

Pratiche leader di Cisco: Operazioni di gestione di Cisco IOS

Sommario

[Riassunto](#)

[Introduzione](#)

[Panoramica](#)

[Obiettivi](#)

[Destinatari](#)

[Prerequisiti](#)

[Creazione di una strategia operativa per la gestione di Cisco IOS](#)

[Identificazione dei deliverable](#)

[Identificazione delle misure principali dei dispositivi](#)

[Definizione di ruoli e responsabilità](#)

[Identificazione delle aree di competenza necessarie](#)

[Identificazione dei principali collaboratori](#)

[Identificazione delle responsabilità](#)

[Risorse di impostazione budget](#)

[Seguire una procedura ottimale per il processo delle operazioni di gestione di Cisco IOS](#)

[Controllo della versione del software](#)

[Gestione degli errori](#)

[Gestione dei problemi](#)

[Standardizzazione della configurazione](#)

[Gestione della disponibilità](#)

[Lista di controllo delle operazioni di gestione di Cisco IOS](#)

[Informazioni correlate](#)

[Servizi e supporto Cisco](#)

[Riassunto](#)

Cisco Leading Practices è una serie di documenti codificati che forniscono linee guida pertinenti e affidabili sulle operazioni di rete per i prodotti e le soluzioni Cisco. Le procedure principali sono sviluppate e supportate dai pluripremiati tecnici TAC e Advanced Services di Cisco, che possono essere utilizzati per creare una serie di procedure leader da emulare. I clienti Cisco hanno applicato queste procedure leader nel proprio ambiente di rete per ottenere prestazioni e disponibilità della rete.

Si consiglia vivamente di integrare queste pratiche leader con i servizi di Cisco e dei suoi partner. Per ulteriori informazioni su come ottimizzare le prestazioni e la disponibilità della rete, contattare il rappresentante commerciale Cisco per informazioni sul sito Web Cisco Advanced Services e per ulteriori informazioni su Network Optimization Support - Focused Engineering Support, Network

Introduzione

Panoramica

I processi operativi relativi alla gestione del software possono contribuire a ridurre la complessità della rete, a diminuire i problemi di supporto reattivo e a migliorare i tempi di risoluzione dei problemi. Questo documento offre una strategia, suggerimenti per gli strumenti e best-practice per la gestione complessiva del software Cisco IOS[®] (Cisco IOS).

Nelle sezioni [Creazione di una strategia operativa per la gestione di Cisco IOS](#) e [Seguito di una procedura ottimale per il processo operativo di gestione di Cisco IOS](#) in questo documento viene illustrata la metodologia consigliata per l'avvio delle operazioni ed elencati i migliori strumenti da utilizzare per la fase operativa. La fase operativa include i processi ottimali per:

Processo	Descrizione
Controllo versione software	Tracciamento, convalida e miglioramento della coerenza del software all'interno delle "tracce" identificate.
Gestione degli errori	Monitoraggio proattivo e implementazione dei messaggi SNMP e Syslog con priorità superiore generati da Cisco IOS.
Gestione dei problemi	Raccogliere in modo rapido ed efficiente le informazioni sui problemi critici per i problemi relativi al software al fine di prevenire il ripetersi di tali problemi.
Standardizzazione della configurazione	"Standardizzazione" delle configurazioni per ridurre la possibilità di utilizzare codice non testato in produzione e per standardizzare il protocollo di rete e il comportamento delle funzionalità.
Gestione della disponibilità	Miglioramento della disponibilità in base a metriche, obiettivi di miglioramento e progetti di miglioramento

In questo documento si presume che siano stati implementati i seguenti processi basati su best practice per la pianificazione, la progettazione e l'implementazione di Cisco IOS:

- Identificare aree software gestibili (tracce software) nell'ambiente in base ai requisiti di piattaforma, modulo, funzionalità, protocollo e topologia.
- Versioni selezionate, certificate e comunicate di Cisco IOS per tracce software.
- Implementazione coerente delle versioni standard di Cisco IOS in ciascuna traccia software.

