Metodologie rozwiązywania problemów

17.6.1

Podstawowe metody rozwiązywania problemów

W poprzednich dwóch tematach dowiedziałeś się o niektórych narzędziach i poleceniach, których można użyć do identyfikacji obszarów problemowych w sieci. Jest to ważna część rozwiązywania problemów. Istnieje wiele sposobów rozwiązywania problemu z siecią. W tym temacie opisano uporządkowany proces rozwiązywania problemów, który może pomóc stać się lepszym administratorem sieci. Dostarcza również kilka dodatkowych poleceń, które pomogą Ci rozwiązać problemy. Problemy natury sieciowej mogą być proste lub złożone, mogą również wynikać z połączenia problemów sprzętowych, programowych i aspektów związanych z łącznością. Technicy muszą być w stanie przeanalizować problem i ustalić przyczynę błędu, zanim będą mogli rozwiązać problem z siecią. Proces ten jest nazywany procesem rozwiązywania problemów.

Powszechnie stosowana i skuteczna metodologia rozwiązywania problemów opiera się na metodzie naukowej.

Tabela pokazuje sześć głównych kroków procesu rozwiązywania problemów.

Krok	Opis
Krok 1. Identyfikacja problemu	• To pierwszy krok w procesie rozwiązywania problemów. • Chociaż narzędzia mogą być używane w tym kroku, rozmowa z użytkownikiem jest często bardzo pomocna.

Krok	Opis
Krok 2. Postawienie hipotezy na temat prawdopodobnej usterki	• Po zidentyfikowaniu problemu spróbuj ustalić hipotezę w zakresie prawdopodobnej przyczyny. • Ten krok często daje więcej niż kilka prawdopodobnych przyczyn problemu.
Krok 3. Sprawdzanie hipotezy w celu ustalenia przyczyny	• Na podstawie prawdopodobnych przyczyn przetestuj swoje hipotezy, aby określić, która jest przyczyną problemu. • Technik często stosuje szybką procedurę, aby przetestować i sprawdzić, czy rozwiązało to problem? • Jeśli szybka procedura nie rozwiąże problemu, może być konieczne badanie problemu dalej w celu ustalenia właściwej przyczyny.
Krok 4. Stworzenie planu działania i wdrożenia rozwiązania	Po ustaleniu właściwej przyczyny problemu należy ustalić planu działania w celu rozwiązania problemu i zaimplementowania rozwiązania.
Krok 5. Weryfikacja rozwiązania i wdrożenie środków zapobiegawczych	• Po usunięciu problemu sprawdź pełną funkcjonalność. • W stosownych przypadkach należy zastosować środki zapobiegawcze.
Krok 6. Dokumentowanie spostrzeżeń, działań i wyników	• W końcowym etapie procesu rozwiązywania problemu, należy udokumentować swoje spostrzeżenia, działania i wyniki. • Jest to bardzo ważne dla przyszłego wykorzystania.

Aby ocenić problem, określ ile urządzeń w sieci ma problem. Jeśli jest to problem z jednym urządzeniem w sieci, zacznij proces rozwiązywania problemu od tego urządzenia. Jeśli problem występuje ze wszystkimi urządzeniami w sieci, rozpocznij proces rozwiązywania problemów na urządzeniu, do którego podłączone są wszystkie inne urządzenia. Powinieneś stworzyć logiczną i spójną metodę, aby zdiagnozować problemy sieci poprzez eliminowanie jednego problemu na raz.

17.6.2

Rozwiązywać lub eskalować?

W niektórych sytuacjach natychmiastowe rozwiązanie problemu może nie być możliwe. Problem powinien zostać eskalowany, gdy wymaga podjęcia decyzji kierownika, pewnej konkretnej wiedzy lub poziomu dostępu do sieci niedostępnego dla technika rozwiązującego problem.

