize Log Insight Upgrade Path.
- Create a snapshot or backup copy of the vRealize Log Insight virtual appliance.
- Obtain a copy of the vRealize Log Insight upgrade bundle `.pak` file for the release you are upgrading to.
- Verify that you are logged in to the vRealize Log Insight*portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is https:///*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Management, click **Cluster**.
3. Click **Upgrade from PAK** to upload the `.pak` file.
4. Accept the new EULA to complete the upgrade procedure.

What to do next

After the master node upgrade process is complete, you can view the remaining upgrade process which is automatic.

Check for the email sent to the Admin to confirm the upgrade completed successfully.

Managing vRealize Log Insight User Accounts 2

Administators can create user accounts and roles to provide access to the vRealize Log Insight web interface.

Only users with the Edit Admin permission can create and edit user accounts. However, users can change their own email and account password without having Edit Admin permission.

This section includes the following topics:

User Management Overview

System administrators use a combination of user logins, role-based access control, permissions, and data sets to manage vRealize Log Insight users. Role-based access control lets administrators manage users and the tasks that they can perform.

Roles are sets of permissions required to perform particular tasks. System administrators define roles as part of defining security policies, and grant the roles to users. To change the permissions and tasks associated with a particular role, the system administrator updates the role settings. The updated settings take effect for all users associated with the role.

- To allow a user to perform a task, the system administrator grants the role to the user.
- To prevent a user from performing a task, the system administrator revokes the role from the user.

Managing access, roles, and permissions for each user is based on their user login account. Each user can be granted multiple roles and permissions.

Users who cannot view or access certain objects or cannot perform certain operations were not granted the permissions to do so.

Role-Based Access Control

Role-based access control lets system administrators control user access to vRealize Log Insight and control tasks that users can perform after they log in. To implement role-based access control, system administrators associate or revoke permissions and roles with or from user login accounts

Users	System administrators can control the access and actions of each user by granting or revoking permissions and roles to or from the login account of the user.
Permissions	Permissions control the allowed actions in vRealize Log Insight. Permissions apply to particular administrative or user tasks in vRealize Log Insight. For example, you can grant the **View Admin** permission to allow a user to view the vRealize Log Insight administrative settings.
Data Sets	Data sets consist of a set of filters. You can use data sets to provide users with access to specific content by associating a data set with a role.
Roles	Roles are collections of permissions and data sets that can be associated with users. Roles provide a convenient way to package all the permissions required to perform a task. One user can be assigned multiple roles.

Create a New User Account in vRealize Log Insight

Users that are given the Super Admin role can create user accounts to provide access to the vRealize Log Insight web user interface.

Prerequisites

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https://*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Verify that you have configured VMware Identity Manager or Active Directory support if you are creating user accounts that use either of these types of authentication. See Enable User Authentication Through VMware Identity Manager and Enable User Authentication Through Active Directory

Procedure

1 Click the configuration drop-down menu icon and select **Administration**.

2 Under Management, click **Access Control**.

3 Click **Users and Groups**.

4 Click **New User**.

5 Choose an option from the **Authentication** drop-down menu.

- If you are using the default, built-in authentication, enter a user name, password, and, optionally, an email address. Copy the password from the **Password** text box and provide it to the user.
- If you are using Active Directory or VMware Identity Manager authentication, enter the domain to which the user belongs, a username, and optionally, the email address for the username account.

6 From the **Roles** list on the right, select one or more predefined or custom user roles.

Option	Description
User	Users can access the full functionality of vRealize Log Insight. You can view log events, run queries to search and filter logs, import content packs into their own user space, add alert queries, and manage your own user accounts to change a password or email address. Users do not have access to the administration options, cannot share content with other users, cannot modify the accounts of other users, and cannot install a content pack from the Marketplace. However, you can import a content pack into your own user space which is visible only to you.
Dashboard User	Dashboard users can only use the Dashboards page of vRealize Log Insight.
View Only Admin	View Admin users can view Admin information, have full User access, and can edit Shared content.
Super Admin	Super Admin users can access the full functionality of vRealize Log Insight, can administer vRealize Log Insight, and can manage the accounts of all other users.

7 Click **Save**.

- For built-in authentication, the information is saved locally.
- For VMware Identity Manager authetication, vRealize Log Insight verifies whether VMware Identity Manager is synchronized with the specified group and its domain. If the group cannot be found, a dialog box informs you that vRealize Log Insight cannot verify that group. You can save the group without verification or cancel to correct the group name or domain.

Configure VMware Identity Manager Access to Active Directory Groups for vRealize Log Insight

You can use Active Directory groups with vRealize Log Insight through VMware Identity Manager single sign-on authentication. Your site must be configured for VMware Identity Manager authentication that is enabled for Active Directory support, and server synchronization must be in place.

You must also import group information to vRealize Log Insight

A VMware Identity Manager user inherits roles that are assigned to any group the user belongs to in addition to the roles that are assigned to the individual user. For example, an Administrator can assign GroupA to the role of **View Admin** and assign the user Bob to the role of **User**. Bob can also be assigned to GroupA. When Bob logs in, he inherits the group role and has privileges for both the **View Admin** and **User** roles.

The group is not a VMware Identity Manager local group, but an Active Directory group that is synchronized with VMware Identity Manager.

Prerequisites

- Verify that you have configured the UPN attribute (userPrincipalName) attribute. It can be configured through the VMware Identity Manager administrator interface at **Identity & Access Management > User Attributes**.
- Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.
- Verify that you configured VMware Identity Manager support in vRealize Log Insight. See Enable User Authentication Through VMware Identity Manager

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Management, click **Access Control**.
3. Click **Users and Groups**.
4. Scroll to the Directory Groups table and click **New Group**.
5. Select **VMware Identity Manager** from the **Type** drop-down menu.

   The default domain name that you specified when you configured VMware Identity Manager support appears in the **Domain** text box.
6. Change the domain name to the Active Directory name for the group.
7. Enter the name of the group that you want to add.
8. From the **Roles** list on the right, select one or more predefined or custom user roles.

Option	Description
User	Users can access the full functionality of vRealize Log Insight. You can view log events, run queries to search and filter logs, import content packs into their own user space, add alert queries, and manage your own user accounts to change a password or email address. Users do not have access to the administration options, cannot share content with other users, cannot modify the accounts of other users, and cannot install a content pack from the Marketplace. However, you can import a content pack into your own user space which is visible only to you.
Dashboard User	Dashboard users can only use the Dashboards page of vRealize Log Insight.

Option	Description
View Only Admin	View Admin users can view Admin information, have full User access, and can edit Shared content.
Super Admin	Super Admin users can access the full functionality of vRealize Log Insight, can administer vRealize Log Insight, and can manage the accounts of all other users.

9 Click **Save**.

vRealize Log Insight verifies whether VMware Identity Manager is synchronized with the specified group and its domain. If the group cannot be found, a dialog box informs you that vRealize Log Insight cannot verify that group. You can save the group without verification or cancel to correct the group name or domain.

Users that belong to the group that you added can use their VMware Identity Manager account to log in to vRealize Log Insight and have the same level of permissions as the group to which they belong.

Import an Active Directory Group to vRealize Log Insight

Instead of adding individual domain users, you can add domain groups to allow users to log in to vRealize Log Insight.

When you enable AD support in vRealize Log Insight, you configure a domain name and provide a binding user that belongs to the domain. vRealize Log Insight uses the binding user to verify the connection to the AD domain, and to verify the existence of AD users and groups.

The Active Director groups that you add to vRealize Log Insight must either belong to the domain of the binding user, or to a domain that is trusted by the domain of the binding user.

An Active Directory user inherits roles that are assigned to any group the user belongs to in addition to the roles that are assigned to the individual user. For example, an Administrator can assign GroupA to the role of **View Admin** and assign the user Bob to the role of **User**. Bob can also be assigned to GroupA. When Bob logs in, he inherits the group role and has privileges for both the **View Admin** and **User** roles.

Prerequisites

- Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.
- Verify that you configured AD support. See Enable User Authentication Through Active Directory

Procedure

1 Click the configuration drop-down menu icon and select **Administration**.

2 Under Management, click **Access Control**.

3 Click **Users and Groups**.

4 Under Directory Groups, click **New Group**.

5 Click Active Directory in the **Type** drop-down menu.

The default domain name that you specified when you configured Active Directory support appears in the **Domain** text box. If you are adding groups from the default domain, do not modify the domain name.

6 (Optional) If you want to add a group from a domain that trusts the default domain, type the name of the trusting domain in the **Domain** text box.

7 Enter the name of the group that you want to add.

8 From the **Roles** list on the right, select one or more predefined or custom user roles.

Option	Description
User	Users can access the full functionality of vRealize Log Insight. You can view log events, run queries to search and filter logs, import content packs into their own user space, add alert queries, and manage your own user accounts to change a password or email address. Users do not have access to the administration options, cannot share content with other users, cannot modify the accounts of other users, and cannot install a content pack from the Marketplace. However, you can import a content pack into your own user space which is visible only to you.
Dashboard User	Dashboard users can only use the Dashboards page of vRealize Log Insight.
View Only Admin	View Admin users can view Admin information, have full User access, and can edit Shared content.
Super Admin	Super Admin users can access the full functionality of vRealize Log Insight, can administer vRealize Log Insight, and can manage the accounts of all other users.

9 Click **Save**.

vRealize Log Insight verifies whether the AD group exists in the domain that you specified or in a trusting domain. If the group cannot be found, a dialog box informs you that vRealize Log Insight cannot verify that group. You can save the group without verification or cancel to correct the group name.

Users that belong to the Active Directory group that you added can use their domain account to log in to vRealize Log Insight and have the same level of permissions as the group to which they belong.

Authenticating Users with Cross-Domain Group Membership

There are two ways that administrators can enable users from another trusted domain to authenticate for vRealize Log Insight.

- Add each user manually.
- Configure a group in the same domain as the users and add the group.

Define a Data Set

You can define a data set to provide users access to specific content.

Text-based constraints are not supported for data sets.

Prerequisites

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https:///*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Management, click **Access Control**.
3. Click **Data Sets**.
4. Click **New Data Set**.
5. Click **Add Filter**.
6. Use the first drop-down menu to select any field defined within vRealize Log Insight.

   For example, **hostname**.

   The list contains all defined fields that are available statically, in content packs, and in custom content.

   Note Numeric fields contain the additional operators **=**, **>**, **<**, **>=**, and **<=**, which string fields do not. These operators perform numeric comparisons. Using them yields different results than using string operators. For example, the filter **response_time = 02** matches an event that contains a **response_time** field with a value 2. The filter **response_time contains 02** does not have the same match.

7. Use the second drop-down menu to select the operation to apply to the field selected in the first drop-down menu.

   For example, select **contains**. The **contains** filter matches full tokens: searching for the string err does not result in `error` as a match.

8. In the text box to the right of the filter drop-down menu, enter the value that you want to use as a filter.

   You can use multiple values. The operator between these values is OR.

   Note The text box is not available if you select the **exists** operator in the second drop-down menu.

9. (Optional) To add more filters, click **Add Filter**.
10. Click **Save**.

What to do next

Associate a data set with a user role. See Create and Modify Roles.

Create and Modify Roles

You can create custom roles or modify predefined roles to allow users to perform certain tasks and access specific content.

Prerequisites

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https:///*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Management, click **Access Control**.
3. Click **Roles**.
4. Click **New Role** or to edit an existing role.

   You must clone Super Admin and User roles first before you can edit them.
5. Modify the **Name** and **Description** text boxes.
6. Select one or more permissions from the Permissions list.

Option	Description
Edit Admin	Can edit Admin information and settings
View Admin	Can view Admin information and settings
Edit Shared	Can edit shared content
Analytics	Can use Interactive Analytics
Dashboard	Can view Dashboards

7. (Optional) From the **Data Sets** list on the right, select a data set to associate with the user role.
8. Click **Save**.

Delete a User Account from vRealize Log Insight

You can delete user accounts by using the vRealize Log Insight Administration user interface.

Prerequisites

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https:///*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Management, click **Access Control**.
3. Click **Users and Groups**.
4. Select the check box beside the user name that you want to delete.
5. Click the **Delete** icon .

Configuring Authentication 3

You can use several authentication methods with your deployment.

Authentication methods include local authentication, VMware Identity Managerauthentication, and Active Directory authentication. You can use more than one method in the same deployment and users then select the type of authentication to use at log in.

vRealize Log Insight includes a version of vRealize Log Insight available from the product download page that includes the following set of features:

- Directory integration to authenticate users against existing directories such as Active Directory or LDAP.
- Single Sign-On integration with other VMware products that also support Single Sign-On capability
- Single Sign-On with several third-party identity providers such as ADFS, Ping Federate, and others.
- Two-factor authentication through integration with third-party software such as RSA SecurID, Entrust, and others. Two-factor authentication with VMware Verify is note included.

Local authentication is a component of vRealize Log Insight. To use it, you create a local user and password that is stored on the vRealize Log Insight server. vRealize Log Insight and Active Directory must be enabled by a product administrator.

This section includes the following topics:

Enable User Authentication Through VMware Identity Manager

When enabled by an administrator, VMware Identity Manager authentication can be used with vRealize Log Insight.

With VMware Identity Manager authentication, users can use a single sign-on for all VMware products that use the same Identity Manager.

Active Directory users can also authenticate through VMware Identity Manager when the Active Directory and VMware Identity Manager servers are synchronized. See VMware Identity Manager documentation for more information about synchronization.

Prerequisites

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https:///*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Configuration, click **Authentication**.
3. Select **Enable Single Sign-On**.
4. In the **Host** text box, enter a host identifier for the VMware Identity Manager instance to use for authenticating users .

   For example, `company-name.vmwareidentity.com`.
5. In the **API Port** text box, specify the port to use to connect to the VMware Identity Manager instance. The default is 443.
6. Optionally, enter the VMware Identity Manager tenant. This is required only if tenant mode is configured as tenant-in-path in VMware Identity Manager.
7. Specify VMware Identity Manager user credentials in the **Username** and **Password** text boxes.

   This information is used only once during configuration for creating a vRealize Log Insight client on VMware Identity Manager and is not stored locally in vRealize Log Insight. The user must have permission to run API commands against the tenant.
8. Click **Test Connection** to verify that the connection works.
9. In the **Redirect URL Host** dropdown menu, select the Hostname or IP to be used in Redirect URL for registering on VMware Identity Manager.

   If at least one virtual IP is defined for the Integrated Load Balancer, VMware Identity Manager will redirect to the VIP selected. If the Integrated Load Balancer is not configured, the master node's IP address is used instead.
10. Select whether to allow log in support for Active Directory users through VMware Identity Manager.

    You can use this option for Active Directory users when VMware Identity Manager is synchronized with that Active Directory instance.
11. Click **Save**.

Enable User Authentication Through Active Directory

You can authenticate users through Active Directory. This simplifies the log in process for users by letting them use a common password for multiple purposes.

Prerequisites

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https://*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Configuration, click **Authentication**.
3. Select **Enable Active Directory support**.
4. In the **Default Domain** text box, type a domain name.

   For example, `company-name.com`.

   Note You cannot list multiple domains in the default domain text box. If the default domain that you specify is trusted by other domains, vRealize Log Insight uses the default domain and the binding user to verify AD users and groups in the trusting domains.

   If you switch to a different domain that already includes users and groups, the authentication will fail for the existing users and groups, and data saved by the existing users will be lost.

5. If you have geo-located or security-restricted domain controllers, manually specify the domain controllers closest to this vRealize Log Insight instance.

   Note Load-balanced Active Directory authorization servers are not supported.

6. Enter the credentials of a binding user that belongs to the default domain.

   vRealize Log Insight uses the default domain and the binding user to verify AD users and groups in the default domain, and in domains that trust the default domain.

7. Specify values for the connection type.

   This connection is used for Active Directory authentication.

8. Click **Save**.

What to do next

Give permissions to AD users and groups to access the current instance of vRealize Log Insight.

Configure the Protocol to Use for Active Directory

You can configure the protocol to use when connecting to Active Directory. By default, when vRealize Log Insight connects to Active Directory, it first tries SSL LDAP, and then non-SSL LDAP if necessary.

If you want to limit the Active Directory communication to one particular protocol, or want to change the order of protocols that are tried, you must apply additional configurations in the vRealize Log Insight virtual appliance.

Prerequisites

- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance. See Configure the Root SSH Password for the vRealize Log Insight Virtual Appliance
- To enable SSH connections, verify that TCP port 22 is open.

Procedure

1. Establish an SSH connection to the vRealize Log Insight virtual appliance and log in as the root user.
2. Navigate to the following location: `/storage/var/loginsight/config`
3. Locate the latest configuration file where [number] is the largest: `/storage/core/loginsight/config/loginsight-config.xml#[number]`
4. Copy the latest configuration file: `/storage/core/loginsight/config/loginsight-config.xml#[number]`
5. Increase the [number] and save to the following location: `/storage/core/loginsight/config/loginsight-config.xml#[number + 1]`
6. Open the file for editing.
7. In the `Authentication` section, add the line that corresponds to the configuration that you want to apply:

Option	Description
`<ad-protocols value="LDAP" />`	For specifically using LDAP without SSL
`<ad-protocols value="LDAPS" />`	For specifically using LDAP with SSL only
`<ad-protocols value="LDAP,LDAPS" />`	For specifically using LDAP first and then using LDAP with SSL.
`<ad-protocols value="LDAPS,LDAP" />`	For specifically using LDAPS first and then using LDAP without SSL

   When you do not select a protocol, vRealize Log Insight attempts to use LDAP first, and then uses LDAP with SSL.

8. Save and close the file.
9. Run the `service loginsight restart` command.

Configuring vRealize Log Insight

4

You can configure and customize vRealize Log Insight to change default settings, network settings, and modify storage resources. You can also configure system notifications.

This section includes the following topics:

vRealize Log Insight Configuration Limits

When you configure vRealize Log Insight, you must stay at or below the supported maximums.

Table 4-1. vRealize Log Insight Configuration Maximums

Item	Maximum
Node Configuration	
CPU	16 vCPUs

Table 4-1. vRealize Log Insight Configuration Maximums (Continued)

Item	Maximum
Memory	32 GB
Storage device (vmdk)	2 TB - 512 bytes
Total addressable storage	4 TB (+ OS drive) A maximum of 4TB addressable log storage on VMDKs with a maximum size of 2TB each. You can have two 2TB VMDKs or four 1TB VMDKs, etc. When you reach the maximum, you will need to scale outward with a larger cluster size instead of adding more disks to existing VMs.
Syslog connections	750
Cluster Configuration	
Nodes	12 (Master + 11 Workers)
Ingestion per Node	
Events per second	15,000 eps
Syslog message length	10 KB (text field)
Ingestion API HTTP POST request	16 KB (text field); 4 MB per HTTP POST request
Integrations	
vRealize Operations Manager	1
vSphere vCenter Server	10
Active Directory domains	1
Email servers	1
DNS servers	2
NTP servers	4
Forwarders	10

Configuring Virtual Appliance Settings

You can modify virtual appliance settings, including storage capacity and memory or CPU capacity.

Configure the Root SSH Password for the vRealize Log Insight Virtual Appliance

By default the SSH connection to the virtual appliance is disabled. You can configure the root SSH password from the VMware Remote Console or when you deploy the vRealize Log Insight virtual appliance.

As a best practice, set the root SSH password when you deploy thevRealize Log Insight .ova file. For more information, see Deploy the vRealize Log Insight Virtual Appliance.

You can also enable SSH and set the root password from the VMware Remote Console.

Prerequisites

Verify that the vRealize Log Insight virtual appliance is deployed and running.

Procedure

1. In the vSphere Client inventory, click the vRealize Log Insight virtual appliance, and open the **Console** tab.
2. Go to a command line by following the key combination specified on the splash screen.
3. In the console, type **`root`**, and press Enter. Leave the password empty and press Enter.

   The following message is displayed in the console: `Password change requested. Choose a new password.`
4. Leave the old password empty and press Enter.
5. Type a new password for the root user, press Enter, type the new password again for the root user, and press Enter.

   The password must consist of at least eight characters, and must include at least one upper case letter, one lower case letter, one digit, and one special character. You cannot repeat the same character more than four times.

The following message is displayed: `Password changed.`

What to do next

You can use the root password to establish SSH connections to the vRealize Log Insight virtual appliance.

Change the Network Settings of the vRealize Log Insight vApp

You can change the network settings of the vRealize Log Insight virtual appliance by editing the vApp properties in the vSphere Client.

Prerequisites

Verify that you have permissions to edit vApp properties.

Procedure

1. Power off the vRealize Log Insight vApp.
2. Right-click the vRealize Log Insight vApp in the inventory and click **Edit Settings**.
3. Click the **Options** tab and select **vApp Options > IP Allocation Policy**.

4 Select an IP allocation option.

Option	Description
Fixed	IP addresses are manually configured. No automatic allocation is performed.
Transient	IP addresses are automatically allocated using IP pools from a specified range when the vApp is powered on. The IP addresses are released when the appliance is powered off
DHCP	A DHCP server is used to allocate the IP addresses. The addresses assigned by the DHCP server are visible in the OVF environments of virtual machines started in the vApp.

5 (Optional) If you select **Fixed**, click **vApp Options > Properties** and assign an IP address, netmask, gateway, DNS and host name for the vRealize Log Insight vApp.

Caution Do not specify more than two domain name servers. If you specify more than two domain name servers, all configured domain name servers are ignored in the vRealize Log Insight virtual appliance.

6 Power on the vRealize Log Insight vApp.

Increase the Storage Capacity of the vRealize Log Insight Virtual Appliance

You can increase the storage resources allocated to vRealize Log Insight as your needs grow.

Increase the storage space by adding a new virtual disk to the vRealize Log Insight virtual appliance. You can add as many disks as you need, up to 4 TB (+ OS drive) total addressable storage. The total can be a combination of two 2-TB disks, or four 1-TB disks, and so on. See vRealize Log Insight Configuration Limits.

Prerequisites

- Log in to the vSphere Client as a user who has privileges to modify the hardware of virtual machines in the environment.
- Shut down the vRealize Log Insight virtual appliance safely. See Power Off the vRealize Log Insight Virtual Appliance

Procedure

1 In the vSphere Client inventory, right-click the vRealize Log Insight virtual machine and select **Edit Settings**.

2 On the **Hardware** tab, click **Add**.

3 Select **Hard Disk** and click **Next**.

4 Select **Create a new virtual disk** and click **Next**.

   a Type the disk capacity.

   vRealize Log Insight supports virtual hard disks of up to 2 TB. If you need more capacity, add more than one virtual hard disk.

   b Select a disk format.