Obiettivi

Questa sezione assiste l'utente nella gestione e manutenzione delle versioni Cisco IOS

standardizzate all'interno dei brani definiti. Verrà illustrato come:

- Sviluppare un processo di controllo della versione del software per garantire la coerenza della versione del software all'interno delle tracce software identificate.
- Monitoraggio, notifica e risoluzione dei processi in base ai messaggi e agli avvisi di gestione degli errori dei dispositivi (SNMP/Syslog) per contribuire alla risoluzione proattiva di potenziali problemi software e di errore.
- Raccolta efficiente delle informazioni sui problemi critici per il software, al fine di ridurre i tempi di risoluzione dei problemi relativi al software.
- Standardizzare le configurazioni dei dispositivi per garantire la coerenza di protocollo, funzionalità, accesso e sicurezza per l'ambiente.

Destinatari

Il presente documento è destinato ai singoli e ai responsabili con orientamento tecnico responsabili del funzionamento quotidiano della rete. Il documento descrive come stabilire i processi operativi per ridurre la complessità della rete, ridurre i problemi di supporto reattivo e migliorare i tempi di risoluzione dei problemi creando la coerenza della rete e migliorando le funzionalità per la gestione proattiva degli errori.

Prerequisiti

Gli utenti che partecipano alle operazioni di gestione di Cisco IOS devono avere una conoscenza approfondita della progettazione e dell'amministrazione dell'infrastruttura di rete, in particolare delle apparecchiature Cisco, e devono poter accedere ai dettagli della topologia, della configurazione dei dispositivi, del profilo di attività, dell'utilizzo delle applicazioni e dei criteri di utilizzo delle risorse della rete di destinazione. È inoltre necessario accedere agli strumenti di informazione disponibili su [Cisco Connection Online](#) (CCO) e utilizzarli. Se non si è ancora [registrati a CCO](#), si consiglia di effettuare la registrazione per accedere agli strumenti descritti in questo documento.

Creazione di una strategia operativa per la gestione di Cisco IOS

Esistono molte strategie e strumenti di qualità per aiutare a gestire gli ambienti Cisco IOS. Questo capitolo si concentra su tre strategie chiave per la gestione delle operazioni di Cisco IOS in ambienti a maggiore disponibilità e include una matrice di strumenti operativi chiave che sono particolarmente utili per la gestione dei problemi di Cisco IOS e Cisco IOS.

La prima strategia chiave è quella di mantenere l'ambiente il più semplice possibile, evitando variazioni nella configurazione e nelle versioni di Cisco IOS il più possibile. La certificazione Cisco IOS è già stata discussa, ma la coerenza della configurazione è un'altra area chiave. Il gruppo di progettazione/architettura deve essere responsabile della creazione degli standard di configurazione. A questo punto, il gruppo responsabile dell'implementazione e delle operazioni ha la responsabilità di configurare gli standard e di mantenerli aggiornati tramite il controllo della versione di Cisco IOS e gli standard/controlli della configurazione di Cisco IOS.

La seconda strategia chiave è la capacità di identificare e risolvere rapidamente i guasti di rete. Il gruppo operativo deve in genere identificare i problemi di rete prima che gli utenti li segnalino, e i problemi devono essere risolti il più rapidamente possibile senza influire ulteriormente o modificare l'ambiente. Due best-practice fondamentali in quest'area sono la gestione dei problemi

e la gestione degli errori (entrambe sono descritte più avanti in questo documento).

Nota: lo strumento Cisco IOS Stack Decoder può essere usato per diagnosticare rapidamente gli arresti anomali del software Cisco IOS.

La terza strategia chiave consiste nel "migliorare costantemente". Il processo principale consiste nel migliorare un programma di miglioramento della disponibilità basato sulla qualità. Eseguendo la root cause analysis su tutti i problemi, inclusi quelli relativi a Cisco IOS, è possibile migliorare il code coverage dei test, i tempi di risoluzione dei problemi e i processi in grado di eliminare o ridurre l'impatto delle interruzioni. L'organizzazione può inoltre esaminare i problemi comuni e creare processi per risolverli più rapidamente.

