# NetApp

# Device resolution

## OnCommand Insight

NetApp
October 24, 2024

# Table of Contents

# Device resolution

You need to discover all of the devices you want to monitor with OnCommand Insight. Discovery is necessary in order to accurately track performance and inventory in your environment. Typically the majority of devices in your environment are discovered through automatic device resolution.

> (i) If you are performing an upgrade and have inactive Auto Resolution rules in the system you are upgrading from, these rules will be deleted during the upgrade. To preserve inactive Auto Resolution rules, activate the rules (check the box) before the upgrade is performed.

After you install and configure data sources, devices in your environment, including switches, storage arrays and your virtual infrastructure of hypervisors and VMs are identified. However, this does not normally identify 100% of the devices in your environment.

After data source type devices have been configured, best practice is to leverage device resolution rules to help identify the remaining unknown devices in your environment. Device resolution can help you resolve unknown devices as the following device types:

- physical hosts
- storage arrays
- tapes
- switches

Devices remaining as "unknown" after device resolution are considered generic devices, which you can also show in queries and on dashboards.

The rules created in turn will automatically identify new devices with similar attributes as they are added to your environment. In some cases, Device resolution also allows for manual identification bypassing the device resolution rules for undiscovered devices within Insight.

Incomplete identification of devices can result in issues including:

- Incomplete paths
- Unidentified multipath connections
- The inability to group applications
- Inaccurate topology views
- Inaccurate data in the Data warehouse and reporting

The Device resolution feature (**Manage** > **Device resolution**) includes the following tabs, each of which plays a role in device resolution planning and viewing results:

- "FC identify" contains a list WWNs and port information of Fibre Channel devices that were not resolved through automatic device resolution. The tab also identifies the percentage of devices that have been identified.
- "IP identify" contains a list of devices accessing CIFs shares and NFS shares that were not identified through automatic device resolution. The tab also identifies the percentage of devices that have been identified.

- "Auto resolution rules" contains the list of rules that are run when performing Fibre channel device resolution. These are rules you create to resolve unidentified Fibre channel devices.
- "Preferences" provides configuration options that you use to customize device resolution for your environment.

# Before you begin

You need to know how your environment is configured before you define the rules for identifying devices. The more you know about your environment the easier it will be to identify devices.

You need to answer questions similar to the following to help you create accurate rules:

- Does your environment have naming standards for zones or hosts and what percentage of these are accurate?
- Does your environment use a switch alias or storage alias and do they match the host name?
- Does your environment use an SRM tool and can you use it to identify host names? What coverage does the SRM provide?
- How often do naming schemes change in your environment?
- Have there been any acquisitions or mergers that introduced different naming schemes?

After analyzing your environment, you should be able to identify what naming standards exist that you can expect to reliability encounter. The information you gathered might be represented graphically in a figure similar to the following:
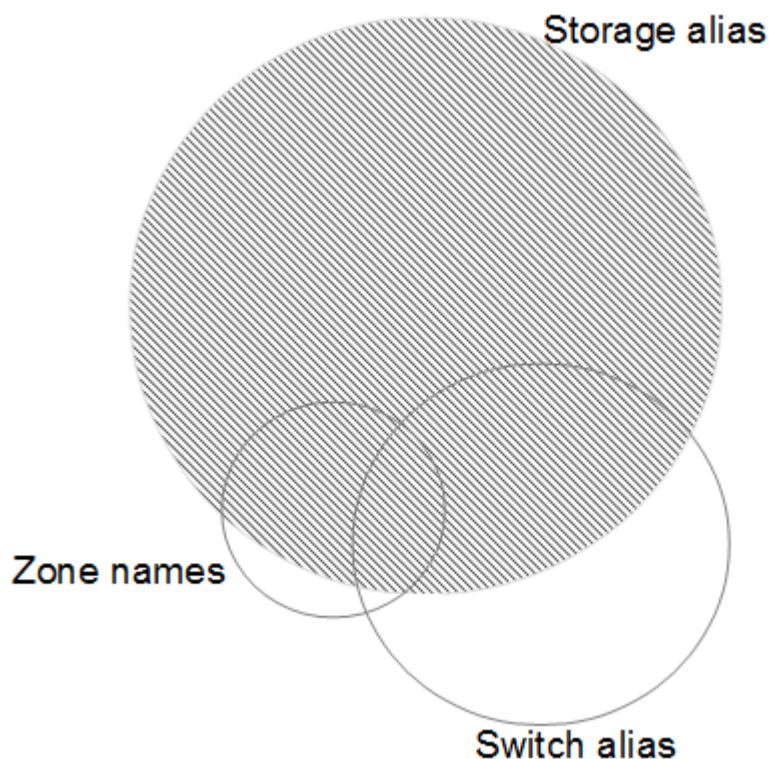