Option	Description
Thick Provision Lazy Zeroed	Creates a virtual disk in the default thick format. The space required for the virtual disk is allocated when the virtual disk is created. The data residing on the physical device is not erased during creation, but is zeroed out on demand later, after first write from the virtual appliance.
Thick Provision Eager Zeroed	Creates a type of thick virtual disk that supports clustering features such as Fault Tolerance. The space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data residing on the physical device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create other types of disks. Create thick provisioned eager zeroed disks whenever possible for better performance and operation of the vRealize Log Insight virtual appliance.
Thin Provision	Creates a disk in thin format. Use this format to save storage space.

   c To select a datastore, browse for the datastore location and click **Next**.

5 Accept the default virtual device node and click **Next**.

6 Review the information and click **Finish**.

7 Click **OK** to save your changes and close the dialog box.

When you power on the vRealize Log Insight virtual appliance, the virtual machine discovers the new virtual disk and automatically adds it to the default data volume. Completely power off the virtual machine first. For information about powering on virtual appliances, see https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html.

Caution After you add a disk to the virtual appliance, you cannot remove it safely. Removing disks from the vRealize Log Insight virtual appliance may result in complete data loss.

Add Memory and CPU to the vRealize Log Insight Virtual Appliance

You can change the amount of memory and CPUs allocated to a vRealize Log Insight virtual appliance after deployment.

You might need to adjust resource allocation if, for example, the number of events in your environment increases.

Prerequisites

- Log in to the vSphere Client as a user who has privileges to modify the hardware of virtual machines in the environment.
- Shut down the vRealize Log Insight virtual appliance safely. See Power Off the vRealize Log Insight Virtual Appliance

Procedure

1. In the vSphere Client inventory, right-click the vRealize Log Insight virtual machine and select **Edit Settings**.
2. On the **Hardware** tab, click **Add**.
3. Adjust the amount of CPU and memory as needed.
4. Review the information and click **Finish**.
5. Click **OK** to save your changes and close the dialog box.

When you power on the vRealize Log Insight virtual appliance, the virtual machine begins to utilize the new resources.

Assign a Permanent License to vRealize Log Insight

You can use vRealize Log Insight only with a valid license key.

You obtain an evaluation license when you download vRealize Log Insight from the VMware Web site. This license is valid for 60 days. When the evaluation license expires, you must assign a permanent license to continue using vRealize Log Insight.

As part of solution interoperability, VMware NSX users or Standard, Advanced, or Enterprise editions can license vRealize Log Insight with their NSX license key. For more information, consult VMware NSX documentation.

You use the Administration section of the vRealize Log Insight Web user interface to check the vRealize Log Insight licensing status and manage your license.

Prerequisites

- Obtain a valid license key from My VMware™.
- Verify that you are logged in to the vRealize Log Insight*portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is https://*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon  and select **Administration**.
2. Under Management, select **License**.

3 In the **License Key** text box, type your license key and click **Set Key**. If you have a VMware NSX license key, enter it here.

4 Verify that the license status is Active, and the license type and expiry day are correct.

Log Storage Policy

The vRealize Log Insight virtual appliance uses a minimum of 100GB of storage for incoming logs.

When the volume of logs imported into vRealize Log Insight reaches the 100GB limit, old log messages are automatically and periodically retired on a first-come-first-retired basis. To preserve old messages, you can enable the archiving feature of vRealize Log Insight. See Enable or Disable Data Archiving in vRealize Log Insight.

Data stored by vRealize Log Insight is immutable. After a log has been imported, it cannot be removed until it is automatically retired.

Managing System Notifications

vRealize Log Insight provides built-in system notifications about activity related to vRealize Log Insight health, such as when disk space is almost exhausted and old log files are about to be deleted. Administrators can configure how often and where system notifications are sent.

System notifications inform you of critical issues that require immediate attention, provide you with warnings that might require a response, and inform you of normal system activity. System notifications are suspended during upgrade, but in effect at all other times.

An administrator can specify how often notifications are sent when triggered and to which email addresses. System notifications concerning vRealize Log Insight can also be sent to third-party applications.

System notifications are distinct from alert queries, which are user-defined. For more information about alert queries, see Add an Alert Query in Log Insight to Send Email Notifications.

vRealize Log Insight System Notifications

vRealize Log Insight provides you with two sets of notifications, general notifications, applicable for all product configurations, and notifications related to clusters for cluster-based deployments.

The following tables list and describe system notifications for vRealize Log Insight.

General System Notifications

vRealize Log Insight sends notifications when conditions might require administrative intervention, including archival failure or alert scheduling delays.

	Notification Name	Description
	Oldest Data Will Be Unsearchable Soon	This notification tells you when vRealize Log Insight is expected to start decommissioning old data from the virtual appliance storage and what the expected size of searchable data is at the current ingest rate. Data that has been rotated out is archived if you have configured archiving, or deleted if you have not. The notification is sent after each restart of the vRealize Log Insight service.
	Repository Retention Time	A retention period is the length of time data is retained on the local disk of your vRealize Log Insight instance. A retention period is determined by the amount of data the system can hold and the current ingestion rate. For example, if you are receiving 10 GB/day of data (after indexing) and you have 300 GB of space, then your retention rate is 30 days. When the storage limit is reached, old data is removed to make way for newly ingested data. This notification tells you when the amount of searchable data that vRealize Log Insight can store at the current ingest rates exceeds the storage space that is available on the virtual appliance. Admin users can define the storage notification threshold. See Configure vRealize Log Insight to Send Health Notifications.

	Notification Name	Description

	Dropped Events	This notification tells you that vRealize Log Insight failed to ingest all incoming log messages.
		■ In case of any TCP Message drops, as tracked by vRealize Log Insight server, a system notification is sent in both cases as follows:
		  ■ Once a day
		  ■ Each time the vRealize Log Insight service is restarted, manually or automatically.
		■ The email contains the number of messages dropped since last notification email was sent and total message drops since the last restart of vRealize Log Insight.
		Note The time in the sent line is controlled by the email client, and is in the local time zone, while the email body displays UTC time.

	Corrupt Index Buckets	This notification tells you that part of the on-disk index is corrupt. A corrupt index usually indicates serious issues with the underlying storage system. The corrupt part of the index is excluded from serving queries. A corrupt index affects the ingestion of new data. vRealize Log Insight checks the integrity of the index upon service start-up. In case of detected corruption, vRealize Log Insight sends a system notification as follows: ■ Once a day ■ Each time the vRealize Log Insight service is restarted, manually or automatically.
	Out of Disk	This notification tells you that vRealize Log Insight is running out of allocated disk space. This notification signals that vRealize Log Insight has most probably run into a storage-related issue.
	Archive Space Will Be Full	This notification tells you that the disk space on the NFS server used for archiving vRealize Log Insight data will be used up soon.

	Notification Name	Description
	Total Disk Space Change	This notification tells you that the total size of the partition for vRealize Log Insight data storage has decreased. This usually signals a serious issue in the underlying storage system. When vRealize Log Insight detects the condition it sends this notification as follows: ■ Immediately ■ Once a day
	Pending Archivings	This notification tells you that vRealize Log Insight cannot archive data as expected. The notification usually indicates problems with the NFS storage that you configured for data archiving.
	License is about to be expired	This notification tells you that the license for vRealize Log Insight is about to expire.
	License is expired	This notification tells you that the license for vRealize Log Insight has expired.
	Unable to connect to AD server	This notification tells you that vRealize Log Insight is unable to connect to the configured Active Directory server.
	Cannot take over High Availability IP address [IP Address] as it is already held by another machine	This notification tells you that the vRealize Log Insight cluster was unable to take over the configured IP Address for the Integrated Load Balancer (ILB). The most common reason for this notification is that another host within the same network holds the IP address, and therefore the IP address is not available to be taken over by the cluster. You can resolve this conflict by either releasing the IP address from the host that currently holds it, or configuring Log Insight Integrated Load Balancer with a Static IP address that is available in the network. When changing the ILB IP address, remember to reconfigure all clients to send logs to the new IP address, or to a FQDN/URL that resolves to this IP address. You must also unconfigure and reconfigure every vCenter Server integrated with vRealize Log Insight from the vSphere integration page.

	Notification Name	Description
	High Availability IP address [IP Address] is unavailable due to too many node failures	This notification tells you that the IP Address configured for the Integrated Load Balancer (ILB) is unavailable. This means that clients trying to send logs to a vRealize Log Insight cluster via the ILB IP address or a FQDN/URL that resolves to this IP address will see it as unavailable. The most common reason for this notification is that a majority of the nodes in the vRealize Log Insight cluster are unhealthy, unavailable, or unreachable from the master node. Another common reason is that NTP time synchronization has not been enabled, or the configured NTP servers have significant time drift between each other. You can confirm that the problem is still ongoing by trying to ping (if allowed) the IP address to verify that it is not reachable. You can resolve this problem by ensuring a majority of your cluster nodes are healthy and reachable, and enabling NTP time synchronization to accurate NTP servers.
	Too many migrations of High Availability IP address [your IP Address] between vRealize Log Insight nodes	This notification tells you that the IP address configured for the Integrated Load Balancer (ILB) has migrated too many times within the last 10 minutes. Under normal operation, the IP address rarely moves between vRealize Log Insight cluster nodes. However, the IP address might move if the current owner node is restarted or put in maintenance. The other reason can be lack of time synchronization between Log Insight cluster nodes, which is essential for proper cluster functioning. In case of latter, you can fix the problem by enabling NTP time synchronization to accurate NTP servers.

	Notification Name	Description
	SSL Certificate Error	This notification tells you that a syslog source has initiated a connection to vRealize Log Insight over SSL but ended the connection abruptly. This may indicate that the syslog source was unable to confirm the validity of the SSL certificate. In order for vRealize Log Insight to accept syslog messages over SSL, a certificate that is validated by the client is required and the clocks of the systems must be synchronized. There may be an issue with the SSL Certificate or with the Network Time Service. You can validate that the SSL Certificate is trusted by your syslog source, reconfigure the source not to use SSL, or reinstall the SSL Certificate. See Configure the vRealize Log Insight Agent SSL Parameters and Install a Custom SSL Certificate.
	vCenter collection failed	This notification tells you that vRealize Log Insight is unable to collect vCenter events, tasks, and alarms. To look for the exact error that caused the collection failure and to see if collection is working currently, look in the `/storage/var/loginsight/plugins/vsphere/li-vsphere.log` file.

	Event Forwarder Events Dropped	This system notification is sent when a forwarder drops events because of connection or overload issues.
		Example:
		`Log Insight Admin Alert: Event Forwarder Events Dropped`
		`This alert is about your Log Insight installation on https://<your_url>`
		
		`Event Forwarder Events Dropped triggered at 2016-08-02T18:41:06.972Z`
		
		`Log Insight just dropped 670 events for forwarder target 'Test',`
		`reason: Pending queue is full.`

	Notification Name	Description
	Alert Queries Behind Schedule	This notification informs you that vRealize Log Insight was unable to run a user alert at its configured time. The reason for the delay may be because of one or more inefficient user alerts or because the system is not properly sized for the ingestion and query load.
	Auto Disabled Alert	If an alert has run at least ten times and its average run time is more than one hour, then the alert is deemed to be inefficient and is disabled to prevent impacting other user alerts.
	Inefficient Alert Query	If an alert takes more than one hour to complete, then the alert is deemed to be inefficient.

System Notifications for Clusters

vRealize Log Insight sends notifications about cluster topology changes, including the addition of new cluster members or transient node communication problems.

Sent by	Notification Name	Description
Master node	Approval needed for new worker node	This notification tells you of a membership request from a worker node. An Admin user needs to approve or reject the request.
Master node	New worker node approved	This notification tells you that an Admin user approved a membership request from a worker node to join a vRealize Log Insight cluster.
Master node	New worker node denied	This notification tells you that an Admin user rejected a membership request from a worker node to join a vRealize Log Insight cluster. If the request was denied by mistake, an Admin user can place the request again from the worker and then approve it at the master node.
Master node	Maximum supported nodes exceeded due to worker node	This notification tells you that the number of worker nodes in the Log Insight cluster has exceeded the maximum supported count due to a new worker node.
Master node	Allowed nodes exceeded, new worker node denied	This notification tells you that an Admin user attempted to add more nodes to the cluster than the maximum allowed node count and the node has been denied.

Sent by	Notification Name	Description
Master node	Worker node disconnected	This notification tells you that a previously connected worker node disconnected from the vRealize Log Insight cluster.
Master node	Worker node reconnected	This notification tells you that a worker node reconnected to the vRealize Log Insight cluster.
Master node	Worker node revoked by admin	This notification tells you that an Admin user revoked a worker node membership and the node is no longer a part of the vRealize Log Insight cluster.
Master node	Unknown worker node rejected	This notification tells you that the vRealize Log Insight master node rejected a request by a worker node because the worker node is unknown to the master. If the worker is a valid node and it should be added to the cluster, log in to the worker node, remove its token file and user configuration at `/storage/core/loginsight/config/`, and run `restart loginsight service` on the worker node.
Master node	Worker node has entered into maintenance mode	This notification tells you that a worker node entered into maintenance mode and an Admin user has to remove the worker node from maintenance mode before it can receive configuration changes and serve queries.
Master node	Worker node has returned to service	This notification tells you that a worker node exited maintenance mode and returned to service.

Sent by	Notification Name	Description
Worker node	Master failed or disconnected from worker node	This notification tells you that a worker node that sends the notification is unable to contact the vRealize Log Insight master node. This might indicate that the master node failed, and might need to be restarted. If the master node failed, the cluster cannot be configured and queries cannot be submitted until it is back online. Worker nodes continue to ingest messages. **Note** You might receive many such notifications because many workers might detect the master node failure independently and raise notifications.
Worker node	Master connected to worker node	This notification tells you that a worker node that sends the notification is reconnected to the vRealize Log Insight master node.

Configuring vRealize Log Insight System Notifications

As an administrator, you can configurevRealize Log Insight system notifications to send system notifications to third-party applications and also to send email to specified users when a notification is triggered.

vRealize Log Insight generates these notifications when an important system event occurs, for example when the disk space is almost exhausted and vRealize Log Insight must start deleting or archiving old log files.

Configure vRealize Log Insight to Send Health Notifications

An administrator can configure vRealize Log Insight to send notifications related to its own health.

If an email message cannot be delivered, you are notified of the error on the Web interface.

Prerequisites

- Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https://*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.
- Verify that the SMTP server is configured for vRealize Log Insight. For more information, see Configure the SMTP Server for vRealize Log Insight.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Configuration, click **General**.

3 Under the Alerts header, set the system notifications.

   a In the **Email System Notifications To** text box, type the email addresses to be notified.

      Use commas to separate multiple email addresses.

   b Select the **Retention notification threshold** check box and set the threshold that triggers the notifications.

      A notification is sent when the amount of data the system can hold is insufficient for the time period specified. This value is calculated based on the current ingestion rate.

4 Click **Save**.

5 Click **Restart Log Insight** to apply your changes.

Configure vRealize Log Insight System Notifications for Third-Party Products

An administrator can configure vRealize Log Insight to send notifications related to its own health to third-party applications.

vRealize Log Insight generates these notifications when an important system event occurs, for example when the disk space is almost exhausted and vRealize Log Insight must start deleting old log files.

Prerequisites

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https://*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 Click the configuration drop-down menu icon and select **Administration**.

2 Under Configuration, click **General**.

3 Under the Alerts header, set the system notifications.

   a In the **Send HTTP Post System Notifications To** text box, type the URLs to be notified.

   b (Optional) Confirm that the **Send a notification when capacity drops below** check box and associated threshold are configured correctly for your environment.

4 Click **Save**.

What to do next

Working with the webhook output for your notification, create a shim to map the vRealize Log Insight webhook format to the format used by your third-party application.

About Using Webhooks to Send System Notifications to Third-Party Products

You can send vRealize Log Insight system notifications to third-party products by using webhooks.

vRealize Log Insight uses webhooks to send alerts over HTTP POST to other applications. vRealize Log Insight sends a webhook in its own proprietary format, but third-party solutions expect incoming webhooks to be in their pwn proprietary format. To use information sent with vRealize Log Insight webhooks, the third-party application must have either native support for the vRealize Log Insight format or you must create a mapping between vRealize Log Insight formats and the format used by the third-party with a shim. The shim translates, or maps, the vRealize Log Insight format to a different format.

System notifications, alerts created with message queries, and alerts created with aggregate queries each have their own webhook format.

You must be a vRealize Log Insight administrator to create system notifications.

HTTP basic authentication is supported. Embed credentials in the url using the form {{https://*username:password@hostname/path*}}

Webhook Format for a System Notification

The format of a vRealize Log Insight webhook depends on the type of query from which it is created. System notifications, user alert message queries, and alerts generated from aggregate user queries each have a different webhook format.

You must be a vRealize Log Insight administrator to configure vRealize Log Insight to send system notifications.

When you send a system notification to a third-party program, you must write a shim to make vRealize Log Insight information understandable by the third-party program's formats.

Webhook Format for System Notifications

The following example shows the vRealize Log Insight webhook format for system notifications.

```
{
   "AlertName":" Admin Alert: Worker node has returned to service  (Host = 127.0.0.2)",
   "messages":[
      {
         "text":"This notification was generated from Log Insight node (Host = 127.0.0.2,
     Node Identifier = a31cad22-65c2-4131-8e6c-27790892a1f9).
     A worker node has returned to service after having been in maintenance mode.
     The Log Insight master node reports that worker node has finished maintenance
     and exited maintenance mode. The node will resume receiving configuration changes and
     serving queries. The node is also now ready to start receiving incoming log messages."

         "timestamp":1458665320514,"fields":[]
      }
   ]
}
```

Add vRealize Log Insight Event Forwarding Destination

You can configure a vRealize Log Insight server to forward incoming events to a syslog or Ingestion API target.

Use event forwarding to send filtered or tagged events to one or more remote destinations such as vRealize Log Insight or syslog or both. Event forwarding can be used to support existing logging tools such as SIEM and to consolidate logging over different networks such as DMZ or WAN.

Note Event forwarders can be standalone or clustered, but an event forwarder is a separate instance from the remote destination. Instances configured for event forwarding also store events locally and can be used to query data.

Prerequisites

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https://*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Verify that the destination can handle the number of events that are forwarded. If the destination cluster is much smaller than the forwarding instance, some events might be dropped.

Procedure

1 Click the configuration drop-down menu icon and select **Administration**.

2 Under Management, click **Event Forwarding**.

3 Click **New Destination** and provide the following information.

Option	Description
Name	A unique name for the new destination.
Host	The IP address or fully qualified domain name. **Caution** A forwarding loop is a configuration in which a vRealize Log Insight cluster forwards events to itself, or to another cluster, which then forwards the events back to the original cluster. Such a loop may create an indefinite number of copies of each forwarded event. The vRealize Log Insight Web interface does not permit you to configure an event to be forwarded to itself. But vRealize Log Insight is not able to prevent an indirect forwarding loop, such as vRealize Log Insight cluster A forwarding to cluster B, and B forwarding the same events back to A. When creating forwarding destinations, take care not to create indirect forwarding loops.

Option	Description
Protocol	Ingestion API or syslog. The default value is Ingestion API (CFAPI). When events are forwarded using the Ingestion API, the event's original source is preserved in the source field. When events are forwarded using syslog, the event's original source is lost and the receiver may record the message's source as the vRealize Log Insight forwarder's IP address or hostname. **Note** The source field may have different values depending on the protocol selected on the Event Forwarder: a For the ingestion API, the source is the initial sender's (the event originator) IP address. b For syslog, the source is the Event Forwarder's vRealize Log Insight instance IP address. Also, the syslog message text contains `_li_source_path` which points to the initial sender's IP address.
Use SSL	You can optionally secure the connection with SSL for the ingestion API. The remote server's trust root is validated and Event Forwarding with SSL does not work with self-signed certificates installed on destination servers by default. If untrusted, import the remote server's trusted root certificate to the forwarder's keystore. See Configure vRealize Log Insight Event Forwarding with SSL.
Tags	You can optionally add tag pairs with predefined values. Tags permit you to more easily query events. You can add multiple comma-separated tags.
Forward Complementary tags	You can choose whether to forward complementary tags for syslog. Complementary tags are tags added by the cluster itself, such as 'vc_username' or 'vc_vmname.' and can be forwarded with the tags coming directly from sources. Complementary tags are always forwarded when Ingestion API is used.
Transport	Select a transport protocol for syslog. You can choose UDP or TCP.

4 (Optional) To control which events are forwarded, click ➕ **Add Filter**.

Select fields and constraints to define the desired events. Only static fields are available for use as filters. If you do not select a filter, all events are forwarded. You can see the results of the filter you are building by clicking **Run in Interactive Analytics**.

Option	Description
matches	Finds strings that match the specified string and wildcard specification. For example, **`test*`** matches strings such as **`test123`** or **`test-run`**, but not **`my-test-run`**. **`test`** matches **`test`**, but not **`test123`**.
does not match	Excludes strings that match that specified string and wildcard specification. For example, **`test*`** filters out **`test123`**, but does not exclude **`mytest123`**.
starts with	Finds strings that start with the specified character string. For example, **`test`** finds **`test123`** or **`test`**, but not **`my-test123`**.
does not start with	Excludes strings that start with the specified character string. For example, **`test`** filters out **`test123`**, but not my-test123.

5 (Optional) Click **Show Advanced Settings** to modify the following forwarding information.

Option	Description
Port	The port to which events are sent on the remote destination. The default value is set based on the protocol specified. Do not change unless the remote destination listens on a different port.
Disk Cache	The amount of local disk space to reserve for buffering events that you configure to be forwarded. Buffering is used when the remote destination is unavailable or unable to process the events being sent to it. If the local buffer becomes full and the remote destination is still unavailable, then the newest local events are dropped and not forwarded to the remote destination even when the remote destination is back online. The default value is 200 MB.
Worker Count	The number of simultaneous outgoing connections to use. Set a higher worker count for a higher network latency to the forwarded destination and for a higher number of forwarded events per second. The default value is 8.

6 To verify your configuration, click **Test**.

7 Click **Save**.

What to do next

- Configure vRealize Log Insight Event Forwarding with SSL.
- You can edit or clone an event forwarding destination. If you edit the destination to change an event forwarder name, all statistics are reset.

Configure vRealize Log Insight Event Forwarding with SSL

You can configure a vRealize Log Insight server to forward incoming events to another Log Insight server via Ingestion API target with SSL.

