Cisco IOS Management per le reti ad alta disponibilità: White paper sulle procedure ottimali

Sommario

Introduzione

L'installazione e la manutenzione di software Cisco IOS® affidabile sono una priorità negli attuali

ambienti di rete business critical che richiedono un rinnovato impegno da parte di Cisco e dei clienti per ottenere una disponibilità continua. Mentre Cisco deve concentrarsi sulla qualità del software, i gruppi di supporto e progettazione della rete devono anche concentrarsi sulle best practice per la gestione del software Cisco IOS. L'obiettivo è una maggiore disponibilità ed efficienza nella gestione del software. Si tratta di un metodo combinato per condividere, apprendere e implementare le procedure ottimali di gestione del software.

Questo documento offre una struttura operativa efficace delle procedure di gestione di Cisco IOS, sia per le aziende che per i provider di servizi, in grado di promuovere una maggiore affidabilità del software, una minore complessità di rete e una maggiore disponibilità della rete. Questa struttura contribuisce inoltre a migliorare l'efficienza di gestione del software identificando le aree di responsabilità e le sovrapposizioni nei test e nelle convalide di gestione del software tra le operazioni di rilascio di Cisco e la base clienti Cisco.

Panoramica delle best practice di Cisco IOS

Le tabelle seguenti forniscono una panoramica delle best practice di Cisco IOS. Queste tabelle possono essere usate come panoramica della gestione delle best practice definite, lista di controllo per l'analisi dei gap per rivedere le attuali pratiche di gestione di Cisco IOS o come struttura per la creazione di processi relativi alla gestione di Cisco IOS.

Le tabelle definiscono i quattro componenti del ciclo di vita della gestione di Cisco IOS. Ogni tabella inizia con una strategia e un riepilogo degli strumenti per l'area del ciclo di vita identificata. Seguendo il riepilogo della strategia e degli strumenti è possibile individuare procedure ottimali specifiche valide solo per l'area del ciclo di vita definita.

Pianificazione - Creazione della struttura di gestione di Cisco IOS—La pianificazione è la fase iniziale della gestione di Cisco IOS necessaria per aiutare un'organizzazione a determinare quando aggiornare il software, dove aggiornare e quale processo verrà utilizzato per testare e convalidare le immagini potenziali.

Procedure ottimali	Dettaglio
Strategia e strumenti per Cisco IOS Planning	Per iniziare a utilizzare la pianificazione della gestione di Cisco IOS, è necessario eseguire una valutazione accurata delle procedure correnti, dello sviluppo di obiettivi raggiungibili e della pianificazione del progetto.
Definizioni del software Version Track	Identifica dove è possibile mantenere la coerenza del software. Un percorso software può essere definito come un raggruppamento di versioni software univoco, differenziato da altre aree in base a requisiti specifici in termini di area geografica, piattaforme, modulo o funzionalità.
Ciclo di aggiorn	Le definizioni dei cicli di aggiornamento possono essere definite come fasi di qualità di

amento e definizioni	base nel software e nella gestione delle modifiche utilizzate per determinare quando avviare un ciclo di aggiornamento del software.
Processo di certificazione	Le fasi del processo di certificazione dovrebbero includere l'identificazione dei brani, le definizioni dei cicli di aggiornamento, la gestione dei candidati, il test e la convalida e almeno un uso pilota della produzione.

Progettazione - Selezione e convalida delle versioni di IOS - La disponibilità di un processo ben definito per la selezione e la convalida delle versioni di Cisco IOS consente alle aziende di ridurre i tempi di inattività imprevisti dovuti a tentativi di aggiornamento non riusciti e a difetti software non pianificati.

Procedure ottimali	Dettaglio
Strategia e strumenti per la selezione e la convalida di Cisco IOS	Definire i processi per la selezione, il test e la convalida delle nuove versioni di Cisco IOS. Questo include un laboratorio di test di rete che emula la rete di produzione
Gestione candidati	La gestione dei candidati consiste nell'identificazione dei requisiti della versione del software e dei rischi potenziali per l'hardware specifico e le funzionalità abilitate.
Test e convalida	Il testing e la convalida sono aspetti critici della gestione del software e delle reti ad alta disponibilità. Test di laboratorio adeguati possono ridurre in modo significativo i tempi di inattività della produzione, aiutare a formare il personale di supporto della rete e semplificare i processi di implementazione della rete.

Implementazione - Implementazione rapida e corretta di Cisco IOS - I processi di implementazione ben definiti consentono alle aziende di implementare rapidamente e con successo le nuove versioni di Cisco IOS.

Procedure ottimali	Dettaglio
Strategia e strumenti per le impleme	La strategia di base per le implementazioni di Cisco IOS è eseguire la certificazione finale tramite un processo pilota e l'installazione rapida utilizzando strumenti di aggiornamento e un processo di implementazione ben

ntazioni di Cisco IOS	definito.
Processo pilota	Per ridurre al minimo l'esposizione potenziale e acquisire in modo più sicuro i problemi di produzione rimanenti, si consiglia un software pilota. Il piano pilota individuale dovrebbe prendere in considerazione la selezione del pilota, la sua durata e la misurazione.
Implementazione	Al termine della fase pilota dovrebbe iniziare la fase di implementazione di Cisco IOS. La fase di implementazione può includere diverse fasi per garantire il successo e l'efficienza dell'aggiornamento software, tra cui avvio lento, certificazione finale, preparazione dell'aggiornamento, automazione dell'aggiornamento e convalida finale.

Operazioni - Gestione dell'implementazione Cisco IOS ad alta disponibilità: le best practice per le operazioni Cisco IOS includono il controllo della versione del software, la gestione dei syslog di Cisco IOS, la gestione dei problemi, la standardizzazione della configurazione e la gestione della disponibilità.

Procedure ottimali	Dettaglio
Strategie e strumenti per le operazioni Cisco IOS	La prima strategia delle operazioni di Cisco IOS è mantenere l'ambiente il più semplice possibile, evitando variazioni nella configurazione e nelle versioni di Cisco IOS. La seconda strategia consiste nella capacità di identificare e risolvere rapidamente gli errori di rete.
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.
Gestione proattiva syslog	La raccolta, il monitoraggio e l'analisi dei syslog sono processi di gestione degli errori consigliati per risolvere un numero maggiore di problemi di rete specifici di Cisco IOS, difficili o impossibili da identificare con altri mezzi.
Gestione dei problemi	Processi dettagliati di gestione dei problemi che definiscono l'identificazione dei problemi, la raccolta di informazioni e un percorso della soluzione ben analizzato. Questi dati possono essere utilizzati per determinare la causa principale.
Standardi	Gli standard di configurazione rappresentano

zzazione della configurazione	la procedura di creazione e gestione di parametri di configurazione globali standard su dispositivi e servizi simili, che determina la coerenza della configurazione globale a livello aziendale.
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.

Panoramica del processo di gestione del ciclo di vita del software

La gestione del ciclo di vita del software Cisco IOS è definita come l'insieme dei processi di pianificazione, progettazione, implementazione e funzionamento consigliati per implementazioni software affidabili e reti a elevata disponibilità. Sono inclusi i processi per selezionare, convalidare e mantenere le versioni di Cisco IOS nella rete.

L'obiettivo della gestione del ciclo di vita del software Cisco IOS è di migliorare la disponibilità della rete riducendo la probabilità di difetti del software identificati in produzione o di errori di modifica/aggiornamento correlati al software. È stato dimostrato che le best practice definite in questa documentazione consentono di ridurre tali difetti e errori di modifica in base all'esperienza pratica di molti clienti Cisco e del team Cisco Advanced Services. La gestione del ciclo di vita del software può inizialmente comportare un aumento delle spese, ma è possibile ridurre il costo complessivo di gestione riducendo le interruzioni e semplificando i meccanismi di installazione e supporto.

Pianificazione - Creazione della struttura di gestione di Cisco IOS

La pianificazione è la fase iniziale della gestione di Cisco IOS necessaria per aiutare un'organizzazione a determinare quando aggiornare il software, dove eseguire l'aggiornamento e quale processo verrà utilizzato per testare e convalidare potenziali immagini.

Le procedure ottimali includono le definizioni dei percorsi di versione del software, il ciclo di aggiornamento e le definizioni, nonché la creazione di un processo di certificazione software interno.

Strategia e strumenti per Cisco IOS Planning

Iniziare la pianificazione della gestione di Cisco IOS con una valutazione accurata delle procedure correnti, dello sviluppo di obiettivi raggiungibili e della pianificazione del progetto. L'autovalutazione deve essere eseguita confrontando le procedure ottimali descritte in questo documento con i processi interni all'organizzazione. Le domande di base dovrebbero includere:

- L'organizzazione dispone di un processo di certificazione software che include test/convalida del software?
- L'organizzazione dispone di standard software Cisco IOS con una quantità limitata di versioni Cisco IOS in esecuzione nella rete?
- L'organizzazione ha difficoltà a stabilire quando aggiornare il software Cisco IOS?
- L'organizzazione ha difficoltà a installare il nuovo software Cisco IOS in modo efficiente ed

efficace?
- L'organizzazione ha problemi di stabilità a seguito dell'installazione di Cisco IOS che hanno un impatto significativo sul costo dei tempi di inattività?

In seguito alla valutazione, l'organizzazione deve iniziare a definire gli obiettivi per la gestione del software Cisco IOS. Inizia riunendo un gruppo interfunzionale di manager e/o lead provenienti da gruppi di pianificazione dell'architettura, progettazione, implementazione e operazioni per definire gli obiettivi di Cisco IOS e i progetti di miglioramento dei processi. L'obiettivo dei meeting iniziali è quello di determinare obiettivi generali, ruoli e responsabilità, assegnare azioni e definire pianificazioni di progetto iniziali. Definire inoltre i fattori critici di successo e le metriche per determinare i vantaggi della gestione software. Le metriche potenziali includono:

- disponibilità (a causa di problemi software)
- costo degli aggiornamenti software
- tempo richiesto per gli aggiornamenti
- numero di versioni software in esecuzione in produzione
- aggiornamenti software modifica percentuali di operazioni riuscite/non riuscite

Oltre alla pianificazione generale della struttura di gestione di Cisco IOS, alcune organizzazioni definiscono anche riunioni di pianificazione software in corso da tenersi mensilmente o trimestralmente. L'obiettivo di questi incontri è esaminare l'attuale installazione del software e iniziare a pianificare eventuali nuovi requisiti software. La pianificazione può includere la revisione o la modifica dei processi di gestione software correnti o semplicemente la definizione dei ruoli e delle responsabilità per le diverse fasi di gestione software.

Gli strumenti nella fase di pianificazione sono costituiti esclusivamente da strumenti di gestione dell'inventario software. Gestione inventario CiscoWorks 2000 Resource Manager Essentials (RME) è lo strumento principale utilizzato in quest'area. CiscoWorks 2000 RME Inventory Manager semplifica notevolmente la gestione delle versioni dei router e degli switch Cisco tramite strumenti di reporting basati sul Web che segnalano e ordinano i dispositivi Cisco IOS in base alla versione del software, alla piattaforma del dispositivo, alle dimensioni della memoria e al nome del dispositivo.

Definizioni del software Version Track

La prima best practice di pianificazione della gestione software Cisco IOS identifica i punti in cui è possibile mantenere la coerenza software. Un percorso software è definito come un raggruppamento di versioni software univoco, differenziato da altre aree in base a requisiti specifici in termini di area geografica, piattaforme, moduli o funzionalità. È consigliabile che una rete esegua una sola versione del software. Ciò consente di ridurre notevolmente i costi correlati alla gestione del software e fornisce un ambiente coerente e di facile gestione. In realtà, tuttavia, la maggior parte delle organizzazioni deve eseguire diverse versioni della rete a causa di problemi di funzionalità, piattaforma, migrazione e disponibilità all'interno di aree specifiche. In molti casi, la stessa versione non funziona su piattaforme eterogenee. In altri casi, l'organizzazione non può attendere che una versione supporti tutti i requisiti. L'obiettivo è quello di identificare il minor numero di tracce software per la rete, prendendo in considerazione i requisiti di test/convalida, certificazione e aggiornamento. In molti casi, l'organizzazione può disporre di un numero leggermente maggiore di percorsi per ridurre i costi complessivi di test/convalida, certificazione e aggiornamento.

Il primo elemento che distingue l'azienda è il supporto delle piattaforme. In genere, gli switch LAN, gli switch WAN, i router principali e i router periferici hanno percorsi software separati. Altre tracce software possono essere necessarie per funzionalità o servizi specifici, come la commutazione

DLSw (Data-Link Switching), QoS (Quality of Service) o la telefonia IP, specialmente se questo requisito può essere localizzato nella rete.

Un altro criterio è l'affidabilità. Molte organizzazioni cercano di eseguire il software più affidabile verso il core di rete e il centro dati, offrendo al contempo funzionalità avanzate più recenti o supporto hardware, verso l'avanguardia. D'altra parte, le funzioni di scalabilità o larghezza di banda sono spesso più necessarie negli ambienti core o dei centri dati. Altre tracce potrebbero essere necessarie per piattaforme specifiche, come siti di distribuzione più grandi che hanno una piattaforma di router WAN diversa. La tabella seguente è un esempio di definizione di traccia software per un'organizzazione di grandi dimensioni.

Brano	Area	Piattaforme hardware	Caratteristiche	Versione Cisco IOS	Stato certificazione
1	Switching per core LAN	6500	QoS	12.1E (A8)	Test
2	Switch di accesso LAN	2924 XL 2948 XL	Protocollo UDLD (Unidirectional Link Detection Protocol), Protocollo Spanning Tree Protocol (STP)	12.0(5.2)XU	Certificato 01/03/01
3	Distribuzione/accesso LAN	5500 6509	Supervisor 3	5.4(4)	Certificato 01/07/01
4	Modulo Route Switch (RSM) dello switch di distribuzione	RSM	Open Shortest Path First (OSPF) Routing	12.0(11)	Certificazione 4/3/02
5	Distribuzione headend WAN	7505 7507 7204 7206	OSPF Frame Relay	12.0(11)	Certificazione 11/1/01
6	accesso WAN	2600	OSPF Frame Relay	12.1(8)	Certificato 01/06/01
7	Connettività IBM	3600	Headend SDLC (Synchronous Data Link Control)	11.3(8)T1	Certificazione 11/1/00

Anche le assegnazioni dei brani possono cambiare nel tempo. In molti casi, le funzionalità o il supporto hardware possono integrarsi in versioni software più diffuse, consentendo la migrazione di diverse tracce. Una volta definite le definizioni dei brani, l'organizzazione può utilizzare altri processi definiti per migrare verso la coerenza e la convalida delle nuove versioni. Anche le definizioni delle tracce sono un'attività costante. Ogni volta che viene identificato un nuovo requisito di funzionalità, servizio, hardware o modulo, è opportuno considerare un nuovo brano.

