Krycí list dokumentu	
Název:	**Specifikace systémových prací** - Projekt redesign infrastruktury WAN/LAN (BC107882)
Typ:	**Doplnění projektu - Prováděcí projekt „Redesign infrastruktury WAN/LAN“**
Určení:	IT
Adresát:	Povodí Labe, státní podnik, Víta Nejedlého 951/8, 500 03 Hradec Králové
Verze:	1.1
Datum vydání:	2.11.2022
Autoři:	Richard Vodička, richard.vodicka@autocont.cz
Správce:	Petr Křivka, petr.krivka@autocont.cz

Pozor dokument obsahuje důvěrné informace!

Tato verze neobsahuje hesla!

Společnost AUTOCONT a.s. tímto uděluje oprávnění pro Povodí Labe, státní podnik k reprodukování, uchovávání nebo přenášení jakýmkoli způsobem včetně elektronického, magnetického, fotografického či jiného záznamu dokumentu Doplnění projektu – Prováděcí projekt „Redesign infrastruktury WAN/LAN“.

_____

Bc. Petr Křivka, Manažer realizačních týmů, AUTOCONT a.s.

Etapa 1.1 (Centrální lokalita)

Systémové práce budou obsahovat minimálně:

Náhrada FortiGate 600D

- Demontáž stávající infrastruktury
- Montáž nových prvků do racku, L2 propojení, HA
- Aktualizace firmware, nastavení lokálních účtů atd.
- Registrace podpory zařízení na stránkách výrobce
- Základní konfigurace IP adresy, NTP, SNMP, logování atd.
- Základní zabezpečení konfiguračního rozhraní (ACL, bezpečné protokoly apod.)
- Migrace konfigurace ze všech stávajících VDOM na nové prvky
- Otestování, testy redundance
- Zaškolení

Síťové přepínače LAN

- Demontáž stávající infrastruktury
- Montáž nových prvků do racku, L2 propojení, sestohování
- Aktualizace firmware, nastavení lokálních účtů, atd.
- Registrace podpory zařízení na stránkách výrobce
- Základní konfigurace IP adresy, NTP, SNMP, logování atd.
- Základní zabezpečení konfiguračního rozhraní (ACL, bezpečné protokoly apod.)
- L3 konfigurace tzn. kompletní migraci stávající konfigurace na nové páteřní prvky (z Cisco)
- L2 konfigurace, přiřazení VLAN, STP, LACP atd.
- Propojení se stávající LAN/WAN
- Konfigurace datacentrových přepínačů pro připojení serverové infrastruktury
- Konfigurace QoS
- Otestování, testy redundance
- Integrace do stávajícího dohledového systému PRTG
- Zaškolení

VMware – výměna 10GE síťových karet (4x ESX server DELL 2x server Lenovo SR590)

- Práce budou prováděny vždy pouze na jednom ESX serveru tak, aby nedošlo k výpadku produkčních serverů
- Zdokumentování stávající síťové konfigurace každého ESXi (Teaming, Security, VLAN, VM portgroup, atd.)
- Upgrade firmware serverů
- Výměna stávajících 1GE karet za 1x 10GE 2-port SFP+
- L2 propojení – redundance DC přepínačů
- Rekonfigurace vSwitch networking na provoz po 10GE (Teaming, Security, vLAN, VM portgroup, atd.).
- Konfigurace NIC Teaming na Active/Standby:
    - Management Network a vMotion = 1. vmnic active, 2.vmnic standby
    - VM Network= 2. vmnic active, 1. vmnic standby
- Označení propojovacích kabelů
- Dokumentaci skutečného nastavení VMware vSphere prostředí
- Akceptační testy SPoF - **Test odolnosti LAN Management Network**
    - Na Management IP testovaného ESXI serveru bude z management stanice puštěn příkaz ping
    - Bude odpojen 1. 10GE port zvoleného ESXi serveru.
    - Test se považuje za úspěšný tehdy:
        - Testovaný ESX stále odpovídá na ping.

