Por qué la computación en nube nos obliga a replantearnos la resiliencia en el Edge

White Paper 256

Revisión 0

por Kevin Brown y Wendy Torell

Resumen del artículo

El uso de la computación en nube en las grandes empresas crece con rapidez. La mayor dependencia de las aplicaciones basadas en nube obliga a las empresas a replantearse el grado de redundancia de los equipos de la infraestructura física (alimentación, refrigeración y redes) que permanecen en las instalaciones, en el "Edge". En este artículo se describen y evalúan las prácticas de infraestructura física más comunes en la actualidad, se propone un método para analizar la resiliencia necesaria y se abordan buenas prácticas que garanticen que los empleados no perderán la conexión con las aplicaciones críticas de su empresa.

Introducción

El crecimiento incesante del Internet of Things (IoT), el volumen en aumento del tráfico digital y la adopción generalizada de las aplicaciones basadas en nube son tendencias tecnológicas clave que están transformando el panorama de los Data Centers.

Los Data Centers grandes o muy grandes acogen actualmente muchas de las aplicaciones críticas de las grandes empresas que antaño residían en Data Centers internos. Sin embargo, no todas las aplicaciones se han trasladado a la nube, y los motivos son diversos: normativas, cultura empresarial, aplicaciones privadas o latencia, por citar unos pocos.

Como consecuencia de esto, ha surgido lo que en este artículo se ha dado en denominar "entorno de Data Center híbrido". Se trata de un entorno compuesto por una combinación de (1) Data Centers de nube centralizados, (2) Data Centers regionales de volumen medio a grande y (3) Data Centers localizados internos de pequeño volumen. Ver la Figura 1. Lo que antes fuera un Data Center de 1 MW en la sucursal de una empresa ahora puede consistir en un par de racks de equipos IT que ejecutan aplicaciones críticas o conectan la red con la nube. El menor volumen y capacidad de los Data Centers internos no debe entenderse como una reducción de su criticidad. De hecho, lo que se conserva en las instalaciones propias pasa a ser mucho más importante con frecuencia.

En este artículo se describen las prácticas más comunes en los tres tipos de Data Centers mencionados anteriormente, se expone cómo han cambiado las expectativas en materia de operatividad, se propone un método para evaluar el nivel de resiliencia requerido para Data Centers en el Edge (internos) con el fin de cumplir los objetivos de negocio y se recogen buenas prácticas para la implementación de micro Data Centers en el Edge.

Figura 1
Existen tres tipos de Data Centers. Este artículo aborda los Data Centers en el Edge.

Tipos de Data Centers

La nube centralizada fue concebida originalmente para determinados tipos de aplicaciones, como correo electrónico, nóminas y redes sociales. Se trataba de aplicaciones en las que el tiempo no era absolutamente crucial. Pero con el traslado de aplicaciones críticas a la nube, resultó evidente que era preciso resolver cuestiones como la latencia, las limitaciones de ancho de banda, la seguridad y otros requisitos normativos. Basta con pensar en la aplicación en automóviles autónomos. Esta aplicación requiere una enorme cantidad de computación para funcionar correctamente y la latencia no es tolerable, ya que podría causar accidentes. Los hospitales son otra aplicación de importancia vital, por ejemplo cuando se utilizan sensores para recoger datos de pacientes o instrumental quirúrgico que proporciona información en tiempo real durante una operación. La necesidad de aproximar la computación al punto de uso es ineludible.

La distribución de contenidos con un ancho de banda elevado es otra aplicación en la que es beneficioso aproximar el contenido al punto de uso. De este modo se reducen los costes del ancho de bando y se mejora la transmisión.

En muchas empresas suele ser necesario (o preferible) conservar algunas aplicaciones críticas en las instalaciones. Esto proporciona un mayor grado de control que permite satisfacer los requisitos normativos y las necesidades de disponibilidad, aunque en ocasiones estas aplicaciones se replican en la nube por motivos de redundancia.