Le organizzazioni che desiderano avviare un processo di tracciamento dovrebbero iniziare con nuovi requisiti di tracciamento o, in alcuni casi, con progetti di stabilizzazione per le reti esistenti. Un'organizzazione può anche avere alcune caratteristiche comuni con le versioni software esistenti che possono rendere possibile la definizione corrente del brano. Nella maggior parte dei casi, la migrazione rapida alle versioni identificate non è necessaria se il cliente dispone di sufficiente stabilità di rete. L'architettura di rete, o gruppo di progettazione, in genere possiede il processo di definizione dei brani. In alcuni casi, una persona può essere responsabile delle definizioni dei brani. In altri casi, i responsabili di progetto sono responsabili dello sviluppo di requisiti software e di nuove definizioni di tracce basate su singoli progetti. È inoltre consigliabile rivedere le definizioni dei brani su base trimestrale per determinare se sono necessari nuovi brani o se i brani precedenti richiedono il consolidamento o l'aggiornamento.

Le organizzazioni che identificano e gestiscono le tracce software con un rigoroso controllo delle versioni hanno dimostrato di avere il successo maggiore con un numero inferiore di versioni software nella rete di produzione. In genere, ciò consente di migliorare la stabilità del software e l'affidabilità complessiva della rete.

Ciclo di aggiornamento e definizioni

Le definizioni dei cicli di aggiornamento sono definite come fasi di qualità di base nel software e nella gestione delle modifiche utilizzate per determinare quando avviare un ciclo di aggiornamento del software. Le definizioni dei cicli di aggiornamento consentono a un'organizzazione di pianificare correttamente un ciclo di aggiornamento del software e di allocare le risorse necessarie. Senza le definizioni del ciclo di aggiornamento, in genere un'organizzazione riscontra un aumento dei problemi di affidabilità del software a causa dei requisiti delle funzionalità nelle versioni stabili correnti. Un'altra esposizione potrebbe essere rappresentata dalla mancanza da parte dell'organizzazione dell'opportunità di testare e convalidare correttamente una nuova versione prima che sia richiesto l'utilizzo della produzione.

Un aspetto importante di questa pratica è l'identificazione di quando e in che misura avviare i processi di pianificazione software. Ciò è dovuto al fatto che una delle principali cause dei problemi software è l'attivazione di una funzionalità, un servizio o una funzionalità hardware in produzione senza la dovuta diligenza, o l'aggiornamento a una nuova versione di Cisco IOS senza considerazioni sulla gestione del software. Un altro problema non è l'aggiornamento. Ignorando i normali cicli e requisiti software, molti clienti si trovano ad affrontare il difficile compito di aggiornare il software attraverso una serie di versioni principali diverse. Il problema è dovuto alle dimensioni delle immagini, alle modifiche del comportamento predefinito, alle modifiche dell'interprete a livello di comando (CLI) e alle modifiche del protocollo.

Cisco consiglia di avviare un ciclo di aggiornamento ben definito, basato sulle best practice definite in questo documento, ogni volta che è necessario un nuovo servizio, una nuova funzionalità o supporto hardware. Il grado di certificazione e test/convalida deve essere analizzato (in base al rischio), per determinare con precisione i requisiti di test/convalida. L'analisi dei rischi può essere eseguita in base alla posizione geografica, alla posizione logica (core, distribuzione o livelli di accesso) o al numero stimato di persone/clienti interessati. Se la funzionalità principale o

la funzionalità hardware è inclusa nella versione corrente, è necessario avviare anche alcuni processi del ciclo di aggiornamento semplificati. Se la funzionalità è relativamente secondaria, considerare il rischio e quindi decidere quali processi avviare. Inoltre, il software deve essere aggiornato entro due anni per garantire che l'organizzazione rimanga relativamente aggiornata e che il processo di aggiornamento non sia troppo complicato.

I clienti devono inoltre tenere presente che non verrà eseguita alcuna correzione dei bug relativi ai software che hanno superato lo stato di fine ciclo di vita. È inoltre necessario tenere in considerazione i requisiti aziendali, in quanto molti ambienti possono tollerare, se non addirittura accogliere con favore, l'aggiunta di ulteriori funzionalità con processi di test/convalida minimi o assenti e con alcuni tempi di inattività. I clienti devono inoltre tenere conto dei dati più recenti raccolti durante le operazioni di rilascio di Cisco quando valutano i requisiti di test. Un'analisi dei bug e delle cause principali ha mostrato che la maggior parte delle cause principali dei bug sono il risultato della codifica degli sviluppatori all'interno dell'area software interessata. Ciò significa che se un'organizzazione aggiunge una particolare funzionalità o modulo alla rete in una versione esistente, è possibile che si sia verificato un bug relativo a tale funzionalità o modulo, ma è possibile che le probabilità che la nuova funzionalità, il nuovo hardware o il nuovo modulo influiscano su altre aree siano molto inferiori. Questi dati dovrebbero consentire alle organizzazioni di ridurre i requisiti di test, quando aggiungono nuove funzionalità o moduli supportati nelle versioni esistenti, testando solo il nuovo servizio o funzionalità in combinazione con altri servizi abilitati. I dati devono essere presi in considerazione anche quando si aggiorna il software in base ad alcuni bug critici trovati nella rete.

Nella tabella seguente vengono indicati i requisiti di aggiornamento consigliati per le organizzazioni aziendali a elevata disponibilità principali:

Trigger gestione software	Requisiti del ciclo di vita del software
Nuovo servizio di rete. Ad esempio, una nuova backbone ATM o un nuovo servizio VPN.	Convalida completa del ciclo di vita del software, inclusi test delle nuove funzionalità (in combinazione con altri servizi abilitati), test della topologia compressi, analisi delle prestazioni what-if e test del profilo dell'applicazione.
La nuova funzionalità di rete non è supportata nella versione software corrente. Gli esempi includono QoS e Multiprotocol Label Switching (MPLS).	Convalida completa del ciclo di vita del software, inclusi test delle nuove funzionalità, insieme ad altri servizi abilitati, test della topologia compressi, analisi delle prestazioni what-if e test del profilo dell'applicazione.
Nuova funzionalità principale o nuovo modulo hardware disponibile nella versione corrente. Ad esempio, aggiungendo un nuovo modulo GigE, supporto multicast o DLSW.	Processo di gestione dei candidati. Possibile convalida completa in base ai requisiti di rilascio. Possibile limitazione dei test e della convalida se la gestione dei candidati identifica la release corrente come potenzialmente accettabile.

Aggiunta di funzionalità secondarie. Ad esempio, un dispositivo TACACS per il controllo degli accessi.	Considerare la gestione dei candidati in base al rischio della funzionalità. Valutare la possibilità di testare o sperimentare la nuova funzionalità in base al rischio.
Software in produzione per due anni o una revisione trimestrale del software.	Gestione dei candidati e decisioni aziendali relative alla gestione completa del ciclo di vita per identificare la release supportabile corrente.

Aggiornamenti di emergenza

In alcuni casi, le aziende devono aggiornare il software a causa di problemi gravi. Ciò può causare problemi se l'organizzazione non dispone di una metodologia di aggiornamento di emergenza. I problemi relativi al software possono variare dagli aggiornamenti non gestiti, in cui il software viene aggiornato senza gestione del ciclo di vita del software, alle situazioni in cui i dispositivi di rete si bloccano continuamente, ma l'organizzazione non esegue l'aggiornamento in quanto la certificazione e i test della prossima versione non sono stati completati. Cisco consiglia un processo di aggiornamento di emergenza in queste situazioni in cui vengono eseguiti test e test pilota limitati in aree meno critiche della rete.

Se si verificano errori irreversibili senza una soluzione apparente e il problema è relativo a un difetto del software, Cisco consiglia di rivolgersi al supporto Cisco per isolare il difetto e determinare se o quando è disponibile una soluzione. Quando la correzione è disponibile, Cisco consiglia un ciclo di aggiornamento di emergenza per determinare rapidamente se il problema può essere risolto con un tempo di inattività limitato. Nella maggior parte dei casi, un'organizzazione esegue una versione supportata del codice e la correzione del problema è disponibile in una versione provvisoria esistente del software.

Le organizzazioni possono anche prepararsi a potenziali aggiornamenti di emergenza. La preparazione include la migrazione alle versioni Cisco IOS supportate e l'identificazione e lo sviluppo delle versioni sostitutive candidate all'interno dello stesso treno Cisco IOS della versione certificata. Il software supportato è importante perché significa che lo sviluppo Cisco sta ancora aggiungendo correzioni ai bug nella sequenza di software identificata. Mantenendo il software supportato nella rete, l'organizzazione riduce i tempi di convalida grazie alla più familiare e stabile base di codice. In genere, una sostituzione candidata è una nuova immagine software provvisoria all'interno dello stesso treno Cisco IOS senza aggiunte di funzionalità o supporto hardware. Una strategia di sostituzione dei candidati è particolarmente importante se l'organizzazione è nella fase iniziale di adozione di un particolare programma software.

Processo di certificazione

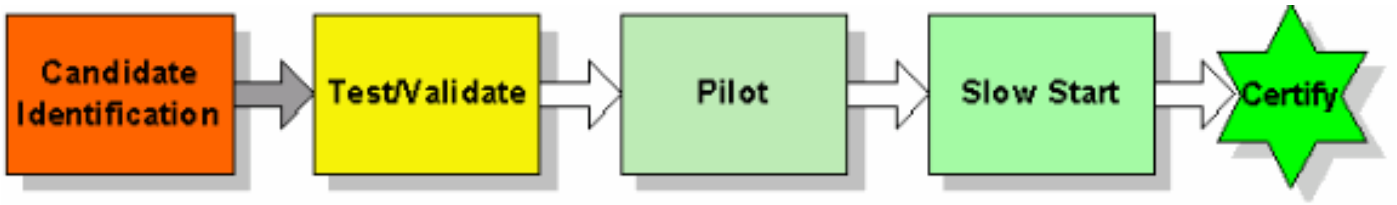
Un processo di certificazione contribuisce a garantire che il software convalidato venga implementato in modo coerente nell'ambiente di produzione dell'organizzazione. Le fasi del processo di certificazione dovrebbero includere l'identificazione dei percorsi, le definizioni dei cicli di aggiornamento, la gestione dei candidati, il test e la convalida e un utilizzo pilota della produzione. Un semplice processo di certificazione, tuttavia, contribuisce ancora a garantire che versioni software coerenti vengano distribuite all'interno dei percorsi identificati.

Avvio di un processo di certificazione attraverso l'identificazione di individui provenienti

dall'architettura, dalla progettazione/implementazione e dalle operazioni per redigere e gestire il processo di certificazione. Il gruppo deve prima prendere in considerazione gli obiettivi aziendali e le risorse per garantire che il processo di certificazione continui ad avere successo. Successivamente, assegnare la responsabilità generale di singoli utenti o gruppi per le fasi chiave del processo di certificazione, tra cui gestione dei percorsi, definizioni di aggiornamento del ciclo di vita, test/convalida e programmi pilota. Ognuna di queste aree deve essere definita, approvata e comunicata formalmente all'interno dell'organizzazione.

Includere anche linee guida per la qualità o l'approvazione in ogni fase del processo di certificazione. Questo processo viene talvolta denominato processo di controllo qualità in quanto è necessario soddisfare alcuni criteri di qualità prima di passare alla fase successiva. Ciò contribuisce a garantire che il processo di certificazione sia efficace e valga le risorse assegnate. In generale, quando si riscontrano problemi di qualità in un'area, il processo spinge indietro di una fase lo sforzo.

I candidati software potrebbero non soddisfare i criteri di certificazione definiti a causa della qualità del software o di comportamenti imprevisti. Quando vengono rilevati problemi che hanno un impatto sull'ambiente, l'organizzazione deve disporre di un processo più semplice per certificare una versione provvisoria successiva. In questo modo è possibile ridurre i requisiti di risorse e in genere è efficace se l'organizzazione è in grado di comprendere quali modifiche sono state apportate e quali problemi sono stati risolti. Non è insolito per un'organizzazione riscontrare un problema con un candidato iniziale e certificare una versione successiva provvisoria di Cisco IOS. Le organizzazioni possono anche eseguire una certificazione limitata o fornire avvertenze in caso di problemi e possono eseguire l'aggiornamento a una versione completamente certificata successiva quando viene convalidata una nuova versione provvisoria. Il diagramma riportato di seguito rappresenta un processo di certificazione di base e include i controlli di qualità (una revisione dopo ogni blocco):



Progettazione - Selezione e convalida delle versioni di Cisco IOS

La disponibilità di una metodologia ben definita per la selezione e la convalida delle versioni di Cisco IOS consente alle aziende di ridurre i tempi di inattività non pianificati dovuti a tentativi di aggiornamento non riusciti e a difetti software non pianificati.

La fase di progettazione comprende la gestione dei candidati e la fase di test/convalida. La gestione dei candidati è il processo utilizzato per identificare versioni specifiche per le tracce software definite. I test e la convalida fanno parte del processo di certificazione e garantiscono che la versione del software identificata abbia esito positivo nel percorso richiesto. Le attività di test e convalida devono essere eseguite in un ambiente lab con topologia e configurazione compresse molto simili all'ambiente di produzione.

Strategia e strumenti per la selezione e la convalida di Cisco IOS

Ogni organizzazione deve disporre di un processo per selezionare e convalidare le versioni Cisco IOS standard per la rete, iniziando da un processo per selezionare la versione Cisco IOS. Il

processo di gestione dei candidati deve essere definito e documentato da un team interfunzionale che comprenda architettura, progettazione e operazioni. Una volta approvato, il processo deve essere consegnato al gruppo di consegna appropriato. Si consiglia inoltre di creare un modello standard di gestione dei candidati che possa essere aggiornato con le informazioni sui candidati man mano che vengono identificati.

Non tutte le organizzazioni dispongono di un ambiente di laboratorio sofisticato in grado di simulare facilmente l'ambiente di produzione. Alcune organizzazioni non eseguono i test di laboratorio a causa dei costi e della capacità di eseguire la sperimentazione di una nuova versione della rete senza alcun impatto significativo sul business. Tuttavia, le organizzazioni ad alta disponibilità sono incoraggiate a creare un laboratorio che simuli la rete di produzione e a sviluppare un processo di test/convalida per garantire un'elevata copertura dei test per le nuove versioni di Cisco IOS. Un'organizzazione dovrebbe permettere circa sei mesi di costruire il laboratorio. Durante questo periodo, l'organizzazione dovrebbe lavorare per creare piani e processi di test specifici per garantire che il laboratorio venga utilizzato al massimo vantaggio. Per Cisco IOS, ciò significa la creazione di piani di test Cisco IOS specifici per ogni traccia software richiesta. Questi processi sono fondamentali nelle organizzazioni più grandi, in quanto molti laboratori non vengono utilizzati per l'introduzione di nuovi prodotti e software.

Nelle sezioni seguenti vengono descritti brevemente gli strumenti di gestione e test/convalida dei candidati da utilizzare per la selezione e la convalida di Cisco IOS.

Strumenti di gestione dei candidati

Nota: per utilizzare la maggior parte degli strumenti forniti di seguito, è necessario essere un utente registrato e aver eseguito l'accesso.

- Note release: fornisce informazioni relative all'hardware, al modulo e al supporto delle funzionalità di una release. Le note di rilascio devono essere esaminate durante la gestione del candidato per garantire che nella potenziale release esista tutto il supporto hardware e software necessario e per comprendere eventuali problemi di migrazione, inclusi diversi comportamenti predefiniti o requisiti di aggiornamento.

Strumenti di test e convalida

Gli strumenti di test e convalida vengono utilizzati per testare e convalidare le soluzioni di rete, inclusi nuovi prodotti hardware, software e applicazioni.

