

UltraDNS Traffic Management User Guide

Customer Guide

Version 1.4 (January 2026)

Find more information at:

vercara.digicert.com

Call USA: +1 (844) 929 - 0808

Call EMEA: +44 808 175 1189

Table of Contents

- Introduction 1**
 - Documentation Conventions 1
- Web Forwarding..... 2**
 - HTTPS Web Forwards with Certificate Management 2
 - HTTPS Web Forwards with UltraDNS Automated Certificates 2
 - Certificate Management 4
 - Automated Certificate Management 6
- SiteBacker Pool 8**
 - Creating a SiteBacker Pool 8
 - Viewing/Editing a SiteBacker Pool..... 9
 - Pool Information..... 9
 - Records List..... 12
 - Probe Types and Definitions 15
 - Scheduled Events 22
 - Notifications 23
 - Alerts 24
 - Data Flow 25
- Traffic Controller Pool..... 29**
 - Creating a Traffic Controller Pool..... 29
 - Viewing/Editing a Traffic Controller Pool 30
 - Pool Information..... 30
 - Records List..... 32
 - Probe Definitions 34
 - Scheduled Events 34
 - Notifications 34
 - Alerts 34

- Data Flow 34
- Sub-pools 35
- Simple Load Balancing Pool 37**
 - Creating a Simple Load Balancing Pool..... 37
 - Viewing/Editing a Simple Load Balancing Pool 38
- Directional Pool 43**
 - Configuration Tips and Rules 43
 - Creating a Directional Pool 43
 - Conflict Resolves To 44
 - Editing a Directional Pool..... 45
 - Add a Record - Geolocation 46
- Simple Monitor / Failover Pool 51**
 - Creating a Simple Monitor/Failover Pool..... 51
 - Editing a Simple Monitor/Failover Pool 52
 - Probe Definition 53
- Resource Distribution Pool 56**
 - Creating a Resource Distribution Pool 56
 - Editing a Resource Distribution Pool 57

Introduction

The UltraDNS Managed Services Portal offers several different advanced Traffic Management solutions to meet your various managed Authoritative DNS needs.

- **Web Forwarding** - Redirect HTTP or Email traffic from one target to another.
- **SiteBacker Pool** - A monitoring and failover service to avoid disruptions of a failed server.
- **Traffic Controller Pool** - Define and manage load balancing configurations to modify weighted traffic away from unresponsive servers.
- **Simple Load Balancing Pool** - Provides basic monitoring for inactivity and allows the use of a backup record to be used in place of an inactive response being returned.
- **Directional Pool** - Provide origin-based routing and the ability to optimize traffic flow of various types of DNS requests based upon the location or source IP address of a site visitor.
- **Simple Monitor / Failover Pool** - Provides a monitor that tracks if a website is available or unreachable and alerts the customer of the unavailability via email notifications.
- **Resource Distribution Pool** - Enables the grouping of IPv4 or IPv6 addresses that you can specify the manner or order in which they respond to queries.

Documentation Conventions

To better assist you in utilizing this user guide to its fullest extent, and to provide an easier navigation experience, please review the following documentation conventions.

- Content that appears in **orange is a hyperlink** to a section in the user guide.
- Content that appears in **blue is a hyperlink** to another location on the internet.
- Content that appears in **bold** in a step-by-step order of operations indicates an object you will click on or select. For example:

1. On the **Tools** menu, click **Options**, and then open the **View** tab.

2. Select the **Bookmarks** checkbox.

- Content that is *italicized* refers to a previously provided definition in the document.
- A Light Bulb it indicates a helpful or important note to pay attention to.
- A warning or hazard image stipulates a restriction or warning.

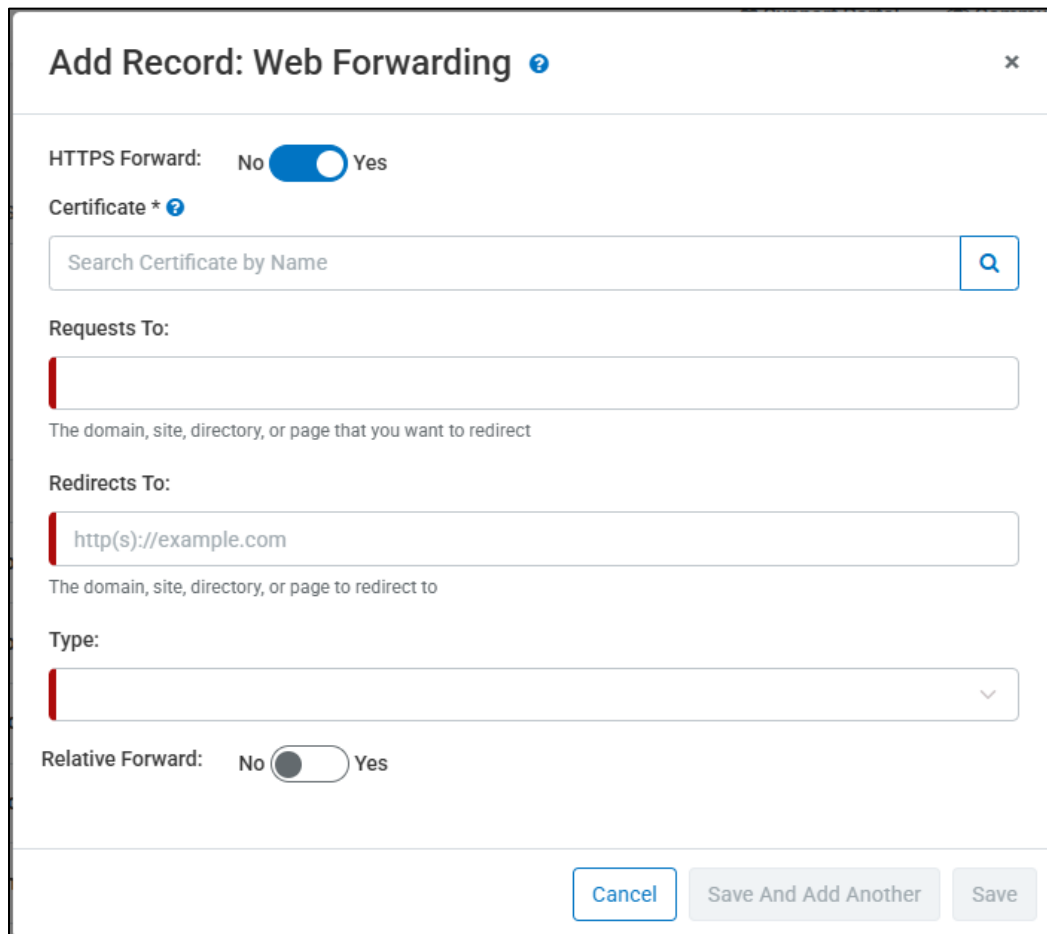


Web Forwarding

A Web Forward (Forwarding) record is used to redirect queries from a domain to another site. With web forwarding, you can register misspellings, alternate extensions (e.g., .biz, .net, etc.) and / or abbreviations, and then forward them to your primary website.

HTTPS Web Forwards with Certificate Management

UltraDNS supports both HTTP and HTTPS forwarding. Historically, HTTPS forwarding has not been supported. However, if the [Certificate Management](#) feature is enabled on your account, you can now create HTTPS Web Forward records by uploading your TLS/SSL certificates, and then applying them to your Web Forwards records.



The screenshot shows a web form titled "Add Record: Web Forwarding" with a close button (X) in the top right corner. The form contains the following fields and controls:

- HTTPS Forward:** A toggle switch currently set to "Yes".
- Certificate *** with a help icon (?): A text input field with the placeholder "Search Certificate by Name" and a search icon (Q) on the right.
- Requests To:** A text input field with a red vertical bar on the left. Below it is the text: "The domain, site, directory, or page that you want to redirect".
- Redirects To:** A text input field containing "http(s)://example.com" with a red vertical bar on the left. Below it is the text: "The domain, site, directory, or page to redirect to".
- Type:** A dropdown menu with a red vertical bar on the left and a downward arrow on the right.
- Relative Forward:** A toggle switch currently set to "No".

At the bottom right of the form are three buttons: "Cancel", "Save And Add Another", and "Save".

HTTPS Web Forwards with UltraDNS Automated Certificates

As an alternative to manually providing and maintaining certificates, customers can choose to enable our Managed Certificate feature, which issues an Encrypted Everywhere certificate for

HTTPS Web Forwarding that provides a fully managed and automated certificate experience. All certificates and key materials are handled within a secure, access-controlled environment.

Utilizing our integration with the DigiCert CertCentral service, we handle the issuance, deployment, and renewal of your certificates, and creating the necessary CAA and DNS-based Domain Control Validation (DCV) TXT records.

To enable this feature on your account, reach out to our Customer Support team. Additional details about Automated Certificate Management can be found [here](#).

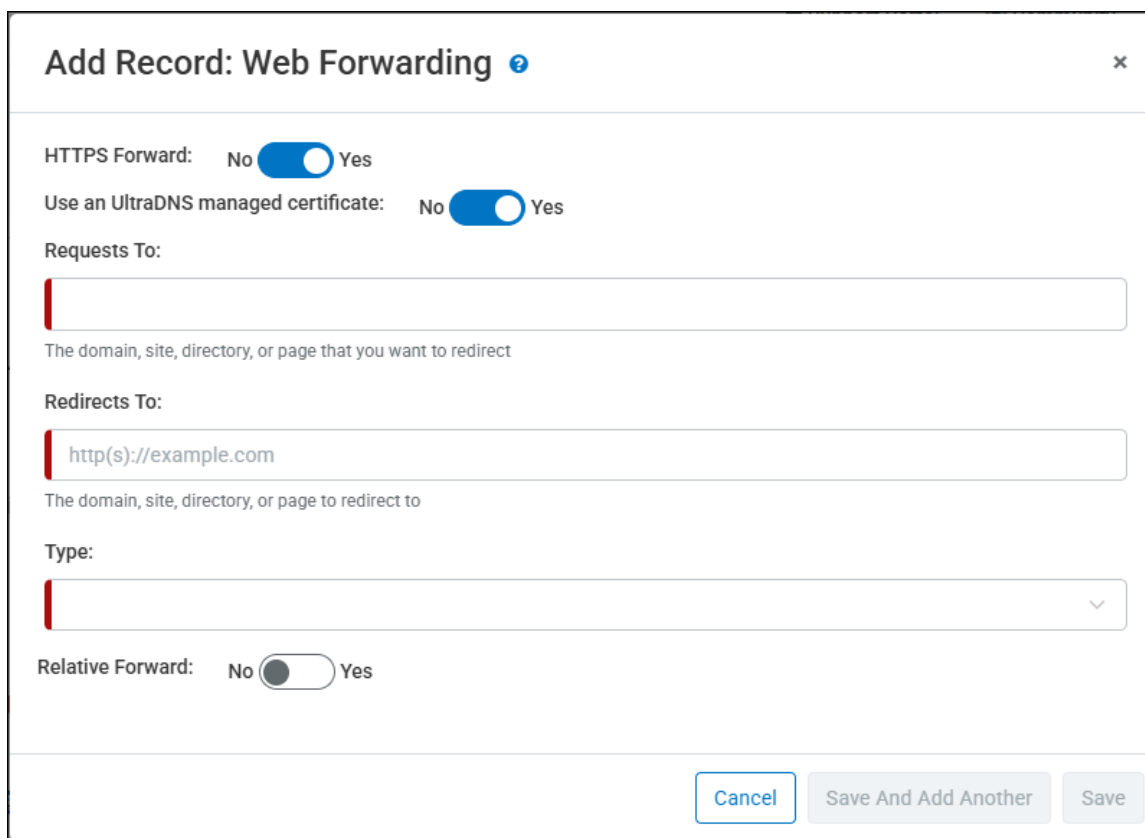
The Web Forwarding record is comprised of the following fields:

- **HTTPS Forward** - Enabling this feature allows you to apply a Certificate to your HTTPS Forward to ensure secure, reliable, and efficient redirection of web traffic.
 - If HTTPS Forward is enabled, search for your certificate and select it from the drop-down menu. Your list of certificates can be found on the [Certificate Management](#) page.
 - If HTTPS Forward is enabled, and the [Automated Certificate Management](#) service is enabled, you can select the Use an UltraDNS Managed Certificate option to have UltraDNS and DigiCert create, maintain, and renew a certificate to validate the HTTPS forwards.
- **Requests To** – The domain, site, directory, or page that you want to redirect. This field can be left blank, and will by default, use your zone/domain name.
 - You can use the wildcard character (*) in the string. Using a wildcard on a redirection record tells the server to match the most specific string and then append any unmatched portion of the source URL to the target URL.
- **Redirects To** – The location that you want to redirect to. This can be a domain, site, directory, or a page.
 - You can use the wildcard character * (asterisk) in this field as well.
- **Type** – Select a redirect type from the drop-down menu.
 - **301 Redirect** - Permanent Redirect
 - **302 Redirect** - Found (unspecified reason redirect)
 - **303 Redirect** - See Other
 - **307 Redirect** - Temporary Redirect
 - **Framed** - Creates an invisible frame set and loads the destination URL in the frame, thus making it more difficult to determine that a redirection has occurred. The disadvantage to this approach is that any bookmarks created by the user while navigating the site will point to the home page of the original URL.
- **Relative Forward** – When enabled, appends a portion of the incoming URL to the Redirects To URL provided by using one of the following options:
 - **Path** – The incoming Parameter will be discarded.
 - **Parameter** – The incoming Path will be discarded.
 - **Parameter & Path (Both)** - Both the Path and Parameter are both appended appropriately.

The following example demonstrates how each Relative Forwarding Type works.

If your **Requests To** field is `www.foo.biz/documents?a=userguide#supp`, and your **Redirects To** field is `www.foo.biz/support?c=sales#home`, then:

- **Path** will append the response to - `www.foo.biz/documents/support?a=userguide#supp`. The Path /Support is appended to the Requests To /documents. The incoming parameter is removed.
- **Parameter** will append the response to - `www.foo.biz/documents?a=userguide&c=Sales#supp`. The incoming path is removed.
- **Parameter and Path** will append the response to - `www.foo.biz/documents/support?a=userguide&c=sales#supp`. The incoming parameter AND path are both appended.



Add Record: Web Forwarding ⓘ

HTTPS Forward: No ☒ Yes

Use an UltraDNS managed certificate: No ☒ Yes

Requests To:

The domain, site, directory, or page that you want to redirect

Redirects To:

The domain, site, directory, or page to redirect to

Type:

Relative Forward: No ☐ Yes ☒

[Cancel](#) [Save And Add Another](#) [Save](#)

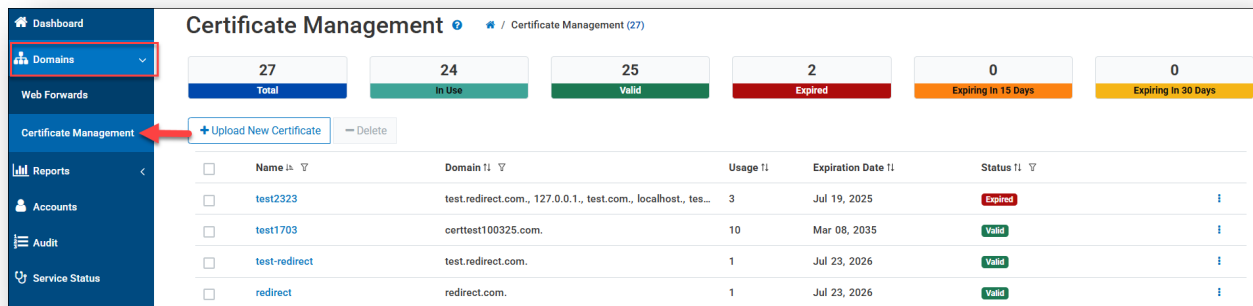
Certificate Management

The **Certificate Management** dashboard displays the list of TLS/SSL Certificates that have been uploaded for the account. These Certificates can be applied to HTTPS Redirects (Web Forward records) to ensure secure, reliable, and efficient redirection of web traffic.