El White Paper 226 de Schneider Electric, Factores impulsores y ventajas del Edge Computing, detalla estas aplicaciones que nos conducen hacia un ecosistema que incluye más Data Centers regionales y localizados. En este apartado se describe cada uno de estos tipos de Data Centers y se exponen las prácticas típicas empleadas en ellos en lo que se refiere a su infraestructura física.

Data Center centralizado

La importancia de los grandes Data Centers centralizados de varios megavatios de potencia, ya formen parte de la nube o sean propiedad de una empresa, suele percibirse como crítica y, por tanto, se han diseñado pensando en la disponibilidad. Existen buenas prácticas adoptadas desde hace años que garantizan el funcionamiento de estos Data Centers. El personal responsable de las instalaciones y de IT gestiona estos centros con el único objetivo de mantener todos los sistemas funcionando en todo momento. Además, suelen estar diseñados y, en ocasiones, certificados conforme a las normas para el TIER 3 o TIER 4 del Uptime Institute. Los proveedores de Colocation y de nube a menudo pregonan las bondades de estas características de diseño de alta disponibilidad como argumento para el traslado a sus Data Centers.

Algunas buenas prácticas observadas son:

- Sistemas críticos redundantes: Los sistemas de alimentación y refrigeración críticos están diseñados con redundancia (frecuentemente 2N) para evitar tiempos de parada en caso de fallo o por mantenimiento.
- Protección física estricta: Es común encontrar sensores biométricos en las puertas, portales de seguridad (man-traps), videovigilancia y guardias de seguridad a todas horas para garantizar la seguridad de los sistemas y que a estos solo acceda el personal autorizado.
- Racks y filas organizados: Además del cierre bajo llave de los racks, los cables de alimentación y redes están organizados para reducir la probabilidad de errores humanos ocasionados al operar los cables incorrectos, conectar fuentes duales a la misma ruta de alimentación, etc. La distribución de aire está planificada y se emplean elementos como tiras de cepillo y paneles ciegos para reducir los puntos calientes.
- Supervisión: Se instalan sensores y contadores de manera que los sistemas de gestión de infraestructuras para Data Centers (DCIM) y de gestión de edificios (BMS) puedan gestionar, controlar y optimizar todos los sistemas del Data Center.

La Figura 2 muestra los tipos de prácticas de seguridad comunes en estos Data Centers:

Sensores biométricos

Portales de seguridad

Guardias de seguridad

Figura 2
Prácticas de seguridad comunes en Data Centers de nube y colocación centralizados

Data Center regional

Los Data Centers regionales están más próximos a los extremos finales (es decir, donde se crean y usan los datos) y son más pequeños que los grandes Data Centers centralizados. Como se describió anteriormente, la razón de ser de estos Data Centers es aproximar al punto de uso las aplicaciones sensibles a la latencia o el ancho de banda. Están ubicados estratégicamente para satisfacer necesidades de gran volumen. Puede considerárseles un "puente" entre los Data Centers centrales y los Data Centers localizados internos.

De manera similar a los grandes Data Centers centralizados, los Data Centers regionales suelen estar diseñados pensando en la seguridad y la disponibilidad. No es raro encontrar diseños TIER 3 en centros como estos. En estos casos se emplean ocasionalmente diseños prefabricados y existen diseños de referencia disponibles como punto de partida (ver el ejemplo de la Figura 3).

Figura 3
Ejemplo de diseño de referencia como punto de partida para la construcción de Data Centers centralizados o regionales

Data Center localizado

Un Data Center localizado es aquel que comparte ubicación con los usuarios del Data Center. Existen varios términos para denominar a estos Data Centers, como Data Center on-premise o micro Data Center. Su tamaño puede variar desde 1-2 MW hasta tan solo 10-20 kW. A medida que las empresas externalizan aplicaciones de negocio a proveedores de nube o Colocation, estos Data Centers van tendiendo hacia el margen inferior de esa horquilla, y en ocasiones conservan únicamente un par de racks en una sala pequeña o un armario.

