White Paper

Dziesięć kroków do optymalnej infrastruktury IT

R&M
Convincing cabling solutions

RITTAL

R&M
Convincing cabling solutions

RITTAL

Spis treści

Streszczenie 3
Wprowadzenie 3
Krok 1: Szafa 5
Krok 2: Zabezpieczenie zasilania prądowego 6
Krok 3: Chłodzenie 7
Krok 4: Bezpieczeństwo 9
Krok 5: Strukturalne okablowanie 10
Krok 6: Zarządzanie biegunowością 12
Krok 7: Monitoring sieci i TAP 12
Krok 8: AIM / DCIM 14
Krok 9: Cykl życia 17
Krok 10: Procesy zarządzania i usługi 18
Literatura 19
O R&M 20
O Rittal 20

Rysunek 1. Szafa Rittal TS IT do zastosowań sieciowych i serwerowych 5
Rysunek 2. Ścieżka zasilania prądowego w centrum danych 6
Rysunek 3. System listw zasilających (PDU) w ramie szafy 7
Rysunek 4. Łańcuch chłodzenia w centrum danych 8
Rysunek 5. Prowadnica powietrza (po lewej stronie poziomu 19'') i kanał powietrzny (po prawej stronie) . 9
Rysunek 6. System monitorowania z czujnikami 9
Rysunek 7. Trzy elastyczne rodzaje urządzeń do okablowania 11
Rysunek 8. Schemat drogi sygnału w module HD TAP 13
Rysunek 9. Typowy link 10GBASE-SR z modułem 50/50 HD TAP w rozdzielni głównej 13
Rysunek 10. Schematyczne zestawienie systemu R&MinteliPhy 15
Rysunek 11. Interfejs DCIM 16
Rysunek 12. Dashboard R&MinteliPhy z prezentacją dostępnych portów 17

Tabela 1: Porównanie pomiędzy architekturą logiczną a strukturyzowaną topologią okablowania 10
Tabela 2: Wartości graniczne długości kanałów dla połączenia 10GBASE-SR z 50/50 TAP 14

R&M
Convincing cabling solutions

RITTAL

Streszczenie

Niniejsza Biała Księga prowadzi w dziesięciu krokach przez całe spektrum infrastruktury fizycznej centrum danych i udziela przy tym instrukcji dotyczących doboru optymalnych komponentów systemowych. Przy czym wymagania klienta stoją na pierwszym miejscu, ponieważ jego pytania są wykorzystywane do wskazania na istotne komponenty systemu i kryteria ich doboru.

W ten sposób szczegółowo potraktowano szafę sieciową i serwerową, przy czym szczególną uwagę poświęcono zabezpieczeniu prądowemu i stosownej klimatyzacji. Ponadto naświetlono aspekty bezpieczeństwa, do których należy także obserwacja i zapis wszystkich ważnych danych infrastruktury − później rejestrowanych, ocenianych i publikowanych ze wsparciem oprogramowania.

Tym samym dokładnie omówiono temat okablowania, przy czym skupiono się na planowaniu strukturalnym oraz zasadach best practice. Ponieważ inwentaryzacja i zarządzanie infrastrukturą fizyczną w wielu instalacjach są prowadzone jeszcze narzędziami „on-board“, jak tabele Excel i grafiki Visio, należy także bliżej przyjrzeć się rozwiązaniom automatycznego zarządzania infrastrukturą (AIM), które umożliwiają aktualną prezentację infrastruktury w każdym momencie.

Jako kolejny krytyczny system do nadzoru sieci przedstawiono Traffic Access Points (TAPs), który pokazuje w jaki sposób najlepiej buduje się otoczenie sieciowe.

Następnie przyjrzano się aspektom serwisowym i usługom w kontekście kompletnego rozwiązania systemowego.

Wprowadzenie

Do podstawowych zadań użytkownika centrum danych należy planowanie centrum danych w zależności od aktualnych i przyszłych wymagań klientów końcowych przedsiębiorstwa. Decydująca dla architektury centrum danych jest kwestia dyspozycyjności, która staje się konieczną przesłanką do zainstalowania rozwiązań redundantnych.

Stanowisko pomocnicze w tym zakresie oferuje Uptime Institute ze swoją klasyfikacją Tier [Ref. 1] czy BSI z określeniem klas dyspozycyjności [Ref. 2, Ref. 3]. Bazując na koncepcji redundancji (np. redundancja modułowa n+1 lub niezależna 2n), należy zaplanować krytyczne ścieżki zasilania prądowego i klimatyzacji. Może to zostać zapoczątkowane przez dwa oddzielne, niezależne od siebie zasilania prądowe nieruchomości i zakończone rozdzielniami prądu A i B w szafie IT.

Drugim, istotnym aspektem jest zaprojektowanie wykorzystania szaf IT. Szafie serwerowej stawiane są inne wymagania niż szafie sieciowej. W związku z tym należy uwzględnić także planowaną rozbudowę w przyszłości przy użyciu aktywnych komponentów (serwer, pamięć, switche). Aktywne urządzenia, które są zamontowane w szafie, określają elektryczną moc pobieraną szafy i konieczną klimatyzację.

Również w związku z celem zastosowania szaf IT należy zaplanować odpowiednie okablowanie. Planiści i użytkownicy centrów danych muszą skrupulatnie i przyszłościowo strukturyzować okablowanie komunikacyjne. Ponieważ także pasywna infrastruktura jest częścią klasyfikacji Tier, musi ona odpowiadać typowym wymaganiom audytu i zgodności stosownie do podstaw i regulacji instrumentów nadzoru. Należy wymienić w szczególności Sarbanes-Oxley Act (SOX) [**Ref. 4**], Basel II [**Ref. 5**], HIPAA [**Ref. 6**] czy PCI DSS [**Ref. 7**].

Dokumentacja towarzysząca do administrowania okablowaniem wspiera pewne planowanie zmian konstrukcyjnych czy rozszerzeń oraz bezproblemowy audyt. Ta dokumentacja może być tworzona i utrzymywana przy pomocy licznych narzędzi – od indywidualnych list Excel do obszernych bazujących na oprogramowaniu narzędzi dokumentacyjnych, jak system AIM. W rezultacie decydujący staje się fakt, czy dokumentacja jest zawsze utrzymywana w aktualnym stanie i odpowiada rzeczywiście zainstalowanemu okablowaniu.

Do podstawowych kwestii należy także rozpatrzenie aspektów bezpieczeństwa planowanego centrum danych. Rozpoczyna się to wraz z nadzorem budynku, pomieszczenia, aż do poszczególnych szaf IT i obejmuje wszystkie elementy bezpieczeństwa fizycznego, jak ochrona antywłamaniowa, ale także oporność ogniowa, wodna, dymowa, obciążenia gruzem, a są to tylko nieliczne aspekty.

W trakcie bieżącej eksploatacji centrum danych należy nadzorować wszystkie zakresy, zbierać informacje i udostępniać je administratorowi systemu na konsoli. Należy przy tym uwzględnić hierarchiczną strukturę centrum danych, już w fazie planowania. Tylko w taki sposób można zapewnić, że odpowiednie czujniki i mechanizmy wykonawcze (jak np. dostęp, temperatura, wilgotność, wycieki, dym) zostaną umiejscowione w odpowiednich miejscach infrastruktury.

W tym kontekście Data Center Infrastructure Management Software musi sprostać różnym potrzebom administratorów IT. Musi być w stanie nadzorować wszystkie komponenty infrastruktury i w razie konieczności wdrażać korekty. Sieć rozdzielonych czujników umożliwia rejestrację i dokumentację wszystkich ważnych parametrów i alarmów oraz ich prezentację w zrozumiałej formie.

W idealnej sytuacji takie oprogramowanie oferuje administratorowi IT także kompletny obraz centrum danych jako zamkniętej jednostki do celów serwisowych. Wytyczną jest tutaj „standard defacto“ ITIL [**Ref. 8**, **Ref. 9**]. Jest to zbiór sprawdzonych metod do zarządzania IT w centrach danych.