A banner across the top of the page displays a quick overview of your uploaded Certificates:

- total Certificates uploaded

- total number of Certificates in use
- total number of valid Certificates
- total number of expired Certificates
- total number of Certificates expiring within 15 days
- total number of Certificates expiring within 30 days



	27	24	25	2	0	0
	Total	In Use	Valid	Expired	Expiring in 15 Days	Expiring in 30 Days
+ Upload New Certificate - Delete						
	Name	Domain	Usage	Expiration Date	Status	
☐	test2323	test.redirect.com., 127.0.0.1., test.com., localhost., tes...	3	Jul 19, 2025	Expired	ⓘ
☐	test1703	certtest100325.com.	10	Mar 08, 2035	Valid	ⓘ
☐	test-redirect	test.redirect.com.	1	Jul 23, 2026	Valid	ⓘ
☐	redirect	redirect.com.	1	Jul 23, 2026	Valid	ⓘ

The **Upload New Certificate** option allows you to create a Certificate, which requires Certificate and Private Key files to be uploaded, and the optional CABUNDLE file in one of the following supported formats: **.pem .key .crt** or **.cer**.

Each Certificate uploaded displays the following details on the Certificate Management page:

- **Name** - The Certificate name provided during the creation of the Certificate.
- **Domain** - The list of domains utilizing the Certificate.
- **Usage** - The current number of records that this Certificate is being applied to.
- **Expiration Date** - The exact date in which the Certificate expires and is no longer be valid.
- **Status** - Indicates the Certificate being Expired or still Valid.
- **Additional Options** - Clicking the ⓘ icon displays the following actions:
 - **Activate** the Certificate - applies the Certificate to a Web Forwards record.
 - **Renew** an expired Certificate - provide new Certificate files for an expired Certificate.
 - **Replace** the Certificate - provide new Certificate files for an existing Certificate.
 - **Delete** the Certificate.

Your Certificates can be applied to a Web Forwards record when selecting the **HTTPS Forward** option.

Automated Certificate Management

As an alternative to manually providing and maintaining certificates, customers can choose to enable our Managed Certificate feature, which issues an Encrypted Everywhere certificate for HTTPS Web Forwarding that provides a fully managed and automated certificate experience.

Utilizing our integration with the DigiCert CertCentral service, we handle the issuance, deployment, and renewal of your certificates, and creating the necessary CAA and DNS-based Domain Control Validation (DCV) TXT records.

To enable this feature on your account, use the **Contact Us** page to reach out to our Customer Support team. Additional details about Automated Certificate Management can be found [here](#).

Records Properties DNSSEC Zone Transfer Snapshot Health Dangling DNS Records						
Add Record ▾		Add Pool ▾		Bulk Import		Show Grouped View
Search Records		Filter on Type: All Records/Pools ▾		Export		
☐	Record Type ↑↓ ▾	Host ↑↓ ▾	Details	TTL ▾	Actions	
☐	A	2020.askform.co.	Points To : 204.74.99.200	300		
☐	A	2024.askform.co.	Points To : 204.74.99.200	300		
☐	A	askform.co.	Points To : 204.74.99.200	300		
☐	AAAA	2020.askform.co.	Points To : 2610:a1:3094:0:0:0:210	300		
☐	AAAA	2024.askform.co.	Points To : 2610:a1:3094:0:0:0:210	300		
☐	AAAA	askform.co.	Points To : 2610:a1:3094:0:0:0:210	300		
☐	NS	askform.co.	Name Server : ns4.ultradns2.com.	301		
☐	NS	askform.co.	Name Server : ns4.ultradns2.org.	301		
☐	NS	askform.co.	Name Server : udnst1.ultradns.net.	301		
☐	NS	askform.co.	Name Server : udnst2.ultradns.net.	301		
☐	TXT	_dnsauth.askform.co.	Comments : _2m679bziss6vmh2vf1kp19s25a7mk5	60		
☐	CAA	askform.co.	Flags : 0 Property Tag : issue Property Value : digicert.com	301		
☐	CAA	askform.co.	Flags : 0 Property Tag : issuewild Property Value : digicert.com	301		
☐	WEBFORWARD	https://2020.askform.co	Managed by : UltraDNS Certificate Name : Auto-provisioned by UltraDNS Default Forward Type : 301 Redirect Default Redirect To : https://2021.askform.co Days to Expiration : 58 HTTPS Forward : Enabled			

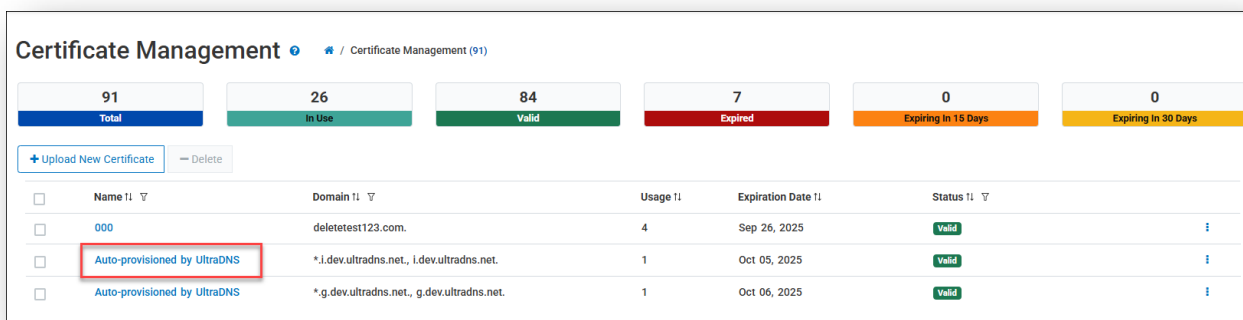
Key Benefits

- HTTPS 301/302 Redirects: works with path and query strings preserved, supporting permanent and

temporary HTTP status codes.

- Wildcard Domain Support: Works across subdomains with one certificate.
- Certificates are automatically renewed 7 days before the expiration date.
- Perfect for protecting all your domains—even those not hosting active sites—with automated, secure redirects.
- Securely redirect old domains during rebrands, M&A, or product launches without needing to manage certificates.

For accounts utilizing the automated Managed Certificate feature, Name column on the Certificate Management page displays the certificate name as Auto-provisioned by UltraDNS. After initial creation, the status may display Pending for several minutes as the certificate is validated, before displaying Valid.



91 Total	26 In Use	84 Valid	7 Expired	0 Expiring in 15 Days	0 Expiring in 30 Days
+ Upload New Certificate - Delete					
☐	Name	Domain	Usage	Expiration Date	Status
☐	000	deletetest123.com.	4	Sep 26, 2025	Valid
☐	Auto-provisioned by UltraDNS	*i.dev.ultradns.net., i.dev.ultradns.net.	1	Oct 05, 2025	Valid
☐	Auto-provisioned by UltraDNS	*g.dev.ultradns.net., g.dev.ultradns.net.	1	Oct 06, 2025	Valid

SiteBacker Pool

A SiteBacker (SB) pool is a grouping of A or CNAME records that monitors your servers and redirects traffic to a host standby in case of server failure.

	With the addition of the Backup Method feature, existing SiteBacker pools will have the following applied: ▪ Pools with All-Fail records default to Backup Response. ▪ Pools without All-Fail records default to Fail Close. Newly created SiteBacker pools default to Backup Response unless an All-Fail record is created, and then by default, switch to Fail Close.
---	---

Creating a SiteBacker Pool

1. Select either an A or AAAA record type, and then click the **+Add Pool** button.
2. Select **SiteBacker (SB)** from the **Select Pool Type** drop-down menu.
3. Provide the **Host** and the **Points To** fields.
4. Click **Save** when finished.

Add Pool Record: A (Address - IPv4) ?

Host:

A valid hostname

Record Type:

A

Points To:

A valid IPv4 address

TTL:

Time to live, in seconds

Select Pool Type

Sitebacker (SB)

Resource Distribution (RD)

Sitebacker (SB)

Traffic Controller (TC)

Simple Load Balancing (SLB)

Simple Monitor/Failover (SF)

Directional (DIR)

Cancel

Save

203.2.3.192
204.74.99.100



A SiteBacker pool cannot contain both A and AAAA records. Individual pools will need to be created to support each of these 2 record types.

Viewing/Editing a SiteBacker Pool

SiteBacker (SB) pools consists of various tabs of available functions and details that beyond just displaying associated records. So, when editing a SiteBacker pool, there are multiple sections that you can edit.

Pool Information

The following record and pool details are displayed in the Pool Information section. Click **Save** after you make any changes.

- **Description** – Defaults to the pool name. The description can be a maximum of 255 characters.
- **Pool Type** – Displays if the pool is a SiteBacker pool, or a Traffic Controller pool.
- **Failover** – Select **Enabled** if you want to enable a failover record or **Disabled** if you want only the

primary record being served.

- **Backup Method** - Determines how UltraDNS responds when all primary records in a SiteBacker pool fail health checks. The possible Backup Methods are:
 - **Fail Closed** - Stops responding if all primary records fail and returns an empty DNS response. This is the default Backup Method for new SB pool.
 - i. *This option prioritizes correctness over availability.*
 - **Backup Response** - Uses an All Fail backup record when all primary records fail, so queries still get an answer. This ensures DNS continues to return an answer during full failure scenarios.
 - This method is only available if a pool contains a configured backup (All-Fail) record.
 - **Fail Open** - Continues serving original records even if all health checks fail, ignoring probe status.
 - This option prioritizes availability and traffic continuity.
 - This method is not available if a pool contains a configured backup (All-Fail) record.
- **Probing** – When probing is **Enabled**, a probe can be sent to verify that a URL can be reached, and that the record can be served.
 - Probing cannot be set to **Disabled** unless Failover is set to **Disabled**.
- **Response Method** – Determines the order in which records are returned.
 - **Round Robin** – The records will rotate (in a round robin fashion).
 - **Fixed** – The records will appear in the order in which they are set.
 - **Random** – The records appear in a completely random order.
- **Max Active records** - Specifies the maximum number of active servers in the pool and determines when SiteBacker takes backup servers offline. For example, consider a pool with six servers. Setting **Max Active** to 4 means SiteBacker takes two servers offline and sends the four active records in the answer.
- **Max Served records** - Specifies whether all records are served, or only a specified number.
- **Configured** - Displays the current number of records (including sub-pools) in the pool.
- **Failure Threshold** - Select the number of priority records which indicates the minimum number of records that must fail for a pool to be labeled 'FAILED'. If the number of failed records in the pool is greater than or equal to the 'Failure Threshold' value, the pool will be labeled FAILED.

[Pool Information](#)
[Probe Definitions](#)
[Scheduled Events](#)
[Notifications](#)
[Alerts](#)

Pool status: OK

Description	Pool Type	Failover	Backup Method	Probing	Response Method
www.otebstbtc2902.com.	SITEBACKER	Enabled	Fail Closed	Enabled	Round Robin

Max Active Record	Max Served Record	TTL	Configured	Failure Threshold	Convert	Save
1	1	120	5	All		

Records List [+ Add Record](#) [- Delete Records](#)

☐	Points To	Record Type	Record State	Status	Probing	Priority	Serving
☐	0:0:0:0:0:ffff:d	AAAA	Normal	— N/A	Disabled	1	✓
☐	[Redacted]	AAAA	Normal	— N/A	Enabled	1	
☐	[Redacted]	AAAA	Normal	— N/A	Enabled	1	
☐	[Redacted]	AAAA	Normal	— N/A	Enabled	1	
☐	test.com.	CNAME	Normal	— N/A	Enabled	1	

Backup Method Behavior

The following table demonstrates the SiteBacker/Traffic Controller pool behavior based on the Backup Method selected, and an example pool configuration with, and without, a configured All-Fail record.

Backup Method	Scenario	Behavior
Fail Closed	1.1.1.1 – Priority 1 – Failure 2.2.2.2 – Priority 2 – Failure 3.3.3.3 – All-Fail – N/A	- Nothing is served. - Once all numbered priorities fail, UltraDNS returns an empty DNS answer. - This is the strict, correctness-first behavior. - If backup method is “Fail Closed” and the All-Fail record is provided in the input, then backup method changes to “Backup Response.”
Backup Response (with an All-Fail)	1.1.1.1 – Priority 1 – Failure 2.2.2.2 – Priority 2 – Failure 3.3.3.3 – All-Fail – Configured	- The All-Fail record (3.3.3.3) is served. - Backup Response explicitly activates the All-Fail record(s) once all numbered priorities fail.
Backup Response (without All-Fail)	1.1.1.1 – Priority 1 – Failure 2.2.2.2 – Priority 2 – Failure No All-Fail record	This configuration is not allowed. An All-fail record MUST be configured if backup method is “Backup Response.”
Fail Open	1.1.1.1 – Priority 1 – Failure 2.2.2.2 – Priority 2 – Failure All-Fail – Not Allowed	UltraDNS ignores the probe status entirely and continues serving based on priority order and pool configuration (pool enters Fail Open if all the configured probes

Backup Method	Scenario	Behavior
		are failing). - Top priority records (based on pool configurations like max-active, max-serve) are served, regardless of probe failures. - Fail Open is temporary and reverts automatically as probes recover. <u>All-Fail records are not allowed</u> if the backup method is Fail Open.

Records List

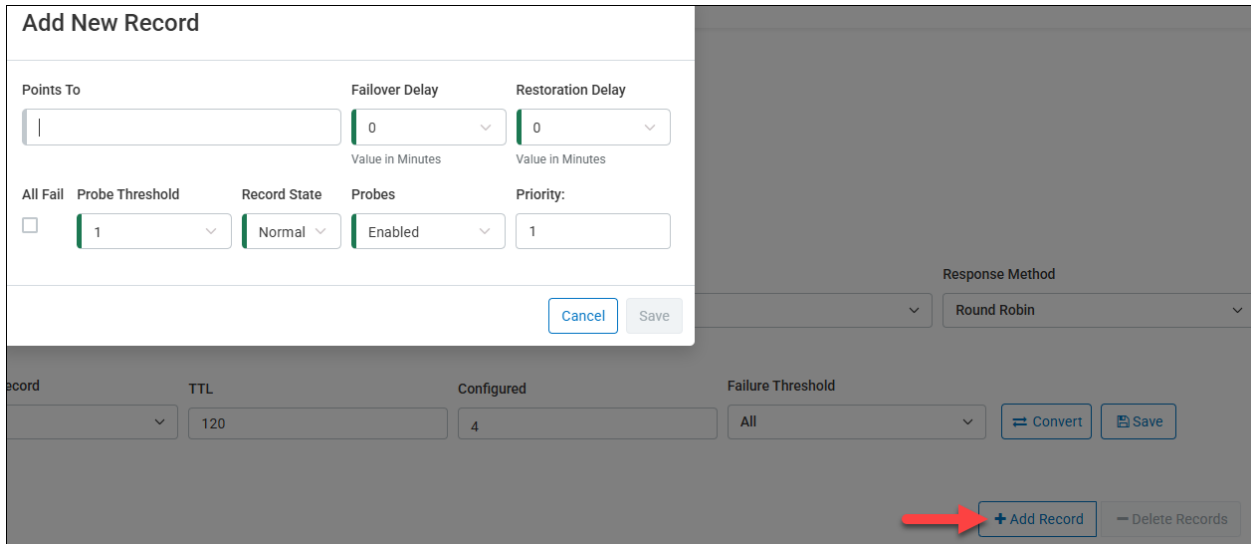
The records list displays all the currently associated records to the SiteBacker pool. From this section, you can Add, Edit, or Delete records from the pool list as needed.