Prerequisites

Event Forwarding with SSL does not work with the self-signed certificate installed on destination servers by default. A custom SSL certificate must be created using the steps in Generate a Certificate Signing Request and then uploaded. See Install a Custom SSL Certificate

Procedure

1 Copy the trusted root certificate into a temporary directory on the forwarder instance. For example `/home`.

2 SSH to the forwarder instance and run the following commands.

```
localhost:~ # cd /usr/java/default/lib/security/
localhost:/usr/java/default/lib/security # ../../bin/keytool
–import –alias loginsight –file /home/cacert.crt –keystore cacerts
```

The default keystore password is **`changeit`**.

Note Java versions might vary with time.

3 Restart thevRealize Log Insight instance.

If you use a vRealize Log Insight cluster environment, this operation should be performed on all nodes with the same certificate.

What to do next

Enable SSL connection. See Enforce SSL-Only Connections.

Synchronize the Time on the vRealize Log Insight Virtual Appliance

You must synchronize the time on the vRealize Log Insight virtual appliance with an NTP server or with the ESX/ESXi host on which you deployed the virtual appliance.

Time is critical to the core functionality of vRealize Log Insight.

By default, vRealize Log Insight synchronizes time with a pre-defined list of public NTP servers. If public NTP servers are not accessible due to a firewall, you can use the internal NTP server of your company. If no NTP servers are available, you can sync time with the ESX/ESXi host where you have deployed the vRealize Log Insight virtual appliance.

Prerequisites

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https://*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 Click the configuration drop-down menu icon and select **Administration**.

2 Under Configuration, click **Time**.

3 From the **Sync time with** drop-down menu, select the time source.

Option	Description
NTP server	Synchronizes the time on the vRealize Log Insight virtual appliance with one of the listed NTP servers.
ESX/ESXi host	Synchronizes the time on the vRealize Log Insight virtual appliance with the ESX/ESXi host on which you have deployed the virtual appliance.

4 (Optional) If you selected NTP server synchronisation, list the NTP server addresses, and click **Test**.

Note Testing the connection to NTP servers might take up to 20 seconds per server.

5 Click **Save**.

Configure the SMTP Server for vRealize Log Insight

You can configure an SMTP to allow vRealize Log Insight to send email alerts.

System alerts are generated when vRealize Log Insight detects an important system event, for example when the storage capacity on the virtual appliance reaches the thresholds that you set.

Prerequisites

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https://*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Configuration, click **SMTP**.
3. Type the SMTP server address and port number.
4. If the SMTP server uses an encrypted connection, select the encryption protocol.
5. In the **Sender** text box, type an email address to use when sending system alerts.

   The **Sender** address appears as the From address in system notification emails. It need not be a real address, and can be something that represents the specific instance of vRealize Log Insight. For example, **`loginisght@example.com`**.
6. Type a user name and password to authenticate with the SMTP server when sending system alerts.
7. Type a destination email and click **Send Test Email** to check the connection.
8. Click **Save**.

Install a Custom SSL Certificate

By default, vRealize Log Insight installs a self-signed SSL certificate on the virtual appliance.

The self-signed certificate generates security warnings when you connect to the vRealize Log Insight web user interface. If you do not want to use a self-signed security certificate, you can install a custom SSL certificate. The only feature requiring a custom SSL certificate is Event Forwarding through SSL. If you have a Cluster setup with ILB enabled, see Enable the Integrated Load Balancer for the specific requirements of a custom SSL certificate.

Note The vRealize Log Insight Web user interface and the Log Insight Ingestion protocol `cfapi` use the same certificate for authentication.

Prerequisites

- Verify that your custom SSL certificate meets the following requirements.
  - The CommonName contains a wildcard or exact match for the M aster node or FQDN of the virtual IP address. Optionally, all other IP addresses and FQDNs are listed as subjectAltName.
  - The certificate file contains both a valid private key and a valid certificate chain.
  - The private key is generated by the RSA or the DSA algorithm.
  - The private key is not encrypted by a pass phrase.
  - If the certificate is signed by a chain of other certificates, all other certificates are included in the certificate file that you plan to import.
  - The private key and all the certificates that are included in the certificate file are PEM-encoded. vRealize Log Insight does not support DER-encoded certificates and private keys.
  - The private key and all the certificates that are included in the certificate file are in the PEM format. vRealize Log Insight does not support certificates in the PFX, PKCS12, PKCS7, or other formats.
- Verify that you concatenate the entire body of each certificate into a single text file in the following order.
  a The Private Key - *your_domain_name*.key
  b The Primary Certificate - *your_domain_name*.crt
  c The Intermediate Certificate - *DigiCertCA*.crt
  d The Root Certificate - *TrustedRoot*.crt
- Verify that you include the beginning and ending tags of each certificate in the following format.

```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: your_domain_name.key)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: your_domain_name.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: DigiCertCA.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----
```

- Verify that you are logged in to the vRealize Log Insight*portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is https:///*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 Generate a Self-Signed Certificate

You can generate a self-signed certificate for Windows or Linux by using the OpenSSL tool.

2 Generate a Certificate Signing Request

Generate a certificate signing request by using the OpenSSL tool for Windows.

3 Request a Signature from a Certificate Authority

Send your certificate signing request to a Certificate Authority of your choice and request a signature.

4 Concatenate Certificate Files

Combine your key and certificate files into a PEM file.

5 Upload Signed Certificate

You can upload a signed SSL certificate.

6 Configure SSL Connection Between the vRealize Log Insight Server and the Log Insight Agents

SSL function allows you to provide SSL only connections between the Log Insight Agents and the vRealize Log Insight Server through the secure flow of Ingestion API. You can also configure various SSL parameters of the Log Insight Agents.

Generate a Self-Signed Certificate

You can generate a self-signed certificate for Windows or Linux by using the OpenSSL tool.

Prerequisites

- Download the appropriate installer for OpenSSL from https://www.openssl.org/community/binaries.html. Use the downloaded OpenSSL installer to install it on Windows.
- Edit the `openssl.cfg` file to add additional required parameters. Make sure the `[req]` section has the `req_extensions` parameter defined.

```
[req]
        .
        .
        req_extensions=v3_req #
```

- Add an appropriate Subject Alternative Name entry for the hostname or IP address of your server, for example *server-01.loginsight.domain*. You cannot specify a pattern for the hostname.

```
[v3_req]
        .
        .
        subjectAltName=DNS:server-01.loginsight.domain
        #subjectAltName=IP:10.27.74.215
```

Procedure

1. Create a folder to save your certificate files, for example `C:\Certs\LogInsight`.
2. Open a command prompt and run the following command.

   ```
   C:\Certs\LogInsight>openssl req –x509 –nodes –newkey 2048 –keyout server.key –out server.crt –days
   3650
   ```

   OpenSSL prompts you to supply certificate properties, including country, organization, and so on.
3. Enter the exact IP address or hostname of your vRealize Log Insight server, or the vRealize Log Insight cluster address if load balancing is enabled.

   This property is the only one for which it is mandatory to specify a value.

Two files are created, `server.key` and `server.crt`.

- `server.key` is a new PEM-encoded private key.
- `server.crt` is a new PEM-encoded certificate signed by `server.key`.

What to do next

- Concatenate the certificate files. See Concatenate Certificate Files.
- Upload the signed certificate. See Upload Signed Certificate.

Generate a Certificate Signing Request

Generate a certificate signing request by using the OpenSSL tool for Windows.

Prerequisites

- Download the appropriate installer for OpenSSL from http://www.openssl.org/related/binaries.html . Use the downloaded OpenSSL installer to install it on Windows.
- Edit the `openssl.cfg` file to add additional required parameters. Make sure the `[req]` section has the `req_extensions` parameter defined.

  ```
  [req]
          .
          .
          req_extensions=v3_req #
  ```
- Add an appropriate Subject Alternative Name entry for the hostname or IP address of your server, for example *server-01.loginsight.domain*. You cannot specify a pattern for the hostname.

  ```
  [v3_req]
          .
          .
          subjectAltName=DNS:server-01.loginsight.domain
          #subjectAltName=IP:10.27.74.215
  ```

Procedure

1. Create a folder to save your certificate files, for example `C:\Certs\LogInsight`.
2. Open a Command Prompt and run the following command to generate your private key.

```
C:\Certs\LogInsight>openssl genrsa –out server.key 2048
```

3. Create a certificate signing request by running the following command.

```
C:\Certs\LogInsight>openssl req –new –key server.key –out server.csr
```

Note This command runs interactively and asks you a number of questions. Your certificate authority will cross check your answers. Your answers must match the legal documents regarding the registration of your company.

4. Follow the onscreen instructions and enter the information that will be incorporated into your certificate request.

Important In the Common Name field, enter the hostname or IP address of your server, for example **`mail.your.domain`**. If you want to include all subdomains, enter **`*your.domain`**.

Your certificate signing request file `server.csr` is generated and saved.

Request a Signature from a Certificate Authority

Send your certificate signing request to a Certificate Authority of your choice and request a signature.

Procedure

- Submit your `server.csr` file to a Certificate Authority.

  Note Request that the Certificate Authority encode your file in the PEM format.

  The Certificate Authority processes your request and sends you back a `server.crt` file encoded in the PEM format.

Concatenate Certificate Files

Combine your key and certificate files into a PEM file.

Procedure

1. Create a new `server.pem` file and open it in a text editor.
2. Copy the contents of your `server.key` file and paste it in `server.pem` using the following format.

```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: server.key)
-----END RSA PRIVATE KEY-----
```

3 Copy the contents of your `server.crt` file and paste it in `server.pem` using the following format.

```
-----BEGIN CERTIFICATE-----
  (Your Primary SSL certificate: server.crt)
-----END CERTIFICATE-----
```

4 If the Certificate Authorities provided you with an intermediate or chained certificate, append the intermediate or chained certificates to the end of the public certificate file in the following format.

```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: server.key)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: server.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: DigiCertCA.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----
```

5 Save your `server.pem` file.

Upload Signed Certificate

You can upload a signed SSL certificate.

Procedure

1 Click the configuration drop-down menu icon and select **Administration**.

2 Under Configuration, click **SSL Certificate**.

3 Browse to your custom SSL certificate and click **Open**.

4 Click **Save**.

5 Restart vRealize Log Insight.

What to do next

After vRealize Log Insight restarts, verify that syslog feeds from ESXi continue to arrive in vRealize Log Insight. For troubleshooting, see ESXi Logs Stop Arriving in Log Insight.

Configure SSL Connection Between the vRealize Log Insight Server and the Log Insight Agents

SSL function allows you to provide SSL only connections between the Log Insight Agents and the vRealize Log Insight Server through the secure flow of Ingestion API. You can also configure various SSL parameters of the Log Insight Agents.

vRealize Log Insight Agents communicate over TLSv.1.2. SSLv.3/TLSv.1.0 is disabled to meet security guidelines.

Main SSL Functions

Understanding of the main SSL functions can help you configure the Log Insight Agents properly.

The vRealize Log Insight Agent stores certificates and uses them to verify the identity of the server during all but the first connection to a particular server. If the server identity cannot be confirmed, the vRealize Log Insight Agent rejects connection with server and writes an appropriate error message to the log. Certificates received by the Agent are stored in `cert` folder.

- For Windows go to `C:\ProgramData\VMware\Log Insight Agent\cert`.
- For Linux go to `/var/lib/loginsight-agent/cert`.

When the vRealize Log Insight Agent establishes secure connection with the vRealize Log Insight Server, the Agent checks the certificate received from the vRealize Log Insight Server for validity. The vRealize Log Insight Agent uses system-trusted root certificates.

- The Log Insight Linux Agent loads trusted certificates from `/etc/pki/tls/certs/ca-bundle.crt` or `/etc/ssl/certs/ca-certificates.crt`.
- The Log Insight Windows Agent uses system root certificates.

If the vRealize Log Insight Agent has a locally stored self-signed certificate and receives a different valid self-signed certificate with the same public key, then the agent accepts the new certificate. This can happen when a self-signed certificate is regenerated using the same private key but with different details like new expiration date. Otherwise, connection is rejected.

If the vRealize Log Insight Agent has a locally stored self-signed certificate and receives valid CA-signed certificate, the vRealize Log Insight Agent silently replaces new accepted certificate.

If the vRealize Log Insight Agent receives self-signed certificate after having a CA-signed certificate, the Log Insight Agent rejects it. The vRealize Log Insight Agent accepts self-signed certificate received from vRealize Log Insight Server only when it connects to the server for the first time.

If the vRealize Log Insight Agent has a locally stored CA-signed certificate and receives a valid certificate signed by another trusted CA, the Agent rejects it. You can modify the configuration options of the vRealize Log Insight Agent to accept the new certificate. See Configure the vRealize Log Insight Agent SSL Parameters.

vRealize Log Insight Agents communicate over TLSv.1.2. SSLv.3/TLSv.1.0 is disabled to meet security guidelines.

Enforce SSL-Only Connections

You can use the vRealize Log Insight Web user interface to configure the vRealize Log Insight Agents and the Ingestion API to allow only SSL connections to the server.

The vRealize Log Insight API is normally reachable through HTTP on port 9000 and through HTTPS on port 9543. Both ports can be used by the vRealize Log Insight Agent or custom API clients. All authenticated requests require SSL, but unauthenticated requests, including vRealize Log Insight agent ingestion traffic, can be performed with either. You can force all API request to use SSL connections. The option does not restrict syslog port 514 traffic or affect the vRealize Log Insight user interface, for which HTTP port 80 requests continue redirecting to HTTPS port 443.

Prerequisites

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https:///*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Configuration, click **SSL**.
3. Under the API Server SSL, select **Require SSL Connection**.
4. Click **Save**.

vRealize Log Insight API allows only SSL connections to the server. Non-SSL connections are refused.

Configure the vRealize Log Insight Agent SSL Parameters

You can edit the vRealize Log Insight agent configuration file to change the SSL configuration, add a path to the trusted root certificates, and define whether certificates are accepted by the agent.

This procedure applies to the vRealize Log Insight agents for Windows and Linux.

Prerequisites

For the vRealize Log Insight Linux agent:

- Log in as **root** or use `sudo` to run console commands.
- Log in to the Linux machine on which you installed the vRealize Log Insight Linux agent, open a console and run `pgrep liagent` to verify that the vRealize Log Insight Linux agent is installed and running.

For the vRealize Log Insight Windows agent:

- Log in to the Windows machine on which you installed the vRealize Log Insight Windows agent and start the Services manager to verify that the vRealize Log Insight agent service is installed.

Procedure

1 Navigate to the folder containing the `liagent.ini` file.

Operating system	Path
Linux	`/var/lib/loginsight-agent/`
Windows	`%ProgramData%\VMware\Log Insight Agent`

2 Open the `liagent.ini` file in any text editor.

3 Add the following keys to the `[server]`section of the `liagent.ini` file.

Key	Description
`ssl_ca_path`	Overrides the default storage path for root Certificate Authority-signed certificates, which are used to verify connection peer certificates. Linux: If no value is specified, the agent attempts to load trusted certificates from `/etc/pki/tls/certs/ca-bundle.crt` file or from `/etc/ssl/certs/ca-certificates.crt` file. Windows: If no value is specified, the vRealize Log Insight Windows agent loads certificates from the Windows root certificate store. When a path for `ssl_ca_path` is specified, it overrides the defaults for both Linux and Windows agents. You can specify as a value a file where multiple certificates in PEM format are concatenated or a directory that contains certificates that are in PEM format and have names of the form hash.0 (see -hash option of the x509 utility).
`ssl_accept_any`	Defines whether any certificates are accepted by the vRealize Log Insight agent. The possible values are `yes`, `1`, `no`, or `0`. When the value is set to yes or `1`, the agent accepts any certificate from the server and establish secure connection for sending data. The default value is no.

Key	Description
ssl_accept_any_trusted	The possible values are yes, 1, no, or 0. If the vRealize Log Insight agent has a locally stored trusted Certificate Authority-signed certificate and receives a different valid certificate signed by a different trusted Certificate Authority, it checks the configuration option. If the value is set to yes or 1, the agent accepts the new valid certificate. If the value is set to no or 0, it rejects the certificate and terminates the connection. The default value is no.
ssl_cn	The Common Name of the self-signed certificate. The default value is VMware vCenter Log Insight. You can define a custom Common Name to be checked against the certificate Common Name field. The vRealize Log Insight agent checks the Common Name field of the received certificate against the host name specified for the hostname key in the [server] section. If ithey do not match, the agent checks the Common Name field against the ssl_cn key in the liagent.ini file. If the values match, the vRealize Log Insight agent accepts the certificate.

Note These keys are ignored if SSL is disabled.

4 Save and close the liagent.ini file.

Example: Configuration

The following is an example of the SSL configuration.

```
proto=cfapi
port=9543
ssl=yes
ssl_ca_path=/etc/pki/tls/certs/ca-bundle.crt
ssl_accept_any=no
ssl_accept_any_trusted=yes
ssl_cn=LOGINSIGHT
```

Change the Default Timeout Period for vRealize Log Insight Web Sessions

By default, to keep your environment secure, vRealize Log Insight Web sessions expire in 30 minutes. You can increase or decrease the timeout duration.

You can modify the timeout period by using the Web UI.

Prerequisites

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https:///*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 Click the configuration drop-down menu icon  and select **Administration**.

2 Under Configuration, click **General**.

3 In the Browser Session pane, specify a timeout value in minutes.

The value –1 disables session timeouts.

4 Click **Save**.

Archives

Enable or Disable Data Archiving in vRealize Log Insight

Data archiving preserves old logs that might otherwise be removed from the vRealize Log Insight virtual appliance due to storage constraints. vRealize Log Insight can store archived data to NFS mounts.

vRealize Log Insight collects and stores logs on-disk in a series of 1-GB buckets. A bucket consists of compressed log files and an index. A bucket contains everything necessary to perform queries for a specific time range. When the size of the bucket exceeds 1 GB, vRealize Log Insight stops writing, closes all files in the bucket and seals the bucket.

When you use data archiving, vRealize Log Insight copies raw compressed log files from the bucket to an NFS mount when the bucket is sealed. Buckets that have been sealed when data archiving is not enabled are not retroactively archived.

The path created within an archive export is in the form **`year/month/day/hour/bucketuuid/data.blob`**, using the timestamp at which the bucket was originally created in UTC.

Note vRealize Log Insight does not manage the NFS mount used for archiving purposes. If system notifications are enabled, vRealize Log Insight sends an email when the NFS mount is about to run out of space or is unavailable. If the NFS mount does not have enough free space or is unavailable for longer than the retention period of the virtual appliance, vRealize Log Insight stops ingesting new data. It begins to ingest data again when the NFS mount has enough free space, becomes available, or archiving is disabled.

Prerequisites

- Verify that you have access to an NFS partition that meets the following requirements.
  - The NFS partition must allow reading and writing operations for guest accounts.
  - The mount must not require authentication.
  - The NFS server must support NFS v3.
  - If using a Windows NFS server, allow unmapped user UNIX access (by UID/GID).

- Verify that you are logged in to the vRealize Log Insight*portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is https://*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Configuration, click **Archiving**.
3. Select **Enable Data Archiving** and enter the path to an NFS partition where logs are archived in the form `nfs://servername<:port-number>/exportname`.

   The port number defaults to 2049.
4. Click **Test** to verify the connection.
5. Click **Save**.

Note Data archiving preserves log events that have since been removed from the vRealize Log Insight virtual appliance due to storage constraints. Log events that have been removed from the vRealize Log Insight virtual appliance, but have been archived are no longer searchable. If you want to search archived logs, you must import them into a vRealize Log Insight instance. For more information about importing archived log files, see Import a vRealize Log Insight Archive into vRealize Log Insight.

What to do next

After vRealize Log Insight restarts, verify that syslog feeds from ESXi continue to arrive in vRealize Log Insight. For troubleshooting, see ESXi Logs Stop Arriving in Log Insight.

Format of the vRealize Log Insight Archive Files

vRealize Log Insight archives data in a specific format.

vRealize Log Insight stores archive files on an NFS server and organizes them in hierarchical directories based on archiving time. For example,

`/backup/2014/08/07/16/bd234b2d-df98-44ae-991a-e0562f10a49/data.blob`

where `/backup` is the NFS location, `2014/08/07/16` is the archiving time, `bd234b2d-df98-44ae-991a-e0562f10a49` is the bucket ID, and `data.blob` is the archived data for the bucket.

The archive data `data.blob` is a compressed file that uses vRealize Log Insight internal encoding. It contains the original content for all of the messages stored in the bucket, together with the static fields such as timestamp, host name, source, and appname.

You can import archived data to vRealize Log Insight, export archive data to a raw text file, and extract message content from archive data. See Export a Log Insight Archive to a Raw Text File or JSON and Import a vRealize Log Insight Archive into vRealize Log Insight.

Import a vRealize Log Insight Archive into vRealize Log Insight

Data archiving preserves old logs that might otherwise be removed from the vRealize Log Insight virtual appliance due to storage constraints. See Enable or Disable Data Archiving in vRealize Log Insight. You can use the command line to import logs that have been archived in vRealize Log Insight.

Note Although vRealize Log Insight can handle historic data and real-time data simultaneously, you are advised to deploy a separate instance of vRealize Log Insight to process imported log files.

Prerequisites

- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance.
- Verify that you have access to the NFS server where vRealize Log Insight logs are archived.
- Verify that the vRealize Log Insight virtual appliance has enough disk space to accommodate the imported log files.

  The minimum free space in the `/storage/core` partition on the virtual appliance must equal approximately 10 times the size of the archived log that you want to import.

Procedure

1. Establish an SSH connection to the vRealize Log Insight vApp and log in as the root user.
2. Mount the shared folder on the NFS server where the archived data resides.
3. To import a directory of archived vRealize Log Insight logs, run the following command.

   ```
   /usr/lib/loginsight/application/bin/loginsight repository import Path-To-Archived-Log-Data-Folder.
   ```

   Note Importing archived data might take a long time, depending on the size of the imported folder.
4. Close the SSH connection.

What to do next

You can search, filter, and analyze the imported log events.

Export a Log Insight Archive to a Raw Text File or JSON

You can use the command line to export a vRealize Log Insight archive to a regular raw text file or in JSON format.

Note This is an advanced procedure. Command syntax and output formats might change in later releases of vRealize Log Insight without backward compatibility.

Prerequisites

- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance.

- Verify that the vRealize Log Insight virtual appliance has enough disk space to accommodate the exported files.

Procedure

1. Establish an SSH connection to the vRealize Log Insight vApp and log in as the root user.
2. Create an archive directory on the vRealize Log Insight vApp.