Aktualna transformacja sieci centrum danych w chmurę odbywa się w formie wzrastających szerokości pasm w portach switchy i routerów oraz wirtualizacji sieci, serwerów oraz pamięci. Ta transformacja oferuje organizacji IT zdefiniowane i skalowalne systemy do rozbudowania infrastruktury sieciowej w łatwym do oszacowania wymiarze. Podczas gdy „chmura“ i „software-defined-everything“ rozwiązują tradycyjną koncepcję indywidualnych urządzeń sieciowych i ich zarządzania, przepływ danych aplikacji oraz „end-user experience“ stają się coraz trudniejsze w pomiarze i nadzorze. Idealnym rozwiązaniem zapewniającym obszerny wgląd w sieć logiczną jest Traffic Access Point (TAP). Dlatego w niniejszej Białej Księdze wspomina się także o TAP, którego komponenty mają pasywne splittery sygnału optycznego i udostępniają je później stosownym urządzeniom pomiarowym.

Krok 1: Szafa

W serwerowni lub centrum danych znajdują się szafy w znormalizowanym, międzynarodowym standardzie 19‘‘ [**Ref. 10**]. Płyty przednie modułów wsuwnych są wielokrotnością jednostki wysokości (U), która odpowiada 1,75 cala (około 4,445 cm). Szafy 19“ o pełnej wysokości zabudowy mają przeważnie wysokość 42 jednostek wysokości, ze stelażem podłogowym i pokrywą osiągają wysokość około 2 metrów.

W zależności od celu zastosowania zabudowa wewnętrzna takiej szafy jest różna. Już kwestia, czy mają tam zostać umieszczone serwery czy też switche, a więc czy chodzi o szafę serwerową czy też sieciową, wymaga odpowiednich optymalizacji.

Rysunek 1. Szafa Rittal TS IT do zastosowań sieciowych i serwerowych

W systemie szaf IT TS firmy Rittal są oferowane dwie różne możliwości w zakresie standardu 19‘‘. W 19“ szafach TS IT, szyny profilowe 19“ są połączone wspornikami wgłębnymi z szynami obudowy, dzięki czemu szafa przy takim rozmieszczeniu może przyjąć do 1500 kg zabudowy. Umożliwiają to wsporniki wgłębne, które przenoszą obciążenie na ramę szafy.

Alternatywnie można zastosować spawaną ramę montażową 19“, która dzięki rezygnacji z dodatkowych szyn do rozbudowy daje szczególnie duże możliwości okablowania. W przypadku zastosowania tej ramy TS IT jest dopuszczona do całkowitego obciążenia 1 000 kg na płaszczyźnie 19“. Rama montażowa 19“ bazuje na tej samej formie profilu co szyny profilowe i dzięki temu pozwala na maksymalną kompatybilność z akcesoriami.

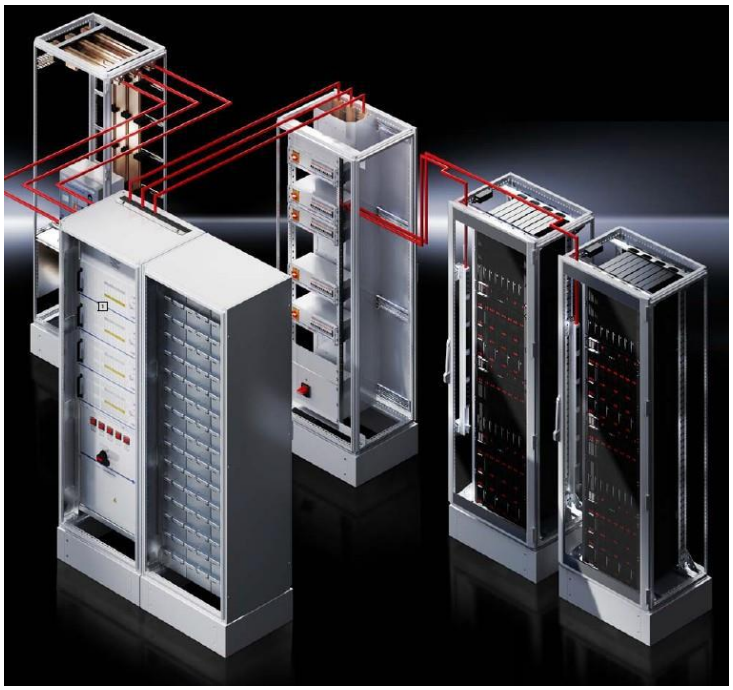
Zasada technologii snap-in została przełożona konsekwentnie na wszystkie akcesoria. Dzięki temu przykładowo można zamontować inteligentną listwę zasilania (Power Distribution Unit – patrz krok 2: Zabezpieczenie zasilania prądowego) firmy Rittal przy użyciu szybkich zamknięć w przestrzeni Zero-U-Space szafy w sposób szybki i nieskomplikowany.

Ponadto w ofercie są szafy wstępnie zmontowane (praktyczne kompletne pakiety), puste szafy do zabudowy indywidualnej, ale także szafy ze stopniem ochrony do zastosowań w surowych warunkach otoczenia. Mimo że standard 19" dla modułów wsuwnych jest właściwe wyznacznikiem, to w przypadku zwykłych szaf serwerowych, wymiary szafy nie są ściśle określone. Zawsze podaje się szerokość i głębokość zewnętrzną szafy. Jedynie wysokość zabudowy wyrażana jest w U. Na rynku dostępna jest np. szafa 42U 600×800 mm. Oznacza to, iż szafa ma do zabudowy 42U oraz szerokość zewnętrzną 600 mm i głębokość zewnętrzną

800 mm. Jeżeli ma być zabudowana przede wszystkim komponentami sieciowymi, odpowiednia jest zazwyczaj szerokość 800 mm, a głębokość 600, 800 lub 1000 mm. Większość działań serwisowych wymaga szerokości 600 i 800 mm oraz głębokości 800, 1000 i 1200 mm.

Krok 2: Zabezpieczenie zasilania prądowego

W zależności od wymagań bezpieczeństwa i koncepcji redundancji, zasilanie jest dostarczane przed jedno lub kilka niezależnych źródeł. W rozdzielni głównej niskiego napięcia prąd jest rozdzielany na różne obszary w ramach infrastruktury IT. Równocześnie główna rozdzielnia niskiego napięcia ma za zadanie przełączanie pomiędzy źródłami prądu − w przypadku redundancji są to zróżnicowane źródła zasilania pierwotnego, a w przypadku usterki rozdzielnia odpowiada za włączanie różnych agregatów zasilania awaryjnego.



Rysunek 2. Ścieżka zasilania prądowego w centrum danych

Do zabezpieczenia i stabilizacji sieci prądowej wtórnej po stronie odbiorników służą bezprzerwowe zasilania prądowe (instalacje UPS). UPS oddziela sieć pierwotną (tzn. przewody dostawcy energii) od zasilania prądowego odbiorników w centrum danych. Nowoczesne systemy UPS przekształcają udostępniany prąd przemienny na prąd stały. Ten prąd stały jest magazynowany w akumulatorze, a następnie po stronie wtórnej (tzn. po stronie odbiorników) zostaje płynnie przekształcony na prąd przemienny. Dodatkowo akumulator jest wykorzystywany w przypadku kompletnego zaniku prądu po stronie pierwotnej.

Po stronie wtórnej, w obszarze odbiorników, znajduje się kolejna podrozdzielnia prądowa dla poszczególnych obszarów centrum danych (wytwarzanie zimna, szeregi szaf IT, oświetlenie, itp.) aż do gniazdka odbiornika końcowego (np. serwera).

Rysunek 3. System listw zasilających (PDU) w ramie szafy

Rodzina produktów Rittal PDU składa się z modeli Basic, Metered, Switched i Managed. To kompletne rozwiązanie systemowe obejmujące rozdział mocy oraz kompleksowe możliwości analizy. Poszczególne zadania PDU są ze sobą powiązane i uzupełniają się. Basic ma tylko funkcję rozdzielczą, Metered mierzy całkowite parametry zużycia, a Switched może dodatkowo załączać poszczególne gniazdka. Managed poza tym dostarcza danych elektrycznych każdego gniazdka z osobna.

Ponadto oferowane są także elastyczne, modułowe systemy PDU, które umożliwiają niewymagające przerw, dokonywane w trakcie eksploatacji zmiany pojedynczych modułów gniazd − np. zmiana z C13 na C19 lub z systemów pasywnych na aktywne.

