IBM Security Directory Suite
8.0.1

Virtual Appliance Administration Guide

Chapter 1. Virtual appliance administration

To administer and manage the Directory Server virtual appliance, log on to the IBM® Security Directory Suite virtual appliance console.

Virtual appliance monitoring

You can view graphs and data about the memory usage, CPU usage, and storage, and configure SNMP monitoring for the virtual appliance.

Viewing the event log

System events are logged when the system settings are changed or when problems occur with the virtual appliance. Use the **Event Log** page to view or export system events on your network.

Procedure

1. From the top-level menu of the virtual appliance console, click **Monitor** > **Logs** > **Event Log**.
2. On the **System Events** tab, take one of the following actions:
   - Click **Start Live Streaming** to view a live update of the event log.
   - Click **Pause Live Streaming** to stop the live updating of the event log.
   - Filter the system events by completing the following steps:
     a. Click the filter icon to display the **Filter** window.
     b. In the **Match** field, you can select either **all rules** or **any rules**.

        Restriction: Regardless of the option you select, you cannot add multiple rules for a filter. The **+** icon for adding another rule is disabled. This is a known limitation.
     c. From the **Column** list, select one of the following columns to filter the events:
        - Any Column
        - Priority
        - Event ID
        - Event Description
        - Time Occurred

        Note: When you select **Any Column** in the **Column** field and specify a filter criteria that applies to the **Time Occurred** column, the virtual appliance does not return results. Select **Time Occurred** in the **Column** field to filter values in that column.
     d. From the **Condition** list, select a filter condition. The available filter conditions vary depending on the column that you selected for filtering. The possible filtering conditions include these options:
        - contains
        - is
        - starts with
        - ends with
        - before
        - after
        - range
     e. In the **Value** field, specify a filter value.

f. Click **Filter** to apply the filter or click **Clear** to clear the filter and view all events.

- Click **Export** to download the displayed event log data to a CSV file.

  Note: The default file name is `export.csv`.

  – In the exported event log file, the **Time Occurred** column shows the time since Epoch (1 January 1970, 00:00:00 Universal time).

  – When you use the table filter on the **Priority** field, the values that can be filtered are in English only (low, medium, and high). This behavior is expected on all language versions of the virtual appliance.

- To clear the filter and display all events, click the **Clear filter** link next to the filter icon under the column headings.

Monitoring memory usage

View the memory graph to see the memory that is used by the virtual appliance.

Procedure

1. From the top-level menu of the virtual appliance console, click **Monitor** > **Monitoring** > **Memory**.

   The **System Memory Statistics** page is displayed.
2. Select a **Date Range**.
   - **1 Day** displays data points for every minute during the last 24 hours.
   - **3 Days** displays data points for every 5 minutes during the last 3 days. Each data point is an average of the activity that occurred in that hour.
   - **7 Days** displays data points every 20 minutes during the last 7 days. Each data point is an average of the activity that occurred in that hour.
   - **30 Days** displays data points for every hour during the last 30 days. Each data point is an average of the activity that occurred in that hour.
3. In the legend area, select **Memory Used** to review the total used memory. The **Details** section displays these statistics:
   - **Total** indicates the total system memory.
   - **Used** indicates the system memory that is used.
   - **Free** indicates the system memory that is available.
   - **As of** indicates the current date, time, and the Coordinated Universal Time (UTC) identifier.

Monitoring the CPU usage

View the CPU graph to see the CPU usage by the virtual appliance.

Procedure

1. From the top-level menu of the virtual appliance console, click **Monitor** > **Monitoring** > **CPU**. The System CPU Statistics page is displayed.
2. Select a **Date Range**.
   - **1 Day** displays data points for every minute during the last 24 hours.
   - **3 Days** displays data points for every 5 minutes during the last 3 days. Each data point is an average of the activity that occurred in that hour.
   - **7 Days** displays data points every 20 minutes during the last 7 days. Each data point is an average of the activity that occurred in that hour.
   - **30 Days** displays data points for every hour during the last 30 days. Each data point is an average of the activity that occurred in that hour.

3. In the legend area, select one or more of the options, **User CPU**, **System CPU**, or **Idle CPU** to view the related CPU usage data on the graph. The **Details** section displays the following corresponding statistics:

   - **User CPU** indicates the CPU use by the user.
   - **System CPU** indicates the CPU use by the system.
   - **Idle CPU** indicates the idle use of the CPU.
   - **As of** indicates the current date, time, and the Coordinated Universal Time (UTC) identifier.

Monitoring the storage

View the storage graph to see the percentage of disk space that is used by the boot and root partitions of the virtual appliance.

Procedure

1. From the top-level menu of the virtual appliance console, click **Monitor** > **Monitoring** > **Storage**. The **Storage Statistics** page is displayed.
2. Select a **Date Range**.
   - **1 Day** displays data points for every minute during the last 24 hours.
   - **3 Days** displays data points for every 5 minutes during the last 3 days. Each data point is an average of the activity that occurred in that hour.
   - **7 Days** displays data points every 20 minutes during the last 7 days. Each data point is an average of the activity that occurred in that hour.
   - **30 Days** displays data points for every hour during the last 30 days. Each data point is an average of the activity that occurred in that hour.
3. In the legend area, select **Root** or **Boot** or both to view the total used storage on the graph. The **Details** section displays the following corresponding statistics:
   - **Boot** indicates the boot partition. It displays the size of the partition and the used and available storage information in MB.
   - **Root** indicates the base file system, where the system user is root. It displays the size of the partition and the used and available storage information in MB.