Identificazione dei deliverable

I servizi offerti dal processo operativo di gestione del software Cisco IOS includono:

- Processi e strumenti di controllo della versione del software
- Monitoraggio e processi di gestione degli errori
- Processi di gestione dei problemi
- Standard di configurazione dei dispositivi e processi di controllo
- Metodologia di disponibilità della rete, processi di reporting e revisione

Identificazione delle misure principali dei dispositivi

Le metriche devono essere definite come parte del piano operativo e utilizzate per determinare se gli strumenti e i processi producono i risultati desiderati. Di seguito sono riportati alcuni esempi di metriche utili per la gestione del software Cisco IOS:

- Disponibilità della rete (a causa di problemi software)
- % di conformità della versione Cisco IOS allo standard (per traccia)
- % Coerenza della configurazione del dispositivo (in base agli standard)
- Metriche di gestione dei problemi (MTTR, n. ticket, codici di chiusura)

Definizione di ruoli e responsabilità

Identificare, qualificare e assemblare un gruppo interfunzionale di manager e/o lead provenienti da gruppi di architettura di rete, progettazione di rete e implementazione/operazioni per garantire la corretta pianificazione, progettazione, implementazione e fasi operative dei progetti di aggiornamento IOS.

Identificazione delle aree di competenza necessarie

Assembla un gruppo interfunzionale di manager e/o lead dai gruppi gestione rete, progettazione rete, implementazione e operazioni per supportare la fase operativa del progetto di gestione Cisco IOS.

Identificazione dei principali collaboratori

- Gestori di rete: Nome, reparto, informazioni di contatto del/dei responsabile/i/ Nome del backup

- principale, reparto, informazioni di contattoNome del backup secondario, reparto, informazioni di contatto se necessario
- Architetti di rete:Nome dell'architetto, reparto, informazioni di contattoNome del backup principale, reparto, informazioni di contattoNome del backup secondario, reparto, informazioni di contatto se necessario
- Tecnici di rete:Nome, reparto, recapito tecnicoNome del backup principale, reparto, informazioni di contattoNome del backup secondario, reparto, informazioni di contatto se necessario
- Tecnici delle operazioni di rete (NOC):Nome, reparto, recapito tecnicoNome del backup principale, reparto, informazioni di contattoNome del backup secondario, reparto, informazioni di contatto se necessario

Identificazione delle responsabilità

- I gestori della rete sono responsabili di:Gestione del piano di progettoAssegnazione/riassegnazione di risorseGestione del controllo delle modificheGestione dello statoGestione dei rapporti sul budget
- Gli architetti della rete sono responsabili di:Analisi degli standard di rete e avvertenze sul rilascioGestione della matrice di aggiornamento softwareGestione della matrice di gestione dei candidatiGestione della matrice dei requisiti di memoria
- Gli ingegneri di rete (NOC) sono responsabili di:Implementazione e conformità agli standard di reteIdentificazione dei problemi software e delle cause principaliAzioni correttive consigliateMonitoraggio della rete

Risorse di impostazione budget

I requisiti di risorse devono essere determinati nella fase operativa per supportare la strategia di gestione del software per l'organizzazione. Ciò include il tempo di personale e le spese in conto capitale necessarie per supportare la strategia software.

In molti casi, è possibile generare un ritorno sul capitale investito (ROI) o un piano di budget per le pratiche di gestione del software in base al costo dei tempi di inattività e ai requisiti di disponibilità. Se l'organizzazione è in grado di determinare i tempi di inattività dovuti a problemi software, la maggior parte di questo costo può essere compensata attraverso le best practice di gestione del software identificate. Se il costo non può essere completamente compensato, l'organizzazione dovrebbe prendere in considerazione una strategia di gestione del software più di base che contribuirà a migliorare la produttività impedendo ulteriori rielaborazioni a causa di problemi software.

Seguire una procedura ottimale per il processo delle operazioni di gestione di Cisco IOS

Le best practice per seguire un processo Cisco IOS Management Operations includono:

Procedur e ottimali	Dettaglio
Controllo della	Implementazione delle sole versioni software standardizzate e monitoraggio della rete per

versione del software	convalidare o eventualmente modificare il software a causa della mancata conformità delle versioni.
Gestione degli errori	La raccolta, il monitoraggio e l'analisi dei messaggi SNMP e Syslog sono processi di gestione degli errori consigliati per risolvere un numero maggiore di problemi di rete specifici di Cisco IOS che sono difficili o impossibili da identificare in altro modo.
Gestione dei problemi	Processi dettagliati di gestione dei problemi che definiscono l'identificazione dei problemi, la raccolta di informazioni e un percorso di soluzione ben analizzato. Questi dati vengono utilizzati per determinare la causa principale.
Standardi di configurazione della configurazione	Gli standard di configurazione rappresentano la procedura di creazione e gestione di parametri di configurazione "globali" standard su dispositivi e servizi simili, che si traducono in una coerenza di configurazione globale a livello aziendale.
Gestione della disponibilità	Miglioramento della qualità utilizzando la disponibilità di rete come parametro per il miglioramento della qualità.

