What's New 'Cliff Notes'

ECX Fabric 6.4

ECX Fabric is an advanced interconnection solution that improves performance by providing a direct, private network connection.

ECX Fabric 6.4 is available as of August, 2019.

Japanese Language Translation

The majority of Equinix Japan's ECX Fabric customers are native Japanese companies, in addition to some global multi-national corporations. Use of the English language is limited to these global companies. Native, local companies still prefer to use the Japanese language for communication. In the Asia-Pacific (APAC) region, Tokyo currently has the second highest port count (after Sydney). Therefore, it is believed that the software localization may attract new customers.

Starting with this release, the ECX portal will support Japanese. Additional languages will be included in subsequent releases. Localized (translated) software interfaces and corresponding documentation will help customers use the product to its fullest capabilities and self-serve with online documentation.

ECX Discovery: Account, Profile Exposure and Visibility Settings

Discovery helps customers find each other and increases the usefulness and density of the ECX platform. To do so, we need to have as much information as possible, which will allow users to properly identify who they want to find. Visibility and exposure settings allow Equinix accounts to self-identify about themselves, making them easier to locate.

The enhanced company profiles will include the following:

- Basic information about the company is gleaned from details available in Marketplace as well as company user input (not just the services offered on ECX)

- Various levels of visibility (public vs private)
    - Company is fully-discoverable, meaning it can be contacted even if an ECX service profile is not defined
    - Company is reachable through connection requests to any existing and publicly visible service profile
    - Company is reachable via email, allowing for access requests or help with services; contact information is not visible unless granted by the customers' users
    - Company is not reachable (visible) by other ECX users, under any circumstances, if their profile is marked as private

Port Utilization Statistics

Customer will be able to view traffic statistics for Cloud Exchange Fabric ports. Traffic is measured in megabits per second (Mbps) and represents the amount of bandwidth being consumed between two points at a given time. Customers can now view and analyze the utilization of inbound and outbound traffic of any port and across all services and profiles active on that port. Port statistics will be displayed per physical port, instead of aggregated stats for a LAG port.

List View Phase II Enhanced Connections

List View Phase I involved showing a list view of connection data for customers who have many connections.

ECX aggregators (NSPs and Resellers) as well as CSPs often use data from list view to align their internal costs to the business functions and to view and access usage trends. Therefore, it is imperative that they have access to the data needed to ensure their success on the ECX platform.

The key highlights of phase II of List View include:

- Export capabilities for the Connections list view, including the ability to export all list view data to a .csv file, which allows customers to manipulate the data to meet their individual business needs.
- Additional fields for the Connections list view include Bandwidth tier/Speed, VLAN ID, End User Name, etc.

Display Port Information

ECX Fabric Portal users wishing to obtain physical port information must currently refer to the Equinix Customer Portal (ECP) for this information. Cable ID is the only shared field between the ECXF and ECP. It allows customers to correlate their ports or port LAG groups for the primary physical port.

Some of the capabilities include the basic list view for ports with filtering criteria, the ability to select a port or port LAG group and view all connections on the port(s), sort/filter functionality similar to connections list view, and click the port name/ID, if selected. The information displayed regarding ports includes: port name, metro, speed, port type, LAG yes/no, total bandwidth of all connections on port, and last updated timestamp.

Custom VC Names

With this release, customers can specify a custom Virtual Connection (VC) name based on their own naming nomenclature requirements.

This feature has a few limitations and dependencies including:

- UI/API limitation: Port and VC name cannot exceed 24 characters
- Hyphens, special characters, letters, numbers, and underscores are allowed, but name cannot end with a hyphen
- Any ECXF user with org-level permissions can edit VC names associated with the org
- Custom port names are *not* included

Microsoft ExpressRoute API Migration from Classic to ARM

Microsoft has asked their ExpressRoute partners to migrate from Classic APIs to Azure Resource Manager (ARM) APIs. This API set provides greater functionality and allows for ease of updating bandwidth changes (increases) and link states in ECXF.

Benefits of this migration:

- Better support from Microsoft
- Decrease in Provisioning API call time – resource management "Shadow" is better on the MSFT side
- New API uses push model instead of only pull mechanism

- Redesign in "read" configurations – so if any other CSP changes their API, updates can be implemented more quickly

ECX Fabric SLA Reporting

Currently, we offer Availability SLA (99.999% for dual ports and 99.9% for single port) and Provisioning Interval SLA. To provide assurance to our customers and to help them easily decide which options best fit their needs, ECX Fabric has an updated SLA policy that includes Network Performance parameters (Latency, Packet loss, and Jitter) along with Availability and Port Provisioning interval.

For more details, refer to the updated SLA here.

Full Bandwidth Resizing Capabilities Phase II

Bandwidth Resizing allows the user to change the bandwidth/speed of their connections without the need to delete and recreate the connections. Phase II involves the completion of capabilities not addressed in Phase I.

The following scenarios of the bandwidth resizing for private Layer 2 connections and/or non-integrated CSPs (includes remote connections) will be supported:

a. Customer has a Layer 2 connection between two ports on the ECX Fabric that they own, not to another CSP. They initially ordered 50M but now want to increase to 1G. In this case, no approvals of the bandwidth upgrade would be required, but they would need to acknowledge a billing increase.
b. Customer has a Layer 2 connection to a non-API Integrated private service profile. The owner of the non-integrated service profile needs to approve the bandwidth upgrade first, and the customer would need to acknowledge a billing increase.

Password Expiration and Rotation

This capability requires a new password every 6 months (from the day of the last password creation). The password reset can be applied using either of the following methods:

- Web portal
    - New password must be set at login
    - Other operations not permitted until the new password is set

- API
    - Fields required to indicate new password is needed
    - Other API functions are not processed until the new password is set

Concurrent Session Control

This feature allows a customer organization's Master administrator to limit the number of concurrent portal sessions that users are allowed. By default, this feature sets the concurrent session limit to 3. Once configurability is introduced, the administrator will be allowed to set the limits from 1 to 3 concurrent sessions.

Unless customers can limit the number of concurrent portal sessions for their users, they are unable to manage the risk posed to them by attackers who may hijack their sessions. There are currently no limits on the number of concurrent ECX sessions, so customers do not have the ability to limit sessions without this feature.

IP Whitelisting

This feature allows a Master administrator for an organization to control from where and when domain users can access the portal. This feature adds the ability to restrict organization login to specified source IP addresses.

When customers are unable to restrict when and from where their users can log in, they have much less control over preventing account misuse. Customers are reluctantly forced to allow access to the portal from any location, which is perceived by some customers to be a major security concern.