   ```
   mkdir /archive
   ```

3. Mount the shared folder on the NFS server where the archived data resides by running the following command.

   ```
   mount –t nfs archive–fileshare:archive directory path /archive
   ```

4. Check the available storage space on the vRealize Log Insight vApp.

   ```
   df –h
   ```

5. Export a vRealize Log Insight archive to a raw text file.

   ```
   /usr/lib/loginsight/application/sbin/repo–exporter –d archive–file–directory output–file
   ```

   For example,

   ```
   /usr/lib/loginsight/application/sbin/repo–exporter –d /archive/2014/08/07/16/bd234b2d–
   df98–44ae–991a–e0562f10a49 /tmp/output.txt
   ```

6. Export a vRealize Log Insight archive message content in JSON format.

   ```
   /usr/lib/loginsight/application/sbin/repo–exporter –F –d archive–file–directory output–file.
   ```

   For example,

   ```
   /usr/lib/loginsight/application/sbin/repo–exporter –F –d /archive/2014/08/07/16/bd234b2d–
   df98–44ae–991a–e0562f10a49 /tmp/output.json
   ```

7. Close the SSH connection.

Restart the vRealize Log Insight Service

You can restart vRealize Log Insight by using the Administration page in the Web user interface.

Caution Restarting vRealize Log Insight closes all active user sessions. Users of the vRealize Log Insight instance will be forced to log in again.

Prerequisites

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https://*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Management, click **Cluster**.
3. Select a cluster node.
4. Click **Restart Master** and click **Restart**.

What to do next

After vRealize Log Insight restarts, verify that syslog feeds from ESXi continue to arrive in vRealize Log Insight. For troubleshooting, see ESXi Logs Stop Arriving in Log Insight.

Power Off the vRealize Log Insight Virtual Appliance

To avoid data loss when powering off a vRealize Log Insight master or worker node, you must power the node off by following a strict sequence of steps.

You must power off the vRealize Log Insight virtual appliance before making changes to the virtual hardware of the appliance.

You can power off the vRealize Log Insight virtual appliance by using the **Power > Shut Down Guest** menu option in the vSphere Client, by using the virtual appliance console, or by establishing an SSH connection to the vRealize Log Insight virtual appliance and running a command.

Prerequisites

- If you plan to connect to the vRealize Log Insight virtual appliance by using SSH, verify that TCP port 22 is open.
- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance.

Procedure

1. Establish an SSH connection to the vRealize Log Insight vApp and log in as the root user.
2. To power off the vRealize Log Insight virtual appliance, run `shutdown –h now`.

What to do next

You can safely modify the virtual hardware of the vRealize Log Insight virtual appliance.

Download a vRealize Log Insight Support Bundle

If vRealize Log Insight does not operate as expected because of a problem, you can send a copy of the log and configuration files to VMware Support Services in the form of a support bundle.

Downloading a cluster-wide support bundle is necessary only if requested by VMware Support Services. You can create the bundle either statically, which uses disk space on the node, or by streaming, which uses no disk space on the node and stores the bundle on your initiating machine by default.

Prerequisites

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https:///*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Management, click **Cluster**.
3. Under the Support header, click **Download Support Bundle**.

   The vRealize Log Insight system collects the diagnostic information and sends the data to your browser in a compressed tarball.
4. Choose the method to create the bundle.
   - Select **Static support bundle** to create a bundle locally. Creation of the bundle consumes disk space on the node.
   - Select **Streaming support bundle** to start streaming the support bundle immediately. This method uses no disk space on the node.
5. Click **Continue**.
6. In the File Download dialog box, click **Save**.
7. Select a location to which you want to save the tarball archive and click **Save**.

What to do next

You can review the contents of log files for error messages. When you resolve or close issues, delete the outdated support bundle to save disk space.

Join or Leave the VMware Customer Experience Improvement Program

You can join or leave the VMware Customer Experience Improvement Program after deploying vRealize Log Insight

You choose whether to participate in the Customer Experience Improvement Program when you install vRealize Log Insight. After installation, you can join or leave the program by following these steps.

Prerequisites

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https://*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon  and select **Administration**.
2. Under Configuration, click **General**.
3. In the Customer Experience Improvement Program pane, select or clear the **Join the VMware Customer Experience Improvement Program** check box.

   When selected, the option activates the Program and sends data to https://vmware.com.
4. Click **Save**.

Configuring vRealize Log Insight Clusters

5

You can add, remove, and upgrade the nodes of a vRealize Log Insight cluster.

Note WAN clustering is not supported by vRealize Log Insight. Current versions of vRealize Log Insight do not support WAN clustering (also called geoclustering, high-availability clustering or remote clustering). All nodes in the cluster should be deployed in the same Layer 2 LAN. In addition, the ports described in Ports and External Interfaces must be opened between nodes for proper communication.

This section includes the following topics:

Add a Worker Node to a vRealize Log Insight Cluster

Deploy a new instance of the Log Insight virtual applicance and add it to an existing Log Insight master node.

Procedure

1 Deploy the vRealize Log Insight Virtual Appliance

Download the vRealize Log Insight virtual appliance. VMware distributes the vRealize Log Insight virtual appliance as an `.ova` file. Deploy the vRealize Log Insight virtual appliance by using the vSphere Client.

2 Join an Existing Deployment

After you deploy and set up a standalone vRealize Log Insight node, you can deploy a new vRealize Log Insight instance and add it to the existing node to form a vRealize Log Insight cluster.

Deploy the vRealize Log Insight Virtual Appliance

Download the vRealize Log Insight virtual appliance. VMware distributes the vRealize Log Insight virtual appliance as an `.ova` file. Deploy the vRealize Log Insight virtual appliance by using the vSphere Client.

Prerequisites

- Verify that you have a copy of the vRealize Log Insight virtual appliance `.ova` file.
- Verify that you have permissions to deploy OVF templates to the inventory.
- Verify that your environment has enough resources to accommodate the minimum requirements of the vRealize Log Insight virtual appliance. See Minimum Requirements.
- Verify that you have read and understand the virtual appliance sizing recommendations. See Sizing the Log Insight Virtual Appliance.

Procedure

1. In the vSphere Client, select **File > Deploy OVF Template**.
2. Follow the prompts in the **Deploy OVF Template** wizard.
3. On the Select Configuration page, select the size of the vRealize Log Insight virtual appliance based on the size of the environment for which you intend to collect logs.

   Small is the minimum requirement for production environments.

   vRealize Log Insight provides preset VM sizes that you can select from to meet the ingestion requirements of your environment. These presets are certified size combinations of compute and disk resources, though you can add extra resources afterward. A small configuration consumes the fewest resources while remaining supported. An extra small configuration is suitable only for demos.

Option	Log Ingest Rate	Virtual CPUs	Memory	IOPS	Syslog Connections (Active TCP Connections)	Events per Second
Extra Small	6 GB/day	2	4 GB	75	20	400
Small	30 GB/day	4	8 GB	500	100	2000
Medium	75 GB/day	8	16 GB	1000	250	5000
Large	225 GB/day	16	32 GB	1500	750	15,000

   Note You can use a syslog aggregator to increase the number of syslog connections that send events to vRealize Log Insight. However, the maximum number of events per second is fixed and does not depend on the use of a syslog aggregator. A vRealize Log Insight instance cannot be used as a syslog aggregator.

   Note If you select **Large**, you must upgrade the virtual hardware on the vRealize Log Insight virtual machine after the deployment.

4 On the Select Storage page, select a disk format.

- **Thick Provision Lazy Zeroed** creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. The data remaining on the physical device is not erased during creation, but is zeroed out on demand later, on first write from the virtual appliance.
- **Thick Provision Eager Zeroed** creates a type of thick virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create other types of disks.

  Important Deploy the vRealize Log Insight virtual appliance with thick provisioned eager zeroed disks whenever possible for better performance and operation of the virtual appliance.

- **Thin Provision** creates a disk in thin format. The disk grows as the data saved on it grows. If your storage device does not support thick provisioning disks or you want to conserve unused disk space on the vRealize Log Insight virtual appliance, deploy the virtual appliance with thin provisioned disks.

Note Shrinking disks on the vRealize Log Insight virtual appliance is not supported and might result in data corruption or data loss.

5 (Optional) On the Setup networks page, set the networking parameters for the vRealize Log Insight virtual appliance.

If you do not provide network settings, such as an IP address, DNS servers, and gateway information, vRealize Log Insight utilizes DHCP to set those settings.

Caution Do not specify more than two domain name servers. If you specify more than two domain name servers, all configured domain name servers are ignored in the vRealize Log Insight virtual appliance.

Use a comma-separated list to specify domain name servers.

6 (Optional) On the Customize template page, set network properties if you are not using DHCP.

7 (Optional) On the Customize template page, select **Other Properties** and set the root password for the vRealize Log Insight virtual appliance.

The root password is required for SSH. You can also set this password through the VMware Remote Console.

8 Follow the prompts to complete the deployment.

For information on deploying virtual appliances, see the *User's Guide to Deploying vApps and Virtual Appliances*.

After you power on the virtual appliance, an initialization process begins. The initialization process takes several minutes to complete. At the end of the process, the virtual appliance restarts.

9 Navigate to the **Console** tab and check the IP address of the vRealize Log Insight virtual appliance.

IP Address Prefix	Description
https://	The DHCP configuration on the virtual appliance is correct.
http://	The DHCP configuration on the virtual appliance failed. a Power off the vRealize Log Insight virtual appliance. b Right-click the virtual appliance and select **Edit Settings**. c Set a static IP address for the virtual appliance.

What to do next

- If you want to configure a standalone vRealize Log Insight deployment, see Configure New Log Insight Deployment.

  The vRealize Log Insight Web interface is available at https://*log-insight-host*/ where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Join an Existing Deployment

After you deploy and set up a standalone vRealize Log Insight node, you can deploy a new vRealize Log Insight instance and add it to the existing node to form a vRealize Log Insight cluster.

vRealize Log Insight can scale out by using multiple virtual appliance instances in clusters. Clusters enable linear scaling of ingestion throughput, increase query performance, and allow high-availability ingestion. In cluster mode, vRealize Log Insight provides master and worker nodes. Both master and worker nodes are responsible for a subset of data. Master nodes can query all subsets of data and aggregate the results.

Important Configure a minimum of three nodes in a vRealize Log Insight cluster to provide ingestion, configuration, and user space high availability.

Prerequisites

- In the vSphere Client, note the IP address of the worker vRealize Log Insight virtual appliance.
- Verify that you have the IP address or host name of the master vRealize Log Insight virtual appliance.
- Verify that you have an administrator account on the master vRealize Log Insight virtual appliance.
- Verify that the versions of the vRealize Log Insight master and worker nodes are in sync. Do not add an older version vRealize Log Insight worker to a newer version vRealize Log Insight master node.
- You must synchronize the time on the vRealize Log Insight virtual appliance with an NTP server. See Synchronize the Time on the Log Insight Virtual Appliance.
- For information on supported browser versions, see the vRealize Log Insight Release Notes.

Procedure

1. Use a supported browser to navigate to the Web user interface of the vRealize Log Insight worker.

   The URL format is https:///*log_insight-host*/, where *log_insight-host* is the IP address or host name of the vRealize Log Insight worker virtual appliance.

   The initial configuration wizard opens.
2. Click **Join Existing Deployment**.
3. Enter the IP address or host name of the vRealize Log Insight master and click **Go**.

   The worker sends a request to the vRealize Log Insight master node to join the existing deployment.
4. Click **Click here to access the Cluster Management page**.
5. Log in as an administrator.

   The Cluster page loads.
6. Click **Allow**.

   The worker joins the existing deployment and vRealize Log Insight begins to operate in a cluster.

What to do next

- To add another worker, deploy a new vRealize Log Insight instance and add it to the cluster using the startup wizard.
- Repeat the procedure to add a minimum of two vRealize Log Insight worker nodes.

Remove a Worker Node from a vRealize Log Insight Cluster

You can remove a worker node that is no longer working correctly from a vRealize Log Insight cluster and add it to a different cluster or start a standalone deployment. Do not remove worker nodes that are operating correctly from a cluster.

Removing a node results in data loss. If a node must be removed, ensure that it has been backed up first. Avoid removing nodes within 30 minutes of adding new nodes.

Prerequisites

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https:///*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Management, click **Cluster**.

3 In the Workers table, find the node you want, click the pause icon, and click **Continue**.

The node is now in maintenance mode.

Note A node in maintenance mode continues to receive logs.

4 Click to remove the node.

vRealize Log Insight removes the node from the cluster and sends out an email notification.

What to do next

Navigate to the Web user interface of the removed node to configure it. You can add the node to different existing vRealize Log Insight cluster or start a new standalone deployment.

Working with an Integrated Load Balancer

You can enable the vRealize Log Insight integrated load balancer (ILB) on a vRealize Log Insight cluster to ensure that incoming ingestion traffic is accepted by vRealize Log Insight even if some vRealize Log Insight nodes become unavailable. You can also configure multiple virtual IP addresses.

It is highly recommended that you enable the ILB in a vRealize Log Insight cluster environment to properly balance traffic across nodes in a cluster and to minimize administrative overhead.

Note External load balancers are not suggested for use with vRealize Log Insight. Support will be removed in a later version.

It is a best practice to include the ILB in all deployments, including single-node instances. Send queries and ingestion traffic to the ILB so that a cluster can easily be supported in the future if needed.

The ILB ensures that incoming Ingestion traffic is accepted by vRealize Log Insight even if some vRealize Log Insight nodes become unavailable. The ILB also balances incoming traffic fairly among available vRealize Log Insight nodes. vRealize Log Insight clients, using both the Web user interface and ingestion (through Syslog or the Ingestion API), should connect to vRealize Log Insight via the ILB address.

ILB requires that all vRealize Log Insight nodes be on the same Layer 2 network, such as behind the same switch or otherwise able to receive ARP requests from and send ARP requests to each other. The ILB IP address should be set up so that any vRealize Log Insight node can own it and receive traffic for it. Typically, this means that the ILB IP address will be in the same subnet as the physical address of the vRealize Log Insight nodes. After you configure the ILB IP address, try to ping it from a different network to ensure that it is reachable.

To simplify future changes and upgrades, you can have clients point to a FQDN that resolves to the ILB IP address, instead of pointing directly to the ILB IP address.

About Direct Server Return Configuration

The vRealize Log Insight load balancer uses a Direct Server Return (DSR) configuration. In DSR, all incoming traffic passes through the vRealize Log Insight node that is the current load balancer node while return traffic is sent from vRealize Log Insight servers directly back to the client without needing to go through the load balancer node.

Multiple Virtual IP Addresses

You can configure multiple virtual IP addresses (vIPs) for the Integrated Load Balancer. You can also configure a list of static tags to each v IP so that each log message received from the vIP is annotated with the configured tags.

Enable the Integrated Load Balancer

When you enable the vRealize Log Insight integrated load balancer (ILB) on a vRealize Log Insight cluster, you can configure one or more virtual IP addresses. You can optionally enable users to access the cluster via FQDN.

Prerequisites

- Verify that all vRealize Log Insight nodes and the specified Integrated Load Balancer IP address are on the same network.
- The vRealize Log Insight master and worker nodes must have the same certificates. Otherwise the vRealize Log Insight Agents configured to connect through SSL reject the connection. When uploading a CA-signed certificate to vRealize Log Insight master and worker nodes, set the Common Name to ILB IP address during certificate generation request. See Generate a Certificate Signing Request.
- You must synchronize the time on the vRealize Log Insight virtual appliance with an NTP server. See Synchronize the Time on the Log Insight Virtual Appliance.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Management, click **Cluster**.
3. Under Configuration, select **New Virtual IP Address** and enter the virtual IP (vIP) address to use for integrated load balancing.
4. (Optional) To configure multiple virtual IP addresses, click **New Virtual IP Address** and enter the IP Address. You can choose to enter the FQDN and tags.
   - Each vIP should be in the same subnet as at least one network interface on each node and the vIP must be available (not used by any other machine).

- Tags let you add fields with predefined values to events for easier querying. You can add multiple comma-separated tags. All events coming into the system thru a vIP are marked with the vIP's tags.
- You can configure a list of static tags (key=value) for an ILB vIP, so that each log message received from the vIP is annotated with the configured tags.

5 (Optional) To enable vRealize Log Insight users to access the cluster via FQDN, point the clients to the FQDN instead of directly to the configured ILB IP address.

6 Click **Save**.

The Integrated Load Balancer is managed by one node in the vRealize Log Insight cluster, declared the leader for that service. The current leader is denoted by the text (ILB) next to the node.

Query the Results of In-Production Cluster Checks

The in-production cluster check service runs a battery of checks periodically at each node. You can query the latest results of the in-product cluster checks using the CLI.

For example, the service determines if the cluster is running and configured as expected or if there are any issues with integrations to other systems. Additional checks are listed below.

- Is NTP configured in a multi-host deployment?
- Can the Active Directory be reached (if it is currently configured)?
- Can Active Directory authentication occur (if it is currently configured)?
- Can the Active Directory hosts and Kerberos hosts be reached (if Active Directory is currently configured)?
- Is the system running in a non-supported two-host deployment?
- Is there enough space in `/tmp` to perform an upgrade?
- Is there enough space in `/storage/core` to perform an upgrade?
- Is `localhost` correctly placed inside `/etc/hosts`?

Procedure

1 At the command line, establish an SSH connection to the vRealize Log Insight virtual appliance and log in as the root user.

2 In the command line, type `/usr/lib/loginsight/application/sbin/query_check_results.sh` and press **Enter**.

Ports and External Interfaces

6

vRealize Log Insight uses specific required services, ports, and external interfaces.

Communication Ports

vRealize Log Insight uses the communication ports and protocols listed in this topic. The required ports are organized based on whether they are required for sources, for the user interface, between clusters, for external services, or whether they can be safely blocked by a firewall. Some ports are used only if you enable the corresponding integration.

Note vRealize Log Insight does not support WAN clustering (also called geoclustering, high-availability clustering, or remote clustering). All nodes in the cluster should be deployed in the same Layer 2 LAN. In addition, the ports described in this section must be opened between nodes for proper communication.

vRealize Log Insight network traffic has several sources.

Admin workstation	The machine that a system administrator uses to manage the vRealize Log Insight virtual appliance remotely.
User workstation	The machine on which a vRealize Log Insight user uses a browser to access the Web interface of vRealize Log Insight.
System sending logs	The endpoint that sends logs to vRealize Log Insight for analysis and search. For example, endpoints include ESXi hosts, virtuals machines or any system with an IP address.
Log Insight Agents	The agent that resides on a Windows or Linux machine and sends operating system events and logs to vRealize Log Insight over APIs.
vRealize Log Insight appliance	Any vRealize Log Insight virtual appliance, master or worker, where the vRealize Log Insight services reside. The base operating system of the appliance is SUSE 11 SP3.

Ports Required for Sources Sending Data

The following ports need to be open to network traffic from sources that send data to vRealize Log Insight, both for connections from outside the cluster and connections load-balanced between cluster nodes.

Source	Destination	Port	Protocol	Service Description
System sending logs	vRealize Log Insight appliance	514	TCP, UDP	Outbound syslog traffic configured as a Forwarder destination
System sending logs	vRealize Log Insight appliance	1514, 6514	TCP	Syslog data over SSL
vRealize Log Insight Agents	vRealize Log Insight appliance	9000	TCP	Log Insight Ingestion API
vRealize Log Insight Agents	vRealize Log Insight appliance	9543	TCP	Log Insight Ingestion API over SSL

Ports Required for the User Interface

The following ports need to be open to network traffic that needs to use the vRealize Log Insight user interface, both for connections outside the cluster and connections load-balanced between cluster nodes.

Source	Destination	Port	Protocol	Service Description
Admin workstation	vRealize Log Insight appliance	22	TCP	SSH: Secure Shell connectivity
User workstation	vRealize Log Insight appliance	80	TCP	HTTP: Web interface
User workstation	vRealize Log Insight appliance	443	TCP	HTTPS: Web interface

Ports Required Between Cluster Nodes

The following ports should only be open on a vRealize Log Insight master node for network access from worker nodes for maximum security. These are in addition to those ports used for sources and UI traffic that are load-balanced between cluster nodes.

Source	Destination	Port	Protocol	Service Description
vRealize Log Insight appliance	vRealize Log Insight appliance	7000	TCP	Cassandra replication and query
vRealize Log Insight appliance	vRealize Log Insight appliance	9042	TCP	Cassandra service for native protocol clients
vRealize Log Insight appliance	vRealize Log Insight appliance	9160	TCP	Cassandra service for Thrift clients
vRealize Log Insight appliance	vRealize Log Insight appliance	59778, 16520-16580	TCP	vRealize Log Insight Thrift service

Ports Required for External Services

The following ports must be open for outbound networj traffic from vRealize Log Insight cluster nodes to remote services.

Source	Destination	Port	Protocol	Service Description
vRealize Log Insight appliance	NTP server	123	UDP	NTPD: Provides NTP time synchronization **Note** The port is open only if you choose to use NTP time synchronization
vRealize Log Insight appliance	Mail Server	25	TCP	SMTP: mail service for outbound alerts
vRealize Log Insight appliance	Mail Server	465	TCP	SMTPS: mail service over SSL for outbound alerts
vRealize Log Insight appliance	DNS server	53	TCP, UDP	DNS: name resolution service
vRealize Log Insight appliance	AD server	389	TCP, UDP	Active Directory
vRealize Log Insight appliance	AD server	636	TCP	Active Directory over SSL
vRealize Log Insight appliance	AD server	3268	TCP	Active Directory Global Catalog
vRealize Log Insight appliance	AD server	3269	TCP	Active Directory Global Catalog SSL
vRealize Log Insight appliance	AD server	88	TCP, UDP	Kerberos
vRealize Log Insight appliance	vCenter Server	443	TCP	vCenter Server Web Service
vRealize Log Insight appliance	vRealize Operations Manager appliance	443	TCP	vRealize Operations Web service
vRealize Log Insight appliance	Third-party log manager	514	TCP,UDP	syslog data

Source	Destination	Port	Protocol	Service Description
vRealize Log Insight appliance	Third-party log manager	9000	CFAPI	Outbound Log Insight Ingestion API (CFAPI) traffic configured as a Forwarder destination
vRealize Log Insight appliance	Third-party log manager	9543	CFAPI	Outbound Log Insight Ingestion API (CFAPI) traffic configured as a Forwarder destination with encryption (SSL/TLS)

Ports That Can be Blocked

The following ports are open but not used by vRealize Log Insight. These ports can be safely blocked by a firewall.

