Guida dell'assistente alla configurazione di IBM®Technical Support Appliance

Versione 2.7.0.0

Agosto 2020

Indice

Introduzione

IBM TSA (Technical Support Appliance) è uno strumento di facile utilizzo, che consente di ricavare maggior valore dai contratti stipulati con il Supporto IBM. TSA rileva elementi IT (information technology) chiave e le relative relazioni all'interno dell'infrastruttura IT, trasmette, quindi, in sicurezza i dati al Supporto IBM per l'analisi. Questi dati forniscono al Supporto IBM conoscenza approfondita delle complesse relazioni tra i server e i componenti di rete nel data center.

L'intento di questo documento è quello di fornire informazioni e indicazioni di ausilio nell'installazione, pianificazione e configurazione di TSA.

Considerazioni sulla rete prerilevamento

Prima di configurare TSA per il rilevamento iniziale e la trasmissione, accertarsi di avere preso in considerazione i seguenti elementi. Si presuppone che TSA sia già stato installato, che sia possibile accedere all'interfaccia Web, che TSA sia stato aggiornato al livello più recente, se così non fosse, consultare la Guida alla configurazione di Technical Support Appliance (a cui si farà riferimento come guida alla configurazione nella parte restante di questo documento).

Considerazioni sulla rete prerilevamento di TSA	
Rete	
	Aprire l'accesso firewall da TSA a IBM. Consultare la sezione, **Requisiti di configurazione per le connessioni al Supporto IBM** nella guida alla configurazione.
	Se si utilizza un proxy SSL per la connessione di ritorno a IBM, assicurarsi che sia configurato in TSA. Consultare la sezione **Configurazione della connettività IBM** nella guida alla configurazione. - L'ispezione SSL non è supportata. Se la si sta utilizzando sul proxy, disabilitare tale funzione per questi flussi.
	Se esistono firewall tra TSA e i dispositivi di destinazione, assicurarsi che le porte richieste siano aperte. Per ulteriori informazioni, consultare la sezione "Considerazioni sul firewall" a pagina 40.

Documentazione utile

Il link sottostante reindirizzerà direttamente al sito Web di informazioni su Technical Support Appliance. In questo sito sarà possibile reperire tutte le informazioni necessarie per iniziare a utilizzare IBM Technical Support Appliance. È possibile accedere alle guide alla configurazione e alla documentazione sulla sicurezza, visualizzare report di esempio e scaricare il codice di installazione di Technical Support Appliance da ibm.com.

Per ulteriori informazioni su Technical Support Appliance andare all'indirizzo: https://ibm.biz/TSAdemo

Panoramica

TSA può rilevare informazioni sull'infrastruttura IT, che includono componenti del sistema operativo, componenti firmware, server fisici, dispositivi di rete, VLAN (virtual LAN - LAN virtuale), ecc. Per ottimizzare l'ampiezza e la profondità delle informazioni che vengono raccolte, sono necessarie attività di configurazione in TSA, per l'identificazione e il rilevamento di dispositivi.

TSA tenta di minimizzare gli impatti sull'ambiente di rete del cliente. Quindi, il processo di rilevamento adotta un approccio iterativo e misurato, per cui un rilevamento completo può richiedere fino a 72 ore. Lo stato del lavoro di rilevamento potrà essere monitorato visualizzando la sezione **Riepilogo lavoro** del pannello **Riepilogo**.

Come parte del processo di rilevamento, TSA inizialmente tenta di rilevare dispositivi nell'ambito definito, senza utilizzare credenziali. Questo implica l'utilizzo di Nmap per il rilevamento e la classificazione dei dispositivi mediante scansione IP poco invasiva, creazione di impronta digitale dello stack e associazione porta. In genere, questa attività non dovrebbe essere tanto importante da attivare un IDS (intrusion detection system), ma tale attivazione potrebbe essere richiesta in caso di rigide impostazioni locali.

Perché TSA raccolga informazioni sull'infrastruttura IT, specificare quanto segue:

- Ambiti
- Credenziali di accesso

Definizione delle serie di ambiti

Una serie di ambiti è un raggruppamento logico di singoli ambiti. Gli ambiti si avvalgono degli indirizzi IP per indicare a TSA da dove iniziare il rilevamento dell'ambiente. Una serie di ambiti è composta da uno o più ambiti. Esistono tre tipi di voci ambito:

- Subnet - Definita da un indirizzo IP e da una subnet mask. Le subnet sono limitate alle subnet di classe C.
- Intervallo IP - Include tutti gli indirizzi IP compresi tra il valore iniziale e quello finale.
- Indirizzo IP / Host - Un singolo Indirizzo IP o Nome host.

> Il nome host viene risolto al momento dell'inserimento, non in fase di rilevamento. Consultare la sezione "Fattori da considerare nella creazione degli ambiti," a pagina 6 per esaminare dettagli.

Se si desidera, è possibile definire esclusioni di ambito per un ambito, specificando una definizione di host, intervallo o subnet. Gli indirizzi IP risultanti non verranno considerati parte dell'ambito né sottoposti a scansione.

TSA supporta tre tipi di serie di ambiti:

1. **Serie di ambiti generali**: consente di rilevare singoli elementi di rete IT. La serie di ambiti contiene uno o più ambiti, che identificano l'ubicazione di questi elementi di rete utilizzando un indirizzo IP, un intervallo di indirizzi IP, una rete o una subnet.
2. **Serie di ambiti dinamici HMC**: consente di specificare l'indirizzo IP di uno o più HMC IBM POWER Systems insieme alle credenziali associate. Inoltre, le informazioni relative a tutte le LPAR gestite dalle HMC possono essere raccolte anche senza l'esigenza di identificare gli indirizzi IP delle LPAR. La serie di ambiti dinamici utilizza le informazioni sulle credenziali fornite dall'utente per accedere correttamente a queste LPAR.
3. **Serie di ambiti dinamici VMware**: consente di specificare l'indirizzo IP di una o più istanze VMware vCenter Server o ESXi insieme alle credenziali associate. Inoltre, le informazioni relative a tutte le macchine virtuali gestite da VMware possono essere raccolte anche senza l'esigenza di identificare gli indirizzi IP delle macchine virtuali. La serie di ambiti dinamici utilizza le informazioni sulle credenziali fornite dall'utente per accedere correttamente a queste macchine virtuali.

Per HMC e VMware vCenter Server / ESXi, si consiglia l'utilizzo di serie di ambiti dinamici. Le serie di ambiti dinamici richiedono un impegno di gran lunga inferiore per la configurazione in TSA rispetto alla creazione e gestione di ambiti di rilevamento per singole LPAR/macchine virtuali. Inoltre, per ambienti in cui vengono aggiunte ed eliminate nel tempo LPAR o macchine virtuali, le serie di ambiti dinamici possono gestire queste operazioni senza necessità di modificare alcuna serie di ambiti.

Per istruzioni dettagliate riguardo alla modalità di definizione degli ambiti di rilevamento in TSA, consultare la sezione **Configurazione degli ambiti di rilevamento** nella guida alla configurazione.

Fattori da considerare nella creazione degli ambiti

Anche se non esistono standard definiti per la configurazione degli ambiti, si possono effettuare alcune considerazioni pratiche per poter risparmiare tempo e fatica:

- Ove sia opportuno, utilizzare serie di ambiti dinamici per definire i rilevamenti delle HMC e delle relative LPAR gestite oppure VMware vCenter Server / ESXi e le relative macchine virtuali gestite. Quando si utilizzano serie di ambiti dinamici, non è necessario definire ambiti per le LPAR o le macchine virtuali.
- Utilizzare ambiti Intervallo IP o Subnet per rilevare molteplici dispositivi, piuttosto che singoli indirizzi IP o nomi host. In questo modo, si porrà un limite al numero di definizioni di ambito e si semplificherà l'amministrazione.

- Se si utilizzano definizioni di ambito subnet, includerne una sola per ogni serie di ambiti. Assicurarsi che la definizione di ambito subnet si risolva in una rete Classe C (256 indirizzi IP) o di classe inferiore.
- Utilizzare la funzione **Importa serie di ambiti generali** per creare una nuova serie di ambiti in base al nome specificato e all'elenco degli indirizzi IP di un file di testo di input. Per ulteriori informazioni, consultare la sezione **Ambiti di rilevamento → Importa serie di ambiti generali** nella guida alla configurazione, per istruzioni.
- TSA attualmente memorizza solo indirizzi IP. Il che significa che i nomi host vengono risolti al momento dell'inserimento e non in quello del rilevamento. Le best practice suggeriscono di utilizzare l'Indirizzo IP o l'Intervallo IP per la definizione dell'ambito, non il nome host.
- Maggiore è il numero degli indirizzi IP che compongono la serie di ambiti, più lungo sarà il tempo di rilevamento. Per ridurre al minimo il tempo impiegato da un rilevamento, configurare gli ambiti in modo che considerino solo gli elementi che si vogliono rilevare.

Quando si utilizzano serie di ambiti generali, limitare il numero cumulativo di indirizzi IP in cui si risolve una serie di ambiti (dopo l'espansione di qualsiasi definizione di ambito di subnet o intervallo) a un massimo di 400. Si potrebbero riscontrare problemi di prestazioni, server o rete durante il processo di rilevamento, se vengono sottoposti a scansione più di 400 indirizzi IP per una singola serie di ambiti.

- TSA non preclude la definizione degli indirizzi IP in più serie di ambiti. In generale, tale procedura dovrebbe essere evitata, poiché aumenta il tempo di rilevamento senza implicare la raccolta di ulteriori informazioni.
- Raggruppare gli ambiti in serie di ambiti che costituiscono un raggruppamento logico di dispositivi:
  - Raggruppare dispositivi dello stesso tipo in una serie di ambiti. Ad esempio, creare una serie di ambiti per i sottosistemi di storage IBM FlashSystem.
  - Raggruppare dispositivi che si trovano nella stessa area geografica.
  - Raggruppare dispositivi in base ai servizi o alle applicazioni di business.

Credenziali di rilevamento

Con poche eccezioni, i rilevamenti richiedono un qualche livello di accesso per acquisire le informazioni dettagliate, necessarie per una completa comprensione del proprio ambiente.

Normalmente, dovrebbero essere creati account di servizio nei dispositivi di rilevamento, che TSA possa utilizzare. Esaminare le sezioni seguenti per conoscere i diritti di accesso specifici, richiesti da ogni tipo di piattaforma. Per semplificare l'amministrazione di questi account di servizio, utilizzare lo stesso nome utente per tutti i dispositivi di una determinata famiglia di prodotti.

L'attività di manutenzione degli account di servizio, che TSA utilizza per la connessione ai dispositivi, può essere semplificata adottando una delle seguenti strategie:

- Creare account di servizio con password senza scadenza
- Utilizzare chiavi SSH per famiglie di prodotti di dispositivi che ne supportino l'utilizzo.

Per istruzioni dettagliate riguardo alla modalità di definizione delle credenziali di accesso nell'appliance, consultare la sezione **Configurazione delle credenziali di rilevamento** nella guida alla configurazione.

Fattori da considerare nella configurazione delle credenziali di rilevamento

L'appliance tenta di utilizzare le credenziali nell'ordine in cui appaiono nell'elenco accessi. Per accelerare il rilevamento, assicurarsi che le credenziali siano elencate nell'ordine più appropriato per il proprio ambiente. Si possono effettuare le seguenti considerazioni:

- Limitare le credenziali a specifiche serie di ambiti, ove appropriato. In questo modo, si porrà un limite ai tentativi di accesso non necessari e verranno migliorate le prestazioni del rilevamento.
- Le chiavi SSH possono essere utilizzate per i rilevamenti di questi dispositivi:
  - AIX
  - Cisco
  - Linux
  - HMC
  - IBM i
  - IVM
  - Sun SPARC (Solaris)
  - SVC / V7000
  - VIOS
  - Fortinet
  - HP-UX
  - IBM FlashSystem

- F5 Big IP
- Check Point

Ad una serie di ambiti è possibile collegare solo una credenziale di chiave SSH.

- La best practice consiste nel creare account di servizio separati, utilizzati esclusivamente da TSA e per cui è richiesto il livello minimo di autorizzazione.

Guida introduttiva

Questa sezione tratta di alcune best practice e suggerimenti per la configurazione di TSA.