In this example the largest number of devices are reliably represented by storage aliases. Rules that identify hosts using storage aliases should be written first, rules using switch aliases should be written next , and the

last rules created should use zone aliases. Due to the overlap of the use of zone aliases and switch aliases, some storage alias rules might identify additional devices, leaving less rules required for zone aliases and switch aliases.

## Steps to defining devices in your environment

Typically, you would use workflow similar to the following to identify devices in your environment. Identification is an iterative process and might require multiple steps of planning and refining rules.
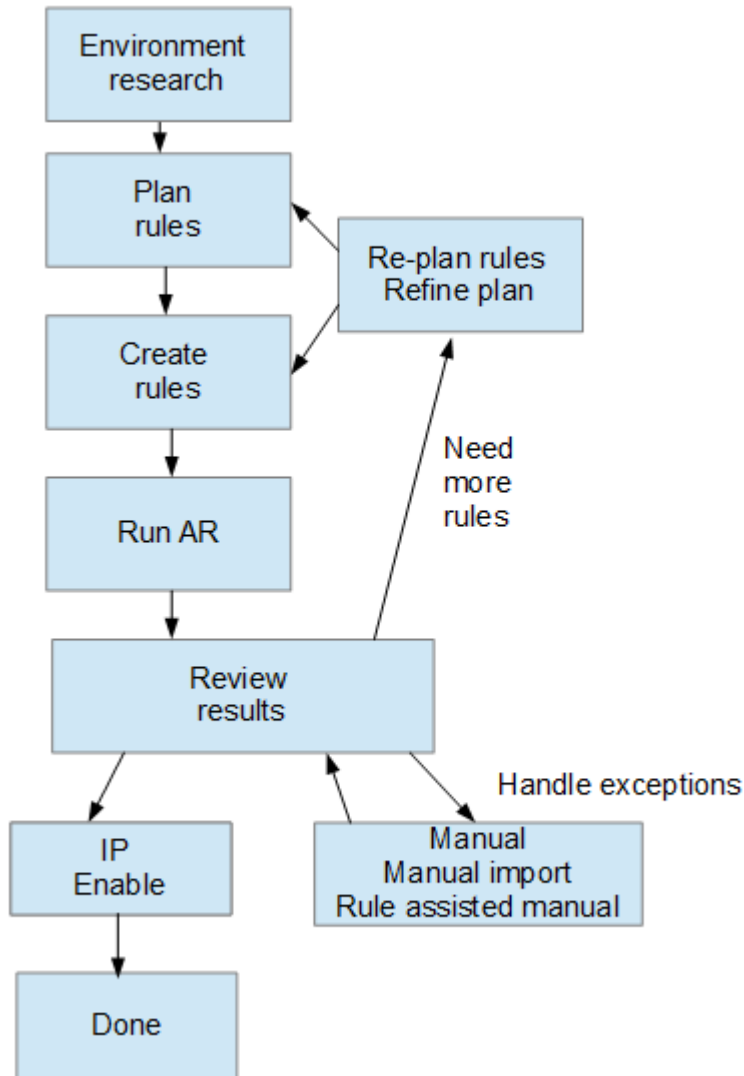


If you have unidentified devices (otherwise known as "unknown" or generic devices) in your environment and you subsequently configure a data source that identifies those devices upon polling, they will no longer be displayed or counted as generic devices.