Krok 3: Chłodzenie

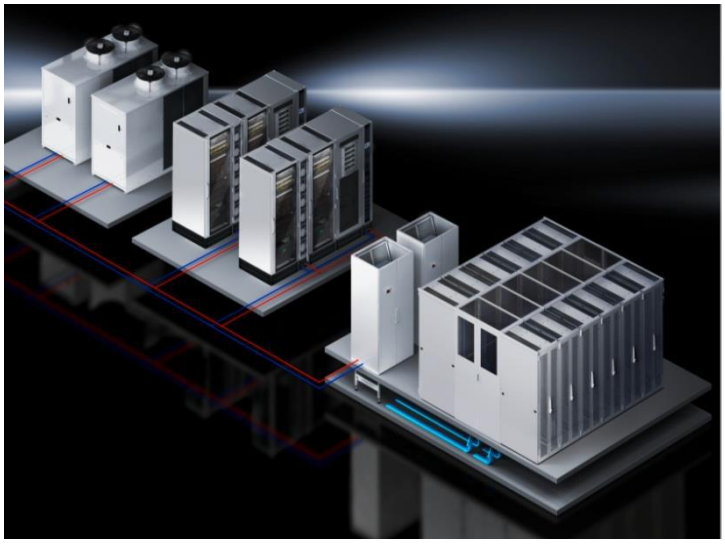
Praktycznie cały prąd dostarczany do centrum danych przekształca się w urządzeniach końcowych w ciepło. Ciepło to musi być z kolei odprowadzone z centrum danych. W tym celu należy w razie potrzeby wytworzyć zimno i rozprowadzić je po serwerowni.

Do wytwarzania zimna stosowane są różne metody. W zależności od wymagań klientów należy tutaj zdecydować o optymalnym zastosowaniu i najkorzystniejszej kombinacji różnych technologii. Chillery wytwarzają zimno z użyciem energii elektrycznej. Często wystarczy jednak schłodzenie ciepłej wody powietrzem zewnętrznym w stopniu odpowiednim do dostarczenia chłodu do serwerowni. Chillery i agregaty chłodzenia swobodnego – przy odpowiednim sterowaniu – mogą się optymalnie uzupełniać.

Szczególną uwagę przy planowaniu centrum danych należy przy tym poświęcić wytarzaniu zimna (rysunek 4), ponieważ przypada na nie większa część kosztów bieżących infrastruktury IT.

W przypadku mniejszego obciążenia cieplnego i instalacji zajmującej większą przestrzeń stosowana jest z reguły klimatyzacja w podłodze technicznej. Poprzez system orurowań schłodzona woda jest transportowana do centrum danych i zasila wymienniki ciepła systemów powietrza obiegowego UKS, Computer Room Air Conditioning (CRAC). CRAC zasysa świeże powietrze z pomieszczenia, schładza je

w wymienniku ciepła i wdmuchuje do uszczelnionej podłogi technicznej. Poprzez perforowane płyty podłogowe zimne powietrze jest kierowane przed szafy IT, po czym zostaje zassane przez urządzenia końcowe.



Rysunek 4. Łańcuch chłodzenia w centrum danych

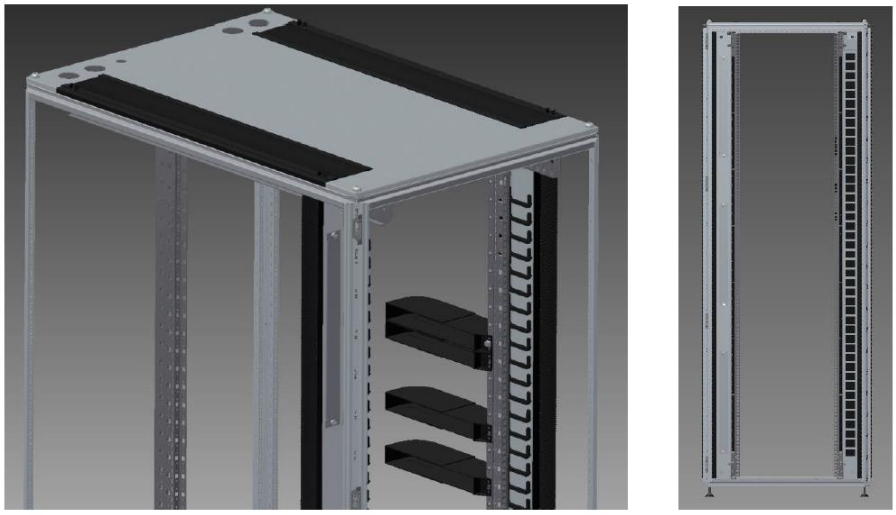
Zaleca się, aby w centrum przetwarzania danych zimne powietrze było odseparowane od ciepłego. W tym celu strefy powietrza pomiędzy dwoma rzędami szaf serwerowych są odizolowane za pomocą dachu oraz drzwi przednich i tylnych. Dodatkowo ciąg ciepły i zimny mogą być wyposażone w czujniki, aby dokładnie kontrolować przebieg temperatury i ciśnienie.

W przypadku wyższych obciążeń cieplnych zaleca się instalowanie urządzeń chłodzących bezpośrednio w szeregu szaf, aby zmniejszyć ilość powietrza do przetłoczenia i osiągnąć wyższą efektywność.

Istnieje także możliwość dostarczenia chłodnej wody do pojedynczej szafy dla serwera wysokowydajnego w aplikacjach high performance (HPC). Urządzenie Liquid Cooling Package (LCP) jest wymiennikiem ciepła, który może zostać zamontowany z boku szafy serwerowej. Chłodne powietrze jest wtedy wdmuchiwane bezpośrednio przed poziom 19“ i zasysane przez serwery. Ciepłe, zużyte powietrze jest ponownie odprowadzane do wymiennika ciepła. Poprzez to efektywne rozwiązanie realizowany jest zamknięty obieg powietrza w szafie. Ważne jest tutaj także, aby wszystkie otwory były uszczelnione panelami zaślepiającymi, co pozwoli uniknąć zawirowania pomiędzy zimnym a ciepłym powietrzem.

Podczas gdy serwer i duża część systemów pamięci są schładzane zgodnie z zasadą chłodzenia „front-to-back“ (tzn. zimne powietrze płynie od przodu przez urządzenie, ciepłe wypływa z tyłu), przy switchach znajdują się także urządzenia z bocznym prowadzeniem powietrza (chłodzenie „left-to-right“), ponieważ strona przednia jest potrzebna dla portów.

Na ilustracji 5 przedstawiono, jak przy pomocy modułu bocznego prowadzenia powietrza, powietrze może być prowadzone do otworów zasysania switcha. W tym rodzaju chłodzenia do szafy jest także doprowadzane zimne powietrze z boku. W tym celu można dodatkowo użyć grodzi poziomu 19", która jest rozszerzana o odpowiednie kanały powietrzne. Dzięki temu można stworzyć kombinację zwykłego chłodzenia „front-to-back“ z chłodzeniem bocznym „left-to-right“ w szafie. Właśnie w przypadku aktywnych komponentów sieciowych ten rodzaj chłodzenia jest bardzo rozpowszechniony.

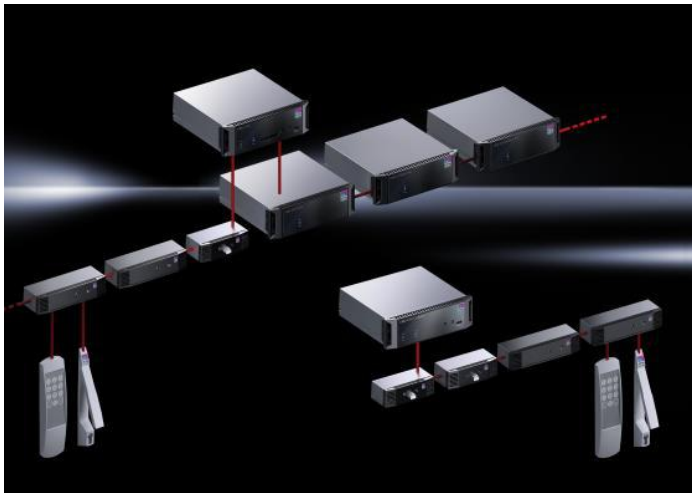


Rysunek 5. Prowadnica powietrza (po lewej stronie poziomu 19'') i kanał powietrzny (po prawej stronie)

Inna możliwość to montaż urządzeń sieciowych w tylnej części przestrzeni 19“. W tym celu zamontowany zostaje także specjalny kanał powietrzny 19“ o wysokości 1U, który dostarcza powietrze z tyłu szafy, gdzie jest ono potrzebne do chłodzenia.

Krok 4: Bezpieczeństwo

Do zadań oprogramowania zarządzania infrastrukturami IT należy odbieranie, ocena i ew. reakcje na wszelkie ważne dla bezpieczeństwa informacje, udostępniane przez czujniki.