Installazione e configurazione iniziali di TSA

Passare in rassegna le istruzioni specificate nelle seguenti sezioni della guida alla configurazione:

- Installazione di Technical Support Appliance
- Accesso a Technical Support Appliance
- Accettazione dell'Accordo di licenza
- Configurazione di Technical Support Appliance utilizzando la procedura guidata di configurazione

Preparazione per i rilevamenti

Si consiglia un processo iterativo nel quale una piccola porzione della rete è inizialmente configurata per il rilevamento e ulteriori sezioni della rete vengono aggiunte ad ogni iterazione, fino alla copertura di tutta la rete desiderata.

> Una best practice consiste nel salvare un backup della propria configurazione di TSA dopo importanti aggiunte/modifiche apportate agli ambiti e/o alle credenziali. Per ulteriori informazioni, consultare la sezione "Backup e ripristino" nella guida alla configurazione di IBM Technical Support Appliance.

Fasi del rilevamento

Per ogni iterazione di rilevamento effettuare le seguenti operazioni:

1. Preparare i dispositivi per il rilevamento. Per qualsiasi requisito di configurazione di dispositivi e credenziali necessario, consultare la sezione "Configurazione del rilevamento dei dispositivi" a pagina 12.
2. Per le serie di ambiti dinamici HMC, effettuare le seguenti operazioni:
   a. Aggiungere gli indirizzi IP delle HMC nella pagina **Serie di ambiti dinamici HMC**.
   b. Aggiungere le credenziali per le HMC nella pagina **Serie di ambiti dinamici HMC**.
   c. Selezionare i tipi di LPAR che si desidera rilevare. Fornire le credenziali relative a ciascun tipo.

> È possibile selezionare i tipi di LPAR da rilevare quando viene creata la serie di ambiti dinamici oppure è possibile aggiungere i tipi di LPAR in una successiva iterazione, modificando la serie di ambiti dinamici.

d. (Facoltativo) Utilizzare la funzione Verifica nella pagina **Serie di ambiti dinamici HMC** per verificare che le credenziali siano correttamente definite e possano essere utilizzate per stabilire una connessione alle HMC o alle relative LPAR.

3. Per serie di ambiti dinamici VMWare, effettuare le seguenti operazioni:
   a. Aggiungere gli indirizzi IP dei VMware vCenter Server.
   b. Aggiungere gli indirizzi IP di qualsiasi host VMware ESXi non gestito da un VMware vCenter Server.
   c. Aggiungere le credenziali per le istanze VMware vCenter Server ed ESXi nella pagina **Serie di ambiti dinamici VMware**.
   d. Selezionare i tipi di macchina virtuale che si desidera rilevare. Fornire le credenziali relative a ciascun tipo.

      È possibile selezionare i tipi di macchina virtuale da rilevare quando viene creata la serie di ambiti dinamici oppure è possibile aggiungere i tipi di macchina virtuale in una successiva iterazione, modificando la serie di ambiti dinamici.

   e. (Facoltativo) Utilizzare la funzione Verifica nella pagina **Serie di ambiti dinamici VMware** per verificare che le credenziali siano correttamente definite e possano essere utilizzate per stabilire una connessione alle istanze VMware vCenter Server ed ESXi, oltre che alle relative macchine virtuali.
4. Per serie di ambiti generali, effettuare le seguenti operazioni:
   a. Aggiungere gli indirizzi IP desiderati nelle serie di ambiti / ambiti appropriati. Se esistono firewall tra l'istanza TSA e i dispositivi di rilevamento, assicurarsi che nel firewall siano aperte le porte appropriate per consentire l'esito positivo del rilevamento. Per informazioni sulle porte a cui si deve avere accesso per ogni tipo di piattaforma, consultare la sezione "Considerazioni sul firewall" a pagina 40.
   b. Creare le credenziali necessarie. Utilizzare la funzione Verifica nel pannello **Nuovo Rilevamento Credenziali** per verificare che la credenziale sia definita correttamente e possa essere utilizzata per stabilire una connessione con un dispositivo di destinazione.
5. Eseguire un rilevamento completo per la scansione degli indirizzi IP aggiunti per questa iterazione.
6. Eseguire una trasmissione per caricare i dati per IBM.

Configurazione del rilevamento dei dispositivi

Oltre a fornire le credenziali, è possibile che siano richiesti prerequisiti specifici per la configurazione dei dispositivi di rilevamento, perché TSA possa rilevare e raccogliere efficacemente informazioni utili sul componente. Questa sezione consente di identificare dispositivi di rilevamento nel proprio ambiente, per cui saranno necessarie configurazioni specifiche. Si consiglia di creare account di servizio con le autorizzazioni minime richieste, fare, inoltre, riferimento alla sezione "Considerazioni sul firewall" per informazioni su porte e protocolli.

- Per dispositivi per cui sono aperte porte SSH & Telnet, TSA tenterà innanzitutto una connessione utilizzando SSH (per motivi di sicurezza). Se questa connessione SSH non riesce, TSA tenterà, quindi, la connessione utilizzando Telnet.

Sistemi operativi e host

Piattaforma
IBM Power Systems • HMC (Hardware Management Console) • IVM (Integrated Virtualization Manager) • Partizioni VIOS (Virtual I/O Server) • AIX • Linux on Power
IBM i
Sistemi UNIX • Solaris • Solaris tramite iLOM • Linux • HP-UX
VMware vCenter Server e VMware ESXi
Windows
Dispositivi ATM

Modulo di gestione

- FSM (Flex System Manager)
- CMM (Chassis Management Module)
- AMM (Advanced Management Module)
- Server blade HP ProLiant tramite HP OnBoard Administrator
- Integrated Management Module (IMM & IMM2)
- Server HP Integrity & HP9000 tramite iLO

Fare clic su ognuno dei link riportati sopra per informazioni dettagliate.

IBM Power Systems

Per IBM Power Systems, dove la configurazione di LPAR è gestita da un'HMC o un IVM, utilizzare serie di ambiti dinamici HMC. Con le serie di ambiti dinamici HMC si crea una definizione di ambito per le HMC e fornire le credenziali per le HMC e le LPAR associate, ma non è necessario creare ambiti per ogni LPAR gestita. Quando l'HMC viene rilevata, TSA determina quali LPAR esistono in quello specifico momento ed esegue automaticamente la scansione di ogni LPAR.

Per IBM Power Systems dove la configurazione di LPAR è generalmente statica, un metodo alternativo alle serie di ambiti dinamici HMC consiste nell'iterare, aggiungendo ambiti e credenziali per le entità nel seguente ordine:

1. **Le istanze HMC o IVM**: L'HMC restituisce informazioni di livello elevato su tutti i componenti Power Systems che gestisce e sulle partizioni logiche in essi contenute. L'IVM restituisce informazioni simili per il singolo sistema che gestisce.
2. **Le partizioni VIOS**: Vengono restituite informazioni sulle risorse e gli adattatori fisici di proprietà di queste partizioni.
3. **Singole partizioni**: In alcuni casi, una partizione non VIOS possiede adattatori fisici.

HMC (Hardware Management Console)

Per rilevare istanze HMC, completare le seguenti operazioni:

Preparazione dell'ambiente:

- Perché TSA possa raccogliere informazioni sulla gestione delle LPAR tramite HMC, HMC deve essere in grado di comunicare con le LPAR mediante strumenti RMC.

Assicurarsi che l'HMC e le LPAR siano configurate per consentire tale comunicazione. Per ulteriori informazioni sugli strumenti RMC per Linux, andare all'indirizzo https://www14.software.ibm.com/webapp/set2/sas/f/lopdiags/yum.html

- Per consentire la raccolta sicura dei dati, deve essere abilitata l'esecuzione di comandi remoti sull'HMC. Per informazioni, consultare la pagina "Enabling and disabling HMC remote commands" (Abilitazione e disabilitazione di comandi remoti su HMC) al seguente indirizzo: https://www.ibm.com/support/knowledgecenter/POWER7/p7ha1/enablinganddisablinghmcremotecommands.htm

Credenziali per l'elenco accessi:

- Per serie di ambiti dinamici HMC - Autenticazione nome utente / password o nome utente / chiave SSH per l'account di servizio HMC.
- Per serie di ambiti di rilevamento generali - Computer: Autenticazione nome utente / password o nome utente / chiave SSH per l'account di servizio HMC.
- L'utente HMC deve disporre dei seguenti ruoli:
  - Ruolo risorsa: AllSystemResources
  - Ruolo attività (basato su **hmcoperator** con attività di riga comandi):
    - Sistema gestito (lshwres, lssyscfg)
    - Partizione logica (lshwres, lssyscfg, viosvrcmd)
    - Configurazione HMC (lshmc)
- Può essere utilizzato, se necessario, un utente (account di servizio) con autorizzazione **hmcviewer**, tuttavia, questo avrà come risultato una raccolta di dati parziale.

> Durante l'esecuzione con autorizzazione **hmcviewer**, non sarà possibile ottenere informazioni sugli adattatori di proprietà delle partizioni VIOS. Per ottenere queste informazioni, assicurarsi che l'account di servizio disponga, come minimo, dell'autorizzazione **hmcoperator**. Se questo non è possibile, aggiungere ambiti e credenziali per rilevare direttamente le partizioni VIOS, oltre all'HMC.

IVM (Integrated Virtualization Manager)

Per rilevare istanze IVM, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Autenticazione nome utente / password oppure nome utente / chiave SSH per l'account di servizio IVM.
- L'account di servizio deve disporre dell'autorizzazione di sola visualizzazione.

Partizioni VIOS (Virtual I/O Server)

Per rilevare istanze VIOS, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Per serie di ambiti dinamici HMC - Autenticazione nome utente / password o nome utente / chiave SSH per l'account di servizio della partizione VIOS.
- Per serie di ambiti di rilevamento generali - Computer: Autenticazione nome utente / password o nome utente / chiave SSH per l'account di servizio della partizione VIOS.
- L'account di servizio deve essere un account amministratore (ad esempio **padmin**).
- L'account di servizio deve disporre di un attributo utente **rlogin=true**. È possibile impostare questo attributo utilizzando SMIT oppure modificando il file **/etc/security/user**.
- Il parametro **PermitUserEnvironment** nel file **/etc/ssh/sshd_config** deve essere impostato su **yes**.

AIX

Per rilevare istanze AIX, completare le seguenti operazioni:

Preparazione dell'ambiente:

- Assicurarsi che siano installati i pacchetti bos.perf.tools e openSSH/openSSL.
- Disabilitare l'errore di tentativo di accesso non valido per l'account di servizio.

Credenziali per l'elenco accessi:

- Per serie di ambiti dinamici HMC - Autenticazione nome utente / password o nome utente / chiave SSH per l'account di servizio della partizione AIX.
- Per serie di ambiti di rilevamento generali - Computer: Autenticazione nome utente / password o nome utente / chiave SSH per l'account di servizio AIX.
- L'account di servizio può essere root o un account con autorizzazione sudo.
- L'account di servizio deve disporre di un attributo utente **rlogin=true**. È possibile impostare questo attributo utilizzando SMIT oppure modificando il file **/etc/security/user**.
- Per abilitare l'account di servizio non root per l'autorizzazione sudo per AIX:

- Installare l'RPM sudo (sudo-1.6.9p15-2noldap) e fileset ssh (openssh.base.server, openssh.base.client sull'istanza AIX).
- Creare un ID utente non root sull'istanza AIX di destinazione, che possa essere utilizzato da TSA per accedere al sistema.
- Modificare **/etc/sudoers** in ogni istanza AIX per consentire a TSA di eseguire i comandi specificati utilizzando l'autorizzazione sudo.