[Controllo della versione del software](#)

Il controllo della versione del software è il processo di implementazione delle sole versioni del software standardizzate e di monitoraggio della rete per convalidare o eventualmente modificare il software a causa della mancata conformità della versione. In generale, il controllo della versione del software viene eseguito utilizzando un processo di certificazione e un controllo standard. Molte organizzazioni pubblicano standard di versione su un server Web centrale. Inoltre, lo staff addetto all'implementazione è in grado di esaminare la versione in esecuzione e di aggiornarla se non è conforme agli standard. Alcune organizzazioni dispongono di un processo di controllo qualità in cui la convalida secondaria viene completata tramite audit per garantire che lo standard venga rispettato durante l'implementazione.

Durante il funzionamento in rete, non è raro vedere versioni di software non standard nella rete, specialmente se la rete è grande e il personale è numeroso. Ciò può essere dovuto a uno dei seguenti motivi:

- Nuovo personale non addestrato
- Comandi di avvio non configurati correttamente
- Implementazioni non controllate

Si consiglia di convalidare periodicamente gli standard di versione del software utilizzando strumenti quali CiscoWorks2000 Resource Manager Essentials (RME) in grado di ordinare tutti i dispositivi in base alla versione di Cisco IOS. Quando viene identificata una versione non standard, questa deve essere immediatamente contrassegnata e deve essere avviato un ticket di risoluzione dei problemi o di modifica per portare la versione allo standard identificato.

Strumenti disponibili

Il CiscoWorks 2000 RME Inventory Manager semplifica notevolmente la gestione delle versioni Cisco IOS dei router e degli switch Cisco tramite strumenti di reporting basati sul Web che segnalano e ordinano i dispositivi in base alla versione del software, alla piattaforma del dispositivo e al nome del dispositivo.

Gestione degli errori

La gestione degli errori è il processo di raccolta, monitoraggio e analisi dei messaggi SNMP e Syslog per risolvere un numero maggiore di problemi di rete specifici di Cisco IOS, difficili o impossibili da identificare in altro modo.

Raccolta di trap SNMP

La raccolta e la notifica delle trap SNMP è un processo di base nella gestione degli errori utilizzato per identificare gli eventi software o hardware e/o gli arresti anomali senza sovraccarico o ritardo del polling SNMP dovuto agli intervalli di polling. I messaggi trap vengono generati direttamente dal dispositivo di rete a un sistema di gestione di rete che fornisce servizi di notifica. La raccolta e la notifica di queste trap è essenziale per la rapida risoluzione di molti eventi di rete, inclusi eventi che non hanno alcun impatto sugli utenti, come la perdita di dispositivi primari o collegamenti in un ambiente ridondante.

Per raccogliere e monitorare queste trap, è necessario configurarle correttamente sul dispositivo e sui sistemi di gestione della rete. I sistemi di gestione della rete devono avvertire il gruppo di operazioni di rete quando viene ricevuta una trap. La notifica può quindi avvenire sotto forma di paging, e-mail o schermate di eventi in un ambiente NOC.

Indipendentemente dalla modalità di presentazione dei dati, queste istanze di errore, o eccezioni, devono essere analizzate e riviste regolarmente (preferibilmente ogni giorno) dal personale di supporto della rete e/o dalle operazioni di rete. È necessario analizzare le cause di tutte le eccezioni rilevate. Alcune eccezioni registrate potrebbero non essere abbastanza critiche da attivare immediatamente un allarme nel Centro operazioni di rete. L'analisi, l'analisi e la risoluzione proattiva di eccezioni di lieve entità possono aiutare i gruppi di supporto di rete a ridurre o prevenire le interruzioni della rete.

Raccolta messaggi Syslog

I messaggi Syslog vengono inviati dal dispositivo a un server di raccolta. Questi messaggi possono essere errori hardware o software oppure possono essere informativi, ad esempio quando qualcuno si trova in configurazione di un terminale su un dispositivo.