Na przykład, po zidentyfikowaniu problemów technik stwierdza, że moduł routera powinien zostać wymieniony. Ten problem powinien zostać eskalowany do zatwierdzenia przez menedżera. Menedżer może być zmuszony do eskalacji problemu, ponieważ może wymagać zatwierdzenia działu finansowego przed zakupem nowego modułu.

Polityka firmy powinna jasno określać, kiedy i jak technik powinien eskalować problem.

17.6.3

Polecenie debug

Procesy systemu operacyjnego, protokoły, mechanizmy i zdarzenia generują komunikaty do komunikowania się ich stanu. Komunikaty te mogą dostarczyć cennych informacji podczas rozwiązywania problemów lub weryfikacji operacji systemu. Polecenie **debug** IOS pozwala administratorowi wyświetlać te wiadomości w czasie rzeczywistym do analizy. Jest to bardzo ważne narzędzie do monitorowania zdarzeń na urządzeniu Cisco IOS.

Wszystkie polecenia **debug** są wprowadzane w uprzywilejowanym trybie EXEC. Cisco IOS pozwala na zawężenie wyjścia **debug** w celu ograniczenia tylko do odpowiedniej funkcji lub informacji. Jest to ważne, ponieważ dane wyjściowe debugowania mają wysoki priorytet w procesie procesora i mogą uniemożliwić korzystanie z systemu. Z tego powodu używaj poleceń **debug** tylko do rozwiązywania określonych problemów.

Na przykład, aby monitorować stan komunikatów ICMP w routerze Cisco, użyj **debug ip icmp**, jak pokazano w przykładzie.

```
R1# debug ip icmp
ICMP packet debugging is on
R1#
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

```
R1#
*Aug 20 14:18:59.605: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
*Aug 20 14:18:59.606: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
*Aug 20 14:18:59.608: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
*Aug 20 14:18:59.609: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
*Aug 20 14:18:59.611: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
R1#
```

Aby wyświetlić krótki opis wszystkich opcji poleceń debugowania, użyj polecenia **debug ?** w trybie uprzywilejowanym EXEC w wierszu poleceń.

Aby wyłączyć określoną funkcję debugowania, dodaj słowo kluczowe **no** przed poleceniem **debug**:

```
Router# no debug ip icmp
```

Alternatywnie możesz wprowadzić formę polecenia **undebug** w trybie uprzywilejowanym EXEC:

```
Router# undebug ip icmp
```

Aby wyłączyć wszystkie aktywne polecenia debugowania jednocześnie, użyj polecenia **undebug all**:

```
Router# undebug all
```

Bądź ostrożny przy użyciu jakiegoś polecenia **debug**. Polecenia takie jak **debug all** i **debug ip packet** generują znaczną ilość danych wyjściowych i mogą korzystać z dużej części zasobów systemowych. Router może być tak zajęty wyświetlaniem komunikatów **debug**, że nie będzie miał wystarczającej mocy obliczeniowej, aby wykonywać swoje funkcje sieciowe, a nawet słuchać poleceń, aby wyłączyć debugowanie. Z tego powodu korzystanie z tych opcji poleceń nie jest zalecane i należy ich unikać.

17.6.4

Polecenie terminal monitor

Połączenia w celu uzyskania dostępu do interfejsu wiersza komend IOS można ustanowić na dwa sposoby:

- **Lokalnie** - Połączenia lokalne (tj. połączenie konsoli) wymagają fizycznego dostępu do portu konsoli routera lub przełącznika za pomocą kabla rollover.
- **Zdalnie** – połączenia zdalne wymagają użycia Telnet lub SSH w celu nawiązania połączenia ze skonfigurowanym urządzeniem IP.

Niektóre wiadomości IOS są automatycznie wyświetlane na połączeniu konsoli, ale nie na zdalnym połączeniu. Na przykład, wyjście **debug** jest domyślnie wyświetlane na połączeniach konsoli. Jednak wyjście **debug** nie jest automatycznie wyświetlane na połączeniach zdalnych. Dzieje się tak dlatego, że wyjście **debug** to komunikaty dziennika, które nie mogą być wyświetlane na liniach vty.

W poniższym wyjściu na przykład, użytkownik ustanowił zdalne połączenie za pomocą Telnet z R2 do R1. Następnie użytkownik wydał polecenie **debug ip icmp**. Jednak polecenie **debug** nie wyświetliło danych wyjściowych.