En muchos de estos Data Centers compactos modernos, las prácticas de diseño suelen implicar un diseño TIER 1, sin prestar gran atención a la redundancia o la disponibilidad.No es raro encontrar lo siguiente en estos pequeños Data Centers on-premise:

- Falta de seguridad: Las salas con frecuencia no están protegidas; los racks están abiertos (sin puertas)
- Desorganización de los racks: La gestión de cables es un aspecto secundario, por lo que están desordenados, hay obstrucciones al flujo de aire en los racks y hay mayor probabilidad de que se produzca un error humano durante las adiciones, traslados o cambios. Ver la Figura 4.
- No hay redundancia: Los sistemas de alimentación (SAI, distribución) generalmente son 1N, lo que disminuye la disponibilidad y la capacidad de mantenerlos en funcionamiento durante el mantenimiento.
- No disponen de refrigeración específica: Estas pequeñas salas y armarios suelen depender de la climatización del edificio, lo que puede sobrecalentar los equipos.

- No existe supervisión DCIM: Estas salas no acostumbran a estar gestionadas ni cuentan con personal o software específicos para gestionar los equipos y evitar tiempos de parada.

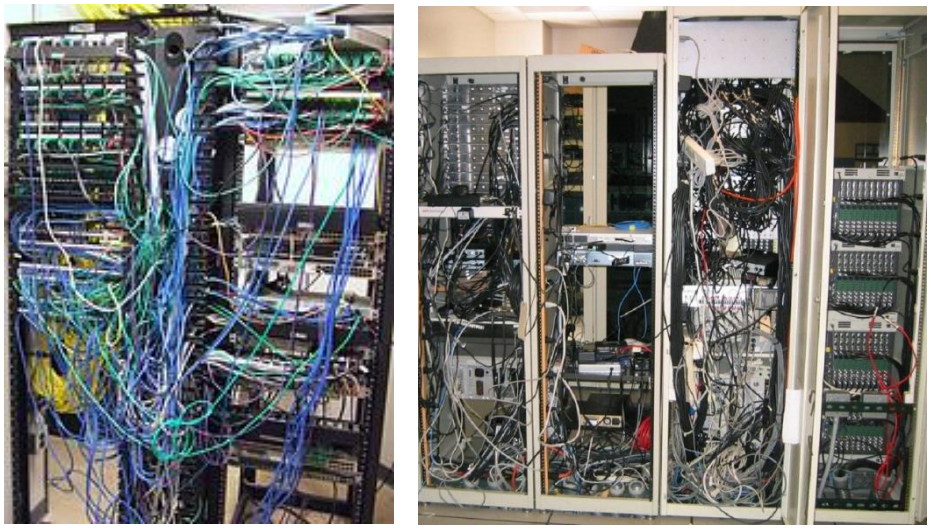

Figura 4
Ejemplos de pequeños Data Centers on-premise con una gestión de cables deficiente y protección escasa.

Estos centros terminan adquiriendo este aspecto porque, cuando las empresas se trasladan a la nube o a centros de Colocation, los pocos racks que quedan se consideran poco importantes. La atención tiende a centrarse en garantizar la disponibilidad de los grandes Data Centers. Sin embargo, se trata de un razonamiento erróneo, ya que a menudo esos racks restantes son tanto o más críticos.

Es suficiente con pensar qué se conserva en las instalaciones: (1) aplicaciones privadas críticas y (2) la conexión de la red con la nube. ¿Qué implicaciones tendría para la productividad no poder acceder a las aplicaciones? Si suponemos que sigue habiendo el mismo número de personas en un centro de trabajo concreto, contar con tan solo un par de racks en las instalaciones incrementa la importancia de cada uno de ellos. Los equipos locales son fundamentales para la conexión con las aplicaciones empresariales de uso cotidiano. Si cada vez más aplicaciones residen en la nube, cuando el punto de acceso falla los empleados no pueden trabajar.