Configuring SNMP monitoring

The current virtual appliance status can be monitored by using SNMP. This status shows an SNMP agent, which can be queried by any SNMP manager or monitoring tools that support SNMP to obtain the status of the running virtual appliance.

About this task

When configured, the SNMP agent listens on all management interfaces. The SNMP Monitoring function can be used to monitor the virtual appliance in an IBM Security Directory Suite monitoring environment. To monitor a virtual appliance, it uses the Agentless Monitoring for Linux OS agent. For more information about configuring the IBM Security Directory Suite monitoring environment and the Agentless Monitoring for Linux OS agent, see the IBM Knowledge Center.

Procedure

1. From the top-level menu of the virtual appliance console, click **Monitor** > **Monitoring** > **SNMP Monitoring**.
2. On the **SNMP Monitoring** page, click **Reconfigure**.
3. On the **Configure SNMP** page, select one of the following SNMP Protocol versions that the agent must use:

- Disabled
- SNMPv1/SNMPv2c
- SNMPv3

Note: If you select **Disabled**, SNMP monitoring is disabled and the fields that are described in the following steps are not available.

4. In the **Port** field, specify the port number on which that the SNMP agent must listen.

   Note: The default port number is 161.

5. Depending on the SNMP protocol version that you selected, you must also configure the following details:

   SNMPv1/SNMPv2c

   a. In the **Community** field, type the name of the community that the SNMP manager uses to authenticate with the SNMP agent.

   SNMPv3

   a. From the **Security level** list, select the security level of the user. The available options are:

      - **noAuthNoPriv**: unauthenticated and unencrypted
      - **authNoPriv**: authenticated by unencrypted
      - **authPriv**: authenticated and encrypted

   b. In the **Security user** field, specify the name of the user to be authenticated.

   c. From the **Auth protocol** list, select the authentication protocol that you want to use: **SHA** or **MDS**.

   d. In the **Auth password** field, specify the password to use for authentication. The password must be a minimum of 8 characters in length.

   e. In the **Auth password (confirm)** field, retype the authentication password.

   f. From the **Privacy protocol** list, select the privacy protocol that you want to use: **CES** or **CBC-DES**.

   g. In the **Privacy password** field, specify the password that must be used as a privacy passphrase. The password must be a minimum of 8 characters in length.

   h. In the **Privacy password (confirm)** field, retype the privacy password.

6. Click **Save Configuration**.

Virtual appliance firmware and fix packs

Use the **Manage** > **Firmware and Fix Pack** menu on the virtual appliance console to create backups, update firmware, apply fix packs, and manage the active partition for virtual appliance.

Managing the firmware settings

The virtual appliance has two partitions with separate firmware on each partition. Partitions are swapped during firmware updates so that you can roll back the firmware updates.

Before you begin

As a precautionary measure to avoid issues, you must ensure that all processes are in the stopped state before you proceed with the this procedure.

About this task

Either partition can be active on the virtual appliance. In the factory-installed state, partition 1 is active and contains the firmware version of the current released product. When you apply a firmware update, the update is installed on partition 2 and your policies and settings are copied from partition 1 to partition 2. The virtual appliance restarts the system by using partition 2, which is now the active partition.

Note: The virtual appliance comes with identical firmware versions installed on both of the partitions so that you have a backup of the initial firmware configuration.

Tip: Avoid swapping partitions to restore configuration and policy settings. Use snapshots to back up and restore configuration and policy settings. See "Managing the snapshots" on page 14.

Procedure

1. From the top-level menu of the virtual appliance console, click **Manage** > **Firmware and Fix Pack** > **Firmware Settings**. The **Firmware Settings** page is displayed.
2. On the **Firmware Settings** page, do one or more of the following actions.
   - To enter or revise the comments about the partition, take the following actions:
     a. Select the partition
     b. Click **Edit** and enter or revise the comment.
     c. Click **Save Configuration**.
   - To create a backup of the active partition, take the following actions:

     Important: Create a backup of your firmware only when you are installing a fix pack that is provided by IBM Customer Support. Fix packs are installed on the active partition and you might not be able to uninstall the fix pack.

     a. Under the **Action** column, click **Create Backup**.
     b. When the **Confirm Backup** message appears, click **Yes**.

     The backup process can take several minutes to complete.
   - To set a partition as active, take the following actions:
     a. Under the **Action** column, click **Set Active**.
     b. When the **Confirm Partition Swap** message appears, click **Yes**.

     Set a partition active when you want to use the firmware that is installed on that partition. For example, you might want to set a partition active to use firmware that does not contain a recently applied update or fix pack.

What to do next

If you set a partition to active, the virtual appliance restarts the system by using the newly activated partition.

Installing a fix pack

Install a fix pack on the virtual appliance to address software maintenance updates for reliability and performance enhancements.

Before you begin

Important: If FIPS mode is enabled for the virtual appliance, see FIPS compliance for important information before you install a fix pack on a FIPS-compliant virtual appliance.

As a precautionary measure to avoid issues, you must ensure that all processes are in the stopped state before you proceed with creating a partition backup or installing a fix pack.

Fix packs are applied to your active partition. You can manually create a backup of your active partition before you apply a fix pack so that you can roll back your changes.

Restriction: You cannot uninstall or roll back a fix pack by using the local management interface. You must use the command-line interface to uninstall a fix pack.

About this task

If a fix pack is installed on the virtual appliance, you can view information about who installed the fix pack, comments, patch size, and the installation date.