Il monitoraggio Syslog richiede il supporto dello strumento Network Management System (NMS) o script per l'analisi e la creazione di report sui dati Syslog. Ciò include la capacità di ordinare i messaggi Syslog per data o periodo di tempo, dispositivo, tipo di messaggio Syslog o frequenza dei messaggi. Nelle reti più grandi, è possibile implementare strumenti o script per analizzare i dati Syslog e inviare avvisi o notifiche ai sistemi di gestione degli eventi o al personale operativo e tecnico. Se non vengono utilizzati avvisi per un'ampia gamma di dati di syslog, l'organizzazione dovrebbe esaminare i dati di syslog con priorità più alta almeno ogni giorno e creare ticket per la risoluzione di potenziali problemi. Per rilevare in modo proattivo problemi di rete che potrebbero non essere rilevati con il normale monitoraggio, è necessario eseguire periodicamente una revisione e un'analisi dei dati storici del syslog per rilevare situazioni che potrebbero non indicare un problema immediato, ma che potrebbero fornire un'indicazione di un problema prima che questo diventi un impatto sul servizio.

Strumenti disponibili

Alcuni dei più comuni strumenti di ricezione delle trap SNMP sono i seguenti:

- HP OpenView Network Node Manager di Hewlett Packard all'indirizzo openview.hp.com
- Spectrum Integrity da Aprisma su www.aprisma.com
- NetView di IBM Tivoli all'indirizzo www.tivoli.com

Lo strumento Syslog più comune per la gestione di Cisco IOS è CiscoWorks2000 RME Syslog Manager. Altri strumenti disponibili includono SL4NT, un programma shareware da www.netal.com che lascia cisco.com e Private IP da OpenSystems all'indirizzo www.opensystems.com

Gestione dei problemi

La gestione dei problemi, un aspetto della gestione degli errori, è la disciplina che disciplina la gestione dei problemi dal momento in cui si verificano, attraverso l'identificazione, la risoluzione dei problemi e la chiusura.

Molti clienti riscontrano ulteriori tempi di inattività dovuti alla mancanza di processi nella gestione dei problemi. È possibile che si verifichino tempi di inattività aggiuntivi quando gli amministratori di rete tentano di risolvere rapidamente il problema utilizzando una combinazione di comandi che hanno un impatto sui servizi o di modifiche alla configurazione anziché dedicare tempo all'identificazione dei problemi, alla raccolta di informazioni e a un percorso di soluzione ben analizzato. Il comportamento osservato in quest'area include il ricaricamento dei dispositivi o la cancellazione delle tabelle di routing IP prima di analizzare un problema e la sua causa principale. In alcuni casi ciò si verifica a causa degli obiettivi di risoluzione dei problemi del supporto di primo livello. L'obiettivo di tutti i problemi relativi al software deve essere quello di raccogliere rapidamente le informazioni necessarie per la root cause analysis prima di ripristinare la connettività o il servizio.

Si consiglia un processo di gestione dei problemi, che deve includere un certo grado di descrizioni predefinite dei problemi e appropriate raccolte di comandi "show" prima di escalation del problema ad un secondo livello di supporto. Il supporto di primo livello non deve mai includere la cancellazione di route o il ricaricamento di dispositivi. Idealmente, l'organizzazione di supporto di primo livello dovrebbe raccogliere rapidamente le informazioni e quindi inoltrare il problema al supporto di secondo livello. Dedicando un po' più di tempo all'identificazione e alla descrizione del problema nel supporto di primo livello, è molto più probabile un'individuazione della root cause, consentendo così una soluzione, l'identificazione del laboratorio e la creazione di report sui bug. Il supporto di secondo livello deve essere ben informato sui tipi di informazioni di cui Cisco potrebbe aver bisogno per diagnosticare un problema o segnalare un bug, tra cui:

- Dump della memoria
- Output informazioni di routing
- Output comando show dispositivo