Esto indica que es necesario cambiar el modo de diseñar estos pequeños Data Centers on-premise. Ya no es posible prestar atención exclusivamente a los Data Centers centrales y regionales y, probablemente, deberá dedicarse más atención a los centros localizados porque son, hoy en día, los eslabones más débiles. En este mismo artículo se describen más adelante buenas prácticas que deberían adoptarse en estos centros para garantizar la conectividad y productividad de la empresa.

Una medida de disponibilidad más amplia

En vista de este entorno híbrido interconectado, es importante dar respuesta a la siguiente pregunta: ¿Debemos replantear nuestro modo de hablar acerca de la criticidad y la redundancia? La finalidad de las herramientas que usamos actualmente en el sector de los Data Centers es dotar a un Data Center concreto de la mayor protección posible. Los niveles TIER nos ayudan a diseñar un centro capaz de alcanzar un grado de disponibilidad en particular, es decir, lograr más nueves. Un fallo se define normalmente como una perturbación sufrida por cualquier equipo IT en un Data Center.

Las herramientas y medidas no contemplan la dependencia de múltiples Data Centers, el número de usuarios a los que afecta un fallo, la criticidad de las funciones de negocio afectadas

o la conmutación entre aplicaciones (software) en caso de fallo. Creemos que esto será necesario en el futuro.

El cambio en las expectativas sobre disponibilidad

Las expectativas de los empleados de hoy son diferentes de las que tenían las generaciones pasadas. A medida que las plantillas envejecen y aumenta el porcentaje de millennials, dichas expectativas aumentan en la misma medida. Esta generación ha crecido con una mentalidad de "siempre disponible, siempre conectado" según la cual equipos y sistemas de IT siempre deben estar en funcionamiento. Muestran escasa tolerancia hacia las interrupciones del servicio. La tecnología es importante para ellos, tanto en su vida diaria como en el lugar de trabajo. Tanto es así, que un 82% de los millennials considera que la tecnología del lugar de trabajo influiría en su decisión de aceptar un nuevo empleo.[1]

Si se tiene en cuenta que esta tendencia se mantendrá, resulta crucial buscar formas más holísticas de informar sobre la resiliencia de los Data Centers que brinden la visibilidad necesaria para modificar el diseño con acierto. Como se suele decir, "no se puede gestionar lo que no se puede medir". Las medidas de resiliencia deben evolucionar en respuesta a las necesidades empresariales actuales.

Un enfoque diferente

Un punto de vista diferente sobre la disponibilidad conduce a actuar de forma distinta. La Tabla 1 compara el paradigma actual (obsoleto) con el nuevo paradigma que se considera necesario para actuar del modo requerido.

Tabla 1
Cambio de paradigma sobre los fallos en Data Centers

Paradigma obsoleto	Nuevo paradigma
Orientado al Data Center centralizado	Orientado a entornos híbridos
Un fallo afecta a los equipos IT de un rack	Un fallo afecta a la experiencia del usuario
No incluye centros remotos ni personas/funciones	La criticidad depende del número de empleados a los que afecta y sus funciones laborales

Pensemos en las compañías eléctricas y su visión de la disponibilidad. No prestan atención solo a sus centrales eléctricas y líneas de alta tensión (su "Data Center centralizado"), sino que van podando ramales, mantienen transformadores locales y miden en última instancia su éxito en función de la electricidad que suministran a sus clientes (sus Data Centers en el "Edge"). El sector de los Data Centers debe adoptar este modelo de suministro en el que el Edge es tan importante (si no más) que los Data Centers centralizados.