Procedure

1. From the top-level menu of the virtual appliance console, click **Manage** > **Firmware and Fix Pack** > **Fix Packs**.

   The **Fix Packs** page with a table that lists the installed fix packs, date of installation, and description is displayed.
2. Click **New**.
3. In the **Add Fix Pack** window, click **Browse for fix pack** to locate, select, and add the fix pack file. The **Browse for fix pack** table displays the selected fix pack details.
4. Click **Save Configuration** to install the fix pack.

Virtual appliance maintenance

Use the **Manage** > **Maintenance** menu on the virtual appliance console to accomplish maintenance tasks such as retrieving log files and core dump files.

Retrieving log files

You can retrieve and view virtual appliance and component-specific log files to troubleshoot issues better.

About this task

The following log files are available:

Appliance

The following log files assist you to debug any configuration failures that occur in the virtual appliance:

- Server Console
- Server Message
- Server Trace
- System Log
- Server System Out

Directory

The following are some of the log files that can assist you to identify issues in IBM Security Directory Suite:

- Administration Server audit log file (`adminaudit.log`) is used to check for suspicious patterns of activity and to detect security violations.
- Bulkload error log file (`bulkload.log`) contains the status and errors that are related to bulkload.
- DB2 CLI commands log file (`db2clicmds.log`) contains errors that are encountered with DB2 commands are run from the CLI.
- Administration Server log file (`ibmslapd.log`) contains status and error messages that are related to the server.
- Lost and found log (`lostandfound.log`) contains errors that occur as a result of a replication conflict.
- Trace file (`traceibmslapd.log`) contains trace information for Directory Server or commands if tracing is enabled.
- Server audit log file (`audit.log`) contains the DNs of the administrative group members and their assigned roles for each time the server starts and whenever their roles change.

- DB2 error log file (`db2cli.log`) contains database errors that occur as a result of LDAP operations.
- Administration Server log (`ibmdiradm.log`) contains the status and errors that are encountered by the administration server.
- Tools log (`idstools.log`) contains status and error messages that are related to the configuration tools.
- Performance tuning tool statistics file (`perftune_stat.log`) contains suggested performance values based on information that is gathered during the basic tuning and advanced tuning phases.

The other log files that are available are: `idsadm.log`, `idsadmdb2.log`, `idsadmdb2cmds.log`, `db2diag.log`, Federated Directory Server `ibmdi.log`, Federated Directory Server `updateinstaller.log`, Web Administration Tool console log, and Web Administration Tool messages log.

In this table, you can also view the log files that are generated when you run certain virtual appliance commands from the command-line interface. For example, if you run the **`idsimigr`** command, the log file `idsimigr_cmd.out.log` can be viewed.

Procedure

1. From the top-level menu of the virtual appliance console, select **Manage** > **Maintenance** > **Log Retrieval and View**.
2. Click **Appliance** or **Directory** tab to view, download, and clear the logs.
3. In the table, select a log file.
4. Take one of the following actions:
   - Click **View** to display the contents of the selected log file.
   - Click **Download** to download a copy of the log file.

     Restriction: The download option works only if the logs are located in the default directory for log files.
   - Click **Refresh** to display the most recent version of the log files, including changes that were made to the data since it was last refreshed.
   - Click **Clear**, and confirm the action to remove the contents from the selected log file.

Managing the core dump files

Use the **Core Dumps** page to delete or download core dump files in the virtual appliance.

About this task

A core dump file stores a large amount of raw data for further examination. Use the core dump files to diagnose or debug errors in the virtual appliance.

Procedure

1. From the top-level menu of the virtual appliance console, select **Manage** > **Maintenance** > **Core Dumps**.

   The **Core Dumps** page displays a table with a list of core dump files.
2. On the **Core Dumps** page, take one of the following actions:
   - Delete the core dump files:
     a. In the **File Name** column, select one or more core dump files that you want to delete. To select all the core dump files, select the check box next to **File Name** in the column heading.
     b. Click **Delete**.
     c. Click **Yes** to confirm.
   - Download the core dump files:

    a. In the **File Name** column, select a core dump file. You can select only one core dump file for downloading.
    b. Click **Download**. The core dump file is downloaded in an archived format such as `.zip`.

- Click **Refresh** to update the table with the most recently generated core dump files.

Activating support mode on virtual appliance

Activate support mode by using a key that is provided by the IBM Support team to address software maintenance or enhancements on the virtual appliance.

Before you begin

1. Raise a Problem Management Record (PMR) with IBM Support.
2. Provide the unique ID (UUID) of your virtual appliance system to IBM Support. The **Appliance UUID** is displayed on the **Support Mode Activation** page.
3. Obtain the support mode activation key for your virtual appliance from IBM Support.

Restriction: While the support mode is activated, the following action(s) must not be performed:

- Modification of appliance date and time
- Firmware upgrade
- Migration tasks

Procedure

1. From the top-level menu of the virtual appliance console, click **Manage** > **Maintenance** > **Support Mode Activation**.

   The **Support Mode Activation** page is displayed, which shows the UUID, current support mode activation status, issue date, and expiration date.
2. Click **Activate Mode**.

   This option is available only if support mode is not already activated on your virtual appliance environment.
3. Click **I agree** to accept the **Support Mode Service Level Agreement** that is displayed.
4. Enter the support mode **Activation Key** that is provided to you by IBM Support.