- **Generatori traffico** (**Traffic Generator**) - Genera flussi di traffico multiprotocollo e velocità dei pacchetti raw utilizzate per modellare la velocità su un particolare collegamento utilizzando protocolli specifici. Gli utenti possono specificare l'indirizzo MAC di origine, di destinazione e i numeri dei socket. Questi valori possono essere incrementati in base ai passaggi specificati oppure configurati per essere statici/fissi o a incrementi casuali. I generatori di traffico possono generare i pacchetti per i seguenti protocolli:IPIPX (Internetwork Packet Exchange)DECnetAppleXerox Network Systems (XNS)Protocollo ICMP (Internet Control Message Protocol)Protocollo IGMP (Internet Group Management Protocol)CLNS (Connectionless Network Service)UDP (User Datagram Protocol)VINES (Virtual Integrated Network Service)Pacchetti Data LinkGli strumenti sono disponibili presso Agilent e Spirent Communications .
- **Packet Counter/Capture/Decoder (Sniffer)**: consente al cliente di acquisire e decodificare in modo selettivo i pacchetti a tutti i livelli del pacchetto e del collegamento dati. Lo strumento ha la capacità di consentire all'utente di specificare i filtri, il che consente l'acquisizione solo di

dati di protocollo specifici. I filtri consentono inoltre all'utente di specificare l'acquisizione dei pacchetti corrispondenti a un particolare indirizzo IP, numero di porta o indirizzo MAC. Sono disponibili strumenti da Sniffer Technologies .

- **Simulatore/emulatore di rete**: consente al cliente di popolare le tabelle di routing di router specifici, in base ai requisiti della rete di produzione. Supporta la generazione di router IP Routing Information Protocol (RIP), OSPF, Intermediate System-to-Intermediate System (IS-IS), Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP) e Border Gateway Protocol (BGP). Gli strumenti sono disponibili da PacketStorm Communications e Spirent Communications.
- **Emulatori di sessione**: generano flussi di traffico multiprotocollo a finestra scorrevole e sono in grado di inviare flussi di traffico multiprotocollo attraverso la rete di test verso il dispositivo ricevente. Il dispositivo ricevente rimanda i pacchetti alla sorgente. Il dispositivo di origine verifica il numero di pacchetti inviati, ricevuti, non in sequenza e di pacchetti con errori. Lo strumento offre inoltre la flessibilità necessaria per definire i parametri della finestra nel protocollo TCP (Transmission Control Protocol), imitando così da vicino le sessioni di traffico client/server nella rete lab. Gli strumenti sono disponibili presso Empirix .
- **Emulatori di rete su larga scala**: consentono di testare la scalabilità di ambienti di grandi dimensioni. Questi strumenti sono in grado di creare e inserire facilmente il traffico di controllo in una topologia di laboratorio per simulare più da vicino un ambiente di produzione. Le funzionalità includono iniettori di routing, router adiacenti di protocollo e router adiacenti di protocollo di livello 2. Gli strumenti sono disponibili presso Agilent e Spirent Communications .
- **Simulatori WAN**: ideali per il test del traffico delle applicazioni aziendali in cui la larghezza di banda e il ritardo possono rappresentare un problema. Questi strumenti consentono alle organizzazioni di testare localmente un'applicazione con il ritardo e la larghezza di banda stimati per verificare il funzionamento dell'applicazione sulla WAN. Questi strumenti vengono spesso utilizzati per lo sviluppo di applicazioni e per la creazione di profili dei tipi di test all'interno delle organizzazioni aziendali. Adtech, una divisione di Spirent Communications e Shunra forniscono strumenti di simulazione WAN.

Gestione candidati

La gestione dei candidati è il processo di identificazione dei requisiti di versione del software e dei rischi potenziali per l'hardware specifico e le funzionalità abilitate. Si consiglia a un'organizzazione di dedicare da quattro a otto ore alla ricerca corretta dei requisiti software, delle note di rilascio, dei difetti software e dei potenziali rischi prima di sperimentare una release. Di seguito sono descritte le basi per la gestione dei candidati:

- Identificazione dei software candidati tramite gli strumenti Cisco Connection Online (CCO).
- Maturità del software di analisi dei rischi, nuova funzionalità o supporto del codice.
- Identificazione e monitoraggio dei bug, dei problemi e dei requisiti software noti durante l'intero ciclo di vita.
- Identifica il comportamento di configurazione predefinito dell'immagine selezionata.
- Mantenere candidati di tipo "roll-out" e "roll-forward" per potenziali modifiche dei candidati.
- Bug-scrubs.
- Supporto Cisco Advanced Services.

L'identificazione dei candidati al software è diventata più complessa con il crescente numero di produzioni e software Cisco in formazione. CCO dispone ora di diversi strumenti, tra cui Cisco IOS upgrade planner, software search tool, software-hardware compatibility matrix e lo strumento di

aggiornamento dei prodotti, che possono aiutare le organizzazioni a identificare potenziali release candidate. Questi strumenti sono disponibili all'indirizzo http://www.cisco.com/cisco/software/navigator.html.

Analizzare quindi i rischi del software potenzialmente idoneo. Si tratta del processo di comprensione della posizione attuale del software sulla curva di maturità e di valutazione dei requisiti per l'installazione con il rischio potenziale del candidato della release. Ad esempio, se un'organizzazione desidera installare il software di distribuzione rapida in un ambiente critico ad alta disponibilità, è necessario considerare i rischi e i requisiti di risorse associati per ottenere la certificazione. Per garantire il successo, un'organizzazione dovrebbe almeno aggiungere risorse di gestione software per le situazioni a rischio più elevato. Se invece è disponibile una versione di distribuzione generale (GD, General Deployment) che soddisfa le esigenze di un'organizzazione, sono necessarie meno risorse di gestione del software.

Quando vengono identificati potenziali rilasci e rischi, eseguire una pulitura dei bug per determinare se sono presenti bug catastrofici identificati che potrebbero impedire la certificazione. Gli agenti Bug Watcher, Bug Navigator e Bug Watcher di Cisco possono aiutare a identificare i potenziali problemi e devono essere utilizzati durante tutto il ciclo di vita del software per identificare potenziali problemi di sicurezza o di difetto.

Un nuovo software candidato deve inoltre essere esaminato per il comportamento di configurazione predefinito potenziale. A tale scopo, è possibile esaminare le note sulla versione per la nuova immagine software ed esaminare le differenze di configurazione con l'immagine potenziale caricata sulle piattaforme designate. La gestione dei candidati può inoltre includere l'identificazione di versioni di backup o di destinazione se la versione scelta non soddisfa i criteri di certificazione in un determinato momento del processo. Monitorando i bug relativi alle funzionalità di un determinato brano, un'organizzazione può gestire i potenziali candidati per la certificazione.

Cisco Advanced Services è anche uno strumento eccellente per la gestione dei candidati. Questo gruppo può fornire ulteriori informazioni sul processo di sviluppo e sulla collaborazione tra un gran numero di esperti del settore in molti ambienti di mercato verticali diversi. In genere, il supporto Cisco offre le migliori funzionalità di scrubing dei bug o di gestione dei candidati, grazie al livello di esperienza e visibilità sulle versioni software di produzione eseguite in altre organizzazioni.

Test e convalida

Il testing e la convalida rappresentano un aspetto critico delle procedure ottimali di gestione e delle reti ad alta disponibilità in generale. Test di laboratorio adeguati possono ridurre in modo significativo i tempi di inattività della produzione, contribuire alla formazione del personale di supporto della rete e semplificare i processi di implementazione della rete. Per essere efficace, tuttavia, l'organizzazione deve allocare le risorse necessarie per creare e mantenere l'ambiente di laboratorio appropriato, applicare le risorse necessarie per eseguire i test corretti e utilizzare una metodologia di test consigliata che includa la raccolta di misurazioni. Senza una di queste aree, un processo di test e convalida potrebbe non soddisfare le aspettative di un'organizzazione.

La maggior parte delle organizzazioni aziendali non dispone dell'ambiente di laboratorio di test consigliato. Per questo motivo, molte organizzazioni hanno implementato soluzioni in modo non corretto, hanno riscontrato errori di modifica della rete o problemi software che avrebbero potuto essere isolati in un ambiente di emulazione. In alcuni ambienti questo è accettabile, in quanto il costo del downtime non compensa il costo di un ambiente di laboratorio sofisticato. In molte organizzazioni, tuttavia, il downtime non può essere tollerato. Queste organizzazioni sono fortemente invitate a sviluppare i laboratori di test consigliati, i tipi di test e le metodologie di test

per migliorare la qualità della rete di produzione.

Laboratorio e ambiente di testing

Il laboratorio deve essere un'area isolata con spazio sufficiente per scrivanie, banchi di lavoro, apparecchiature di prova, armadi per apparecchiature o rack. La maggior parte delle grandi aziende necessita di un numero di rack compreso tra quattro e dieci per riprodurre l'ambiente di produzione. È consigliabile utilizzare una certa protezione fisica per mantenere un ambiente di test durante l'esecuzione dei test. In questo modo è possibile evitare che un test di laboratorio venga interrotto a causa di altre priorità di laboratorio, tra cui l'assunzione di prestiti per l'hardware, la formazione o le prove di implementazione. La sicurezza logica è consigliata anche per impedire l'ingresso di percorsi falsi nella rete di produzione o l'uscita dal laboratorio da traffico indesiderato. A tale scopo, è possibile usare filtri di routing e elenchi degli accessi estesi su un router gateway lab. La connettività alla rete di produzione è utile per i download di software e l'accesso alla rete di laboratorio dall'ambiente di produzione.

La topologia di laboratorio deve essere in grado di simulare l'ambiente di produzione per qualsiasi piano di test specifico. Si consiglia di riprodurre le configurazioni hardware, topologia di rete e funzionalità. Ovviamente, riprodurre la topologia effettiva è quasi impossibile, ma ciò che può essere fatto è riprodurre la gerarchia della rete e l'interazione tra i dispositivi di produzione. Ciò è importante per l'interazione di protocolli o funzionalità tra più dispositivi. Alcune topologie di test saranno diverse in base ai requisiti di test del software. WAN edge I test di Cisco IOS, ad esempio, non devono richiedere dispositivi di tipo LAN o test e possono richiedere solo router di edge WAN e router di distribuzione WAN. Il segreto sta nel simulare le funzionalità software senza duplicare la produzione. In alcuni casi, è possibile utilizzare gli strumenti per simulare comportamenti su larga scala, ad esempio il numero di nodi adiacenti del protocollo e le tabelle di routing.

Sono inoltre necessari strumenti per supportare alcuni tipi di test, migliorando la capacità di simulare l'ambiente di produzione e di raccogliere i dati di test. Gli strumenti che aiutano a simulare la produzione includono gli strumenti di raccolta del traffico, i generatori di traffico e i dispositivi di simulazione WAN. Gli Smartbit sono un buon esempio di dispositivo in grado di raccogliere e riprodurre il traffico di rete o generare grandi volumi di traffico. Un'organizzazione può inoltre trarre vantaggio da dispositivi che consentono di raccogliere dati, ad esempio analizzatori di protocollo.

Il laboratorio richiede anche una certa gestione. Molte organizzazioni più grandi hanno un responsabile di laboratorio a tempo pieno che ha la responsabilità della gestione della rete di laboratorio. Altre organizzazioni utilizzano l'architettura esistente e i team di progettazione per la convalida in laboratorio. Le responsabilità di Lab Management includono l'ordine delle apparecchiature di laboratorio e la tracciatura degli asset, il cablaggio, la gestione dello spazio fisico, la definizione delle regole e della direzione del laboratorio, la pianificazione del laboratorio, la documentazione di laboratorio, l'impostazione delle topologie di laboratorio, la scrittura di piani di test, l'esecuzione di test di laboratorio e la gestione dei potenziali problemi identificati.

Tipi di test

In generale, è possibile eseguire diversi tipi di test. Prima di creare un laboratorio di test completo e un piano di test in grado di testare tutto in una moltitudine di configurazioni, è necessario che un'organizzazione comprenda i diversi tipi di test, le finalità dei test e se Cisco Engineering, Technical Marketing o Customer Advocacy debbano o possano essere responsabili di alcuni dei vari test. I piani di test dei clienti riguardano generalmente i tipi di test più esposti. La tabella seguente aiuta a comprendere i diversi tipi di test, il momento in cui devono essere eseguiti i test e

le parti responsabili.

Tra i test riportati di seguito, il test corretto del set di funzionalità, della topologia e della combinazione di applicazioni specifiche di un'organizzazione è in genere il più utile. È importante sapere che Cisco esegue test completi sulle funzionalità e sulla regressione, ma non è in grado di testare il profilo dell'applicazione dell'organizzazione con una combinazione specifica di topologia, hardware e funzionalità configurate. Non è infatti possibile testare l'intera gamma di funzionalità, hardware, moduli e permutazioni topologiche. Inoltre, Cisco non può testare l'interoperabilità con apparecchiature di terze parti. Cisco consiglia alle organizzazioni di testare la combinazione precisa di hardware, moduli, funzionalità e topologia presenti nel proprio ambiente. Questo test deve essere condotto in laboratorio, con una topologia compressa che rappresenta l'ambiente di produzione dell'organizzazione con altri tipi di test di supporto, quali prestazioni, interoperabilità, interruzione delle attività e burn-in.