```
R2# telnet 209.165.200.225
Trying 209.165.200.225 ... Open
 Authorized access only!
User Access Verification
Password:
R1> enable
Password:
R1# debug ip icmp
ICMP packet debugging is on
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
! No debug output displayed>
```

Aby wyświetlić komunikaty dziennika (logi) na terminalu (konsoli wirtualnej), użyj polecenia **terminal monitor** uprzywilejowanego trybu EXEC. Aby zatrzymać wyświetlanie komunikatów na terminalu, użyj polecenia **terminal no monitor** uprzywilejowanego trybu EXEC.

Na przykład zwróć uwagę na to, jak polecenie **terminal monitor** zostało teraz wprowadzone, a polecenie **ping** wyświetla wynik **debug**.

```
R1#  terminal monitor
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
*Aug 20 16:03:49.735: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.737: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.738: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.740: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.741: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
R1# no debug ip icmp
ICMP packet debugging is off
R1#
```

Uwaga:Zamiarem polecenia **debug** jest przechwytywanie danych na żywo przez krótki okres czasu (tj. kilka sekund do minuty) . Zawsze wyłączaj **debug** , gdy nie jest wymagany.

17.6.5

Sprawdź, czy zrozumiałeś - Metodologia rozwiązywania

problemów

Sprawdź swoją wiedzę na temat metod rozwiązywania problemów, wybierając NAJLEPSZĄ odpowiedź na poniższe pytania.

1. Technik rozwiązuje problem z siecią i właśnie ustalił hipotezę prawdopodobnych przyczyn. Jaki będzie następny krok w procesie rozwiązywania problemów?

- ( ) Dokumentowanie spostrzeżeń, działań i wyników
- ( ) Stworzenie planu działania i wdrożenia rozwiązania
- ( ) Identyfikacja problemu
- ( ) Sprawdzanie hipotezy w celu ustalenia przyczyny
- ( ) Weryfikacja rozwiązania i wdrożenie środków zapobiegawczych

2. Technik rozwiązuje problem z siecią. Po rozwiązaniu problemu technik stwierdza, że przełącznik powinien zostać wymieniony. Co następnie technik powinien zrobić?

- ( ) Wyślij e-mail wszystkich użytkowników, aby dać im znać, że przełącznik zostanie wymieniony.
- ( ) Eskaluj zgłoszenie problemów do menedżera, aby zatwierdzić wymianę.
- ( ) Kup nowy przełącznik i wymień wadliwy.
- ( ) Rozwiąż problem.

3. Technik używa polecenia **debug ip icmp** uprzywilejowanego trybu EXEC do przechwytywania wyjścia routera na żywo. Które polecenia zatrzymają działanie polecenia **debug** na routerze Cisco? (Wybierz dwie odpowiedzi).

- [ ] **debug ip icmp off**
- [ ] **no debug debug ip icmp**

- [ ] **no debug ip icmp**
- [ ] **undebug all**
- [ ] **undebug debug ip icmp**

4. Technik ustanowił zdalne połączenie z routerem R1 aby obserwować wyjście **debug**. Technik wydaje polecenie **debug ip icmp**, a następnie wykonuje ping na odległy cel. Jednak nie jest wyświetlany żaden wynik. Które polecenie musiałby wprowadzić technik, aby wyświetlać komunikaty dziennika (logi) na zdalnym połączeniu?

- ( ) **monitor debug output**
- ( ) **monitor terminal**
- ( ) **terminal monitor**
- ( ) **terminal monitor debug**

Sprawdź

Rozwiązanie

Resetuj

17.5 Polecenia na komputerze i w systemie IOS
17.7 Przykłady rozwiązywania problemów