   The support mode activation key looks like the following example:

   ```
   1693315ab07f8948bbb1fc60a4e5326180b45f3c351781e3c7dc89096cf1d4099d00a71213b6c873
   19c9cbc879106e273a27b2fb60549213ff0cebf3af5e84608568256ce12b6c4ce938732cffdbc7f7
   c3dd0165eb916c5d51061d8d032d09d336bdd809d922e57ccc3e29d0ab1eb6bbfa7cafac0ef1e5bb
   6e1deb21fb4609381d8b4cf6897f0046e4152a28478db9eff8f4f4bc672868a8d86ec567d52ec52c
   0999578fce3a05be9aaf8939e25e0107a01b7c821ead59d18e5422867821824e1d62d9e0aa84d852
   602d2ed98c4ff60a88b7f3d114d9775c44fc02da12769d761a79f3b3bb16b6c5ca1b1fb379fbcfde
   3d661960a82802bfb0f7de56054920d9
   ```
5. Click **Save Configuration**.

   The **Support Mode Activation Status** is displayed as enabled, which indicates that the shell prompt is now enabled on your virtual appliance environment to debug the reported issue.

   The **Issue Date** and **Expiration Date** fields are also updated with the activated support mode details.

   After support mode is activated, the title banner on the virtual appliance console displays the message: "Support Mode activated. Do not use the Support Mode in production environment."
6. After the support operations are completed on the virtual appliance, click **Deactivate Mode** if instructed to do so by IBM Support. Support mode is also deactivated automatically when the activation key expires.

   After support mode is deactivated, the message on the title banner on the virtual appliance console is not displayed any more.

Viewing information about the product

View the **About** page to learn about the IBM Security Directory Suite virtual appliance and its content.

Procedure

1. From the top-level menu of the virtual appliance console, click **Manage** > **Maintenance** > **About**.
2. View the product-specific information for the virtual appliance.

Results

The following information is displayed in the **About** page:

Product Name
Displays the name of product that you are using.

Product Version
Displays the version of product that you are using.

Installed Fix Packs
Displays the last fix pack level that was installed for the version of the product that you are using.

Build number
Displays the current build number for the version of the product that you are using.

Build Date and Time
Displays the date and the exact time and the time zone on which the last build occurred.

FIPS Mode Status
Indicates whether FIPS 140-2 mode is enabled. For more information, see FIPS compliance.

For example:

```
Product Name:          IBM Security Directory Suite
Product Version:       8.0.1
Installed Fix Packs:   None
Build Number:          20150814-1017
Build Date and Time:   May 18, 2016 8:49:16 PM
FIPS Mode Status:      Disabled
```

Virtual appliance network settings

Use the **Manage** > **Network Settings** menu on the virtual appliance console to configure virtual appliance network settings such as the hosts file, static routes, and application interfaces.

Managing the hosts file

The hosts file is used to map host names to IP addresses. To manage the hosts file with the virtual appliance, use the **Manage Hosts File** page.

Procedure

1. From the top-level menu of the virtual appliance console, click **Manage** > **Network Settings** > **Hosts File**. All current host records with their IP addresses and host names are displayed.
2. On the **Manage Hosts File** page, work with host records or host names.
   - To add a host record, take the following actions:
     a. Select the root level **Host Records** entry or do not select any entries.
     b. Click **New**. The **Create Host** record page is displayed.
     c. In the **Address** field, specify the IP address of the host record.
     d. In the **Host Name** field, specify the host name of the host record.

    e. Click **Save**.

- To add a host name to a host record, take the following actions:

    a. Select the host record entry to which you want to add the host name.

    b. Click **New**.

    c. On the **Add Hostname to Host Record** page, enter the host name.

    d. Click **Save**.

  Note: You can add multiple host names to the same host record entry by repeating this process.

- To remove a host record, take the following actions:

    a. Select the host record entry that you want to delete.

    b. Click **Delete**.

    c. When the confirmation message appears, click **Yes** to confirm the deletion.

- To remove a host name from a host record, take the following actions:

    a. Select the host name entry that you want to delete.

    b. Click **Delete**.

    c. When the confirmation message appears, click **Yes** to confirm the deletion.

  Note:

  – If the selected host name is the only associated host name for the IP address, then the entire host record (the IP address and host name) is removed.

  – You must not delete localhost entries like `127.0.0.1` and `::1` from the `etc/hosts` file.

- To display the most recent version of the data, click **Refresh**.

Configuring static routes

Configure static routes to the paired protection interfaces on your virtual appliance to enable network routers to redirect users to block pages or authentication pages.

About this task

This task is only necessary for networks that contain an extra network segment between the user segment and the virtual appliance.

Note: If you selected IPv6 Configuration Mode as `Automatic` when you configured the initial virtual appliance settings after installation, then you cannot update the default gateway value for IPv6. The option to edit is disabled under **Static Routes**.

Procedure

1. From the top-level menu of the virtual appliance console, click **Manage** > **Network Settings** > **Routes**.
2. On the **Static Routes** page, complete one of the following steps.

- To specify the IPv4 default gateway, take the following actions:

    a. In the **IPv4 Default Gateway** field, specify an address value. For example: `192.0.2.5`.

    b. Click **Save**.

  Note: Click **Reset** to update the displayed value back to the current default gateway. It does not make any updates to the actual default gateway value.

- To specify the IPv6 default gateway, take the following actions:

    a. In the **IPv6 Default Gateway** field, specify an address value. For example: `2001:0DB8:0000:0000:02AB:00FF:FE29:9C6A`.

    b. Click **Save**.

Note: Click **Reset** to update the displayed value back to the current default gateway. It does not make any updates to the actual default gateway value.