Test	Panoramica dei test	Test responsabilità
Caratteristiche e funzionalità	Determina se le funzionalità base di Cisco IOS e i moduli hardware Cisco funzionano come annunciato. È necessario testare la funzionalità della feature o del modulo e le opzioni di configurazione della feature. La rimozione e l'aggiunta della configurazione devono essere verificate. Sono inclusi i test di base per l'interruzione delle attività e i test di burn-in.	Test dei dispositivi Cisco
Regressione	Determina se la funzionalità o il modulo funziona in combinazione con altri moduli e funzionalità e se la versione di Cisco IOS	Test di regressione Cisco

	funziona in combinazione con altre versioni di Cisco IOS in relazione alle funzionalità definite. Include alcuni test di burn-in e di interruzione.	
Prestazioni di base del dispositivo	Determina le prestazioni di base della funzionalità o del modulo per determinare se la funzionalità o i moduli hardware Cisco IOS soddisfano i requisiti minimi in fase di caricamento.	Cisco Device Testing
Combinazione topologia/funzionalità/hardware	Determina se le funzionalità e i moduli funzionano come previsto in una specifica combinazione di topologia e modulo/funzionalità/hardware. Questo test deve includere la verifica del protocollo, la verifica delle funzionalità, la verifica dei comandi **show**, il test di burn-in e il test di interruzione.	Cisco testa le topologie pubblicizzate standard in laboratori quali Enterprise Solutions Engineering (ESE) e Network Solutions Integration Test Engineering (NSITE). I clienti ad alta disponibilità devono testare le combinazioni di funzionalità/modulo/topologia in base alle esigenze, in particolare con il software per utenti meno esperti e le topologie non standard.
Interruzione (What-if)	Include tipi o comportamenti comuni di interruzione che possono verificarsi in un	Cisco è responsabile dei test di base delle interruzioni. I clienti sono in ultima analisi responsabili dei problemi di prestazioni

	ambiente con funzionalità, moduli o topologie specifiche e il potenziale impatto sulle funzionalità. I test delle interruzioni includono lo scambio delle schede, i link flap, gli errori dei dispositivi, gli errori dei collegamenti e gli errori delle schede.	dovuti alla scalabilità del singolo ambiente. Il test delle interruzioni deve essere eseguito, se possibile, nell'ambiente di laboratorio del cliente.
Prestazioni di rete (What-if)	Analizza il carico del dispositivo in relazione a una combinazione di funzionalità, hardware e topologia specifica. L'attenzione è rivolta alla capacità e alle prestazioni dei dispositivi, quali CPU, memoria, utilizzo dei buffer e utilizzo dei collegamenti in relazione a un tipo di traffico impostato e ai requisiti delle risorse per protocolli, router adiacenti, numero di route e altre funzionalità. Il test consente di garantire la scalabilità in	I clienti sono in ultima analisi responsabili del carico e della scalabilità dei dispositivi. I problemi di carico e scalabilità sono spesso sollevati dalle vendite Cisco o dai servizi avanzati e vengono spesso testati con i laboratori Cisco, ad esempio i laboratori CPOC (Customer Proof-of-Concept Labs).

	ambienti di grandi dimensioni.	
Correzione dei bug	Assicura che le correzioni dei bug correggano il difetto identificato.	Cisco testa le correzioni dei bug per assicurarsi che siano state risolte. Inoltre, i clienti devono eseguire i test per essere certi che il bug riscontrato sia risolto e che non interrompa altri aspetti del modulo o della funzionalità. Le release di manutenzione sono testate per la regressione, mentre le release provvisorie non lo sono.
Gestione della rete	Analizza le funzionalità di gestione SNMP (Simple Network Management Protocol), l'accuratezza delle variabili MIB SNMP, il supporto trap e il supporto Syslog.	Cisco è responsabile del test delle funzionalità SNMP di base e dell'accuratezza delle variabili MIB. I clienti devono convalidare i risultati della gestione della rete e sono in ultima analisi responsabili della strategia e della metodologia di gestione per le installazioni di nuove tecnologie.
Emulazione di rete su larga scala	L'emulazione di rete su larga scala utilizza strumenti come il simulatore di router di Agilent e la suite di strumenti di test di Spirent per simulare ambienti di grandi dimensioni. Ciò può includere i vicini di protocollo, il	I clienti Cisco sono in genere responsabili degli aspetti dei test di simulazione della rete che riproducono il loro ambiente di rete, che possono includere il numero di vicini/adiacenze del protocollo di routing, le dimensioni della tabella di routing associata e altre risorse in produzione.

	conteggio dei PVC (Permanent Virtual Circuit) del frame relay, le dimensioni delle tabelle di routing, le voci della cache e altre risorse tipicamente richieste nella produzione che non sono in laboratorio per impostazione predefinita.	
Interoperabilità	Verifica tutti gli aspetti relativi alla connettività con apparecchiature di rete di terze parti, in particolare se è richiesta l'interoperabilità dei protocolli o dei segnali.	I clienti Cisco sono in genere responsabili di tutti gli aspetti dei test di interoperabilità.
Masterizzazione	Analizza le risorse del router nel tempo. I test di masterizzazione richiedono in genere che un dispositivo sia sottoposto a un certo carico con analisi dell'utilizzo delle risorse, inclusi memoria, CPU e buffer, nel tempo.	Cisco esegue test di masterizzazione di base. Si consiglia di effettuare test presso i clienti in relazione a combinazioni esclusive di topologia, dispositivi e funzionalità.

Metodologia di testing

Una volta che un'organizzazione è a conoscenza di ciò che sta testando, è necessario sviluppare una metodologia per il processo di testing. Lo scopo di una metodologia di test basata su best practice è quello di contribuire a garantire che i test concordati siano completi, ben documentati,

facilmente riproducibili e utili per individuare potenziali problemi di produzione. La documentazione e la ricreazione di scenari lab sono particolarmente importanti per il test di versioni successive o per il test delle correzioni dei bug rilevate nell'ambiente lab. Le fasi di una metodologia di test sono illustrate di seguito. È inoltre possibile eseguire alcune operazioni di test contemporaneamente.

1. Creare una topologia di test che simuli l'ambiente di produzione sottoposto a test. Un ambiente di test del perimetro della WAN può includere solo alcuni router di base e un router perimetrale, mentre un test della LAN può includere più dispositivi in grado di rappresentare al meglio l'ambiente.
2. Configurare le funzionalità che simulano l'ambiente di produzione. La configurazione dei dispositivi di laboratorio deve corrispondere esattamente alle configurazioni hardware e software dei dispositivi di produzione previsti.
3. Scrivere un piano di test, definendo test e obiettivi, documentando la topologia e definendo test funzionali. I test includono la convalida di protocollo di base, la convalida del comando show, il test di interruzione e il test di burn-in. Nella tabella seguente è riportato un esempio di un test specifico all'interno di un piano di test.
4. Convalida funzionalità di routing e protocollo. Documento o baseline: previsti risultati del comando **show**. I protocolli devono includere sia protocolli di layer 2, quali ATM, Frame Relay, Cisco Discovery Protocol (CDP), Ethernet e Spanning-Tree, sia protocolli di layer 3, quali IP, IPX e multicast.
5. Convalidare la funzionalità della feature. Documento o baseline: previsti risultati del comando **show**. Le funzionalità possono includere comandi di configurazione globali e qualsiasi funzionalità critica, ad esempio autenticazione, autorizzazione e accounting (AAA).
6. Simulare il carico previsto nell'ambiente di produzione. La simulazione del carico può essere eseguita con i dispositivi di raccolta del traffico o i generatori. Convalidare le variabili di utilizzo previste dei dispositivi di rete, inclusi CPU, memoria, utilizzo del buffer e statistiche dell'interfaccia, con un'analisi di eventuali perdite di pacchetti. Documento o baseline: previsti risultati del comando **show**.
7. Eseguire i test di interruzione delle attività nei punti in cui è previsto che il dispositivo e il software gestiscano o prevengano il carico insufficiente. Ad esempio, la rimozione della scheda, il link flapping, il route flapping e le tempeste broadcast. Verificare che vengano generate le trap SNMP corrette in base alle funzionalità utilizzate nella rete.
8. I risultati dei test e le misurazioni dei dispositivi devono essere ripetibili.

Nome test	**Failover HSRP (Hot Standby Router Protocol)**
Requisiti di configurazione del test	Applicare il carico all'interfaccia del gateway primario. Il traffico dovrebbe essere all'incirca del 20% verso il gateway dalla prospettiva della stazione utente e del 60% verso la prospettiva della stazione utente. Inoltre, aumentare il traffico a un carico superiore.
Passaggi test	Monitorare STP e HSRP tramite i comandi **show**. Interrompere la connessione dell'interfaccia del gateway primario e quindi ripristinare la connessione dopo la raccolta delle informazioni.
Misurazioni previste	CPU durante il failover. Visualizzare l'interfaccia prima, durante e dopo il gateway primario e secondario. Mostra HSRP prima, durante e

	dopo.
Risultati previsti	Il gateway primario esegue il failover sull'altro gateway del router entro due secondi. i comandi **show** riflettono correttamente la modifica. Il failover sul gateway primario si verifica quando viene ripristinata la connettività.
Risultati effettivi	
Superato o non superato	
Modifiche necessarie per ottenere il superamento	

Misurazioni dispositivo

Durante la fase di prova, effettuare e documentare le seguenti misurazioni per verificare che il dispositivo funzioni correttamente:

- Utilizzo memoria
- Carichi CPU
- Utilizzo buffer
- Statistiche interfaccia
- Tabelle cicli di lavorazione
- Debug specifico

Le informazioni relative alle misurazioni variano a seconda del particolare test implementato. A seconda dei problemi specifici da affrontare, possono essere disponibili ulteriori informazioni per la misurazione.

Per ogni applicazione sottoposta a test, misurare i parametri per garantire che non vi sia un impatto negativo sulle prestazioni per l'applicazione in questione. A tale scopo, è possibile utilizzare una baseline delle prestazioni che consente di confrontare le prestazioni prima e dopo l'installazione. Esempi di test di misurazione delle applicazioni sono:

- Tempo medio necessario per l'accesso a una rete.
- Tempo medio necessario per la copia di un gruppo di file NFS (Network File System).
- Tempo medio necessario per avviare un'applicazione e visualizzare la prima schermata.
- Altri parametri specifici dell'applicazione.

Implementazione - Implementazione rapida e corretta di Cisco IOS

Un processo di implementazione ben definito consente alle aziende di implementare in modo efficiente le nuove versioni di Cisco IOS.

La fase di attuazione comprende il processo pilota e il processo di attuazione. Il processo pilota garantisce la riuscita della versione Cisco IOS nell'ambiente e il processo di implementazione consente implementazioni Cisco IOS su larga scala, rapide e corrette.

Strategia e strumenti per le implementazioni di Cisco IOS

La strategia per le implementazioni Cisco IOS è quella di eseguire la certificazione finale tramite un processo pilota e un'installazione rapida utilizzando strumenti di aggiornamento e un processo di implementazione ben definito.

Prima di avviare un processo pilota di rete, molte organizzazioni creano linee guida generali. Le linee guida per i piloti devono includere le aspettative per tutti i piloti, come i criteri di successo, le posizioni di volo accettabili, la documentazione di volo, le aspettative dei proprietari dei piloti, i requisiti di notifica degli utenti e la durata prevista dei piloti. Un team interfunzionale di progettazione, implementazione e operazioni è normalmente coinvolto nella creazione di linee guida generali e di un processo pilota. Una volta creato il processo pilota, i singoli gruppi di attuazione possono di norma condurre con successo i progetti pilota utilizzando i metodi migliori identificati.

Dopo aver approvato la distribuzione e la certificazione finale di una nuova versione del software, l'organizzazione deve iniziare a pianificare l'aggiornamento di Cisco IOS. La pianificazione inizia con l'identificazione dei nuovi requisiti dell'immagine, tra cui piattaforma, memoria flash e configurazione. Normalmente, i gruppi di progettazione e architettura definiscono nuovi requisiti dell'immagine software nella fase di gestione candidata del ciclo di vita della gestione di Cisco IOS. Una volta identificati i requisiti, ciascun dispositivo deve essere convalidato ed eventualmente aggiornato dal gruppo di implementazione. Il modulo CiscoWorks 2000 Software Image Manager (SWIM) può inoltre eseguire la fase di convalida tramite la convalida dei requisiti Cisco IOS rispetto all'inventario dei dispositivi. Una volta convalidati e/o aggiornati tutti i dispositivi ai nuovi standard di immagine corretti, il gruppo di implementazione può avviare un processo di implementazione lento utilizzando il modulo SWIM di CiscoWorks2000 come strumento di distribuzione del software.

Dopo che la nuova immagine è stata distribuita correttamente più volte, l'organizzazione può iniziare una distribuzione rapida utilizzando CiscoWorks SWIM.

Cisco IOS Inventory Management

Lo strumento di gestione dell'inventario CiscoWorks 2000 Resource Manager Essentials (RME) semplifica notevolmente la gestione delle versioni dei router e degli switch Cisco tramite strumenti di reporting basati sul Web che segnalano e ordinano i dispositivi Cisco IOS in base alla versione del software, alla piattaforma del dispositivo e al nome del dispositivo.

Cisco IOS SWIM

Il software CiscoWorks 2000 SWIM può contribuire a ridurre le complessità del processo di upgrade soggette a errori. I collegamenti integrati a CCO correlano le informazioni online di Cisco sulle patch software con i software Cisco IOS e Catalyst implementati nella rete, evidenziando le note tecniche correlate. I nuovi strumenti di pianificazione individuano i requisiti di sistema e inviano notifiche quando sono necessari aggiornamenti hardware (ROM di avvio, RAM flash) per

supportare gli aggiornamenti delle immagini software proposte.

Prima di avviare un aggiornamento, i prerequisiti di una nuova immagine vengono convalidati in base ai dati di inventario dello switch di destinazione o del router per garantire la riuscita dell'aggiornamento. Quando si aggiornano più dispositivi, SWIM sincronizza le attività di download e consente all'utente di monitorare lo stato del processo. I processi pianificati vengono controllati tramite un processo di conclusione, che consente ai responsabili di autorizzare le attività di un tecnico prima di avviare ogni task di aggiornamento. RME 3.3 include la capacità di analizzare gli aggiornamenti software per le piattaforme Cisco IGX, BPX e MGX, semplificando notevolmente e riducendo il tempo necessario per determinare l'impatto di un aggiornamento software.

Processo pilota

Per ridurre al minimo l'esposizione potenziale e acquisire in modo più sicuro i problemi di produzione rimanenti, si consiglia un software pilota. I programmi pilota sono in genere più importanti per le installazioni di nuove tecnologie, tuttavia molte nuove installazioni software saranno collegate a nuovi servizi, funzionalità o hardware, dove un progetto pilota è più critico. Il piano pilota individuale dovrebbe prendere in considerazione la selezione del pilota, la sua durata e la misura. La selezione pilota è il processo di identificazione di quando e dove un pilota dovrebbe essere eseguito. La misurazione pilota è il processo di raccolta dei dati necessari per identificare i risultati positivi e negativi o i potenziali problemi.

La selezione pilota consente di identificare dove e come verrà completato un progetto pilota. Un pilota può iniziare con un dispositivo in un'area a basso impatto ed estendersi a più dispositivi in un'area ad alto impatto. Di seguito sono riportate alcune considerazioni relative alla selezione pilota in cui l'impatto può essere ridotto:

- Installato in un'area della rete resiliente all'impatto di un singolo dispositivo dovuto alla ridondanza.
- In un'area della rete con un numero minimo di utenti dietro il dispositivo selezionato che possono gestire qualche possibile impatto sulla produzione.
- Prendere in considerazione la separazione del progetto pilota in base alle linee dell'architettura. Ad esempio, è possibile sperimentarlo nei livelli di accesso, distribuzione e/o core della rete.

La durata di questo pilota deve essere basata sul tempo necessario per testare e valutare in modo sufficiente tutte le caratteristiche del dispositivo. Ciò dovrebbe includere sia il burn-in che la rete in condizioni di carico di traffico normale. La durata dipende anche dalla fase di aggiornamento del codice e dall'area della rete in cui Cisco IOS è in esecuzione. Se Cisco IOS è una nuova versione principale, è preferibile un periodo pilota più lungo. Se invece l'upgrade è una release di manutenzione con nuove funzionalità minime, sarà sufficiente un periodo pilota più breve.

Durante la fase pilota è importante monitorare e documentare i risultati in modo simile ai test iniziali. Ciò può includere indagini sugli utenti, raccolta dati pilota, raccolta problemi e criteri di successo/fallimento. Le persone dovrebbero essere direttamente responsabili del monitoraggio e del monitoraggio dei progressi dei progetti pilota per garantire che tutti i problemi siano identificati e che gli utenti e i servizi coinvolti nel progetto pilota siano soddisfatti dei risultati del progetto pilota. La maggior parte delle organizzazioni certificherà una release se viene eseguita con successo in un ambiente pilota o di produzione. Questo passaggio è un fallimento critico in alcuni ambienti a causa di un successo percepito quando non vengono identificati o documentati criteri di misurazione o di successo.