  # Cmnd alias specification

  ```
  Cmnd_Alias TSA_CMDS = /usr/bin/lparstat, /usr/sbin/no,
  /usr/sbin/nfso, /usr/bin/lslicense, /usr/sbin/vmo,
  /usr/sbin/ioo, /usr/sbin/lvmo, /usr/sbin/schedo,
  /usr/bin/sysdumpdev, /usr/sbin/smtctl, /usr/sbin/emgr,
  /usr/bin/sissasraidmgr, /usr/sbin/lswpar,
  /usr/sbin/cpuextintr_ctl, /usr/sbin/lsnim, /usr/sbin/raso,
  /usr/sbin/bosdebug, /usr/sbin/chedition,
  /usr/esa/bin/esacli, /usr/sbin/bootinfo,
  /usr/bin/mpio_get_config, /usr/bin/cat /etc/objrepos/CuData,
  /usr/bin/cat /etc/objrepos/CuData.vc, /usr/bin/cat
  /var/adm/ras/bootlog, /usr/bin/cat
  /etc/lpp/diagnostics/data/diagrpt*.dat, /usr/bin/tapeutil,
  /usr/lpp/OV/bin/opcagt, /usr/DynamicLinkManager/bin/dlnkmgr
  view, /usr/sbin/powermt version, /usr/sbin/powermt display,
  /usr/bin/pcmpath query, /usr/sbin/datapath query
  ```

  # User privilege specification

  ```
  <User Name> ALL = NOPASSWD: TSA_CMDS
  ```

  <User Name> è l'account di servizio non root che TSA utilizza per raccogliere informazioni su AIX. Questo <User Name> corrisponde ad un utente su ogni istanza AIX. Il file **/etc/sudoers** in ogni istanza AIX deve essere aggiornato con la precedente specifica.

  Oppure

  Un'alternativa alla modifica sopra riportata a **/etc/sudoers** è l'utilizzo della seguente specifica del privilegio utente:

  ```
  <User Name> ALL = NOPASSWD: ALL
  ```

  <User Name> è l'account di servizio non root che TSA utilizza per raccogliere informazioni su AIX. Questa specifica utente consente all'account di servizio di utilizzare l'autorizzazione sudo su qualsiasi comando AIX.

Linux on Power

Per rilevare istanze Linux on Power, completare le seguenti operazioni:

Preparazione dell'ambiente:

- Disabilitare l'errore di tentativo di accesso non valido per l'account di servizio.

Credenziali per l'elenco accessi:

- Per serie di ambiti dinamici HMC - Autenticazione nome utente / password o nome utente / chiave SSH per l'account di servizio della partizione Linux.
- Per serie di ambiti di rilevamento generali - Computer: Autenticazione nome utente / password o nome utente / chiave SSH per l'account di servizio Linux.
- Per abilitare l'account di servizio non root per l'autorizzazione sudo per Linux:
  - Creare un ID utente non-root sull'effettiva istanza Linux di destinazione che possa essere utilizzato da TSA per accedere al sistema.
  - Modificare **/etc/sudoers** in ogni istanza Linux per consentire a TSA di eseguire i comandi specificati utilizzando l'autorizzazione sudo.

    # Cmnd alias specification

    ```
    Cmnd_Alias TSA_CMDS = /usr/sbin/lsvpd, /sbin/lsvpd,
    /usr/sbin/lscfg, /sbin/lscfg, /usr/sbin/lsmcode,
    /sbin/lsmcode, /usr/sbin/lvmdiskscan, /sbin/lvmdiskscan,
    /usr/sbin/dmidecode, /usr/bin/mtlib, /usr/bin/tapeutil,
    /usr/bin/crontab, /sbin/fdisk, /bin/ls -alR /boot/*,
    /bin/cat /proc/irq/*, /bin/cat /proc/net/vlan/config,
    /bin/cat /proc/ppc64/rtas/*, /bin/cat /proc/sys/kernel/cap-
    bound, /bin/cat /proc/sys/kernel/random/entropy_avail
    ```

    # User privilege specification

    ```
    <User Name> ALL = NOPASSWD: TSA_CMDS
    ```

    - <User Name> è l'account di servizio non root che TSA utilizza per raccogliere informazioni su Linux. Questo <User Name> corrisponde ad un utente su ogni istanza Linux. Il file **/etc/sudoers** in ogni istanza Linux deve essere aggiornato con la precedente specifica.

    Oppure

    Un'alternativa alla modifica sopra riportata a **/etc/sudoers** è l'utilizzo della seguente specifica del privilegio utente:

    ```
    <User Name> ALL = NOPASSWD: ALL
    ```

    - <User Name> è l'account di servizio non root che TSA utilizza per raccogliere informazioni su Linux. Questa specifica utente consente all'account di servizio di utilizzare l'autorizzazione sudo su qualsiasi comando Linux.

- Se si utilizza il portale IBM Proweb per AIX, come parte dell'offerta di supporto con IBM, si consiglia di configurare TSA utilizzando serie di ambiti dinamici HMC.

  Come alternativa, è possibile configurare TSA per il rilevamento delle HMC e delle partizioni logiche (incluse le VIOS) nei Power Systems.

- Se si esegue la scansione utilizzando serie di ambiti dinamici HMC, si ottengono informazioni più dettagliate sulla configurazione del sistema operativo per ogni LPAR, che possono essere richiamate e analizzate da ProWeb.

> Per informazioni sull'aggiunta di ambiti e credenziali per gli ambienti HMC, consultare la sezione **Ambiti dinamici HMC** nella guida alla configurazione di IBM Technical Support Appliance.

- Livello di dati raccolti per il report mediante scansione di varie entità Power Systems:
  - Eseguendo la scansione solo delle HMC, si otterranno tutte le informazioni essenziali sulla scheda Identificato, sulle schede Topologia HMC, Firmware Power Systems, Suggerimenti IBM i, Suggerimenti Linux, HMC/VIOS/AIX e Contratto ed alcune informazioni sugli adattatori.
  - Eseguendo direttamente la scansione delle partizioni VIOS si otterranno informazioni supplementari sul firmware dell'adattatore e sullo storage connesso.
  - Eseguendo direttamente la scansione delle LPAR si otterranno ulteriori informazioni sulle LPAR, che includeranno dettagli del sistema operativo e istanze di software specifico, ad esempio PowerHA, GPFS e PowerSC.

IBM i

Istanze di IBM i vengono rilevate utilizzando una connessione SSH. Se sull'istanza IBM i non è installato e configurato SSH, completare le seguenti operazioni:

Preparazione dell'ambiente:

Assicurarsi che, per IBM i 7.2, siano installati e configurati i seguenti prodotti/opzioni:

- IBM Portable Utilities for i, 5733-SC1
- Qshell, 5770-SS1, opzione 30
- Portable App Solutions Environment, 5770-SS1, opzione 33
- IBM Developer Kit for Java, 5770-JV1

Assicurarsi che, per IBM i 7.3, siano installati e configurati i seguenti prodotti/opzioni:

- IBM Portable Utilities for i, 5733-SC1
- Qshell, 5770-SS1, opzione 30
- Portable App Solutions Environment, 5770-SS1, opzione 33
- IBM Developer Kit for Java, 5770-JV1 opzione 16
- Java SE 8 32 bit

Assicurarsi che, per IBM i 7.4, siano installati e configurati i seguenti prodotti/opzioni:

- IBM Portable Utilities for i, 5733-SC1
- Qshell, 5770-SS1, opzione 30
- Portable App Solutions Environment, 5770-SS1, opzione 33
- IBM Developer Kit for Java, 5770-JV1 opzione 16
- Java SE 8 32 bit

Per avviare il daemon SSH, eseguire questo comando:

```
SBMJOB CMD (CALL PGM (QP2SHELL) PARM('/QOpenSys/usr/sbin/sshd'))
```

Per avviare il servizio SSHD su IBM i, eseguire questo comando:

```
STRTCPSVR SERVER(*SSHD)
```

Per Per ulteriori informazioni sulla modalità di configurazione di SSH su IBM i, consultare i capitoli 21-23 di questo Redbook - http://www.redbooks.ibm.com/redpapers/pdfs/redp4163.pdf

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio può avere qualsiasi classe utente, anche ***USER**, sebbene siano necessari ulteriori requisiti di autorizzazione oggetto per raccogliere informazioni relative alle PTF (raccolta eseguita mediante il comando **DSPPTF**).
- **DSPPTF** prevede le seguenti limitazioni per l'autorizzazione oggetto:
  - Il comando viene fornito con l'autorizzazione pubblica ***EXCLUDE**
  - **I profili utente QPGMR**, **QSYSOPR**, **QSRV** e **QSRVBAS** vengono forniti con autorizzazioni private all'uso di questo comando
  - Come sempre, il profilo utente **QSECOFR** o qualsiasi profilo utente con una classe utente ***SECOFR** può eseguire questo comando
- È possibile modificare le autorizzazioni dell'oggetto **QSYS/DSPPTF** di tipo oggetto ***CMD**, per consentire ad altri eventuali utenti di eseguire questo comando.
- Se viene creato un nuovo account di servizio per TSA, saranno validi i seguenti suggerimenti:
  - Creare il profilo utente con classe utente ***USER**

- Utilizzare il comando **GRTOBJAUT** per consentire a questo profilo utente di eseguire il comando **DSPPTF**; l'oggetto è **QSYS/DSPPTF** di tipo oggetto ***CMD**.

Sistemi UNIX

Solaris

Per il rilevamento di dispositivi Solaris, completare le seguenti operazioni:

Preparazione dell'ambiente:

- Sui sistemi Solaris, accertarsi che sia installato il pacchetto SUNWscpu (Compatibilità del codice sorgente).
- Su alcuni sistemi Solaris, è necessario che sia installato e configurato SNEEP per ottenere i numeri di serie.

Credenziali per l'elenco accessi:

- Computer: Autenticazione nome utente / password o nome utente / chiave SSH per l'account di servizio.
- L'account di servizio può essere non root.

Solaris tramite Oracle iLOM

Per il rilevamento di dispositivi Solaris tramite Oracle iLOM, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio può disporre di privilegi di **Operatore** o **Amministratore**.

Linux

Se l'istanza Linux è in esecuzione su un IBM Power System, fare riferimento alla sezione Linux on Power a pagina 16, in IBM Power Systems, per istruzioni.

Per rilevare dispositivi Linux on x86, completare le seguenti operazioni:

Preparazione dell'ambiente:

- Assicurarsi che sia installato il pacchetto pciutils. Il comando `lspci` in esso contenuto viene utilizzato per raccogliere informazioni su adattatori e connessioni per dispositivi di storage esterni.

Credenziali per l'elenco accessi:

- Per serie di ambiti dinamici VMware - Autenticazione nome utente / password o nome utente / chiave SSH per l'account di servizio della macchina virtuale Linux.

- Per serie di ambiti di rilevamento generali – Computer: Autenticazione nome utente / password o nome utente / chiave SSH per l'account di servizio Linux.
- Impostare `/bin/sh` come shell per questo account.
- Per Linux (x86), l'account di servizio può essere root o un account con autorizzazione `sudo` .
- Per eseguire il rilevamento utilizzando un account di servizio non root, aggiungere quanto segue al file **/etc/sudoers** sul sistema Linux.

  # Cmnd alias specification

  ```
  Cmnd_Alias TSA_CMDS = /usr/sbin/dmidecode
  ```

  # User privilege specification

  ```
  <User Name> ALL = NOPASSWD: TSA_CMDS
  ```

  > <User Name> è l'account di servizio non root che TSA utilizza per raccogliere informazioni su Linux. Questo <User Name> corrisponde ad un utente su ogni istanza Linux. Il file **/etc/sudoers** in ogni istanza Linux deve essere aggiornato con la precedente specifica.

  Oppure

  Un'alternativa alla modifica sopra riportata a **/etc/sudoers** è l'utilizzo della seguente specifica del privilegio utente:

  ```
  <User Name> ALL = NOPASSWD: ALL
  ```

  > <User Name> è l'account di servizio non root che TSA utilizza per raccogliere informazioni su Linux. Questa specifica utente consente all'account di servizio di utilizzare l'autorizzazione sudo su qualsiasi comando Linux.

HP-UX

Per il rilevamento di dispositivi HP-UX, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Autenticazione nome utente / password oppure nome utente / chiave SSH per l'account di servizio.
- Per abilitare l'account di servizio non root per l'autorizzazione sudo per HP-UX:
  - Modificare **/usr/local/etc/sudoers** in ogni dispositivo HP-UX per consentire a TSA di eseguire i comandi specificati utilizzando l'autorizzazione sudo.

    # Cmnd alias specification

```
Cmnd_Alias TSA_CMDS
=/usr/sbin/diskinfo,/opt/hpvm/bin/hpvmstatus

# User privilege specification
<User Name> ALL=(ALL) NOPASSWD:TSA_CMDS
```

- <User Name> è l'account di servizio non root che TSA utilizza per raccogliere informazioni su HP-UX.