Destination	Port	Protocol	Service Description
vRealize Log Insight appliance	111	TCP, UDP	RPCbind service that converts RPC program numbers into universal addresses
vRealize Log Insight appliance Tomcat service	9007	TCP	Tomcat services

Monitor the Status of the vRealize Log Insight Windows and Linux Agents

7

You can monitor the status of the vRealize Log Insight Windows and Linux agents and view current statistics about their operation.

Only those agents that are configured to send data through CFAPI appear on the Agents page. Agents that are configured to send data through syslog appear on the Hosts page, as with other syslog sources.

Note If you change a host IP for a vRealize Log Insight server in agent configuration, the agent resets page stats to zero.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the **View Admin** permission. The URL format is https://*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Management, click **Agents**.

What to do next

You can use the information from the Agents page to monitor the operation of the installed vRealize Log Insight Windows and Linux agents.

Enable Agent Auto-Update from the Server

8

You can enable auto-update for all agents from the vRealize Log Insight server.

Auto-update applies the latest available update to all agents connected to the server. You can disable the auto-update feature for individual servers by editing the agent's `liagent.ini` file. For more information, see *Working with vRealize Log Insight Agents*.

Auto-update is disabled for the server by default.

Prerequisites

Agents must have an active status and be version 4.3 or later.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Click **Agents** from the menu on the left.
3. Click the toggle control for **Enable Auto-update for all agents** on the Agents page.

Agents connected to this server are updated when an update is present.

Working with Agent Groups

9

Using vRealize Log Insight server, you can configure agents from within the application's user interface. Agents poll the vRealize Log Insight server on a regular basis to determine if new configurations are available.

You can group agents that require the same configuration. For example, you might group all vRealize Log Insight Windows agents separately from the vRealize Log Insight Linux agents.

In the **All Agents** menu, existing agent groups from content packs are listed automatically. The agents listed relate to content packs that you have already installed, (for example the vSphere content pack) that use agent groups.

Content pack groups are read-only.

Only configuration sections beginning with `[winlog]`, `[filelog]`, and `[parser]` are used in content packs. Additional sections are not exported as part of a content pack. Only single-line comments (lines beginning with `;`) under the `[winlog]`, `[filelog]`, and `[parser]` sections, are preserved in a content pack.

See *Working with vRealize Log Insight Agents* for information about configuring agents including information on merging configurations between local and server-side configurations.

- Agent Group Configuration Merging

  With agent groups, agents can be part of multiple groups and they can belong to the default group *All Agents*—enabling centralized configuration.

- Create an Agent Group

  You can create a group of agents that are configured with the same parameters.

- Edit an Agent Group

  You can edit the name and description of an agent group, change the filters, and edit the configuration.

- Add a Content Pack Agent Group as an Agent Group

  You can add an agent group that was defined as part of a content pack to your active groups and apply an agent configuration to the group.

- Delete an Agent Group

  You can delete an agent group to remove it from the active groups list.

Agent Group Configuration Merging

With agent groups, agents can be part of multiple groups and they can belong to the default group *All Agents*—enabling centralized configuration.

Merging occurs server-side—and the resulting configuration is merged with the agent-side configuration. The merged configuration is a result of the following rules.

- The individual group configurations have a higher priority and overrides the All Agents group settings.
- The All Agents group configuration overrides the local configuration.
- You cannot configure sections with the same name in different groups except with the All Agents groups. However, the sections in individual groups have a higher priority.

Note To prevent agent loss, the **hostname** and **port** parameters of an agent configuration cannot be changed centrally from the server.

The merged configuration is stored in the agent-side `liagent-effective.ini` file.

Create an Agent Group

You can create a group of agents that are configured with the same parameters.

Prerequisites

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https://*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Management, click **Agents**.
3. In the **All Agents** menu, click **New Group**.
4. Provide a unique name and a description for the agent group and click **New Group**.

   The agent group is created and appears in the **All Agents** list, but is not saved.
5. Specify one or more of the following filters to the agent group.

   Filters can contain wildcards, such as * and ?.

   - IP address
   - hostname

- version
- OS

For example, you can select the OS filter `contains` and specify the value `windows` to identify all your Windows agents for configuration.

6 Specify the agent configuration values in the Agent Configuration area and click **Save New Group**.

The agent configuration is applied after the next polling interval.

Edit an Agent Group

You can edit the name and description of an agent group, change the filters, and edit the configuration.

Prerequisites

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https://*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 Click the configuration drop-down menu icon and select **Administration**.

2 Under Management, click **Agents**.

3 In the **All Agents** menu, select the name of the appropriate agent group and click the pencil icon to edit it.

4 Make your changes.

Item to Edit	Action
Name or **Description**	Make the necessary changes and click **Save**.
Filters or **Configuration**	Make the necessary changes and click **Save Group**.

Add a Content Pack Agent Group as an Agent Group

You can add an agent group that was defined as part of a content pack to your active groups and apply an agent configuration to the group.

Prerequisites

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https://*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 Click the configuration drop-down menu icon and select **Administration**.

2 Under Management, click **Agents**.

3 In the **All Agents** menu, select an agent template for the Available Templates list.

4 Click **Copy Template** to copy the content pack agent group to your active groups.

5 Click **Copy**.

6 Select the required filters and click **Save new group**.

The content pack agent group is added to the active groups and the agents are configured according to the filters that you specified.

Delete an Agent Group

You can delete an agent group to remove it from the active groups list.

Prerequisites

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https://*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 Click the configuration drop-down menu icon and select **Administration**.

2 Under Management, click **Agents**.

3 In the **All Agents** menu, select the name of the agent group to delete, by clicking the X icon next to its name.

4 Click **Delete**.

The agent group is removed from the active groups.

Configuring and Using the vRealize Log Insight Importer

10

The vRealize Log Insight Importer is a command-line utility used to import offline logs of historical data from local machines to the vRealize Log Insight server.

vRealize Log Insight is a real-time log analysis tool that streams syslog events or agent events into vRealize Log Insight, but there may be times when you need to import logs that were collected in the past. With vRealize Log Insight Importer, you can import support bundles and archived logs to ingest data that was collected over a period of time. You can analyze logs from support bundles gathered from vRealize Log Insight or any VMware product.

vRealize Log Insight Importer includes the following features and capabilities.

- vRealize Log Insight Importer sends data over the ingestion API.
- It supports filelog collection, including recursive directory collection.
- The Importer can read data from zip, tar, or gz archive files.
- You can specify that data be read recursively from a nested archive, such as a nested zip file, or specify a directory within an archive.
- 7-Zip is not supported.

Using vRealize Log Insight Importer

Ensure that vRealize Log Insight has access to the NFS server on which archived data is stored. If the NFS server becomes inaccessible due to network failure or errors on the NFS server, the import of archived data might fail. Be aware of the following restrictions apply when working with vRealize Log Insight Importer.

When logs are extracted from a bundle during ingestion, a log bundle name is automatically determined and added as a bundle tag to all extracted logs. The tag name is the filename of the log or the directory name in case of directory sources. Bundle tags differentiate bundles on a vRealize Log Insight Server.

This tag overrides any tags with the same name that are specified in the manifest file. The tag can be overridden by command line tags that use the same name.

The following limitations are in effect:

- vRealize Log Insight Importer does not check for available disk space on the vRealize Log Insight virtual appliance. Therefore, the import of archived logs might fail if the virtual appliance runs out of disk space.
- vRealize Log Insight does not display progress information during log imports. As the import of archived data is in progress, you are unable to infer from the console output how much time is left before the import finishes or how much data is already imported.

Supported Operating Systems

The vRealize Log Insight Importer is supported on the following operating systems:

- Windows 32 bit and 64 bit
- Linux 32 bit and 64 bit

The Linux version does not run on an Apple Macintosh system.

This section includes the following topics:

About the vRealize Log Insight Importer Manifest File

vRealize Log Insight Importer uses a manifest configuration file to determine the log format and to specify the location of the data to import. The manifest file has the same format as the `liagent.ini` configuration file and is similar in structure.

You can create your own manifest files to import arbitrary log files. Although creating a manifest file is optional, if you use a manifest file, you do not need to know the absolute path to the data files.

If you do not create a manifest file, vRealize Log Insight Importer uses the default manifest which collects all `.txt` and `.log` files (`include=*.log*;*.txt*`) and applies the auto parser (extracts timestamp + kvp) on the extracted logs.

If the `liagent.ini` configuration file is used as a manifest file, vRealize Log Insight Importer extracts only the `[filelog]` sections as a manifest. All options for the `[filelog]` section are supported in vRealize Log Insight Importer.

For additional options supported in the `[filelog]` section and configuration examples, see the vRealize Log Insight agent documentation in the *vRealize Log Insight Agent Administration Guide*.

To Create a Manifest File

You can copy and paste the contents of the agent configuration file into a new .txt file. To identify a dynamic path, remove the leading " / " before the directory path.

Specifying the Directory Path

The directory specified in the `[filelog]` section can be either relative to the source or absolute. To specify a relative path, do not include the leading slash under Linux, otherwise the path is treated by vRealize Log Insight Importer as absolute.

To indicate name patterns in the value of the directory key, you can use the * and ** characters.

- Use * as a placeholder for a single directory. Use it to indicate one level of nesting with an arbitrary folder name. For example, use `directory = log_folder_*` to indicate any folder that starts with the string `log_folder_`.
- Use ** to indicate an arbitrary level of nesting with any folder name. For example, you can use `directory = **/log` to indicate any folder with the name `log` at any level of nesting within the source directory.

Install, Configure, and Run the vRealize Log Insight Importer

You can install vRealize Log Insight Importer on Windows and Linux. You can also install the vRealize Log Insight Importer on a vRealize Log Insight server and run it from the server.

Prerequisites

- Verify that you can access the VMware Download site to download the vRealize Log Insight Importer.
- Review About the vRealize Log Insight Importer Manifest File and create a manifest file to use with the importer. For more information, see vRealize Log Insight Importer Manifest File Configuration Examples.
- Review the vRealize Log Insight Importer Configuration Parameters to identify the required and available optional parameters.
- If you use the `honor_timestamp` parameter, verify that you have appropriate login credentials.
- If you import a support bundle, you must configure the `honor_timestamp` and the user name and password.

Procedure

1. Download the vRealize Log Insight Importer installation package from the VMware Download site and install the tool on your system. The installation packages include the MSI installer for Windows and POSIX installation packages (RPM, DEB and BIN) for Linux.

   The vRealize Log Insight Importer tool is installed in the following locations.

Operating System	File Name	Installation Location
Windows	loginsight-importer.exe	C:\Program Files (x86)\VMware\Log Insight Importer
Linux	loginsight-importer	/usr/lib/loginsight-importer

Note

- After installation, the importer installation directory is added to the PATH environment variable on Windows, and a symlink to the `loginsight-importer` executable is added to `/usr/bin/` on Linux. So the client can call `loginsight-importer` from the shell without specifying a path prefix.
- When you install vRealize Log Insight Importer, a number of VMware product manifest files are also installed. You can use these files or modify them for your needs when running vRealize Log Insight Importer. These manifest files are located in `C:\Program Files (x86)\VMware\Log Insight Importer\Manifests` for Windows, and `/usr/lib/loginsight-importer/manifests` for Linux.
- If you uninstall the `.bin` package, you need to delete the `/usr/bin/loginsight_importer` symlink also.

2 Start the vRealize Log Insight Importer tool by entering the following command at a command prompt.

```
/usr/bin/loginsight-importer.exe
```

3 Enter the manifest file name at the prompt.

4 Define the configuration parameters and press **Enter**.

vRealize Log Insight Importer begins to extract the log entries from the directories specified in the parameters. The total number of processed files, extracted log messages, sent log messages, and the run time is displayed.

5 After the import is complete, press **Ctrl+C** on Windows or Linux to exit the tool.

What to do next

From the vRealize Log Insight Interactive Analytics tab, you can refresh the view to list the imported log events. If you imported a support bundle and used the `honor_timestamp`, the Dashboard should also display the events over time.

vRealize Log Insight Importer Manifest File Configuration Examples

The sample vRealize Log Insight Importer manifest files provide examples of parameter configurations.

The value of the directory key should be either relative to the source or absolute. The following example shows how to collect logs from files with a `.log` extension which reside two levels lower than the source directory and name of the last folder ends with the `_log` string.

```
[filelog|importer_test]
directory=*\*_log
include=*.log
event_marker=^\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2} [A-Z]{4} LOG
```

The following example shows how to collect all files with the extension `.log` from all sub-folders of the source directory including the source itself.

```
[filelog|sbimporter_test_channel]
directory = **
include = *.log
```

The following example shows how to collect logs from all files in the source directory (but not from sub-folders) except files that have an `.ini` extension. We interpret files as UTF-16LE encoded.

```
[filelog|quotes_channe3]
directory=
charset=UTF-16LE
exclude=*.ini
tags={"Provider" : "Apache"}
```

The following example shows how to collect logs from all files with the extension `.log` in the source directory (but not from sub-folders). The timestamp of events is parsed in the log file using the Common Log Format (CLF) parser and the extracted historical timestamp is applied. The log format parsed by the CLF parser is `2015-03-25 22:11:46,786 | DEBUG | pool-jetty-76 | AuthorizationMethodInterceptor | Authorizing method: public abstract`.

```
[filelog|vcd-container-debug]
directory=
include=*.log
parser=vcd

[parser|vcd]
base_parser=clf
format=%{%Y-%m-%d %H:%M:%S%f}t %M
```

vRealize Log Insight Importer Configuration Parameters

The vRealize Log Insight Importer configuration includes required and optional parameters.

Required Parameters	Description
`--source <path>`	Specifies the path to the support bundle directory or path to the zip, gzip, or tar archive of the bundle. The value is added to all send messages as the value of the `bundle` tag.
`--server <hostname>`	Destination server hostname or IP address.

Options	Description
`--port <port>`	Port for connection. If not set then port 9000 is used for non-SSL connections and port 9543 is used for an SSL connection.
`--logdir <path>`	Specifies the path to the logs directory. If this is not set, the path is: $(LOCALAPPDATA)\VMware\Log Insight Importer\log on Windows and ~/.loginsight-importer/log on Linux.
`--manifest <file-path>`	Specifies the path to the manifest file (.ini format). If this is not set, the `importer.ini` file in the source directory is used. If the `importer.ini` file does not exist or is not found in the source directory, vRealize Log Insight Importer will apply the default (hardcoded) manifest and collect all `.txt` and `.log` files (`include=*.log*;*.txt*`), and also apply the auto parser (extracts timestamp + kvp).
`--no_ssl`	Do not use SSL for connections. This should not be set for authenticated connections (for example if --honor_timestamp is used).
`--ssl_ca_path <path>`	Path to the trusted root certificates bundle file.
`--tags <tags>`	Set tags for all sent events. For example `--tags "{ \"tag1\" : \"value1\", \"tag2\":\"value2\"}"` **Note** The tags option can accept `hostname` as a tag name. The value of the `hostname` tag from the command line is used instead of the FQDN of the sending machine as the value of the `hostname` field for all events extracted by vRealize Log Insight Importer. This is opposite of the tags parameter in the manifest file and extracted fields by parsers, which ignore the `hostname` field. A log bundle name, either a filename or a directory name in case of directory sources, is automatically determined and added as a `bundle` tag to all logs extracted from that specific bundle during the ingestion. This tag helps you to differentiate bundles on vRealize Log Insight Server. A `bundle` tag overrides tags with that same name from manifest file. But it can be overridden by command line tags, if there is one with `bundle` name.
`--username <username >`	Username for authentication. Required if `--honor_timestamp` is set.
`--password <password>`	Password for authentication. Required if `--honor_timestamp` is set. The username/password pair disables the allowed time-drift on vRealize Log Insight server so it is possible to import data with a historical timestamp.

Options	Description
`--honor_timestamp`	Applies the extracted timestamp. The configured parsers extract the timestamp from the log entries and the `--honor_timestamp` applies the extracted timestamp. ■ If the timestamp is extracted using configured parsers, then the events will have that timestamp applied. ■ If there is an event in the logs file, with no extracted timestamp, then the successfully extracted timestamp from the previous event in the same log file will be applied. ■ If no timestamp is found or parsed in the file then the `MTIME` of the log file will be applied as the timestamp. **Note** If a manifest file was not provided, the default hardcoded manifest that the vRealize Log Insight Importer will use has the Automatic Log parser enabled. In this case, vRealize Log Insight Importer extracts the timestamp from the log entries if the `--honor_timestamp` parameter is used.
`--debug_level <1|2>`	Increases the verbosity level of the log file. This should only be changed when troubleshooting. Under normal operations this flag should not be used.
`--help`	Display help and exit.

Monitoring vRealize Log Insight 11

You can monitor the vRealize Log Insight virtual appliance and the hosts and devices that send log events to vRealize Log Insight.

This section includes the following topics:

Check the Health of the vRealize Log Insight Virtual Appliance

You can check available resources and active queries on the vRealize Log Insight virtual appliance, and view current statistics about the operation of vRealize Log Insight.

Prerequisites

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https://*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Management, click **System Monitor**.
3. If vRealize Log Insight is running as a cluster, click **Show resources for** and choose the node you want to monitor.

4 Click the buttons on the System Monitor page to view the information that you need.

Option	Description
Resources	View information about the CPU, memory, IOPS (read and write activity), and storage usage on the vRealize Log Insight virtual appliance. The charts on the right represent historical data for the last 24 hours, and are refreshed at five-minute intervals. The charts on the left display information for the last five minutes, and are refreshed every three seconds.
Active Queries	View information about the queries that are currently active in vRealize Log Insight.
Statistics	View statistics about the log ingest operations and rates. To view more detailed statistics, click **Show advanced statistics**.

What to do next

You can use the information from the System Monitor page to manage resources on the vRealize Log Insight virtual appliance.

Monitor Hosts That Send Log Events

You can view a list of all hosts and devices that send log events to vRealize Log Insight and monitor them.

Entries in host tables expire three months after the last ingested event.

Prerequisites

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https:///*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 Click the configuration drop-down menu icon and select **Administration**.

2 Under Management, click **Hosts**.

Note If you have configured a vCenter Server to send events and alarms, but have not configured the individual ESXi hosts to send logs, the Hostname column lists both the vCenter Server and the individual ESXi hosts as the source instead of listing just the vCenter Server.

Integrating vRealize Log Insight with VMware Products

12

vRealize Log Insight can integrate with other VMware products to use events and log data, and to provide better visibility into events that occur in a virtual environment.

Integration with VMware vSphere

vRealize Log Insight Administrator users can set up vRealize Log Insight to connect to vCenter Server systems at two-minute intervals, and collect events, alarms, and tasks data from these vCenter Server systems. In addition, vRealize Log Insight can configure ESXi hosts via vCenter Server. See Connect vRealize Log Insight to a vSphere Environment.

Integration with VMware vRealize Operations Manager

You can integrate vRealize Log Insight with vRealize Operations Manager vApp and vRealize Operations Manager Installable. Integrating with the Installable version requires additional changes to the vRealize Operations Manager configuration. For information about configuring vRealize Operations Manager Installable to integrate with vRealize Log Insight, see the *Log Insight Getting Started Guide*.

vRealize Log Insight and vRealize Operations Manager can be integrated in two independent ways.

Notification Events	vRealize Log Insight Administrator users can set up vRealize Log Insight to send notification events to vRealize Operations Manager based on queries that you create. See Configure vRealize Log Insight to Send Notification Events to vRealize Operations Manager.
Launch in Context	Launch in context is a feature in vRealize Operations Manager that lets you launch an external application via URL in a specific context. The context is defined by the active UI element and object selection. Launch in context lets the vRealize Log Insight adapter add menu items to a number of different views within the Custom user interface and the vSphere user interface of vRealize Operations Manager. See Enable Launch in Context for vRealize Log Insight in vRealize Operations Manager.

Note Notification events do not depend on the launch in context configuration. You can send notification events from vRealize Log Insight to vRealize Operations Manager even if you do not enable the launch in context feature.

If the environment changes, vRealize Log Insight administrator users can change, add, or remove vSphere systems from vRealize Log Insight, change or remove the instance of vRealize Operations Manager to which alert notifications are sent, and change the passwords that are used to connect to vSphere systems and vRealize Operations Manager.

This section includes the following topics:

- Connect vRealize Log Insight to a vSphere Environment
- Configure vRealize Log Insight to Pull Events, Tasks, and Alarms from vCenter Server Instance
- Using vRealize Operations Manager with vRealize Log Insight
- vRealize Operations Manager Content Pack for vRealize Log Insight

Connect vRealize Log Insight to a vSphere Environment

Before you configure vRealize Log Insight to collect alarms, events, and tasks data from your vSphere environment, you must connect vRealize Log Insight to one or more vCenter Server systems.

vRealize Log Insight can collect two types of data from vCenter Server instances and the ESXi hosts that they manage.

- Events, tasks, and alerts are structured data with specific meaning. If configured,vRealize Log Insight pulls events, tasks, and alerts from the registered vCenter Server instances.
- Logs contain unstructured data that can be analyzed in vRealize Log Insight. ESXi hosts or vCenter Server Appliance instances can push their logs to vRealize Log Insight through syslog.

Prerequisites

- For the level of integration that you want to achieve, verify that you have user credentials with enough privileges to perform the necessary configuration on the vCenter Server system and its ESXi hosts.

Level of Integration	Required Privileges
Events, tasks, and alarms collection	■ **System.View** **Note** **System.View** is a system-defined privilege. When you add a custom role and do not assign any privileges to it, the role is created as a Read Only role with three system-defined privileges: **System.Anonymous**, **System.View**, and **System.Read**.
Syslog configuration on ESXi hosts	■ **Host.Configuration.Change settings** ■ **Host.Configuration.Network configuration** ■ **Host.Configuration.Advanced Settings** ■ **Host.Configuration.Security profile and firewall**

  Note You must configure the permission on the top-level folder within the vCenter Server inventory, and verify that the **Propagate to children** check box is selected.

- Verify that you know the IP address or domain name of the vCenter Server system.
- Verify that you are logged in to the vRealize Log Insight*portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is https:///*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Integration, click **vSphere**.
3. Type the IP address and credentials for a vCenter Server, and click **Test Connection**.

   It is recommended that you use service account credentials.
4. (Optional) To register another vCenter Server, click **Add vCenter Server** and repeat steps 3 through 5.

   Note Do not register vCenter Server systems with duplicate names or IP addresses.
   vRealize Log Insight does not check for duplicate vCenter Server names. You must verify that the list of registered vCenter Server systems does not contain duplicate entries.
5. Click **Save**.