Rysunek 6. System monitorowania z czujnikami

Ochrona przed nadużyciem danych jest jednym z najważniejszych czynników bezpieczeństwa w przedsiębiorstwie. System monitoringu Rittal CMC (rysunek 6) reguluje dostęp do szafy i dokumentuje dostęp osób (autoryzacja przy pomocy karty czipowej, transpondera, karty magnetycznej) lub nieuprawnione próby dostępu (czujnik wandalizmu). System monitoringu rejestruje ponadto przy pomocy czujników ważne dla bezpieczeństwa parametry, jak temperatura, wilgotność, dym, strumień powietrza i wyciek. Dodatkowo

rejestruje on wszystkie wartości zużycia urządzeń końcowych. Przy pomocy poszczególnych systemów monitoringu nadrzędne oprogramowanie zarządzania infrastrukturą centrum danych może uzyskać także dostęp do odpowiednich urządzeń końcowych i np. ustawić prędkość obrotową wentylatorów lub moc pomp.

Krok 5: Strukturalne okablowanie

TIA-942-A [**Ref. 13**] i EN 50600-2-4 [**Ref. 13**] oferują wytyczne dotyczące okablowania strukturalnego centrów danych. Aby zaimplementować strukturyzowane rozwiązanie okablowania, zaleca się topologię gwiazdy. Dzięki niej można osiągnąć maksymalną elastyczność sieci. Infrastruktura okablowania powinna zostać zaprojektowana w taki sposób, aby możliwe były działania „Moves“, „Adds“, „Changes“ (MAC), bez niekorzystnego wpływania na samo okablowanie. Działania MAC obejmują konfiguracje sieci, wzrastające lub zmieniające się aplikacje użytkowników i/lub protokoły.

Wymienione standardy mogą być wykorzystywane podczas planowania infrastruktury fizycznej jako środki pomocnicze, jednak nie ma żadnego standardu, do którego można sięgnąć w przypadku infrastruktury logicznej. Architektury logiczne zależą od preferencji klienta, wpływają na nie także producenci urządzeń sieciowych. Generalnie nowoczesne architektury logiczne mogą zostać podzielone na cztery warstwy:

1. Core
2. Spine
3. Leaf
4. Storage

Kluczowe zadanie dla wielu planistów polega teraz na przełożeniu topologii sieci logicznej na strukturę okablowania zgodnie ze standardem TIA-942-A i normą EN 50600-2-4. To przełożenie wpływa na niektóre elementy bezpieczeństwa rozwiązania okablowania, jak liczba szklanych włókien, dobór sprzętu i prowadzenie kabli. Pierwszy krok to przeniesienie stref standardów TIA-942-A lub EN 50600-2-4 (MDA, HDA, ZDA, EDA) na właściwą architekturę logiczną (Spine, Leaf, Storage). Poniższa tabela 1 pokazuje porównanie pomiędzy obydwoma strefami właściwego standardu.

Tabela 1: Porównanie pomiędzy architekturą logiczną a strukturyzowaną topologią okablowania

Architektura logiczna	EN 50600-2-4	TIA 942-A
Core & Spine	Main Distributor	Main Distribution Area (MDA)
Spine	Intermediate Distributor	Horizontal Distribution Are (HDA)
Leaf & Storage	Zone Distributor	Zone Distribution Area (ZDA)
Storage	Equipment Outlet	Equipment Distribution Area (EDA)

Aby przenieść sieć logiczną na strukturyzowaną strukturę okablowania, centrum danych jest dzielone na bazie swojej topologii logicznej. W każdej strefie do okablowania powinno być stosowane rozwiązanie interconnect „Middle of Row“ (MoR). W ramach strefy stosowane są EDA „Top of Rack“ (ToR) Interconnect. EDA obsługują switche, serwery i urządzenia magazynowania danych w każdej szafie, a ZDA z kolei obsługują EDA. Po drugiej stronie ZDA prowadzą okablowanie do szaf rozdzielni głównej i MDA.

Kolejnym krokiem jest określenie liczby wymaganych przewodów optycznych, aby zaimplementować strukturyzowane rozwiązanie okablowania. Aby określić łączną liczbę, należy uwzględnić zarówno redundancję, jak również potrzeby sieci.

Wynikający z tego design będzie prawdopodobnie wymagał większej liczby przewodów optycznych, które muszą zostać poprowadzone w kablach „Trunk“. Kable „Trunk“ w centrum danych są zwykle układane

w podłogach technicznych i w kanałach kablowych ponad szeregami szaf. System prowadzenia kabli w wielu centrach danych ewoluował z biegiem lat i dlatego rzadko występuje w stanie zoptymalizowanym. Przyczyny mogą być następujące:

- kable zostały ułożone długo po instalacji inicjującej, nie przeprowadzono żadnego strukturyzowanego planowania i nie zostały one poprawnie połączone w wiązki.
- dokumentacja ułożonego okablowania nie istnieje lub jest niekompletna. W wyniku tego uszkodzone lub nieużywane kable nie mogą zostać usunięte.

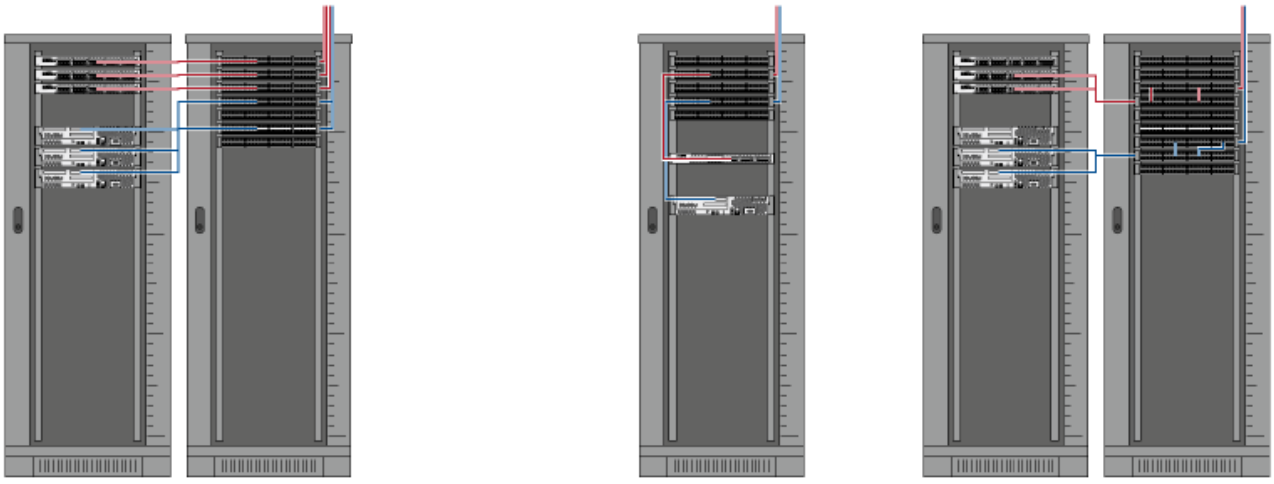
Rozwiązaniem mogą być systemy okablowań jak np. wieloprzewodowe kable z włókien szklanych, które zajmują mniejszą powierzchnię. Również systemy prowadzenia, jak np. konwencjonalne korytka kablowe lub korytka kratkowe, są ciągle zalecane, ponieważ wiążą one te kable i prowadzą przez centrum danych w sposób systematyczny. Tym samym w otoczeniu tworzy się także miejsce na cyrkulację powietrza.

Pozostaje jeszcze ważna kwestia: Co z prowadzeniem kabli? Czy można układać je w podłodze technicznej? Przez jedno złącze urządzenia można zasilać tylko jeden element (np. jeden serwer) w tej samej szafie. W wyniku tego, jeżeli to możliwe, kable nie powinny być wciągane do podłogi technicznej. Zamiast tego wykorzystuje się jedną z poniższych możliwości:

- Trasy lub korytka przebiegające górą.
- Systemy korytek, jak system „Raceway“ R&M, podobnie do konwencjonalnych tras i korytek, jest montowany powyżej szaf.
- Systemy podpodłogowe, jak „Raised Floor Solution“ R&M, zawierające pola prowadzenia kabli w boksie, który jest budowany przed szafami w pustej podłodze.