VMware vCenter Server e VMware ESXi

Per ambienti VMware, utilizzare serie di ambiti dinamici VMware. Con le serie di ambiti dinamici VMware si crea una definizione di ambito per VMware vCenter Server / ESXi e si forniscono le credenziali per VMware e le macchine virtuali associate, ma non è necessario creare ambiti per ogni macchina virtuale gestita. Quando viene rilevato il VMware vCenter Server / ESXi, TSA determina quali macchine virtuali esistono in quello specifico momento ed esegue automaticamente la scansione di ogni macchina virtuale.

Per ambienti VMware dove la configurazione di macchine virtuali è generalmente statica, un metodo alternativo alle serie di ambiti dinamici VMware consiste nell'iterare, aggiungendo ambiti e credenziali per le entità nel seguente ordine:

1. **Le istanze del server vCenter**: Vengono restituite informazioni di livello elevato sugli host ESXi che gestiscono e sui guest VM (Virtual Machine - Macchina Virtuale) in essi contenuti.
2. **Host ESXi**: Aggiungere host ESXi che non sono gestiti da un vCenter Server.
3. **Singoli guest VM (Virtual Machine - Macchina virtuale)**: È possibile la raccolta di informazioni più dettagliate, riguardanti il sistema operativo.

Quando si configura TSA per ambienti VMware, si consiglia l'esecuzione delle seguenti azioni:

1. Configurare TSA per rilevare VMware vCenter Server, se disponibili. Il rilevamento di un VMware vCenter Server automaticamente fa sì che TSA raccolga informazioni su tutti gli host VMware ESXi gestiti dal vCenter Server. Non sono necessarie informazioni sulla configurazione relative agli host ESXi.
2. Configurare TSA in modo che rilevi gli host VMware ESXi solo quando l'host ESXi non è gestito da un VMware vCenter Server.
3. Installare gli strumenti VMware su ogni macchina virtuale che risieda sugli host ESXi. Se non sono installati gli strumenti VMware, alcuni dati di inventario, ad esempio l'indirizzo IP o il sistema operativo installato, non saranno disponibili.
4. Configurare ogni host VMware ESXi in modo che l'interfaccia CIM sia attiva. L'interfaccia CIM consente a TSA di raccogliere informazioni dettagliate sugli adattatori contenuti

nell'host ESXi. Per ulteriori informazioni sul provider CIM, consultare l'"Appendice C" a pagina 44.

Per rilevare istanze del vCenter Server, oltre ad informazioni sui server ESXi che gestiscono, completare le seguenti operazioni:

Preparazione dell'ambiente

- Installare gli strumenti VMware su ogni macchina virtuale che risieda sugli host ESXi.
- Configurare ogni host VMware ESXi in modo che l'interfaccia CIM sia attiva.
- La porta CIM (5989) deve essere raggiungibile dal TSA (non bloccata da firewall, ecc.) per un rilevamento completo.

Credenziali per l'elenco accessi:

- Per serie di ambiti dinamici VMware - Nome utente / password per l'account di servizio del VMware vCenter Server.
- Per serie di ambiti di rilevamento generali - Computer: Nome utente / password per l'account di servizio VMware vCenter Server.
- L'account di servizio deve disporre di autorizzazioni del ruolo **Amministratore** o almeno autorizzazioni per un ruolo di sola lettura personalizzato, con i seguenti privilegi aggiuntivi:
  - Globale → Licenze
  - Globale → Impostazioni
  - Host → CIM
  - Host → Configurazione → Modifica impostazioni
  - Host → CIM→ Interazione CIM

Per il rilevamento diretto di dispositivi ESXi, completare le seguenti operazioni:

Preparazione dell'ambiente

- Installare gli strumenti VMware su ogni macchina virtuale che risieda sugli host ESXi.
- Configurare ogni host VMware ESXi in modo che l'interfaccia CIM sia attiva.

Credenziali per l'elenco accessi:

- Per serie di ambiti dinamici VMware - Nome utente / password per l'account di servizio VMware ESXi.

- Per serie di ambiti di rilevamento generali - Computer: Nome utente / password per l'account di servizio VMware ESXi.
- L'account di servizio deve disporre delle autorizzazioni di ruolo di **Amministratore**.

Windows

TSA supporta il rilevamento di istanze Windows con i metodi seguenti:

- WINRM
- SMB1

> Windows tramite WINRM è preferibile, perché si tratta dell'interfaccia più sicura.

Windows tramite WINRM

Per il rilevamento di dispositivi Windows tramite WINRM, completare le seguenti operazioni:

Preparazione dell'ambiente:

Il modo più comune per preparare l'ambiente consiste nell'utilizzare un certificato server generato da un'autorità di certificazione, che sia installato sul server Windows di destinazione. Il certificato deve soddisfare le seguenti condizioni:

- I certificati radice e intermedio emessi dall'autorità di certificazione si trovano nei certificati delle Autorità di certificazione radice attendibili.
- Il certificato server è installato nei Certificati personali
- Il certificato server deve indicare di essere stato emesso per il nome host completo del server.
- Il certificato server deve includere la chiave privata per il server.

Il seguente comando configura WINRM per connessioni HTTPS remote:

```
winrm quickconfig -transport:https
```

Questo comando svolge le seguenti azioni:

- Abilita WINRM, se al momento non è attivo
- Modifica il servizio WINRM, in modo che WINRM si avvi automaticamente ai riavvii
- Configura il listener WINRM HTTPS
- Modifica le regole del firewall Windows per consentire connessioni HTTPS remote

Il comando produce il seguente output. Immettere **y** per confermare le modifiche.

```
Il servizio WinRM è già in esecuzione su questa macchina.
WinRM non è configurato per consentire l'accesso da remoto a
questa macchina per la gestione.
Devono essere apportate le seguenti modifiche:
```

```
Creare un listener WinRM in HTTPS://* per l'accettazione di
richieste WS-Man a qualsiasi IP su questa macchina.
Configurare l'impostazione CertificateThumbprint per il servizio,
da utilizzare per l'autenticazione CredSSP.
Configurare LocalAccountTokenFilterPolicy per concedere i diritti
amministrativi agli utenti locali da postazione remota.

Eseguire queste modifiche [y/n]? y

WinRM è stato aggiornato per la gestione da remoto.

È stato creato un listener WinRM in HTTPS://* per l'accettazione
di richieste WS-Man a qualsiasi IP su questa macchina.
Sono state configurate le impostazioni richieste per il servizio.
È stata configurata l'impostazione LocalAccountTokenFilterPolicy
per concedere i diritti amministrativi agli utenti locali da
postazione remota.
```

Infine, per consentire l'autenticazione di id utente / password in HTTPS, emettere il seguente comando:

`winrm set winrm/config/service/auth @{Basic="true"}`

Un'alternativa consiste nell'utilizzare un certificato autofirmato. Le istruzioni per questa configurazione si trovano nell'Appendice D: Windows con WINRM a pagina 52.

Credenziali per l'elenco accessi:

- Per serie di ambiti dinamici VMware: Nome utente / password per l'account di servizio.
- Per serie di ambiti di rilevamento generali: Computer (Windows): Nome utente / password per l'account di servizio.
- L'account di servizio deve essere membro di uno dei seguenti gruppi:
  - Administrators
  - WinRMRemoteWMIUsers__

Per aggiungere un utente al gruppo WinRMRemoteWMIUsers__, utilizzare il seguente comando:

`net localgroup WinRMRemoteWMIUsers__ [user_id] /add`

Windows tramite SMB1

Per il rilevamento di dispositivi Windows, completare le seguenti operazioni:

Preparazione dell'ambiente:

- Assicurarsi che WSH (Windows Scripting Host) o il servizio WMI (Windows Management Instrumentation) e VBScript siano abilitati sul dispositivo di destinazione.

- Assicurarsi che la porta 445 non sia bloccata da politiche di sicurezza IP o firewall, poiché TSA richiede il protocollo Server Message Block (SMBv1) su TCP/IP.
- Per applicare le politiche di sicurezza, selezionare **Start → Pannello di controllo → Strumenti di amministrazione**, quindi, attenersi alla seguente navigazione in base al fatto che le proprie politiche siano memorizzate localmente o in un'Active Directory:
    - Politica memorizzata localmente: **Strumenti di amministrazione → Criteri di sicurezza locali → Criteri di sicurezza IP** su computer locale
    - Politiche memorizzate in Active Directory: **Strumenti di amministrazione → Impostazioni di protezione dominio predefinito → Criteri di sicurezza IP** su Active Directory oppure **Strumenti di amministrazione → Impostazioni di protezione controller di dominio predefinito → Criteri di sicurezza IP** su Active Directory
- TSA richiede l'accesso alla condivisione disco di amministrazione remota, nascosta, per l'accesso al sistema %TEMP% e ad altre directory. È necessario accedere anche all'IPC$ (Interprocess Communications share) perché TSA possa accedere ai registri remoti. Assicurarsi che il servizio Server Interprocess Communication Share sia avviato. Per avviare il servizio Server, selezionare il seguente percorso → **Pannello di controllo → Strumenti di amministrazione → Servizi → Server**.
- Assicurarsi che il Servizio Registro di sistema remoto sia attivo. Tale servizio è necessario perché TSA possa stabilire una sessione con il dispositivo Windows.

Credenziali per l'elenco accessi:

Windows release 2012 R2 e successive versioni:

- Per serie di ambiti dinamici VMware - Account amministratore base / password. Questo account funzionerà indipendentemente dalle impostazioni UAC (User Account Control - Controllo dell'account utente).

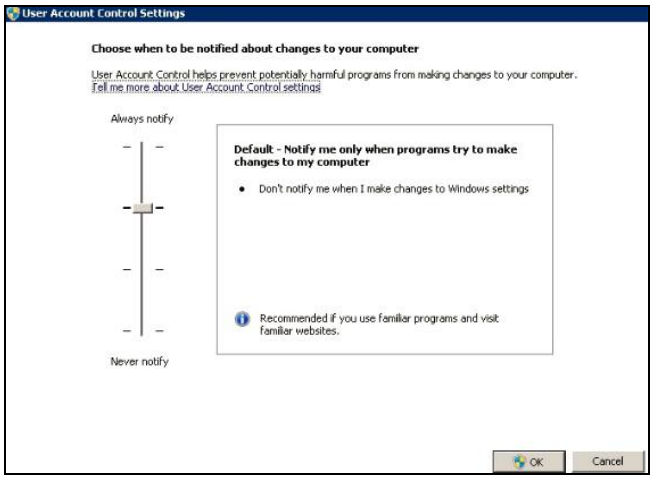
- Per serie di ambiti di rilevamento generali - Computer (Windows): Account amministratore base / password. Questo account funzionerà indipendentemente dalle impostazioni UAC (User Account Control - Controllo dell'account utente).

È possibile utilizzare un account diverso dall'account amministratore base, se verranno soddisfatte determinate condizioni. L'account deve essere un account amministratore locale o di dominio e le impostazioni UAC devono soddisfare determinati requisiti. Fare riferimento alla seguente tabella per conoscere le combinazioni di tipo account e impostazione UAC supportate. Fare riferimento alla documentazione di Microsoft Windows per ulteriori dettagli riguardanti il Controllo dell'account utente.

	Impostazioni UAC (User Account Control- Controllo dell'account utente)			
	Notifica sempre	**Notifica solo quando un'app tenta di eseguire modifiche nel computer (impostazione predefinita)**	**Notifica solo quando un'app tenta di eseguire modifiche nel computer (non attenuare il desktop)**	**Non notificare mai**
Amministratore base	**Sì**	**Sì**	**Sì**	**Sì**
Utente nel gruppo Amministratori di dominio	**No**	**Sì**	**Sì**	**Sì**
Utente nel gruppo Amministratori locali	**No**	**Sì**	**Sì**	**Sì**
Account non amministratore (Dominio o Locale)	**No**	**No**	**No**	**No**

Per accedere alle impostazioni Controllo dell'account utente, fare clic su **Start**, quindi, fare clic su **Pannello di controllo**. Immettere **uac** nella casella di ricerca e, quindi, fare clic su **Modifica impostazioni Controllo dell'account utente**.