What to do next

- Start collecting events, tasks, and alarms data from the vCenter Server instance that you registered. See Configure vRealize Log Insight to Pull Events, Tasks, and Alarms from vCenter Server Instance.
- Start collecting syslog feeds from the ESXi hosts that the vCenter Server manages. See Configure an ESXi Host to Forward Log Events to vRealize Log Insight.

vRealize Log Insight as a Syslog Server

vRealize Log Insight includes a built-in syslog server that is constantly active when the vRealize Log Insight service is running.

The syslog server listens on ports 514/TCP, 1514/TCP, and 514/UDP, and is ready to ingest log messages that are sent from other hosts. Messages that are ingested by the syslog server become searchable in the vRealize Log Insight Web user interface near real time. The maximum syslog message length that vRealize Log Insight accepts is 10 KB.

Configure an ESXi Host to Forward Log Events to vRealize Log Insight

ESXi hosts or vCenter Server Appliance instances generate unstructured log data that can be analyzed in vRealize Log Insight.

You use the vRealize Log Insight Administration interface to configure ESXi hosts on a registered vCenter Server to push syslog data to vRealize Log Insight.

Caution Running parallel configuration tasks might result in incorrect syslog settings on the target ESXi hosts. Verify that no other administrative user is configuring the ESXi hosts that you intend to configure.

A vRealize Log Insight cluster can use an integrated load balancer to distribute ESXi and vCenter Server Appliance syslog feeds between the individual nodes of the cluster.

For information on filtering syslog messages on ESXi hosts before messages are sent to vRealize Log Insight, see the *Configure Log Filtering on ESXi Hosts* topic in the Setting Up ESXi section, of the **vSphere Installation and Setup** guide.

For information on configuring syslog feeds from a vCenter Server Appliance, see Configure vCenter Server to Forward Log Events to vRealize Log Insight.

Note vRealize Log Insight can receive syslog data from ESXi hosts version 5.5 and later.

Prerequisites

- Verify that the vCenter Server that manages the ESXi host is registered with your vRealize Log Insight instance. Or, you can register the ESXi host and configure vCenter Server in a single operation.
- Verify that you have user credentials with enough privileges to configure syslog on ESXi hosts.
  - **Host.Configuration.Advanced settings**
  - **Host.Configuration.Security profile and firewall**

  Note You must configure the permission on the top-level folder within the vCenter Server inventory, and verify that the **Propagate to children** check box is selected.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Integration, click **vSphere**.
3. Locate the vCenter Server instance that manages the ESXi host from which you want to receive syslog feeds.
4. Select the **Configure ESXi hosts to send logs to Log Insight** check box.

   By default, vRealize Log Insight configures all reachable ESXi hosts of version 5.5 and later to send their logs through UDP.
5. (Optional) To modify the default configuration values, click **Advanced Options**.
   - To change the protocol for all ESXi hosts, select **Configure all ESXi hosts**, select a protocol, and click **OK**.
   - To set up specific ESX hosts logging only or to change the protocol for selected ESXi hosts, use the following steps:
     a. Select **Configure specific ESXi hosts**.
     b. Select one or more hosts from the **Filter by host** list.
     c. Set protocol value.
     d. Click **OK**.
6. (Optional) If you are using clusters, open the drop-down menu for the **Target** text box and select the hostname or IP address for the load balancer that distributes syslog feeds.
7. Click **Save**.

Modify an ESXi Host Configuration for Forwarding Log Events to vRealize Log Insight

ESXi hosts or vCenter Server Appliance instances generate unstructured log data that can be analyzed in vRealize Log Insight.

You use the vRealize Log Insight Administration interface to configure ESXi hosts on a registered vCenter Server to push syslog data to vRealize Log Insight.

Caution Running parallel configuration tasks might result in incorrect syslog settings on the target ESXi hosts. Verify that no other administrative user is configuring the ESXi hosts that you intend to configure.

After the initial configuration is set up, you can enable an option to automatically configure an ESXi host with the default protocol when it is added to a cluster.

A vRealize Log Insight cluster can use an integrated load balancer to distribute ESXi and vCenter Server Appliance syslog feeds between the individual nodes of the cluster.

For information on filtering syslog messages on ESXi hosts before configuredmessages are sent to vRealize Log Insight, see the *Configure Log Filtering on ESXi Hosts* topic in the Setting Up ESXi section, of the **vSphere Installation and Setup** guide.

For information on configuring syslog feeds from a vCenter Server Appliance, see Configure vCenter Server to Forward Log Events to vRealize Log Insight.

Note vRealize Log Insight can receive syslog data from ESXi hosts version 5.5 and later.

Prerequisites

- Verify that the vCenter Server that manages the ESXi host is registered with your vRealize Log Insight instance.
- Verify that you have user credentials with enough privileges to configure syslog on ESXi hosts.
  - **Host.Configuration.Advanced settings**
  - **Host.Configuration.Security profile and firewall**

  Note You must configure the permission on the top-level folder within the vCenter Server inventory, and verify that the **Propagate to children** check box is selected.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Integration, click **vSphere**.
3. Select the **Configure ESXi hosts to send logs to Log Insight** check box.
4. Click **Advanced Options**.
5. To change the protocol for selected ESXi hosts, use the following steps:
   a. Select one or more hosts from the **Filter by host** list.
   b. Set protocol value.
   c. To choose to have an ESXi host configured automatically with the default protocol when it is added to a vRealize Log Insight cluster, select **Automatically configure all ESXi hosts**.
   d. Click **Configure**.
6. (Optional) If you are using clusters, you can specify a load balancer by opening the drop-down menu for the **Target** text box on the **vSphere Integration** screen and selecting the hostname or IP address for the load balancer.

vRealize Log Insight Notification Events in vRealize Operations Manager

You can configure vRealize Log Insight to send notification events to vRealize Operations Manager based on the alert queries that you create.

When you configure a notification alert in vRealize Log Insight, you select a resource in vRealize Operations Manager that is associated with the notification events. See Add an Alert Query in Log Insight to Send Notification Events to vRealize Operations Manager.

Listed below are sections of the vRealize Operations Manager UI where notification Events appear.

- Home > **Recommendations** dashboard > **Top Health Alerts For Descendants** widget
- Home > **Alerts** Tab
- On all Custom Dashboards that include widgets with notification events

For additional information on where notification events appear, see the VMware vRealize Operations Manager Documentation Center.

Configure vCenter Server to Forward Log Events to vRealize Log Insight

The vSphere Integration collects task and events from vCenter Server, but not the low-level internal logs from each vCenter Server component. These logs are leveraged by the vSphere Content Pack.

Configuration for vCenter Server 6.5 and later releases should be done through the vCenter Server Appliance Management Interface. For more information about how to forward log events from vCenter Server, see vSphere documentation about redirecting vCenter Server Appliance log files to another machine.

For earlier versions of vSphere, although the vCenter Server Appliance does contain a syslog daemon that could be used to route logs, the preferred method is to install a vRealize Log Insight agent.

For information about installing vRealize Log Insight agents, see the *vRealize Log Insight Agent Administration Guide* in the vRealize Log Insight Information Center.

The vSphere content pack contains agent groups defining specific log files to collect from vCenter Server installations. The configuration is visible at `https://LogInsightServerFqdnOrIP/contentpack?contentPackId=com.vmware.vsphere`.

For information about working with agent groups, see Chapter 9 Working with Agent Groups

For information about vCenter Server log file locations, see `http://kb.vmware.com/kb/1021804` and `http://kb.vmware.com/kb/1021806`.

Configure vRealize Log Insight to Pull Events, Tasks, and Alarms from vCenter Server Instance

Events, tasks, and alerts are structured data with specific meaning. You can configure vRealize Log Insight to collect alarms, events, and tasks data from one or more vCenter Server systems.

You use the Administration UI to configure vRealize Log Insight to connect to vCenter Server systems. The information is pulled from the vCenter Server systems by using the vSphere Web Services API and appears as a vSphere content pack in the vRealize Log Insight Web user interface

Note vRealize Log Insight can pull alarms, events, and tasks data only from vCenter Server 5.1 and later.

Prerequisites

Verify that you have user credentials with **System.View** privileges.

Note You must configure the permission on the top-level folder within the vCenter Server inventory, and verify that the **Propagate to children** check box is selected.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Integration, click **vSphere**.
3. Locate the vCenter Server instance from which you want to collect data, and select the **Collect vCenter Server events, tasks, and alarms** check box.
4. Click **Save**.

vRealize Log Insight connects to the vCenter Server every two minutes and ingests all new information since the last successful poll.

What to do next

- Analyze vSphere events using the vSphere content pack or custom queries.
- Enable vSphere content pack alerts or custom alerts.

Using vRealize Operations Manager with vRealize Log Insight

Requirements for Integrating With vRealize Operations Manager

To integrate vRealize Log Insight with vRealize Operations Manager, you must specify credentials for vRealize Log Insight to authenticate against vRealize Operations Manager. vRealize Operations Manager supports both local user accounts and multiple LDAP sources.

To determine the username for a local user account:

1 Open the vRealize Operations Manager web interface.

2 Select **Access Control**.

3 Identify or create the integration user. The Source Type field is **Local User**.

4 The username that should be entered within the vRealize Log Insight administration user interface is the content of the **User Name** field.

To determine the user name format for the LDAP user account that must be provided in vRealize Log Insight, follow these instructions:

1 Open the vRealize Operations Manager web interface.

2 Select Access Control.

3 Identify or create the integration user. Note the **User Name** and **Source Type** fields. For example, a user named **`integration@example.com`** from the source **Active Directory - ad**.

4 Select **Authentication Sources**.

5 Identify the authentication source corresponding to the **Source Type** from Step 3. Note the **Source Display Name** field. For example, "ad".

6 The username that should be entered within the vRealize Log Insight administration user interface is combined from Step 3 and Step 5, in the form UserName@SourceDisplayName. For example, integration@example.com@ad.

Prerequisites

Verify that the integration user account has permissions to manipulate objects in vRealize Operations Manager. See Minimum Required Permissions for a Local or Active Directory User Account.

Minimum Required Permissions for a Local or Active Directory User Account

To integrate vRealize Log Insight with vRealize Operations Manager, you must specify credentials for vRealize Log Insight to authenticate against vRealize Operations Manager. To manipulate objects in vRealize Operations Manager, a user account must have the required permissions.

vRealize Operations Manager License

If you assign permissions to a user for Launch in Context, the user can also configure alert integration. Use the information in the alert integration table to assign permissions for alert integration only.

Table 12-1. Alert Integration

Action	Permissions and Objects to Select
Create a custom role with the listed permissions.	1 Administration -> Resource Kind Management [Check All] 2 Administration -> Resource Management [Check All] 3 Administration -> Rest APIs a All other, Read, Write APIs b Read access to APIs
Assign the preceding role to the local or Active Directory user (new or existing) and select objects/object hierarchies to assign.	1 Adapter Instance -> vRealizeOpsMgrAPI [Check All] 2 vSphere Hosts and Clusters [Check All] 3 vSphere Networking [Check All] 4 vSphere Storage [Check All]

For Launch in Context Integration to work, a user with administrator privilege is required. If both Alert and Launch in Context are enabled, a user with administrator privileges is required.

Action	Permissions and Objects to Select
Assign the Adminstrator role to a user account.	From the **Objects** tab on the **Assign Groups and Permissions** page: 1 For **Select Role**, choose **Administrator**. 2 Select **Assign this role to the user**. 3 Select **Allow Access to All Objects in the System**.

Configure vRealize Log Insight to Send Notification Events to vRealize Operations Manager

You can configure vRealize Log Insight to send alert notifications to vRealize Operations Manager.

You can integrate vRealize Log Insight with vRealize Operations Manager vApp and vRealize Operations Manager Installable. Integrating with the Installable version requires additional changes to the vRealize Operations Manager configuration. For information about configuring vRealize Operations Manager Installable to integrate with vRealize Log Insight, see the *Log Insight Getting Started Guide*.

Integrating vRealize Log Insight alerts with vRealize Operations Manager allows you to view all information about your environment in a single user interface.

You can send notification events from multiple vRealize Log Insight instances to a single vRealize Operations Manager instance. You can enable launch in context for a single vRealize Log Insight instance per vRealize Operations Manager instance.

vRealize Log Insight uses the vRealize Operations Manager REST API to create resources and relationships in vRealize Operations Manager for configuring the launch-in-context adapter.

Prerequisites

- Create an integration user account in vRealize Operations Manager with required permissions. For more information, see Requirements for Integrating With vRealize Operations Manager.

- Verify that you know the IP address or host name of the target vRealize Operations Manager instance.
- Verify that you are logged in to the vRealize Log Insight*portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is https:///*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Note In an environment running a vRealize Operations Manager cluster with a configured load balancer, you can use the load balancer IP address if one is available.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Integration, select **vRealize Operations Manager**.
3. Type the IP address or host name of the master node or the load balancer if one is configured. Use a vRealize Operations Manager user credential and click **Test Connection**. vRealize Log Insight uses the credentials to push notification events to vRealize Operations Manager. Make sure that the configured user has the minimum permissions required for the integration to work. See Minimum Required Permissions for a Local or Active Directory User Account.
4. In the vRealize Operations Manager pane, select **Enable alerts integration**.
5. Click **Save**.

What to do next

- See relevant pages in the vRealize Operations Manager UI to view the notification events that vRealize Log Insight sends.

Enable Launch in Context for vRealize Log Insight in vRealize Operations Manager

You can configure vRealize Operations Manager to display menu items related to vRealize Log Insight and launch vRealize Log Insight with an object-specific query.

You can integrate vRealize Log Insight with vRealize Operations Manager vApp and vRealize Operations Manager Installable.

Integrating with vApp install and Installable (Windows, Linux) requires additional changes to the vRealize Operations Manager configuration. See the topic about installing the vRealize Log Insight Management Pack (Adapter) in vRealize Operations Manager 6.x and later in the vRealize Log Insight 4.0 information center.

Note that the vRealize vRealize Log Insight Management Pack is pre-installed in vRealize Operations Manager 6.0 and later and does not require configuration changes.

vRealize Operations Manager Installable (Windows version) is discontinued from vRealize Operations Manager 6.5 and later.

Important One instance of vRealize Operations Manager supports launch in context for only one instance of vRealize Log Insight. Because vRealize Log Insight does not check whether other instances are already registered with vRealize Operations Manager, you might override the settings of another user.

Prerequisites

- Verify that you are logged in to the vRealize Log Insight*portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is https://*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.
- Verify that you know the IP address or host name of the target vRealize Operations Manager instance.
- Verify that you have the required user credentials. See Minimum Required Permissions for a Local or Active Directory User Account.
- If you are using vRealize Operations Manager 6.5 or later, use the procedure for enabling launch in context in the vRealize Operations Manager 6.5 information center.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Integration, select **vRealize Operations Manager**.
3. Type the IP address or FQDN of the vRealize Operations Manager master node or load balancer if one is configured and click **Test Connection**.

   Note For Launch in Context functionality, you must provide a vRealize Operations Manager user with administrator privileges.
4. Click **Save**.

vRealize Log Insight configures the vRealize Operations Manager instance. This operation might take a few minutes.

Items related to vRealize Log Insight appear in the menus of vRealize Operations Manager.

What to do next

Launch a vRealize Log Insight query from the vRealize Operations Manager instance. See vRealize Log Insight Launch in Context

vRealize Log Insight Launch in Context

When you enable launch in context for vRealize Log Insight, a vRealize Log Insight resource is created in vRealize Operations Manager.

The resource identifier contains the IP address of the vRealize Log Insight instance, and is used by vRealize Operations Manager to open vRealize Log Insight.

Launch in Context in vRealize Operations Manager 6.5 and Later

For information about enabling launch in context, see the vRealize Operations Manager information center.

Launch in Context in the vSphere User Interface of vRealize Operations Manager 6.4 and Earlier

The launch in context options that are related to vRealize Log Insight appear in the **Actions** drop-down menu of the vSphere user interface. You can use these menu items to open vRealize Log Insight, and search for log events from an object in vRealize Operations Manager.

The available launch in context action depends on the object that you select in vRealize Operations Manager inventory. The time range of the queries is limited to 60 minutes before you click a launch in context option.

Table 12-3. Objects in vRealize Operations Manager UI and Their Corresponding Launch in Context Options and Actions

Object selected in vRealize Operations Manager	Launch in Context Option in the Actions Drop-Down Menu	Action in vRealize Operations Manager	Action in vRealize Log Insight
World	**Open vRealize Log Insight**	Opens vRealize Log Insight.	vRealize Log Insight displays the **Interactive Analytics** tab.
vCenter Server	**Open vRealize Log Insight**	Opens vRealize Log Insight.	vRealize Log Insight displays the **Interactive Analytics** tab.
Data center	**Search for logs in vRealize Log Insight**	Opens vRealize Log Insight and passes the resource names of all host systems under the selected data center object.	vRealize Log Insight displays the **Interactive Analytics** tab and performs a query to find log events that contain names of hosts within the data center.
Cluster	**Search for logs in vRealize Log Insight**	Opens vRealize Log Insight and passes the resource names of all host systems under the selected Cluster object.	vRealize Log Insight displays the **Interactive Analytics** tab and performs a query to find log events that contain names of hosts within the cluster.

Table 12-3. Objects in vRealize Operations Manager UI and Their Corresponding Launch in Context Options and Actions (Continued)

Object selected in vRealize Operations Manager	Launch in Context Option in the Actions Drop-Down Menu	Action in vRealize Operations Manager	Action in vRealize Log Insight
Host System	**Search for logs in vRealize Log Insight**	Opens vRealize Log Insight and passes the resource name of the selected Host object.	vRealize Log Insight displays the **Interactive Analytics** tab and performs a query to find log events that contain the name of the selected Host system.
Virtual Machine	**Search for logs in vRealize Log Insight**	Opens vRealize Log Insight and passes the IP address of the selected virtual machine and the resource name of the related host system.	vRealize Log Insight displays the **Interactive Analytics** tab and performs a query to find log events that contain the IP address of the virtual machine, and the name of the host where the virtual machine resides.

On the **Alerts** tab, if you select an alert and select **Search for logs in Log Insight** from the in-context menu, the time range of the query is limited to one hour before the alert is triggered. For example, if an alert was triggered at 2:00 PM, the query in vRealize Log Insight displays all log messages that occurred between 1:00 PM and 2:00 PM. This helps you identify events that might have triggered the alert.

You can open vRealize Log Insight from metric charts in vRealize Operations Manager. The time range of the query thatvRealize Log Insight runs matches the time range of the metric chart.

Note The time that you see in vRealize Log Insight and vRealize Operations Manager metric charts might differ if the time setting of the virtual appliances is different.

Launch in Context in the vRealize Operations Manager 6.4 and Earlier User Interface

The launch in context icon  appears on several pages of the user interface, but you can launch vRealize Log Insight only from the pages that display vRealize Log Insight notification events:

- The Alerts Overview page.
- The Alert Summary page of a vRealize Log Insight notification alert.
- The Alerts widgets on your dashboards, when a vRealize Log Insight notification alert is selected.

When you select a vRealize Log Insight notification event in the Custom user interface, you can choose between two launch in context actions.

Table 12-4. Launch in Context Options and Actions in vRealize Operations Manager UI

Launch in Context Option in vRealize Operations Manager	Action in vRealize Operations Manager	Action in vRealize Log Insight
Open vRealize Log Insight	Opens vRealize Log Insight.	vRealize Log Insight displays the **Dashboards** tab and loads the vSphere Overview dashboard.
Search for Logs in vRealize Log Insight	Opens vRealize Log Insight and passes the ID of the query that triggered the notification event.	vRealize Log Insight displays the **Interactive Analytics** tab and performs the query that triggered the notification event.

When you select an alert that has not originated from vRealize Log Insight, the launch in context menu contains the **Search for VM and Host Logs in vRealize Log Insight** menu item. If you select this menu item, vRealize Operations Manager opens vRealize Log Insight and passes the identifiers of the object that triggered the alert. vRealize Log Insight uses the resource identifiers to perform a search in the available log events.

Two-Way Launch in Context

Launch in Context is also available from vRealize Log Insight to vRealize Operations Manager.

If you integrate vRealize Log Insight with vRealize Operations Manager, you can perform a Launch in Context from a vRealize Log Insight event by selecting the gear icon to the left of the event and selecting the option to view in vRealize Operations Manager.

For information about Launch in Context from vRealize Operations Manager to vRealize Log Insight, see vRealize Log Insight Launch in Context.

Procedure

1. In vRealize Log Insight, navigate to the **Interactive Analytics** tab.
2. Locate an event that contains inventory mapping fields and hover over the event.
3. Click the gear icon and select **Open Analysis** in vRealize Operations Manager from the drop-down menu.

   A new browser tab opens directing you to the vRealize Operations Manager instance integrated with vRealize Log Insight. Once you authenticate, you are directed to the **Environment** > **Analysis** section of vRealize Operations Manager with the object selected.

   Note When multiple vRealize Log Insight instances are connected to the same vRealize Operations Manager instance, only the last vRealize Log Insight instance integrated with vRealize Operations Manager has the Launch in Context feature. This also means that the Launch in Context feature is overridden whenever a vRealize Log Insight instance is integrated with a vRealize Operations Manager instance that was previously integrated with a different vRealize Log Insight instance.

Disable Launch in Context for vRealize Log Insight in vRealize Operations Manager

You can uninstall the vRealize Log Insight adapter from the vRealize Operations Manager instance to remove menu items related to vRealize Log Insight from the vRealize Operations Manager user interface.

You use the Administration UI of vRealize Log Insight to disable launch in context. If you do not have access to vRealize Log Insight or if the vRealize Log Insight instance is deleted before the connection with vRealize Operations Manager is disabled, you can unregister vRealize Log Insight from the Administration UI of vRealize Operations Manager. See the Help in the vRealize Operations Manager Administration portal.

Caution One instance of vRealize Operations Manager supports launch in context for only one instance of vRealize Log Insight. If another instance of vRealize Log Insight has been registered after you registered the instance that you want to disable, the second instance overrides the settings of the first one without notifying you.

Prerequisites

- Verify that you are logged in to the vRealize Log Insight*portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is https:///*log-insight-host*, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Integration, select **vRealize Operations Manager**.
3. Deselect the **Enable Launch in Context** check box.
4. Click **Save**.

vRealize Log Insight configures the vRealize Operations Manager instance to remove the vRealize Log Insight adapter. This operation might take a few minutes.