- To create a route, take the following actions:

  a. Click **New**.

  b. In the **Add Route** window, define values in the following fields.

     i) **Destination (Host or Network)**

     ii) **Gateway**

     iii) **Metric**

     iv) **Interface or Segment**

  c. Click **Save Configuration**.

- To modify an existing route, take the following actions:
  - From the **Static Routes** table, select an existing route.
  - Click **Edit** to change the settings.
  - In the **Edit Route** window, edit the values in the fields.
  - Click **Save Configuration**.
- To delete a route, take the following actions:
  - From the **Static Routes** table, select an existing route.
  - Click **Delete**.
  - Click **Yes** to confirm your action.

Results

The new and edited system routes are displayed in the **Currently active system routes** table.

Note: If you want your appliance to use application IP address instead of management IP addresses while communicating over network, you can add static routes to the virtual appliance. You specify destination details as the Destination (Host or Network) and the application IP address as the Interface or Segment.

Managing application interfaces

You can enable an application interface for Directory Server to listen on the IP address that you specify. To manage application interfaces, use the **Application Interfaces** page of the virtual appliance console.

About this task

According to the hardware requirements for the virtual appliance server, three network interface cards are required. Two interfaces are used to configure the management interfaces, M1 and M2. The third interface, P1, can be enabled as the application interface for Directory Server. Other interfaces, if any, can be configured as backup.

Procedure

1. From the top-level menu of the virtual appliance console, click **Manage** > **Network Settings** > **Application Interfaces**.

   The **Application Interfaces** page displays the **Interface** tab with a table that has the following columns.

   Type
   Indicates whether the type is IPv4 or IPv6.

   Address
   Specifies the IP address of the application interface.

Interface FQDN
Specifies the full qualified domain name for the application interface.

Netmask/Prefix
Indicates the netmask or prefix of the application interface.

2. On the **Application Interfaces** page, you can create, edit, or delete an application interface and test connectivity.

   - To create an application interface, take the following actions:

     a. Click **New**. The **Add Address** window is displayed.

     b. Select **IPv4** or **IPv6** to indicate the type of address you want to add.

        IPv4
        IPv4 defines each interface on a network uniquely. IPv4 is a 32-bit numeric address, which is written in decimal as four sets of digits, which are separated by periods, with no spaces or consecutive periods. Each number can be 0 - 255. For example:

        ```
        192.0.2.5
        ```

        IPv6
        IPv6 improves the efficiency of routing and provides greater security. IPv6 is a 128-bit IP address, which is written in hexadecimal and separated by colons. For example:

        ```
        2001:db8:8484:3:220:f9ff:fe25:70cf
        ```

     c. In the **Interface FQDN** field, specify the fully qualified domain name for the application interface.

     d. In the **Address** field, specify the IP address for the application interface.

     e. If you selected **IPv4**, in the **NetMask** field, specify the netmask of the application interface.

     f. If you selected **IPv6**, in the **Prefix** field, specify the prefix of the application interface.

     g. Click **Save**.

     h. In the **Confirm Action** window, a message indicates that editing the application interface restarts the virtual appliance. Click **Yes** to confirm.

     The application interface record is listed in the Interface table.

   - To edit an existing application interface, take the following actions:

     a. Select an application interface from the table.

     b. Click **Edit**. The **Edit Address** window is displayed.

     c. Modify the values in the fields as required.

     d. Click **Save**.

     e. In the **Confirm Action** window, a message indicates that editing the application interface restarts the virtual appliance. Click **Yes** to confirm.

   - To delete an application interface, take the following actions:

     a. Select an application interface from the table.

     b. Click **Delete**.

     c. In the **Confirm Action** window, click **Yes** to confirm.

   - To test connectivity, take the following actions:

     Note: The **Test** option is available only for IPv4 interface and fully qualified domain name (FQDN).

     a. On the **Application Interfaces** page, click **Test**. The **Ping Server** window is displayed.

     b. In the **Server** field, enter the IP address of the server for which you want to test the connection.

     c. Click **Test**.

d. If the connection is successful, a notification message is displayed. If the connection failed, an error message is displayed.

- Click **Refresh** to display the most recent version of the application interfaces data, including changes that were made to the data since it was last refreshed.

Results

After you configure the application interface, the virtual appliance is restarted automatically.

On the **Appliance Dashboard**, the **Interfaces** widget lists the application interface that you configured as:

Type	Name	Address
Application	P.1	*IP_address*

What to do next

After you enable the application interface, use the `idssethost` command to configure Directory Server to bind to the IP address.

Virtual appliance system settings

Use the **Manage** > **System Settings** menu on the virtual appliance console to work with system settings such as the date and time, administrator password, session timeout, snapshots, support files, system alerts, and other settings.

Managing the date and time settings

Use the **Date/Time** page to configure the date, time, time zone, and NTP server information of the virtual appliance.

About this task

When you install the virtual appliance, accept the current default system date to avoid any issues.

Note: You must not modify the date and time settings when support mode is activated. Support mode activation is indicated by a message on the title banner of the virtual appliance console. See Activating support mode on virtual appliance.