Quella che segue, è l'impostazione predefinita:



Dispositivi ATM

È possibile rilevare determinati modelli di dispositivi ATM. Per rilevare i dispositivi ATM, incluse le informazioni di base sui relativi componenti, completare le seguenti operazioni:

Preparazione dell'ambiente:

- Modelli Wincor Nixdorf - Attenersi alle istruzioni fornite per Windows tramite SMB.

Modulo di gestione

Per IBM Flex Systems la scelta migliore è l'iterazione, con l'aggiunta di ambiti e credenziali per le entità nel seguente ordine:

1. **L'FSM (Flex System Manager):** Vengono restituite informazioni di livello elevato sui Flex System Manager e sugli Chassis che gestiscono, insieme ai relativi nodi di elaborazione associati.

   > Se non sono presenti FSM, si consiglia di effettuare la scansione dei CMM e di qualsiasi HMC che gestisca nodi di elaborazione POWER su sistemi Flex.

2. **Il CMM (Chassis Management Module):** Per chassis non gestiti da un FSM, fare riferimento a ciascun CMM per richiamare informazioni di livello elevato su ogni chassis e sui relativi nodi associati.
3. **I Nodi di elaborazione:** Vengono restituite informazioni dettagliate sul sistema operativo.

Dispositivi FSM (Flex System Manager)

Per il rilevamento di dispositivi FSM, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio deve disporre dell'autorizzazione **SMAdmin**.

Dispositivi CMM (Chassis Management Module)

Per il rilevamento di dispositivi CMM, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio deve disporre almeno dell'autorizzazione **operatore**.

Dispositivi AMM (Advanced Management Module)

Per il rilevamento di dispositivi AMM, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio deve disporre almeno dell'autorizzazione **operatore**.

Server blade HP Proliant tramite HP OnBoard Administrator

Per server HP (Hewlett Packard) ProLiant, la scelta migliore è quella di aggiungere ambiti e credenziali per le entità di HP OBA (HP OnBoard Administrator). HP OBA restituirà informazioni di livello elevato su HP OnBoard Administrator, sull'enclosure che gestisce e sui nodi di elaborazione contenuti all'interno dell'enclosure.

Per il rilevamento di un server blade HP Proliant tramite HP OBA (OnBoard Administrator), completare le seguenti operazioni:

Preparazione dell'ambiente:

- HP OBA deve trovarsi in modalità attiva.

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio deve disporre dell'autorizzazione **Amministratore OA**, **Operatore OA** oppure **utente OA in** HP Onboard Administrator. Si consiglia il ruolo **autorizzazione utente OA**.

> TSA raccoglie informazioni solo dagli HP OnBoard Administrator in stato attivo. Non viene raccolta alcuna informazione dagli HP OnBoard Administrator in stato di standby.

Dispositivi IMM (Integrated Management Module) & IMM2 (Integrated Management Module II)

Per il rilevamento di dispositivi IMM & IMM2, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio può disporre di qualsiasi autorizzazione valida.

Server HP Integrity & HP9000 tramite iLO

iLO è una scheda processore separata all'interno di un server HP Integrity & HP9000, che fornisce informazioni di base sull'hardware relative al server. La scheda iLO si attiva non appena il server viene collegato, anche se il server stesso non viene ancora acceso.

Per il rilevamento delle informazioni di inventario a livello di riepilogo, tramite iLO, per server HP Integrity & HP9000, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio può utilizzare qualsiasi livello di autorizzazione valido. Si consiglia l'autorizzazione **Utente**.

Dispositivi di rete

Questa sezione fornisce informazioni dettagliate sui seguenti tipi di dispositivi di rete:

Piattaforma
Switch BNT
Switch Brocade
Check Point
Switch Cisco
F5 Big-IP (TMOS)
Fortinet (FortiOS)
Switch SAN (Storage Area Network) tipo b IBM
Switch Juniper
Palo Alto Networks (PAN-OS)
Switch QLogic

Fare clic su ognuno dei link riportati sopra per informazioni dettagliate.

Switch BNT

Per il rilevamento di switch BNT, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio deve disporre dell'autorizzazione **admin**.

Brocade

Per il rilevamento di dispositivi Brocade, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- Modalità Fabric virtuale disabilitata: l'account di servizio può utilizzare qualsiasi autorizzazione valida. Si consiglia l'autorizzazione **Utente**.
- Modalità Fabric virtuale abilitata: l'account di servizio richiede l'autorizzazione **Amministratore** nel sistema operativo Fabric.

Check Point

Per il rilevamento di sistemi Check Point, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Autenticazione nome utente / password oppure nome utente / chiave SSH per l'account di servizio.
- L'account di servizio deve disporre dell'autorizzazione amministratore (**adminRole**).
- L'account di servizio deve disporre dell'accesso SSH per eseguire comandi CLI.

Cisco

Per il rilevamento di dispositivi Cisco, è possibile utilizzare le seguenti credenziali di computer o le credenziali SNMP:

Credenziali per l'elenco accessi:

- Computer o Altro (Dispositivo Cisco) o Altro (Lavori Cisco): Nome utente / password o nome utente / chiave SSH per l'account di servizio.
- L'account di servizio richiede privilegi di ruolo **network-admin**.
- SNMP: Immettere la stringa community (per SNMPv1 e SNMPv2).
- SNMP (SNMPv3):
  - Immettere:
    - nome utente
    - password
    - password privata (facoltativo)
  - Selezionare il protocollo di autenticazione: nessuno, MD5, SHA

> È importante che sia resa disponibile una singola stringa community per TSA, che ha accesso di sola lettura a TUTTI i dispositivi di rete dell'ambito.

F5 Big-IP (TMOS)

Per il rilevamento dei sistemi F5 Big-IP su cui è in esecuzione TMOS, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Autenticazione nome utente / password oppure nome utente / chiave SSH per l'account di servizio.
- L'account di servizio deve disporre dell'autorizzazione amministratore F5.
- L'account di servizio deve disporre dell'accesso SSH per eseguire comandi CLI TMSH.

Fortinet (FortiOS)

Per il rilevamento di dispositivi Fortinet su cui è in esecuzione FortiOS, completare le seguenti operazioni:

Preparazione dell'ambiente

- Assicurarsi che la console di sistema sia configurata per visualizzare l'intero output del comando:

```
config system console
set output standard
end
```

Credenziali per l'elenco accessi:

- Computer: Autenticazione nome utente / password oppure nome utente / chiave SSH per l'account di servizio.
- L'account di servizio deve disporre almeno di autorizzazioni di sola lettura.

Switch SAN (Storage Area Network) tipo b IBM

Per il rilevamento di dispositivi SAN tipo b IBM, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- Modalità Fabric virtuale disabilitata: l'account di servizio può utilizzare qualsiasi autorizzazione valida. Si consiglia l'autorizzazione **Utente**.
- Modalità Fabric virtuale abilitata: l'account di servizio richiede l'autorizzazione **Amministratore** nel sistema operativo Fabric.

Juniper

Per rilevare dispositivi Juniper, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.

- L'account di servizio deve disporre dell'autorizzazione amministratore.

> **Nota**: per il rilevamento di informazioni sulla dimensione della memoria è necessario che sul dispositivo sia installato Junos® versione 12.1 o successive.

Palo Alto Networks (PAN-OS)

Per il rilevamento di sistemi Palo Alto Network su cui è in esecuzione PAN-OS, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio deve disporre dell'autorizzazione Superutente o Superutente (sola lettura).
- L'account di servizio deve avere accesso API REST (porta 443).

Switch QLogic

Per il rilevamento di switch QLogic, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio deve disporre dell'autorizzazione amministratore.

Dispositivi di storage

Questa sezione fornisce informazioni dettagliate sui seguenti tipi di dispositivi Storage e Nastro:

Piattaforma
Storage EMC Corporation
HP StorageWorks P2000 Modular Smart Array
IBM DS3xxx, DS4xxx o DS5xxx
IBM DS6xxx o DS8xxx
IBM FlashSystem, v9000
IBM ProtecTier
IBM SVC o V7000/V3700
Libreria nastro IBM TS3100
Libreria nastro IBM TS3200

Piattaforma
Libreria nastro IBM TS3310
Librerie nastro IBM TS3494, TS3953
Librerie nastro IBM TS3500, TS3584
Libreria nastro IBM TS4500
Libreria nastro IBM TS7700
IBM V7000 Unified
IBM XIV
nSeries o NetApp

Fare clic su ognuno dei link riportati sopra per informazioni dettagliate.

Storage EMC Corporation

EMC CLARiiON / VNX / VMAX

Per il rilevamento di dispositivi EMC CLARiiON / VNX / VMAX, completare le seguenti operazioni:

Preparazione dell'ambiente:

- Assicurarsi che un'istanza del prodotto EMC SMI-S Provider sia installata su un sistema Windows o Linux. Per impostazione predefinita, TSA segue il suggerimento di EMC SMI-S per rilevare l'ubicazione del provider utilizzando SLP. Se la politica per la sicurezza di rete blocca il traffico di rete SLP, è possibile configurare TSA per un accesso diretto a EMC SMI-S Provider, senza l'utilizzo di SLP.
- Se la sicurezza di rete non consente il traffico di rete SLP, utilizzare la pagina **Impostazioni di rilevamento→ Impostazioni di connessione** per fornire informazioni sulle porte che gli EMC SMI-S Provider utilizzeranno per ascoltare richieste di query.
- Accertarsi che almeno uno degli indirizzi IP che l'SMI-S Provider sta utilizzando sia definito in una serie di ambiti. TSA si connetterà all'SMI-S Provider per recuperare informazioni sui dispositivi EMC che gestisce. Gli indirizzi IP dei singoli dispositivi EMC non è necessario che siano inseriti in una serie di ambiti. TSA tenta di

connettersi all'SMI-S Provider utilizzando HTTPS, se disponibile, altrimenti verrà utilizzato HTTP.

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio può utilizzare qualsiasi ruolo valido. Si consiglia il ruolo **monitor**.

> In TSA, è necessario immettere solo le credenziali per l'SMI-S Provider. Non si dovranno immettere credenziali per i dispositivi EMC.

Dominio dati EMC

Per il rilevamento di dispositivi Dominio dati EMC, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio può disporre dell'autorizzazione minima richiesta.

HP StorageWorks P2000 Modular Smart Array

Per il rilevamento di sistemi HP Storage, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio può disporre dell'autorizzazione minima richiesta.

Storage IBM DS3xxx, DS4xxx o DS5xxx

Per il rilevamento di dispositivi IBM DS3xxx, DS4xxx o DS5xxx, completare le seguenti operazioni:

Preparazione dell'ambiente:

- Assicurarsi che la gestione dello storage consenta l'utilizzo di comandi **smcli** remoti.

Credenziali per l'elenco accessi:

- Per dispositivi di storage non protetti, non sono richieste credenziali.
- Per dispositivi di storage protetti, completare le seguenti operazioni:
  - Computer: Nome utente / password per l'account di servizio.
  - L'account di servizio può avere il ruolo **amministratore** o **monitor**. Si consiglia il ruolo **monitor**.

Storage IBM DS6xxx / DS8xxx

Per il rilevamento di dispositivi IBM DS6xxx / DS8xxx, completare le seguenti operazioni:

Preparazione dell'ambiente:

- Assicurarsi che la gestione dello storage consenta l'utilizzo di comandi **dscli** remoti.

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio deve disporre del ruolo **monitor**.

IBM FlashSystem, v9000

Per il rilevamento di IBM FlashSystem, completare le seguenti operazioni:

Preparazione dell'ambiente:

- Per modelli non recenti, l'MCP (Management Control Port - Porta di controllo gestione) deve trovarsi in stato attivo, ai fini dell'esito positivo del rilevamento del sistema.
  - Per controllare che un sistema sia in stato attivo, eseguire il comando - `system status`.
  - Se uno dei due indirizzi IP si disattiva, lo stato del sistema diventerà passivo. Per rendere attiva l'altra porta Ethernet, eseguire il comando - `sync activate`.
  - Il sistema rilevato deve essere l'indirizzo IP di gestione e/o il nodo di configurazione.

Credenziali per l'elenco accessi:

- Computer: Autenticazione nome utente / password oppure nome utente / chiave SSH per l'account di servizio.
- L'account di servizio può utilizzare qualsiasi ruolo valido. Si consiglia il ruolo **monitor**.