Add a DNS Search Path and Domain

You can add a DNS search path and domain to improve the vRealize Operations Manager inventory matching.

Adding a DNS search path and domain improves matching when a virtual machine label and search domain resolve to the IP address of the host that sends log messages to vRealize Log Insight. For example, if you have a virtual machine named linux_01 in vRealize Operations Manager and the host name linux_01.company.com resolves to 192.168.10.10, then adding a search domain allows vRealize Log Insight to recognize and match that resource.

Procedure

1. Perform a guest shutdown of the vRealize Log Insight virtual appliance.

2 Once the virtual machine is powered down, select **Edit Settings**.

3 Select the **Options** tab.

4 From **vApp Options** > **Advanced**, click **Properties**.

5 Find the `vami.searchpath.VMware_vCenter_Log_Insight` and `vami.domain.VMware_vCenter_Log_Insight` keys.

   If the keys do not exist, create them.

6 Set the DNS search path and domain.

7 Power on the virtual appliance.

What to do next

After vRealize Log Insight boots, you can validate the DNS configuration by logging in and viewing the contents of the `/etc/resolv.conf` file. Near the bottom of the file you should see the search and domain options.

Remove the vRealize Log Insight Adapter

When you enable launch in context on a vRealize Operations Manager 6.2 and later instance, vRealize Log Insight creates an instance of the vRealize Log Insight adapter on the vRealize Operations Manager instance.

The instance of the adapter remains in the vRealize Operations Manager instance when you uninstall vRealize Log Insight. As a result, the launch in context menu items continue to appear in the actions menus, and point to a vRealize Log Insight instance that no longer exists.

To disable the launch in context functionality in vRealize Operations Manager, you must remove the vRealize Log Insight adapter from the vRealize Operations Manager instance.

You can use the command line utility cURL to send REST calls to vRealize Operations Manager.

Note These steps are only required if Launch in Context was enabled.

Prerequisites

- Verify that cURL is installed on your system. Note that this tool is preinstalled in the vRealize Operations Manager virtual appliance and the steps can be performed from the appliance using IP address `127.0.0.1`.
- Verify that you know the IP address or host name of the target vRealize Operations Manager instance.
- Depending on the vRealize Operations Manager license that you own, verify that you have the minimum credentials required to remove the management pack. See Minimum Required Permissions for a Local or Active Directory User Account.

Procedure

1 In cURL, run the following query on the vRealize Operations Manager virtual appliance to find the vRealize Log Insight adapter.

```
curl –k –u "admin" https://ipaddress/suite–
api/api/adapterkinds/LogInsight/resourcekinds/LogInsightLogServer/resources
```

Where *admin* is the administrator login name and *ipaddress* is the IP address (or hostname) of the vRealize Operations Manager instance. You are prompted to enter the password for the user: *admin*.

From the curl output find the GUID value assigned to the identifier: `<ops:resource creationTime="{TIMESTAMP}" identifier="{GUID}">`. You can use this GUID value in the below command that removes the adapter instance.

2 Run the following command to remove the vRealize Log Insight adapter.

```
curl –k –u "admin" –X DELETE https://ipaddress/suite–api/api/adapters/{GUID}
```

Where *admin* is the administrator login name and *ipaddress* is the IP address (or hostname) of the vRealize Operations Manager instance. You are prompted to enter the password for the user: *admin*.

vRealize Log Insight launch in context items are removed from the menus in vRealize Operations Manager. For more information about launch in context, see the topic *vRealize Log Insight Launch in Context* of the vRealize Log Insight in-product help.

vRealize Operations Manager Content Pack for vRealize Log Insight

The vRealize Operations Manager content pack for vRealize Log Insight contain dashboards, extracted fields, saved queries, and alerts that are used to analyze all logs redirected from a vRealize Operations Manager instance.

The vRealize Operations Manager content pack provides a way to analyze all logs redirected from a vRealize Operations Manager instance. The content pack contains dashboards, queries and alerts to provide diagnostics and troubleshooting capabilities to the vRealize Operations Manager administrator. The dashboards are grouped according to the major components of vRealize Operations Manager like Analytics, UI, and Adapters to provide better manageability. You can enable various alerts to send notification events in vRealize Operations Manager and e-mails to administrators.

You can download the vRealize Operations Manager content pack from https://solutionexchange.vmware.com/store/loginsight?src=Product_Product_LogInsight_YES_US.

See Working with Content Packs.

Security Considerations for vRealize Log Insight

13

Use vRealize Log Insight features to safeguard your environment from attack.

This section includes the following topics:

Ports and External Interfaces

vRealize Log Insight uses specific required services, ports, and external interfaces.

Communication Ports

vRealize Log Insight uses the communication ports and protocols listed in this topic. The required ports are organized based on whether they are required for sources, for the user interface, between clusters, for external services, or whether they can be safely blocked by a firewall. Some ports are used only if you enable the corresponding integration.

Note vRealize Log Insight does not support WAN clustering (also called geoclustering, high-availability clustering, or remote clustering). All nodes in the cluster should be deployed in the same Layer 2 LAN. In addition, the ports described in this section must be opened between nodes for proper communication.

vRealize Log Insight network traffic has several sources.

Admin workstation The machine that a system administrator uses to manage the vRealize Log Insight virtual appliance remotely.

User workstation The machine on which a vRealize Log Insight user uses a browser to access the Web interface of vRealize Log Insight.

System sending logs The endpoint that sends logs to vRealize Log Insight for analysis and search. For example, endpoints include ESXi hosts, virtuals machines or any system with an IP address.

Log Insight Agents The agent that resides on a Windows or Linux machine and sends operating system events and logs to vRealize Log Insight over APIs.

vRealize Log Insight appliance Any vRealize Log Insight virtual appliance, master or worker, where the vRealize Log Insight services reside. The base operating system of the appliance is SUSE 11 SP3.

Ports Required for Sources Sending Data

The following ports need to be open to network traffic from sources that send data to vRealize Log Insight, both for connections from outside the cluster and connections load-balanced between cluster nodes.

Source	Destination	Port	Protocol	Service Description
System sending logs	vRealize Log Insight appliance	514	TCP, UDP	Outbound syslog traffic configured as a Forwarder destination
System sending logs	vRealize Log Insight appliance	1514, 6514	TCP	Syslog data over SSL
vRealize Log Insight Agents	vRealize Log Insight appliance	9000	TCP	Log Insight Ingestion API
vRealize Log Insight Agents	vRealize Log Insight appliance	9543	TCP	Log Insight Ingestion API over SSL

Ports Required for the User Interface

The following ports need to be open to network traffic that needs to use the vRealize Log Insight user interface, both for connections outside the cluster and connections load-balanced between cluster nodes.

Source	Destination	Port	Protocol	Service Description
Admin workstation	vRealize Log Insight appliance	22	TCP	SSH: Secure Shell connectivity
User workstation	vRealize Log Insight appliance	80	TCP	HTTP: Web interface
User workstation	vRealize Log Insight appliance	443	TCP	HTTPS: Web interface

Ports Required Between Cluster Nodes

The following ports should only be open on a vRealize Log Insight master node for network access from worker nodes for maximum security. These are in addition to those ports used for sources and UI traffic that are load-balanced between cluster nodes.

Source	Destination	Port	Protocol	Service Description
vRealize Log Insight appliance	vRealize Log Insight appliance	7000	TCP	Cassandra replication and query
vRealize Log Insight appliance	vRealize Log Insight appliance	9042	TCP	Cassandra service for native protocol clients
vRealize Log Insight appliance	vRealize Log Insight appliance	9160	TCP	Cassandra service for Thrift clients
vRealize Log Insight appliance	vRealize Log Insight appliance	59778, 16520-16580	TCP	vRealize Log Insight Thrift service

Ports Required for External Services

The following ports must be open for outbound networj traffic from vRealize Log Insight cluster nodes to remote services.

Source	Destination	Port	Protocol	Service Description
vRealize Log Insight appliance	NTP server	123	UDP	NTPD: Provides NTP time synchronization **Note** The port is open only if you choose to use NTP time synchronization
vRealize Log Insight appliance	Mail Server	25	TCP	SMTP: mail service for outbound alerts
vRealize Log Insight appliance	Mail Server	465	TCP	SMTPS: mail service over SSL for outbound alerts
vRealize Log Insight appliance	DNS server	53	TCP, UDP	DNS: name resolution service

Source	Destination	Port	Protocol	Service Description
vRealize Log Insight appliance	AD server	389	TCP, UDP	Active Directory
vRealize Log Insight appliance	AD server	636	TCP	Active Directory over SSL
vRealize Log Insight appliance	AD server	3268	TCP	Active Directory Global Catalog
vRealize Log Insight appliance	AD server	3269	TCP	Active Directory Global Catalog SSL
vRealize Log Insight appliance	AD server	88	TCP, UDP	Kerberos
vRealize Log Insight appliance	vCenter Server	443	TCP	vCenter Server Web Service
vRealize Log Insight appliance	vRealize Operations Manager appliance	443	TCP	vRealize Operations Web service
vRealize Log Insight appliance	Third-party log manager	514	TCP,UDP	syslog data
vRealize Log Insight appliance	Third-party log manager	9000	CFAPI	Outbound Log Insight Ingestion API (CFAPI) traffic configured as a Forwarder destination
vRealize Log Insight appliance	Third-party log manager	9543	CFAPI	Outbound Log Insight Ingestion API (CFAPI) traffic configured as a Forwarder destination with encryption (SSL/TLS)

Ports That Can be Blocked

The following ports are open but not used by vRealize Log Insight. These ports can be safely blocked by a firewall.

Destination	Port	Protocol	Service Description
vRealize Log Insight appliance	111	TCP, UDP	RPCbind service that converts RPC program numbers into universal addresses
vRealize Log Insight appliance Tomcat service	9007	TCP	Tomcat services

vRealize Log Insight Configuration Files

Some configuration files contain settings that affect vRealize Log Insight security.

Note All security-related resources are accessible by the root account. Protecting this account is critical to the security of vRealize Log Insight.

Table 13-1. Log Insight Configuration Files

File	Description
`/usr/lib/loginsight/application/etc/loginsight-config-base.xml`	The default system configuration for vRealize Log Insight.
`/storage/core/loginsight/config/loginsight-config.xml#number`	The modified (from the default) system configuration forvRealize Log Insight.
`/usr/lib/loginsight/application/etc/jaas.conf`	The configuration for active directory integration.
`/usr/lib/loginsight/application/etc/3rd_config/server.xml`	The system configuration for Apache Tomcat server.
`/storage/var/loginsight/apache-tomcat/conf/tomcat-users.xml`	The system configuration for Apache Tomcat server.
`/usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/server.xml`	The system configuration for Apache Tomcat server.
`/usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/tomcat-users.xml`	User information for Apache Tomcat server.

vRealize Log Insight Public Key, Certificate, and Keystore

The public key, the certificate, and the keystore of vRealize Log Insight are located on the vRealize Log Insight virtual appliance.

Note All security-related resources are accessible by the root account. Protecting this account is critical to the security of vRealize Log Insight.

- `/usr/lib/loginsight/application/etc/public.cert`
- `/usr/lib/loginsight/application/etc/loginsight.pub`
- `/usr/lib/loginsight/application/etc/3rd_config/keystore`
- `/usr/lib/loginsight/application/etc/truststore`
- `/usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/keystore`

vRealize Log Insight License and EULA File

The end-user license agreement (EULA) and license file are located on the vRealize Log Insight virtual appliance.

Note All security-related resources are accessible by the root account. Protecting this account is critical to the security of vRealize Log Insight.

File	Location
License	`/usr/lib/loginsight/application/etc/license/loginsight_dev.dlf`
License	`/usr/lib/loginsight/application/etc/license/loginsight_cpu.dlf`
License	`/usr/lib/loginsight/application/etc/license/loginsight_osi.dlf`
License Key file	`/usr/lib/loginsight/application/etc/license/loginsight_license.bak`
End-user license agreement	`/usr/lib/loginsight/application/etc/license/release/eula.txt`

vRealize Log Insight Log Files

The files that contain system messages are located on the vRealize Log Insight virtual appliance.

File	Description
`/storage/var/loginsight/alert.log`	Used to track information about user-defined alerts that have been triggered.
`/storage/var/loginsight/apache-tomcat/logs/*.log`	Used to track events from Apache Tomcat server.
`/storage/var/loginsight/cassandra.log`	Used to track cluster configuration storage and replication in Apache Cassandra.
`/storage/var/loginsight/plugins/vsphere/li-vsphere.log`	Used to trace events related to integration with vSphere Web Client.
`/storage/var/loginsight/loginsight_daemon_stdout.log`	Used for the standard output of vRealize Log Insight daemon.
`/storage/var/loginsight/phonehome.log`	Used to track information about trace data collection sent to VMware (if enabled).
`/storage/var/loginsight/pi.log`	Used to track database start or stop events.
`/storage/var/loginsight/runtime.log`	Used to track all run time information related to vRealize Log Insight.
`/var/log/firstboot/stratavm.log`	Used to track the events that occur at first boot and configuration of the vRealize Log Insight virtual appliance.
`/storage/var/loginsight/systemalert.log`	Used to track information about system notifications that vRealize Log Insight sends. Each alert is listed as a JSON entry.
`/storage/var/loginsight/systemalert_worker.log`	Used to track information about system notifications that a vRealize Log Insight worker node sends. Each alert is listed as a JSON entry.

File	Description
/storage/var/loginsight/ui.log	Used to track events related to the vRealize Log Insight user interface.
/storage/var/loginsight/ui_runtime.log	Used to track runtime events related to the vRealize Log Insight user interface.
/storage/var/loginsight/upgrade.log	Used to track events that occur during vRealize Log Insight upgrade.
/storage/var/loginsight/usage.log	Used to track all queries.
/storage/var/loginsight/vcenter_operations.log	Used to track events related to the vRealize Operations Manager integration
/storage/var/loginsight/watchdog_log*	Used to track the run time events of the watch dog process, which is responsible for restarting vRealize Log Insight if it is shutdown for some reason.

Log Messages Related to Security

The `ui_runtime.log` file contains user audit log messages in the following format.

- `[2013-05-17 20:40:18.716+0000] [http-443-5 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged in: Name: admin | Role: admin]`
- `[2013-05-17 20:39:51.395+0000] [http-443-5 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged out: Name: admin | Role: admin]`
- `[2013-09-18 12:39:34.823-0700] [http-9443-3 WARN /127.0.0.1] [com.vmware.loginsight.web.actions.misc.LoginActionBean][Bad username/password attempt (username: myusername)]`
- `[2013-09-18 12:40:08.761-0700] [http-9443-3 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged in: Active Directory User: SAM=myusername, Domain=vmware.com,UPN=myusername@vmware.com]`
- `[ 2013-09-18 12:40:20.232-0700] [http-9443-3 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged out: Active Directory User: SAM=myusername, Domain=vmware.com,UPN=myusername@vmware.com]`
- `[2013-09-18 12:40:36.933-0700] [http-9443-3 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged in: Local User: Name=myusername, Role=user]`
- `[2013-09-18 12:40:40.429-0700] [http-9443-3 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged out: Local User: Name=myusername, Role=user`
- `[2013-11-13 23:26:21.569+0000] [http-443-4 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Created new user: Active Directory User: SAM=username, Domain=vmware.com, UPN=username@vmware.com]`

- [2013-11-14 22:44:11.017+0000] [http-443-6 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Created new user: Local User: Name=username, Role=admin]
- [2013-12-05 21:03:36.751+0000] [http-443-3 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Removed users: [Active Directory User: SAM=username, Domain=vmware.com, UPN=username@vmware.com]]
- [2013-12-05 21:04:16.707+0000] [http-443-3 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Removed users: [Local User: Name=username, Role=admin]]
- [http-9443-3 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Created new group: (domain=vmware.com, group=VMware Employees, role=user)]
- [2013-12-05 13:07:04.108-0800] [http-9443-2 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Removed groups: [(domain=vmware.com, group=VMware Employees, role=user)]]

vRealize Log Insight User Accounts

You must set up a system and a root account to administer vRealize Log Insight.

vRealize Log Insight Root User

vRealize Log Insight currently uses the root user account as the service user. No other user is created.

Unless you set the root password property during deployment, the default root password is blank. You must change the root password when you log in to the vRealize Log Insight console for the first time.

SSH is disabled until the default root password is set.

The root password must meet the following requirements.

- Must be at least eight characters long
- Must contain at least one uppercase letter, one lowercase letter, one digit, and one special character
- Must not repeat the same character four times

vRealize Log Insight Admin User

When you start the vRealize Log Insight virtual appliance for the first time, vRealize Log Insight creates the admin user account for its Web user interface.

The default password for admin is blank. You must change the admin password in the Web user interface during the initial configuration of vRealize Log Insight.

Active Directory Support

vRealize Log Insight supports integration with Active Directory. When configured, vRealize Log Insight can authenticate or authorize a user against Active Directory.

See Enable User Authentication Through Active Directory.

Privileges Assigned to Default Users

The vRealize Log Insight service user has root privileges.

The Web user interface admin user has the administrator privileges only to the vRealize Log Insight web user interface.

vRealize Log Insight Firewall Recommendations

To protect sensitive information gathered by vRealize Log Insight, place the server or servers on a management network segment protected by a firewall from the rest of your internal network.

Required Ports

The following ports need to be open to network traffic from sources that send data to vRealize Log Insight.

Port	Protocol
514/UDP, 514/TCP	Syslog
1514/TCP, 6514/TCP	Syslog-TLS (SSL)
9000/TCP	vRealize Log Insight Ingestion API
9543/TCP	vRealize Log Insight Ingestion API - TLS (SSL)

The following ports need to be open to network traffic that needs to use the vRealize Log Insight UI.

Port	Protocol
80/TCP	HTTP
443/TCP	HTTPS

The following set of ports should only be open on a vRealize Log Insight master node for network access from worker nodes for maximum security.

Port	Protocol
16520:16580/TCP	Thrift RPC
59778/TCP	log4j server
12543/TCP	database server

Security Updates and Patches

The vRealize Log Insight virtual appliance uses SUSE Linux Enterprise Server 11 (x86_64), version 11, patch level 3 as the guest operating system.

VMware will release patches to address security issues.

Before you apply an upgrade or patch to the guest operating system, take into account the dependencies. See Chapter 6 Ports and External Interfaces.

Backup, Restore, and Disaster Recovery

14

To guard against expensive data center downtime, follow these best practices for performing vRealize Log Insight backup, restoration, and disaster recovery operations.

This section includes the following topics:

Backup, Restore, and Disaster Recovery Overview

VMware delivers a comprehensive, integrated portfolio of Business Continuity and Disaster Recovery (BCDR) solutions that provide high availability, data protection, and disaster recovery.

Use the backup, restore, and disaster recovery information in this document for vRealize Log Insight components, including the master node, worker node and forwarder.

- For information about master and worker cluster members, including configuration, log data and customization, see Backup Nodes and Clusters.
- For information about Linux or Windows agent local configuration, see Backup Linux or Windows Agents.

The information in this document does not apply to the following tools and products. You must to obtain information about these tools and products from multiple resources.

- Third-party tools that are specifically used for backup, restore, and disaster recovery. For more information, see the vendor documentation.

- vSphere Data Protection, Site Recovery Manager, and Symantec NetBackup. For additional information on VMware BCDR solutions, see http://www.vmware.com/business-continuity/business-continuity and the VMware vCloud Suite documentation.
- Backup, restore, and disaster recovery capability for products that integrate with vRealize Log Insight.
  - vRealize Operations Manager
  - vSphere Web Client server
  - ESXi hosts

Using Static IP Addresses and FQDN

You can use static IP addresses and FQDN to avoid risk during backup, restoration, and disaster recovery operations.

Static IP Addresses for vRealize Log Insight Cluster Nodes and Load Balancer

When you use static IP addresses for all nodes in a vRealize Log Insight cluster, you eliminate the need to update the IP addresses of the cluster nodes when the IP addresses change.

vRealize Log Insight includes all node IP addresses in each cluster node configuration file as described in Knowledge Base article 2123058

All products that integrate with vRealize Log Insight (ESXi, vSphere, vRealize Operations) use the cluster master node's fully qualified domain name (FQDN) or IP address as the syslog target. Those products might use the FQDN or IP address of the load balancer, if configured, as the syslog target. Static IP addresses reduce the risk of constantly updating the syslog target IP address in multiple locations.

Provide static IP addresses and optional virtual IP addresses for the load balancer. When configuring an integrated load balancer, provide the optional FQDN for the virtual IP address. The FQDN is used when an IP address is not reachable for any reason.

FQDN for vRealize Log Insight Cluster Nodes and Worker Node

When you use an FQDN for all nodes in the vRealize Log Insight cluster, you can save time on post-restoration and recovery configuration changes, assuming that the same FQDN can be resolved on the recovery site.

For the master node (load balancer when used), a fully resolvable FQDN is required. Otherwise, the ESXi hosts fail to feed the syslog messages to vRealize Log Insight or to any remote target.

For system notifications, vRealize Log Insight uses FQDN host names, if available, instead of IP addresses.

You can reasonably assume that only underlying IP addresses change post-backup and restoration or disaster recovery operations. Using FQDN eliminates the need to change the syslog target address (master node FQDN or internal load balancer FQDN) on all the external devices that feed logs to the vRealize Log Insight cluster.

Verify that join requests from a vRealize Log Insight worker node use the FQDN of the vRealize Log Insight master node.

The master node host value in the configuration file on each of the nodes is based on the value used by the first worker node sending a join request. Using the FQDN of the master node for the join request prevents making any manual changes to the master node host value post-disaster recovery. Otherwise, the worker nodes cannot rejoin the master node until the master node host name is updated in the configuration files on all restored cluster nodes.

Planning and Preparation

Before implementing a backup, restoration, or disaster recovery procedure, review the planning and preparation information in this topic.

The following recommendations should be included in a backup, restoration, and disaster recovery plan.

Test Backup Operations

Perform a test run of the backup, restoration, and disaster recovery operations in a test or staging environment before performing these operations on a live production setup.

Perform a full backup of the entire vRealize Log Insight cluster. Do not rely on automatic procedures to back up individual files and configurations.

Verify Fixes

Verify that fixes are implemented and warnings and errors are addressed before performing backup, restoration, and disaster recovery operations. Backup, restoration, and disaster recovery tools usually provide visual validations and steps to ensure that backup, restoration, and disaster recovery configurations are successfully created.

Scheduling Backups

Depending on the cluster configuration, the first backup operation is usually a full backup. You should allow for an extended period of time for the first backup to complete. Successive backups, which can be incremental or full backups, finish relatively faster compared to the first backup operation.