Centra danych często mają pola rozdzielni i aktywne komponenty sieciowe w szafie lub w dwóch szafach znajdujących się bezpośrednio obok siebie. Takie opcje rozkładu umożliwiają bardziej elastyczne prowadzenie kabli, co pokazują schematy na rysunku 7.

- Z lewej: Podział komponentów na dwie szafy, pojedyncze kable rozrządowe od szafy do szafy.
- Środek: wszystkie komponenty w jednej szafie, łatwe prowadzenie pomiędzy jednostkami wysokości.
- Po prawej: Podział komponentów na dwie szafy, gotowe kable tworzą połączenie pomiędzy szafami czy rozdzielniami a aktywnymi urządzeniami.



Interconnect Combined Cross connect

Rysunek 7. Trzy elastyczne rodzaje urządzeń do okablowania

Następnie należałoby wspomnieć, iż przejrzyste prowadzenie kabli ułatwia instalację, jak również działania „Moves“, „Adds“, „Changes“ (IMAC) w centrum danych. Dlatego okablowanie rozrządcze musi być zaplanowane tak skrupulatnie jak okablowanie instalacyjne.

Krok 6: Zarządzanie biegunowością

Migracja do kolejnej generacji switchy będzie wymagać skrupulatnego planowania liczby włókien szklanych. Stan techniki, jak systemy Ethernet 40G i 100G, wymaga sześciokrotnej lub dwunastokrotnej liczby włókien szklanych na indywidualny link. Systemy Ethernet 40G wykorzystują 12-włóknowy wtyk MTP® jako interfejs optycznego transceivera. Wraz z najnowszą generacją Ethernet 100G, która również stosuje 12-włóknowe wtyki MTP®, liczba włókien szklanych odpowiada tej w systemach 40G [**Ref. 11**].

Zarządzaniem biegunowością nazywamy wykonanie zadania w taki sposób, aby sygnał, który został przesłany z transceivera do portu transmitera (Tx), został odebrany w innym transceiverze na porcie odbiorczym (Rx). Głównym celem biegunowości w infrastrukturze kabli jest zapewnienie, aby w każdym linku porty Tx zostały połączone z portami RX na przeciwnym końcu. Jeżeli biegunowość nie będzie planowana i aktywnie regulowana, należy wykorzystać jedyną pozostającą metodę, jaką jest instalacja kabli Patch.

Aby zapewnić zachowanie biegunowości okablowania strukturalnego, TIA 568-C.0 definiuje trzy typy biegunowości. Każda z tych metod ma jednak wadę, która gdzieś w połączeniu musi zostać usunięta. Oznacza to, iż należy użyć dwóch różnych kabli Patch lub modułów MTP® lub zrealizować skomplikowany projekt „Trunk”.

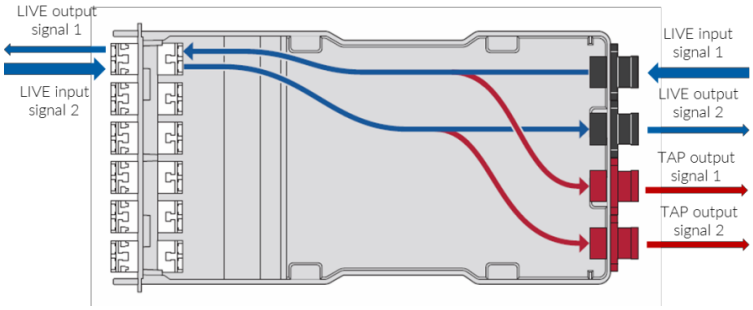
Aby uniknąć tego problemu, firma R&M zaprojektowała rozwiązanie MTP®, które sprytnie realizuje kwestię zarządzania biegunowością – moduł typu S MTP®. Metoda ta wymaga tylko jednego kabla Patch i modułu MTP®. Wykluczenie włókien szklanych sygnałów duplex (jak w przypadku 10GBASE-SR lub 16G Fibre Channel) ma miejsce w gotowym module. Schemat okablowania Trunk i kabli Patch pozostaje taki sam – nawet w przypadku transmisji optycznej równoległej w systemach Ethernet 40/100G.

Krok 7: Monitoring sieci i TAP

W czasie, gdy „chmura” i „software-defined everthing“ nakreślają koncepcje poszczególnych urządzeń i zarządzania urządzeniami, coraz trudniej można zmierzyć i zoptymalizować „traffic“ i „end-user experience“. Menadżerowie sieci centrów danych stoją przed problemem osiągnięcia lepszej widzialności w swoich sieciach, aby w taki sposób stworzyć podstawę do poprawy wydajności aplikacji i zapewnić integralność systemu bezpieczeństwa.

Aby w takim otoczeniu utrzymać obszerną widzialność tak zwane „Traffic Access Points“ (TAPs) to najdokładniejszy, najpewniejszy i najoszczędniejszy rodzaj dostępu do przepływu danych. TAP do pasywny, optyczny splitter, który generuje identyczną kopię sygnału optycznego. Kabel z włókien szklanych z sygnałem wejściowym jest łączony z wejściem splittera. Sygnał splittera jest następnie separowany w wyjściu live, które zostało połączone z urządzeniem odbiorczym „in-band”, i wyjściem monitora, powiązanym z miernikiem „out-of-band“. W związku z faktem, iż jeden TAP wykorzystuje takie splittery w sposób dwukierunkowy, może zostać wykonana kompletna kopia ruchu pomiędzy dwoma urządzeniami.

Rysunek 8 pokazuje schemat drogi sygnału 24-włóknowego modułu Multimode HD TAP. Wtyki MTP® po prawej stronie grafiki zapewniają dwa połączenia dla ruchu live via kabel „Trunk“, i dwa wtyki MTP® (czerwone) dla kanałów TAP. Są one na końcu połączone via Trunk MTP® lub kabel Fanout MTP®-LC z urządzeniami monitorującymi. Lewa strona ilustracji pokazuje przód modułu z jego dwunastoma portami LC-Duplex do podłączenia kabli Patch.



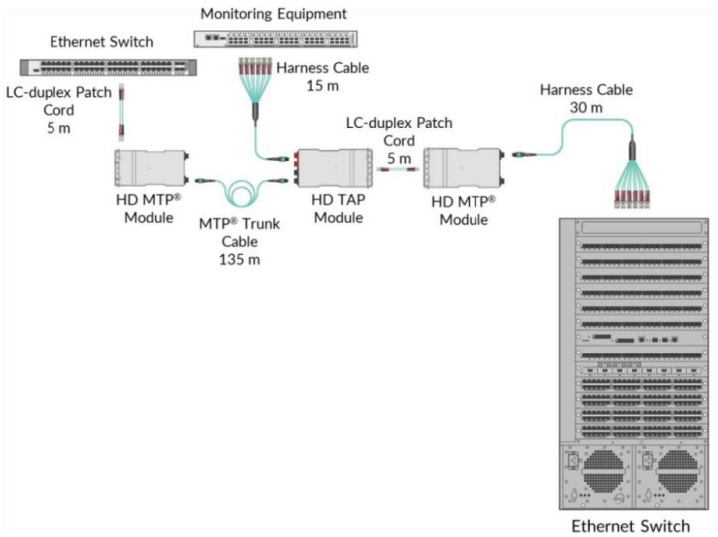
Rysunek 8. Schemat drogi sygnału w module HD TAP

Stopień w jakim splitter rozdziela wchodzący sygnał optyczny pomiędzy obydwoma wyjściami, nazywany jest stosunkiem splittera. Standardy TAP R&M wykorzystują stosunek 50/50. Oznacza to, iż 50% sygnału wejściowego kierowane jest do wyjścia live, a 50% do wyjścia TAP. Z definicji stosunek splittera 50/50 ma tłumienie 3dB. Łączna tłumienność połączenia musi zostać skalkulowana skrupulatnie z uwzględnieniem tego dodatkowego tłumienia.

Oprócz strat spowodowanych podziałem sygnału optycznego, splitter nie wytwarza żadnej latencji lub innej zmiany sygnału. Wydajność zostaje zachowana – niezależnie od faktu, czy miernik jest podłączony do wyjścia TAP, czy też nie. Pozwala to na instalowanie modułu HD TAP bez późniejszych zmartwień, ponieważ nie wymaga on konserwacji.

