New Generic Top-Level Domains

21 October 2013

Centralized Zone Data Service

Frequently Asked Questions

During ICANN 47 Durban, staff gave a presentation on the Centralized Zone Data Service (then known as the CZDAP), ICANN's solution for scaling zone data provision as hundreds of new gTLDs are added to the Internet. During the session, we received quite a few answers that we were unable to address due to time constraints. Below, find answers to these and a variety of other questions we've received about the CZDS. Additional questions and answers may be accessed via the help pages: https://czds.icann.org/en/help

End User

Q: Will the user be able to change the IP address they use for access?

A: Yes, in the user profile section you can identify one or more IP addresses from which you intend to access SFTP servers.

Q: If an end user is provided with access to multiple TLDs – for example, 1,400 – does s/he have to download each data file individually?

A: No, we have created the CZDS API which is a token-based system allowing the bulk download of SFTP credentials. The token ensures that access can be automated, allowing individuals to fetch new zone data without logging in manually. In cases where abuse is detected, expiring the token (done either by CZDS admin or Registry Operator users themselves) removes the ability of any script to complete further downloads until the new, valid user token is entered into the script.

The tools for bulk download of SFTP credentials are already created. All information regarding the tools can be found in the open source repository on.

https://github.com/fourkitchens/CZDS-tools

Q: It might be useful to have a download page that shows all the files I have access to instead of having to access each individual page. There should be one page with a list of all the TLDs I have access to and there should be some metadata attached to that. For example, when was it last updated by the Registry and other stuff you'd see at FTP. There should be an FTP account where I could see all the stuff.

A: This feature is not available at this time.

Q: Is there a possibility of having some kind of historical data for example last week, or the last four weeks for example?

A: That functionality is not offered by the system.

Q: Is there a way to challenge a Registry denial?

A: The Registry Agreement requires a gTLD registry to offer zone data at no cost to the data consumer. If an end user believes that a registry is denying access unfairly or gets no response from a registry, they may file a complaint with the ICANN Compliance department who will reach out to the registry and investigate.

Q: When will new gTLD Registries be required to start providing their zone data? At signing of contract, at technical delegation, or has that not been decided yet?

A: New gTLD Registries are required to start providing their zone data upon delegation.

Q: How do Registries get their zone data into the CZDS system? FTP upload or zone transfer?

A: There are two options – the Registry Operator can either maintain control of their data by merely approving access and providing the users (via CZDS) with access credentials to their SFTP server; or they can allow ICANN to do periodic zone transfers (AXFR) and configure the data on their behalf, which would then be available for users to download directly through the CZDS system.

Q: If a Registry Operator chooses to provide zone access through its own systems, rather than through the direct download method via the Centralized Zone Data Service system, what would that process look like?

A: The Registry Operator must choose "SFTP credentials" as their download method. When an end user makes a request, the Registry Operator will approve the request and provide the end user with their SFTP server name and login credentials. The end user must then fetch the data at the specified host by entering the user name and password they were provided with in CZDS.

Before storing the credentials, the CZDS website will encrypt them using each individual user's public key.

Q: How should a Registry Operator deliver their zone file to the CZDS? Should files be sent via an API, uncompressed?

A: The Registry Operator should provide their TSIG key and server address to the CZDS Admin and/or allow transfers (AXFR) from the list of designated ICANN IP addresses. ICANN will perform the transfer and deliver the data in the specified format for direct download via CZDS by the end user.

Q: Are new gTLD registries required to provide zone data data to the system?

A: Yes. A new gTLD registry is required (under Specification 4, Section 2 of the gTLD Registry Agreement) to provide zone data to the end users who request it. New gTLD registries are also required to use the CZDS. They may do so either by allowing ICANN to perform the zone data transfer or they may provide their SFTP server name with credentials and the end user can fetch the data outside the system.

Q: As a future registry can I approve all requests automatically?

A: You can bulk approve all requests at once by selecting all requests and clicking approve, but at the moment you cannot "pre-approve" all requests by default. ICANN will explore adding this auto-approval feature to a future release.

Q: How does a Registry Operator know there is a request pending for them to approve or deny?

A: The Registry Operator has the ability to turn the email notifications feature on or off. So they may be notified every time there is a new request; but if they start to get a high volume, they may turn it off. In this case, they will need to periodically login and check for new requests.

Q: If a Registry Operator must release the zone file prior to signing the Registry Agreement, wouldn't it be better to use "approve" as the default?

A: To be precise, a new Registry Operator is obligated to provide their zone data *after* signing the Registry Agreement, upon delegation, not *prior* to signing the Registry Agreement. An automated pre-approval feature is not currently available.