# Planning device resolution rules for your environment

Using rules to identify devices in your environment is typically an iterative process that requires a thorough analysis of your environment and the creation of multiple rules to identify as many devices as possible. The best case scenario is to set a goal to identify 100% of the devices in your environment.

The most efficient order for rules is to place the most restrictive rules first, resulting in most entries not pattern matching, with the process proceeding to less restrictive rules. This allows Insight to apply more patterns to each entry increasing the possibility of patterns matching and of positive host identification.

When you create rules, your objective should be to create rules that address the largest number of unidentified devices possible. For example, creating rules that follow a pattern of coverage similar to the following is far more efficient that creating 30 rules with lower percentages of coverage:

| Rule | Percentage of coverage |
|---|---|
| Rule 1 | 60% |
| Rule 2 | 25% |
| Rule 3 | 8% |
| Rule 4 | 4% |
| Rule 5 | 1% |

# Creating device resolution rules

You create device resolution rules to identify hosts, storage, and tapes that are not automatically identified currently by OnCommand Insight. The rules that you create identify devices currently in your environment and also identify similar devices as they are added to your environment.

## About this task

When you create rules you start by identifying the source of information that the rule runs against, the method used to extract information, and whether DNS lookup is applied to the results of the rule.

| Source that is used to identify the device |
|---|
| <ul><li>SRM aliases for hosts</li><li>Storage alias containing an embedded host or tape name</li><li>Switch alias containing an embedded host or tape name</li><li>Zone names containing an embedded host name</li></ul> |
| Method that is used to extract the device name from the source |
| <ul><li>As is (extract a name from an SRM)</li><li>Delimiters</li><li>Regular expressions</li></ul> |

| | |
|---|---|
| DNS lookup | |
| Specifies if you use DNS to verify the host name. | |

You create rules in the Auto Resolution Rules tab. The following steps describe the rule creation process.

## Steps

1. Click **Manage** > **Device resolution**

2. In the **Auto resolution rules** tab, click **+Add**

   The New Rule screen is displayed.

   (i) The New Rule screen includes a **?** icon, that provides help and examples for creating regular expressions.

3. In the **Type** list select the device you want to identify.

   You can select Host or Tape.

4. In the **Source** list, select the source you want to use to identify the host.

   Depending on the source you chose, Insight displays the following response:

   ◦ Zones lists the zones and WWN that need to be identified by Insight.

   ◦ SRM lists the unidentified aliases that need to be identified by Insight

   ◦ Storage alias lists storage aliases and WWN that need to be identified by Insight

   ◦ Switch alias lists the switch aliases that need to be identified by Insight

5. In the **Method** list select the method you want to employ to identify the host.

| Source | Method |
|---|---|
| SRM | "As is", "Delimiters", "Regular expressions" |
| Storage alias | "Delimiters", or "Regular expressions" |
| Switch alias | "Delimiters", or "Regular expressions" |
| Zones | "Delimiters", or "Regular expressions" |

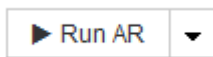   ◦ Rules using "Delimiters" require the delimiters and the minimum length of the host name.

   The minimum length of the host name is number of characters that Insight should use to identify a host. Insight performs DNS lookups only for host names that are this long or longer.

   For rules using Delimiters, the input string is tokenized by the delimiter and a list of host name candidates is created by making several combinations of the adjacent token. The list is then sorted, largest to smallest. For example, for vipsnq03_hba3_emc3_12ep0 the list would result in the following:

- vipsnq03_hba3_emc3_12ep0

- vipsnq03_hba3_emc3

- hba3 emc3_12ep0

- vipsnq03_hba3

- emc3_12ep0

- hba3_emc3

- vipsnq03

- 12ep0

- emc3

- hba3

  ◦ Rules using "Regular expression" require a regular expression, the format, and cases sensitivity selection.
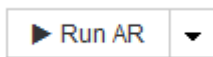
6. Click ![Run AR ▼] to run all rules, or click the down-arrow in the button to run the rule you created (and any other rules that have been created since the last full run of AR.)

## Results

The results of the rule run are displayed in the FC identify tab.