Wyjścia TAP są zwykle umiejscawiane pomiędzy dwoma dowolnymi urządzeniami sieciowymi, jak switche, routery i urządzenia „Storage", aby zapewnić dostęp do monitoringu personelowi sieciowemu i zabezpieczającemu. Ponieważ wyjścia TAP są stosowane już podczas pierwotnej instalacji jako część infrastruktury, eliminuje się „downtime", które byłyby konieczne w przypadku doraźnej instalacji podczas bieżącej pracy centrum danych. Aby skompletować „Visibility-Eco-System", urządzenia TAP są łączone z urządzeniami monitorującymi, łącznie z odbiornikami, osprzętem i oprogramowaniem analizującym.

Mimo iż urządzenia TAP w planowaniu połączenia nie są rozważane jako typowe źródła tłumienia, mogą jednak zostać uwzględnione w budżecie na tych samych warunkach co łączniki wtykowe lub moduły konwersji.



Rysunek 9. Typowy link 10GBASE-SR z modułem 50/50 HD TAP w rozdzielni głównej

Dołączenie TAP 50/50 prowadzi do dodatkowego tłumienia 3,9 dB, zarówno w ścieżce live-traffic, jak i w ścieżce TAP. To dodatkowe tłumienie redukuje możliwe długości kanałów 10GBASE-SR. W takiej konfiguracji topologicznej kanał live traffic (który prowadzi ze switcha core do switcha agregacji) składa się z modułu HD TAP, dwóch modułów HD MTP®, dwóch kabli Patch LC-Duplex, jednego kabla MTP®-LC-Duplex. Łączna długość wynosi tutaj 175 metrów. Wszystkie kable bazują na włóknach OM4.

Krótka ścieżka TAP (przebiegająca od switcha core do urządzenia monitorującego) składa się z modułu HD TAPl, modułu HD MTP®, dwóch kabli zespolonych MTP®-LC-Duplex i kabla Patch LC-Duplex – o długości łącznej 50 metrów. Długa ścieżka TAP (łącząca tutaj switch agregacji z urządzeniem monitorującym) składa się z TAP, modułu HD MTP®, kabla Patch LC-Duplex, kabla Trunk MTP® i kabla zespolonego MTP®-LC-Duplex. Tym samym długość całkowita wynosi 155 metrów.

Powstające w wyniku tego tłumienie jest teraz obliczane dla każdej z tych ścieżek i może być porównane z maksymalnymi długościami kanałów. Maksymalne długości dla powyższego przykładu (rysunek 9) przedstawiono w tabeli 2.

Tłumienia ścieżki live od lewej do prawej to:

0,35 dB + 3,9 dB + 0,35 dB = 4,6 dB

Tłumienia krótkiej ścieżki TAP od lewej do prawej to:

3,9 dB + 0,35 dB = 4,25 dB

I tłumienia długiej ścieżki TAP od lewej do prawej to:

0,35 dB + 3,9 dB = 4,25 dB

Tabela 2: Wartości graniczne długości kanałów dla połączenia 10GBASE-SR z 50/50 TAP

Ścieżka sygnałowa	Tłumienność [dB]	Maksymalna długość kanału [m]	
		OM3	OM4
Ścieżka live	4,60	170 m	230 m
Krótka ścieżka TAP	4,25	190 m	260 m
Długa ścieżka TAP	4,25	190 m	260 m

Jeżeli teraz porówna się maksymalne długości kanałów z topologią na ilustracji 9, można zauważyć, iż budżet mocy wspiera wszystkie ścieżki – wymaganiem jest stosowanie włókien OM4.

Krok 8: AIM / DCIM

Ponieważ średnia powierzchnia centrum danych wynosi dzisiaj pomiędzy 1 000 a 2 500 m² i zawiera często tysiące portów sieciowych, ręczne kontrolowanie kabli nie jest praktyczną opcją. Mimo to ciągle wielu menedżerów sieci prowadzi swoją inwentaryzację i zarządzania infrastrukturą fizyczną przy pomocy tabel Excela – lub nawet na papierze czy w formie fiszek. Nie ma możliwości przeprowadzenia planów rozwojowych i analizy ryzyka na takiej podstawie, nie mówiąc o zachowaniu standardów i sprawdzonych metod sterowania bezpieczeństwem danych czy o dyspozycyjności.

Systemy zautomatyzowanego zarządzania infrastrukturą (AIM) oferują natomiast rozwiązanie polegające na udostępnieniu funkcji do ilustrowania, zarządzania, analizy i planowania okablowania oraz szaf. Systemy te

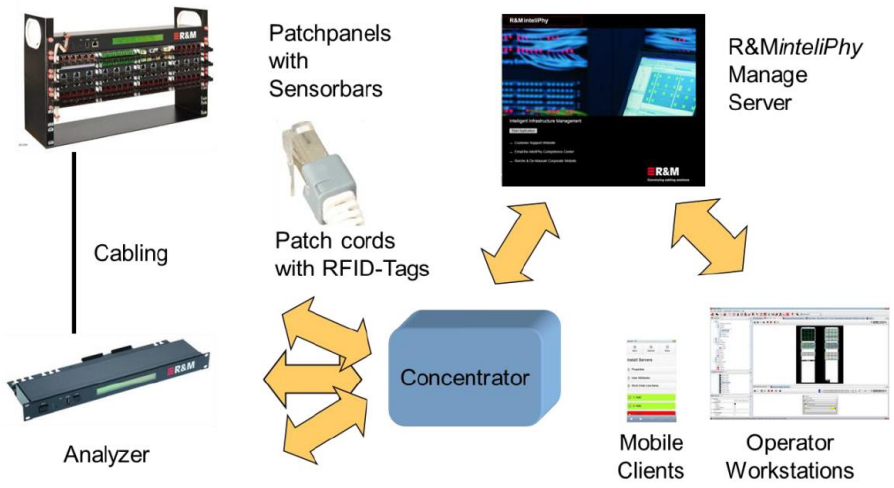
poprawiają efektywność operacyjną i ułatwiają bieżące zarządzanie infrastrukturą pasywną. Zintegrowane systemy hardware i software automatycznie wykrywają wetknięcia i wypięcia kabla, a także dokumentują infrastrukturę okablowania, podobnie jak podłączone urządzenie. Umożliwia to bieżące, płynne zarządzanie infrastrukturą, jak również wymianę danych z „Data Center Infrastructure Management“ (DCIM), „Building Management“ (BMS), zarządzanie usługami IT (ITSM), „Asset Lifecycle“, systemami zarządzania bezpieczeństwem i innymi platformami. Dzięki temu można nadzorować wszystkie elementy i zarządzać nimi przy pomocy jednego uniwersalnego narzędzia software.

Cała infrastruktura jest przedstawiona w spójnej bazie danych i oferuje tym samym precyzyjne informacje o aktualnym stanie i przyszłych wymaganiach centrum danych w czasie rzeczywistym. Jednolita baza danych pokazuje zalety w kilku specyficznych obszarach. Administracja infrastrukturą okablowania i połączonymi urządzeniami jest ciągle aktualna. Ponadto jest to podstawą efektywnych procesów i systemów zarządzania instalacjami oraz infrastrukturą IT. Stałe Asset Tracking i Asset Management w zestawieniu z powiadomieniami „Event“ wspierają bezpieczeństwo sieci fizycznej.

Przeprowadzone niedawno przez R&M badanie w jednej z europejskich instalacji pokazało, iż można zredukować czas potrzebny do śledzenia i dokumentowania okablowania o 85%. Po wdrożeniu R&M*inteliPhy*, AIM bazującego na RFID, aktualność i brak błędów można było zwiększyć do prawie 100%.

R&MinteliPhy może być każdej chwili doposażony do platformy R&Ms HD. Cały system jest przedstawiony na rysunku 10 i składa się z:

- analizatora
- serwera zarządzania R&MinteliPhy
- klientów zarządzania R&MinteliPhy
- etykiet RFID
- listwy czujnikowej



Rysunek 10. Schematyczne zestawienie systemu R&MinteliPhy

Analizator jest połączony ze wszystkimi listwami czujników za pośrednictwem systemu kabli „Daisy-Chain“. Odczytuje listwy czujników i dostarcza do serwera aktualnych danych o wszelkich stanach połączeń. Analizator jest umieszczony w szafie 19" lub, w celu oszczędności miejsca, na szynach nośnych wewnątrz szafy. Analizator może pokryć kilka szaf i maksymalnie 2 000 portów. Jeżeli w jednej instalacji występuje kilka analizatorów, stosowany jest koncentrator, który łączy informacje wszystkich analizatorów i komunikuje się z serwerem.