Procedure

1. From the top-level menu of the virtual appliance console, click **Manage** > **System Settings** > **Date/Time**. The **Date/Time** page is displayed.
2. You can configure the following options on the **Date/Time** page:
   - In the **Date** field, specify the day, month, and year for the virtual appliance.
   - In the **Time** field, specify the time.
   - In the **Time Zone** field, specify the time zone for the virtual appliance.
   - Select **Enable NTP** to specify that virtual appliance must use an NTP (Network Time Protocol) server.
   - In the **NTP Server Addresses** field, specify the IP address of the NTP server that virtual appliance must use. You can enter multiple NTP server addresses, which are separated by commas.
3. Click **Save Configuration**.
4. Optional: Click **Reset** to set the configuration again or differently.

   Note: After you enable NTP, UDP port 123 is always listening even if the local clock is disabled. Listening on UDP port 123 is standard NTP behavior. You can choose to block UDP port 123 with a firewall but blocking the port essentially disables the NTP feature.

Managing the administrator settings

Use the administrator settings to change the password that you use to access your virtual appliance. You can also access the length of idle time that can pass before your session times out.

About this task

If you want to change only the session timeout value, leave the password fields empty. After step 1, proceed directly to step 5.

Procedure

1. From the top-level menu of the virtual appliance console, click **Manage** > **System Settings** > **Administrator Settings**.
2. On the **Administrator Settings** page, type your current password in the **Current Password** field.
3. Type your new password in the **New Password** field.
4. Type your new password again in the **New Password Confirmation** field.
5. Under **Administrator Session**, in the **Session Timeout in minutes** field, click the arrows to specify the amount of time that the session is allowed to be idle before you are automatically logged out.
6. Click **Save Configuration**.
7. Click **Reset** to reset the values back to what they were previously.

Managing the snapshots

Use snapshots to restore prior configuration and policy settings to the virtual appliance.

Before you begin

Before you create or apply a snapshot, you must stop all services and servers that are running. Use the **Server Control** widget on the **Appliance Dashboard** to stop the servers. To stop other services, such as the log management tool or SNMP agent, use the virtual appliance command-line interface.

About this task

Snapshots include all configuration files of IBM Security Directory Suite components, including Directory Server, Federated Directory Server, and SCIM.

Snapshots are stored on the virtual appliance. However, you can download the snapshots to an external drive in case of system failure.

Procedure

1. From the top-level menu of the virtual appliance console, click **Manage** > **System Settings** > **Snapshots**.

   The **Snapshots** page is displayed in a table that contains the file name and a comment or description about each snapshot.
2. On the **Snapshots** page, you can create, edit, delete, apply, or download a snapshot.
   - To create a snapshot, take the following actions:
     a. Click **New**.
     b. On the **Add Snapshot** window, specify helpful comments in the **Comments** field, so that the snapshot is easy to identify in the virtual appliance.
     c. Click **Save Configuration**.
   - To edit the comment for a snapshot, take the following actions:
     a. Select a snapshot.
     b. Click **Edit**.

c. On the **Edit Snapshot** window, edit the existing comment in the **Comments** field.

d. Click **Save Configuration**.

- To delete snapshots, take the following actions:

  a. Select one or more snapshots.

  b. Click **Delete**.

  c. Click **Yes** to confirm.

- To apply a snapshot, take the following actions:

  a. Select a snapshot.

  b. Click **Apply**.

  c. Click **Yes** to confirm.

- To download snapshots, take the following actions:

  – Select one or more snapshots.

  – Click **Download**.

  – Browse to the location where you want to save the snapshot.

  – Save the file.

  Note: If you download multiple snapshots, the snapshots are compressed into a `.zip` file.

- To upload a snapshot, take the following actions:

  – Click **Upload**.

  – In the **Upload Snapshot** window, click **Browse for Snapshot**.

  – Select the snapshot that you want to upload. The snapshot information is displayed in the **Files to upload** table.

  – In the **Comments** field, type a comment to describe the snapshot.

  – Click **Save Configuration**.

  Note: You can upload only one snapshot at a time.

- Click **Refresh** to display the most recent list of snapshots in the table.

Managing support files

IBM Customer Support uses support files to help you troubleshoot problems with the virtual appliance. Support files contain all log files, temporary and intermediate files, and command output that is needed to diagnose customer support problems.

About this task

Support files might contain customer-identifiable information, such as IP addresses, host names, user names, and policy files. Support files do not contain confidential information, such as passwords, certificates, and keys. All files inside a support file contain text that can be inspected and censored by the customer.

The support file contents are stored in a `.zip` file.

Tip: You can create multiple support files to track an issue over time.

Procedure

1. From the top-level menu of the virtual appliance console, click **Manage** > **System Settings** > **Support Files**.
2. On the **Support Files** page, you can create, delete, and download the support files, or edit the comments about the files.

- To create a support file, take the following actions:

  a. Click **New**.

  b. In the **Comment** field of the **Create Support File** window, type a comment to describe the support file.

  c. Click **Save Configuration**.

  A new support file is created for the virtual appliance. The file name is auto-generated and indicates the product name, version, date, and host name of the virtual appliance.

- To edit the comments for a support file, take the following actions:

  a. In the table that displays the list of support files, click to select a support file.

  b. Click **Edit**.

  c. On the **Edit Support File** window, edit the existing comment in the **Comments** field.

  d. Click **Save Configuration**.

- To delete a support file, take the following actions:

  a. In the table that displays the list of support files, click to select one or more support files that you want to delete.

  b. Click **Delete**.

  c. Click **Yes** to confirm.

- To download a support file, take the following actions:

  a. In the table that displays the list of support files, click to select one or more support files that you want to download.

  b. Click **Download**.

  c. Browse to the location where you want to save the support file and save the file.

  Note: If you download multiple support files, the selected `.zip` files are compressed into a single file named `support.zip`.