IBM ProtecTIER

Per rilevare dispositivi ProtecTIER, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio deve disporre di privilegi di amministratore.

Storage IBM SVC, V7000/V3700

Per il rilevamento di dispositivi SVC e V7000/V3700, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Nome utente / password o nome utente / chiave SSH per l'autenticazione.

- L'account di servizio può utilizzare qualsiasi ruolo valido. Si consiglia il ruolo **monitor**.

Libreria nastro IBM TS3100

Per il rilevamento di dispositivi Libreria nastro TS3100, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio deve disporre dell'autorizzazione amministratore.

Libreria nastro IBM TS3200

Per il rilevamento di dispositivi Libreria nastro TS3200, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio deve disporre dell'autorizzazione amministratore.

Libreria nastro IBM TS3310

Per il rilevamento di dispositivi Libreria nastro TS3310, completare le seguenti operazioni:

Preparazione dell'ambiente:

- Il servizio Web è configurato sempre in modalità protetta.

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio deve disporre dell'autorizzazione amministratore.

Librerie nastro IBM TS3494, TS3953

Per il rilevamento di dispositivi Libreria nastro TS3494, TS3953, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio può disporre dell'autorizzazione minima richiesta.

Librerie nastro IBM TS3500, TS3584

Sono obbligatori i seguenti prerequisiti:

- La Libreria nastro TS3500 deve trovarsi al livello firmware 8xxx (o superiore).
- L'ALMS (Advanced Library Management System) deve essere installato e abilitato.

Sono supportate connessioni sia SSL che non SSL.

Per il rilevamento di dispositivi Libreria nastro TS35xx, completare le seguenti operazioni:

Preparazione dell'ambiente:

- L'interfaccia Web TS3500 può essere configurata per **Nessuna protezione della password** o **Protezione della password**
  - Se è attivata **Protezione della password**, creare una credenziale, come descritto nella sezione **Credenziali per l'elenco accessi** sottostante.
  - Se **Protezione della password** è disabilitata, non sono richieste credenziali.

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio deve disporre dell'autorizzazione amministratore.

Libreria nastro IBM TS4500

Sono obbligatori i seguenti prerequisiti:

- La libreria nastro TS4500 deve trovarsi al livello firmware 1.4.1.2 o superiori (fino a 1.7.0.0).
- L'ALMS (Advanced Library Management System) deve essere installato e abilitato.


Sono supportate connessioni sia SSL che non SSL.

Per il rilevamento di dispositivi Libreria nastro TS4500, completare le seguenti operazioni:

Preparazione dell'ambiente:

- L'interfaccia Web TS4500 può essere configurata solo per **Protezione della password**.

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio deve essere associato al ruolo **Servizio**.

Libreria nastro IBM TS7700

Per il rilevamento di dispositivi Libreria nastro TS7700, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio necessita unicamente dell'autorizzazione **Sola lettura**.

Storage IBM V7000 Unified

Per il rilevamento di dispositivi V7000 Unified, completare le seguenti operazioni:

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio può utilizzare qualsiasi ruolo valido. Si consiglia il ruolo **monitor**.

Storage IBM XIV

Per il rilevamento di dispositivi XIV, completare le seguenti operazioni:

Preparazione dell'ambiente:

- Assicurarsi che la gestione dello storage consenta l'utilizzo di comandi **xcli** remoti.

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio deve disporre del ruolo utente di **sola lettura**.
- Tenere presente che i sistemi XIV possono avere una soglia bassa per i tentativi di collegamento non validi, prima di generare avvisi. Se si utilizza un vasto insieme di credenziali, si potrebbe superare questo limite e causare la segnalazione di problemi superflui. Provare a raggruppare i dispositivi XIV in una singola serie di ambiti e a limitare le relative credenziali di account di servizio a tale serie di ambiti.

Storage nSeries o NetApp

Per il rilevamento di dispositivi nSeries o NetApp, completare le seguenti operazioni:

Preparazione dell'ambiente:

- La raccolta dei dati è supportata per sistemi configurati con Data ONTAP CLI, RLM CLI e SP CLI. Tuttavia, la BMC CLI non è supportata.
- L'opzione **telnet.distinct.enable** deve essere attivata.

Credenziali per l'elenco accessi:

- Computer: Nome utente / password per l'account di servizio.
- L'account di servizio può disporre dell'autorizzazione minima richiesta.

Considerazioni sul firewall

I firewall posizionati tra l'appliance e i dispositivi di rilevamento potrebbero impedire l'esecuzione di un rilevamento completo e con esito positivo.

Nei casi in cui è necessario attraversare un firewall, è possibile che si debbano aprire porte nel firewall, in base al tipo di dispositivo che l'utente ha intenzione di rilevare. Di norma, dovrebbero essere aperte le porte 22 (SSH) e 161 (SNMP), seguite da quelle appropriate, indicate nella seguente tabella, in base ai dispositivi supportati.

Endpoint di rilevamento	**Porte**	**Interfaccia / Protocollo**
Numerosi	161	SNMP
Dispositivi di storage		
DS6000 / DS8000	1750 (HTTP) o 1751 (HTTPS)	DSCLI
DS3000 / DS4000 / DS5000	2463	SMCLI
XIV	7778	XCLI
nSeries o NetApp	22 / 23	SSH o Telnet
SVC o V7000/V3700	22	SSH
V7000 Unified	22	SSH
IBM TS3500	443 / 80	HTTPS o HTTP
IBM TS4500	443 / 80	HTTPS o HTTP
IBM TS7700	443 / 80	HTTPS o HTTP
IBM TS3100 / TS3200 / TS3310	80	HTTP
IBM TS3494, TS3953	23	Telnet
IBM ProtecTier	22	SSH
HP Storage	22 / 23	SSH o Telnet
IBM Flash System, v9000	22	SSH

Endpoint di rilevamento	Porte	Interfaccia / Protocollo
Storage EMC Corporation - CLARiion/VNX/VMAX	427 - (valore predefinito) quando è consentito il rilevamento SLP, altrimenti, se il rilevamento SLP è disabilitato, questa porta non verrà utilizzata. Porte HTTPS / HTTP configurate da EMC SMI-S Provider; i valori predefiniti sono 5989 / 5988	SLP, HTTPS / HTTP
	È possibile abilitare o disabilitare l'opzione di rilevamento SLP, per il rilevamento di dispositivi di storage EMC tramite gli EMC SMI-S Provider.	
Storage EMC Corporation – Dominio dati EMC	22	SSH*
Sistemi operativi e host		
FSM	22 / 23	SSH o Telnet
CMM	22 / 23	SSH o Telnet
AMM	22 / 23	SSH o Telnet
Server blade HP Proliant tramite HP OnBoard Administrator	22 / 23	SSH o Telnet
IMM & IMM2	22 / 23	SSH o Telnet
HP iLO per i server HP Integrity / HP 9000	22 / 23	SSH* o Telnet
Dispositivi di rete		
Brocade	161 / 22 /23	SNMP, SSH, Telnet
Switch SAN (Storage Area Network) tipo b IBM	22 /23	SSH, Telnet
Cisco	161 / 22 / 23	SNMP, SSH, Telnet
BNT	22 / 23	SSH o Telnet
Juniper	22 / 23	SSH o Telnet

Endpoint di rilevamento	Porte	Interfaccia / Protocollo
QLogic	22 / 23	SSH* o Telnet
Fortinet (FortiOS)	22 / 23	SSH o Telnet
Palo Alto Networks (PAN-OS)	443	HTTPS
F5 Big-IP (TMOS)	22 / 23	SSH o Telnet
Check Point	22 / 23	SSH o Telnet
Sistemi operativi / Piattaforme server		
HMC	22	SSH
VIOS	22	SSH
AIX	22	SSH
Linux	22	SSH
Windows	445	SMBv1
VMware vCenter	443	HTTPS
VMware ESXi	443, 5989	HTTPS
IVM	22 / 23	SSH o Telnet
IBM i	22	SSH
SUN	22	SSH

- TSA supporta unicamente SSH v1 per i dispositivi che riportano il contrassegno SSH*.

Problemi di rilevamento

La maggior parte dei problemi di rilevamento sono dovuti a problematiche relative all'accesso o alle autorizzazioni.

I più comuni problemi di accesso sono causati dai firewall che impediscono l'accesso alle porte necessarie sul dispositivo. Le porte che devono essere aperte e raggiungibili variano in base al tipo di dispositivo. Consultare la sezione "Considerazioni sul firewall" a pagina 40 per determinare quali porte siano utilizzabili.

I più comuni problemi inerenti le autorizzazioni includono i seguenti:

- **Nessuna credenziale definita**. Assicurarsi che le credenziali per i dispositivi siano definite in TSA e che siano creati gli account di servizio appropriati sui dispositivi.
- **Nome utente o password della credenziale non corretti**. Utilizzare la funzione **Verifica** quando si crea o si modifica una credenziale, per verificare che la credenziale sia valida.
- **Password della credenziale scaduta**.
- **La credenziale manca delle autorizzazioni necessarie sul dispositivo**. Per stabilire i requisiti di credenziale per un dispositivo di destinazione, consultare la sezione Configurazione del rilevamento dei dispositivi a pagina 12.
- **Utilizzare un tipo di credenziale valido**. Per dispositivi Windows, creare una credenziale 'Computer (Windows)' e non una credenziale 'Computer'.

Controllare la pagina **Stato autenticazione (Strumenti → Stato autenticazione)** per verificare se se la password di qualche credenziale dell'account di servizio sia scaduta o se la credenziale abbia smesso di funzionare.

Considerazioni sulle attività da svolgere periodicamente

Una volta definite le parti desiderate della rete in TSA ed eseguita con esito positivo la scansione, si può impostare TSA per l'esecuzione di rilevamenti e trasmissioni con frequenza periodica, in base alle pianificazioni desiderate.

Quelle che seguono, sono alcune delle attività previste, da svolgere periodicamente:

- Esaminare i report generati da TSA con il rappresentante IBM di riferimento su base periodica.
- Eseguire periodicamente un backup tramite l'interfaccia utente di TSA, per salvare una copia della configurazione di TSA.

Questa operazione non implicherà il salvataggio dei dati raccolti da TSA. Verranno salvate solo le informazioni sulla configurazione.

- Controllare periodicamente la pagina **Stato autenticazione (Strumenti → Stato autenticazione)** per verificare se la password di qualche credenziale dell'account di servizio sia scaduta o se la credenziale abbia smesso di funzionare.
- Quando vengono aggiornate le password per gli account di servizio sui dispositivi, assicurarsi di aggiornare le password anche in TSA, per mantenere la sincronizzazione tra la definizione della credenziale in TSA e la credenziale sul dispositivo di destinazione.
- Se la propria politica di sicurezza lo consente, prendere in considerazione la possibilità di configurare gli account di servizio con password senza scadenza o utilizzare chiavi SSH. In questo modo, si elimina la necessità di aggiornare periodicamente le password nell'interfaccia utente TSA e sui dispositivi.

Risoluzione dei problemi

Sessione attiva per il rilevamento AMM

I dispositivi AMM hanno un'impostazione per limitare il numero di sessioni attive simultanee (un massimo di 20). Se il valore di tale impostazione non è sufficientemente elevato da consentire a TSA di creare una sessione, non sarà possibile rilevare il dispositivo AMM.

Per modificare il limite delle sessioni attive di un dispositivo AMM, seguire questa procedura:

1. Accedere all'interfaccia Web AMM immettendo l'indirizzo IP del dispositivo AMM in un browser Web.
2. Andare a **Controllo MM → Profili di accesso**.
3. Fare clic sull'ID di accesso che TSA sta utilizzando per il rilevamento del dispositivo.
4. Incrementare il valore dell'impostazione **Numero massimo di sessioni attive simultanee**.
5. Fare clic su **Salva** nell'angolo inferiore destro della pagina.

Appendice A: Termini e definizioni

Si presuppone che il lettore abbia una conoscenza approfondita delle reti e dei protocolli IP (Internet Protocol).