Add a Record

	SiteBacker pool cannot contain both A and AAAA records. Individual pools will need to be created to support each of these two record types.
--	---

To add a new record to your pool:

1. Click the **+Add Record** button.
2. Provide the IP address or hostname for the record in the **Points To** field.
3. Select the **Failover Delay** value from the drop-down menu. The Failover Delay field specifies the time SiteBacker waits after detecting that the pool record has failed before confirming that the record is still in failure and activating secondary records. The default value is 0 minutes.
4. Select the **Restoration Delay** value from the drop-down menu. The Restoration Delay field specifies the time SiteBacker waits after detecting that the failed record—that was failed-over from—is no longer in a failure state and will now failback to. A value of 0 minutes indicates **immediate** failback.
5. Check the box to designate if this record will be a part of the **All Fail** record(s) or not. If selecting an All Fail record, all other fields will be greyed out and not able to be configured.
6. Select the **Probe Threshold** value from the drop-down menu.
7. Select the **Record State** value from the drop-down menu.
8. Choose whether to **Enable** or **Disable** Probes for the record.
9. Provide an integer value for the **Priority** of the record.
10. Click **Save** when you are finished.



Records List

The records list displays the records in a SiteBacker pool with the following details.

- **Points To** - Displays the IPv4 or IPv6 address or hostname for the record.
- **Record Type** - The available record types can include A, AAAA, SB (SiteBacker) / TC (Traffic Controller), or CNAME.
- **Record State** - Indicates how the record should behave.
 - Normal (default) - Indicates that a pool record succeeds and fails with normal behavior (SiteBacker serves records with the highest priority first).
 - Force Fail - Forces a record into a not-served state.
 - Force Active - Forces a record into a served state.
- **Status** - The status of record which can be one of the following:
 - **OK** - The number of records serving is equal to the Max Active value, and all the active records are top priority records. For example, if a pool has a Max Active of 1 and the Priority 1 record is serving, the pool will be marked OK.
 - **WARNING** - The number of records serving is equal to the Max Active value, and the active records are not top priority records. For example, if a pool has a Max Active of 1 and the Priority 1 records is not serving and the Priority 2 record is serving, the pool will be marked WARNING.
 - **CRITICAL** - The number of records serving is less than the Max Active value, or the All Fail record is being served. For example, if a pool has a Max Active of 2, and only one record is serving, the pool will be marked CRITICAL.
 - **FAILED** - No records are serving and there is not an All Fail record configured, or the Failure Threshold has been reached.
 - **N/A** - Indicates that probing has not taken place for the record. This happens if probing is disabled, the probe URL is missing, or the probe is newly configured and has not yet executed.

- **Probing** - Signifies if Probing is enabled for the record or not.
- **Priority** - Displays the priority value for the records, which is used to determine the order in which records are returned via the Response Method.
- **Serving** - Signifies if the record is Available to Serve or not (meaning if a probe was successful or not). A check mark indicates that serving is available, while an X indicates it is not.

Records List 								+ Add Record	- Delete Records
☐		Points To	Record Type	Record State	Status	Probing	Priority	Serving	
☐		1.1.1.1	A	Normal	N/A	Enabled	1		
☐		8.8.4.4	A	Normal	N/A	Enabled	1		
☐		8.8.8.8	A	Normal	N/A	Enabled	1		
☐		1.2.32.3	A	Normal	N/A	Enabled	All Fail		

Probes

The Probes list includes Enabled (the default) or Disabled state.

Tip: Combinations of the Record State and Probes states produce the following results:

- **Record State Force Active + Probes Enabled** = forces a record into a served state and probes the record, but does not act on the results.
- **Record State Force Active + Probes Disabled** = forces a record into a served state and does not probe the record.
- **Record State Force Fail + Probes Enabled** = forces a record into a not-served state and probes the record, but does not act on the results.
- **Record State Force Fail + Probes Disabled** = forces a record into a not-served state and does not probe the record.

Probe Definitions

There are 2 types of probes:

- **Pool Level** - These probe types probe all records in a pool.
- **Record Level** - These probe types probe only a specific record.

Within these 2 types of probes are probe classes: HTTP/HTTPS, PING, FTP, TCP, SMTP, DNS, PROXY.

	For SiteBacker pools containing AAAA records, only TCP, HTTP, and DNS probe types are supported.
---	--

×

Add New Probe

Probe Type

HTTP ▾

Select Host

Pool Level ▾

Select Probing Regions ⓘ

Select Agent Regions

Region Threshold ⓘ

▾

Probe Interval

15 Minutes ▾

Select at least two Regions

HTTP Headers ⓘ

Delete Selected

☐ Headers

Add Header Key

:

Add Header Value

Add

Maximum 5 headers can be added

Press Enter to add multiple header values

HTTP Probe Transactions

+ Add

– Delete

☐

URL

Version

Method

Transmitted Data

Follow Redirect

Cancel

Save Probe

Create a Probe

1. Click the **+Add Probe** button.
2. Select the **Probe Type** (class) from the drop-down menu.
3. Select the **Host** type, which can either be Pool, or a specific record within your pool.
4. Click in the **Select Regions** box to select a maximum of four regions to possibly probe from.
5. Select the **Region Threshold** value from the drop-down menu. This will determine how many probe failures are required before a failover occurs.
6. Select the **Probe Interval** value from the drop-down menu. This will determine how often a probe runs.
7. Provide the specific details required for the probe type selected.
8. Click the **Save Probe** button when you are finished.

Probe Types and Definitions

All probes require a Probe Interval (30 seconds or 1-15 minutes) and an Agent Threshold. The

Agent Threshold is the number of agents running the probe that must fail for SiteBacker/Traffic Controller to consider the probe failed. Records also have thresholds to determine the number of probes that must fail for SiteBacker/Traffic Controller to indicate the failure and possibly take further action.

Probe Values

HTTP Probe	Minimum value	Maximum value
Total Run Time (seconds)	0	60
Run Time (seconds)	0	60
Connect Time (seconds)	0	20
Ping Probe	Minimum value	Maximum value
Round Trip Time (ms)	0	20000
Run Time (seconds)	0	60
FTP Probe	Minimum value	Maximum value
Connect Time (Seconds)	0	20
Run Time (Seconds)	0	60
DNS	Minimum value	Maximum value
Run Time (seconds)	0	30
TCP	Minimum value	Maximum value
Connect Time	0	20
SMTP Availability	Minimum value	Maximum value
Connect Time (Seconds)	0	20
Run Time (Seconds)	0	60
SMTP Sendmail	Minimum value	Maximum value
Connect Time (Seconds)	0	20
Run Time (Seconds)	0	60

HTTP/HTTPS

- The HTTP probe verifies an HTTP service by making a request to a web server and testing the response. Any status code in a response other than a number in the 200's (including 301 - Moved Permanently) will fail a probe, regardless of a specified search string.
- The HTTP probe requires Port (typically 80 for HTTP and 443 for HTTPS), Host name, Web page, Protocol (HTTP or HTTPS), and Method (GET or POST). The Transmitted Data field applies to the POST method only.
- If Follow Redirects is set to Yes (default is No), and you have configured Web Forwarding redirection, then SiteBacker will follow the redirection with these restrictions:
- For DNS-level and web server-level redirects, SiteBacker will follow 300, 301, 302, and 307 redirect codes.

- For DNS-level and web server-level redirects, SiteBacker will not follow HTTP 303, 304, 305, and 306 redirect codes.
- If IP addresses are pool records in a Load Balancing pool, and the domain name is the hostname for the Load Balancing pool, SiteBacker will not recognize the DNS-level redirect; however, if the domain name is a CNAME pool record, SiteBacker will recognize the DNS-level redirect.
- If the domain name (example.com) is a CNAME pool record in a Load Balancing pool, redirects from example.com/pageA.html to example.com/pageB.html will not work, and the HTTP probe will fail.
- If a non-apex level host name (hostname.example.com) is configured as a CNAME pool record in a Load Balancing pool, then a redirect to another host name will not work and the HTTP probe will fail.

Ping

- The ping probe determines if a host is reachable across the network via the ICMP echo request/reply protocol (also known as ping).
- The ping probe requires Number of packets (defaults to 3) and Size of packets (does not include the IP and ICMP headers and defaults to 56 bytes).
- **Not supported if the SiteBacker pool contains AAAA records.**

FTP

- The FTP probe verifies an FTP service. This probe requires Port (typically 21), Passive Mode (if Yes, initiates both connections to the FTP server), and Path to file (for example, /pub/testfile).
- You can also specify a username and password, if required by your FTP service.
- **Not supported if the SiteBacker pool contains AAAA records.**

TCP

- The TCP probe attempts connection to a specified port (Port is the only required field). If you specify a Control IP Address, you can provide a control mechanism that allows the web administrators to stop the TCP port on the control system and thus cause a failover of resources to backup resources.

SMTP Availability and SMTP Send Mail

- The SMTP probes test a mail server.
- SMTP Availability requires the Port (default 25), Connect time, and Run time.
- SMTP Send Mail requires the Port (default 25), Mail From Address, Mail To Address, Connect time and Run time.
- **Not supported if the SiteBacker pool contains AAAA records.**

DNS

- A DNS probe verifies a DNS service. This probe requires two fields: Port (defaults to 53) and TCP only (defaults to No, which means that the probe uses UDP first, and then TCP if the UDP fails; Yes,

skips UDP and just uses TCP). If you set the Resource Record type to NULL and leave the Name to query blank, the application sends a bogus A record query and expects a name error in response, thus verifying the DNS service. You can complete these fields with valid data for your site.

- If you select a record in the Resource Record type list and leave Name to query blank, the DNS probe ensures the query returns a properly formatted response.
- If you select a record in the Resource Record type list and complete the Name to query, the DNS probe ensures the appropriate record responds to the query. The Resource Record Type AXFR tests if an AXFR (complete zone transfer) is completed successfully. AXFR ignores the Response field.

Proxy

- The proxy probe connects to a proxy server and has it request the specified URL.
- The proxy probe requires the URL and Port.
- **Not supported if the SiteBacker pool contains AAAA records.**

Configuring HTTP Probe Headers

Configuring the HTTP Probe Headers allows you to tailor monitoring and test server configurations for accurate results, and mimic realistic traffic to improve monitoring accuracy. Probe Headers consist of a **key:value** pair, and each Probe can only consist of 5 configured headers.

Use the [List of HTTP Header Fields](#) link to view the various types of Probe Headers that are available.

Known Issues and Limitations

HTTP/1

For HTTP/1 multi-valued probe headers, the list of values will be sent as `"key": ["val1", "val2"]`. We are aware that some servers may expect the values to be sent as a string resembling `"key": "val1, val2"`. In these instances, the probe header can be configured as a single value, such as: `"key": ["val1, val2"]`.

If a server expects the values to be sent as `"key": "val1"` and `"key": "val2"`, the probe may fail because a single header is being sent with multiple values.

HTTP/2

For HTTP/2 multi-valued probe headers, the list of values will be sent as `"key": "val1"` `"key": "val2"`. We are aware that some servers may expect the values to be sent as a string resembling `"key": "val1, val2"`. In these instances, the probe header can be configured as a single value, such as: `"key": ["val1, val2"]`.

Restrictions

The following restrictions apply to the design and length of the HTTP Probe Headers:

- Duplicate Key values are not allowed.
- Each header Key length cannot exceed 50 characters.
- Each header Value length cannot exceed 512 characters.
- Each total header length (Key + Value) cannot exceed 562 characters.
- The total character length of all 5 headers cannot exceed 2810 characters.
- The Key value only supports alphanumeric characters, hyphens (-), and underscores (_).

The following Header types are not allowed due to potential conflicts with protocol-level operations and/or security concerns:

- **Host**
- **Connection**
- **Content-Length**
- **Cookie**
- **:method**
- **:authority**
- **:scheme**
- **:path**

When configuring an HTTP Probe Header:

1. Provide the **Header Key**. Header keys are not case sensitive.
2. Provide the **Header Value**.
3. Press the Enter key to add multiple header-values to the Key.
4. Click the **Add** button to apply the indicated Key:Value pair.

Add New Probe ✕

Probe Type

HTTP ▾

Select Host

Pool Level ▾

Select Probing Regions ⓘ

Select Agent Regions

Select at least two Regions

Region Threshold ⓘ

▾

Probe Interval

15 Minutes ▾

HTTP Headers ⓘ Delete Selected

☐	Headers	
☐	Content	test, test1
☐	Authorization	Test2, Test34, Test13 www.test.com

Add Header Key

:

Add Header Value

Add

Maximum 5 headers can be added

Press Enter to add multiple header values

- Add up to a maximum of 5 Key:Value pairs for the HTTP Probe.
- Configure your **HTTP Probe Transactions**, and then click **Save Probe**.

HTTP Probe Transactions

Configuring an HTTP Probe Transaction allows you to configure and customize specific probing attributes and expected results for your Probe.

The HTTP Probe Transaction consists of the following fields.

- **URL** – The URL that is being probed. You can select the **Validate URL** button to ensure the URL you are attempting to probe is a valid URL that can be reached.
- **Version** – The HTTP Method version number for the server.
 - HTTP/1
 - HTTP/1.1
 - HTTP/2
- **Method** – The type of method to determine the results of the Probe Transaction.
 - GET
 - POST

- **Transmitted Data** - Allows you to provide specific details to be included with the Probe details.
- **Follow Redirect** - Indicating Yes or No will determine if the Probe will continue to the redirected URL (if there is one), or return the results based upon the URL initially indicated.
- **Expected HTTP Response** - Select from the dropdown menu the response type that is expected to be returned by the probe when returned.
- **Advanced Options** – Selecting the Advanced Option will allow you to provide a custom HTTP code, or multiple codes.
- **Probe Fail Specifications** – The Probe Fail Specifications allow you to configure various custom parameters for the probe, which include run duration time, and search string parameters.



HTTP probes will only correctly work if the indicated server supports the configured HTTP protocol version, otherwise the probe will fail. Meaning, if your server is not configured for HTTP/2, and you have indicated HTTP/2 as the Protocol Version, the probe will fail.

Add New Probe

HTTP Probe Transaction ?

Probe Fail Definitions

URL	Version	Method	Transmitted Data
http(s)://www.example.com/	HTTP/1.0	GET	
Validate URL			

Follow Redirect

Expected HTTP Response

☐ Advanced Option

Probe Fail Specifications

	Fail
Total Run Time	
Connect Time	20
Run Time	60
Search String	

Once you have configured a Probe Transaction, click the **Done** button to add it to the Probe.