La disponibilidad de dos sistemas en serie (se depende de que ambos estén disponibles) se calcula como:

$$\text{Disponibilidad}_{\text{sistema}} = \text{Disponibilidad}_1 * \text{Disponibilidad}_2$$

Comencemos pensando en un solo usuario que depende de que su Data Center interno local y el Data Center central estén disponibles o sean productivos. Para calcular la disponibilidad de los Data Centers desde su perspectiva, emplearíamos esta fórmula. Si, por ejemplo, el

[1] http://www.dell.com/learn/us/en/uscorp1/press-releases/2016-07-18-future-workforce-study-provides-key-insights (Último acceso del 31/10/2016)

Data Center central tuviera una disponibilidad del 99,98% (Data Center TIER 3 con 1,6 horas de tiempo de parada) y su Data Center interno tuviera una disponibilidad del 99,67% (Data Center TIER 1, con 28,8 horas de tiempo de parada), el tiempo de parada total desde la perspectiva de ese usuario sería 99,98% * 99,67%, es decir, 99,65% (30,7 horas de tiempo de parada).

Si ahora se asume el punto de vista del director de información (CIO), ¿cómo evaluar el impacto de todo el ecosistema de Data Centers sobre la productividad y la conectividad de la empresa? No todos los Data Centers dependen de que todos los demás Data Centers funcionen para que los empleados puedan trabajar. Por ejemplo, una sucursal de Londres no dependería de la sucursal de California, pero ambas pueden depender de un Data Center central situado en Nueva York.

No todos los Data Centers afectan por igual a la empresa. El número de empleados afectado es un factor. Por ejemplo, un Data Center on-premise con 1.000 empleados puede considerarse más crítico que otro con 10. La Tabla 2 muestra la cantidad de horas-persona de tiempo de parada de un ecosistema de ejemplo compuesto por un Data Center central TIER 3 y 10 Data Centers localizados TIER 1, cada uno con 100 empleados. Resulta evidente, según la tabla, que los Data Centers TIER 1 en el Edge son los que dictan el tiempo de parada global. Cuanto mayor sea el número de centros en el Edge, menor será el número de horas sin fallos en ningún centro.

Tabla 2

Disponibilidad de 10 Data Centers en el Edge y un Data Center central teniendo en cuenta su impacto sobre el personal

Disponibilidad del Data Center						
Descripción	**Disponibilidad**	**Tiempo de parada (hrs)**	**N.º de centros**	**N.º de personas/centro**	**Total de personas afectadas**	**Horas-persona de tiempo de parada/año**
Data Centers Edge Tier 1	99,67%	28,82	10	100	1.000	28.820
Data Center central Tier 3	99,98%	1,58	1	0	1.000	1.580
					Horas-persona de tiempo de parada/año	30.400
					Disponibilidad	99,65%

La tabla anterior refleja un escenario sencillo con dos tipos de Data Centers en el que cada tipo afecta a 1.000 personas. Cuando hay más Data Centers, con grados de disponibilidad y número de personas afectadas diferentes, los cálculos no son tan sencillos. Además, es un cálculo incompleto, ya que excluye la calificación de los centros dependiendo de la función de negocio desarrollada en cada uno. Un centro que ejerce la función de atención al cliente o fabricación probablemente será más crítico que otro lleno de administradores que podrían trabajar remotamente en caso de caída de la red.

Por nuestra parte, proponemos que el mejor método para evaluar todos los centros holísticamente es con un cuadro de puntuación como el ejemplo de la Tabla 3. Dicho cuadro ayudará a los CIO y managers de Data Centers a identificar los centros de mayor prioridad para centrar las mejoras en ellos. El cuadro de puntuación recoge la disponibilidad y los tiempos de parada de cada centro en el entorno de Data Centers híbrido (medido en condiciones ideales) y, sobre todo, una puntuación de criticidad para cada uno. Ver el cuadro lateral para conocer más acerca de justificación científica de las puntuaciones de criticidad[2]. En el caso de los Data Centers, la "gravedad de los efectos de un fallo" se basa en:

- El número de personas afectadas
- La función realizada

Análisis de criticidad

El análisis de criticidad cualitativo es un método demostrado para evaluar riesgos y priorizar las medidas correctivas (también denominado análisis de modos de fallo, efectos y criticidad o FMECA, por sus siglas en inglés). Está bien documentado en publicaciones dedicadas a la ingeniería de fiabilidad. Este análisis incluye la calificación de la gravedad de los efectos de un fallo con un número de prioridad de riesgo (RPN). El RPN está compuesto por 3 factores: (1) gravedad del fallo, (2) probabilidad de aparición y (3) detección del fallo.2

[2] http://www.weibull.com/hotwire/issue46/relbasics46.htm (Último acceso del 31/10/2016)

Es habitual usar una escala del 1 al 5 en la que 1 significa que el impacto para la empresa si el centro sufre un fallo es mínimo y 5 representa el mayor impacto. Aunque se trata de un sistema de puntuación cualitativo, ofrece un método sistemático para el examen de todos los centros del ecosistema de Data Centers de la empresa. Es preciso señalar que cada empresa tendrá sus propias preferencias sobre cómo obtener los valores empleados. La clave reside en disponer de un método coherente para puntuar todos los centros.

En este ejemplo, cinco Data Centers componen un ecosistema hipotético. El tiempo de parada anual de cada uno se multiplica por su puntuación de "gravedad de los efectos de un fallo" para obtener su puntuación ponderada.

A continuación basta con ordenarlos por puntuación y asignar a la más alta la máxima prioridad a la hora de efectuar mejoras en los Data Centers. También puede calcularse el porcentaje de la puntuación para cada centro (como muestra el ejemplo en "Influencia del centro en la puntuación") y asignar la máxima prioridad a los centros con un porcentaje más elevado.

Tabla 3

Ejemplo de cuadro de puntuación para la mejora de entornos de Data Centers híbridos

Tarjeta de puntuación de Data Center					
Nombre del centro	**Disponibilidad**	**Tiempo de parada anual (horas)**	**Gravedad de los efectos del fallo (1-5)***	**Puntuación (ponderada por criticidad)**	**Impacto del centro en la puntuación**
1	99,98%	1,752	2	3,5	0,4%
2	99,20%	70,08	4	280,3	30,0%
3	99,60%	35,04	1	35,0	3,7%
4	98,60%	122,64	5	613,2	65,5%
5	99,98%	1,752	2	3,5	0,4%
			Puntuación de criticidad global:	*935,6*	

Este es un método de paso y repetición. Una vez mejorada la disponibilidad del centro 4 de este ejemplo, otro ascenderá a la cabeza de la lista. De este modo se mejoran los centros de mayor impacto a lo largo de un ciclo de mejora continua.

Una vez implementado un método de obtención de informes adecuado podrá determinarse qué centros precisan mejoras en su diseño para garantizar la máxima productividad y el retorno de la inversión para la empresa. **En la mayoría de los casos, este ejercicio demuestra que los Data Centers del Edge, cuya disponibilidad suele ser menor, tienen mayor importancia para la empresa.**

Buenas prácticas en el Edge

Una vez contamos con las medidas y métodos adecuados, la necesidad de replantear el diseño de los sistemas de Data Centers en el Edge se hace evidente. Las prácticas de diseño típicas en el Edge (como ya se expuso anteriormente) son inadecuadas, dada la naturaleza crítica de estos centros. Las mejoras deben abordar estos aspectos:

- Seguridad física
- Supervisión (DCIM), prácticas operativas, supervisión remota
- Refrigeración y energía redundantes
- Conectividad de red dual

En los apartados siguientes se describen las principales buenas prácticas que deben adoptarse en el Edge. El White Paper 174 de Schneider Electric, *Opciones prácticas para implementar equipos de IT en sucursales y salas de servidores pequeñas*, explica en detalle cómo

llevar a cabo mejoras realistas en materia de alimentación, refrigeración, racks, seguridad física y supervisión en sucursales y salas de servidores pequeñas con una carga de IT máxima de 10 kW.