Implementazione

Dopo aver completato la fase pilota nella rete di produzione, iniziare la fase di implementazione di Cisco IOS. La fase di implementazione comprende diverse fasi per garantire il successo dell'aggiornamento software e l'efficienza dell'implementazione, tra cui lento avvio dell'implementazione, certificazione finale, preparazione dell'aggiornamento, automazione dell'aggiornamento e convalida finale.

L'implementazione con avvio lento è il processo di implementazione lenta di una release appena testata per garantire che l'immagine abbia un'esposizione completa all'ambiente di produzione prima della certificazione finale e della conversione in scala reale. Alcune organizzazioni possono iniziare con un dispositivo e un giorno di esposizione prima di passare a due aggiornamenti del dispositivo il giorno successivo e forse altri ancora il giorno successivo. Quando sono stati messi in produzione circa dieci dispositivi, l'organizzazione può attendere fino a una o due settimane prima della certificazione finale per la particolare versione di Cisco IOS. Dopo la certificazione finale, l'organizzazione può distribuire più rapidamente la versione identificata con un livello di affidabilità molto più elevato.

Dopo un processo di avvio lento, tutti i dispositivi identificati per l'aggiornamento devono essere esaminati e convalidati utilizzando l'inventario dei dispositivi e una matrice degli standard minimi Cisco IOS per bootstrap, DRAM e flash per verificare che i requisiti siano soddisfatti. I dati possono essere acquisiti tramite strumenti interni, strumenti SNMP di terze parti o tramite l'utilizzo di CiscoWorks2000 RME. CiscoWorks 2000 SWIM esamina o analizza queste variabili prima dell'implementazione. Tuttavia, è sempre una buona idea sapere cosa aspettarsi durante i tentativi di implementazione.

Se sono pianificati più di cento dispositivi simili per l'aggiornamento, si consiglia di utilizzare un metodo automatico. È stato dimostrato che l'automazione consente di migliorare l'efficienza dell'aggiornamento e di aumentare la percentuale di successo dell'aggiornamento dei dispositivi durante installazioni di grandi dimensioni, in base a un aggiornamento interno di 1000 dispositivi con e senza SWIM. Cisco consiglia di utilizzare CiscoWorks 2000 SWIM per installazioni di grandi dimensioni a causa del grado di verifica eseguito durante l'aggiornamento. Se viene rilevato un problema, SWIM esce anche da una versione di Cisco IOS. Il servizio SWIM consente di creare e pianificare processi di aggiornamento, in cui un processo viene configurato con i dispositivi, le immagini di aggiornamento desiderate e il tempo di esecuzione del processo. Ogni processo deve contenere al massimo dodici aggiornamenti di dispositivi e possono essere eseguiti fino a dodici processi contemporaneamente. Inoltre, SWIM verifica che la versione di aggiornamento Cisco IOS pianificata sia in esecuzione dopo l'aggiornamento. Si consiglia di attendere circa venti minuti per ogni aggiornamento (compresa la verifica) del dispositivo. Utilizzando questa formula, un'organizzazione può aggiornare trentasei dispositivi all'ora. Cisco consiglia inoltre di aggiornare un massimo di cento dispositivi alla sera per ridurre la potenziale esposizione ai problemi.

In seguito a un aggiornamento automatico, è necessario eseguire alcune operazioni di convalida per garantire il successo. Lo strumento SWIM di CiscoWorks 2000 consente di eseguire script personalizzati in seguito all'aggiornamento per un'ulteriore verifica. La verifica include la verifica che il router disponga del numero appropriato di percorsi, la verifica che le interfacce logiche/fisiche siano attive e attive o la verifica che il dispositivo sia accessibile. L'elenco di controllo di esempio seguente può convalidare completamente la riuscita di un'implementazione di Cisco IOS:

- Il dispositivo è stato ricaricato correttamente?
- Il dispositivo è percorribile e raggiungibile tramite le piattaforme NMS (Network Management

System)?
- Le interfacce previste nel dispositivo sono attive e attive?
- Il dispositivo ha le adiacenze del protocollo di routing corrette?
- La tabella di routing è compilata?
- Il dispositivo trasmette il traffico in modo corretto?

Operazioni - Gestione dell'implementazione Cisco IOS ad alta disponibilità

Le operazioni basate su procedure ottimali per l'elevata disponibilità dell'ambiente Cisco IOS consentono di ridurre la complessità della rete, migliorare i tempi di risoluzione dei problemi e migliorare la disponibilità della rete. La sezione relativa alle operazioni della gestione di Cisco IOS include la strategia, gli strumenti e le metodologie di best practice consigliate per la gestione di Cisco IOS.

Le best practice per le operazioni di Cisco IOS includono il controllo della versione del software, la gestione dei syslog di Cisco IOS, la gestione dei problemi, la standardizzazione della configurazione e la gestione della disponibilità. Il controllo della versione del software è il processo di rilevamento, convalida e miglioramento della coerenza del software all'interno delle tracce software identificate. La gestione dei syslog di Cisco IOS è il processo di monitoraggio proattivo e l'azione su messaggi Syslog con priorità superiore generati da Cisco IOS. La gestione dei problemi consiste nella raccolta rapida ed efficiente di informazioni critiche sui problemi relativi al software, al fine di prevenire il ripetersi di tali problemi. La standardizzazione della configurazione è il processo di 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. La gestione della disponibilità è il processo di miglioramento della disponibilità basato su metriche, obiettivi di miglioramento e progetti di miglioramento.

Strategie e strumenti per le operazioni Cisco IOS

Esistono molte strategie e strumenti di qualità per aiutare a gestire gli ambienti Cisco IOS. La prima strategia chiave per le operazioni di Cisco IOS è 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. Il gruppo di implementazione e operazioni ha quindi la responsabilità di configurare e mantenere gli standard tramite il controllo della versione e gli standard/controllo della configurazione di Cisco IOS.

La seconda strategia per le operazioni di Cisco IOS è la capacità di identificare e risolvere rapidamente i problemi di rete. I problemi di rete devono in genere essere identificati dal gruppo operativo prima che gli utenti li chiamino. I problemi dovrebbero anche essere risolti il più rapidamente possibile senza ulteriori impatti o cambiamenti per l'ambiente. Alcune best-practice in quest'area sono relative alla gestione dei problemi e alla gestione dei syslog di Cisco IOS. Cisco Output Interpreter è uno strumento per la diagnosi rapida dei crash del software Cisco IOS.

La terza strategia è un miglioramento costante. 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 correlati a Cisco IOS, le aziende possono 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.

Gli strumenti per le operazioni Cisco IOS includono la gestione dell'inventario per il controllo della versione del software (CiscoWorks2000 RME), la gestione Syslog per gestire i messaggi Syslog e i manager di configurazione dei dispositivi per gestire la coerenza della configurazione dei dispositivi.

Gestione Syslog

I messaggi syslog sono messaggi inviati dal dispositivo a un server di raccolta. Questi messaggi possono essere errori (ad esempio, un collegamento che non funziona) o informazioni, come quando qualcuno ha configurato un terminale su un dispositivo.

Gli strumenti di gestione Syslog registrano e tengono traccia dei messaggi Syslog ricevuti da router e switch. Alcuni strumenti dispongono di filtri per consentire la rimozione dei messaggi indesiderati che possono ridurre quelli importanti. Gli strumenti Syslog devono inoltre consentire la creazione di report in base ai messaggi ricevuti. I report possono essere visualizzati per periodo di tempo, dispositivo, tipo di messaggio o priorità del messaggio.

Lo strumento Syslog più comune per la gestione di Cisco IOS è CiscoWorks2000 RME Syslog Manager. Sono disponibili altri strumenti, tra cui SL4NT, un programma shareware di Netal e Private IP di OpenSystems.

CiscoWorks Device Configuration Manager

CiscoWorks 2000 Device Configuration Manager gestisce un archivio attivo e fornisce un modo semplice per aggiornare le modifiche alla configurazione su più router e switch Cisco. Gestione configurazione esegue il monitoraggio della rete per rilevare eventuali modifiche alla configurazione, aggiorna l'archivio quando viene rilevata una modifica e registra le informazioni relative alla modifica nel servizio di controllo delle modifiche. Un'interfaccia utente basata sul Web consente di ricercare nell'archivio attributi di configurazione specifici e di confrontare il contenuto di due file di configurazione per identificare facilmente le differenze.

Cisco Output Interpreter

Cisco Output Interpreter è uno strumento utilizzato per diagnosticare gli arresti anomali forzati del software. Lo strumento può aiutare a identificare i difetti del software senza chiamare il Technical Assistance Center (TAC) di Cisco o può essere utilizzato come informazione primaria per TAC in seguito a un arresto anomalo del software. Queste informazioni aiuteranno in genere a risolvere il problema più rapidamente, almeno in termini di raccolta delle informazioni necessarie.

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, il personale 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, non è raro vedere versioni non standard nella rete, soprattutto se la rete e il personale operativo sono grandi. Ciò può essere dovuto a personale più recente non addestrato, comandi di avvio non configurati correttamente o implementazioni non controllate. È sempre consigliabile convalidare periodicamente gli standard di versione del software utilizzando strumenti quali CiscoWorks 2000 RME in grado di ordinare tutti i dispositivi in base alla versione di Cisco IOS. Quando vengono identificate delle non-norme, queste devono essere immediatamente contrassegnate e deve essere avviato un trouble ticket o change ticket per portare la versione allo standard identificato.

Gestione proattiva syslog

La raccolta, il monitoraggio e l'analisi dei syslog sono processi di gestione degli errori consigliati per risolvere un numero maggiore di problemi di rete specifici di Cisco IOS, difficili o impossibili da identificare con altri mezzi. La raccolta, il monitoraggio e l'analisi dei syslog consentono di migliorare i tempi di risoluzione dei problemi identificando e risolvendo numerosi errori in modo proattivo prima che si verifichino problemi di rete più gravi o che vengano segnalati dagli utenti. Syslog fornisce anche un metodo più efficiente per raccogliere un'ampia varietà di problemi rispetto al polling SNMP coerente per un elevato numero di variabili MIB. La raccolta, il monitoraggio e l'analisi Syslog vengono eseguiti utilizzando la configurazione Cisco IOS corretta, gli strumenti di correlazione Syslog, ad esempio CiscoWorks2000 RME, e/o la gestione degli eventi Syslog. La gestione degli eventi Syslog viene eseguita analizzando i dati Syslog raccolti per individuare i messaggi critici identificati e quindi inoltrando un avviso o una trap a un gestore eventi per la notifica e la risoluzione in tempo reale.

Il monitoraggio Syslog richiede il supporto dello strumento NMS o script per l'analisi e la creazione di report sui dati Syslog. Ciò include la possibilità 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.

Gestione dei problemi

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.

In ambienti di grandi dimensioni è consigliabile un processo di gestione dei problemi. Questo processo deve includere un certo grado di descrizioni predefinite dei problemi e raccolte di comandi **show** appropriate prima dell'escalation a un secondo livello. Il supporto di primo livello non deve mai essere l'eliminazione di route o il ricaricamento di dispositivi. In modo ottimale, l'organizzazione di primo livello deve raccogliere rapidamente le informazioni ed eseguire l'escalation a un secondo livello. Inizialmente dedicando qualche minuto all'identificazione o alla descrizione del problema, 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 avere una conoscenza approfondita dei tipi di informazioni di cui Cisco potrebbe aver bisogno per diagnosticare un problema o segnalare un bug. Sono inclusi i dump della memoria, l'output delle informazioni di routing e l'output del comando **show del** 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. I comandi di configurazione globale influiscono in genere sull'accesso ai dispositivi, sul loro comportamento generale e sulla sicurezza dei dispositivi. In Cisco IOS questo include comandi di servizio, comandi IP, comandi vty, comandi della porta della console, comandi di log, comandi AAA/TACACS+, comandi SNMP e comandi 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 (Domain Name System) 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 dispositivi simili anche a livello globale per garantire la coerenza della configurazione globale o per verificare periodicamente i dispositivi in base agli standard di configurazione globale corretti. Gli standard di configurazione dei protocolli e delle interfacce permettono di mantenere gli standard per la configurazione delle interfacce e dei protocolli.

La coerenza della configurazione di protocolli e interfacce migliora la disponibilità della rete riducendo la complessità della rete, fornendo il comportamento previsto di dispositivi e protocolli e migliorando la supportabilità della rete. L'incoerenza nella configurazione del protocollo o dell'interfaccia può causare comportamenti imprevisti dei dispositivi, problemi di routing del traffico, problemi di connettività maggiori e tempi di supporto reattivi più lunghi. Gli standard di configurazione interfaccia devono includere i descrittori dell'interfaccia CDP, la configurazione della cache e 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 della VLAN
- Protocollo VTP (Virtual Trunking Protocol)
- HSRP

Nota: è possibile avere altri standard di configurazione specifici del protocollo, a seconda di ciò che è configurato all'interno della rete.

Un esempio di standard IP può includere:

- Dimensioni subnet
- Spazio di indirizzi IP utilizzato
- Protocollo di routing utilizzato
- 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. Infatti, senza modelli di configurazione standardizzati, è quasi impossibile testare, convalidare o certificare adeguatamente una versione Cisco IOS per una rete di dimensioni moderatamente grandi.

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 o errori 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 hanno un processo di miglioramento della qualità.

Appendice A - Panoramica delle versioni Cisco IOS

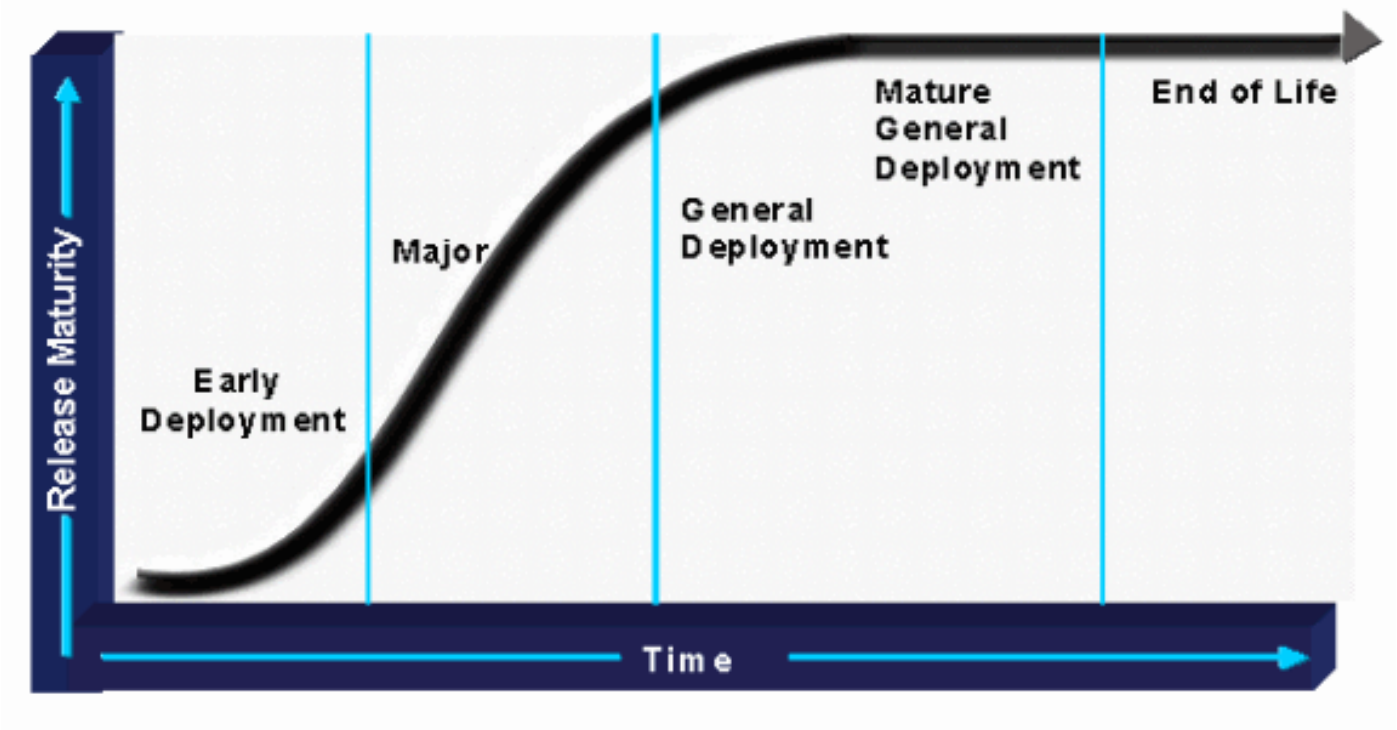
La strategia di rilascio del software Cisco IOS è basata sullo sviluppo di software audio, sul controllo della qualità e sulla riduzione dei tempi di commercializzazione, fattori fondamentali per il successo delle reti dei clienti Cisco.