Scheduled Events

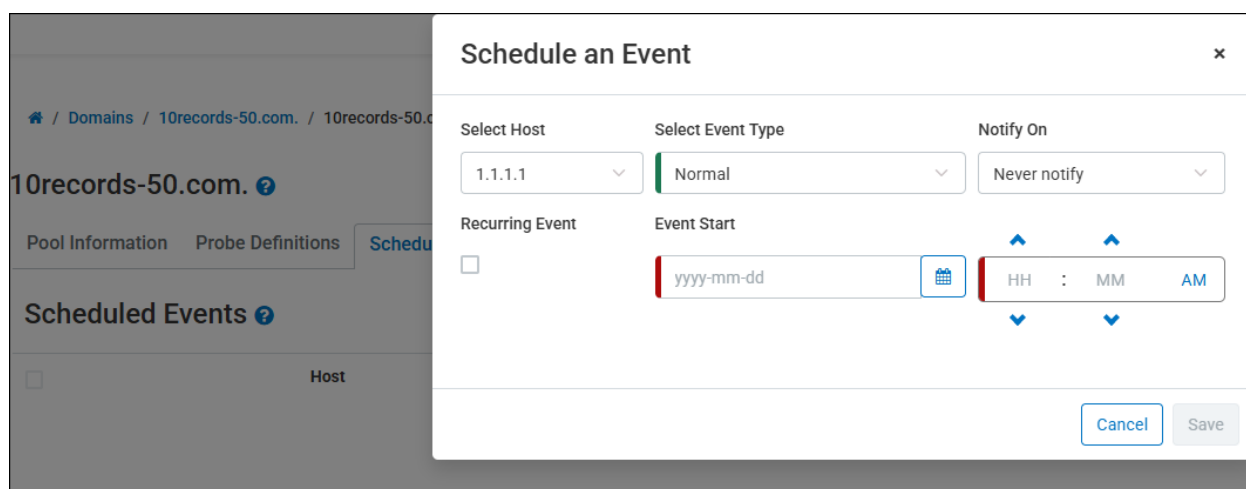
The Scheduled Events tab lists upcoming events for your pool records. For example, you can schedule an event to test the failover functionality of your pool.

Schedule an Event

1. Click the **+Add Event** button.
2. From the **Select Host** drop-down menu, select a record.
3. Select an **Event Type** from the drop-down menu:
 - The default value, **Normal**, indicates that a pool record succeeds and fails with normal

behavior (that is, SiteBacker serves records with the highest priority first).

- **Force Active - Test** forces a record into a served state and probes the record but does not act on the results.
 - **Force Active - No Test** forces a record into a served state and does not probe the record.
 - **Force Fail - Test** forces a record into a not-served state and probes the record but does not act on the results.
 - **Force Fail - No Test** forces a record into a not-served state and does not probe the record.
4. Select how the **Notify On** configuration should be set.
 - **Never Notify** - You won't receive notifications related to the scheduled events.
 - **Notify only on error** - You will only receive an email notification if there is an error or failure.
 - **Notify on error and success** - You will receive an email notification for both failures and successes.
 5. Select the check box for **Recurring Event** if you wish to schedule this event more than once.
 6. Select the **Event Start** by either typing in a date by following the designated format, or by using the calendar icon. Additionally, you can set the specific hour and minute you want the event to begin.
 7. Click **Save** when you are finished.



Notifications

The Notifications tab allows you to add email addresses that you can then associate different notification types to.

1. In the Email List section, provide a valid email address in the addr-spec format. Multiple email addresses can be separated with a space or comma.
2. Once an email address is provided, select the different **event types** for each record that you want to receive notifications for.
 - **Probe Event**
 - **Record Event**

○ **Scheduled Event**

3. Click **Save** once you've added the necessary email addresses and selected the notification types per record that you want to receive.

Add New Notification ×

Email List

Enter a new tag

Notifications Set

Pool Records	Probe Event	Record Event	Scheduled Event
1.1.1.1	Disabled	Disabled	Disabled
8.8.4.4	Disabled	Disabled	Disabled
8.8.8.8	Disabled	Disabled	Disabled

Cancel

Save

Alerts

The Alerts section displays all the alerts for the pool's probes with the following details.

- **Latest Probe Status** - Displays the most recent returned probe status result.
- **IP Address** - Displays the IP Address that was probed / associated to the probe.
- **Probe Type** - Displays whether the Probe was a POST (send a request) or a GET (receive a response).
- **Date/Time** - The Date and Time in which the alert occurred.

Click on the link for a probe alert to obtain additional alert details.

Tip: Add an email address to the Notifications section for automatic event notifications.

Pool Information

Probe Definitions

Scheduled Events

Notifications

Alerts

Alerts List ?

Latest Probe Status	IP Address	Probe Type	Date/Time
---------------------	------------	------------	-----------

Data Flow

Figures in this section indicate:

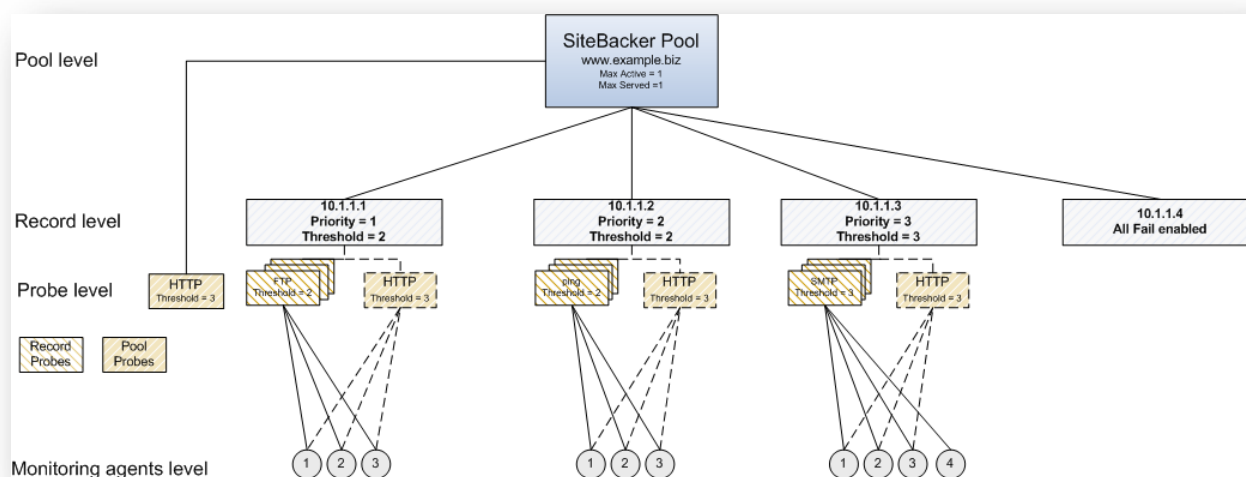
- Pool probes with dashed lines
- Record probes with solid lines
- Served records with lines
- Failed records and probes with red lines

The following figure presents a sample SiteBacker Pool serving the fictitious Web site www.example.biz.

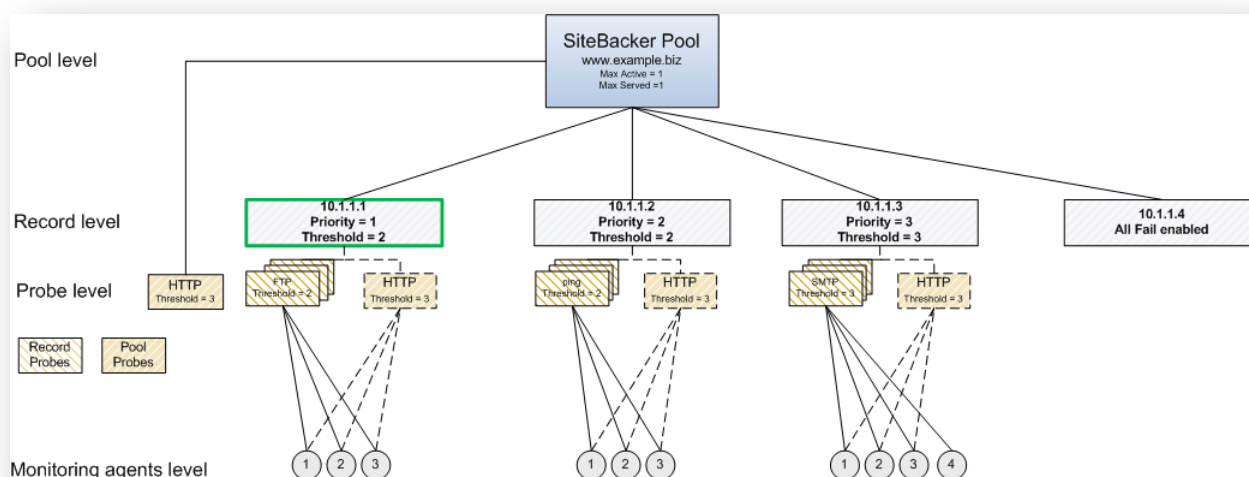
The server 10.1.1.1 has the highest priority. Given the pool's Max Active and Max Served parameters of 1, SiteBacker serves the 10.1.1.1 record in most circumstances.



If the Max Active and Max Served parameters were 2, SiteBacker would serve both 10.1.1.1 and 10.1.1.2 in normal operations. If one of those records failed, SiteBacker would bring up 10.1.1.3. If all records failed, SiteBacker would bring up 10.1.1.4 (the *All Fail* record).



SiteBacker Pool Example

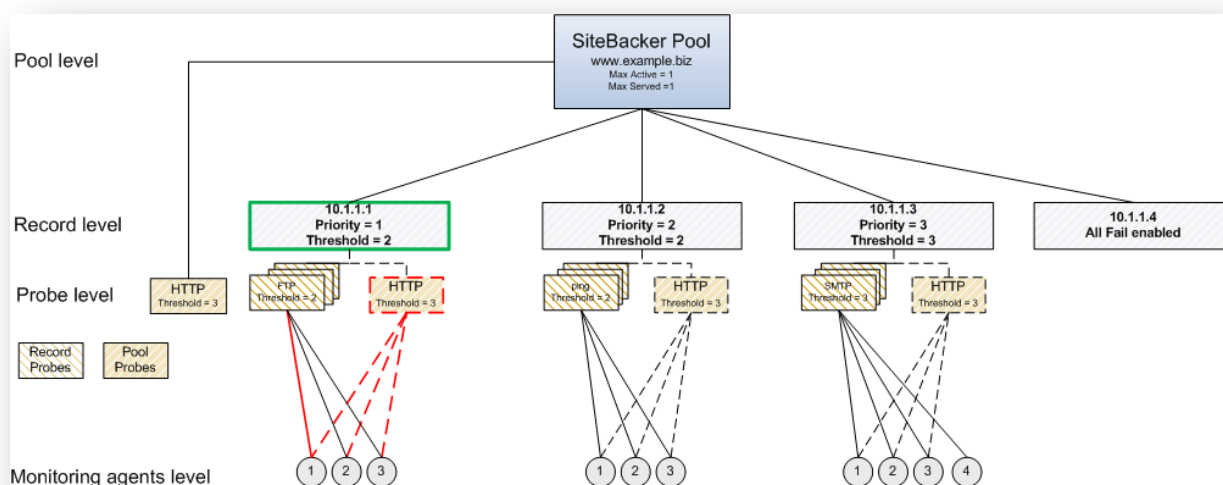


SiteBacker Pool Serving Highest-Priority Record

In the next figure, the HTTP pool probe for 10.1.1.1 failed at all three locations, and the FTP record probe failed at one location.

Because the HTTP probe has met its threshold of 3, the probe status changes to failed. However, because the FTP record probe *has not met* its threshold, its status is good, even though it has failed at one location.

At the record level, only one probe has failed (the HTTP probe), so the record does not meet its threshold of 2, and SiteBacker continues to serve 10.1.1.1.

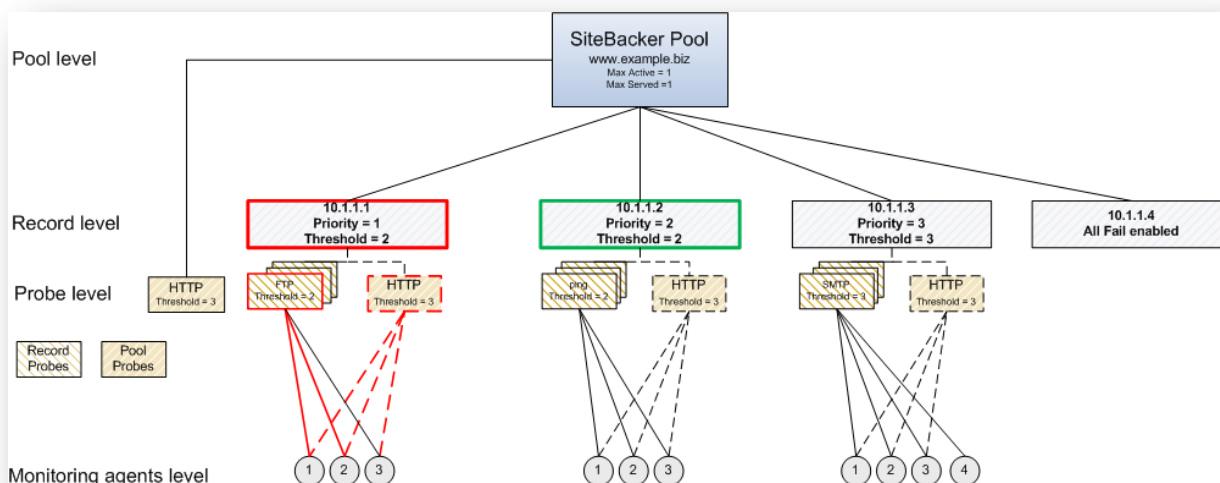


SiteBacker Pool with Probe Failures Not Meeting Record Threshold

If the FTP probe fails at the second location, then the FTP probe status meets its threshold of two, and, because *both* the HTTP probe and the FTP probes have failed, the 10.1.1.1 record

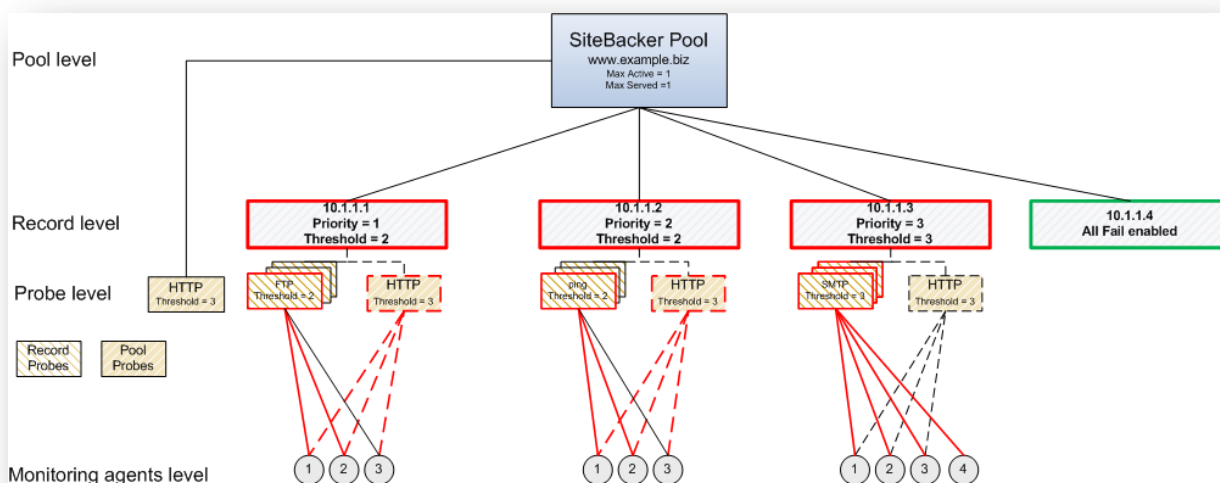
meets its threshold of 2, and the record fails.