Configuring system alerts

Configure system alerts for virtual appliance to send notifications about system settings changes and virtual appliance status or issues.

About this task

Available objects include system alerts that are predefined in the virtual appliance and any system alert objects that you created.

Important: Predefined system alert objects cannot be deleted from the virtual appliance because they contain all the events that take place on the virtual appliance. When you create objects such as SNMP, email, or syslog, you can delete these created objects.

Procedure

1. From the top-level menu of the virtual appliance console, click **Manage** > **System Settings** > **System Alerts**.

   The **System Alerts** page displays the **Available Objects** pane and the **Added Objects** pane.

2. On the **System Alerts** page, you can create a system alert object, edit or delete an object that you created, and specify the objects for which you want to receive alerts.

   - To create a system alert object, take the following actions:

     a. On the **System Alerts** page, click **New**.

     b. From the list, select **SNMP**, **Email**, or **Remote Syslog**.

See these related topics to configure one or more of the following system alert objects:

- "Configuring SNMP objects" on page 17
- "Configuring email objects" on page 18
- "Configuring remote syslog objects" on page 18

- To receive notifications when a system event occurs, take the following actions:
  a. Select one or more system alert objects from the **Available Objects** pane.
  b. Move the selected objects to the **Added Objects** pane.
- To edit a system alert object, take the following actions:
  a. Select the object in the **Available Objects** or the **Added objects** pane.
  b. Click **Edit**.
  c. Change the values in the fields according to your requirements.
  d. Click **Save Configuration**.
- To delete a system alert object:
  a. Select the object in the **Available Objects** or the **Added objects** pane.
  b. Click **Delete**.
  c. Click **Yes** to confirm.

3. Click **Save Configuration**.
4. Click **Reset** to revert to the last updated changes.

Configuring SNMP objects

Configure Simple Network Management Protocol (SNMP) objects to enable the virtual appliance to send system alerts to an SNMP manager. The SNMP notifications identify certain values and send them to an SNMP manager.

Procedure

1. From the top-level menu of the virtual appliance console, click **Manage** > **System Settings** > **System Alerts**.
2. On the **System Alerts** page, take one of the following actions:
   - Click **New** > **SNMP** to display the **Add SNMP Object** window.
   - Select an existing SNMP object that is displayed and then click **Edit** to display the **Edit SNMP Object** window.
3. On the **General** tab, specify a meaningful **Name** for the system alert object.
4. Select an **SNMP Version** from the list: **V1**, **V2C**, or **V3**.
5. In the **SNMP Manager** field, specify the fully qualified domain name (FQDN), IP address, or host name, of the SNMP manager. The specified SNMP host must be accessible to the virtual appliance to send SNMP traps.
6. In the **Port** field, specify the port number that the SNMP manager monitors for notifications. The default port number is 162.
7. Based on the SNMP version that you selected, specify the following details:

   SNMP V1 or V2C

   a. In the **Community** field, specify the name of the community that is used to authenticate with the SNMP agent.

   SNMP V3

   a. Specify the **User Name** to be authenticated in the SNMP database.
   b. On the **Notification Type** tab, select **Inform** or **Trap** in the **Notification Type** field.

c. Optional: Specify the **SNMP Timeout** in seconds.

d. On the **Authentication and Privacy** tab, select **Enabled** from the **Enable Authentication** list to enable authentication.

e. Specify the relevant **Authentication Passphrase**.

f. From the **Authentication Type** list, select an authentication type: **SHA** or **MDS**.

g. From the **Enable Privacy** list, select **Enabled** to enable privacy.

h. Specify the relevant **Privacy Passphrase**.

i. From the **Privacy Type** list, select a privacy protocol: **AES** or **DES**.

8. In the **Comment** field, type a comment to describe the SNMP system alert object.
9. Click **Save Configuration**.

What to do next

After you configure an SNMP object, add the object to the **Added Objects** pane on the **System Alerts** page, so that the virtual appliance initiates the response when specified events occur.

Configuring email objects

Create email objects to send an email notification to specified users or to administrators when specified events occur on your network. You can also select the event parameters to include in the message so that important information about detected events is provided.

Procedure

1. From the top-level menu of the virtual appliance console, click **Manage** > **System Settings** > **System Alerts**.
2. On the **System Alerts** page, take one of the following actions:
   - Click **New** > **Email** to display the **Add Email Object** window.
   - Select an existing email object that is displayed and then click **Edit** to display the **Edit Email Object** window.
3. Specify a meaningful **Name** for the system alert object.
4. In the **From** field, specify the email address that is displayed in the *From* field of the email.
5. In the **To** field, specify the email address or group of addresses that must receive the email. Separate individual email addresses with a comma or a semicolon.
6. In the **SMTP Server** field, specify the fully qualified domain name, IP address, or host name of the mail server. The SMTP server must be accessible to the virtual appliance to sent send email notifications.
7. In the **SMTP Port** field, specify the custom port that is used to connect to the SMTP server. The default is 25.
8. In the **Comment** field, type a comment to describe the email system alert object.
9. Click **Save Configuration**.

What to do next

After you configure an email object, add the object to the **Added Objects** pane on the **System Alerts** page, so that the virtual appliance initiates the response when specified events occur.

Configuring remote syslog objects

Configure remote syslog objects to enable the system to record system events in a remote log file.