## Starting an automatic device resolution update

A device resolution update commits manual changes that have been added since the last full automatic device resolution run. Running an update can be used to commit and run only the new manual entries made to the device resolution configuration. No full device resolution run is performed.

**Steps**

1. Log into the Insight web UI.

2. Click **Manage** > **Device Resolution**

3. In the **Device resolution** screen, click the down-arrow in the **Run AR** button.

4. Click **Update** to start the update.

## Rule assisted manual identification

This feature is used for special cases where you want to run a specific rule or a list of rules (with or without a one-time reordering) to resolve unknown hosts, storage, and tape devices or group of them.

**Before you begin**

You have a number of devices that have not been identified and you also have multiple rules that successfully identified other devices.

**About this task**

> ⓘ If your source only contains part of a host or device name, use a regular expression rule and format it to add the missing text.

**Steps**

1. Log into the OnCommand Insight web UI.

2. Click **Manage** > **Device resolution**

3. Click the **FC Identify** tab.

   The system displays the identified and unidentified devices.

4. Select multiple unidentified devices.

5. Click **Identify** > **Set host resolution** or **> Set tape resolution**

   The system displays the Identify screen which contains a list of all of the rules that successfully identified devices.

6. Change the order of the rules to an order that meets your needs.

   The order of the rules are changed in the Identify screen, but are not changed globally.

7. Select the method that that meets your needs.

   OnCommand Insight executes the host resolution process in the order in which the methods appear, beginning with those at the top.

   When rules that apply are encountered, rule names are shown in the rules column and identified as manual.

# Fibre Channel device resolution

The FC Identify screen displays the WWN and WWPN of Fibre Channel devices whose hosts have not been identified by automatic device resolution. The screen also displays any devices that have been resolved by manual device resolution.

Devices that have been resolved by manual resolution contain a status of "OK" and identify the rule used to identify the device. Missing devices have a status of "Unidentified". The total coverage for identification of devices is listed on this page.

| ☐▾ | WWN | Port WWN | IP | Name | Type | Status | Rule | |
|---|---|---|---|---|---|---|---|---|
| ☐ | 30:E0:00:00:00:00:00:00 | 10:B0:00:00:00:00:28:20 | 1.1.1.1 | ResolvedHost1 | Host | OK | Hosts by zone | |
| ☐ | 30:E0:00:00:00:00:00:02 | 10:B0:00:00:00:00:28:22 | 2.2.2.2 | ResolvedHost2 | Host | OK | *Rule deleted* | |
| ☐ | 30:E0:00:00:00:00:00:03 | 10:B0:00:00:00:00:28:23 | | | Unknown | Unidentified | | |
| ☐ | 30:E0:00:00:00:00:00:04 | 10:B0:00:00:00:00:28:24 | | | Unknown | Unidentified | | |
| ☐ | 30:E0:00:00:00:00:00:05 | 10:B0:00:00:00:00:28:25 | | | Unknown | Unidentified | | |

+Add  
Total coverage  
**30% (3/10)**

FC identify (10)  
Identify ▾  Unidentify  filter...

Showing 1 to 5 of 10 entries  
< 1 2 >

You perform bulk actions by selecting multiple devices on the left-hand side of the FC identify screen. Actions can be performed on a single device by hovering over a device and selecting the identify or unidentify buttons on the far right of the list.

The Total coverage link displays a list of the "number of devices identified/number of devices available" for your configuration:

- SRM alias
- Storage alias
- Switch alias
- Zones
- User defined

## Adding a Fibre Channel device manually

You can manually add a Fibre Channel device to OnCommand Insight using the manual add feature available in the Device resolution FC Identify tab. This process might be used for pre-identification of a device that is expected to be discovered in the future.

**Before you begin**

To successfully add a device identification to the system you need to know the WWN or IP address and the device name.

**About this task**

You can add a Host, Storage, Tape or Unknown Fibre Channel device manually.

**Steps**

1. Log in to the Insight web UI
2. Click **Manage** > **Device resolution**
3. Click the **FC Identify** tab.
4. Click the add button.