This causes SiteBacker to fail the 10.1.1.1 record and serve the record with the next highest priority, 10.1.1.2.



SiteBacker Pool with Failed Record

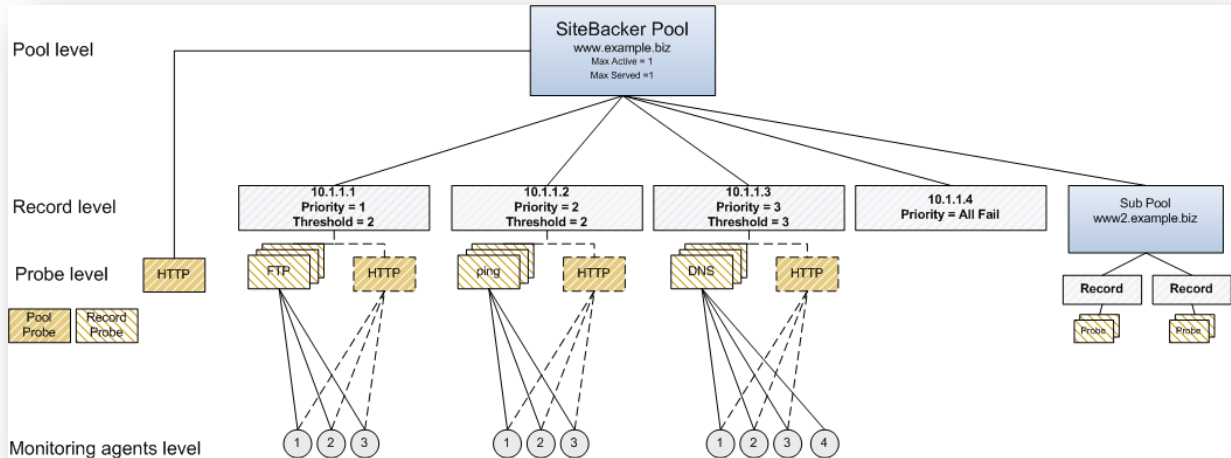
Next, a catastrophe causes the 10.1.1.1, 10.1.1.2, and 10.1.1.3 records to fail (note that to meet the 10.1.1.3 record threshold, 3 probes had to fail). Because SiteBacker cannot serve any records in the active set, it serves the 10.1.1.4 (All Fail) record. The All Fail record may display, for example, a web page stating that the service is down.



SiteBacker Serving the All Fail Record

Sub Pools

You can also create a second SiteBacker or Traffic Controller Pool and configure that pool as a sub-pool to the primary pool. SiteBacker and Traffic Controller treat the sub-pool as an internal reference. In this case, if the sub-pool is an in-domain hostname, the system will serve the sub-pools records as the response. If the sub-pool is a hostname that is outside of the domain, the system will treat it as a CNAME and only deliver the hostname as the response.



SiteBacker Pool with Sub Pool

Traffic Controller Pool

A Traffic Controller (TC) pool is a grouping of A or CNAME records that extends SiteBacker as a Global Server Load Balancing solution. Traffic Controller and SiteBacker pools are very similar in their makeup, therefore in this guide, certain tabs may be referred to the SiteBacker section that has already explained their usage.

	With the addition of the Backup Method feature, existing Traffic Controller pools will have the following applied: ▪ Pools with All-Fail records default to Backup Response. ▪ Pools without All-Fail records default to Fail Close. Newly created Traffic Controller pools default to Backup Response unless an All-Fail record is created, and then by default, switch to Fail Close.
---	---

Creating a Traffic Controller Pool

1. Select either an A or AAAA record type, and then click the **+Add Pool** button.
2. Select **Traffic Controller (TC)** from the **Select Pool Type** drop-down menu.
3. Provide the **Host** and the **Points To** fields.
4. Click **Save** when finished.

Add Pool Record: A (Address - IPv4)

Host:

A valid hostname

Record Type:

A 

Points To:

A valid IPv4 address

TTL:

Time to live, in seconds

Select Pool Type

Traffic Controller (TC) 

Resource Distribution (RD)

Sitebacker (SB)

Traffic Controller (TC) 

Simple Load Balancing (SLB)

Simple Monitor/Failover (SF)

Directional (DIR)

Cancel

Save



Traffic Controller pools cannot contain both A and AAAA records. Individual pools will need to be created to support each of these two record types.

Viewing/Editing a Traffic Controller Pool

Traffic Controller pools consist of various tabs of available functions and details that go beyond just displaying associated records. So, when editing a Traffic Controller pool, there are multiple sections that you can edit.

Pool Information

The following record and pool details are displayed in the Pool Information section. Click **Save** after you make any changes.

- **Description** – Defaults to the pool name. The description can be a maximum of 255 characters.

© 2026 DIGICERT, INC. ALL RIGHTS RESERVED.

30

- **Pool Type** – Displays if the pool is a SiteBacker pool, or a Traffic Controller pool. This field cannot be edited.
- **Failover** – Select **Enabled** if you want to enable a failover record or **Disabled** if you wish to only serve the primary record.
- **Backup Method** - Determines how UltraDNS responds when all primary records in a SiteBacker pool fail health checks. The possible Backup Methods are:
 - **Fail Closed** - Stops responding if all primary records fail and returns an empty DNS response. This is the default Backup Method for new SB pool.
 - i. *This option prioritizes correctness over availability.*
 - **Backup Response** - Uses an All Fail backup record when all primary records fail, so queries still get an answer. This ensures DNS continues to return an answer during full failure scenarios.
 - This method is only available if a pool contains a configured backup (All-Fail) record.
 - **Fail Open** - Continues serving original records even if all health checks fail, ignoring probe status.
 - This option prioritizes availability and traffic continuity.
 - This method is not available if a pool contains a configured backup (All-Fail) record.
- **Probing** – When probing is **Enabled**, a probe can be sent to verify that a URL can be reached, and that the record can be served.
 - Probing cannot be set to **Disabled** unless Failover is set to **Disabled**.
- **Max Active to LB** - Specifies the maximum number of active servers in the pool and determines when Traffic Controller takes backup servers offline. For example, consider a pool with six servers. Setting **Max Active** to 4 means Traffic Controller takes two servers offline and sends the four active records in the answer.
- **TTL** - Specifies the Time to live value for the pool.
- **Configured** - Displays the current number of records (including sub-pools) in the pool.
- **Failure Threshold** – Select from the dropdown menu the number of priority records, which indicates the minimum number of records that must fail for a pool to be labeled 'FAILED'. If the number of failed records in the pool is greater than or equal to the 'Failure Threshold' value, the pool will be labeled FAILED.

[Pool Information](#)
[Probe Definitions](#)
[Scheduled Events](#)
[Notifications](#)
[Alerts](#)

Pool status: OK

Description:
 Pool Type:
 Failover:
 Backup Method:
 Probing:

Max Active To LB:
 TTL:
 Configured:
 Failure Threshold:

Records List [+](#) [+ Add Record](#) [- Delete Records](#)

☐	Points To	Record Type	Record State	Status	Probing	Weight	Priority	Serving
☐	1.2.3.4	A	Normal	→ N/A	Enabled	2	1	✓
☐	1.2.3.5	A	Normal	→ N/A	Enabled	2	2	✓
☐	1.1.1.1	A	Normal	→ N/A	Enabled	-	All Fail	✓

Backup Method Behavior

Refer to the [Backup Method Behavior](#) section for example behavior on how the SiteBacker/Traffic Controller pool behaves based on the Backup Method selected

Records List

The records list displays all the currently associated records to the Traffic Controller pool. From this section, you can Add, Edit, or Delete records from the pool list as needed.

Add a Record

To add a new record to your pool:

1. Click the **+Add Record** button.
2. Provide the IP address or hostname for the record in the **Points To** field.
3. Select the **Failover Delay** value from the drop-down menu, which is measured in minutes.
 - The Failover Delay specifies the time that Traffic Controller waits after detecting that the pool record has failed before confirming that the record is still in failure and activating secondary records. The default value is 1 minute.
 - This same failover delay value (in minutes) will act as failback delay time. In other words, if the failover delay value is x mins, then record will be failed-over and fail-backed after x mins.
4. Provide an even integer value for the **Weight** for the record.
 - The Weight value determines the traffic load to send to each server in the pool.
5. Check the box to designate if this record will be a part of the All Fail record(s) or not.
6. Select the **Probe Threshold** value from the drop-down menu.
7. Select the **Record State** value from the drop-down menu.
8. Choose whether to **Enable** or **Disable** Probes for the record.
9. Provide an integer value for the **Priority** of the record.

10. Click **Save** when you are finished.

Add New Record

Points To	Failover Delay	Restoration Delay	Weight
	0	0	2
	Value in Minutes	Value in Minutes	Enter Even Number [Default is 2]
All Fail	Probe Threshold	Record State	Probes
☐	1	Normal	Enabled
			Priority:
			1

Records List

The records list displays the records in your Traffic Controller pool with the following details.

- **Points To** - Displays the IPv4 or IPv6 address or hostname for the record.
- **Record Type** - The available record types can include A, AAAA, SB (SiteBacker) / TC (Traffic Controller), or CNAME.
- **Record State** - Lists how the record should behave.
 - The default value, Normal, indicates that a pool record succeeds and fails with normal behavior (that is, SiteBacker serves records with the highest priority first).
 - Force Fail - Forces a record into a not-served state.
 - Force Active - Forces a record into a served state.
- **Status** - The status of record which can be one of the following:
 - **OK** - The number of records served is equal to the Max Active value, and all the active records are top priority records. For example, if a pool has a Max Active of 1 and the Priority 1 record is serving, the pool will be marked OK.
 - **WARNING** - The number of records serving is equal to the Max Active value, and the active records are not top priority records. For example, if a pool has a Max Active of 1 and the Priority 1 records is not serving and the Priority 2 record is serving, the pool will be marked WARNING.
 - **CRITICAL** - The number of records serving is less than the Max Active value, or the All Fail record is being served. For example, if a pool has a Max Active of 2, and only one record is serving, the pool will be marked CRITICAL.
 - **FAILED** - No records are serving and there is not an All Fail record configured, or the Failure Threshold has been reached.
 - **N/A** - Indicates that probing has not taken place for the record. This happens if probing is disabled, the probe URL is missing, or the probe is newly configured and has not yet executed.

- **Probing** - Signifies if Probing is enabled for the record or not.
- **Weight** – The integer value that helps determine the traffic load that is sent to each server in the pool.
- **Priority** - Displays the priority value for the records, which is used to determine the order in which records are returned via the Response Method.
- **Serving** - Signifies if the record is Available to Serve or not (meaning if a probe was successful or not). A check mark indicates that serving is available, while an X indicates it is not.

Records List 									+ Add Record	- Delete Records
☐		Points To	Record Type	Record State	Status	Probing	Weight	Priority	Serving	
☐		1.1.1.1	A	Normal	N/A	Enabled	2	1		
☐		trafficcontroller.com.10records-50.com.	TC	Normal	OK	Enabled	2	1		
☐		trafficcontroller1.com.10records-50.com.	CNAME	Normal	N/A	Enabled	2	1		

Probe Definitions

For the Probe Definition details, please refer to the [Probe Definitions](#) section.



HTTP probes only work if the indicated server supports the configured HTTP protocol version, otherwise the probe will fail. Meaning, if your server is not configured for HTTP/2, and you have indicated HTTP/2 as the Protocol Version, the probe will fail.

Scheduled Events

For the Scheduled Events details, please refer to the [Scheduled Events](#) section.

Notifications

For the Notification details, please refer to the [Notifications](#) section.

Alerts

For the Alerts details, please refer to the [Alerts](#) section.

Data Flow

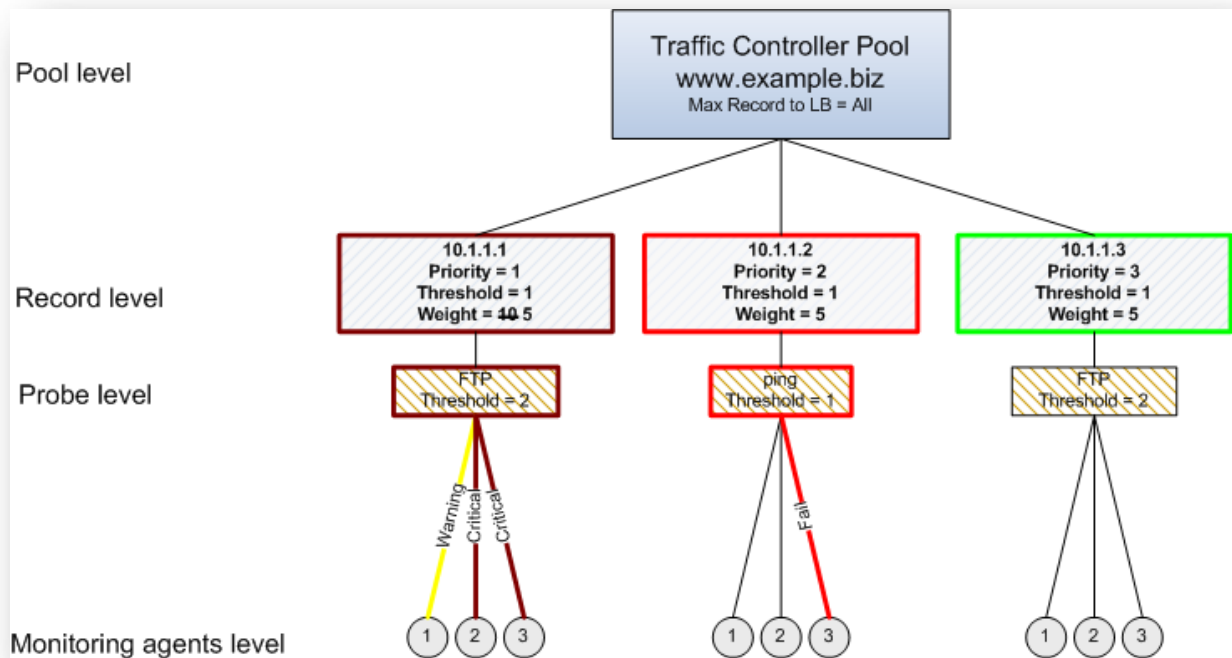
Each record in a Traffic Controller pool includes a *weighted value* that determines the traffic load to send to each server in the pool.

Traffic Controller sends e-mails to warn you when records have reached your configured threshold. If a record transitions to a critical state, Traffic Controller reduces the weighted value by 50%.

The following example shows a Traffic Controller pool with three A records.