Q: I don't want to have to log in every day and approve. It would be nice to just pre-approve, or auto approve everything.

A: Registry Operators are not required to login and approve every day, but they are responsible for validating the end users' requests. The 24-hour rule means Registry Operators are required to upload their zone data every 24 hours – and this process can be automated.

Q: Is there any expectation about how quickly registries should be responding to the requests? And is ICANN Compliance going to be checking it?

A: There is no specific turnaround time mandated, but it is expected that registries will respond in a reasonable time. ICANN Contractual Compliance will enforce the requirement to provide access to zone data.

Q: Does the Registry Operator have to approve every request for zone data? For example, can .veryprivate who does not actually agree with the concept of sharing this data by default deny every request?

A: The base new gTLD Registry Agreement requires registries to offer access to their zone files. There are certain conditions under which they can deny requests. Please refer to the Registry Agreement for the conditions in which a Registry Operator can deny a request for zone file access.

Q: If an end user makes multiple requests for data, and the Registry Operator has reviewed and approved at least one of these requests, will the Registry Operator then have the ability to batch approve all other requests from that user?

A: The Registry Operator must approve each individual TLD request from the users. Each approval is good for at least 90 days, or longer if the Registry chooses.

Q: Is there any punishment for *not* granting approvals for access to zone data?

A: Please reference your Registry Agreement for this information.

Q: If a Registry Operator manages multiple TLDs, how many accounts, with separate sets of login credentials, will be required to maintain in order to manage zone data access requests for all of its TLDs?

A: An account on CZDS should represent exactly one individual until another policy is specified. One individual account may operate multiple TLDs. CZDS contains functionality that allows Registry Operator users and Super Managers to be granted authority to enter into terms and conditions on behalf of all the TLDs associated with an assigned Registry. The specific details for each "Super Manager" rely on the business decisions of each Registry. For example a Registry Operator could assign one or many Registry Operator users to manage zone data access for multiple TLDs under their control, depending on their volume.

Q: Can there be more than one registry operator contact?

A: Yes, the Super Manager feature allows a Registry Operator to appoint/add other Registry Operator users to manage their TLD. The Super Manager must confirm that any Registry Operators they appoint have authority to enter into terms and conditions on behalf of the Registry.

Q: As a portfolio of Registries, will one Registry Operator be able to log in and see everything that's attached or will there be multiple logins?

A: Once an individual Registry Operator user is associated with a Registry, they can see all requests for any TLDs they manage using a single login.

Q: If I appoint someone to Super Manager, how can I audit what they've done? For example, what if I login and I have 5 registries and I appoint my admin to go and become this role for the 5 registries and they hit "approve all" and then leave the company?

A: If the designated Registry Operator user leaves the company, the Super Manager may demote them to an end user, rather than a Registry Operator user. They will not be able to approve any more requests, but everything they approved in the past is valid until the terms and conditions expire. If you did not want to approve all requests, you can revoke one or more or all requests so the end users would then have to login and re-request access.

Q: Are there plans to build a sandbox - both SFTP version as well as HTTP version?

A: There are no plans to build a sandbox. Registries may work with the CZDS Admin in order to get set up properly in the system and test their zone file transfers. ICANN will help ensure everything is working properly before the Registry Operator begins approving end user requests.

Q: Will the terms and conditions replace the zone file access agreement?

A: Yes, in fact the language of the terms and conditions was taken directly from current zone file agreements.

Q: Do we get to create our own Terms & Conditions as Registries; and if so do we get to create different versions for each of our TLDs?

A: Section 2.1.1 of Specification 4 to the new gTLD registry agreement specifies that the zone file access agreement "will be standardized, facilitated and administered by a Centralized Zone Data Access Provide."

Q: If a registry detects abuse by a user, what is the process for notifying ICANN?

A: The Registry Operator may revoke a user's access for breach of the access agreement between the user and the Registry Operator. Any inquiries or reports about the CZDS system should be sent to CZDS@icann.org.

Security

Q: "How does CZDS use public key encryption?" What does the initial download key do? The data is ASCII and readable, why should this data be decrypted? Why not use HTTPS for example?

A: HTTPS protects the confidentiality of information, in this case access credentials to zone file servers, from server to client, i.e., between two parties. However, CZDS involves three parties: the registry operator, the zone file user, and the CZDS operator, who acts as an intermediary. Using HTTPS only would protect the information from one party to the other but not the whole chain of communication between two parties through the intermediary. By using public key encryption we can ensure privacy from the registry operator to the zone file user. The CZDS operator (the intermediary) will not have access to the credentials.