Termine	**Definizione**
Dispositivo di rilevamento	Fa riferimento ai componenti dell'infrastruttura IT implementati, che possono essere rilevati da TSA. Esempi tipici di dispositivi includono: Server, Computer (IBM, Dell, HP e così via), Elementi di storage ed Elementi di rete (tra cui switch, bridge, router).

Appendice B: Argomenti vari

Funzioni di scaricamento dell'interfaccia utente

In alcuni casi, quando si utilizza un browser Web, l'azione Scarica tutti i log (dalla pagina **Log attività**), gli scaricamenti dei file (dalla pagina **Cronologia rilevamento**) o gli scaricamenti della documentazione (dalla pagina **Documentazione**) non si completano con esito positivo. Per risolvere questo problema, provare ad utilizzare un altro browser Web supportato, come documentato nella Guida alla configurazione di IBM Technical Support Appliance. Se non è possibile farlo, provare a ripristinare le impostazioni predefinite per le proprietà del browser in uso.

Appendice C: CIM Provider per VMware ESXi

Per CIM Provider si intende una serie di plug-in VMware ESXi, in grado di raccogliere ulteriori informazioni su hardware e firmware relative al server su cui è in esecuzione VMware ESXi.Sia TSA che VMware vCenter possono usufruire di queste informazioni supplementari.

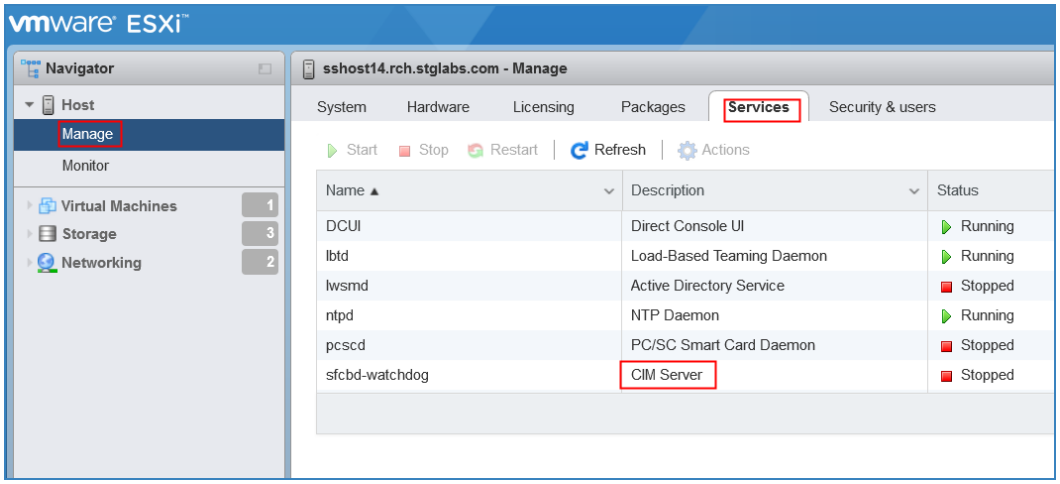
I plug-in CIM Provider sono sviluppati dai produttori del server e dei componenti. Per garantire che i plug-in CIM Provider siano inclusi in ESXi, utilizzare un'immagine di installazione personalizzata, nella quale siano inclusi i plug-in CIM Provider. Per istanze VMware ESXi esistenti, su cui non è installato il CIM Provider, ottenere i plug-in necessari dai produttori del server e dei componenti e installarli in ESXi. VMware fornisce un elenco dei vari plug-in forniti dai produttori.

Per ulteriori informazioni, consultare il documento all'indirizzo https://www.vmware.com/resources/compatibility/pdf/vi_cim_guide.pdf.

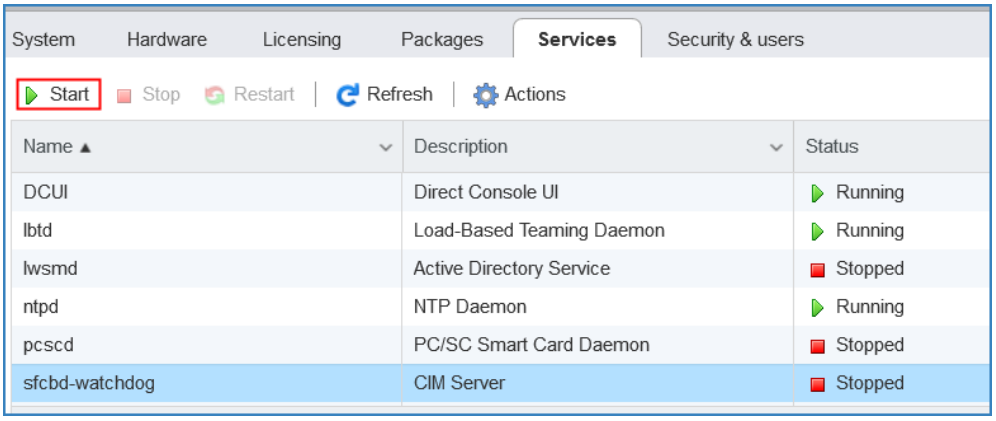
Per stabilire se il CIM Provider è attivo e per attivare il CIM Provider nel caso non sia attivo, svolgere le seguenti operazioni.

Sul Client Web VMware vSphere

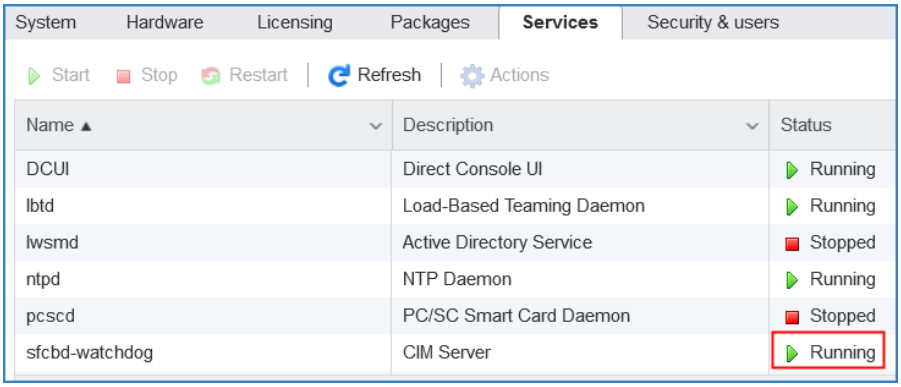
- Accedere al Client Web VMware vSphere.
- Fare clic su **Host → Gestisci** nella finestra di navigazione sulla sinistra e selezionare la scheda **Servizi** nel riquadro di destra.
- Viene visualizzata una serie di servizi, che include il **Server CIM**.



- Se il **Server CIM** si trova nello stato **Arrestato**, selezionarlo e fare clic su **Avvia**.

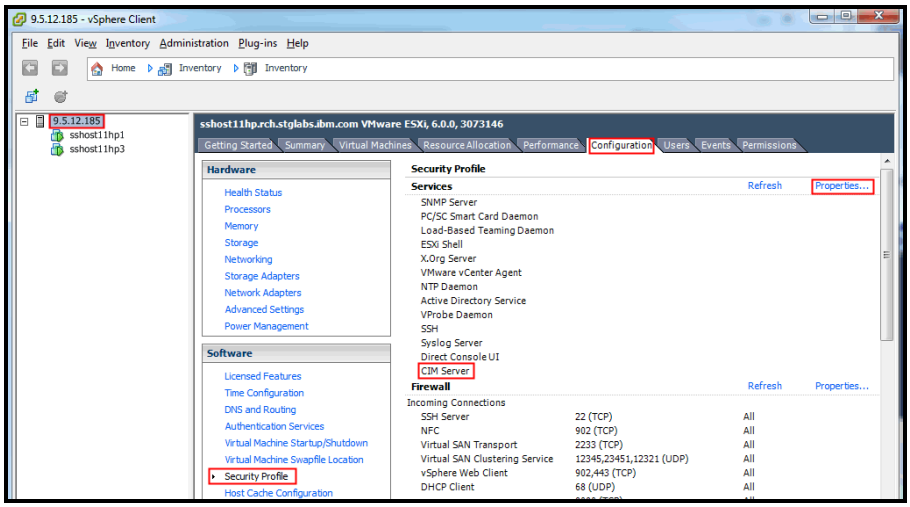


- Il servizio Server CIM si avvia e lo stato diventerà **In esecuzione**.

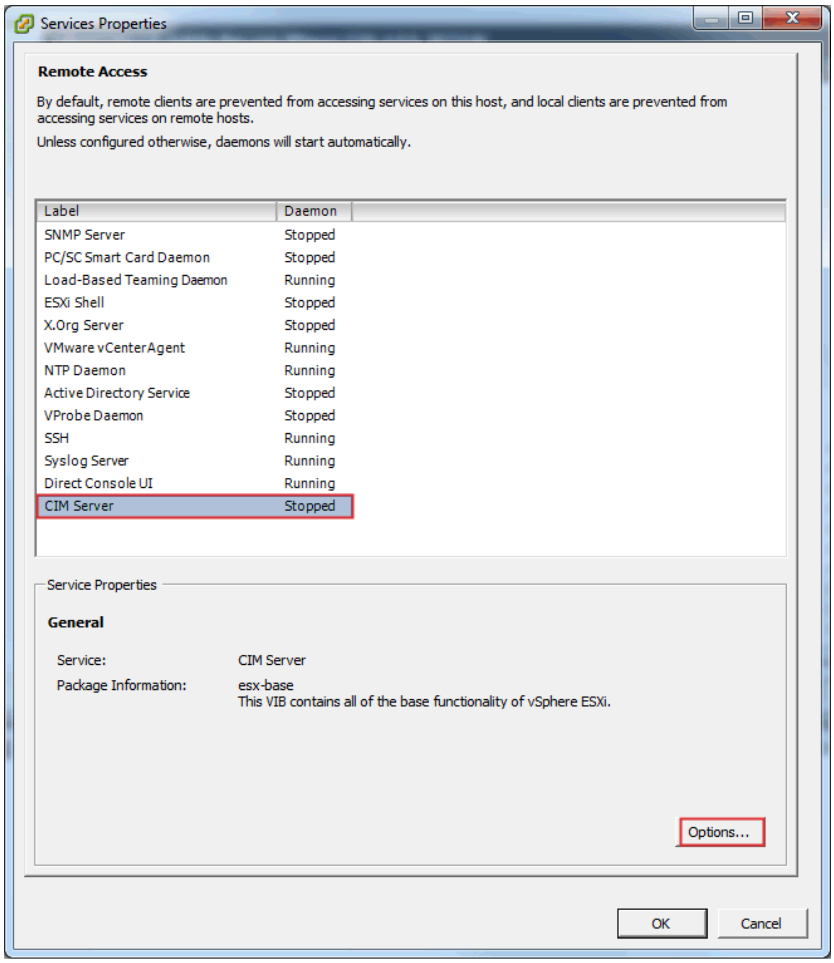


Sul Client VMware vSphere

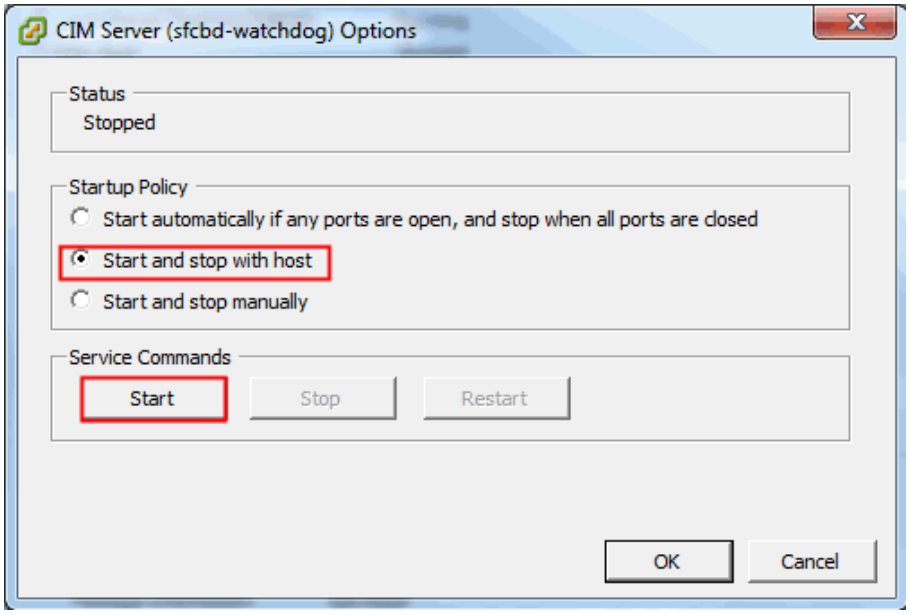
- Avviare il client VMware vSphere.
- Fare clic sull'IP del server ESXi nella finestra di navigazione sulla sinistra e selezionare la scheda **Configurazione** nel riquadro di destra.
- Selezionare **Profilo di sicurezza** dal menu di selezione **Software** nel riquadro di destra. Viene visualizzata una serie di servizi, che includono **Server CIM** nella sezione **Servizi** .