Standardizzazione della configurazione

Gli standard di configurazione globale dei dispositivi rappresentano la pratica di mantenere i parametri di configurazione "globale" standard su dispositivi e servizi simili, con conseguente coerenza della configurazione globale a livello aziendale. I comandi di configurazione globale sono comandi che si applicano all'intero dispositivo e non a singole porte, protocolli o interfacce e

in genere influiscono sull'accesso ai dispositivi, sul loro comportamento generale e sulla sicurezza dei dispositivi. In Cisco IOS, sono inclusi i seguenti comandi:

- Servizio
- IP
- VTY
- Porta della console
- Registrazione
- AAA/TACACS+
- SNMP
- Banner

Negli standard di configurazione globale dei dispositivi è inoltre importante una convenzione di denominazione dei dispositivi appropriata che consenta agli amministratori di identificare il dispositivo, il tipo di dispositivo e la posizione del dispositivo in base al nome DNS del dispositivo. La coerenza della configurazione globale è importante per il supporto e l'affidabilità complessivi di un ambiente di rete, in quanto contribuisce a ridurre la complessità della rete e a migliorarne il supporto. Le difficoltà di supporto si verificano spesso senza standardizzazione della configurazione a causa di un comportamento errato o incoerente dei dispositivi, dell'accesso SNMP e della sicurezza generale dei dispositivi.

Il mantenimento degli standard di configurazione globale dei dispositivi viene in genere eseguito da un gruppo di progettazione o un gruppo operativo interno che crea e gestisce i parametri di configurazione globale per dispositivi di rete simili. È inoltre buona norma fornire una copia del file di configurazione globale nelle directory TFTP in modo che possa essere scaricato inizialmente su tutti i dispositivi di cui è stato appena eseguito il provisioning. È inoltre utile un file accessibile dal Web che fornisce al file di configurazione standard una spiegazione di ciascun parametro di configurazione. Alcune organizzazioni configurano periodicamente tutti i dispositivi simili per garantire la coerenza della configurazione globale oppure controllano periodicamente i dispositivi per verificare la correttezza degli standard di configurazione globale.

Gli standard di configurazione dell'interfaccia o del protocollo rappresentano la pratica di mantenere gli standard per la configurazione dell'interfaccia e del protocollo, che migliora la disponibilità della rete riducendo la complessità della rete, fornendo il comportamento previsto dei dispositivi e dei protocolli e migliorando la supportabilità della rete. L'incoerenza della configurazione dell'interfaccia o del protocollo può causare comportamenti imprevisti dei dispositivi, problemi di routing del traffico, problemi di connettività maggiori e un aumento dei tempi di supporto reattivi.

Gli standard di configurazione interfaccia possono includere:

- CDP (Cisco Discovery Protocol)
- Descrittori di interfaccia
- Configurazione cache
- Altri standard specifici del protocollo

Gli standard di configurazione specifici del protocollo possono includere:

- Configurazione routing IP
- Configurazione DLSW
- Configurazione dell'elenco degli accessi
- configurazione ATM
- Configurazione Frame Relay

- Configurazione Spanning Tree
- Assegnazione e configurazione VLAN
- VTP (Virtual Trunking Protocol)
- HSRP (Hot Standby Routing Protocol)
- Altri a seconda della configurazione della rete

Ad esempio, gli standard IP possono includere le dimensioni della subnet, lo spazio degli indirizzi IP utilizzato, il protocollo di routing utilizzato e la configurazione del protocollo di routing.

Il mantenimento degli standard di configurazione di protocolli e interfacce è in genere di responsabilità dei gruppi di progettazione e implementazione della rete. Il gruppo di ingegneri deve essere responsabile dell'identificazione, della verifica, della convalida e della documentazione degli standard. Il gruppo di implementazione è quindi responsabile dell'utilizzo dei documenti tecnici o dei modelli di configurazione per il provisioning di nuovi servizi. Il gruppo di ingegneri dovrebbe creare una documentazione su tutti gli aspetti degli standard richiesti per garantire la coerenza. È inoltre necessario creare modelli di configurazione per consentire l'applicazione degli standard di configurazione. Anche i gruppi operativi dovrebbero essere formati sugli standard e dovrebbero essere in grado di identificare problemi di configurazione non standard. La coerenza della configurazione è di grande ausilio nelle fasi di test, convalida e certificazione. Senza modelli di configurazione standardizzati, è quasi impossibile testare, convalidare o certificare in modo adeguato una versione di Cisco IOS per una rete moderatamente grande.