The 10.1.1.1 record is now in critical state. Traffic Controller continues to serve the record and reduces its weight by half (meaning Traffic Controller sends 50% less traffic to this server).

The 10.1.1.2 record has failed, so Traffic Controller brings up the 10.1.1.3 record. Because the record weights are equal, half the traffic goes to 10.1.1.1 and half to 10.1.1.3.



Traffic Controller Data Flow (critical states in dark brown)

Sub-pools

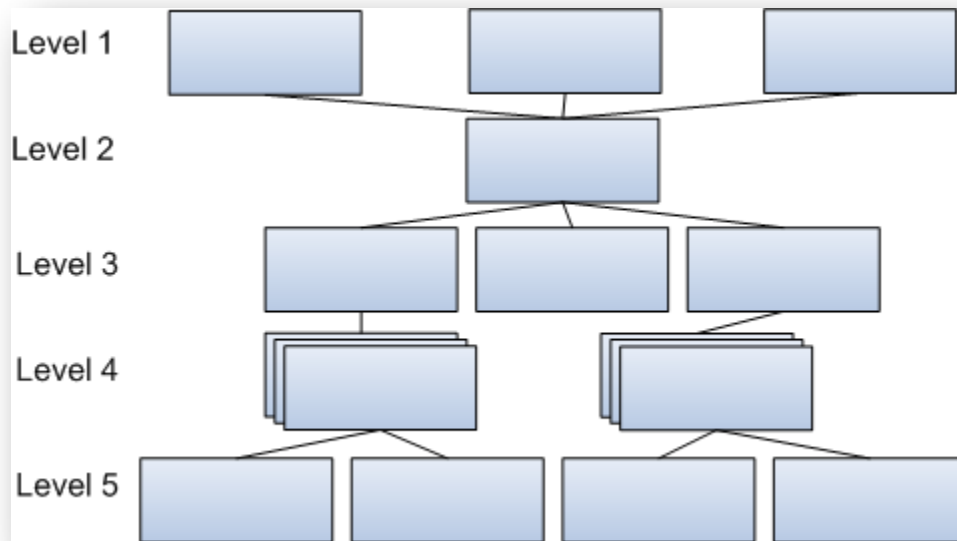
You can add a pool as a record to another pool. The sub-pool (or chained pool) has its own records and probes and provides another backup and load balancing choice to SiteBacker/Traffic Controller.

A sub-pool is *equivalent to a pool record* from the perspective of the primary pool and it uses the same rules to determine whether to serve a record or another pool. If you query a primary SiteBacker pool's name, you will receive all active records in the primary pool *and*—if the sub-pool is active for the primary pool—all records in the sub-pool. However, if you query the sub-pool's name, you receive only the sub-pool's active records.

A sub-pool is equivalent to its set of pool records from the perspective of the DNS. For example, when a sub-pool is active in a primary pool, SiteBacker serves any active sub-pool records in addition to any other active records and sub-pools in the primary pool, but the sub-pool counts as one server, just like any pool record, when the primary pool calculates its maximum active servers.

Traffic Controller records have assigned weight values. If a Traffic Controller pool is an active sub-pool, the application evaluates the weight of each record and distributes the traffic accordingly.

UltraDNS supports an unlimited number of sub-pools up to five levels deep.



Sub-pool chains restricted to 5 levels

Simple Load Balancing Pool

Simple Load Balancing (SLB) Pools are used to define a pool of up to five IPv4 A records (primary records) or IPv6 AAAA records, an HTTP(S) monitor, and a backup (All Fail) IPv4 / IPv6 address. One resource record will be served based upon the Response Method that is configured.

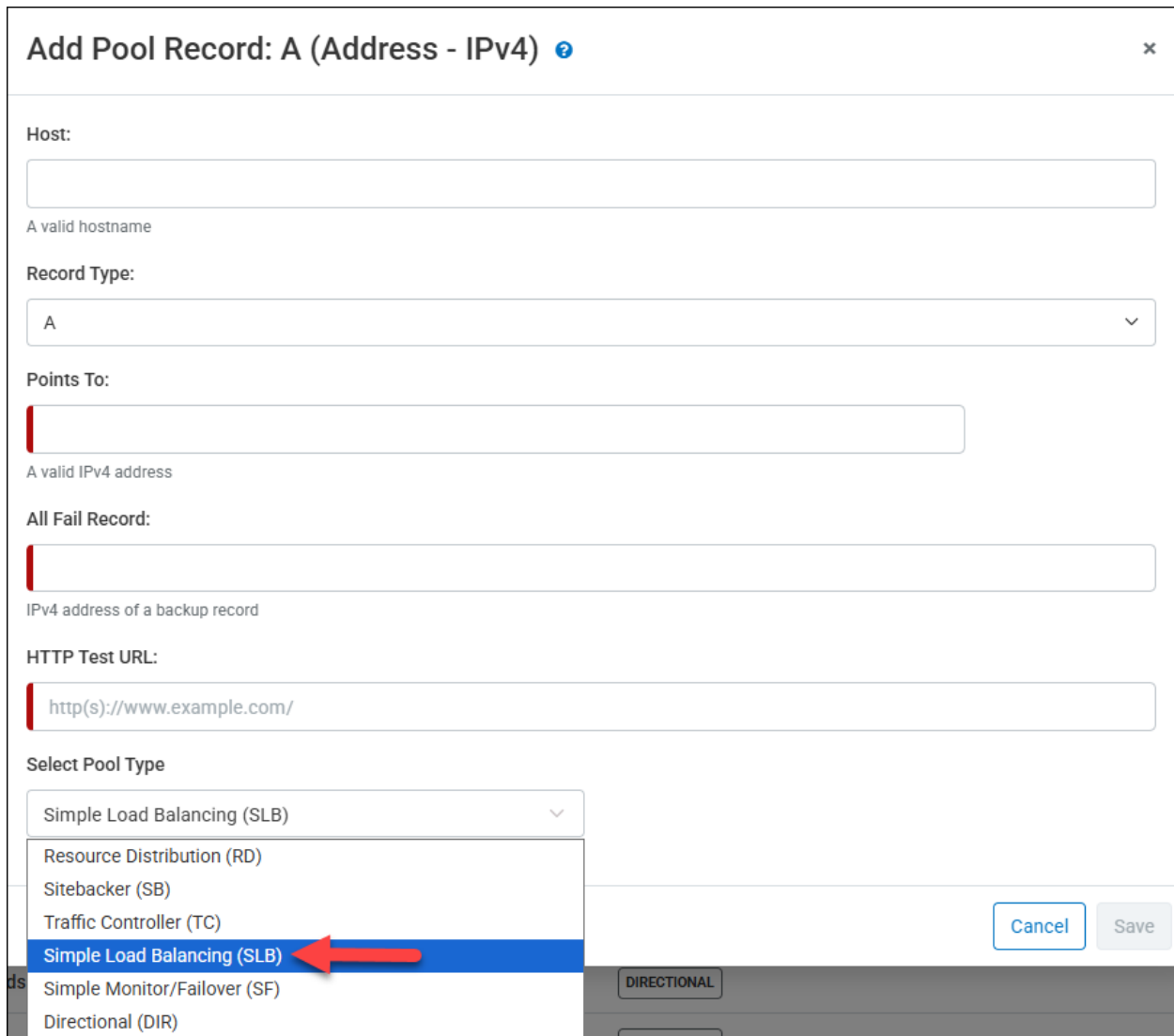
When using Simple Load Balancing, the defined monitor (probe) sends HTTP(S) GET or POST requests from four locations pointed at the target addresses once every five minutes. Optionally, the request to the target system can include HTTP(S) request data, and/or the HTTP response data can be searched for specific content. If no search string is specified, the probe of the target is considered Successful if any non-error HTTP response from the target is received. The availability of the target system is evaluated upon receipt of each successful or unsuccessful probe result from each location.



Simple Failover is configured to send an email alert whenever the status of a monitored endpoint changes. The email notification is sent to the primary and secondary email address provided for the Primary User of the account only. To change the email address, navigate to the Accounts section of the portal, and update the Primary User's contact information.

Creating a Simple Load Balancing Pool

1. Select either an A or AAAA record type, and then click the **+Add Pool** button.
2. Select **Simple Load Balancing (SLB)** from the **Select Pool Type** drop-down menu.
3. Provide the **Host** and the **Points To** fields.
4. Provide the **All Fail Record** (the backup record).
5. Include the **HTTP Test URL** that will be used to verify the service is available.
6. Click **Save** when finished.



Add Pool Record: A (Address - IPv4) ✕

Host:

A valid hostname

Record Type:

A

Points To:

A valid IPv4 address

All Fail Record:

IPv4 address of a backup record

HTTP Test URL:

http(s)://www.example.com/

Select Pool Type

- Simple Load Balancing (SLB)
- Resource Distribution (RD)
- Sitebacker (SB)
- Traffic Controller (TC)
- Simple Load Balancing (SLB)**
- Simple Monitor/Failover (SF)
- Directional (DIR)

Cancel Save

Viewing/Editing a Simple Load Balancing Pool

Records

Once your Simple Load Balancing pool is created, you will see three tabs that comprise the pool. The first tab is the **records** tab, which displays the primary records for the pool, and allows you to set the Forced State, and enabling Probes or not.

Add Primary Record

1. Click in the **Add Primary Record** field and provide an IP address for the new record.
2. Select the **Forced State** from the drop-down menu.
 - **Not Forced** - Indicates the record could be served if the probe succeeds or will not be served if the probe fails.

- **Forced Active** - Indicates that the record should be served even if the probe fails and determines that the record cannot be served.
 - **Forced Inactive** - Indicates that the record should NOT be served even if the probe succeeds and indicates that the record can be served.
3. Select whether **Probing** should be enabled or not. If Probing is NOT enabled, the primary record cannot be served unless the forced state is set to Forced Active.
 4. Click the **+Add** button to add the new record to the list of primary records.
 5. Always remember to keep your **All Fail Record** up to date, as this will be the backup record served if the primary records all fail.
 6. Click **Save** when you are finished adding records to save this list and your settings.

localhost123SLB.com.10records-50.com.

Records

Information

Probe Definition

Primary Records

— Delete Selected

⇌ Convert

Record	Forced State	Probing Enabled	Available To Serve
☐ 10.1.1.14	Not Forced	Yes	Yes
☐ 14.14.14.12	Not Forced	Yes	Yes

Add primary record

Not Forced

No

+ Add

IP address of Record

Forced State

Probing Enabled

All Fail Record:

10.1.1.77

IP address of a backup record

All Fail Serving?

No

Cancel

Save

Information

The information tab provides details about how the records will be served and returned. If you make any changes to this section, make sure to click the **Save** button afterwards.

- **Description** – You can provide a description for the SLB pool if you wish, but by default, it will display the pool name.
- **TTL** – The Time to live in seconds for the pool.
- **Response Method** – Select a method which is responsible for selecting records to be served in the return response.
 - **Round Robin** - The order of the records being returned is determined in a "Round Robin" fashion, based upon the priority of the active records.
 - **Random** - The order of the records being returned is random and ignores the priority of the active records.
 - **Priority Hunt** - The order of the records being returned is fixed and is based on the priority value of the active records (High to Low). The highest priority record is always returned.
- **Serving Preference** – Determines if records will be selected from the Primary records or the All Fail records.
 - **Auto Select** - The default serving method, which will serve either the primary records or the All Fail Record depending on the probe results (and the forced state) of the primary records.
 - **Serve Primary** - Indicates that only the primary records are served based upon the probe results (and the forced state) of the primary records.
 - **Serve All Fail** - Indicates that only the All Fail Record will be served, thereby ignoring the probe results (and the forced state) of the primary records.

localhost123SLB.com.10records-50.com.

Records

Information

Probe Definition

Description:

localhost123SLB.com

An optional description

TTL:

120

Time to live, in seconds

Response Method:

Round Robin

Round Robin

Random

Priority Hunt

Serving Preference:

Auto Select

Serve Primary

Serve All Fail

Cancel

Save

Probe Definition

When using Simple Load Balancing, an HTTP(S) probe is automatically configured for the pool.

The All Fail Record's IP address is not probed. This probe can be configured for either GET or POST. The Probe monitors the Target System (each record in the primary records pool once every 300 seconds from each of four geographic regions).

Response data can optionally be validated for the presence of specific content from the Search String field on a successful response. If no Search String is specified, the probe is considered as successful if any non-error response (not HTTP 2xx response) from the target is received. The probe will follow an HTTP 3xx Redirect received from the target system. Availability of the target system is evaluated upon receipt of each successful or unsuccessful probe result from each location.

From the **Probe Definition** tab, you can do the following:

- **HTTP Test URL** – Provide an http(s) URL to run a test probe against to verify it can be queried.
- **HTTP Method** – You can select either **GET** to retrieve data from the test probe, or **POST** to send data to the URL with the test probe.
 - If you select **POST**, the **Transmitted Data** field will appear, allowing you to specify the data you wish to send.
- **Search String** – You can provide a specific search string that should be present in a test probe response for the probe to be considered successful.
- **Region Failure Sensitivity** – Allows you to specify the conditions under which UltraDNS will serve the **All Fail Record** instead of one of the **Primary records**.
 - **High** - Probes in two or more regions are reporting failure of the probe target.
 - **Low** - Probes in ALL (four) regions are reporting failure of the probe target.

Once you have provided all the Probe details, click the Test Probe button to test your newly configured probe information to verify the functionality of the probe. UltraDNS will attempt to execute the configured probe towards the probe target system. When the test probe is complete, the results will be displayed below the pool name of your Simple Load Balancing pool.

localhost123SLB.com.10records-50.com.