- Selezionare la voce **Proprietà...** nella sezione **Servizi**.



- Se il **Server CIM** si trova nello stato **Arrestato**, selezionarlo e fare clic su **Opzioni...**. Verrà visualizzata la seguente finestra di dialogo.



- Selezionare la **Politica di avvio (opzione Avvia e arresta con** host) e fare clic su **Avvia** per attivare il Server CIM.

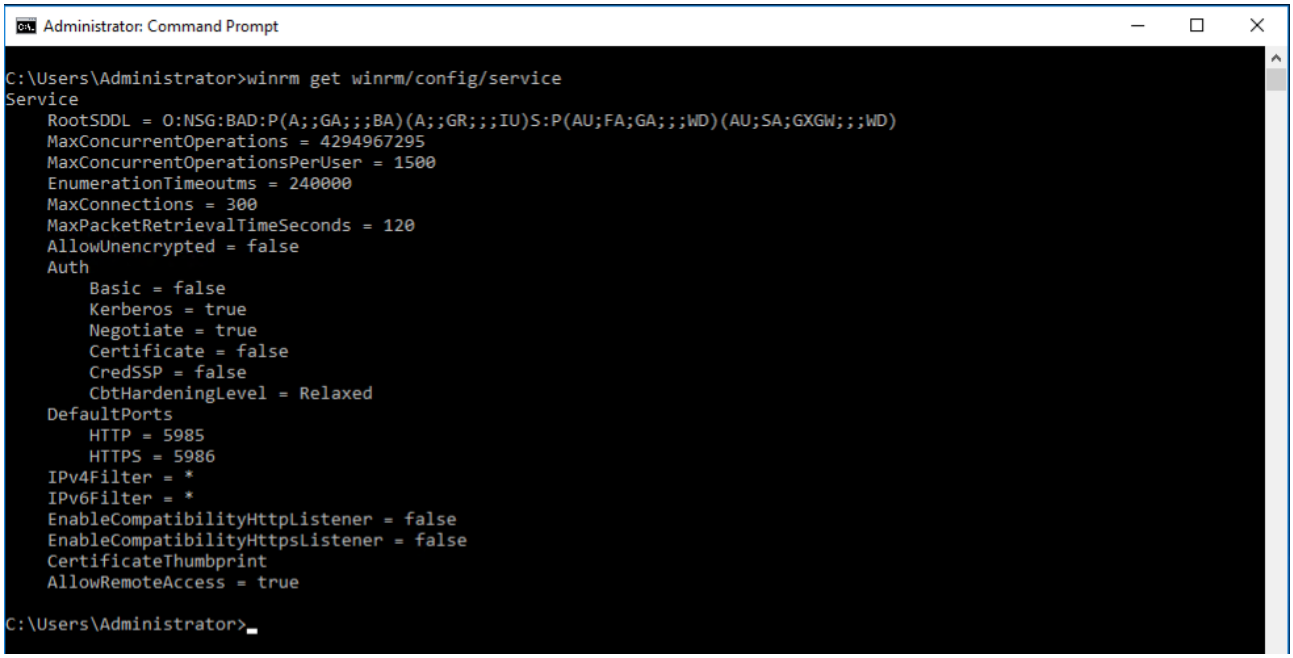
Appendice D: Windows con WINRM

Per Windows Server 2012 e 2016, il servizio WINRM verrà avviato automaticamente. Tuttavia, la gestione remota non è abilitata per impostazione predefinita. Ecco un breve schema degli elementi richiesti per abilitare WINRM, in modo che consenta connessioni da remoto utilizzando un certificato autofirmato:

- Abilitare WINRM per accettare connessioni HTTPS autenticate con ID utente / password
- Associare un certificato autofirmato al listener HTTPS per WINRM che è stato abilitato.
- Modificare il firewall Windows per consentire connessioni in entrata tramite la porta 5986 (la porta HTTPS WINRM predefinita)

I seguenti comandi preparano WINRM a consentire connessioni remote tramite HTTPS:

- Determinare lo stato corrente del servizio WINRM utilizzando questo comando:



winrm get winrm/config/service

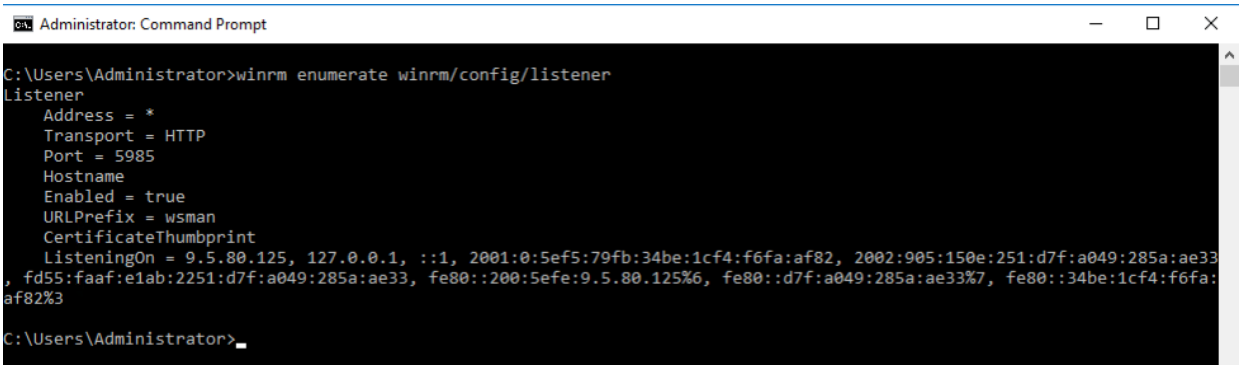
- Il valore per **AllowUnencrypted** deve essere *false*. Se il valore fosse *true*, utilizzare il seguente comando per modificarlo in *false*:
  winrm set winrm/config/service @{AllowUnencrypted="false"}

- Il valore per **Basic** deve essere *true*. Se il valore fosse *false*, utilizzare il seguente comando per modificarlo in *true*:

  winrm set winrm/config/service/auth @{Basic="true"}

- Determinare se WINRM dispone di un listener HTTPS utilizzando questo comando:

  winrm enumerate winrm/config/listener

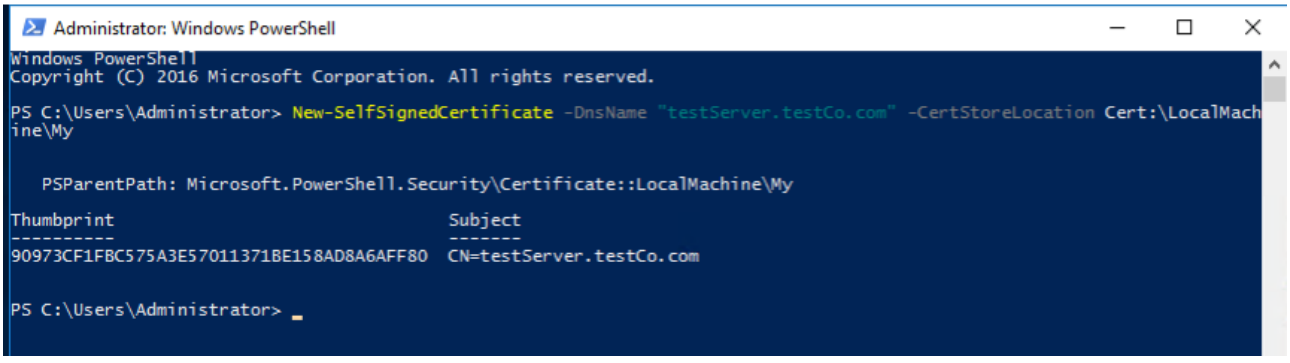


- Nell'esempio di comando precedente, esiste solo un listener HTTP, quindi, è necessario configurare un listener HTTPS. Per abilitare il listener HTTPS, nel caso non sia configurato:
  - Utilizzando PowerShell, creare un certificato autofirmato:

    New-SelfSignedCertificate -DnsName "myHost@myBusiness.com" -CertStoreLocation Cert:\LocalMachine\My

    > Sostituire il valore DnsName **(myHost@myBusiness.com)**, nell'esempio riportato sopra, con il nome dominio completo Windows del server Windows.

  - Salvare l'identificazione personale del certificato per la fase successiva



- Creare il listener HTTPS:

  winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="myHost@myBusiness.com"; CertificateThumbprint="[COPIED_CERTIFICATE_THUMBPRINT]"}

- Controllare per verificare che HTTPS ora sia configurato:
  winrm enumerate winrm/config/listener
- Modificare il firewall Windows per consentire connessioni remote in entrata a WINRM:
  - Andare a **Pannello di controllo → Sistema e sicurezza → Windows Firewall**
  - Fare clic su **Impostazioni avanzate.** Verrà visualizzata la finestra **Windows Firewall con sicurezza avanzata**.
  - Fare clic su **Regole in entrata**.
  - Selezionare il menu **Azioni** e fare clic su **Nuova regola**. Viene visualizzata la **Creazione guidata nuova regola connessioni in entrata.**
  - Selezionare **Porta** e fare clic su **Avanti.**
  - Selezionare **TCP → Porte locali specifiche:** e specificare 5986. Fare clic su **Avanti.**
  - Selezionare l'opzione **Consenti la connessione** e fare clic su **Avanti.**
  - Selezionare le caselle di spunta **Dominio**, **Privato** e **Pubblico**, se non sono già selezionate e fare clic su **Avanti.**
  - Assegnare alla nuova regola un nome (ad esempio, Windows Remote Management (HTTPS-In) e fare clic su **Fine.**

Note legali

IBM Corporation
Marketing Communications
Systems and Technology Group
Route 100
Somers, New York 10589
Prodotto negli Stati Uniti
Agosto 2020.

Questo documento è stato elaborato per prodotti e/o servizi offerti negli Stati Uniti. È possibile che IBM non metta a disposizione i prodotti, i dispositivi o i servizi illustrati in questo documento in altri paesi.

Le informazioni potranno subire modifiche senza preavviso. Rivolgersi al contatto commerciale IBM locale per informazioni sui prodotti, i dispositivi e i servizi disponibili nella propria area.

Tutte le dichiarazioni relative a futuri orientamenti e intenti di IBM sono soggette a modifica o ritiro senza preavviso e indicano solo finalità e obiettivi.

IBM, il logo IBM, POWER, System I, System p, i5/OS sono marchi o marchi registrati di International Business Machines Corporation negli Stati Uniti e/o in altri paesi. Un elenco completo dei marchi di proprietà di IBM negli Stati Uniti è reperibile all'indirizzo http://www.ibm.com/legal/copytrade.shtml.

Altri nomi di società, prodotti e servizi possono essere marchi o marchi di servizio di altri.

I prodotti hardware IBM sono fabbricati con parti nuove o parti nuove e usate. Indipendentemente da ciò, sono comunque valide le condizioni della garanzia.

Questa apparecchiatura è soggetta alle regole FCC. Risulterà conforme alle regole FCC appropriate prima della consegna finale all'acquirente.

Informazioni riguardanti i prodotti non IBM sono state ottenute dai fornitori di questi prodotti.

Domande sulle funzionalità dei prodotti non IBM dovrebbero essere rivolte ai relativi fornitori.

L'indirizzo dell'home page di IBM in Internet è http://www.ibm.com.

L'indirizzo dell'home page di IBM System p in Internet è http://www.ibm.com/systems/p.

L'indirizzo dell'home page di IBM System I in Internet è http://www.ibm.com/systems/i.

PSW03007-ITIT-00