Il processo si articola in quattro categorie di release, descritte di seguito:

- Early Deployment release (ED)
- Versione principale
- Versione di distribuzione limitata (LD)
- GD (General Deployment release)

Cisco crea e gestisce un piano IOS contenente informazioni su singole versioni, mercati di destinazione, percorsi di migrazione, descrizioni di nuove funzionalità e così via.

La figura seguente illustra il ciclo di vita della versione del software Cisco IOS:



Release ED

Le versioni ED di Cisco IOS sono veicoli che introducono nuovi sviluppi sul mercato. Ogni revisione di manutenzione di una release ED include non solo correzioni di bug, ma anche una serie di nuove funzionalità, supporto di nuove piattaforme e miglioramenti generali ai protocolli e all'infrastruttura Cisco IOS. Ogni due anni, le funzionalità e le piattaforme delle versioni ED vengono trasferite alla versione principale successiva di Cisco IOS.

Esistono quattro tipi di release ED, ognuna con un modello di release leggermente diverso e le fasi cardine del ciclo di vita. Le versioni ED possono essere classificate come:

- **Versioni Consolidated Technology Early Deployment (CTED)**: il nuovo modello di rilascio di Cisco IOS utilizza il treno di rilascio consolidato ED, noto anche come "T", per introdurre nuove funzionalità, nuove piattaforme hardware e altri miglioramenti a Cisco IOS. Sono denominate tecnologie consolidate perché trascendono le definizioni delle unità aziendali interne (BU) e delle LOB (Line Of Business). Esempi di versioni consolidate della tecnologia sono Cisco IOS 11.3T, 12.0T e 12.1T.
- **Versioni STED (Specific Technology Early Deployment)**: le versioni STED hanno caratteristiche di utilizzo delle funzionalità simili a quelle delle versioni CTED, con la differenza che sono destinate a una tecnologia specifica o a un mercato specifico. Vengono sempre rilasciati su piattaforme specifiche e sono sotto la sola supervisione di un Cisco BU. Le versioni STED sono identificate tramite due lettere aggiunte alla versione principale. Esempi

di versioni STED sono Cisco IOS 11.3NA, 11.3MA, 11.3WA e 12.0DA.

- **Versioni SMED (Market Early Deployment) specifiche**: le SMED di Cisco IOS si differenziano dalle STD per il fatto che sono destinate a un segmento di mercato verticale specifico (ISP, aziende, istituzioni finanziarie, società di telecomunicazioni e così via). Le PMI prevedono requisiti specifici in termini di funzionalità tecnologiche solo per piattaforme specifiche di rilievo utilizzate dal mercato verticale previsto. Si possono distinguere dai CTED per il fatto che sono costruiti solo per piattaforme specifiche rilevanti per il mercato verticale, mentre i CTED sarebbero costruiti per più piattaforme basate su un requisito tecnologico più ampio. Le versioni Cisco IOS SMED sono identificate da un carattere alfabetico aggiunto alla versione principale (proprio come la CTED). Esempi di SMED sono Cisco IOS 12.0S e 12.1E.
- **Versioni di implementazione rapida, note anche come X Releases (XED)**: le versioni Cisco IOS XED introducono nuovi componenti hardware e nuove tecnologie sul mercato. Non forniscono revisioni per la manutenzione del software né revisioni intermedie periodiche. Se viene rilevato un difetto nell'ambiente XED prima della sua convergenza con il CTED, viene avviata una ricostruzione del software e al nome viene aggiunto un numero. Ad esempio, Cisco IOS versione 12.0(2)XB1 e 12.0(2)XB2 sono esempi di ricostruzioni 12.0(2)XB.

Release principali

Le versioni principali sono i veicoli di implementazione principali per i prodotti software Cisco IOS. Sono gestiti dalla divisione Technology di Cisco IOS e consolidano funzionalità, piattaforme, funzionalità, tecnologie e la proliferazione di host rispetto alle precedenti versioni ED. Le versioni principali di Cisco IOS richiedono maggiore stabilità e qualità. Per questo motivo, le versioni principali non accettano l'aggiunta di funzionalità o piattaforme. Ogni revisione della manutenzione fornisce solo correzioni dei bug. Ad esempio, il software Cisco IOS versione 12.1 e 12.2 è una versione principale.

Le versioni principali includono aggiornamenti pianificati per la manutenzione, denominati versioni di manutenzione, che vengono testati per verificare la regressione, includono le correzioni più recenti dei bug e non supportano nuove piattaforme o funzionalità. Il numero di una release principale identifica la release principale e il relativo livello di manutenzione. Nel software Cisco IOS versione 12.0(7), la versione 12.0 è il numero della versione principale e il livello di manutenzione è 7. Il numero di versione completo è 12.0(7). Analogamente, la versione 12.1 è una versione principale e la versione 12.1(3) è la terza versione di manutenzione della versione principale del software Cisco IOS, la 12.1.

Versioni Limited Deployment (LD)

LD è la fase di maturità di Cisco IOS tra FCS e l'implementazione generale per le versioni principali. Le versioni ED di Cisco IOS sono disponibili solo nella fase di implementazione limitata in quanto non raggiungono mai la certificazione GD.

Versioni General Deployment (GD)

Ad un certo punto durante il ciclo di vita della release, Cisco dichiarerà una release principale pronta per la certificazione GD. Solo una versione principale può ottenere lo stato GD. Una volta che Cisco ha verificato che la versione è stata rispettata, l'attività cardine di certificazione GD si conclude nel modo seguente:

- Dimostrata dall'ampia esposizione del mercato in diverse reti.
- La qualifica viene valutata in base alle metriche, analizzate per verificare la stabilità e le tendenze dei bug.

- Valutazione attraverso sondaggi sulla soddisfazione dei clienti.
- Una riduzione della tendenza normalizzata del cliente ha rilevato difetti nella release rispetto alle precedenti quattro release di manutenzione.

Un team interfunzionale di certificazione GD di Customer Advocacy, composto da tecnici TAC, tecnici AES (Advanced Engineering Services), tecnici System Test Engineering e tecnici Cisco IOS, è costituito per valutare ogni difetto rilevante della release. Questo team fornisce l'approvazione finale per la certificazione GD. Una volta raggiunto lo stato GD per una release, anche tutte le successive revisioni della release vengono considerate GD. Di conseguenza, una volta che una release è stata dichiarata GD; entra automaticamente nella fase di manutenzione limitata. Mentre in questa fase, la modifica tecnica del codice, incluse le correzioni con una rielaborazione importante del codice, è strettamente limitata e controllata da un responsabile di programma. In questo modo si evita che vengano introdotti bug avversi nelle versioni software Cisco IOS certificate GD. Il GD viene ottenuto mediante una particolare versione di manutenzione. Gli aggiornamenti di manutenzione successivi per tale release sono anch'essi release GD. Ad esempio, il software Cisco IOS versione 12.0 ha ottenuto la certificazione GD alla versione 12.0(8). Pertanto, i software Cisco IOS versione 12.0(9), 12.0(10) e così via sono versioni GD.

Immagini sperimentali o diagnostiche

Le immagini sperimentali o diagnostiche vengono talvolta definite speciali tecniche e vengono create solo quando sono stati identificati problemi software critici. Queste immagini non fanno parte del normale processo di rilascio. Le immagini in questa categoria sono build specifiche del cliente progettate per aiutare a diagnosticare un problema, testare la correzione di un bug o fornire una correzione immediata. È possibile fornire una correzione immediata quando non è possibile attendere la successiva versione provvisoria o di manutenzione. Le immagini sperimentali o diagnostiche possono essere create su qualsiasi base software supportata, incluse le versioni di manutenzione o provvisorie di qualsiasi tipo di release. Non esistono convenzioni ufficiali di denominazione, ma in molti casi lo sviluppatore aggiungerà al nome dell'immagine di base le iniziali, exp (per sperimentali) o cifre aggiuntive. Queste immagini sono supportate solo temporaneamente, in combinazione con lo sviluppo di Cisco, in quanto le operazioni di rilascio di Cisco TAC e Cisco IOS non mantengono la documentazione di supporto, ad esempio le tabelle dei simboli o la cronologia delle immagini di base. Queste immagini non vengono sottoposte a test interni di Cisco.

Cicli di vita

A un certo punto, le versioni GD sono sostituite da nuove versioni con le più recenti tecnologie di rete. È stato pertanto stabilito un processo di smobilizzo con le seguenti tre fasi principali:

- **Fine vendita (EOS)**: per le release principali, la data EOS è tre anni dopo la data della prima spedizione commerciale (FCS). In questo modo viene impostata una data finale entro la quale è possibile acquistare la release per i nuovi sistemi. La versione EOS continua ad essere disponibile per il download da Cisco Connection Online (CCO) per gli aggiornamenti della manutenzione.
- **End of Engineering (EOE)**: la release EOE è l'ultima release di manutenzione per la release GD e in genere segue circa tre mesi dopo la release EOS. I clienti possono continuare a ricevere supporto tecnico da Cisco TAC, nonché scaricare la versione EOE da CCO. Il bollettino sui prodotti che annuncia le versioni e le date EOS ed EOE è pubblicato un anno prima della data EOS pianificata. A questo punto, i clienti devono iniziare a valutare l'opportunità di aggiornare il software Cisco IOS per sfruttare le più recenti tecnologie di rete.
- **Fine del ciclo di vita (EOL)**: al termine del ciclo di vita della versione, tutto il supporto per la

versione del software Cisco IOS è terminato e non è più disponibile per il download alla data di fine ciclo di vita. In generale, la data di fine ciclo di vita è cinque anni dopo la data di fine ciclo di vita. Un bollettino di fine ciclo di vita del prodotto viene pubblicato circa un anno prima della data effettiva di fine ciclo di vita.

Convenzione di denominazione della versione di Cisco IOS

La convenzione di denominazione delle immagini Cisco IOS fornisce un profilo completo di tutte le immagini rilasciate. Il nome include sempre l'identificativo della release principale e l'identificativo della release di manutenzione. Il nome può includere anche un identificatore di treno, un identificatore di ricostruzione (per la release di manutenzione), gli identificatori di funzionalità specifiche delle unità operative (BU) e gli identificatori di ricostruzione degli identificatori di funzionalità specifici delle unità operative. Il formato può essere suddiviso come segue:

Sezione convenzione di denominazione	Spiegazione
x.y	Combinazione di due identificatori di cifre separati (uno o due) separati da un '.' che identifica il valore di rilascio principale. Questo valore viene determinato dal reparto marketing di Cisco IOS. Esempio: 12.1
z	Da una a tre cifre che identifica la release di manutenzione di x.y. Questo avviene ogni otto settimane. I valori sono 0 in versione beta, 1 in FCS e 2 per la prima release di manutenzione. Esempio: 12.1(2)
p	Un carattere alfa che identifica una ricostruzione di x.y(z). Il valore inizia con una "a" minuscola per la prima ricostruzione, quindi con una "b" e così via. Esempio: 12.1(2 bis)

A	Una o tre lettere alfa sono il designatore del treno di rilascio e sono obbligatorie per le versioni CTED, STED e X. Identifica inoltre una famiglia di prodotti o piattaforme. Le versioni con tecnologia ED utilizzano due lettere. La prima lettera rappresenta la tecnologia e la seconda viene utilizzata per la differenziazione. Ad esempio:
	`A = Access Server/Dial technology (example:11.3AA)`
	`B = Broadband (example:12.2B)`
	`D = xDSL technology (example:12.2DA)`
	`E = Enterprise feature set (example:12.1E)`

	H = SDH/SONET technology (example:11.3HA) N = Voice, Multimedia, Conference (example:11.3NA) M = Mobile (example:12.2MB) S = Service Provider (example:12.0S) T = Consolidated Technology (example:12.0T) W = ATM/LAN Switching/Layer 3 (example:12.0W5) Una "X" nella prima posizione del nome della release identifica una release unica basata sul treno "T" CTED. Ad esempio, XA, XB, XC e così via. Una "X" o "Y" nella seconda posizione del nome della release identifica una release ED di breve durata basata su, o affiliata a, una release STED. Ad esempio, 11.3NX (basato su 11.3NA), 11.3WX (basato su 11.3WA) e così via.
o	Indicatore numerico facoltativo a una o due cifre che identifica una ricostruzione di un particolare valore di rilascio. Lasciare vuoto se non rappresenta una ricostruzione. Inizia con 1, quindi con 2 e così via. Esempio: 12.1(2)T1, 12.1(2)XE2
u	Indicatore numerico a una o due cifre che identifica la funzionalità della release specifica dell'unità di business. Il valore viene determinato dal team di marketing dell'unità di vendita. Esempio: 11.3(6)WA4, 12.0(1)W5
v	Identificatore numerico da una a due cifre che identifica la release di manutenzione del codice specifico dell'unità di backup. I valori sono 0 in versione beta, 1 in FCS e 2 come prima release di manutenzione. Esempio: 11.3(6)WA4(9), 12.0(1)W5(6)
p	Un identificatore di carattere alfa che identifica una ricostruzione di una specifica release della tecnologia. Il valore inizia con una "a" minuscola per la prima ricostruzione, quindi con una "b" e così via. Esempio: 11.3(6)WA4(9a) sarebbe una ricostruzione di 11.3(6)WA4(9).

Il grafico seguente etichetta le diverse sezioni della convenzione di denominazione di Cisco IOS:

Appendice B - Affidabilità Cisco IOS

L'affidabilità di Cisco IOS è un'area in cui Cisco si impegna costantemente a migliorare. Prima di discutere le best practice orientate al cliente, è necessaria una certa comprensione della qualità e dell'affidabilità dei prodotti Cisco IOS interni. Queste sezioni hanno lo scopo principale di fornire una panoramica dei più recenti sforzi di Cisco nella qualità del software Cisco IOS e di indicare le ipotesi dei clienti riguardo all'affidabilità del software.