Procedure

1. From the top-level menu of the virtual appliance console, click **Manage** > **System Settings** > **System Alerts**.

2. On the **System Alerts** page, take one of the following actions:
    - Click **New** > **Remote Syslog** to display the **Add Remote Syslog Object** window.
    - Select an existing remote syslog object that is displayed and then click **Edit** to display the **Edit Remote Syslog Object** window.
3. Specify a meaningful **Name** for the object.
4. In the **Remote Syslog Collector** field, specify the fully qualified domain name, IP address, or host name of the of the host on which you want to save the log. The host must be accessible to the virtual appliance.
5. In the **Remote Syslog Collector Port** field, specify the custom port that is used to connect to the syslog collector. The default is 514.
6. Select **QRadar Format Enabled** to enable the virtual appliance to send events in QRadar LEEF format instead of RFC5424 remote syslog format.
7. In the **Comment** field, type a comment to describe the remote syslog object.
8. Click **Save Configuration**.

What to do next

After you configure an remote syslog object, add the object to the **Added Objects** pane on the **System Alerts** page, so that the virtual appliance initiates the response when specified events occur.

Restarting or shutting down the virtual appliance

Use the **Restart or Shutdown** page to restart or shut down the virtual appliance.

About this task

Certain operations require that you restart the virtual appliance for the changes to take effect.

Procedure

1. From the top-level menu of the virtual appliance console, click **Manage** > **System Settings** > **Restart or Shut down**.
2. On the **Restart or Shutdown** page, take one of the following actions:
    - Click **Restart**. Restarting the virtual appliance takes it offline for several minutes.
    - Click **Shut down**. Shutting down the virtual appliance takes it offline and makes it inaccessible over the network until you restart it.

Restarting the local management interface

Use the command-line interface to restart the local management interface (LMI) for virtual appliance.

About this task

After certain operations such as product license activation or Admin DN password change, the LMI needs to be restarted for the changes to take effect.

Procedure

1. Access the command-line interface (CLI) of the virtual appliance by using either an `ssh` session or the console.
2. From the command-line interface, log on to the IBM Security Directory Suite virtual appliance. The following message is displayed:

    ```
    Welcome to the IBM Security Directory Suite appliance
    Enter "help" for a list of available commands
    ```

3. Enter the following command:

```
lmi restart
```

Managing advanced tuning settings

You can set tuning parameters that are used with the virtual appliance.

About this task

Note: Change these advanced tuning parameter values only under the supervision of IBM software support.

Procedure

1. Click **Manage System Settings** > **Advanced Tuning Parameters**.
2. Perform any of the following actions.

Table 1. Advanced tuning operations

Button	Procedure
New	a. Click **New**. A dialog opens. b. Type the name for the key. c. Type a value for the key. Multiple values can be specified as a space-separated list. d. Type a comment that describes the key that you created. e. Click **Save Configuration**.
Edit	a. Select a key. b. Click **Edit**. A dialog opens. c. Modify then name for the key. d. Modify the value for the key. Multiple values can be specified as a space-separated list. e. Modify the comment that describes the key. f. Click **Save Configuration**.
Delete	a. Select one or more keys. If you want to delete all the keys, select the **Key** check box. b. Click **Delete**. A confirmation message is displayed. c. Click **Yes** to delete the key or **No** to cancel the operation.

The following advanced tuning parameters are available:

Table 2. Advanced tuning parameters

Parameter	Description
`lmi.security.ciphers`	Enables specific ciphers for the local management interface. Valid values are specified as a space-separated list. The virtual appliance supports all the cipher suites that are supported by Java 8. For a list of the supported cipher suites, see Cipher Suites.

Table 2. Advanced tuning parameters (continued)

Parameter	Description
lmi.security.protocol	Enables specific protocols for the local management interface. Valid values are TLS, TLSv1, and TLSv1.2. The default value is TLSv1.2.
wat.security.ciphers	Enables specific ciphers for the Web Administration Tool. Valid values are specified as a space-separated list. Tool supports all the cipher suites that are supported by Java 8. For a list of the supported cipher suites, see Cipher Suites.
wat.security.protocol	Enables specific protocols for the Web Administration Tool. Valid values are TLS, TLSv1, and TLSv1.2. The default is TLSv1.2
wat.min.heapsize	To set a minimum Web Administration Tool heap size. The size ranges from 4m to 2048m. The default value is 4m.
wat.max.heapsize	To set a maximum Web Administration Tool heap size. The size ranges from 488m to 8048m. The default value is 488m.
sysctl.net.ipv4.tcp_keepalive_time	Time value in seconds. For example: 120. For TCP/IP settings for IBM Security Directory Suite, see TCP/IP Settings.
sysctl.net.ipv4.tcp_keepalive_intvl	Time value in seconds. For example: 120. For TCP/IP settings for IBM Security Directory Suite, see TCP/IP Settings.
sysctl.net.ipv4.tcp_keepalive_probes	Time value in seconds. For example: 60. For TCP/IP settings for IBM Security Directory Suite, see TCP/IP Settings.
update.disable.remote.discovery	Specifies whether the virtual appliance attempts to look for updates on the internet. Set value to 1 to disable remote discovery. When disabled, the IBM Security Directory Suite **Monitor** > **Event Logs** > **System Events** virtual appliance management page will not show the following error message: `GLGUP1012E An attempt to download the primary update catalog has failed. Common causes of this failure are not having a license installed and DNS.`
kernel.disable.spectre	To disable the Spectre and Meltdown fix for the IBM Security Directory Suite virtual appliance, set the value to `true` This parameter is only available from IBM Security Directory Suite virtual appliance, Version 8.0.1.9 and later.

IBM®