   The Add Device dialog is displayed

5. Enter the WWN or IP address, the device name, and select the device type.

**Results**

The device you enter is added to the list of devices in the FC Identify tab. The "Rule" is identified as Manual.

## Importing Fibre Channel device identification from a CSV file

You can manually import Fibre Channel device identification into OnCommand Insight Device Resolution feature using a list of devices in a CSV file.

**Before you begin**

You must have a correctly formatted CSV file in order to import device identifications directly into the Device Resolution feature. The CSV file for Fibre Channel devices requires the following information:

| WWN |
|-----|
| IP |
| Name |
| Type |

> ⓘ    As a best practice, it is recommended to first export the FC Identify information to a CSV file, make your desired changes in that file, and then import the file back into FC Identify. This ensures that the expected columns are present and in the proper order.

To import FC Identify information:

**Steps**

1. Log into the Insight web UI.
2. Click **Manage** > **Device Resolution**
3. Select the **FC identify** tab.
4. Click **Identify** > **Identify from file**
5.   a. Navigate to the folder containing your CSV files for import and select the desired file.

   The devices you enter are added to the list of devices in the FC Identify tab. The "Rule" is identified as "Manual".

## Exporting Fibre Channel device identifications to a CSV file

You can export existing Fibre Channel device identifications to a CSV file from the OnCommand Insight device resolution feature. You might want to export a device identification so that you can modify it and then import it back into Insight where it is then used to identify devices that are similar to those originally matching the exported identification.

**About this task**

This scenario might be used when devices have similar attributes that can be easily edited in the CSV file and then imported back into the system.

When you export a Fibre Channel device identification to a CSV file, the file contains the following information in the order shown:

| WWN |
|-----|

| | |
|---|---|
| IP | |
| Name | |
| Type | |

**Steps**

1. Log into the Insight web UI.
2. Click **Manage** > **Device Resolution**
3. Select the **FC identify** tab.
4. Select the Fibre Channel device or devices whose identification you want to export.
5. Click the export ⬆ icon.
6. Chose if you want to open the CSV file or save the file.

# IP device resolution

The IP Identify screen displays any iSCSI and CIFS or NFS shares that have been identified by automatic device resolution or by manual device resolution. Unidentified devices are also shown. The screen includes the IP address, Name, Status, iSCSI node, and share name for devices. The percentage of devices that have been successfully identified is also displayed.



## Adding IP devices manually

You can manually add an IP device to OnCommand Insight using the manual add feature available in the IP Identify screen.

**Steps**

1. Log in to the Insight web UI.
2. Click **Manage** > **Device resolution**
3. Click the **IP Identify** tab.
4. Click the add button.

The Add Device dialog is displayed

5. Enter the address, IP address, and a unique device name.

**Results**

The device you enter is added to the list of devices in the IP Identify tab.

## Importing IP device identification from a CSV file

You can manually import IP device identifications into the Device Resolution feature using a list of device identifications in a CSV file.

**Before you begin**

You must have a correctly formatted CSV file in order to import device identifications. The CSV file for IP devices requires the following information:

| Address |
| --- |
| IP |
| Name |

> ⓘ As a best practice, it is recommended to first export the IP Identify information to a CSV file, make your desired changes in that file, and then import the file back into IP Identify. This ensures that the expected columns are present and in the proper order.

To import IP Identify information:

**Steps**

1. Log into the Insight web UI.
2. Click **Manage** > **Device Resolution**
3. Select the **IP identify** tab.
4. Click **Identify** > **Identify from file**
5.   a. Navigate to the folder containing your CSV files for import and select the desired file.

   The devices you enter are added to the list of devices in the IP Identify tab.

## Exporting IP device identification to a CSV file

You can export existing IP device identifications from Insight using the Device Resolution feature. You might want to export a device identification so that you can modify it and then import it back into Insight so that it can be used to identify devices that are similar to those in the exported identification.

**About this task**

When you export an IP device identification to a CSV file, the file contains the following information in the order shown:

| Address |
| --- |
| IP |
| Name |

**Steps**

1. Log into the Insight web UI.
2. Click **Manage** > **Device Resolution**
3. Select the **IP Identify** tab.
4. Select the IP device or devices whose identification you want to export.
5. Click the export ⬆ icon.
6. Chose if you want to open the CSV file or save the file.