Records Information **Probe Definition**

HTTP Test URL:

https://www.google.com/

HTTP Method:

GET

Search String:

status: ok

Search for string in HTTP response

Region Failure Sensitivity:

High

Test Probe

Cancel

Save

Directional Pool

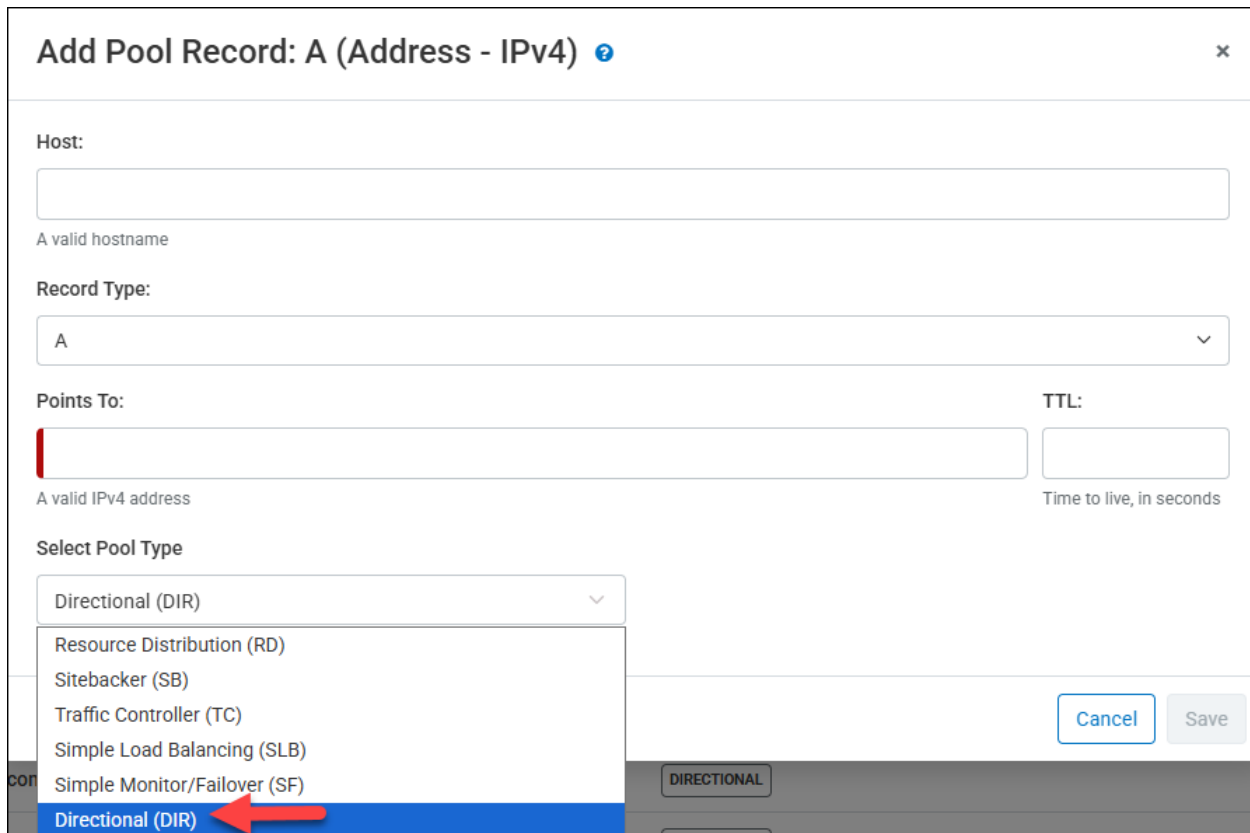
A Directional DNS record represents a Directional Load Balancing (DIR) pool, which is a collection of records configured to use your geographic location or source IP address to determine a response.

Configuration Tips and Rules

- Create any Resource Distribution/SiteBacker/Traffic Controller pools first if you plan to route traffic for a region or group of regions to the RD/SB/TC pools.
- Directional pools on the zone apex (for example, the example.com zone) cannot contain CNAME records.
- Combinations of A and CNAME records or AAAA and CNAME records are allowed in the same pool.
- The record type No Response is available for all pools, but other record types may only exist in their own pool. The No Response record blocks traffic from specified regions by returning No Error, No Response.

Creating a Directional Pool

1. Select either an A or AAAA record type, and then click the **+Add Pool** button.
2. Select **Directional (DIR)** from the **Select Pool Type** drop-down menu.
3. Complete the **Host** and **Points To** fields.
4. Optionally you can provide a **TTL** (Time to Live) value.
5. Click **Save** when finished.



There are three types of possible Directional pools:

- **Geolocation & Source IP** – Responses are based upon a user's geographic location and IP address.
- **Geolocation** – Responses are based upon a user's geographic location.
- **Source IP** – Responses are based upon a user's IP address.

Conflict Resolves To

If your Directional Pool contains both Geolocation and SourceIP records, then an additional drop-down menu will appear when you view/edit your pool. When there is a conflict between a matching Geolocation group and a matching Source IP group, the selected type takes precedence.

Select a record type from the drop-down list, and then click the **Save Changes** button. You can change the selected record type whenever you need.

Ignore ECS

Enabling the Ignore ECS option determines whether to ignore the EDNSO (which is an extended label type allowing for greater DNS message size) Client Subnet data when available in the DNS request. We recommend that if you are not familiar with this concept, do not check the box to

enable this feature.

A/CNAME Directional Pool ?

Description:

Conflict Resolves To: ?

Ignore ECS: ?

ARecord_DR.com

Geolocation

▼

☐

Save changes

Editing a Directional Pool

After you have created a Directional Pool, you will see the **Pool records** screen. From here, you can add additional records and customize whether you want them to contain Geolocation data, SourceIP details, or a combination of both.

From the pool records screen, you can see the currently associated records, along with the **Groups** assigned to them. You can click on

- The  icon denotes that the record contains Geolocation data.
- The  icon denotes that SourceIP details are associated to the record.
- **All Non-Configured** implies that every geographic region is associated to the record, as well as any preconfigured SourceIP details.

A/CNAME Directional Pool ?

Description:

Conflict Resolves To: ?

Ignore ECS: ?

ARecord_DR.com

Geolocation

▼

☐

Save changes

Pool Records

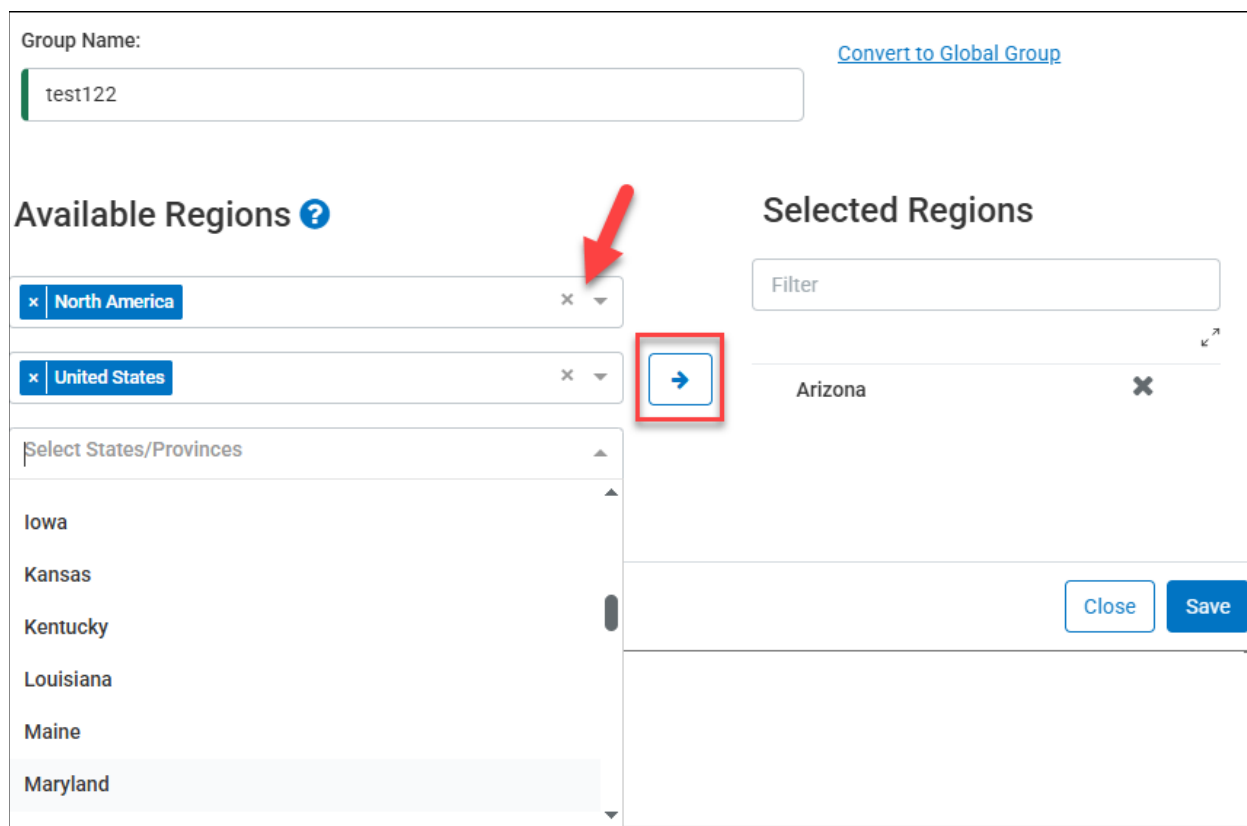
☐	Groups	Record Type ↑↓	Points To ↑↓
☐ 	 test122	A 	1.12.2.2
☐ 	 test1	A 	1.2.3.1
☐ 	 0-0-abcd1 (global)	A 	12.11.1.1
☐ 	 All Non-Configured	A 	121.1.1.6

Add a Record - Geolocation

Adding Geolocation details to your record works in a "drill-down" manner, meaning that you can select specific states and provinces from a within a selected territory, or select an entire overarching region (continent) instead. There is no limit to the number of regions / territories / states that can be associated to your record.

To add a Geolocation record:

1. Click the **+Add** button.
2. Select a **Record Type** from the drop-down menu.
 - **A** record
 - **CNAME** record
 - **No Response**
3. Provide the IPv4 address for the record in the **Points To** field.
 - Optionally, you can add the **TTL** value.
4. Click **Add a Group** when finished.
5. Select Geolocation from the **Add Directional Group** drop-down menu.
6. Select **Create New Group** to associate new Geolocation details to the record or select **Assign Global Group** to associate a pre-configured **Directional Groups** to your record.
 - If you opt to use an existing Account-level Directional Group, select the **Group Name** from the drop-down list of groups you have access to.
7. Provide a **Group Name** for your record.
8. Click in the **Select Regions** field to select any applicable regions for your record.
 - In the following example, we selected North America.
9. Once you've selected your region(s), click outside of the **Available Regions** field.
 - If you click on the **arrow** at this point, you will select the region and by default, every country and state / province as well.



Group Name: [Convert to Global Group](#)

Available Regions ?

- North America
- United States

Select States/Provinces

- Iowa
- Kansas
- Kentucky
- Louisiana
- Maine
- Maryland

Selected Regions

Filter

Arizona

Close Save

- Click in the **Select Countries** field and select any applicable territories for your record.
 - If you select the **arrow** at this point, you will select the country / countries and by default, every associated state / province.
- Click in the **Select States/Provinces** field and select any applicable states or provinces for your record. Once you have made your selections, click the **arrow** to move your selections to the **Selected Regions** column.
 - To remove a selected location, click the **X** next to the location name.
- Once you have made all your selections, click **Save** to complete the record, or click **Add Another Group** to associate SourceIP data to the record as well.

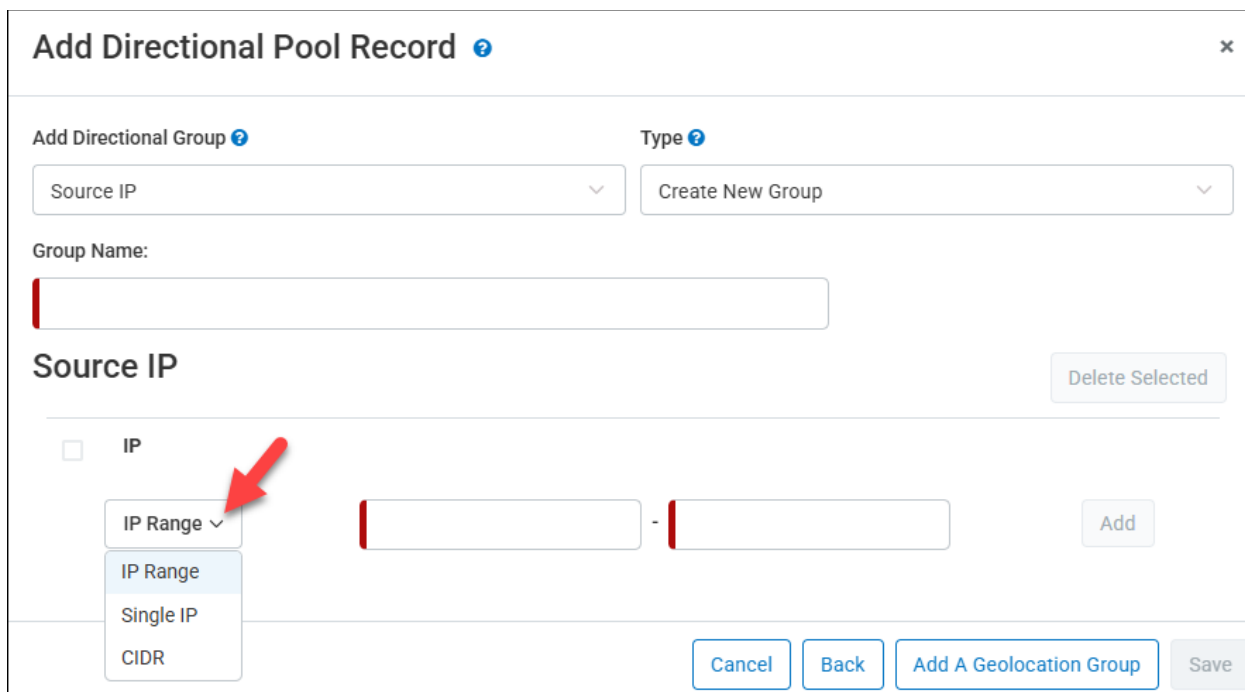
Add a Record – SourceIP

A Source IP Directional Pool tailors a response based on your IP address (either IPv4 or IPv6). The UI portal supports standard IPv6 address notation: eight groups of four hexadecimal digits, separated by a colon (:). You can simplify the notation by omitting leading zeros in a group, or by replacing one or any number of consecutive groups of 0 with two colons (::). For example, these IPv6 addresses are equivalent:

```
3FFE:0B80:0447:0001:0000:0000:0000:0001
3FFE:0B80:0447:1:0:0:0:1
3FFE:0B80:0447:1::1
```

To add a SourceIP record:

1. Click the **+Add** button.
2. Select a **Record Type** from the drop-down menu.
 - **A** record
 - **CNAME** record
 - **No Response**
3. Provide the IPv4 address for the record in the **Points To** field.
 - Optionally, you can add the **TTL** value.
4. Click **Add a Group** when finished.
5. Select the **SourceIP** from the **Add Directional Group** drop-down menu.
6. Select **Create New Group** to associate new SourceIP details to the record or select **Assign Global Group** to associate a pre-configured **Directional Groups** to your record.
 - If you opt to use an existing Global Directional Group, select the **Group Name** from the drop-down list of Global Groups you have access to.
7. Provide a **Group Name** for your record.
8. Select the **SourceIP Type** in which you will provide your IP address details.
 - **IP Range** – Provide a beginning and ending IP address to create a range.
 - **Single IP** – Provide a single IP address for the record.
 - **CIDR** – Specify the network and routing prefix. For example, 192.168.0.0/16 or 2001::/64.
 - i. Note: The UI Portal automatically converts the CIDR notation to an IP range.



9. Once you have selected your input type, provide your Source IP details, and then click the **Add** button.
10. You can add as many IP addresses as you wish. Click **Save** when you are done or click **Add Another Group** if you want to associate Geolocation data with the record.

Overlaps

You **CANNOT** overlap regions or Source IP ranges at the record pool level. However, Global Directional Groups (both Geolocation and Source IP) may overlap. For example, you could have a North America group consisting of Canada, the United States, and Mexico, and three groups consisting of Canada, the United States, and Mexico separately; or you may have overlapping networks.

Converting a Mixed Pool to a Geolocation or Source IP Pool

Carefully consider before converting a Mixed Pool (a pool that contains BOTH Geolocation and Source IP Groups and records) to a Geolocation or Source IP Pool (pools that contain ONLY Geolocation or Source IP Groups and records). Once you click **Convert**, the groups and records that do not match the pool type will be removed.

Convert to Global Group

Once you have successfully created a record containing either SourceIP data or Geolocation details, you can convert your saved settings to a Global Directional Group.