The CZDS website generates a 2048-bit RSA key pair (not PGP). Both the private and public keys are generated on the CZDS web server. The private key is sent down the wire via HTTPS so that the user can download it, and then it is destroyed and never written to disk, browser session, or any mechanism that could store the data. The public key is stored with the user's other profile data in the CZDS website. This key pair (the private key stored by each user, and their public key stored on CZDS) is required for decrypting SFTP credentials. HTTPS is not used in order to protect the credentials from being exposed by a third party

CZDS generates a private/public key pair. The *public* key remains on the server (just like a public SSH key remains on a server), and while we don't intend for this key to be revealed publicly, it would a non-critical security event if this public key were to leak into the world somehow. Thus we do store it in the database. Meanwhile, after creation of the key pair, the *private* key is sent to the user during a one-time operation (it is transmitted along with the web page which contains instructions for downloading the key). The user should download this private key and keep it safe. We have a very prominent message advising users to keep the key safe when they view the page containing the key.

If the user navigates away from the page containing their private key without downloading it, they have effectively lost the ability to decrypt credentials, and will have to generate a new private/public key pair, which is easy to do within the CZDS interface. In cases where the user attempts to generate a new key and a public key is already stored in their account, the interface issues a warning before overwriting their existing public key (so they don't accidentally overwrite a valid key).

For decryption, the user supplies their *private* key to the web page containing the encrypted credentials, which are then decrypted using JavaScript, the client-side programming language of all web browsers. The private key is NOT sent to the server during this operation. The decryption happens on each user's computer.

There is a SEPARATE token (for API access) that is *completely unrelated* to the encryption/decryption keys. The API token allows a user to bulk download SFTP credentials, and it has absolutely no part in the decryption process. The API token is an optional feature of CZDS, and some users might not even create one.

Q: If the RSA private key is used to decrypt SFTP credentials, and this API key provides bulk access to these SFTP credentials. Does the API system bypass the RSA encryption of the credentials? or will they (credentials) need to be decrypted out-of-band?"

No. The API does not bypass decryption. No piece of the system can bypass decryption because the credentials are never stored in plaintext, and the private key required for decryption is never stored on the server.

Other

Q: If there is a change in the terms and conditions, what mechanism will be in place to notify the end user? Will there be a consequence to the end user of not acknowledging the change in terms, such as a denial of data?

A: Whenever terms and conditions are changed or updated, the Registry Operator may choose to revoke access for all its current users; so they must login and re-request zone file access under the new terms. Otherwise, the end user will remain under the obligations of the terms and conditions to which they agreed for each individual TLD. It is important to note that revoking access within the CZDS system will not automatically deny access to an end user who is accessing zone data via SFTP. It is under the Registry Operator's control outside of CZDS to change the credentials for users who have been revoked or expired in the system.

Q: What data elements are you providing in CZDS?

A: TLD zone files contain the list of domain names that are registered and active for a given registry. It also contains other DNS records that the registries use depending on the registry services they offer. The format of a zone file is defined in RFC 1035 and subsequent RFCs. The required format of the zone files distributed by the CZDS is actually a subset of these RFCs, as defined by the Zone File Access Advisory Group in their Strategy Proposal, page 9 section 5.1.7 and included in Specification 4 of the Registry Agreement.

Q: Whose IP addresses are you accessing and are you getting them through the DNS system. How does it show up and how are you doing it and how does it map?

A: The IP address of the end user is provided by the user when they create their user profile and is passed to the Registry Operator.

Q: If a user downloads data for a Registry, is the Registry getting history of the people using it?

A: The Registry Operator has a history of requests per user, but not a history of downloads by the user. It may be possible to log direct downloads in the CZDS system, but it is currently not a feature of the system.

Q: Is approval per request to download, or per access for the TLD?

A: Per TLD. Access is granted once to obtain zone data for the TLD for the duration of the terms and conditions – a minimum of 90 days or as long as the Registry chooses. Upon expiration of the terms and conditions, the user must request access again.

Q: We need subject matter experts to get full automation to get this to scale. What about gaming, how often can I download it? It would be great to have one button access.

A: There is a requirement in the terms and conditions limiting how many times an end user can access the zone files; once in a 24 hour period. The files are uploaded once every 24 hours, so if an end user were to download them more than once each day, they would not get any new information. Also, a user is not allowed to perform a direct download in CZDS more than three times per TLD every 24 hours. They will receive an error message if they attempt to do so.