# Setting options in the Preferences tab

The device resolution preferences tab lets you create an auto resolution schedule, specify storage and tape venders to include or exclude from identification, and set DNS lookup options.

## Auto resolution schedule

An auto resolution schedule can specify when automatic device resolution is run:

| Option | Description |
| --- | --- |
| Every | Use this option to run automatic device resolution on intervals of days, hours, or minutes. |
| Every day | Use this option to run automatic device resolution daily at a specific time. |
| Manually | Use this option to only run automatic device resolution manually. |
| On every environment change | Use this option to run automatic device resolution whenever there is a change in the environment. |

If you specify manually, nightly automatic device resolution is disabled.

## DNS processing options

DNS processing options allow you to select the following features:

- When DNS lookup result processing is enabled, you can add a list of DNS names to append to resolved devices.
- You can select "Auto resolution of IPs:" to enables automatic host resolution for iSCSI initiators and hosts accessing NFS shares by using DNS lookup. If this is not specified, only FC-based resolution is performed.
- You can choose to allow underscores in host names and to use a "connected to" alias instead of the standard port alias in results.

## Including or excluding specific storage and tape vendors

You can include or exclude specific storage and tape vendors for automatic resolution. You might want to exclude specific vendors if you know, for example, that a specific host will become a legacy host and should be excluded from your new environment. You can also re-add vendors that you earlier excluded but no longer want excluded.

> ⓘ Device resolution rules for tape only work for WWNs where the Vendor for that WWN is set to **Included as Tape only** in the Vendors preferences.

# Regular expression examples

If you have selected the regular expression approach as your source naming strategy, you can use the regular expression examples as guides for your own expressions used in the OnCommand Insight automatic resolution methods.

## Formatting regular expressions

When creating regular expressions for OnCommand Insight automatic resolution, you can configure output format by entering values in a field named `FORMAT`.

The default setting is `\1`, which means that a zone name that matches the regular expression is replaced by the contents of the first variable created by the regular expression. In a regular expression, variable values are created by parenthetical statements. If multiple parenthetical statements occur, the variables are referenced numerically, from left to right. The variables can be used in the output format in any order. Constant text can also be inserted in the output, by adding it to the `FORMAT` field.

For example, you might have the following zone names for this zone naming convention:

```
[Zone number]_[data center]_[hostname]_[device type]_[interface number]
```

- S123_Miami_hostname1_filer_FC1
- S14_Tampa_hostname2_switch_FC4
- S3991_Boston_hostname3_windows2K_FC0
- S44_Raleigh_hostname4_solaris_FC1

And you might want the output to be in the following format:

```
           [hostname]-[data center]-[device type]
```

To do this, you need to capture the host name, data center, and device type fields in variables, and use them in the output. The following regular expression would do this:

```
.*?_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_.*
```

Because there are three sets of parentheses, the variables \1, \2 and \3 would be populated.

You could then use the following format to receive output in your preferred format:

```
\2-\1-\3
```

Your output would be as follows:

```
hostname1-Miami-filer
hostname2-Tampa-switch
hostname3-Boston-windows2K
hostname4-Raleigh-solaris
```

The hyphens between the variables provide an example of constant text that is inserted in the formatted output.

## Example 1 showing zone names

In this example, you use the regular expression to extract a host name from the zone name. You could create a regular expression if you have something similar to the following zone names:

- S0032_myComputer1Name-HBA0
- S0434_myComputer1Name-HBA1
- S0432_myComputer1Name-HBA3

The regular expression that you could use to capture the host name would be:

```
 S[0-9]+_([a-zA-Z0-9]*)[_-]HBA[0-9]
```

The outcome is a match of all zones beginning with S that are followed by any combination of digits , followed by an underscore, the alphanumeric hostname (myComputer1Name), an underscore or hyphen, the capital letters HBA, and a single digit (0-9). The hostname alone is stored in the **\1** variable.

The regular expression can be broken into its components:

- "S" represents the zone name and begins the expression. This matches only an "S" at the beginning of the zone name.