Un entorno seguro y protegido

Los pequeños Data Centers locales suelen encontrarse en una sala de fácil acceso, como un espacio de oficina compartido. No suelen disponer de un espacio dedicado, por lo que los racks están abiertos y desprotegidos. Esto supone un riesgo para la seguridad, ya sea por actos deliberados o accidentales.

Las buenas prácticas destinadas a reducir estos riesgos incluyen:

- Traslado de los equipos a una sala o armario con cerradura.
- Instalar un control de accesos biométrico o de otra clase.
- En entornos difíciles, alojar los equipos en un armario que los proteja contra incendios, inundaciones, humedad, vandalismo y efectos de los campos electromagnéticos.
- Implementar supervisión ambiental y de seguridad a todas horas, junto con videovigilancia.

La Figura 5 muestra algunos ejemplos de armarios seguros. Suelen estar prefabricados e incorporar toda la infraestructura de apoyo necesaria.

Figura 5
Ejemplos de micro Data Centers de Schneider Electric

Gestión de Data Centers

Es frecuente que el protocolo de gestión y operaciones sea diferente para cada centro situado en el Edge, si es que existe un protocolo. Gestionar cientos o miles de centros en el Edge puede ser lento y costoso, y la disponibilidad de muchos de ellos depende de sistemas de infraestructura compartidos, como grupos electrógenos, cuadros eléctricos y enfriadoras.

Las buenas prácticas destinadas a reducir estos riesgos incluyen:

- Realizar un inventario de los métodos y sistemas de gestión existentes.
- Consolidar todos los equipos de los centros en una plataforma de supervisión centralizada.
- Implementar supervisión remota cuando los recursos son limitados. Ver el White Paper 237, La supervisión remota digital y cómo afecta a las operaciones y el mantenimiento del Data Center, para conocer en detalle cómo la supervisión remota puede contribuir a reducir los tiempos de parada.

Alimentación y refrigeración

Por regla general, en los centros del Edge los sistemas de infraestructura y refrigeración (como SAI y aire acondicionado) no disponen de redundancia. Esto crea numerosos puntos únicos de fallo, además de impedir el mantenimiento de los sistemas durante el funcionamiento. En algunos casos, las salas carecen de refrigeración específica, lo que provoca sobrecalentamiento en los equipos. También es frecuente compartir los sistemas de la infraestructura con el resto de un edificio multiusos, por lo que la disponibilidad del Data Center depende de la disponibilidad de dichos recursos.

Las buenas prácticas destinadas a reducir estos riesgos incluyen:

- Medir temperatura y humedad para conocer el grado de refrigeración necesario (flujo de aire pasivo, flujo de aire activo o refrigeración específica).
- Contemplar rutas de alimentación redundantes para el mantenimiento durante el funcionamiento en centros críticos.
- Procurar que los circuitos críticos estén conectados al grupo electrógeno de emergencia.

La **Figura 6** muestra un ejemplo de micro Data Center TIER 3 compuesto por una solución integrada prefabricada en un armario de 42U individual con SAI y distribución de alimentación redundantes.

Figura 6
Ejemplo de micro Data Center en un solo rack con redundancia integrada

Conectividad de red

Como ya se explicó anteriormente, la conectividad con la nube es crucial para los centros del Edge. Sin embargo, es frecuente que esa conexión la proporcione un solo proveedor de servicios de Internet, lo que representa un punto único de fallo. La organización caótica de los cables en los armarios de red también da lugar a errores humanos.

Las buenas prácticas destinadas a reducir estos riesgos incluyen:

- Contemplar la incorporación de un segundo proveedor de red en centros críticos.
- Organizar los cables de red mediante sistemas para la gestión de cables (canalizaciones, sistemas de enrutamiento, bridas, etc.).