        - V managementu vCenter je testovaný ESXi server stále dostupný a zároveň GUI identifikuje odpojenou vmnic.
        - Po opětovném zapojení 10GE portu testovaný ESXi stále odpovídá na ping a v GUI identifikuje zapojení.
    - Stejný postup aplikován pro druhý 10GE port
- Akceptační testy SPoF - **Test odolnosti LAN při vMotion**
    - Bude odpojen 1. 10GE port na zdrojovém ESXi serveru.
    - Test se považuje za úspěšný tehdy:
        - vMotion referenční VM na jiný ESXI server bude dokončena.
        - Po opětovném zapojení odpojeného 10GE portu a kontrole stavu ve vCenter bude stejný postup aplikován pro druhý 10GE port.
- Akceptační testy SPoF - **Test odolnosti LAN VM Network**
    - Z referenční VM bude spuštěn příkaz ping na default GW a současně na jinou domluvenou IP adresu v jiném segmentu.
    - Bude provedeno fyzické odpojení 1. 10GE portu ESX serveru, na kterém aktuálně běží referenční VM.
    - Test se považuje za úspěšný tehdy:
        - Ping z referenční VM stále pokračuje. Při failover a failback může dojít k výpadku v řádu jednotek ping.
        - Po opětovném zapojení odpojeného 10GE portu referenční VM stále odpovídá na ping.
    - Po opětovném zapojení odpojeného 10GE portu se stejný postup opakuje i u druhého 10GE LAN portu.
    - · Test bude proveden na všech VM portgroup.
- Akceptační testy budou provedeny postupně na všech ESXi hostech.

SW pro centrální management (FortiManager)
- Instalace SW Appliance do prostředí VMware
- Aktualizace, základní nastavení (IP adresa, management atd.)
- Registrace podpory zařízení na stránkách výrobce
- Připojení všech podporovaných zařízení v LAN/WAN infrastruktuře zadavatele
- Vytvoření balíčků politik pro jednotlivé skupiny zařízení
- Synchronizace balíčků politik s registrovanými zařízeními
- Vytvoření vzorové template pro zjednodušení konfigurace
- Vytvoření vzorové template pro upgrade firmware
- Nastavení monitoringu provozu všech SD-WAN sítí a VPN
- Otestování komunikace
- Zaškolení

Etapa 1.2 a 1.3 (Koncové lokality)

Systémové práce budou obsahovat minimálně:

- Demontáž stávající infrastruktury
- Montáž nových prvků do racku, L2 propojení, sestohování
- Aktualizace firmware, nastavení lokálních účtů atd.
- Základní konfigurace IP adresy, NTP, SNMP, logování atd.
- Základní zabezpečení konfiguračního rozhraní (ACL, bezpečné protokoly apod.)
- L2 konfigurace, přiřazení VLAN migrace a doplnění stávající konfigurace, STP, LACP atd.
- Propojení se stávající LAN/WAN
- Konfigurace QoS
- Otestování, testy redundance
- Integrace do stávajícího dohledového systému PRTG
- Zaškolení

Etapa 2.1 (FortiNAC)

Systémové práce budou obsahovat minimálně:

- Instalace SW Appliance do prostředí VMware
- Aktualizace, základní nastavení (IP adresa, management, certifikáty atd.)
- Registrace podpory zařízení na stránkách výrobce
- Integrace do stávající Microsoft domény
- Integrace do Fortinet Security Fabric
- Konfigurace parametrů síťové visibility
- Konfigurace parametrů klasifikace koncových zařízení
- Konfigurace L3 typu síťového nasazení
- Konfigurace izolované karanténní VLAN
- Připojení všech podporovaných zařízení v LAN/WAN infrastruktuře zadavatele
- Konfigurace pravidel zařízení dle klasifikace
- Konfigurace bezpečnostních politik pro přístup do sítě zadavatele
- Konfigurace a instalace FortiNAC agent na vzorové koncové zařízení
- Konfigurace vzorového portálu pro registraci hostů do sítě zadavatele
- Konfigurace vzorového reportu
- Otestování komunikace
- Zaškolení

Etapa 2.2 (WiFi)

Systémové práce budou obsahovat minimálně:

- Montáž bezdrátových přístupových bodů
- Aktualizace firmware, nastavení lokálních účtů apod.
- Registrace podpory zařízení na stránkách výrobce
- Základní konfigurace IP adresy, NTP, SNMP, logování atd.
- Konfigurace SSID, bezpečnostní politiky, mapování VLAN, autentizace atd.
- Integrace s řešením FortiNAC
- Otestování, testy redundance
- Integrace do stávajícího dohledového systému PRTG
- Zaškolení

Etapa 3 (FortiClient)

Systémové práce budou obsahovat minimálně:

- Instalace SW Appliance na definovaný server v doméně zadavatele
- Aktualizace, základní nastavení management console
- Registrace podpory zařízení na stránkách výrobce
- Integrace do stávající Microsoft domény
- Integrace do Fortinet Security Fabric
- Konfigurace skupin pro správu koncových zařízení
- Konfigurace profilů koncových zařízení, min. pro zařízení v síti a mimo síť zadavatele
- Konfigurace politiky a detekce On-fabric pravidel
- Konfigurace a instalace FortiClient na vzorové koncové zařízení
- Konfigurace a integrace Zero Trust tagů, konfigurace pravidel FortiGate dle těchto tagů
- Otestování komunikace
- Zaškolení