Additional Documentation and Tools

Verify that you are following the documentation for allocating resources for the vRealize Log Insight backup, restoration, and disaster recovery tools.

Verify that you are following the tool-specific best practices and recommendations for third-party backup, restoration, and disaster recovery tools.

For virtual machines deployed using VMware products, use additional tools that can provide special features and configurations to support backup, restoration, and disaster recovery.

Forwarders and Clusters

For forwarders, apply the backup, restoration, and disaster recovery steps for the main vRealize Log Insight cluster. See Restore Nodes and Clusters.

Based on the customer requirements, you might have a single or multiple vRealize Log Insight forwarders. In addition, the forwarders can be installed as a standalone node or as a cluster. For the purpose of backup, restoration, and disaster recovery operations, vRealize Log Insight forwarders are identical to the primary vRealize Log Insight cluster nodes and handled the same way.

Backup Nodes and Clusters

It is a best practice to set up scheduled backups or replication for vRealize Log Insight nodes and clusters.

vRealize Log Insight does not support quiesced snapshots. If you try to create an a quiesced snapshot, the snapshot is created, but quiescence is not applied. For more information, see the VMware Knowledge Base article Log Insight virtual appliance becomes unresponsive during quiesced snapshots.

Prerequisites

- Verify that no configuration problems exist on source and target sites before performing the backup or replication operations.
- Verify that cluster resource allocation is not at capacity.

  In configurations with reasonable ingestion and query loads, the memory and swap usage can reach almost 100% capacity during backup and replication operations. Because memory is near capacity in a live environment, part of the memory spike is due to the vRealize Log Insight cluster usage. Also, the scheduled backup and replication operations can contribute significantly to the memory spike.

  In some cases, worker nodes are disconnected momentarily for 1 to 3 minutes before rejoining master nodes, possibly because of high memory usage.
- Reduce the memory throttling on vRealize Log Insight nodes by doing one or both of the following:
  - Allocate additional memory over the vRealize Log Insight recommended configurations.
  - Schedule the recurring backups during off-peak hours.

Procedure

1. Enable regular backup or replication of vRealize Log Insight forwarders by using the same procedures that you use for the vRealize Log Insight server.
2. Verify that the backup frequency and backup types are appropriately selected based on the available resources and customer-specific requirements.

3 If the resources are not a problem and if it is supported by the tool, enable concurrent cluster node backups to speed up the backup process.

4 Back up all the nodes at the same time.

What to do next

Monitoring—As the backup is in progress, check any environment or performance problems in the vRealize Log Insight setup. Most backup, restore, and disaster recovery tools provide monitoring capabilities.

During the backup process, check all the relevant logs on the production system because the user interface might not display all problems.

Backup Linux or Windows Agents

You backup agents by backing up installation and configuration information on the server side. A separate backup of the agent node is not required.

Agents are typically installed on Linux or Windows systems that also used for some other application or service and might be included in existing backup procedures. A full file-level or block-level backup of the machine that includes the entire agent installation and its configuration is sufficient for recovery. Agents support both local and server-provided configuration.

If the agent is configured entirely from the vRealize Log Insight server, without any local change to the `liagent.ini` configuration file, you can avoid creating a backup of the agent installation at all. Instead, perform a fresh installation of the agent and retrieve the server backup.

If the agent has a custom local configuration, backup the `liagent.ini` file and restore it along with a fresh installation of the agent. If you use the agent nodes for more than installing the agent software and if these nodes need a full backup, follow the same backup procedure as for any other virtual machine.

If the agent configuration is done on the client side (on the agents) and if the agent nodes are used only for vRealize Log Insight agent software installation, making a backup of the agent configuration file is sufficient.

Prerequisites

Verify that the agent configuration is on the vRealize Log Insight server side.

Procedure

1 Backup the `liagent.ini` file.

2 Replace the file on the recovered agent or Linux or Windows machine with the backup file.

Restore Nodes and Clusters

Nodes must be restored in a specific order and some restoration scenarios may require manual configuration changes.

Depending on the tool used for restoring, you can restore the virtual machines to the same host, a different host on the same data center, or a different host on a target remote data center. See Changing Configurations After Restoration

Prerequisites

- Verify that the restored nodes are in the powered off state.
- Verify that the cluster instances are powered off before restoring the cluster to a new site.
- Verify that no split-brain behavior occurs when the same IP addresses and FQDNs are used on the recovery site.
- Verify that no one is accidentally using a partially working cluster on the primary site.

Procedure

1. Restore the master node first before restoring worker nodes.
2. Restore worker nodes in any order.
3. (Optional) Restore the forwarders if configured.

   Be sure the vRealize Log Insight server (the master node and all the worker nodes in a cluster setup) are restored before restoring the forwarders.
4. Restore any recovered agents.

What to do next

- When restoring a vRealize Log Insight cluster, if the same IP addresses are used, verify that all restored node IP addresses and FQDNs are associated with their original counterparts.

  For example, the following scenario would fail. In a three-node cluster with nodes A, B, and C, node A is restored with IP address B, node B is restored with IP address C, and node C is restored with IP address A.

  - If the same IP addresses are used for only a subset of restored nodes, verify that for these nodes, all restored images are associated with their original IP addresses.
- Most backup restoration and disaster recovery tools provide a monitoring view for watching the progress of the restoration operations for failures or warnings. Take appropriate actions on any identified problems.
- If manual configuration changes are required before the site can be fully restored, follow the guidelines in the Changing Configurations After Restoration.
- When a successful restoration is finished, perform a spot check of the cluster that was restored.

Changing Configurations After Restoration

The recovery target and IP customizations applied during the backup configuration determine which manual configuration changes are required. You must apply configuration changes to one or more vRealize Log Insight nodes before the restored site can become fully functional.

Restore to the Same Host

Recovering a vRealize Log Insight cluster to the same host is straightforward and can be performed by any tool.

Prerequisites

Review important information about Planning and Preparation.

Procedure

1. Power off the existing cluster before beginning the restoration operation. By default, the same IP addresses and FQDNs are used for the restored cluster nodes.
2. (Optional) Provide a new name for the cluster.

   During the restoration process, the original copy of the cluster is overwritten with the restored version unless a new name is provided to the virtual machine.
3. (Optional) If possible, verify that all network, IP, and FQDN settings that are used for the production environment are preserved in the restored and recovered site.

What to do next

After a successful restoration and a sanity check, delete the old copy to conserve resources and to prevent accidental split-brain situations if a user powers on the old copy.

Restore to a Different Host

When you perform a restoration to a different host, you must make configuration changes on the vRealize Log Insight cluster.

Making changes to the configuration files directly from the appliance console is not officially supported in vRealize Log Insight 3.0 and later releases. See Knowledge Base article 2123058 for information about how to make these changes by using the Web UI interface.

These configuration changes are specific to vRealize Log Insight builds that can be used with any backup recovery tool.

Recovering to a different host requires manual configuration changes on the vRealize Log Insight cluster. You can assume that the restored vRealize Log Insight nodes have different IP addresses and FQDNs than their source counterparts from which a backup was taken.

Prerequisites

Review important information about Planning and Preparation.

Procedure

1 List all new IP addresses and FQDNs that were assigned to each vRealize Log Insight node.

2 Make the following configuration changes on the master node by using the steps described in Knowledge Base article 2123058.

a In the vRealize Log Insight config section, look for lines that resemble the following lines.

```
<distributed overwrite-children="true">
  <daemon host="prod-es-vrli1.domain.com" port="16520" token="c4c4c6a7-f85c-4f28-
a48f-43aeea27cd0e">
    <service-group name="standalone" />
  </daemon>
  <daemon host="192.168.1.73" port="16520" token="a5c65b52-aff5-43ea-8a6d-38807ebc6167">
    <service-group name="workernode" />
  </daemon>
  <daemon host="192.168.1.74" port="16520" token="a2b57cb5-a6ac-48ee-8e10-17134e1e462e">
    <service-group name="workernode" />
  </daemon>
</distributed>
```

The code shows three nodes. The first node is the master node, which shows `<service-group name=standalone>`, and the remaining two nodes are worker nodes, which show `<service-group name="workernode">`

b For the master node, in the newly recovered environment, verify that the DNS entry that was used in the pre-recovery environment can be reused.

- If the DNS entry can be reused, update only the DNS entry to point to the new IP address of the master node.
- If the DNS entry cannot be reused, replace the master node entry with a new DNS name (pointing to the new IP address).
- If the DNS name cannot be assigned, as a last option, update the configuration entry with the new IP address.

c Update the worker node IP addresses as well to reflect the new IP addresses.

d In the same configuration file, verify that you have entries that represent NTP, SMTP, and database and appenders sections.

```
<ntp>
  <ntp-servers value="ntp1.domain.com, ntp2.domain.com" />
</ntp>

<smtp>
  <server value="smtp.domain.com" />
  <default-sender value="source.domain.com@domain.com" />
</smtp>

<database>
  <password value="xserttt" />
  <host value="vrli-node1.domain.com" />
  <port value="12543" />
</database>
```

- If the configured NTP server values are no longer valid in the new environment, update these values in the `<ntp>...</ntp>` section
- If the configured SMTP server values are no longer valid in the new environment, update these values in the `<smtp>...</smtp>` section.
- Optionally, change the `default-sender` value in the SMTP section. The value can be any value but as a good practice, represent the source from where the email is being sent.
- In the `<database>..</database>` section, change the host value to point to the master node FQDN or IP address.

e In the same configuration file, update the vRealize Log Insight ILB configuration section.

```
<load-balancer>
<leadership-lease-renewal-secs value="5" />
<high-availability-enabled value="true" />
<high-availability-ip value="10.158.128.165" />
<high-availability-fqdn value="LB-FQDN.eng.vmware.com" />
<layer4-enabled value="true" />
<ui-balancing-enabled value="true" />
</load-balancer>
```

f Under the `<load-balancer>...</load-balancer>` section, update the `high-availability-ip` value if it is different from the current setting.

g Ensure that you also update the FQDN of the load balancer.

h Restart from the Web UI through the Cluster tab on the Administration page. For each node listed, select its host name or IP address to open the details panel and click **Restart Log Insight**.

The configuration changes are automatically applied to all cluster nodes.

i Wait 2 minutes after the vRealize Log Insight service starts to allow enough time for the Cassandra service to start before bringing other worker nodes online.

What to do next

Verify that the restored vRealize Log Insight nodes have been assigned different IP addresses and FQDNs than their source counterparts from which a backup was taken.

Verify Restorations

You must verify that all restored vRealize Log Insight clusters are fully functional.

Prerequisites

Confirm that the backup and restoration process is complete before verifying node and cluster configurations.

Procedure

1 Log in to vRealize Log Insight using the internal load balancer (ILB) IP address or the FQDN (if configured).

2 Click the configuration drop-down menu icon  and select **Administration**.

3 Verify the following:

a Verify that you can access all individual cluster nodes using the respective IP addresses or FQDNs.

b Verify the status of cluster nodes from the cluster page and ensure that the ILB, if configured, is also in an active state.

c Verify the vSphere integration. If required, reconfigure the integration. Reconfiguration is required when the ILB and/or the master node IP address or FQDN is changed post-recovery.

d Verify the vRealize Operations Manager integration and reconfigure again if needed.

e Verify that all content packs and UI features are functioning properly.

f Verify that vRealize Log Insight forwarders and agents are functioning properly, if configured.

4 Verify that other key features of vRealize Log Insight are functioning as expected.

What to do next

Make any necessary adjustments to your backup and recovery plan to address any issues that may have been identified during your backup, restoration, and verification operations.

Disaster Recovery

A well-documented and well-tested recovery plan is essential to quickly returning a cluster to a working state.

The choice of replication type is critical when configuring a virtual machine for disaster recovery. Consider the Recovery Point Objective (RPO), the Recovery Time Objective (RTO), and the cost and scalability when deciding on a replication type.

In a disaster recovery scenario, sometimes you cannot restore to the same site if the primary site is fully down. But based on the option you choose, some manual steps are required to fully restore and return the vRealize Log Insight cluster to a running state.

Unless the vRealize Log Insight cluster is fully down and inaccessible, verify that the cluster instances are powered off before restoring the cluster to a new site.

During an outage or disaster, recover the vRealize Log Insight cluster as soon as possible.

Troubleshooting vRealize Log Insight 15

You can solve common problems related to vRealize Log Insight administration before calling VMware Support Services.

This section includes the following topics:

vRealize Log Insight Runs Out of Disk Space

A vRealize Log Insight master or worker node might run out of disk space if you are using a small virtual disk, and archiving is not enabled.

Problem

vRealize Log Insight runs out of disk space if the rate of incoming logs exceeds 3 percent of the storage space per minute.

Cause

In normal situations, vRealize Log Insight never runs out of disk because every minute it checks if the free space is less than 3 percent. If the free space on the vRealize Log Insight virtual appliance drops below 3 percent, old data buckets are retired.

However, if the disk is small and log ingestion rate is so high that the free space (3 percent) is filled out within 1 minute, vRealize Log Insight runs out of disk.

If archiving is enabled, vRealize Log Insight archives the bucket before retiring it. If the free space is filled before the old bucket is archived and retired, vRealize Log Insight runs out of disk.

Solution

- Increase the storage capacity of the vRealize Log Insight virtual appliance. See Increase the Storage Capacity of the vRealize Log Insight Virtual Appliance.

Import of Archived Data Might Fail

The import of archived data might fail if the vRealize Log Insight vRealize Log Insight virtual appliance runs out of disk space.

Problem

The vRealize Log Insight repository import utility does not check for available disk space on the vRealize Log Insight virtual appliance. Therefore, the import of archived logs might fail if the virtual appliance runs out of disk space.

Solution

Increase the storage capacity of the vRealize Log Insight virtual appliance and start the import again. Increase the Storage Capacity of the vRealize Log Insight Virtual Appliance. Note, though, that information that was successfully imported before failure will be duplicated.

Use the Virtual Appliance Console to Create a Support Bundle of vRealize Log Insight

If you cannot access the vRealize Log Insight Web user interface, you can download the support bundle by using the virtual appliance console or after establishing an SSH connection to the vRealize Log Insight virtual appliance.

Prerequisites

- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance.
- If you plan to connect to the vRealize Log Insight virtual appliance by using SSH, verify that TCP port 22 is open.

Procedure

1. Establish an SSH connection to the vRealize Log Insight vApp and log in as the root user.
2. To generate the support bundle, run `loginsight-support`.

   To generate a support bundle and include only files that have changed within a certain time period, execute the `loginsight-support` command with the `--days` constraint. For example, `--days=1` will only include files that have changed within 1 day.

The support information is collected and saved in a `*.tar.gz` file that has the following naming convention: `loginsight-support-YYYY-MM-DD_HHMMSS.xxxxx.tar.gz`, where `xxxxx` is the process ID under which the `loginsight-support` process ran.

What to do next

Forward the support bundle to VMware Support Services as requested.

Reset the Admin User Password

If an Admin user forgets the password to the Web user interface, the account becomes unreachable.

Problem

If vRealize Log Insight has only one Admin user and the Admin user forgets the password, the application cannot be administered. If an Admin user is the only user of vRealize Log Insight, the whole Web user interface becomes inaccessible.

Cause

vRealize Log Insight does not provide a user interface for Admin users to reset their own passwords, if the user does not remember their current password.

Note Admin users who are able to log in can reset the password of other Admin users. Reset the Admin user password only when all Admin user accounts' passwords are unknown.

Solution

Prerequisites

- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance. See Configure the Root SSH Password for the vRealize Log Insight Virtual Appliance
- To enable SSH connections, verify that TCP port 22 is open.

Procedure

1. Establish an SSH connection to the vRealize Log Insight virtual appliance and log in as the root user.
2. Type `li-reset-admin-passwd.sh` and press **Enter**.

   The script resets the Admin user password, generates a new password and displays it on the screen.

What to do next

Log in to the vRealize Log Insight Web user interface with the new password and change the Admin user password.

Reset the Root User Password

If you forget the password of the root user, you can no longer establish SSH connections or use the console of the vRealize Log Insight virtual appliance.

Problem

If you cannot establish SSH connections or use the console of the vRealize Log Insight virtual appliance, you cannot accomplish some of the administration tasks, nor can you reset the password of the admin user.

Solution

You may not be able to log in as root for a variety of reasons including:

- You have not changed the default password. By default, vRealize Log Insight sets a blank password for the root user and disables SSH access. Once the password is set, SSH access for the root user is enabled.
- You set an SSH key during the deployment of the vRealize Log Insight virtual appliance. If an SSH key is specified through OVF, then password authentication is disabled. Either log in with the set SSH key or see the solution steps below.
- You entered the password incorrectly multiple times and you are now temporarily locked out. In this case, entering the correct password will not get you in until the lock out period has elapsed. You can either wait or restart the virtual appliance.

Procedure

1. In the vSphere Client, perform a guest shutdown of the vRealize Log Insight virtual appliance.
2. After the virtual machine is powered down, select **Edit Settings**.
3. Select the **Options** tab.
4. Under **vApp Options** > **Advanced**, select **Properties**.
5. Find and edit the `vm.rootpw` key.

   If you do not see a `vm.rootpw` key then add a new one.

   If you are using SSH keys instead of password authentication, then edit or add the `vm.sshkey` key.
6. Enter a password.

   You can add an SSH key here instead if you are not using password authentication.
7. Power on the virtual appliance.

What to do next

After vRealize Log Insight boots, validate that you can log in as the root user.

Alerts Could Not Be Delivered to vRealize Operations Manager

vRealize Log Insight notifies you if an alert event cannot be sent to vRealize Operations Manager. vRealize Log Insight retries sending the alert every minute until the problem is resolved.

Problem

A red sign with an exclamation mark appears in the vRealize Log Insight toolbar when an alert could not be delivered to vRealize Operations Manager.

Cause

Connectivity problems prevent vRealize Operations Manager vRealize Log Insight from sending alert notifications to vRealize Operations Manager.

Solution

- Click on the red icon to open the list of error messages, and scroll down to view the latest message.

  The red sign disappears from the toolbar when you open the list of error messages, or if the problem is resolved.
- To fix the connectivity problem with vRealize Operations Manager, try the following.
  - Verify that the vRealize Operations Manager vApp is not shut down.
  - Verify that the you can connect to vRealize Operations Manager via the **Test Connection** button in the **vRealize Operations Manager** section of the **Administration** page of the vRealize Log Insight Web user interface.
  - Verify that you have the correct credentials by logging directly into vRealize Operations Manager.
  - Check vRealize Log Insight and vRealize Operations Manager logs for messages related to connectivity problems.
  - Verify that no alerts are filtered out in vRealize Operations Manager vSphere User Interface.

Unable to Log In Using Active Directory Credentials

You cannot log in to the vRealize Log Insight Web user interface when you use Active Directory credentials.

Problem

You cannot log in to vRealize Log Insight by using your Active Directory domain user credentials, despite that an administrator has added your Active Directory account to vRealize Log Insight.

Cause

The most common causes are expired passwords, incorrect credentials, connectivity problems, or lack of synch between the vRealize Log Insight virtual appliance and Active Directory clocks.

Solution

- Verify that your credentials are valid, your password has not expired, and your Active Directory account is not locked.
- If you have not specified a domain to use with Active Directory authentication, verify that you have an account on the default domain stored in the latest vRealize Log Insight configuration at `/storage/core/loginsight/config/loginsight-config.xml#[number]` where [number] is the largest.
- Find the latest configuration file: `/storage/core/loginsight/config/loginsight-config.xml#[number]` where `[number]` is the largest.
- Verify vRealize Log Insight has connectivity to the Active Directory server.
  - Go to the **Authentication** section of the **Administration** page of the vRealize Log Insight Web user interface, fill in your user credentials, and click the **Test Connection** button.
  - Check the vRealize Log Insight `/storage/var/loginsight/runtime.log` for messages related to DNS problems.
- Verify that the vRealize Log Insight and Active Directory clocks are in synch.
  - Check the vRealize Log Insight `/storage/var/loginsight/runtime.log` for messages related to clock skew.
  - Use an NTP server to synchronize the vRealize Log Insight and Active Directory clocks.

SMTP does not work with STARTTLS option enabled

When you configure the SMTP server with the STARTTLS option enabled, test emails fail. Add your SSL certificate for the SMTP server to the Java truststore to resolve the problem.

Prerequisites

- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance.
- If you plan to connect to the vRealize Log Insight virtual appliance by using SSH, verify that TCP port 22 is open.

Procedure

1. Establish an SSH connection to the vRealize Log Insight vApp and log in as the root user.
2. Copy the SSL certificate for the SMTP server to the vRealize Log Insight vApp.
3. Run the following command.

```
`/usr/java/latest/bin/keytool -import -alias certificate_name -file path_to_certificate -
keystore /usr/java/latest/lib/security/cacerts`
```

Note The outer quotes are inserted by using the back quote symbol that is on the same key as tilde on your keyboard. Do not use single quotes.

4 Enter the default the password **changeit**.

5 Run the `service loginsight restart` command.

What to do next

Navigate to **Administration > Smtp** and use **Send Test Email** to test your settings. See Configure the SMTP Server for vRealize Log Insight

Upgrade Fails Because the Signature of the .pak file Cannot Be Validated

vRealize Log Insight upgrade fails because of a corrupted `.pak` file, expired license or insufficient disk space.

Problem

Upgrading vRealize Log Insight fails and you see an error message `Upgrade Failed. Failed to upgrade: Signature of the PAK file cannot be validated`.

Cause

The error might occur for the following reasons:

- The uploaded file is not a `.pak` file.
- The uploaded `.pak` file is not complete.
- The license of vRealize Log Insight has expired.
- The vRealize Log Insight virtual appliance root file system does not have enough disk space.

Solution

- Verify that you are uploading a `.pak` file.
- Verify the md5sum of the `.pak` file against the VMware download site.
- Verify that at least one valid license is configured on vRealize Log Insight.
- Log in to the vRealize Log Insight virtual appliance and run `df –h` to check the available disk space.

> **Note** Do not put files on the vRealize Log Insight virtual appliance root file system.

Upgrade Fails with an Internal Server Error

vRealize Log Insight upgrade fails with an Internal Server Error because of a connection problem.

Problem

Upgrading vRealize Log Insight fails and you see an error message `Upgrade Failed. Internal Server Error`.

Cause

A connection problem occurred between the client and the server. For example, when you attempt to upgrade from a client that is on a WAN.

Solution

- Upgrade LI from a client on the same LAN as the server.