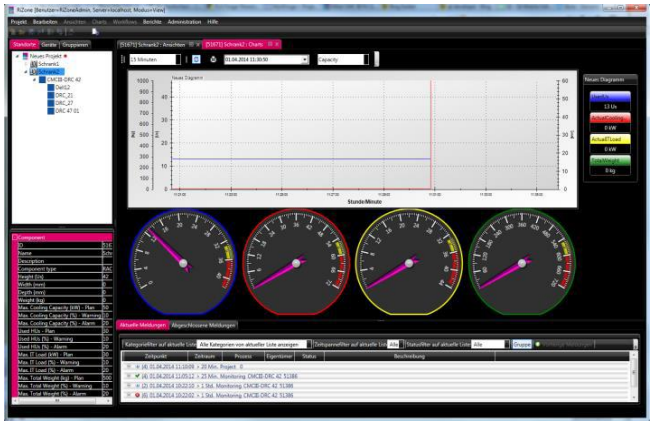
W centralnej pozycji serwer zarządzania R&MinteliPhy kontroluje i nadzoruje całą infrastrukturę w czasie rzeczywistym. Ponadto oferuje on kompletny dobór narzędzi administracyjnych i automatyzacyjnych. Systemy innych oferentów mogą być łatwo integrowane przy pomocy standaryzowanych złączy. Serwer jest niezależny od systemu operacyjnego, dostępny także jako obsługa bazująca na „chmurze".

Przeglądarka lub smartfon to wszystko, co jest potrzebne do użytkowania R&MinteliPhy. Graficzny interfejs użytkownika umożliwia intuicyjną obsługę i pozwala na dostęp do wszystkich funkcji – od automatycznego routingu do planowania czasowego projektów MAC. Z systemem może pracować jednocześnie kilku użytkowników.

Etykieta RFID na wtyku zawiera wszystkie informacje konieczne do jednoznacznego zidentyfikowania kabli i wtyków. Dający się doposażyć plastikowy klip z etykietą pasuje do wszystkich wtyków włókien szklanych i miedzianych R&M. Listwa czujnikowa wykrywa bezstykowo etykietę RFID. Może być dodatkowo umieszczona na wszystkich panelach Patch kompatybilnych z R&MinteliPhy. Listwa rejestruje wtyki i połączenia. Diody LED wskazują status roboczy portów i wspierają technika podczas prowadzenia kabli.

Zainstalowany proces AIM umożliwia organizacjom optymalizację procesów ekonomicznych z perspektywy infrastruktury. Eliminuje „zapomniane" moce i ułatwia analizę „end-to-end". W wyniku tego umożliwia sprawne zarządzanie infrastrukturą i wspiera analizy prognozujące. Ponieważ w systemie AIM cała infrastruktura przedstawiona jest w spójnej bazie danych, zapytania dotyczące wolnych portów w szafach sieciowych lub dostępnego miejsca w szafie mogą być opracowane w szybki i łatwy sposób.

Oprogramowanie DCIM (Data Center Infrastructure Management) optymalnie wspiera administratora IT w pokonywaniu wyzwań wynikających z obserwacji pojedynczych urządzeń i sterowania nimi, aż po całościową optymalizację centrum danych z uwzględnieniem ekonomicznych warunków brzegowych oraz w aspektów dyspozycyjności i bezpieczeństwa.



Rysunek 11. Interfejs DCIM

Oprogramowanie DCIM kontroluje wszystkie komponenty infrastruktury IT konieczne do bezpiecznej eksploatacji serwerów, pamięci masowych, routerów oraz switchy i steruje nimi. Należą tutaj:

- zasilanie i zabezpieczenie prądowe
- wytwarzanie i rozdział zimna
- nadzór pomieszczenia i szaf
- bezpieczeństwo centrum danych
- zarządzanie aktywami i mocami
- wydajność i zużycie energii

Dla administratora IT decydujące jest współgranie poszczególnych obszarów jego centrum danych, jak fizyczna infrastruktura IT, sieć, serwer, systemy budynkowe, systemy ERP, a to tylko niektóre z nich. Oprogramowanie DCIM oferuje inteligentne interfejsy, aby udostępnić całościowy, transparentny widok.

Oprogramowanie DCIM może przedstawiać łączne użycie (kW/h, €, CO2) i efektywność centrum danych przy pomocy analizy trendów. Pozwala na definiowanie obwodów regulacyjnych w celu ustawienia optymalnego punktu roboczego centrum danych zgodnie z potrzebami. Tym samym umożliwia stałą optymalizację infrastruktury IT w celu osiągnięcia ciągłych potencjałów redukcji kosztów.

Z reguły systemy DCIM oferują standardowy interfejs SNMP umożliwiający połączenie tych nadrzędnych systemów zarządzania siecią i serwerami.

Krok 9: Cykl życia

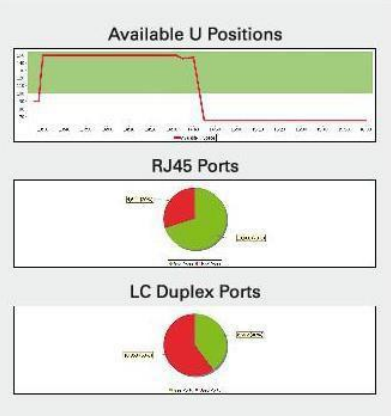
Dla menedżera IT użytkowa żywotność serwera wynosi od czterech do pięciu lat. Umowa outsourcingowa na zarządzanie dla przedsiębiorstwa usługowego IT może trwać cztery lata. Rozwijające się technologie i popyt na nowe aplikacje biznesowe tworzą w serwerze, switchach, pamięciach i okablowaniu warunki dla coraz to nowszych modyfikacji z częstotliwością zapierającą dech w piersiach.

W takim właśnie otoczeniu łatwo o utratę przeglądu aktywów IT. Miały już miejsce przypadki, gdzie przedsiębiorstwo płaciło za przedłużone umowy serwisowe na serwery fizyczne, które nie były już częścią centrum danych. Bez systemu zarządzania infrastrukturą urządzenie może zostać usunięte z szafy i przeleżeć wiele miesięcy w magazynie bez możliwości wyśledzenia tego zdarzenia.

Równocześnie typowe centrum danych posiada żywotność od 10 do 15 lat. Architektury okablowań mają nieprawdopodobny wpływ na zdolność centrum danych do dopasowania się do zmian architektury, wzrastających wymagań co do pasm oraz działań „moves“, „adds“ i „changes“.

Standardy okablowań są ciągle pisane i opracowywane na nowo. Na przykład standardy ITA są sprawdzane co pięć lat i mogą być wtedy potwierdzone, odrzucone lub opracowane na nowo. Standardy ISO/IEC są pisane na czas żywotności dziesięciu lat. Standardy użytkowe IEEE są definiowane i regularnie sprawdzane z perspektywy aktualnej przydatności produktów. Są one odniesieniem dla aktualnych standardów okablowania.

Jeżeli architektury okablowania nie zostaną wybrane poprawnie na początku, rozwój wymagań technicznych co do sieci może zmusić do przedwczesnej wymiany architektury. Przezorne działy IT powinny w związku z tym przygotować swoje sieci na przyszłość, integrując do swoich strategii wsparcie dla Ethernet 40/100 Gigabit Ethernet i systemu AIM.



Rysunek 12. Dashboard R&MinteliPhy z prezentacją dostępnych portów

Często pomijanym aspektem jest przechowywanie zapasowych kabli Patch. Sensowne jest natomiast utrzymywanie zapasu małej liczby kabli Patch o różnych długościach. Doświadczenie pokazuje, że najczęściej stosowane są kable o długościach 1, 2 i 5 metrów. Typy zależą od specyficznej aplikacji, ale generalnie obowiązuje zasada, iż magazyn powinien posiadać kable RJ45 kat. 6A i kable OM4 LC-Duplex, w razie potrzeby nawet 12-włóknowe kable Patch OM4 MTP®.

Korzystając z funkcji analizy systemu AIM, można użyć precyzyjnej rejestracji zainstalowanego okablowania i używanych portów, aby przewidzieć, jakie kable i w jakiej ilości należy przechowywać w magazynie.

Na końcu cyklu życia „Product Lifecycle Management“ powinien określić te urządzenia, które wpływają negatywnie na optymalną pracę, np. poprzez zbyt wysokie koszty energii, i dlatego powinny zostać wyłączone z obiegu. Wiek urządzenia może być również parametrem, ponieważ koszty konserwacji wzrastają na końcu cyklu życia.