- The characters [0-9] in brackets indicate that what follows "S" must be a digit between 0 and 9, inclusive.
- The + sign indicates that the occurrence of the information in the preceding brackets has to exist 1 or more times.
- The _ (underscore) means that the digits after S must be followed immediately by only an underscore character in the zone name. In this example, the zone naming convention uses the underscore to separate the zone name from the host name.
- After the required underscore, the parentheses indicate that the pattern contained within will be stored in the \1 variable.
- The bracketed characters [a-zA-Z0-9] indicate that the characters being matched are all letters (regardless of case) and numbers.
- The * (asterisk) following the brackets indicates that the bracketed characters occur 0 or more times.
- The bracketed characters [_-] (underscore and dash) indicate that the alphanumeric pattern must be followed by an underscore or a dash.
- The letters HBA in the regular expression indicate that this exact sequence of characters must occur in the zone name.
- The final set of bracketed characters [0-9] match a single digit from 0 through 9, inclusive.

## Example 2

In this example, skip up to the first underscore "", then match E and everything after that up to the second "", and then skip everything after that.

**Zone:** `Z_E2FHDBS01_E1NETAPP`

**Hostname:** `E2FHDBS01`

**RegExp:** `.?(E.?).*?`

## Example 3

The parentheses "( )" around the last section in the Regular Expression (below) identifies which part is the hostname. If you wanted VSAN3 to be the host name, it would be: _([a-zA-Z0-9]).*

**Zone:** `A_VSAN3_SR48KENT_A_CX2578_SPA0`

**Hostname:** `SR48KENT`

**RegExp:** `_[a-zA-Z0-9]+_([a-zA-Z0-9]).*`

## Example 4 showing a more complicated naming pattern

You could create a regular expression if you have something similar to the following zone names:

- myComputerName123-HBA1_Symm1_FA3
- myComputerName123-HBA2_Symm1_FA5
- myComputerName123-HBA3_Symm1_FA7

The regular expression that you could use to capture these would be:

```
([a-zA-Z0-9]*)_.*
```

The `\1` variable would contain only `myComputerName123` after being evaluated by this expression.

The regular expression can be broken into its components:

- The parentheses indicate that the pattern contained within will be stored in the \1 variable.
- The bracketed characters [a-zA-Z0-9] mean that any letter (regardless of case) or digit will match.
- The * (asterisk) following the brackets indicates that the bracketed characters occur 0 or more times.
- The _ (underscore) character in the regular expression means that the zone name must have an underscore immediately following the alphanumeric string matched by the preceding brackets.
- The . (period) matches any character (a wildcard).
- The * (asterisk) indicates that the preceding period wildcard may occur 0 or more times.

  In other words, the combination .* indicates any character, any number of times.

## Example 5 showing zone names without a pattern

You could create a regular expression if you have something similar to the following zone names:

- myComputerName_HBA1_Symm1_FA1
- myComputerName123_HBA1_Symm1_FA1

The regular expression that you could use to capture these would be:

```
(.*?)_.*
```

The \1 variable would contain *myComputerName* (in the first zone name example) or *myComputerName123* (in the second zone name example). This regular expression would thus match everything prior to the first underscore.

The regular expression can be broken into its components:

- The parentheses indicate that the pattern contained within will be stored in the \1 variable.
- The .* (period asterisk) match any character, any number of times.
- The * (asterisk) following the brackets indicates that the bracketed characters occur 0 or more times.
- The ? character makes the match non-greedy. This forces it to stop matching at the first underscore, rather than the last.
- The characters _.* match the first underscore found and all characters that follow it.

## Example 6 showing computer names with a pattern

You could create a regular expression if you have something similar to the following zone names:

- Storage1_Switch1_myComputerName123A_A1_FC1

- Storage2_Switch2_myComputerName123B_A2_FC2
- Storage3_Switch3_myComputerName123T_A3_FC3

The regular expression that you could use to capture these would be:

```
.*?_.*?_([a-zA-Z0-9]*[ABT])_.*
```

Because the zone naming convention has more of a pattern, we could use the above expression, which will match all instances of a hostname (myComputerName in the example) that ends with either an A, a B, or a T, placing that hostname in the \1 variable.