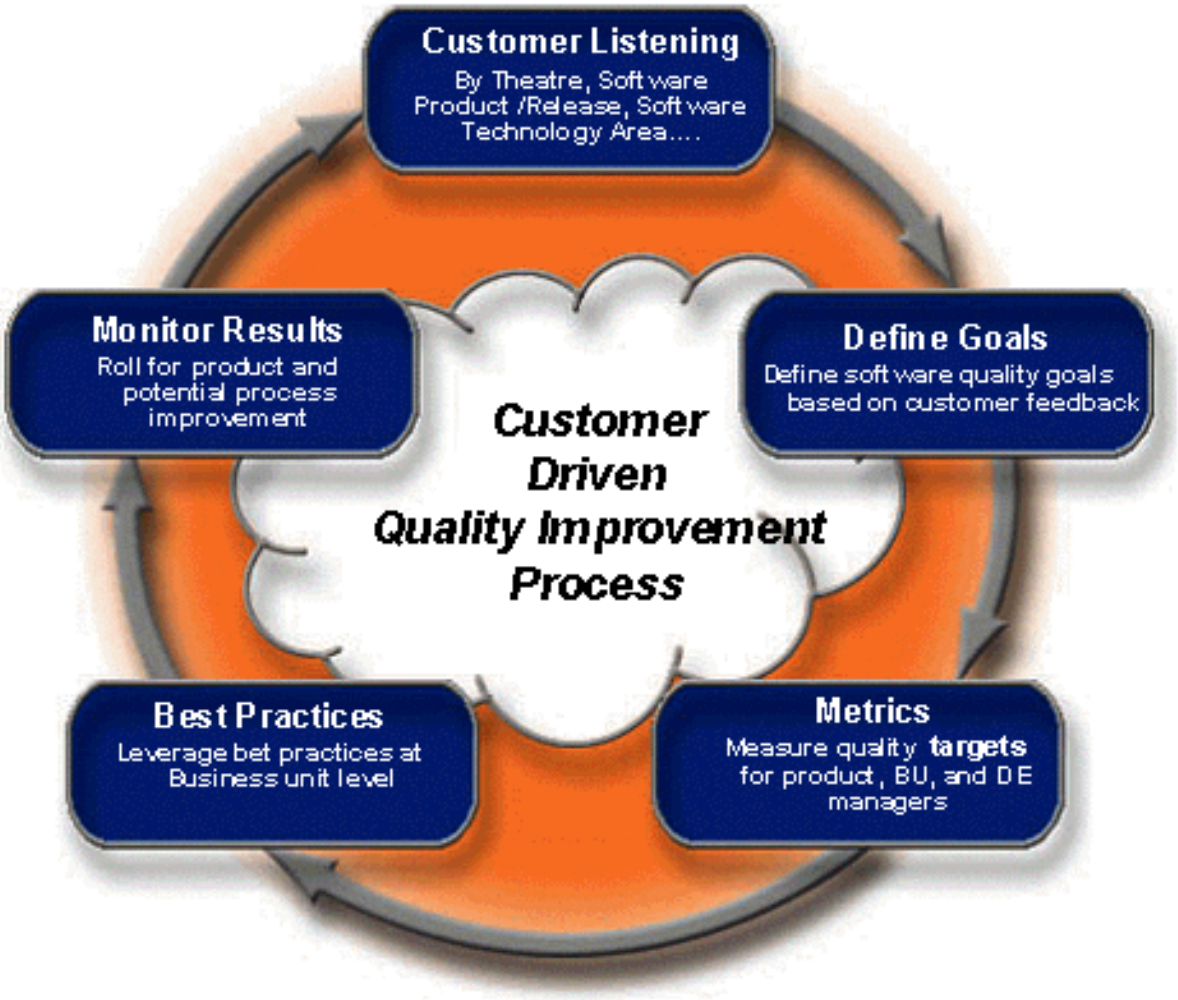
Programma di qualità Cisco IOS

Cisco ha un processo di sviluppo IOS ben definito chiamato GEM Great Engineering Methodology (GEM). Questo processo ha un ciclo di vita in tre fasi:

- Strategia e pianificazione
- Esecuzione
- Implementazione

Le aree generali all'interno del ciclo di vita includono l'introduzione delle funzionalità, la definizione delle priorità, lo sviluppo, il processo di test, le fasi di introduzione del software, la spedizione del primo cliente (FCS, First Customer Shipped), GD e la progettazione di supporto. Cisco segue anche una serie di linee guida sulle best-practice in materia di qualità del software fornite da organizzazioni quali International Standards Organization (ISO), Telcordia (in precedenza Bellcore), IEEE e Carnegie Mellon Software Engineering Institute. Queste linee guida sono incorporate nei processi GEM di Cisco. I processi di sviluppo software Cisco sono certificati ISO 9001 (1994).

Il processo principale per il miglioramento della qualità del software Cisco IOS è un processo gestito dal cliente tramite il quale Cisco ascolta i clienti, definisce gli obiettivi e i parametri, implementa le best practice e controlla i risultati. Questo processo è guidato da un team di più organizzazioni impegnato a migliorare la qualità del software. Di seguito è riportato un diagramma del processo di miglioramento della qualità di Cisco IOS:



Il processo di miglioramento della qualità ha obiettivi misurabili distinti per l'esercizio 2002 e oltre. L'obiettivo principale di questi obiettivi è quello di ridurre i difetti identificando i problemi software in una fase precedente del ciclo di test, ridurre il backlog dei difetti, migliorare la coerenza delle funzioni e la chiarezza delle versioni del software, nonché fornire pianificazioni prevedibili e una qualità del software. Le iniziative per affrontare queste aree includono nuovi strumenti di copertura dei test (che identificano le aree di copertura dei test più debole), miglioramenti del processo di azioni correttive dei test e miglioramenti dei test di regressione del sistema Cisco IOS. Per risolvere questi problemi sono state impiegate ulteriori risorse e per tutte le principali versioni del software Cisco IOS è in corso un impegno esecutivo e interfunzionale.

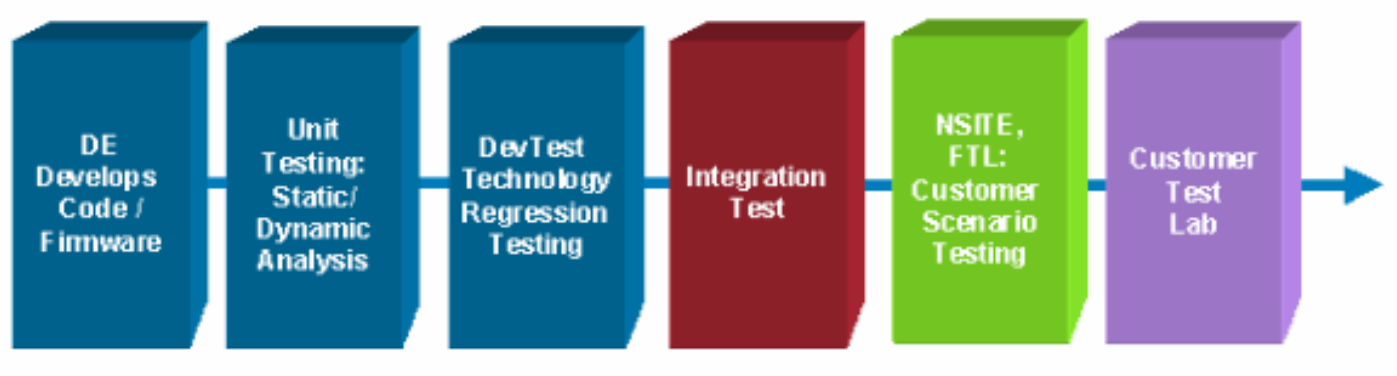
Test di rilascio di Cisco IOS

Una parte integrante dell'impegno di Cisco per la qualità dell'affidabilità del software riguarda la qualità, l'ambito e la copertura dei test. In generale, Cisco ha i seguenti obiettivi di qualità IOS:

- Ridurre i difetti di regressione interni rilevati di Cisco. Ciò include una migliore qualità nello sviluppo e l'identificazione di un maggior numero di problemi nell'analisi statica/dinamica.
- Riduzione dei difetti riscontrati dai clienti
- Ridurre il totale dei difetti in sospeso
- Aumentare la chiarezza delle versioni software e la coerenza delle funzionalità
- Fornire release di caratteristiche e manutenzione con programmazioni e qualità

I test interni Cisco possono essere considerati un processo in cui vengono identificati diversi difetti in fasi diverse dei test. L'obiettivo generale è quello di trovare il giusto tipo di difetti nel laboratorio giusto. Questo è importante per diverse ragioni. Il primo e più importante è che una copertura

adeguata dei test potrebbe non esistere nelle fasi di test successive. I costi dei test aumentano notevolmente da uno stadio all'altro a causa della capacità di automatizzare le fasi precedenti e della crescente complessità e competenza richieste successivamente. Il diagramma seguente mostra lo spettro dei test per Cisco IOS.



La prima fase è lo sviluppo del software. Cisco ha compiuto diversi sforzi in quest'area per contribuire a migliorare la qualità iniziale del software. I gruppi di sviluppo eseguono inoltre revisioni del codice o anche più revisioni del codice per garantire che altri sviluppatori approvino le modifiche al software o il nuovo codice delle funzionalità.

La fase successiva è l'unit test. Gli unit test utilizzano strumenti che esaminano l'interazione software senza l'utilizzo di un laboratorio. DevTest sono test di laboratorio che includono test di funzionalità/funzionalità e test di regressione. Il test delle funzionalità è stato progettato per esaminare la funzionalità di una determinata feature. Sono incluse la configurazione, la deconfigurazione e il test di tutte le permutazioni di feature definite nella specifica di feature. Il test di regressione viene eseguito in un impianto di test automatizzato progettato per convalidare la funzionalità e il comportamento delle funzionalità su base continuativa. Il test è incentrato principalmente sulle funzionalità di routing, switching e gestione in diverse topologie di rete che utilizzano ping e limitano la generazione del traffico. Il test di regressione viene eseguito solo su una combinazione limitata di funzionalità, piattaforme, versioni software e topologie, a causa del numero eccessivo di permutazioni possibili; tuttavia, attualmente vengono utilizzati oltre 4000 script di test di regressione. I test di integrazione sono progettati per ampliare le funzionalità dei test di laboratorio per una suite più completa di prodotti e interoperabilità. I test di integrazione aumentano inoltre il code coverage del test, espandendo i test di interoperabilità, stress e prestazioni, test di sistema e test negativi (test di eventi imprevisti).

La fase successiva prevede test completi per gli ambienti comuni dei clienti. Questi sono illustrati nel diagramma precedente come Financial Test Lab (FTL) e NSITE, Customer Scenario Testing. La FTL è stata creata per fornire test per la comunità finanziaria mission critical. NSITE è un gruppo che fornisce test più approfonditi per diverse tecnologie Cisco IOS. I laboratori NSITE e FTL si concentrano su aree quali la scalabilità e i test delle prestazioni, l'upgrade, la disponibilità e la resilienza, l'interoperabilità e la manutenzione. I servizi sono incentrati sui problemi di provisioning in blocco, sulla gestione/correlazione degli eventi e sulla risoluzione dei problemi sotto carico. Altri laboratori sono presenti in Cisco per diversi mercati verticali e servono a testare queste aree.

Il laboratorio finale indicato nel diagramma riportato sopra è il laboratorio del cliente. I test eseguiti dai clienti rappresentano un'estensione della qualità e sono consigliati per gli ambienti ad alta disponibilità, al fine di garantire che la combinazione esatta di funzionalità, configurazione, piattaforme, moduli e topologia sia stata completamente testata. I test devono includere la scalabilità e le prestazioni della rete nella topologia identificata, test di applicazioni specifiche, test negativi nella configurazione identificata, test di interoperabilità per dispositivi non Cisco e test di

burn-in.

Software MTBF

Una delle metriche più comuni dell'affidabilità complessiva è il tempo medio tra due guasti (MTBF). L'MTBF per l'affidabilità del software è utile perché le funzionalità di analisi sono state sviluppate per l'affidabilità dell'hardware utilizzando l'MTBF. L'affidabilità dell'hardware può essere determinata in modo più accurato utilizzando alcuni standard esistenti. Cisco utilizza il metodo di conteggio delle parti basato sui dati MTBF standard di Telcordia Technologies. Il software MTBF, tuttavia, non dispone di metodologie di analisi corrispondenti e deve basarsi sulla misurazione sul campo per l'analisi MTBF.

Negli ultimi tre anni Cisco ha eseguito misurazioni sul campo dell'affidabilità software per la rete IT interna Cisco e questo lavoro è documentato all'interno di Cisco. Il lavoro si basa su arresti anomali forzati del software per i dispositivi Cisco IOS, misurabili usando le informazioni sulle trap SNMP di gestione della rete e le informazioni sui tempi di attività. Lo studio identifica l'affidabilità del software utilizzando un modello statistico di distribuzione lognormale per le versioni del software identificate. Il tempo medio di riparazione (MTTR) di un errore software si basa sui tempi medi di riavvio e ripristino del router. Negli ambienti aziendali vengono utilizzati sei minuti di ripristino e quindici minuti per i provider di servizi Internet (ISP) di maggiori dimensioni. Il risultato di questo studio in corso è che il software generalmente raggiunge una disponibilità minima al momento del rilascio, o dopo alcune versioni di manutenzione, ed è ancora più elevato nel tempo, come misurato utilizzando software forzato crash come unica fonte di downtime. Lo studio ha identificato i potenziali valori MTBF come un intervallo compreso tra 5.000 ore per il software di installazione iniziale e 50.000 ore per il software di installazione generale.

Il problema più comune è che gli arresti anomali forzati del software non includono tutti i tempi di interruzione dovuti a problemi di affidabilità del software. Se questa metrica viene utilizzata per migliorare la qualità, può contribuire a migliorare la percentuale di arresti anomali forzati del software, ma può ignorare altre aree critiche dell'affidabilità del software. Questo commento rimane in gran parte senza risposta a causa della difficoltà di prevedere con precisione l'affidabilità del software utilizzando una metodologia statistica. Gli statistici sulla qualità del software Cisco hanno concluso che sarebbe necessario un insieme più ampio di dati accurati per prevedere in modo affidabile l'MTBF del software utilizzando una più ampia gamma di tipi di interruzione delle attività. Inoltre, l'analisi statistica teorica sarebbe difficile a causa di variabili quali la complessità della rete, l'esperienza del personale nella risoluzione dei problemi relativi al software, la progettazione della rete, le funzionalità abilitate e i processi di gestione del software.

Al momento, non è stato completato alcun lavoro di settore per prevedere con maggiore precisione l'affidabilità del software con le misurazioni sul campo a causa della difficoltà di raccogliere con precisione questo tipo di dati sensibili. Inoltre, la maggior parte dei clienti non desidera che Cisco raccolga le informazioni sulla disponibilità direttamente dalla rete a causa della natura proprietaria dei dati sulla disponibilità. Alcune organizzazioni raccolgono tuttavia dati sull'affidabilità del software e Cisco incoraggia le organizzazioni a raccogliere metriche sulla disponibilità dovute a interruzioni del software e a eseguire la root cause analysis su tali interruzioni. Le organizzazioni con una maggiore affidabilità del software hanno utilizzato questo approccio proattivo per migliorare l'affidabilità del software attraverso una serie di procedure che possono controllare.