- Etiquetar y codificar por colores los cables de red para evitar errores humanos.

Conclusión

La adopción de la nube anima a un número cada vez mayor de empresas a adoptar entornos de Data Centers híbridos con Data Centers basados en la nube y on-premise (en el Edge). Pese a que los equipos que quedan en la instalación se han visto reducidos en sus dimensiones físicas, ahora son incluso más críticos que antes. Esto se debe a que:

- Al aumentar el número de aplicaciones en la nube, la conectividad con esta es crucial para la continuidad de las operaciones de la empresa.
- Existe una cultura en auge entre los empleados que demanda tecnologías "siempre conectadas" y no tolera las interrupciones ocasionadas por los tiempos de parada.

Por desgracia, en la mayoría de los Data Centers del Edge existentes hoy en día son frecuentes las malas prácticas de diseño que dan lugar a costosos tiempos de parada. Es necesario adoptar un método sistemático para evaluar la disponibilidad de todos los Data Centers de un entorno híbrido para garantizar que se invierte donde el retorno vaya a ser mayor.

Se ha propuesto un método basado en un cuadro de puntuación con el cual ejecutivos y managers pueden estudiar su entorno de forma holística sobre la base del número de personas y funciones de negocio correspondientes a cada Data Center. De esta forma es posible identificar los centros más importantes a los que destinar la inversión.

Los micro Data Centers prefabricados representan un modo simple de crear un entorno seguro y altamente disponible en el Edge. Las buenas prácticas, como el uso de SAI redundantes, un rack protegido y organizado, una gestión de cables correcta y una circulación de aire adecuada, la supervisión remota y la conectividad de red dual proporcionan a los centros de mayor importancia crítica la disponibilidad que requieren.

Acerca de los autores

Kevin Brown es Director de Tecnología de la división de Data Centers de Schneider Electric. Kevin es licenciado en ingeniería mecánica por la Cornell University. Antes de incorporarse a Schneider Electric, Kevin ejerció como Director de Desarrollo de Mercado en Airxchange, un fabricante de componentes y productos de ventilación de recuperación de energía del sector del HVAC. Antes de trabajar en Airxchange, Kevin desempeñó varios puestos de gestión en Schneider Electric, entre los que se incluyen los de Director del Grupo de Desarrollo de Software y Vicepresidente Senior de Soluciones para Data Centers.

Wendy Torell es Analista de Investigación Senior en el Data Center Science Center de Schneider Electric. Su función consiste en investigar las mejores prácticas en el diseño y el funcionamiento de Data Centers, publicar White Papers y artículos y desarrollar TradeOff Tools que ayuden a los clientes a optimizar la disponibilidad, la eficiencia y los costes de sus entornos de Data Centers. También asesora a los clientes sobre la disponibilidad de enfoques científicos y prácticas de diseño para ayudarles a cumplir sus objetivos de Data Centers. Obtuvo su licenciatura en Ingeniería mecánica en el Union College de Schenectady, Nueva York, y su MBA en la Universidad de Rhode Island. Wendy también es ingeniera especializada en fiabilidad acreditada por la ASQ.

Recursos

Cost Advantages of Micro Data Centers
White Paper 223

Impulsores y ventajas del Edge Computing
White Paper 226

La supervisión remota digital y cómo afecta a las operaciones y el mantenimiento del Data Center
White Paper 237

Accede a todos los White Papers
whitepapers.apc.com

Accede a todas las TradeOff Tools™
tools.apc.com

Contacto

Para enviar comentarios y observaciones acerca del contenido de este White Paper:

Data Center Science Center
dcsc@schneider-electric.com

Si eres cliente y tienes dudas concretas sobre tu proyecto de Data Center:

Ponte en contacto con tu representante de Schneider Electric en
www.apc.com/support/contact/index.cfm

© 2016 Schneider Electric. All rights reserved.