Krok 10: Procesy zarządzania i usługi

Aby zawsze utrzymywać centrum danych w normalnym stanie roboczym, należy stworzyć obszerny plan konserwacji dla wszystkich elementów infrastruktury. Ten plan konserwacji musi być zgodny z planem każdego dostawcy i należy go zaimplementować do systemu DCIM lub AIM. Poniższy ustęp powinien pokazać indywidualne procesy zarządzania, które są pokrywane przez te systemy.

„Operation Management“ musi implementować infrastrukturę monitoringu, aby oferować informacje o stanie i awariach elementów infrastruktury centrum danych. Dodatkowe dane do użycia w procesach zarządzania, jak zarządzanie energią, cyklem życia, mocami i dyspozycyjnością mogą być rejestrowane przez czujniki i zapisywane w centralnej bazie danych.

„Incident Management“ jest kluczem do usuwania błędów i do powrotu do normalnego stanu roboczego. Systemy te przetwarzają komunikaty o awariach. Zdarzenia są rejestrowane, nadzorowane, rozwiązywane lub zamykane. Do celów analizy w zarządzaniu dyspozycyjnością protokołowanie zdarzeń rejestruje początek i koniec każdej awarii. Zaleca się, aby każde zdarzenie i reakcja zostały ponownie przeanalizowane. Należy to uczynić w miarę możliwości również tam, gdzie dokonano zmian, aby zapobiec powracającym usterkom i poprawić reakcję.

Oczywiście celem „Incident Management“ jest zminimalizowanie czasu awarii. Dlatego dla każdego zdarzenia należy zgłosić Key Performance Indicator (KPI) „średni czas naprawy“ (MTTR). Tam, gdzie występuje umowa na świadczenie usług (Service Level Agreement, SLA), dotrzymanie SLA jest rozszerzonym KPI dla „Incident Management“.

Procesy, jak „Incident Management“, zarządzanie mocami, zarządzanie energią lub zarządzanie dyspozycyjnością mogą zainicjować zmiany dla procesu Change Management. W przypadku rejestracji autor „Changes“ powinien poinformować o zmianie i pożądanych efektach. „Changes“ powinny zostać zaplanowane w taki sposób, aby umożliwić właściwą koordynację. Czasy awarii należy zminimalizować poprzez koordynację „Changes“ z identycznym systemem. Należy udostępnić zasoby, aby upewnić się, iż można pomyślnie zakończyć „Change“. Dlatego Change Management musi udostępnić dla Operation Mangement informacje o planowanych „Changes“ [**Ref. 12**].

Zasada ta jest możliwa tylko wtedy, gdy wszystkie „Changes“ są nadzorowane, a autor jest informowany automatycznie o statusie – w szczególności, jeżeli „Change“ zakończono sukcesem.

Końcowym aspektem jest zarządzanie mocami, które powinno optymalizować wykorzystanie udostępnionych mocy centrum danych. Ponadto należy monitorować, analizować, zarządzać mocami infrastruktury centrum danych.

W zarządzaniu mocami należy rozróżnić trzy kategorie:

a) moc całkowita centrum danych: maksymalna moc zaprojektowana podczas kompletnej budowy;

b) moc udostępniona: moc rzeczywiście zainstalowanej infrastruktury;

c) moc wykorzystywana: moc wykorzystywana w rzeczywistości przez IT i instalację.

W idealnej sytuacji płynności zarządzania mocami nie ogranicza się do poziomu pomieszczenia, ale umożliwia nawet zarządzanie warstwą pojedynczych jednostek wysokości − lub jeszcze lepiej: na poziomie portu.

Literatura

Ref. 1 Uptime Institute, Tier Definition: http://uptimeinstitute.com/TierCertification

Ref. 2 BSI: klasy dyspozycyjności: https://www.bsi.bund.de/DE/Themen/weitereThemen/Hochverfuegbarkeit/HVKompendium/hvkompendium_node.html

Ref. 3 BITKOM Leitfaden betriebssicheres Rechenzentrum: http://www.bitkom.org/files/documents/131213_Leitfaden_BRZ_web.pdf

Ref. 4 Sarbanes-Oxley Act legal text: http://www.sec.gov/about/laws/soa2002.pdf

Ref. 5 Basel II: http://www.bis.org/publ/bcbs107.pdf

Ref. 6 Health Insurance Portability and Accountability Act legal text: http://www.gpo.gov/fdsys/pkg/CRPT-104hrpt736/pdf/CRPT-104hrpt736.pdf

Ref. 7 Payment Card Industry Data Security Standard: http://www.bis.org/publ/bcbs107.pdf

Ref. 8 ITIL Best Practices: https://www.axelos.com/itil

Ref. 9 IT Service Management: ISO/IEC 20000 Norm: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=60329

Ref. 10 19“ Standard: EIA 310-D, IEC 60297 und DIN 41494 SC48D

Ref. 11 IEEE 802.3bm: http://standards.ieee.org/about/get/802/802.3.html

Ref. 12 EN 50600-2-6: Management and operational information

Ref. 13 ANSI / TIA-942-A: Telecommunications Infrastructure Standard for Data Centers

Ref. 14 EN 50600-2-4: Telecommunications cabling infrastructure

O R&M

Jako działający w skali światowej dostawca systemów Connectivity dla wydajnych i wysokiej jakości sieci centrów danych, firma R&M oferuje kompletne doradztwo i skrojone na miarę rozwiązania. Użytkownik infrastruktury i Operation Manager są tym samym w stanie zbudować i użytkować elastyczne, niezawodne i niedrogie oraz zorientowane biznesowo infrastruktury IT.

Niniejszy zaczątek od firmy R&M – «Convincing Cabling Solutions» – umożliwia organizacjom kompletne planowanie swoich sieci biurowych, centrów danych oraz sieci dostępu, ich optymalizację i łączenie. Systemy kontroli infrastruktury, włókna szklanego i miedzi w przedsiębiorstwie dbają o bezkompromisową jakość produktu spełniającego również najwyższe standardy. Ponieważ nawet produkty najwyższej jakości nie mogą jednak zagwarantować bezbłędnej pracy, R&M tworzy wspólnie z klientami gruntowną analizę na podstawie strukturalnego i zorientowanego na przyszłość projektu sieci fizycznej, spełniającego perfekcyjnie ich wymagania.

Szukasz kompetentnego doradztwa i usług utrzymujących stale wysoki poziom? W takim przypadku firma R&M jest właściwym partnerem do rozmów.

Szczegółowe informacje można znaleźć pod adresem www.rdm.com.

O Rittal

Firma Rittal z siedzibą w Herborn w Hesji to wiodący światowy dostawca systemowy szaf sterowniczych, systemów rozdziału prądu, klimatyzacji, infrastruktury IT oraz oprogramowania i serwisu. Rozwiązania systemowe Rittal stosowane są w niemal wszystkich branżach, głównie w przemyśle motoryzacyjnym, energetyce, budownictwie maszyn i urządzeń oraz w branży informatyczno-komunikacyjnej (ICT). Zatrudniając 10 000 pracowników i posiadając 58 spółek córek, Rittal działa na całym świecie.

Do szerokiego spektrum zastosowań należą rozwiązania infrastruktury dla modułowych i energooszczędnych centrów przetwarzania danych, od innowacyjnych koncepcji bezpieczeństwa, aż po fizyczne zabezpieczanie danych i systemów. Wiodący dostawcy oprogramowania, firmy Eplan i Cideon, uzupełniają łańcuch wartości o interdyscyplinarne rozwiązania inżynieryjne, a Rittal dzięki swoim systemom automatyzacji (w skrócie RAS) – o rozwiązania automatyzacji budowy aparatury sterowniczej i rozdzielczej.

Rittal został założony w roku 1961 i jest największym przedsiębiorstwem prowadzonej przez właściciela Friedhelm Loh Group. Grupa jest obecna na całym świecie z 18 fabrykami i 78 międzynarodowymi spółkami córkami. Cała grupa zatrudnia ponad 11 500 pracowników, a jej obroty w 2014 roku wyniosły ok. 2,2 miliarda euro. W 2015 r. to rodzinne przedsiębiorstwo zostało wyróżnione po raz siódmy z rzędu tytułem najlepszego pracodawcy w Niemczech.

Pozostałe informacje są dostępne na stronie www.rittal.com i www.friedhelm-loh-group.com.