1. Click on the **Globe** or **IP** icon to edit the record.
2. Click the **Convert to Global Group** link.
3. Provide a new **Global Group Name**, and then click the **Checkmark** icon.

Edit Directional Group ✕

Group Name:

test1

Convert to Global Group

Source IP

Delete Selected

☐ IP

☐  1.1.1.2

IP Range ▾

 -

Add

Close

Save

Simple Monitor / Failover Pool

Simple Monitor/Failover (SF) provides probing, notifications, and failover of a web site's IPv4 address record to one other IPv4 address.

When using Simple Monitor/Failover, the defined probe sends HTTP(S) GET or POST requests from four locations towards the target system once every five minutes. The target system may be any host. Optionally, the request to the target system can include HTTP(S) Request data and/or the HTTP response data can be searched for specific content. If no search string is specified, the probe of the target is considered as successful if any non-error HTTP response from the target is received. The availability of the target system is evaluated upon receipt of each successful or unsuccessful probe result from each location.

Simple Monitoring is a subset of Simple Failover and Simple Load Balancing (SLB). You can run all Simple Failover calls as a Simple Monitor call instead by ensuring that the Failover record information is removed from the body of the call. Examples will be provided for each call.

Simple Monitoring is designed to provide single resource record sites with a very basic website availability monitor. This monitor tracks whether a website is available or unreachable and alerts the customer to unavailability via email notification. This feature does not provide fail-over assistance to an alternative record (i.e., All fail), nor does it provide any measurement statistics on the health of the website (beyond whether the site is available or down).



Simple Failover is configured to send an email alert whenever the status of a monitored endpoint changes. The email notification is sent to the Zone Owner's (the user that created the Zone/Domain) email address.

Creating a Simple Monitor/Failover Pool

1. Select either an A or AAAA record type, and then click the **+Add Pool** button.
2. Select **Simple Monitor / Failover (SF)** from the **Select Pool Type** drop-down menu.
3. Provide the **Host** and the **Points To** fields.
4. Optionally you can provide the **TTL** value.
5. Provide the **All Fail Record** (the backup record).
6. Include the **HTTP Test URL** that will be used to verify the service is available.
7. Click **Save** when finished.

Add Pool Record: A (Address - IPv4)

Host:

A valid hostname

Record Type:

A

▼

Points To:

A valid IPv4 address

TTL:

Time to live, in seconds

All Fail Record:

IPv4 address of a backup record

HTTP Test URL:

Select Pool Type

Simple Monitor/Failover (SF) ▼

Resource Distribution (RD)

Sitebacker (SB)

Traffic Controller (TC)

Simple Load Balancing (SLB)

Simple Monitor/Failover (SF)

Directional (DIR)

Cancel

Save

RD POOL

Editing a Simple Monitor/Failover Pool

When editing a Simple Monitor/Failover Pool, the following fields can be changed.

- **Description** – You can provide a description for the SF pool if you wish, but by default, it will display the pool name.
- **TTL** – You can set the Time to live value for the pool (optional).
- **Primary** – The primary record for the pool. This can be changed at any point, and if you are serving the primary record, the **Primary Serving** section will display “Yes.”

- **Add Backup (Failover)** – In the event that you have a backup record that you want to failover (fall back to) should your primary record fail, click in the checkbox. This will display the **Failover** field.
 - **Failover** – Provide the IP Address for the backup record that you want to failover to in the event your primary record fails.
 - If you are not currently in a failover situation, the **Failover Serving** will display “No.”

Edit Simple Failover Pool ?

abc123.10records-50.com.

Manual Failover Convert

Description:

abc123

An optional description

TTL:

30

Time to live, in seconds

Primary:

1.2.1.3

Primary Serving?:

Yes

Add Backup (Failover)?:

☒

Failover:

13.13.12.12

Failover Serving?:

No

Probe Definition

HTTP Test URL:

http://test.com/

HTTP Method:

GET

Search String:

status: ok

Region Failure Sensitivity:

High

Test Probe

Cancel Save

Probe Definition

When using Simple Monitor / Failover, an HTTP(S) probe is automatically configured for the Primary IP address. The Failover IP address is not probed.

This probe can be configured for GET or POST. It monitors the target system once every 300 seconds from each of four geographic regions. If POST is selected, the Transmitted Data

section must be completed. Target system is the configured Primary IPv4 address.

- **HTTP Test URL** – Provide the URL that you wish to run the probe against.
- **HTTP Method** – You can select either **GET** to retrieve data from the test probe, or **POST** to send data to the URL with the test probe.
 - If you select **POST**, the **Transmitted Data** field will appear, allowing you to specify the data you wish to send.
- **Search String** – You can provide a specific search string that should be present in a test probe response for the probe to be considered successful.
- **Region Failure Sensitivity** – Allows you to specify the conditions under which UltraDNS will serve the **All Fail Record** instead of one of the **Primary records**.
 - **High** - Probes in two or more regions are reporting failure of the probe target.
 - **Low** - Probes in ALL (four) regions are reporting failure of the probe target.
- Click the **Test Probe** button once you have configured your probe details. The Probe result will be displayed at the top of the screen once completed.
- Click **Save** if you make any alterations to the screen.

Manual Failover

If you need to failover to your backup record, AND if you have specified the **Failover** record, you can click the **Manual Failover** button to begin the failover process.

1. Click the **Manual Failover** button.
2. Verify that the backup record you will be pointing to is correct.
3. Click the **Yes** button.
 - As per the disclaimer, please allow at least 15 seconds to see the updated **Primary Serving** and **Failover Serving** status changes before proceeding.
4. Click **Save** when you are finished.

abc123.10records-50.com.

Manual Failover **Convert**

Description: abc123 TTL: 30

An optional description Time to live, in seconds

Primary: 1.2.1.3

Add Backup (Failover)? ☒

Failover: 13.13.12.12

Probe Definition

HTTP Test URL: http://test.com/

Search String: status: ok Region Failure Sensitivity: High **Test Probe**

Manual Failover Confirmation

You have chosen to perform a(n) Manual Failover. The pool abc123.10records-50.com. will now point to 13.13.12.12.

After performing this operation, please wait 15 seconds to see the updated "Primary Serving" and "Failover Serving" status.

Are you sure you want to continue?

No **Yes**

Additionally, you can see which records within the pool have been configured for Manual Failover by the **Pool Status** icon. The hand icon indicates that the record is set for Manual Failover.

Undo Manual Failover

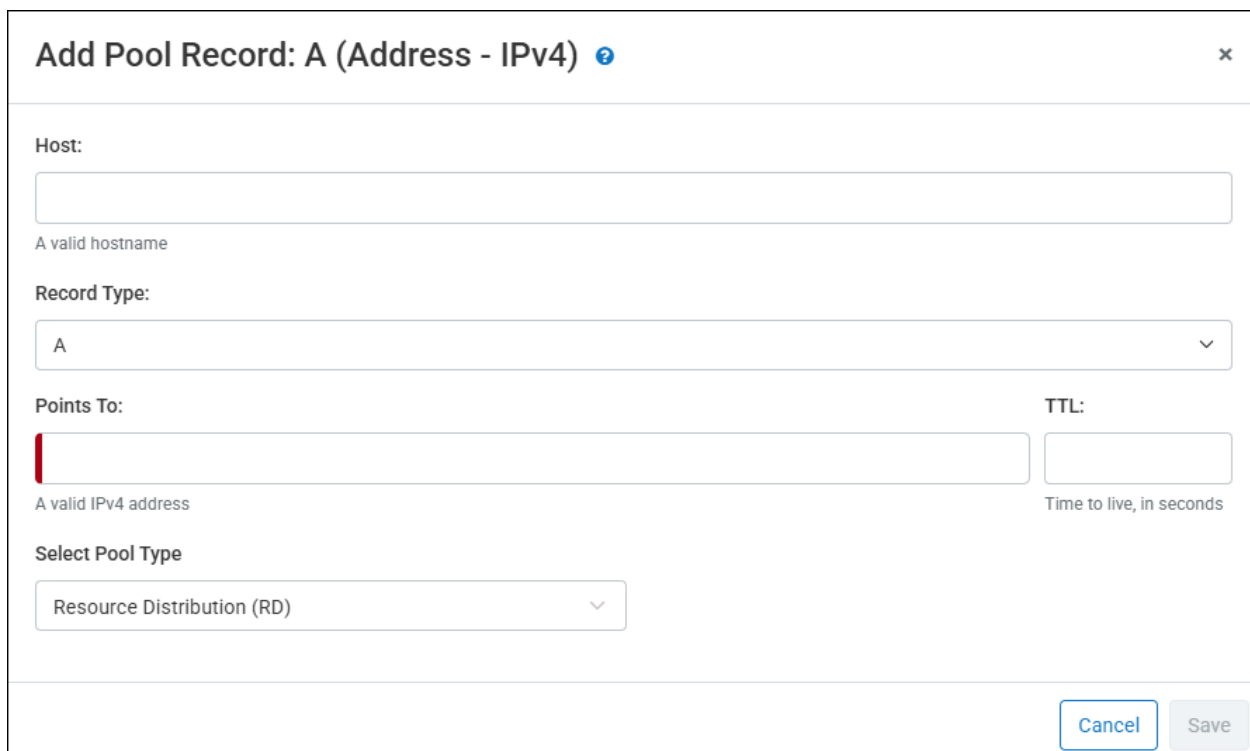
1. To failback to your primary record, first ensure that the **Failover Serving** status says Yes.
2. Next, make sure the **Primary** displays the correct IP Address.
3. Click the **Undo Manual Failover** button.
4. Ensure the details are correct, and then click the **Yes** button.
 - o As per the disclaimer, please allow at least 15 seconds to see the updated **Primary Serving** and **Failover Serving** status changes before proceeding.
5. Click **Save** when you are finished.
- 6.

Resource Distribution Pool

A Resource Distribution Pool is simply a grouping of type A (IPv4 address) or type AAAA (IPv6 address) records, in which you can specify how the records answer a query.

Creating a Resource Distribution Pool

1. Select either an A or AAAA record type, and then click the **+Add Pool** button.
2. Select **Resource Distribution (RD)** from the **Select Pool Type** drop-down menu.
3. Provide the **Host**, the **Points To**, and the **TTL** (optional).
4. Click **Save** when finished.



Add Pool Record: A (Address - IPv4) ✕

Host:

A valid hostname

Record Type:
 ▼

Points To: TTL:

A valid IPv4 address Time to live, in seconds

Select Pool Type
 ▼

Cancel Save

Once an RD pool is created, you can edit the pool record to add additional records (IP addresses) under the pool. You can also edit the Serving Method and the TTL value for pool.

The Serving Methods act as follows:

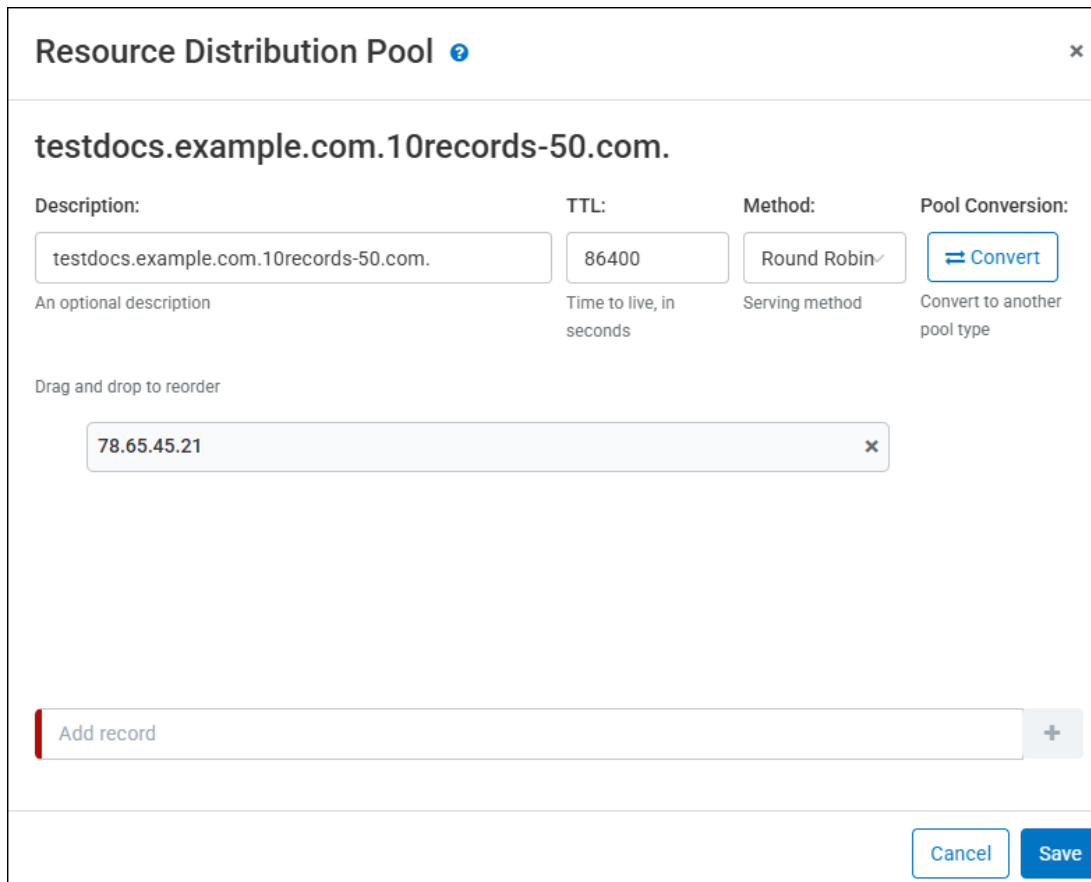
- **Round Robin**¹ (default) – The records will rotate in priority.
- **Fixed** – The records will appear in a set order.

¹ https://en.wikipedia.org/wiki/Round-robin_DNS

- **Random** – The records will appear in a random order.

Editing a Resource Distribution Pool

1. Click the **Pencil** icon next to the RD Pool record.
2. Change the Description, TTL, and/or Method values as needed.
3. Click into the **Add Record** field and provide a new record.
4. Click the **Plus Icon** to add the new record to the pool.



The screenshot shows the 'Resource Distribution Pool' configuration window. At the top, the title is 'Resource Distribution Pool' with a help icon and a close icon. Below the title, the pool name 'testdocs.example.com.10records-50.com.' is displayed. The configuration is divided into four sections: 'Description:' with a text input field containing 'testdocs.example.com.10records-50.com.' and a subtext 'An optional description'; 'TTL:' with a text input field containing '86400' and a subtext 'Time to live, in seconds'; 'Method:' with a dropdown menu showing 'Round Robin' and a checkmark, with a subtext 'Serving method'; and 'Pool Conversion:' with a 'Convert' button and a subtext 'Convert to another pool type'. Below these sections, there is a 'Drag and drop to reorder' area containing a single record '78.65.45.21' with a delete 'X' icon. At the bottom, there is an 'Add record' input field with a plus icon to its right. At the very bottom right, there are 'Cancel' and 'Save' buttons.

5. Click **Save** to update the pool.

You can use a “drag and drop” function to re-order your records. Click on a record and then move it to a new location in the list of existing records.

- The order / rank determines the priority and sorting of the records and how they will be queried. No two records can have the same priority.

The **X** icon will delete the record from the pool. Whenever you make changes, click the **Save** button.