Presupposti per l'affidabilità del software

In seguito ai commenti dei clienti, agli studi proattivi eseguiti dal gruppo Cisco IOS Technologies e

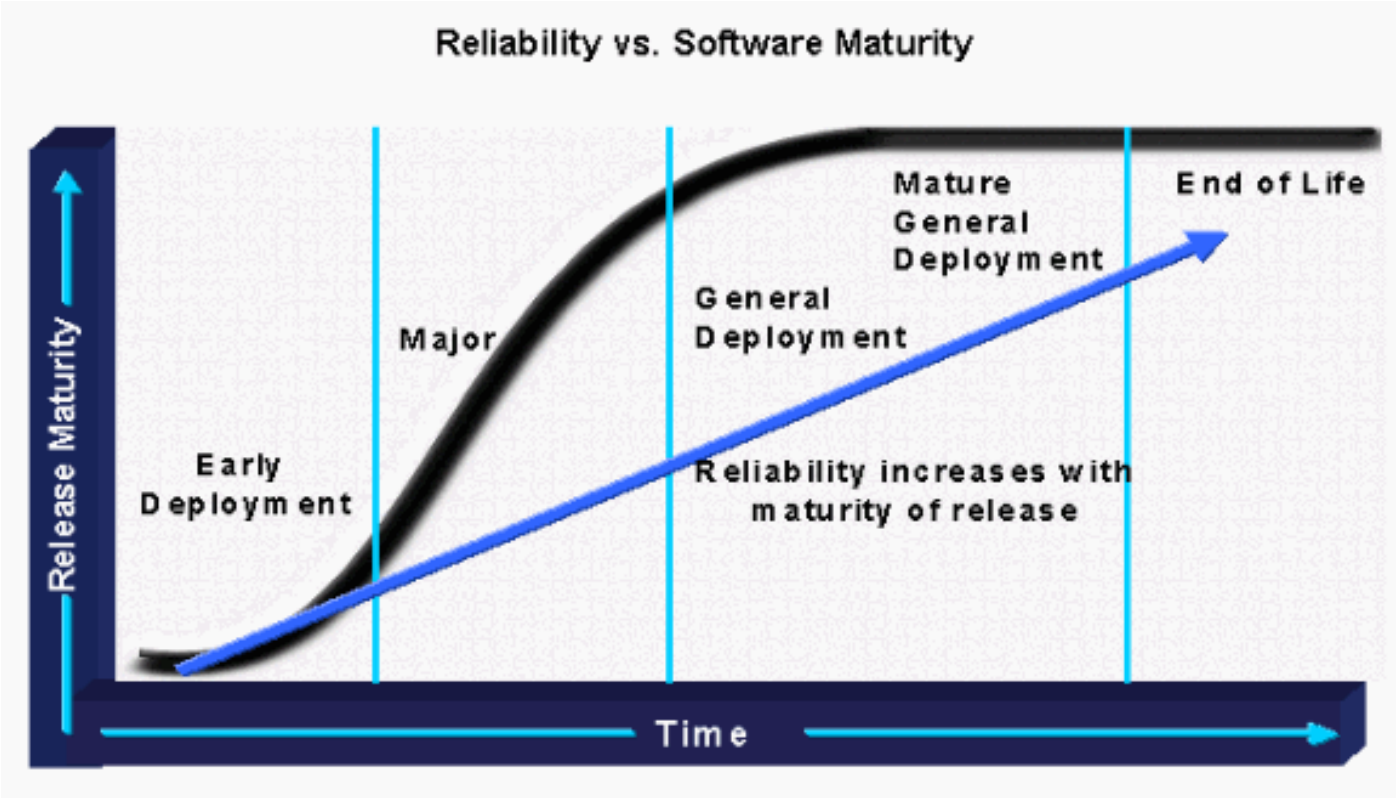
all'analisi della root cause eseguita dal team Cisco Advanced Services, è stato possibile formulare alcune nuove ipotesi e best practice per migliorare l'affidabilità del software. Tali presupposti sono basati su responsabilità di test, maturità o età del software, funzionalità abilitate e numero di versioni software distribuite.

Responsabilità test

Il primo nuovo presupposto riguarda la verifica della responsabilità. Cisco è sempre responsabile del test e della convalida di nuove funzionalità e funzionalità per garantire che funzionino con i nuovi prodotti. Cisco è inoltre responsabile dei test di regressione per verificare che le nuove versioni software siano compatibili con le versioni precedenti. Tuttavia, Cisco non è in grado di convalidare tutte le funzionalità, le topologie e le piattaforme in base a tutte le potenziali avvertenze che un ambiente del cliente può suscitare (specifiche di progettazione, profili di carico e traffico). Le procedure ottimali per l'elevata disponibilità includono test in una topologia di laboratorio compressa che simula la rete di produzione utilizzando funzionalità, progettazione, servizi e traffico delle applicazioni definiti dal cliente.

Affidabilità e maturità del software

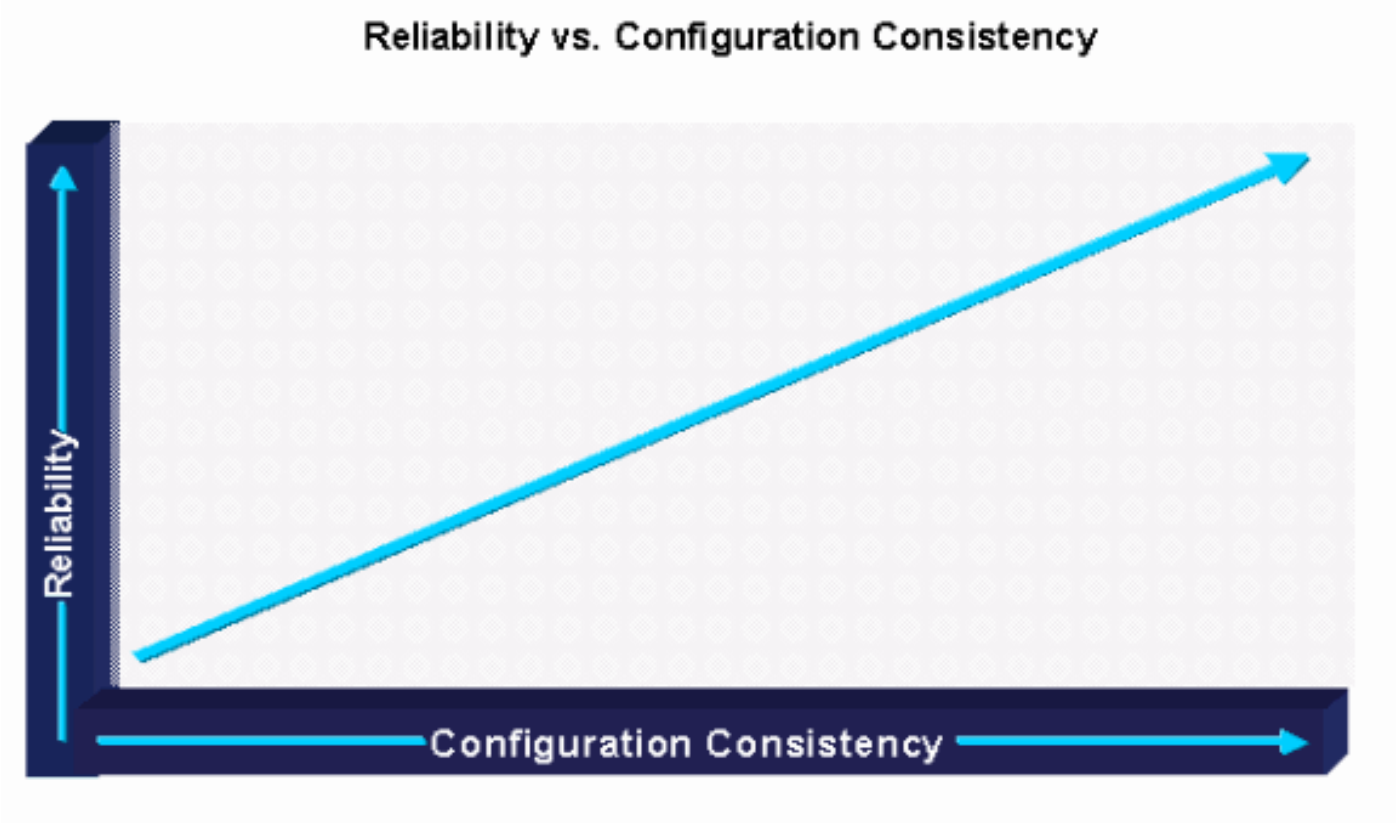
L'affidabilità del software è principalmente un fattore di maturità del software. Il software matura man mano che viene esposto (utilizzato) e i bug identificati vengono corretti. Le operazioni di rilascio di Cisco si sono basate su un'architettura di rilascio del treno per garantire che il software matura senza l'aggiunta di nuove funzionalità. I clienti che richiedono un'elevata disponibilità sono alla ricerca di software più maturi con le funzionalità di cui hanno bisogno ora. Esiste quindi un compromesso tra la maturità del software, i requisiti di disponibilità e i driver aziendali per nuove funzionalità o caratteristiche. Molte organizzazioni dispongono di standard o linee guida per una maturità accettabile. Alcuni accetteranno solo il quinto rilascio provvisorio di un particolare treno. Per altri, potrebbe essere la nona o la certificazione GD. In ultima analisi, l'organizzazione deve decidere i livelli accettabili di rischio in termini di maturità del software.



Affidabilità e quantità di caratteristiche e standard

L'affidabilità del software è anche un fattore che determina la quantità di codice testato ed eseguito in un ambiente di produzione. Con l'aumento della quantità di piattaforme hardware e moduli diversi, aumenta anche la quantità di codice utilizzato, il che in genere aumenta l'esposizione ai difetti del software. Lo stesso si può dire per la quantità di protocolli configurati, la varietà di configurazioni e persino la varietà di topologie o progetti implementati. Fattori di progettazione, configurazione, protocolli e moduli hardware possono contribuire alla quantità di codice da utilizzare e all'aumento del rischio o dell'esposizione a difetti software.

Le operazioni di rilascio del software ora hanno un software speciale che in genere limita il codice disponibile in una particolare area. Le Business Unit hanno consigliato progettazioni e configurazioni che sono state testate in modo più approfondito in Cisco e che sono maggiormente utilizzate dai clienti. I clienti hanno inoltre iniziato ad adottare best practice per topologie modulari e configurazioni standard standardizzate per ridurre la quantità di esposizione del codice non testato e migliorare l'affidabilità complessiva del software. Alcune reti ad alta disponibilità dispongono di linee guida di configurazione standard rigorose, standard di topologia modulare e controllo della versione del software per ridurre il rischio di esposizione del codice non testato.

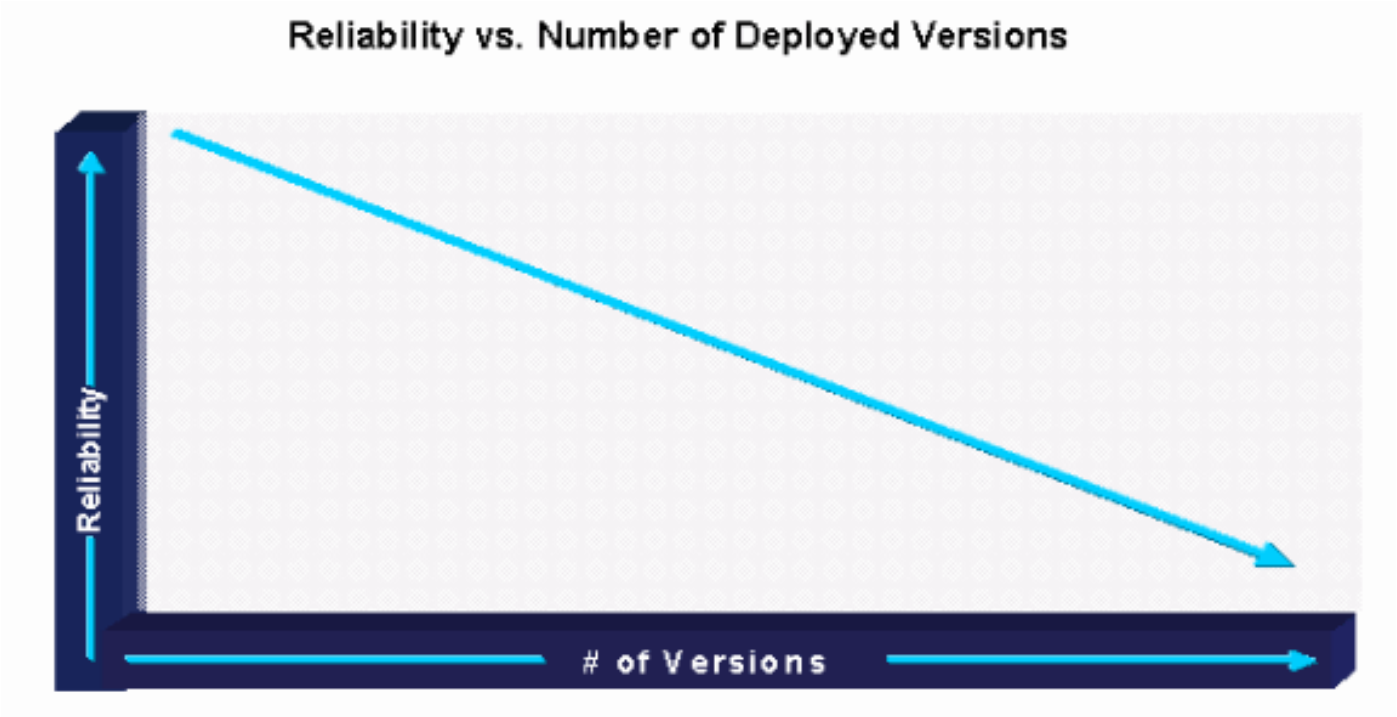


Affidabilità rispetto al numero di versioni distribuite

Un altro fattore di affidabilità del software è l'interoperabilità tra le versioni e la quantità di codice che viene utilizzato con più versioni. Con l'aumento della quantità di versioni software, aumenta anche la quantità di codice utilizzato, che aumenta l'esposizione ai difetti del software. Il rischio per l'affidabilità aumenta in modo quasi esponenziale a causa dell'esercizio di codice aggiuntivo con più versioni. È ormai riconosciuto che le organizzazioni devono eseguire almeno una manciata di versioni nella rete per soddisfare specifici requisiti di funzionalità e piattaforma. L'esecuzione di oltre cinquanta versioni in un ambiente di rete prevalentemente omogeneo, tuttavia, è normalmente indicativa di problemi software dovuti all'impossibilità di analizzare o convalidare correttamente queste numerose versioni.

Per migliorare l'affidabilità del software, Cisco Development esegue test di regressione del software per verificare che versioni software diverse siano compatibili. Inoltre, il codice software è

più modulare e i moduli core hanno meno probabilità di cambiare in modo significativo tra le versioni nel tempo. Le operazioni di rilascio di Cisco hanno inoltre modificato la quantità di software disponibile per i clienti in quanto le versioni con difetti noti o i problemi di interoperabilità vengono rapidamente rimossi da CCO in caso di rilevamento di difetti.



Informazioni correlate

- Sistemi operativi Cisco Internetworking (IOS)
- Documentazione e supporto tecnico – Cisco Systems