The regular expression can be broken into its components:

- The .* (period asterisk) match any character, any number of times.
- The ? character makes the match non-greedy. This forces it to stop matching at the first underscore, rather than the last.
- The underscore character matches the first underscore in the zone name.
- Thus, the first .*?_ combination matches the characters *Storage1_* in the first zone name example.
- The second .*?_ combination behaves like the first, but matches *Switch1_* in the first zone name example.
- The parentheses indicate that the pattern contained within will be stored in the \1 variable.
- The bracketed characters [a-zA-Z0-9] mean that any letter (regardless of case) or digit will match.
- The * (asterisk) following the brackets indicates that the bracketed characters occur 0 or more times.
- The bracketed characters in the regular expression [ABT] match a single character in the zone name which must be A, B, or T.
- The _ (underscore) following the parentheses indicates that the [ABT] character match must be followed up an underscore.
- The .* (period asterisk) match any character, any number of times.

The result of this would therefore cause the \1 variable to contain any alphanumeric string which:

- was preceded by some number of alphanumeric characters and two underscores
- was followed by an underscore (and then any number of alphanumeric characters)
- had a final character of A, B or T, prior to the third underscore.

## Example 7

**Zone:** myComputerName123_HBA1_Symm1_FA1

**Hostname:** myComputerName123

**RegExp:** ([a-zA-Z0-9]+)_.*

## Example 8

This example finds everything before the first _.

**Zone:** `MyComputerName_HBA1_Symm1_FA1`

`MyComputerName123_HBA1_Symm1_FA1`

**Hostname:** `MyComputerName`

**RegExp:** (.?)_.

## Example 9

This example finds everything after the 1st _ and up to the second _.

**Zone:** `Z_MyComputerName_StorageName`

**Hostname:** `MyComputerName`

**RegExp:** .?(.?).*?

## Example 10

This example extracts "MyComputerName123" from the zone examples.

**Zone:** `Storage1_Switch1_MyComputerName123A_A1_FC1`

`Storage2_Switch2_MyComputerName123B_A2_FC2`

`Storage3_Switch3_MyComputerName123T_A3_FC3`

**Hostname:** `MyComputerName123`

**RegExp:** .?.?([a-zA-Z0-9]+)[ABT]_.

## Example 11

**Zone:** `Storage1_Switch1_MyComputerName123A_A1_FC1`

**Hostname:** `MyComputerName123A`

**RegExp:** .?.?([a-zA-z0-9]+).*?

## Example 12

The ^ (circumflex or caret) **inside square brackets** negates the expression, for example, [^Ff] means anything except uppercase or lowercase F, and [^a-z] means everything except lowercase a to z, and in the case above, anything except the _. The format statement adds in the "-" to the output host name.

**Zone:** `mhs_apps44_d_A_10a0_0429`

**Hostname:** `mhs-apps44-d`

**RegExp:** `([^_])_([AB]).*``Format in OnCommand Insight: `\1-\2 ()_

18

`([^_])_().*`Format in OnCommand Insight: `\1-\2-\3`

## Example 13

In this example, the storage alias is delimited by "\" and the expression needs to use "\\" to define that there are actually "\" being used in the string, and that those are not part of the expression itself.

**Storage Alias:** `\Hosts\E2DOC01C1\E2DOC01N1`

**Hostname:** `E2DOC01N1`

**RegExp:** `\\.?\\.?\\(.*?)`

## Example 14

This example extracts "PD-RV-W-AD-2" from the zone examples.

**Zone:** `PD_D-PD-RV-W-AD-2_01`

**Hostname:** `PD-RV-W-AD-2`

**RegExp:** `[^-]-(.-\d+).+`

## Example 15

The format setting in this case adds the "US-BV-" to the hostname.

**Zone:** `SRV_USBVM11_F1`

**Hostname:** `US-BV-M11`

**RegExp:** `SRV_USBV([A-Za-z0-9]+)_F[12]`

**Format:** `US-BV-\1`