Gestione della disponibilità

La gestione della disponibilità è il processo di miglioramento della qualità che utilizza la disponibilità della rete come parametro per il miglioramento della qualità. Molte organizzazioni stanno misurando la disponibilità e il tipo di interruzione delle attività. I tipi di interruzione possono includere:

- Hardware
- Software
- Collegamento/vettore
- Alimentazione/ambiente
- Progettazione
- Errore utente/processo

Identificando le interruzioni ed eseguendo la root cause analysis subito dopo il ripristino, l'organizzazione può identificare i metodi per migliorare la disponibilità. Quasi tutte le reti che hanno raggiunto un'elevata disponibilità dispongono di un processo di miglioramento della qualità.

Lista di controllo delle operazioni di gestione di Cisco IOS

Passaggio 1: [Definizione dei requisiti e degli obiettivi aziendali](#) (solo clienti [registrati](#))

Passaggio 2: [Valutazione dello stato corrente delle procedure di gestione del software Cisco IOS](#) (solo utenti [registrati](#))

Passaggio 3: [Definizione di ruoli e responsabilità](#) (solo clienti [registrati](#))

Passaggio 4: [Sviluppo di un piano di progetto per la gestione del software](#) (solo clienti [registrati](#))

[Informazioni correlate](#)

È stata creata un'appendice per aiutare il cliente ad ottenere altre preziose informazioni relative a Cisco IOS, quali: Nozioni di base di Cisco IOS, processi software Cisco IOS interni, analisi dell'affidabilità del software, programma di qualità interno Cisco, metodologie di test interne Cisco e analisi sul campo che mostrano le attuali prassi di settore e l'esperienza complessiva dei clienti con il software Cisco IOS

- Gestione Cisco IOS: Per ulteriori informazioni sulla gestione e le best practice di Cisco IOS, consultare il white paper "Cisco IOS Management for High Availability Networking" al seguente indirizzo:
http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a00800a998b.shtml
- Per informazioni specifiche su come eseguire i probe di rete, sui comandi CLI da utilizzare, su come analizzare e interpretare i dati del traffico di rete e su come stabilire i criteri di utilizzo delle applicazioni, visitare il sito <http://www.cisco.com>. Questo sito offre una gamma completa di soluzioni di supporto, formazione, documentazione tecnica e consulenza.
- Cisco IOS ha convenzioni di denominazione specifiche definite qui:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_tech_note09186a0080101cda.shtml
- Le informazioni sulla disponibilità della versione Cisco IOS sono disponibili qui:
http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html
- Le versioni Cisco IOS vengono alla fine rimosse da CCO e non possono più essere ordinate. Assicurarsi di impostare le aspettative dei clienti di conseguenza.
- I bollettino sui prodotti Cisco IOS vengono utilizzati per annunciare le versioni dei prodotti Cisco IOS ai clienti. Contengono brevi informazioni sul contenuto della release. Fare clic qui per verificare la disponibilità delle nuove versioni di Cisco IOS
http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html
- Il team di risposta agli incidenti sulla sicurezza dei prodotti gestisce la sicurezza dei prodotti Cisco. Tutti i problemi relativi alla sicurezza di Cisco IOS devono essere segnalati a questo team. Cisco pubblica le sue vulnerabilità di sicurezza.
<http://tools.cisco.com/security/center/publicationListing>
- Difetti Cisco IOS: Si consiglia di differire l'operazione per i difetti gravi di Cisco IOS. Qualunque dipendente Cisco può effettuare una raccomandazione.
- I problemi sul campo relativi a Cisco IOS vengono comunicati ai clienti tramite i consigli di Cisco IOS.
http://www.cisco.com/en/US/products/products_security_advisory09186a0080b20ee1.shtml
- Funzioni Cisco IOS: Lo strumento Feature Navigator consente ai clienti di individuare le versioni che supportano funzionalità specifiche e viceversa.
<http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>
- Cisco Software Advisor consente ai clienti di trovare il supporto software per le funzionalità o il supporto software per l'hardware. <http://tools.cisco.com/Support/Fusion/FusionHome.do> (solo utenti [registrati](#))

Servizi e supporto Cisco

- Servizi di supporto tecnico
- Servizi specifici per le tecnologie e le soluzioni di rete Cisco